



UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

ESCUELA DE POSTGRADO

PROGRAMA DE MAESTRÍA EN CIBERSEGURIDAD Y GESTIÓN DE LA INFORMACIÓN

Marco De Trabajo para Diseñar una Solución de Gobierno de Ciberseguridad Industrial

TRABAJO DE INVESTIGACIÓN

Presentado como parte de los requisitos para optar el grado académico de Maestro en
Ciberseguridad y Gestión de la Información

AUTOR(ES)

Guarda Higginson, Ernesto	0000-0003-4522-5695
Medina Burga, Cristhian Constantino	0000-0001-9226-0640
Vadillo Vidal, Christian Edward	0000-0002-2637-3118

ASESOR(ES)

Castillo Debarbieri, Milagros Cecilia	0000-0003-1361-5285
---------------------------------------	---------------------

Lima, 24 de marzo de 2023

Dedicatoria

A nuestros seres queridos que nos han brindado su apoyo en tiempo, sabiduría y afecto impulsándonos a ser mejores personas y profesionales.

Agradecimientos

A nuestros profesores, colegas y amigos que nos brindaron su conocimiento, orientación y experiencia.

A nuestros asesores, gracias por su guía y consejos constantes.

Resumen

En el presente estudio se desarrolla un marco de trabajo que brinda una solución de gobierno de ciberseguridad industrial personalizada a las necesidades particulares de las empresas. Se abordan los problemas que se derivan de la carencia de lineamientos estandarizados en materia de gobierno de ciberseguridad para las empresas del sector industrial, el análisis de investigaciones previas, el desarrollo del artefacto y la validación de este.

Mediante una adaptación de un marco que ofrece lineamientos para crear gobierno y estándares de ciberseguridad industrial se crean los factores necesarios para desarrollar el artefacto del estudio.

Finalmente se realiza la validación del artefacto a través de una herramienta creada en base a los lineamientos resultantes de las fases planteadas en la metodología de la investigación utilizada en el estudio.

Palabras clave: gobierno, diseño, ciberseguridad, sector industrial, IACS

Framework for Designing an Industrial Cybersecurity Governance Solution

Abstract

In this study, a framework is developed that provides an industrial cybersecurity governance solution customized to the particular needs of companies. The problems arising from the lack of standardized guidelines in cybersecurity governance for companies in the industrial sector, the analysis of previous research, the development of the artifact and its validation are addressed.

Through an adaptation of a framework that offers guidelines to create government and industrial cybersecurity standards, the necessary factors are created to develop the study artifact.

Finally, the validation of the artifact is carried out through a tool created based on the guidelines resulting from the phases proposed in the research methodology used in the study.

Keywords: government, design, cybersecurity, industrial sector, IACS

e202010663_Ernesto Guarda Higginson_Marco De Trabajo para Diseñar una Solución de Gobierno de Ciberseguridad Industrial

INFORME DE ORIGINALIDAD



FUENTES PRIMARIAS

1	repositorio.ucr.ac.cr Fuente de Internet	4%
2	vbook.pub Fuente de Internet	3%
3	vsip.info Fuente de Internet	1%
4	upc.aws.openrepository.com Fuente de Internet	1%
5	repositorioacademico.upc.edu.pe Fuente de Internet	1%
6	Submitted to Centro Europeo de Postgrado - CEUPE Trabajo del estudiante	1%
7	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	1%
8	repositorio.espe.edu.ec	

Tabla de Contenido

Lista de Tablas.....	10
Lista de Figuras	12
1.1. Antecedentes	13
1.2. Problemática	14
<i>1.1.1 Preguntas de investigación</i>	15
<i>1.1.2 Identificar la importancia del estudio</i>	15
<i>1.1.3 Objetivo general</i>	17
<i>1.1.4 Objetivos específicos</i>	17
1.3. Alcance y limitaciones	18
1.4. Justificación y viabilidad	18
Capítulo II. Marco conceptual	19
2.1 Bases teóricas	20
2.2 Investigaciones	20
2.3 Marco conceptual	21
<i>2.3.1 Conceptos</i>	21
<i>2.3.2 Estándares</i>	24
Capítulo III. Estado del Arte	27
3.1 Revisión sistemática de la literatura	27
<i>3.1.1 Búsqueda de palabras clave</i>	27
<i>3.1.2 Preguntas de investigación</i>	28
<i>3.1.3 Estrategia y procesos de búsqueda</i>	28
<i>3.1.4 Selección de artículos para el diseño</i>	29
<i>3.1.5 Matriz del conocimiento</i>	30
3.2 Estado del arte	34
<i>3.2.1 Planificación</i>	34
<i>3.2.2 Desarrollo</i>	35
3.3 Resultados	46
<i>3.3.1 Aspectos cubiertos</i>	46
<i>3.3.2 Actividades</i>	47
Capítulo IV. Metodología de Investigación	49
4.1 Metodología	49
<i>4.1.1 Definir objetivos:</i>	49
<i>4.1.2 Diseñar y desarrollar:</i>	50

4.1.3	<i> Demostrar:</i>	50
4.1.4	<i> Evaluar:</i>	50
4.1.5	<i> Comunicar:</i>	50
4.2	 Hoja de ruta para el desarrollo del artefacto	50
4.2.1	<i> Definición del problema y motivación</i>	50
4.2.2	<i> Definición de los objetivos</i>	51
4.2.3	<i> Definición del artefacto</i>	51
4.2.4	<i> Definición de las métricas</i>	53
4.2.5	<i> Evaluación del artefacto</i>	54
Capítulo V. Desarrollo del Artefacto		55
5.1	 Componentes del artefacto.	55
5.1.1	<i> Estrategia empresarial:</i>	59
5.1.2	<i> Metas empresariales:</i>	60
5.1.3	<i> Perfil de riesgo:</i>	61
5.1.4	<i> Problemas relacionados con la ciberseguridad industrial:</i>	64
5.1.5	<i> Escenarios de amenazas:</i>	66
5.1.6	<i> Requisitos de cumplimiento:</i>	66
5.1.7	<i> Rol de ciberseguridad:</i>	66
5.1.8	<i> Modelo de compra de proveedores para ciberseguridad industrial:</i>	67
5.1.9	<i> Estrategia de adopción de tecnología:</i>	68
5.1.10	<i> Requisitos de ciberseguridad:</i>	68
5.2	 Fases de la implementación	70
5.2.1	<i> Análisis de artículos de investigación</i>	70
5.2.2	<i> Benchmarking de estándares aplicables al sector industrial</i>	70
5.2.3	<i> Adaptación de COBIT a ciberseguridad industrial en base a ISA/IEC 62443-2-1</i>	71
5.2.4	<i> Creación de los factores de diseño</i>	71
5.2.5	<i> Ejecución del marco de trabajo</i>	88
Capítulo VI. Protocolo de Validación		90
6.1	 Proceso de validación del artefacto	90
6.1.1	<i> Estrategia empresarial:</i>	90
6.1.2	<i> Metas empresariales:</i>	90
6.1.3	<i> Perfil de riesgo:</i>	91
6.1.4	<i> Problemas relacionados con la ciberseguridad</i>	92
6.1.5	<i> Escenario de amenazas</i>	92
6.1.6	<i> Requisitos de cumplimiento</i>	92

6.1.7	<i>Rol de la ciberseguridad</i>	93
6.1.8	<i>Modelo de abastecimiento</i>	93
6.1.9	<i>Estrategia de adopción tecnológica</i>	93
6.2	Resultados de la validación	94
6.2.1	<i>Estrategia empresarial:</i>	94
6.2.2	<i>Metas empresariales:</i>	95
6.2.3	<i>Perfil de riesgo:</i>	97
6.2.4	<i>Problemas relacionados con la ciberseguridad:</i>	98
6.2.5	<i>Escenario de amenazas:</i>	100
6.2.6	<i>Requisitos de cumplimiento:</i>	101
6.2.7	<i>Rol de la ciberseguridad</i>	103
6.2.8	<i>Modelo de abastecimiento:</i>	104
6.2.9	<i>Estrategia de adopción tecnológica</i>	105
Capítulo VII. Conclusiones y Recomendaciones		109
7.1	Conclusiones	109
7.2	Recomendaciones	110
Referencias		111

Lista de Tablas

Tabla 1 <i>Criterios de inclusión y exclusión de artículos de investigación</i>	29
Tabla 2 <i>Matriz de conocimiento</i>	30
Tabla 3 <i>Artículos científicos seleccionados para el estudio</i>	34
Tabla 4 <i>Contribución de artículos de investigación</i>	46
Tabla 5 <i>Referencias de investigación</i>	47
Tabla 6 <i>Objetivos de gobierno y gestión</i>	55
Tabla 7 <i>Factor de diseño: Estrategia empresarial</i>	60
Tabla 8 <i>Factor de diseño: Metas empresariales</i>	60
Tabla 9 <i>Factor de diseño: Perfil de riesgo</i>	61
Tabla 10 <i>Factor de diseño: Problemas relacionados con la ciberseguridad industrial</i>	65
Tabla 11 <i>Factor de diseño: Escenario de amenazas</i>	66
Tabla 12 <i>Factor de diseño: Requisitos de cumplimiento</i>	66
Tabla 13 <i>Factor de diseño: Rol de Ciberseguridad</i>	67
Tabla 14 <i>Factor de diseño: Modelo de abastecimiento de proveedores para ciberseguridad industrial</i>	67
Tabla 15 <i>Factor de diseño: Estrategias de adopción de tecnología</i>	68
Tabla 16 <i>Requisitos de ciberseguridad</i>	69
Tabla 17 <i>Tabla asignación Factor de diseño 1</i>	72
Tabla 18 <i>Tabla puntuación de Metas empresariales y de alineamiento</i>	74
Tabla 19 <i>Tabla de puntuación Factor de Diseño 2</i>	75
Tabla 20 <i>Tabla de puntuación Factor de diseño 3</i>	77
Tabla 21 <i>Tabla puntuación Factor de diseño 4</i>	79
Tabla 22 <i>Tabla puntuación Factor de diseño 5</i>	81
Tabla 23 <i>Tabla de puntuación Factor diseño 6</i>	83
Tabla 24 <i>Tabla puntuación Factor de diseño 7</i>	84
Tabla 25 <i>Tabla puntuación Factor de diseño 8</i>	85
Tabla 26 <i>Tabla de puntuación de Factor de diseño 9</i>	87
Tabla 27 <i>Niveles de prioridad de estrategias empresariales</i>	90
Tabla 28 <i>Niveles de prioridad de metas empresariales</i>	91
Tabla 29 <i>Mapa de calor de la matriz de riesgo</i>	91
Tabla 30 <i>Relación impacto / riesgo</i>	91
Tabla 31 <i>Medición nivel existencia de problema</i>	92

Tabla 32 <i>Niveles de Rol de Ciberseguridad</i>	93
Tabla 33 <i>Objetivos priorizados por cada empresa</i>	107
Tabla 34 <i>Definición de controles Empresa 1 Hidrocarburos</i>	107
Tabla 35 <i>Definición de controles Empresa 2 Cementera</i>	108
Tabla 36 <i>Definición de controles Empresa 3 Minera</i>	108

Lista de Figuras

Figura 1 <i>Preparación para afrontar un incidente de ciberseguridad</i>	14
Figura 2 <i>Evolución de avisos por sector</i>	15
Figura 3 <i>Marcos de investigación</i>	17
Figura 4 <i>Modelo Core de COBIT 2019</i>	25
Figura 5 <i>Marco de ciberseguridad IEC 62443</i>	26
Figura 6 <i>Diversidad de atributos de ciberseguridad SIS en el sector de petróleo y gas en alta mar</i>	39
Figura 7 <i>Algunos elementos principales hacia una estrategia holística de ciberseguridad</i> ..	40
Figura 8 <i>Marcos de investigación</i>	44
Figura 9 <i>Marco clave de CPS</i>	45
Figura 10 <i>Derivación del marco CPS</i>	46
Figura 11 <i>Factores de diseño COBIT adaptado</i>	48
Figura 12 <i>Marco de trabajo IEC 62443</i>	48
Figura 13 <i>Representación gráfica del marco de trabajo</i>	53
Figura 14 <i>FD1 Empresa 1 Hidrocarburos</i>	94
Figura 15 <i>FD1 Empresa 2 Cementera</i>	94
Figura 16 <i>FD 1 Empresa 3 Minera</i>	95
Figura 17 <i>FD2 Empresa 1 Hidrocarburos</i>	95
Figura 18 <i>FD2 Empresa 2 Cementera</i>	96
Figura 19 <i>FD2 Empresa 3 Minera</i>	96
Figura 20 <i>FD3 Empresa 1 Hidrocarburos</i>	97
Figura 21 <i>FD3 Empresa 2 Cementera</i>	97
Figura 22 <i>FD3 Empresa 3 Minera</i>	98
Figura 23 <i>FD4 Empresa 1 Hidrocarburos</i>	99
Figura 24 <i>FD4 Empresa 2 Cementera</i>	99
Figura 25 <i>FD4 Empresa 3 Minera</i>	99
Figura 26 <i>FD5 Empresa 1 Hidrocarburos</i>	100
Figura 27 <i>FD5 Empresa 2 Cementera</i>	101
Figura 28 <i>FD5 Empresa 3 Minera</i>	101
Figura 29 <i>FD6 Empresa 1 Hidrocarburos</i>	101
Figura 30 <i>FD6 Empresa 2 Cementera</i>	102
Figura 31 <i>FD6 Empresa 3 Minera</i>	102
Figura 32 <i>FD7 Empresa 1 Hidrocarburos</i>	103
Figura 33 <i>FD7 Empresa 2 Cementera</i>	103
Figura 34 <i>FD7 Empresa 3 Minera</i>	103
Figura 35 <i>FD8 Empresa 1 Hidrocarburos</i>	104
Figura 36 <i>FD8 Empresa 2 Cementera</i>	105
Figura 37 <i>FD8 Empresa 3 Minera</i>	105
Figura 38 <i>FD9 Empresa 1 Hidrocarburos</i>	105
Figura 39 <i>FD9 Empresa 2 Cementera</i>	106
Figura 40 <i>FD9 Empresa 3 Minera</i>	106

Capítulo I: Problemática

1.1. Antecedentes

Mediante la investigación realizada se ha encontrado antecedentes que muestran la necesidad de lineamientos de gobierno de ciberseguridad industrial.

En este momento, las políticas de privacidad, las normas técnicas y los procedimientos de implementación en los niveles local, regional/estatal, nacional e internacional a menudo son inconsistentes. Esto abre la puerta a importantes riesgos de ciberseguridad y privacidad en la red eléctrica que deben gestionarse (Brown et al., 2018).

Entre los atributos principales relacionados con la ciberseguridad están los estándares rectores y marcos regulatorios, indican que se requiere un esfuerzo para mejorar las prácticas actuales y los niveles de desempeño considerando la carencia de un enfoque claro, eficaz e integrado para la práctica de seguridad. En este sentido en su estudio proponen unos pasos estratégicos para desarrollar un marco más holístico para gestionar la ciberseguridad en un contexto industrial dinámico y complejo que está sometido a los rápidos esfuerzos de digitalización (Zhu & Liyanage, 2021).

Los problemas de seguridad de la información deben abordarse a fondo y, por lo tanto, las soluciones a estos problemas no pueden ser unilaterales o limitadas. Argumentan que un marco de trabajo de seguridad debe ser completo e integrado para poder lograr el objetivo de un sistema. Crean su propio marco de trabajo con la idea de que se convierta en un referente para el problema que estudian en su investigación. Además, indican que cada sector debe coordinarse entre sí para la gobernanza y la seguridad de las infraestructuras críticas nacionales (Setiawan et al., 2016).

Fraile, R (n.d.) señaló en un informe para el diario peruano Gestión que, sin lineamientos claros sobre cómo proteger la infraestructura crítica en el sector energético, son blancos fáciles para el cibercrimen. Por eso, entender y reconocer esta realidad es clave para

entender cuándo invertir, cómo generar estrategias de prevención, detección, colaboración y cómo responder a los ciberataques.

1.2. Problemática

Existen diversas fuentes de información que permiten definir de manera concreta la realidad de la ciberseguridad en el sector, por ejemplo:

En un informe de Delloite, Lara et al. (2019) mostraron que las dos industrias con más accidentes confirmados fueron energía y recursos, que supuso el 41,67 % del total de accidentes, y consumo y distribución supuso el 16,67 % del total de accidentes.

Menos del 50% de las empresas de energía y recursos se sienten preparadas para enfrentar incidentes de seguridad. Este es un hecho muy destacable ya que es uno de los sectores clave y estratégicos de cualquier país.

Figura 1

Preparación para afrontar un incidente de ciberseguridad



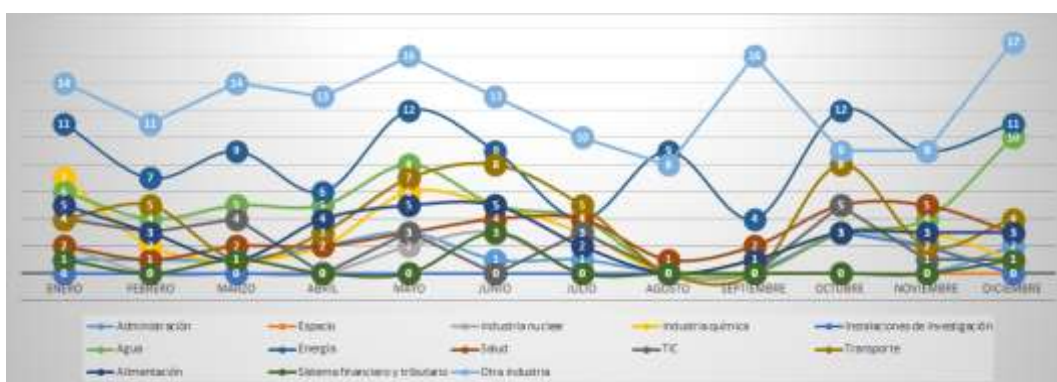
Nota. La infografía muestra el nivel de preparación de las empresas para afrontar un incidente de ciberseguridad del sector energía y recursos. De “*Las preocupaciones del CISO El estado de la ciberseguridad en el 2019.*”, por Lara et al., 2019.

En un estudio realizado por el INCIBE-CERT en 2019 indica que la industria más atacada es el sector energético, eso debido a muchos factores, por ejemplo, los beneficios económicos que los ciberdelincuentes obtienen como rescates para liberar el control de

infraestructuras críticas o devolver la información privada, el impacto que puede tener en un país en el que se paralicen las infraestructuras críticas de la nación puede ser dañino en muchos aspectos.

Figura 2

Evolución de avisos por sector



Nota. Seguridad Industrial 2019 En Cifras | INCIBE-CERT, (n.d.). Evolución de avisos por sector. Recuperado de <https://www.incibe-cert.es/blog/seguridad-industrial-2019-cifras>

1.1.1 Preguntas de investigación

Con base en los antecedentes y la problemática planteamos las siguientes preguntas:

- ¿Cuáles son los estándares y marcos de trabajo que se utilizan para diseñar soluciones de **gobierno de ciberseguridad**?
- ¿Qué tipos de problemas se abordan en la ciberseguridad industrial?
- ¿Qué problemas se desencadenan por un gobierno deficiente?
- ¿Cómo se abordan los problemas relacionados a gobierno de **ciberseguridad**?

1.1.2 Identificar la importancia del estudio

La Cuarta Revolución Industrial o también conocida como "Industria 4.0" es una tendencia en la automatización y el intercambio de datos en el marco de las tecnologías actuales, incluyendo especialmente los sistemas ciber físicos, Internet de las Cosas (IoT) y la

computación en la nube. En el sector industrial tales tecnologías se van incorporando cada vez más y a una mayor velocidad, pero estas cuentan con inherentes riesgos de ciberseguridad que de no ser abordados adecuadamente implican un gran riesgo para la empresa y los abonados de los servicios de las mismas.

El objetivo del estudio es ofrecer lineamientos estructurados para diseñar soluciones de gobierno de ciberseguridad con la finalidad que las empresas del sector industrial cuenten con bases priorizadas según su necesidad particular y el estado actual en el que se encuentre la ciberseguridad.

Este marco de trabajo les permitirá a las empresas del sector industrial contar con objetivos priorizados alineados a su estado actual y los controles que debe ser abordados para poder alcanzar un nivel de seguridad basado en estándares aplicables en la industria.

El estudio tiene por finalidad brindar factores de diseño estructurados y alineados al sector industrial particularmente, esto es logrado mediante la síntesis y adecuación de estándares y buenas prácticas de ciberseguridad que son aplicados en diversos sectores con el objetivo diseñar la solución de gobierno adecuada para la empresa.

Debido a los estándares investigados en el estudio se puede correlacionar el marco de trabajo puede vincularse a otros estándares, marcos y buenas prácticas, permitiendo el diseño de soluciones en gobierno de ciberseguridad enfocadas al sector industrial y los controles necesarios para alcanzar un cierto nivel de seguridad. En función de sus necesidades, garantice la seguridad asignando valores que le permitan medir los requisitos de seguridad del entorno y la red de su empresa.

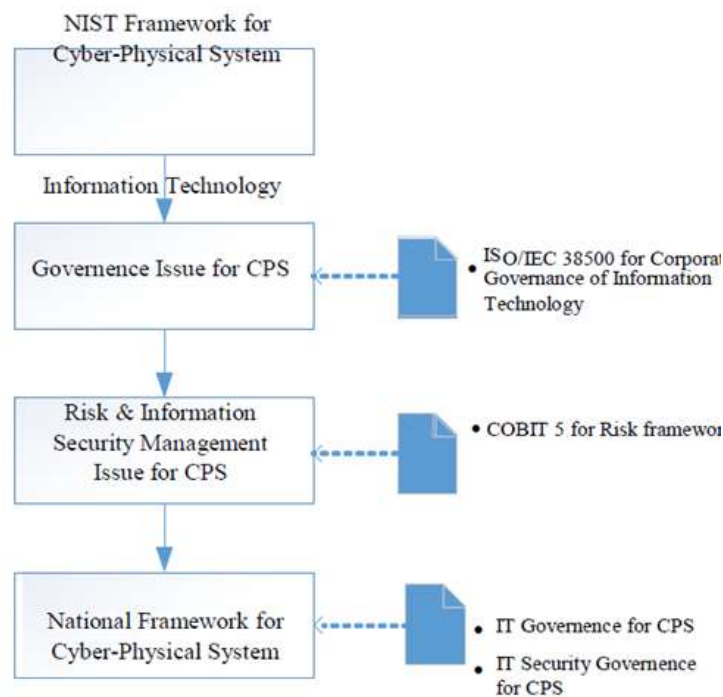
1.1.2.1 Datos preliminares

En los hallazgos obtenidos mediante el estado del arte los investigadores desarrollaban marcos de trabajo específicos para el problema que deseaban resolver, entre los más destacados y orientados a ciberseguridad industrial utilizaban estándares que les permitían obtener

lineamientos estructurados para abordar los problemas que investigaban, los utilizados con mayor frecuencia fueron COBIT, NIST, IEC, ISO 27001 por mencionar algunos.

Figura 3

Marcos de investigación



Nota. La infografía muestra los estándares utilizados para crear el marco de ciberseguridad. De. "Research Framework. Recuperado", por Setiawan et al., 2016

1.1.3 Objetivo general

Para fines de este estudio planteamos el siguiente objetivo general:

- Desarrollar un marco de trabajo para diseñar una solución de gobierno de ciberseguridad industrial.

1.1.4 Objetivos específicos

Para cumplir el objetivo general planteamos los siguientes objetivos específicos:

Analizar los estándares y buenas prácticas de ciberseguridad aplicables al sector industrial.

- I. Crear factores de diseño que permitan el diseño de soluciones de gobierno de la ciberseguridad industrial.

II. Evaluar la efectividad de marco de trabajo en una empresa del sector industrial.

1.3. Alcance y limitaciones

En el presente estudio nos enfocamos en el diseño de una solución de gobierno de ciberseguridad del sector industrial y la relación que guarda con la gestión de riesgo y vulnerabilidades de las tecnologías (IT y OT) utilizadas en esta industria.

1.4. Justificación y viabilidad

La importancia de contar con lineamientos para abordar la ciberseguridad industrial, según la investigación realizada, es una parte crucial de la solución, la ausencia o deficiencia de ellos puede conllevar a dejar vulnerabilidades sin remediar, realizar inversiones erróneas, evitar el cumplimiento de las regulaciones nacionales que podrían derivar en sanciones. En base a los estudios analizados, los investigadores proponían marcos de trabajo para solucionar los problemas particulares que estudiaban, los equipos que plantean soluciones están conformados por expertos en ciberseguridad multidisciplinarios lo cual permitía desarrollar soluciones holísticas y estructuradas basados en la combinación de estándares que podían ser adaptados al sector estudiado.

Capítulo II. Marco conceptual

En la actualidad las amenazas cibernéticas tienen múltiples maneras de ingresar en las organizaciones, ya sea por un empleado que maneja información a través de dispositivos extraíbles, correos, aplicaciones o incluso sistemas desarrollados internamente.

En esta época de pandemia por el COVID-19 se volvió mucho más común y evidente debido al trabajo remoto o trabajo desde casa el cual permite que el personal se conecte a los equipos en las organizaciones a través de internet, en una encuesta realizada por la ISIL tomando como muestra cerca de 250 empresas en el Perú cerca del 89% de su fuerza laboral ya se encontraba trabajando de manera remota y en dicha encuesta también demostraba que la mayoría de empresas no estaba preparada para implementar la modalidad de trabajo remoto. Esto ha implicado un crecimiento del 242% en ataques cibernéticos en los múltiples sectores organizacionales, entre ellos los sectores de energía y recursos, así como el de consumo y distribución han sido unos de los más afectados con un 41.67% y un 16.67% respecto al total de incidencias (Trabajo Remoto En Perú: Tendencias y Estadísticas, n.d.).

Se ha llegado a una nueva era de ciber crimen en la cual se realizan ataques dirigidos a las organizaciones con el fin de ocasionar daño. Por lo cual la seguridad requiere el compromiso de la alta dirección y esto es lo que define las bases para un sistema de gobierno en ciberseguridad el cual representara un conjunto de responsabilidades y practicas ejercida por los responsables correspondientes. De acuerdo a los marcos de ciberseguridad publicados, se verifica que su base está orientado en seguridad de la información pero en sectores de servicios lo que implica que dichos marcos solo cubran parte de las necesidades de organizaciones de otros sectores por ello se plantea desarrollar un marco para sistemas de gobierno en ciberseguridad para el sector industrial lo que permitirá a las organizaciones de este sector, independientes de su tamaño, grados de riesgo o tipos de contramedidas ante amenazas

externas, aplicar las mejores prácticas para la gestión de riesgos y permita optimizar de manera continua la seguridad de sus infraestructuras.

2.1 Bases teóricas

A continuación, se presentan las bases teóricas que sustentan la investigación sobre el desarrollo de un marco de trabajo para sistemas de gobierno de ciberseguridad industrial destinadas a organizaciones del sector como método para crear o afianzar un sistema de gobierno.

El estudio se relaciona con los múltiples estándares aplicables al sector industrial, como COBIT 2019, ISA/IEC 62443-1-1, ISA/IEC 62443-2-1 e ISA/IEC 62443-3-3 las cuales especifican un conjunto de conceptos, componentes y controles que son valorados como medios para mejorar los procesos internos frente a la ciberseguridad en las organizaciones. En ese sentido se ha tomado en consideración informes emitidos sobre el estado actual del sector, así como las deficiencias que brindan un sistema de gobierno mal implementado. En un informe realizado por Deloitte, Lara et al. (2019) se menciona que los sectores que presentan mayor cantidad de incidencias son los de energía, esto se refuerza con los informes de INCIBE – CERT (n.d.) el cual muestra que el sector energético es uno de los más afectados, ya que vulneran y afectan infraestructuras críticas o también realizan el robo información privada. Esto representa un gran impacto socioeconómico de un país ya que puede paralizar las infraestructuras críticas de la nación. Por ello este marco tiene como objetivo el desarrollo del marco de gobierno en este sector para mitigar y optimizar los procesos internos de dichas organizaciones.

2.2 Investigaciones

De la revisión de las investigaciones, se evidencia que existe poca referencia específica sobre gobierno de ciberseguridad para el sector industrial, existiendo mayor referencia para los

sectores de banca, seguros y energía eléctrica siendo en mucho de los casos que existen normas legales y regulaciones.

Es así, que los autores Brown, Zhou y Ahmadi en su trabajo de investigación “Smart grid governance: An international review of evolving policy issues and innovations” hacen referencia en su publicación sobre la necesidad de hacer una revisión de las políticas en materia de ciberseguridad en vista que las empresas industriales se encuentran integrando tecnologías exponiendo sus operaciones a ataques.

Además, de la revisión de la investigación de Zhu y P. Liyanage, “Cybersecurity of Offshore Oil and Gas Production Assets Under Trending Asset Digitalization Contexts - A Specific Review of Issues and Challenges in Safety Instrumented Systems” se infiere que, las empresas de la industria de hidrocarburos cuentan con sistemas de gestión de seguridad funcional, y en algunos casos cuentan con sistemas de gestión de ciberseguridad, pero están separados, lo que los hace ni efectivos ni eficientes.

2.3 Marco conceptual

2.3.1 Conceptos

Ciberseguridad. – Proteger los activos de información abordando las amenazas que ponen en riesgo la información procesada, almacenada y transmitida por los sistemas de información interconectados.

Marco de trabajo. – Es un conjunto de conceptos, prácticas y reglas para tratar una determinada clase de problemas para referenciar, descubrir y resolver nuevos problemas de la misma naturaleza.

IACS. – (*Industrial Automation and Control System*) Es el sistema de recolección o control de la automatización industrial.

ISA. – (*International Society of Automation*) Es una asociación profesional sin fines de lucro compuesta por ingenieros, técnicos y directivos dedicados a la automatización industrial.

IEC. – (*International Electrotechnical Commission*) Es una organización internacional de estándares que formula y publica estándares internacionales para todas las tecnologías eléctricas, electrónicas y relacionadas, denominadas colectivamente "electrotecnología".

COBIT. – (*Control Objectives for Information and Related Technologies*) Es un marco para el gobierno y la gestión de la tecnología de la información corporativa en toda la empresa.

INCIBE. – (Instituto Nacional de Ciberseguridad de España) Es una sociedad mercantil estatal y medios de comunicación propios, una sociedad anónima propiedad del Ministerio de Asuntos Económicos y Transformación Digital de España a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial.

CERT. – (*Computer Emergency Response Team*) Que es el centro de respuesta para incidentes de seguridad en el campo de la tecnología de la información.

IoT. – (*Internet of Things*) Describe los sensores, el poder de procesamiento, el software y otras tecnologías que permiten que los objetos físicos se conecten e intercambien datos con otros dispositivos y sistemas a través de Internet u otras redes de comunicación.

NIST. – (*National Institute of Standards and Technology*) Es un laboratorio de ciencias físicas y una agencia no reguladora del Departamento de Comercio de los Estados Unidos.

ISO. – (*International Organization for Standardization*) Es una organización internacional de normalización compuesta por representantes de las organizaciones nacionales de normalización de sus países miembros.

IT. – (*Information technology*) La abreviatura en inglés de Tecnología de la Información.

OT. – (*Operational technology*) La abreviatura en inglés de Tecnologías de la operación.

ISACA. – Una asociación global que brinda a los profesionales de TI conocimientos, certificaciones, capacitación y comunidad en auditoría, gobierno, riesgo, privacidad y ciberseguridad.

SIS. – (*Safety instrumented system*) La abreviatura en inglés de Sistema instrumentado de seguridad.

CPS. – (*Cyber Physical System*) La abreviatura en inglés de Sistema ciberfísico.

FAT. – (*Factory Acceptance Test*) La abreviatura en inglés de Prueba de aceptación en fábrica.

SAT. – (*Site Acceptance Test*) La abreviatura en inglés de Prueba de aceptación del sitio.

SCADA. – (*Supervisory control and data acquisition*) La abreviatura en inglés de Control de supervisión y Adquisición de Datos.

PLC. – (*Programmable logic controller*) La abreviatura en inglés de Controlador lógico programable.

DCS. – (*Distributed control system*) La abreviatura en inglés de Sistema de control distribuido.

DoS. – (*Denial-of-Service*) La abreviatura en inglés de ataque de denegación de servicio, es un ataque a un sistema informático o red que hace que un servicio o recurso sea inaccesible para los usuarios legítimos.

RTU. – (*Remote terminal unit*) La abreviatura en inglés de Unidad terminal Remota.

SLA. – (*Service-level agreement*) La abreviatura en inglés de Acuerdo de nivel de servicio.

SL. – (*Security level*) La abreviatura en inglés de Nivel de seguridad.

FR. – (*Fundamental requirement*) La abreviatura en inglés de Requerimiento fundamental.

FFIEC. – (*Federal Financial Institutions Examination Council's*) La abreviatura en inglés de Consejo Federal de Examinación de Instituciones Financieras, es un organismo interinstitucional formal del gobierno de los EE. UU., que consta de cinco agencias de supervisión bancaria, con la autoridad para desarrollar principios, estándares y formatos de informes uniformes para promover la unificación de la supervisión de las instituciones financieras.

2.3.2 Estándares

Como parte del análisis previo realizado, el estudio utilizará como referencia COBIT 2019, ISA/IEC 62443-1-1, ISA/IEC 62443-2-1 e ISA/IEC 62443-3-3.

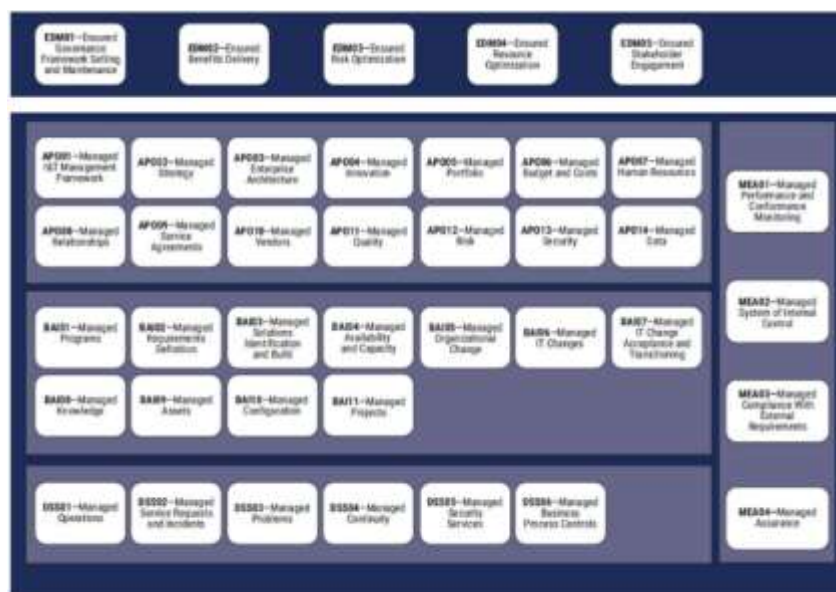
2.3.2.1 COBIT

COBIT 2019 ayuda a las organizaciones y/o empresas a establecer objetivos de TI tangibles que se alinean con las estrategias comerciales. Según ISACA (2018), el 73 % de las empresas que han adoptado el marco han visto mejoras en la forma en que funcionan sus negocios e integración de TI. Además, los profesionales de COBIT pueden establecer controles y herramientas para ayudar a los administradores de TI a lograr los objetivos de desempeño comercial esperados y maximizar el valor de los sistemas de información. Éstos incluyen:

- Modelo de madurez de COBIT: Ayuda a determinar el nivel de rendimiento que deben alcanzar los elementos de TI para cumplir los objetivos empresariales.
- Actividades de mejora: ISACA brinda asesoramiento sobre cómo identificar y eliminar problemas que limitan la capacidad de una organización para implementar el marco COBIT.

Figura 4

Modelo Core de COBIT 2019



Nota. La infografía muestra el modelo core de COBIT. De “*Guía de diseño COBIT 2019: Diseño de una solución de Gobierno de Información y Tecnología*”, por ISACA, 2018

2.3.2.2 IEC 62443

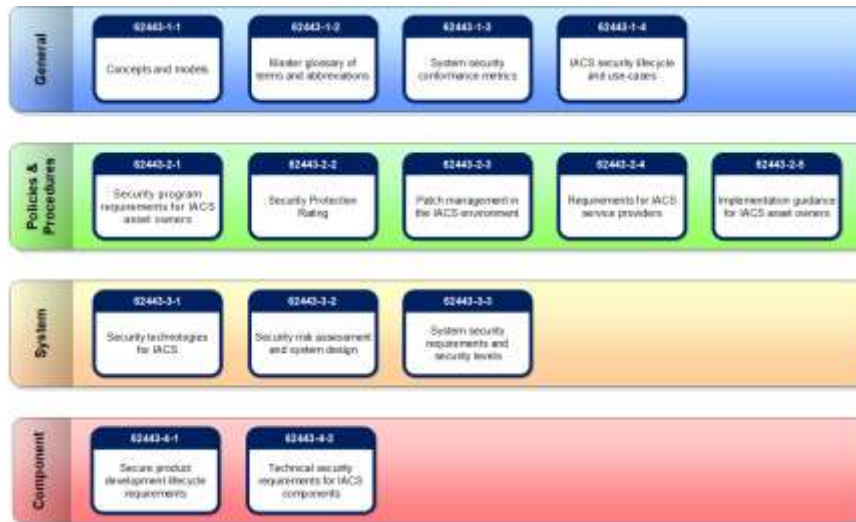
La IEC 62443 es una serie de estándares cuyo objetivo principal es facilitar el manejo de las vulnerabilidades de IACS en respuesta a ataques informáticos y tomar medidas para mitigarlos. Desde sus inicios, su propósito ha sido crear un vínculo entre la ciberseguridad y el IACS, definiendo un conjunto de requisitos mínimos para alcanzar niveles de seguridad cada vez más estrictos, contribuyendo así a mejorar la seguridad de los entornos industriales.

Se basa en conceptos previamente definidos por ISA-99, con orígenes que se remontan a 2002, año en que ISA (International Society of Automation) comenzó a abordar la necesidad de definir estándares de ciberseguridad industrial. Para alinear la nomenclatura ISA-99 con la

nomenclatura IEC (International Electrotechnical Commission), ISA-99 pasó a llamarse ISA-62443 en 2010 (ISA, 2007, 2009, 2013).

Figura 5

Marco de ciberseguridad IEC 62443



Nota. La infografía muestra el marco IEC 62433. De “*Work Products ANSI/ISA-62443-3-3 Security for Industrial Automation and Control Systems Part 3-3 System security requirements and security levels*”, por ISA, 2013

Capítulo III. Estado del Arte

Con la intención de crear un Marco de Trabajo para Diseñar una Solución de Gobierno de Ciberseguridad industrial se está realizando el actual trabajo de investigación. Teniendo ello como finalidad es que realizamos con detenimiento la identificación del problema y las causas que podrían ser sus causantes teniendo como finalidad plantear la solución adecuada. Posterior a la identificación del problema se ha procedido a realizar de manera sistemática la búsqueda de trabajos de investigación que nos permitan contar con bases teóricas y prácticas que apoyen a la solución a diseñar. Mediante las siguientes palabras claves “governance”, “issue” y “cybersecurity” se plantearon cuatro (4) preguntas de investigación. Se consultaron repositorios de artículos científicos tales como Scopus, IEEE Xplore, Web of Science, Springer y ACM, en ellos se utilizaron las palabras clave planteadas. Como indicador de pertinencia y calidad se eligieron los artículos de investigación que no superan los 5 años de antigüedad y que se encuentran en los cuartiles Q1 y Q2 según Scimago Journal & Country rank (Scimagojr).

3.1 Revisión sistemática de la literatura

3.1.1 *Búsqueda de palabras clave*

Las palabras claves que utilizamos para la búsqueda de los artículos científicos son los siguientes:

- “Governance”
- “Issue”
- “Cybersecurity”
- “Industrial”
- “Framework”
- “Oil and Gas”
- “Impact”

- “Risk”
- “Cost”

3.1.2 Preguntas de investigación

- ¿Cuáles son las buenas prácticas y marcos de trabajo utilizados para diseñar soluciones de **gobierno de ciberseguridad**?
- ¿Qué tipos de **problemas** se abordan en la **ciberseguridad** industrial?
- ¿Qué **problemas** se desencadenan por un **gobierno** deficiente?
- ¿Cómo son abordados los **problemas** relacionados a **gobierno** de ciberseguridad?

3.1.3 Estrategia y procesos de búsqueda

La metodología aplicada para la selección de artículos científicos relacionados al proyecto titulado Marco de Trabajo para Diseñar una Solución de Gobierno de Ciberseguridad Industrial, está dividida en tres fases:

- **Planificación:** Fase en la cual se elaboran las preguntas de investigación para realizar la búsqueda sistemática de artículos científicos afines al trabajo de investigación.
- **Desarrollo:** En esta fase se aplican los criterios inclusión y exclusión para la selección de los artículos y se procede a contestar las preguntas de investigación planteadas.
- **Resultados:** En la fase final se obtiene el análisis basado en la matriz del conocimiento de la investigación.

3.1.4 Selección de artículos para el diseño

3.1.4.1 Periodo

Los artículos que forman parte del estado del arte tienen como año de publicación entre el 2016 y 2021.

3.1.4.2 Criterios de inclusión y Exclusión

En la Tabla 1 se muestran los criterios de selección de los artículos.

Tabla 1

Criterios de inclusión y exclusión de artículos de investigación

Criterios de Inclusión	Criterios de Exclusión
Artículos publicados en revistas científicas y ponencias o trabajos presentados en congresos, simposios y eventos similares que indexen a Scopus, IEEE Xplore, Web of Science, Springer y ACM.	Artículos que se publicaron antes de la exclusión de 2016.
Estudios que presentan evidencias y aporte en la validación de la propuesta	Estudios que no incluyen discusiones del “objeto de estudio”
Artículos escritos en el idioma en inglés: Marcos de Trabajo, Modelos, Metodologías, Herramientas o Técnicas.	Los artículos científicos no están en inglés y utilizan referencias de estudio sin validación.

3.1.5 Matriz del conocimiento

Tabla 2

Matriz de conocimiento

Grupo de Investigación	Cuartil	Título	Autor	Año	Revista
Solución	Q1	A Security-Aware Framework for Designing Industrial Engineering Processes	Panagiotis Dedousis; George Stergiopoulos; George Arampatzis; Dimitris Gritzalis	2021	IEEE Access
	Q1	State-industry relations and cybersecurity governance in Europe	Antonio Calcara, Raffaele Marchetti	2021	REVIEW OF INTERNATIONAL POLITICAL ECONOMY
	Q1	A Survey of IIoT Protocols: A Measure of Vulnerability Risk Analysis Based on CVSS	Santiago Figueroa-Lorenzo, Javier Añorga, Saioa Arrizabalaga	2020	ACM Computing Surveys
	Q2	Analysis of Cyber Incident Categories Based on Losses	Jay P. Kesan, Linfeng Zhang	2020	ACM Transactions on Management Information Systems
	Q1	Information Security Governance on National Cyber Physical Systems	Ahmad Budi Setiawan, Aries Syamsudin, Ashwin Sasongko Sastrosubroto	2016	2016 International Conference on Information Technology Systems and Innovation
	Q1	Cybersecurity of Offshore Oil and Gas Production Assets Under Trending Asset Digitalization Contexts: A Specific Review of Issues and Challenges in Safety Instrumented Systems	Pengyu Zhu · Jayantha P. Liyanage	2021	Springer Natural - European Journal for Security Research
	Q2	Quantifying e-governance efficacy towards Indian-EU strategic dialogue	Soni Vivek, Anand Rashmi, Dey Prasanta Kumar, Dash Ambika Prasad, Banwet Devinder Kumar	2017	TRANSFORMING GOVERNMENT- PEOPLE PROCESS AND POLICY

Q2	Smart grid governance: An international review of evolving policy issues and innovations	Brown Marilyn A., Zhou Shan, Ahmadi Majid	2018	WILEY INTERDISCIPLINARY REVIEWS-ENERGY AND ENVIRONMENT
Q1	Assessing Cyberbiosecurity Vulnerabilities and Infrastructure Resilience	Schabacker Daniel S., Levy Leslie-Anne, Evans Nate J., Fowler Jennifer M., Dickey Ellen A.	2019	FRONTIERS IN BIOENGINEERING AND BIOTECHNOLOGY
Q1	Artificial intelligence for sustainability: Challenges, opportunities, and a research agenda	Nishant Rohit, Kennedy Mike, Corbett Jacqueline	2020	INTERNATIONAL JOURNAL OF INFORMATION MANAGEMENT
Q2	Machine Learning for Energy Systems	Sidorov Denis, Liu Fang, Sun Yonghui	2020	ENERGIES
Q1	Urgency in energy justice: Contestation and time in prospective shale extraction in the United States and United Kingdom	Partridge Tristan, Thomas Merryn, Pidgeon Nick, Harthorn Barbara Herr	2018	ENERGY RESEARCH & SOCIAL SCIENCE
Q1	A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities	Habibzadeh, Nussbaum, Anjornshoa, Kantarci, Soyota	2019	SUSTAINABLE CITIES AND SOCIETY
Q1	An urban ecology critique on the "Smart City" model	Colding Johan, Barthel Stephan	2017	JOURNAL OF CLEANER PRODUCTION
Q1	The Political Premises of Contemporary Urban Concepts: The Global City, the Sustainable City, the Resilient City, the Creative City, and the Smart City	Hatuka Tali, Rosen-Zvi Issachar, Birnhack, Michael, Toch, Eran, Zur, Hadas	2018	PLANNING THEORY & PRACTICE
Q1	Cybersecurity of Offshore Oil and Gas Production Assets Under Trending Asset Digitalization Contexts - A Specific Review of Issues and Challenges in Safety Instrumented Systems	Pengyu Zhu, Jayantha P.Liyanage	2021	European Journal for Security research

Problema	Q1	SCADA security issues and FPGA implementation of AES — A review	Amrik Singh;Ajay Prasad;Yoginder Talwar	2016	2016 2nd International Conference on Next Generation Computing Technologies
	Q1	Gaps and Opportunities in Situational Awareness for Cybersecurity	Robert Gutzwiller, Josiah Dykstra, Bryan Payne	2020	Digital Threats: Research and Practice
	Q1	Governance of Collaborative Networked Organisations: Stakeholder Requirements	Todor Tagarev	2020	The 11th IEEE International Conference on Dependable Systems, Services and Technologies
	Q1	Catch Me if You Can: An In-Depth Study of CVE Discovery Time and Inconsistencies for Managing Risks in Critical Infrastructures	Thomas R.J., Gardiner J., Chothia T., Samanis E., Perrett J., Rashid A.	2020	2020 Joint Workshop on CPS&IoT Security and Privacy
	Q2	The industrial internet of things: The evolution of automation in the oil and gas complex	Alguliyev, R.M., Fataliyev, T.Kh., Mehdiyev, Sh.A.	2019	SOCAR Proceedings
	Q1	Sustainable cybersecurity? Rethinking approaches to protecting energy infrastructure in the European High North	Cassotta, Sandra; Sidortsov, Roman	2019	ENERGY RESEARCH & SOCIAL SCIENCE
	Q1	Seeking Public Values of Digital Energy Platforms	Niet, Irene A., Dekker, Romy, van Est, Rinie	2021	SCIENCE TECHNOLOGY & HUMAN VALUES
	Q1	Editorial: Industrial Internet: Security, Architectures, and Technologies	Yang Q., Malekian R., Wang C., Rawat D.	2020	IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS
	Q1	Promises and limits of community-based organizations in bridging mismatches of scale: a case study on collaborative governance on federal lands	Lee Jean, Baggio Jacopo	2021	ECOLOGY AND SOCIETY

	Q1	A first look at social factors driving CCS perception in Brazil: A case study in the Reconcavo Basin	Netto Anna Luisa Abreu, Camara George, Rocha Expedito, Silva Aldo Luiz, Andrade Jose Celio Silveira, Peyerl Drielli, Rocha Paulo	2020	INTERNATIONAL JOURNAL OF GREENHOUSE GAS CONTROL
	Q1	Hedging, Investment Efficiency, and the Role of the Information Environment	Lobo, Ranasinghe, Yi	2020	JOURNAL OF ACCOUNTING AUDITING AND FINANCE
	Q1	Simulation for Cyber Risk Management – Where are we, and Where do we Want to Go?	Sachin Shetty; Indrajit Ray; Nurcin Ceilk; Michael Mesham; Nathaniel Bastian; Quanyan Zhu	2019	2019 Winter Simulation Conference
Técnica	Q1	Declining Arctic Ocean oil and gas developments: Opportunities to improve governance and environmental pollution control	Gulas Sarah, Downton Mitchell, D'Souza Kareina, Hayden Kelsey, Walker Tony R	2017	MARINE POLICY
	Q1	Oil Prices: Governance Failures and Geopolitical Consequences	Escribano Gonzalo, Valdes Javier	2017	GEOPOLITICS

3.2 Estado del arte

3.2.1 Planificación

Los artículos seleccionados, de acuerdo con las preguntas formuladas, fueron 29 como se visualiza en la Tabla 2:

Tabla 3

Artículos científicos seleccionados para el estudio

Question	Scopus	IEEE Explorer	Web of Science	ACM	Springer	Total
RQ1	0	3	6	0	0	9
RQ2	2	1	2	0	1	6
RQ3	0	0	6	1	0	7
RQ4	0	2	3	2	0	7

Los artículos resultados de la búsqueda sistemática fueron agrupados en tres (3) grupos: El primer grupo está formado por once (11) artículos relacionados con el problema y se describen como los riesgos de un gobierno de ciberseguridad ineficiente, las brechas a disminuir y el impacto que estas tienen en la industria. El segundo grupo formado por quince (15) artículos enfocados en las diversas soluciones creadas para mitigar el problema existente del gobierno de ciberseguridad. El grupo final formado por tres (3) artículos, están orientados en las técnicas que permitieron dar solución al problema encontrado y cómo fueron implementados en el sector industrial.

En la siguiente sección se presentará el resumen de cada artículo contestando las cuatro (4) preguntas de investigación planteadas y el aporte de los autores relacionado a cada pregunta, cual fue el proceso que emplearon para la resolución del problema que hacían frente.

3.2.2 *Desarrollo*

Pregunta 1: ¿Cuáles son las buenas prácticas y frameworks utilizados para implementar gobierno de ciberseguridad?

Artículo N° 15

Título:

Smart grid governance: An international review of evolving policy issues and innovations

Aporte:

Los autores Brown et al. (2018) plantean realizar una revisión internacional sobre las políticas e innovaciones en las redes inteligentes donde ponen el contexto de la evolución a nivel de transmisión y distribución de las redes eléctricas en su alcance económico y político, qué políticas y planes energéticos enfrenta el mundo ante el crecimiento rápido del consumo energético y la preocupación por el uso de renovables y generación mínima en la huella de carbono para impactar en lo menor posible al medio ambiente. Por ello, ante la necesidad de mejorar la eficiencia de consumo y brindar soluciones a nivel de usuario se vienen implementando tecnología, específicamente redes inteligentes, pero esto lleva a tener que preocuparnos por la ciberseguridad ya que se tienen evidencias de ciberataques a empresas del sector eléctrico llevando a afectar millones de usuarios y con pérdidas económicas que pueden llegar a los billones de dólares americanos.

Los autores realizaron el análisis de las políticas en Estados Unidos enfocándose en 6 tipos de políticas:

Políticas de medición de redes

- Estándares y reglas de interconexión
- Objetivos de medición inteligente

- Políticas de precios dinámicos
- Políticas de vehículos eléctricos
- Política de privacidad de datos y ciberseguridad

Asimismo, realizan el análisis de las políticas en Europa (Italia y Reino Unido), en Asia (Japón, Corea del Sur, República Popular de China e India) donde evalúan las políticas de privacidad de datos y ciberseguridad.

Luego de este análisis, realizan un análisis macro del mundo en desarrollo llevándolos a la conclusión que es necesario que estandarizar las políticas de acuerdo con las regulaciones de cada país y Estado, así como también impulsar el crecimiento de las redes promoviendo la inversión para hacer que sea más confiable y eficiente.

Proceso:

Definición de la muestra

Se adopta un enfoque de investigación inductivo. Es un análisis de distintas políticas de varios países, principalmente de países que son potencia y que cuentan con recursos suficientes y políticas bien definidas. En los países que están en desarrollo es necesario contar con políticas de apoyo para poder ejecutar el despliegue rápido de redes inteligentes y que cuenten con políticas de ciberseguridad. Con el análisis de las distintas políticas se puede identificar claramente cuáles son esas políticas que se deben de implementar y aprender de las experiencias asumiendo retos y desafíos.

Definición de mediciones para la muestra

La estrategia de investigación fue exploratoria donde pone en evidencia que es necesaria la introducción de regulaciones y políticas para las redes inteligentes y que sin estas no será posible lograr el despliegue de ellas y por ello enumera las distintas políticas que son necesarias para llegar a esta renovación tecnológica en el sector eléctrico.

Resultados:

Los autores hacen hincapié que es necesario contar con regulaciones y políticas para proteger los intereses de los usuarios e impulse el avance tecnológico permitiendo una mayor eficiencia que a su vez permita reducir la huella de carbono. Que existan incentivos e inversión por partes de los gobiernos para impulsar el cambio del uso de petróleo por el uso de la energía eléctrica, pero garantizando la seguridad de los datos y ciberseguridad.

Pregunta 2: ¿Qué tipos de problemas se abordan en la ciberseguridad industrial?**Artículo N° 11****Título:**

Cybersecurity of Offshore Oil and Gas Production Assets Under Trending Asset Digitalization Contexts - A Specific Review of Issues and Challenges in Safety Instrumented Systems

Aporte:

Los autores Zhu y Liyanage (2021) indican que el sector de producción de petróleo y gas en alta mar no son una excepción a la digitalización industrial, los cambios de prácticas y procesos tradicionales se están trasladando a soluciones de digitalización por lo que realiza una extensión de un estudio que cubría con el contexto industrial mediante una investigación aplicada. Bajo tales contextos industriales modernos y crecientes incertidumbres se exploran y revisan algunos problemas y desafíos críticos relacionados con los sistemas instrumentados de seguridad (SIS) para ayudar y mejorar las prácticas actuales sobre la ciberseguridad de SIS dentro de los sistemas de producción de O&G en altamar en contextos cambiantes y modernos.

Problemas técnicos: Son los relacionados con la ciberseguridad del SIS que surgen debido al uso activo de varios dispositivos/sistemas digitales programables, datos compartidos, teledetección, etc., que son condiciones necesarias para la vigilancia remota y el apoyo a los procesos tanto upstream como midstream

Problemas operativos: Los sistemas instrumentados de seguridad consisten en principio en diferentes flujos de trabajo que cubren la vida útil funcional de los SIS. La gestión de la seguridad funcional del SIS sigue los estándares y directrices de la industria, por ejemplo, IEC 61511 y NOG-070. Sin embargo, la práctica actual de la industria trata la ciberseguridad como un dominio separado de los problemas de seguridad funcional

Problemas organizativos y humanos: El estudio indica que hay varios incidentes que ocurrieron durante los últimos años subrayan claramente la carencia de un enfoque organizacional claro, así como la asignación insuficiente de los recursos internos necesarios para mejorar la eficiencia y la eficacia de las contramedidas no técnicas para lograr la ciberseguridad.

Proceso:

Tipo de investigación

Se adopta un enfoque de investigación inductivo. Es una continuación de un estudio de investigación aplicada relacionado con el soporte de decisiones basado en datos para SIS realizado en estrecha cooperación con la industria de altamar. Los datos industriales que proporcionaron la base podrían combinarse con la exposición industrial práctica, la experiencia, las fuentes disponibles públicamente, la literatura académica, así como los informes de auditoría.

Estrategia de investigación

La estrategia de investigación subyacente es exploratoria y ha hecho una contribución significativa a la identificación de varios problemas y desafíos que se

enfrentan actualmente, así como a asegurar el ciclo de vida de SIS e IACS en eventos generales relacionados con la seguridad en la industria del petróleo y el gas en alta mar en los últimos años. activos.

Enfoque de análisis

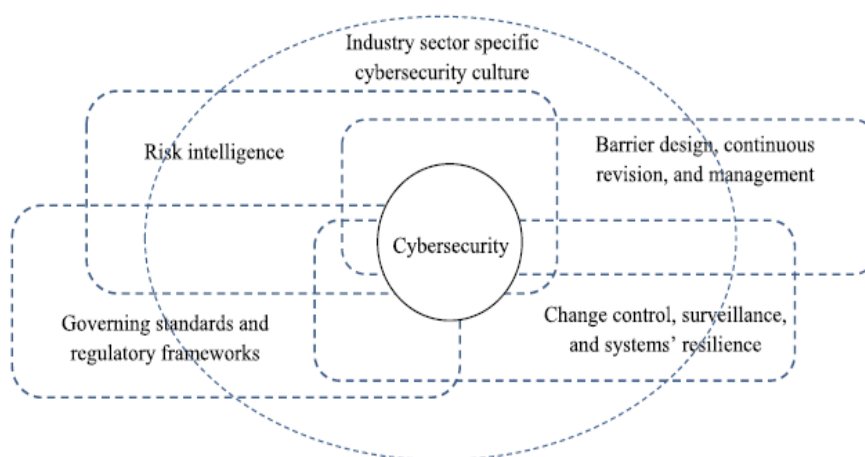
Se utilizó un enfoque cualitativo con un enfoque específico en cómo las nuevas condiciones y problemas que surgen de la digitalización pueden afectar potencialmente el funcionamiento de los sistemas instrumentados de seguridad y, por lo tanto, tanto la seguridad del proceso como la ciberseguridad.

Resultados:

Los autores exploran sistemáticamente los desafíos específicos de seguridad y ciberseguridad que enfrentan los sistemas de control industrial en el nuevo contexto de digitalización y mayor conectividad, con un enfoque en los sistemas instrumentados de seguridad en la producción de petróleo y gas en alta mar.

Figura 6

Diversidad de atributos de ciberseguridad SIS en el sector de petróleo y gas en alta mar

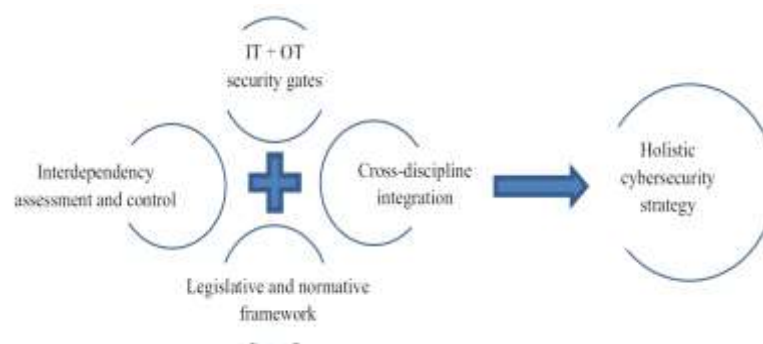


Nota. La infografía muestra la diversidad de atributos de ciberseguridad SIS en el sector de petróleo y gas en alta mar. De “*The diversity of cybersecurity attributes of SIS in offshore oil and gas sector.*”, por Zhu & Liyanage, 2021.

Se definieron y elaboraron cinco atributos principales relacionados con la ciberseguridad del SIS, a saber: normas rectoras y marcos regulatorios, inteligencia de riesgos, diseño de barreras, revisión y gestión continuas, control de cambios, vigilancia y resiliencia del sistema, y cultura de ciberseguridad específica del sector de la industria. El estudio exploró una variedad de problemas y desafíos con respecto a la gestión de SIS e IACS, desde la perspectiva de la ciberseguridad. Los problemas y desafíos identificados no son exclusivos de un operador, sino que aparentemente son generales para toda la industria de altamar. Los autores enfatizaron las complejidades inherentes de los factores clave ocultos detrás de los temas, así como las crecientes interdependencias, que generan efectos latentes en la seguridad y protección de un sistema de control industrial en las condiciones modernas de crecimiento industrial. En la misma forma señalaron que se requiere un esfuerzo de toda la industria para mejorar las prácticas actuales y los niveles de desempeño, considerando la carencia de un enfoque claro, efectivo y, lo que es más importante, integrado para la seguridad y la protección del SIS. Hacia el final se propusieron un par de pasos estratégicos como pasos iniciales hacia el desarrollo de un marco más holístico para gestionar la ciberseguridad de los SIS en un contexto industrial dinámico y complejo que está sujeto a rápidos esfuerzos de digitalización.

Figura 7

Algunos elementos principales hacia una estrategia holística de ciberseguridad



Nota. La infografía muestra algunos elementos principales hacia una estrategia holística de ciberseguridad. De “*Some principal elements towards a holistics cybersecurity strategy*”. por Zhu & Liyanage, 2021.

En tal esfuerzo, También se necesitan las debidas consideraciones sobre los niveles de integración de las tecnologías antiguas y nuevas, la dinámica de la participación humana con diferentes niveles de habilidades digitales, los procesos de trabajo digitales, los cambios en los sistemas de gestión de operaciones, los patrones de flujo de datos e información y la diversidad de las partes interesadas. En general, las condiciones y desarrollos actuales exigen un cambio de los regímenes de seguridad y protección para fortalecer las características defensivas y de resiliencia de los sistemas críticos de activos.

Pregunta 3: ¿Qué problemas se desencadenan por un gobierno deficiente?

Artículo N° 22

Título:

Oil Prices: Governance Failures and Geopolitical Consequences

Aporte:

Los autores Escribano y Valdés (2017) brindan una nueva perspectiva en la gobernanza energética global y las nuevas realidades, así como su impacto social y económico sobre las geografías del petróleo. En la cual se divide en 3 secciones: El enfoque geopolítico en gobernanza y los vacíos legales que implica, El impacto de las políticas de gobernanza en los precios para países importadores y productores y las consecuencias a largo y corto plazo y las principales percepciones entre la interacción entre geopolítica y gobernanza energéticas.

Proceso:

Tipo de enfoque de investigación

Se adopta un enfoque de investigación inductivo con el cual se realizará el análisis sobre las geografías del petróleo ya que explora como en el contexto actual la energía

destaca como un factor clave en la geopolítica de los precios, así como define el comportamiento entre productores y consumidores en un ámbito global, así como las consecuencias de las fallas de gobernanza.

Estrategia de investigación

La estrategia de investigación fue exploratoria ya que ayuda a comprender la naturaleza de no haber aplicado políticas de gobernanza adecuada como problema principal y se basa en experiencias y problemáticas mostradas desde los registros de la crisis del petróleo de 1973 así como el desafío que representó para los productores e importadores en esa época.

Enfoque de análisis

Se utilizó un enfoque cualitativo tomando en cuenta las principales áreas de trabajos sobre el sector energético haciendo énfasis en los vacíos dejados por las crecientes complejidades de la gobernanza energética global. Mostrando las consecuencias y los replanteamientos en las políticas de gobernanza para facilitar el replanteamiento y/o reutilización de políticas energéticas.

Resultados:

Los autores exploraron las fallas significativas de gobernanza energética con lo cual argumentan que los enfoques geopolíticos encuentran un nicho en el vacío dejado por las complejidades de las políticas de gobernanza y que tal falla agrega un nuevo elemento transversal que provoca el resurgimiento de la geopolítica del petróleo como 'gobernanza por otros medios' como alternativa a la fallida gobernanza energética externa. Con respecto al petróleo, los principales esfuerzos de gobernanza se han dedicado a reducir la volatilidad del precio del petróleo a través de la liberalización, la financiación y una mayor transparencia para mitigar los efectos de la información incompleta. Sin embargo, ninguna de estas propuestas se ha considerado seriamente y la volatilidad del

precio del petróleo continúa provocando cambios de poder económico y volatilidad geopolítica.

Pregunta 4: ¿Cómo son abordados los problemas relacionados a gobierno de ciberseguridad?

Artículo N° 09

Título:

Information Security Governance on National Cyber Physical Systems

Aporte:

En este estudio los autores Setiawan et al. (2016) indican que el desarrollo de la tecnología de Internet y su uso en todos los aspectos de la vida día a día progresan rápidamente. Internet ya no es solo un enlace entre humanos, sino que se conecta entre cualquier objeto conectado. Este fenómeno se ha convertido en un detonante para que muchas organizaciones aseguren la información.

Los autores proponen un marco para la implementación de gobernanza de seguridad de la información en sistemas ciber físicos (CPS) en Indonesia. El principal problema de este estudio es cómo funciona la gobernanza de la seguridad de la información en la CPS Nacional. En primer lugar, se brinda un enfoque teórico básico que incluye los antecedentes teóricos de CPS. Se realiza la revisión, descripción y análisis del marco de trabajo de CPS propuesto. Varios aspectos de la gobernanza de seguridad y la gestión de riesgos de CPS son revisados estableciendo que este marco mostrará que en CPS la ciberseguridad requería medidas de seguridad exhaustivas e integradas

Proceso:

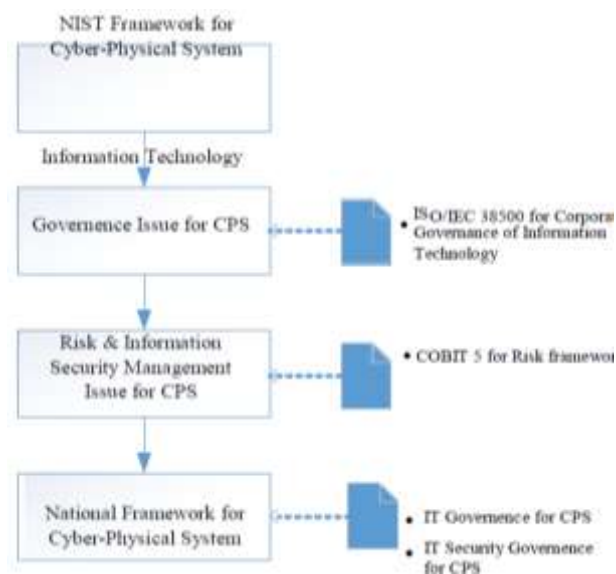
Enfoque

La investigación se lleva a cabo mediante la recopilación de datos cualitativos, la revisión de la literatura y la implementación de los estándares de mejores prácticas para

la seguridad o CPS utilizando el marco del NIST Framework for Cyber-Physical System Rel. 0.8 combinado con ISO / IEC 38500 para Gobierno Corporativo de Tecnología de la Información y COBIT 5 Seguridad de la Información.

Figura 8

Marcos de investigación



Nota. La infografía muestra los estándares utilizados para la creación de un nuevo marco de ciberseguridad. De “*Information Security Governance on National Cyber Physical Systems.*”, por Setiawan et al., 2016

Desarrollo

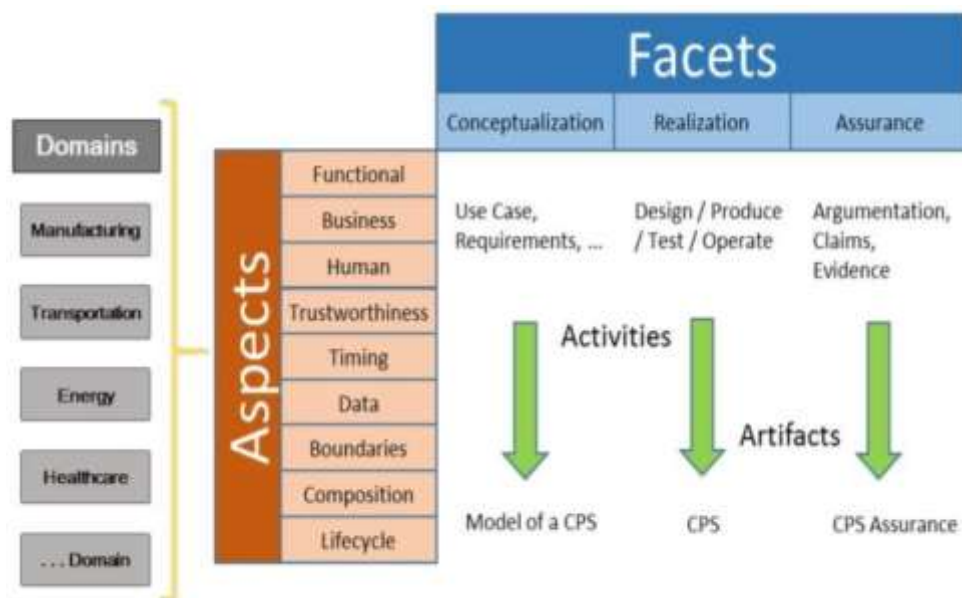
El marco se desarrolla a través de un proceso de análisis que siguió una secuencia definida de pasos.

- Identificar dominios de CPS; Estas son las áreas de implementación de CPS en las que las partes interesadas pueden tener inquietudes específicas de dominio y entre dominios.
- Identificar inquietudes transversales, como sociales, comerciales, técnicas, etc. Las partes interesadas pueden tener inquietudes que se superponen o son instancias de inquietudes conceptuales más amplias.

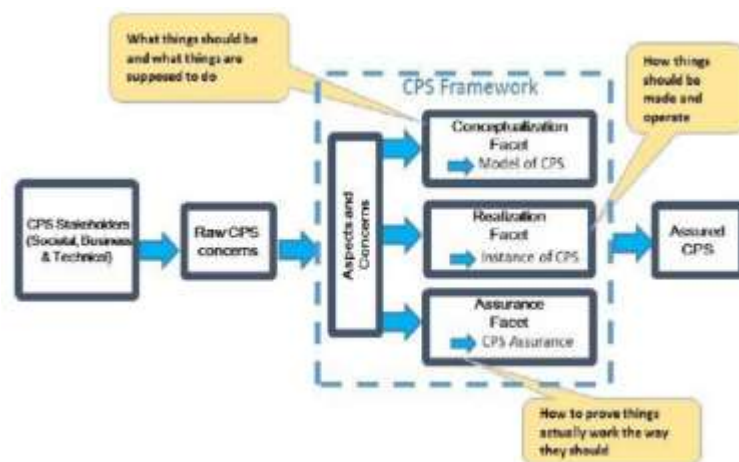
- Analizar inquietudes transversales para producir aspectos, o agrupación de inquietudes conceptualmente equivalentes o relacionadas.
- Abordar preocupaciones (aspectos) a través de actividades y artefactos organizados dentro de tres facetas fundamentales de conceptualización, realización y garantía.

Figura 9

Marco clave de CPS



Nota. La infografía muestra el marco clave de CPS. De “*Information Security Governance on National Cyber Physical Systems.*”, por Setiawan et al., 2016

Figura 10*Derivación del marco CPS*

Nota. La infografía muestra la derivación del marco CPS. De “*Information Security Governance on National Cyber Physical Systems.*”, por Setiawan et al., 2016

3.3 Resultados**3.3.1 Aspectos cubiertos**

A continuación, se presentan los resultados de las búsquedas y análisis de los 29 artículos encontrados en las diversas bases de conocimiento consultadas. Los hemos recopilado y agrupado según el tipo de contribución hacia el problema que estamos investigando, tal como se aprecia en la Tabla 4:

Tabla 4*Contribución de artículos de investigación*

Tipo	Paper	Total
Arquitectura	[PAPER 20], [PAPER 28], [PAPER 29]	3
Buenas Prácticas	[PAPER10], [PAPER12], [PAPER19], [PAPER25], [PAPER26], [PAPER15], [PAPER16]	7
Caso de estudio	[PAPER4], [PAPER7], [PAPER8], [PAPER13], [PAPER14], [PAPER22]	6
Estado situacional	[PAPER23], [PAPER24], [PAPER27]	3
Framework	[PAPER1], [PAPER3], [PAPER9], [PAPER18], [PAPER11]	5
Herramienta	[PAPER2], [PAPER17]	2
Método	[PAPER5], [PAPER6]	2
Software	[PAPER21]	1

De la recopilación de los artículos mencionados destacan 4 que nos brindan soluciones que se encuentran alineadas a nuestro problema de investigación:

Tabla 5

Referencias de investigación

Referencias	Tipo de contribución	Aporte
[PAPER 15]	BUENAS PRÁCTICAS	Buenas prácticas de gobierno y políticas del sector industrial eléctrico
[PAPER 11]	FRAMEWORK	Enfoque sistemático de desafíos específicos de ciberseguridad y como abordarlos
[PAPER 22]	CASO DE ESTUDIO	Las consecuencias que se dan por fallas de políticas complejas de gobernanza en el sector energético
[PAPER 9]	FRAMEWORK	Un marco de trabajo que aborda de manera integrada y completa la ciberseguridad en el sector industrial

3.3.2 Actividades

En base a los artículos analizados, nos orientaremos a definir nuestras actividades en base a las mejores soluciones planteadas en ellos, por tal razón construiremos una solución en base a los siguientes marcos de trabajo:

3.3.2.1 COBIT:

Para las actividades de evaluación del entorno empresarial, utilizaremos factores de diseño COBIT

Figura 11

Factores de diseño COBIT adaptado



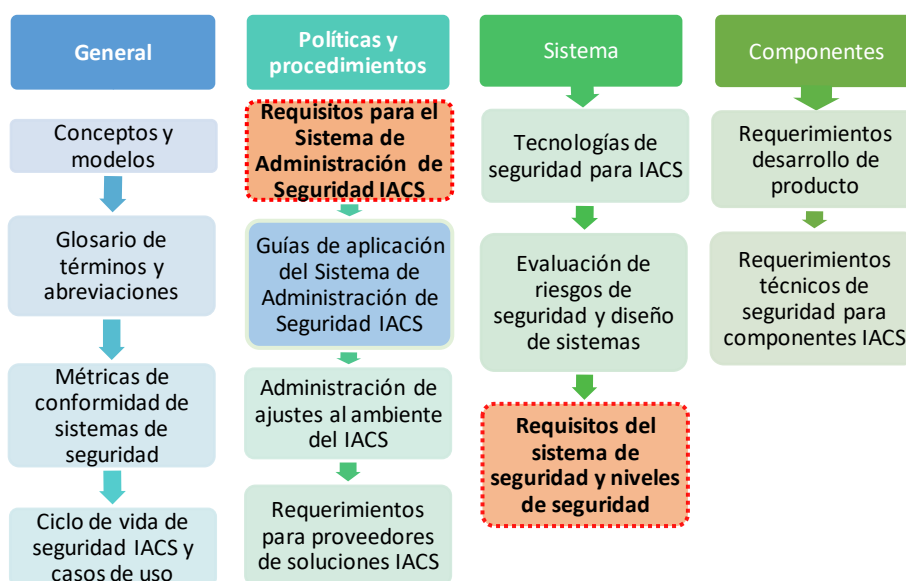
Nota. La infografía muestra la adaptación de los factores de diseño para ciberseguridad industrial. De COBIT, 2018

3.3.2.2 IEC 62443:

Para las actividades de referencia de un marco de trabajo del sector industrial usaremos la IEC 62443.

Figura 12

Marco de trabajo IEC 62443



Nota. La infografía muestra el marco de trabajo IEC 62443. De ISA, 2007

Capítulo IV. Metodología de Investigación

En este capítulo se aborda la metodología que se ha empleado para el desarrollo de la investigación. Es necesario contar con una metodología porque permite diseñar sistemáticamente el estudio garantizando unos resultados válidos y confiables que responderán los objetivos de la investigación.

Para el desarrollo del trabajo de investigación se utilizó el enfoque “Design Science Research Methodology for Information Systems Research”, cuya estructura permite abordar los puntos necesarios del desarrollo investigativo pertinente.

Esta metodología incorpora los principios, las prácticas y los procedimientos necesarios para llevar a cabo la investigación. Proporciona consistencia con la literatura revisada, un modelo de proceso nominal y un modelo mental para presentar y evaluar las investigaciones promoviendo la aceptación de estas.

4.1 Metodología

La Metodología de Investigación en Ciencias del Diseño para la Investigación de Sistemas de Información tiene seis actividades:

Identificar el problema y motivación: En esta actividad, se define una pregunta de investigación específica y se demuestra el valor de la solución. La definición del problema se utilizará para desarrollar una solución eficaz. La racionalización del valor de la solución motiva con éxito a los investigadores y al público de la investigación a buscar soluciones y aceptar los resultados, y contribuye a comprender el razonamiento asociado con la comprensión del problema por parte del investigador.

4.1.1 *Definir objetivos:*

En esta actividad, los objetivos de la solución deben inferirse de la definición del problema. Los objetivos pueden ser cuantitativos o cualitativos. El objetivo debe inferirse razonablemente de la especificación del problema.

4.1.2 Diseñar y desarrollar:

Esta actividad implica identificar la funcionalidad requerida del artefacto y su arquitectura, y luego crear el artefacto real.

4.1.3 Demostrar:

Esta actividad demuestra la efectividad de los artefactos para resolver problemas. Esto puede implicar su uso en experimentos, simulaciones, estudios de casos, pruebas u otras actividades apropiadas.

4.1.4 Evaluar:

Esta actividad implica comparar los objetivos de la solución con las observaciones reales utilizando los artefactos en la demostración. Observe y mida qué tan bien el artefacto apoya la solución del problema.

4.1.5 Comunicar:

La campaña comunica, en su caso, el problema y su importancia, el artefacto, su utilidad y novedad, el rigor de su diseño y su eficacia a los investigadores y otras audiencias relevantes (por ejemplo, profesionales en ejercicio).

Este estudio abordará los primeros 5 pasos de la metodología.

4.2 Hoja de ruta para el desarrollo del artefacto

4.2.1 Definición del problema y motivación

En base al contexto de la ciberseguridad y a la cuarta revolución industrial (Sistemas Cyber-físicos) en el estudio se plantea que es necesario contar con lineamientos base para abordar las crecientes amenazas de ciberseguridad en el sector industrial.

El uso de los sistemas cyber-físicos es el camino que tomará la industria, por lo mismo se requerirán lineamientos base para poder abordar adecuadamente las amenazas de ciberseguridad implícitas en estos sistemas.

Mediante la búsqueda estructurada de investigaciones relacionadas con el problema identificado se cuenta con bases para brindar orientación a la solución idónea que aborda las particularidades específicas del sector industrial.

Con la adecuada estructuración de un marco de trabajo se pueden entregar lineamientos que permitan abordar y priorizar las necesidades de ciberseguridad del sector industrial permitiéndoles proteger los ICS de acuerdo con sus necesidades y posibilidades.

El marco de trabajo será empleado para brindar objetivos de ciberseguridad priorizados y los controles con los que deben contar, basados en estándares que aplican al sector industrial, alineándose a las necesidades de la empresa.

4.2.2 Definición de los objetivos

En cuanto a los temas planteados, se propuso crear un marco que permitiera diseñar soluciones de gobierno para ciberseguridad industrial.

Realizar un análisis de estándares de ciberseguridad y diseño de gobierno que se puedan aplicar al sector industrial para obtener una base.

Mediante la adecuación de los estándares analizados se crearán factores de diseño que permitan medir el contexto de la ciberseguridad en la empresa.

A través de una herramienta se realizará la validación de lo propuesto en el marco, dicha herramienta proporciona la facilidad adecuada para que un experto en ciberseguridad industrial obtenga los resultados del marco.

4.2.3 Definición del artefacto

El marco de trabajo brindará los objetivos priorizados y los controles que deben ser abordados en el gobierno de ciberseguridad alineados a las necesidades de la empresa.

Contará con 9 factores de diseño:

1. Estrategia empresarial

2. Metas empresariales
3. Perfil de riesgo
4. Problemas relacionados con la ciberseguridad
5. Escenario de amenazas
6. Requisitos de cumplimiento
7. Rol de la ciberseguridad
8. Modelo de abastecimiento
9. Estrategia de adopción tecnológica

Que proporciona los objetivos priorizados para la solución de gobierno

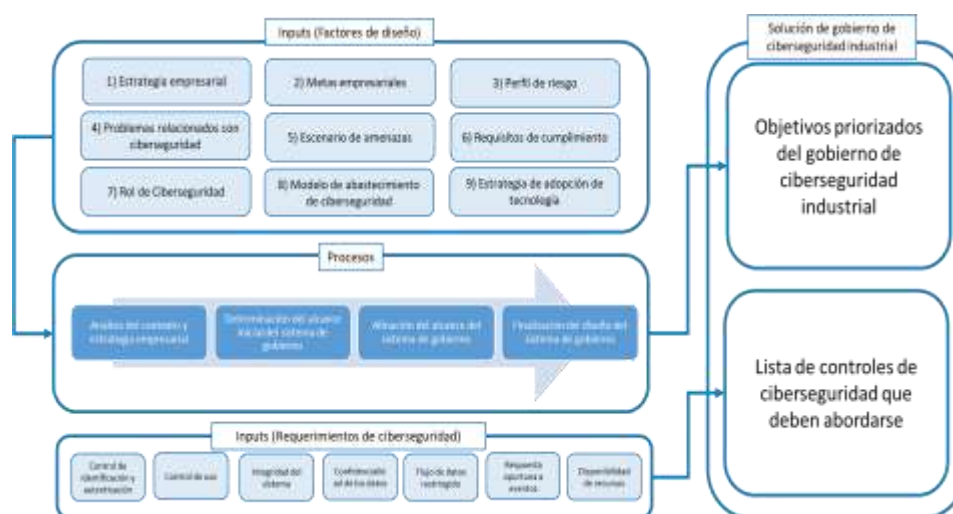
Y un módulo de requerimientos de ciberseguridad que aborda:

1. Control de identificación y autenticación
2. Control de uso
3. Integridad del sistema
4. Confidencialidad de datos
5. Flujo de datos restringido
6. Respuesta oportuna a eventos
7. Disponibilidad de recursos

Que según los niveles actuales y objetivo de nivel de seguridad (SL) proporcionará una lista de controles que deben ser abordados en la solución de gobierno.

Figura 13

Representación gráfica del marco de trabajo



4.2.4 Definición de las métricas

La herramienta tendrá la finalidad medir el contexto y los requerimientos de ciberseguridad actuales y objetivo de la empresa.

Contexto: $\sum FD$

- FD = factor de diseño

La medición del contexto de ciberseguridad dará como resultado los objetivos prioritarios alineados a las necesidades de la empresa.

Requerimientos de ciberseguridad (RS):

- RS actual: Promedio (NSA)
NSA = Nivel de seguridad actual
- RS objetivo: Promedio (NSO)
NSO = Nivel de seguridad objetivo

La medición de los requerimientos de ciberseguridad dará como resultado la lista de controles de ciberseguridad actuales y objetivo, también dará en términos porcentuales la diferencia que existe entre ambos niveles.

4.2.5 Evaluación del artefacto

El marco de trabajo será evaluado mediante la entrega de la herramienta a expertos de ciberseguridad que laboran en empresas del sector industrial con la finalidad que en base a las respuestas ingresadas le proporcionen los objetivos que deben priorizar y la lista de controles que deben abordar en el gobierno de ciberseguridad.

Capítulo V. Desarrollo del Artefacto

En el presente capítulo, se desarrollará el artefacto luego del análisis e investigación de documentos que hacen referencia a lineamientos y normas que sean aplicables a la industria para la formulación de un modelo de gobierno en ciberseguridad industrial. Principalmente, se enfocará a las normas y buenas prácticas de COBIT 2019 e ISA/IEC 62443.

5.1 Componentes del artefacto.

Se ha definido la estructura del artefacto en 2 etapas, la primera busca definir el perfil y carácter de cada organización pues cada una de ellas tiene particularidades tales como el tamaño de la organización, sector industrial al que pertenecen, la regulación local a la que se encuentran sometidas, al entorno de amenaza y otras que puedan definir a cada organización. Para ello, se utilizó la referencia de la Guía de diseño COBIT 2019: Diseño soluciones de Gobierno de Información y tecnología para adaptarse al contexto de la ciberseguridad industrial y alinear los 40 objetivos clave del gobierno y la gestión para relacionarlos con los procesos gubernamentales.

Tabla 6

Objetivos de gobierno y gestión

ID	Objetivos de gobierno y gestión	Adaptación Cyber Industrial
O1	Asegurar el establecimiento y mantenimiento de un marco de gobierno	Ofrece una perspectiva coherente que se integra y alinea con las prácticas de gobierno corporativo. Las decisiones sobre ciberseguridad industrial deben estar en línea con la estrategia y objetivos empresariales para lograr el valor esperado. En este sentido, es importante asegurar que los procesos relacionados con la ciberseguridad industrial sean controlados de manera efectiva y transparente, cumpliendo con los requisitos legales, contractuales y normativos, así como con los requisitos de gobierno de la alta dirección.
O2	Asegurar la entrega de beneficios	Asegurar el mejor valor para las iniciativas, los servicios y los activos habilitados para la ciberseguridad industrial; brinde soluciones y servicios rentables; y comprenda de manera confiable y precisa los costos y beneficios probables de satisfacer las necesidades comerciales de manera efectiva y eficiente.

O3	Asegurar la optimización del riesgo	Asegurar que los riesgos comerciales asociados con la ciberseguridad industrial no excedan el apetito y la tolerancia al riesgo de la empresa, identifique y gestione el impacto de los riesgos de ciberseguridad industrial en el valor comercial y minimice las posibles fallas de cumplimiento.
O4	Asegurar la optimización de recursos	Asegurar que las necesidades de recursos de su empresa se satisfagan de manera óptima, optimice los costos de ciberseguridad industrial, aumente la probabilidad de beneficio y prepárese para cambios futuros.
O5	Asegurar la participación de las partes interesadas	Asegurar el apoyo de las partes interesadas para la estrategia y la hoja de ruta de ciberseguridad industrial, comuníquese con las partes interesadas de manera oportuna y eficaz, y establezca una base de informes para mejorar el rendimiento. Identificar áreas de mejora y confirmar que los objetivos y estrategias relacionados con la ciberseguridad industrial están alineados con la estrategia de la empresa.
O6	Gestionar el marco de gestión de ciberseguridad industrial	Establecer un enfoque integral de gestión para cumplir con los requisitos del gobierno corporativo, incluyendo componentes como procesos de gestión, estructura organizacional, funciones y responsabilidades, actividades confiables y repetibles, elementos informativos, políticas y procedimientos, habilidades y capacidades, cultura y comportamiento; así como servicios e infraestructura.
O7	Gestionar la estrategia	Brindar soporte a la estrategia de transformación digital en su organización entregando el valor requerido mediante una hoja de ruta con cambios incrementales. Adoptar un enfoque integral sobre ciberseguridad industrial asegurando que cada iniciativa esté claramente vinculada a la estrategia general sin afectar la disponibilidad de los procesos. Facilitar el cambio en cada aspecto de su organización desde canales y procesos hasta datos cultura habilidades modelos operativos e incentivos.
O8	Gestionar la arquitectura empresarial	Representar los diferentes elementos que conforman una compañía y sus interacciones, así como los principios que guían su diseño y evolución para alcanzar objetivos operativos y estratégicos efectivos y estándar.
O9	Gestionar la innovación	Lograr una ventaja competitiva, innovación comercial, una mejor experiencia del cliente y una mayor eficiencia y eficiencia operativas aprovechando las tecnologías emergentes que deben ser respaldadas por la ciberseguridad industrial.
O10	Gestionar el portafolio	Optimizar el rendimiento de toda la cartera en respuesta al rendimiento de proyectos, productos y servicios individuales, así como las cambiantes prioridades y necesidades comerciales.
O11	Gestionar el presupuesto y los costes	Promover alianzas entre la ciberseguridad industrial y las partes interesadas comerciales para utilizar los recursos relacionados con la ciberseguridad industrial de manera eficaz y eficiente, y brindar a las empresas transparencia y responsabilidad sobre el costo y el valor de las soluciones y los servicios. Permite a las

		empresas tomar decisiones informadas sobre el uso de soluciones y servicios de ciberseguridad industrial.
O12	Gestionar los recursos humanos	Optimizar las capacidades de los recursos humanos para alcanzar los objetivos comerciales, con un enfoque en la seguridad de los empleados.
O13	Gestionar las relaciones	Fomentar la adquisición de conocimientos, habilidades y comportamientos adecuados para lograr mejores resultados, aumentar la credibilidad y la confianza mutua, y utilizar eficientemente los recursos, lo que fomenta relaciones productivas con los grupos de interés de la empresa.
O14	Gestionar los acuerdos de servicio	Asegurar que los productos, servicios y niveles de servicio de ciberseguridad industrial satisfagan las necesidades actuales y futuras de la empresa.
O15	Gestionar los proveedores	Optimizar las capacidades de ciberseguridad industrial disponibles para respaldar las estrategias y hojas de ruta de ciberseguridad industrial, minimizar los riesgos asociados con proveedores deficientes o que no cumplen, y garantizar precios competitivos.
O16	Gestionar la calidad	Asegurarse de que las soluciones técnicas y los servicios se proporcionen de manera coherente para cumplir con los requisitos de calidad de la empresa y las necesidades de las partes interesadas.
O17	Gestionar riesgos	Integrar la gestión de riesgos empresariales relacionados con la ciberseguridad industrial con la gestión de riesgos empresariales globales, equilibrando los costos y beneficios de la gestión de riesgos empresariales.
O18	Gestionar la seguridad	Mantener el impacto y presencia de incidentes de ICS relacionados con la ciberseguridad industrial dentro del nivel de apetito de riesgo de la empresa.
O19	Gestionar los datos	Garantizar la disponibilidad de activos de datos históricos y en tiempo real para lograr los objetivos empresariales.
O20	Gestionar los programas	Obtener el valor comercial esperado y reducir el riesgo de demoras inesperadas, costos y erosión del valor. Mejorar la comunicación y el compromiso empresarial y del usuario final, garantizar el valor y la calidad de los entregables del proyecto, realizar un seguimiento de los proyectos dentro de los proyectos y maximizar las contribuciones de los proyectos a la cartera.
O21	Gestionar la definición de requerimientos	Crear la mejor solución para las necesidades de su empresa mientras se minimiza el riesgo.
O22	Gestionar la identificación y construcción de soluciones	Crear soluciones oportunas y rentables (técnicas, procesos empresariales y flujos de trabajo) que respalden los objetivos estratégicos y operativos corporativos.

O23	Gestionar la disponibilidad y capacidad	Mantener la disponibilidad del servicio, la gestión eficiente de los recursos y la optimización del rendimiento del sistema anticipando las necesidades futuras de rendimiento y capacidad.
O24	Gestionar los cambios organizativos	Preparar e involucrar a las partes interesadas para el cambio empresarial y reducir el riesgo de fracaso.
O25	Gestionar los cambios de TO	Facilitar la ejecución de cambios rápida y confiable para el negocio. Reducir el riesgo de afectar negativamente la disponibilidad del entorno modificado.
O26	Gestionar la aceptación y la transición de los cambios de TO	Implementar soluciones seguras basadas en los resultados esperados y acordados.
O27	Gestionar el conocimiento	Proporcionar el conocimiento y la información de gestión necesarios para apoyar a todos los involucrados en el gobierno y la gestión de la ciberseguridad industrial de una empresa para tomar decisiones informadas.
O28	Gestionar los activos	Considerar todos los activos de ciberseguridad industrial y optimizar el valor que proporciona su uso.
O29	Gestionar la configuración	Proporcionar suficiente información sobre los activos del servicio para gestionar los servicios de manera eficiente. Evaluar el impacto de los cambios y manejar los incidentes de servicio.
O30	Gestionar los proyectos	Lograr los resultados del proyecto y reducir el riesgo de demoras inesperadas, costos y erosión del valor al mejorar la comunicación, el compromiso del negocio y del usuario final. Asegurar el valor, la calidad de los entregables del proyecto y maximizar su contribución a los programas y al portafolio de inversión establecido.
O31	Gestionar las operaciones	Proporcionar resultados de los servicios operativos respaldados por la ciberseguridad industrial según lo planificado.
O32	Gestionar las peticiones y los incidentes del servicio	Lograr los resultados del proyecto y reducir el riesgo de demoras inesperadas, costos y erosión del valor al mejorar la comunicación, el compromiso del negocio y del usuario final. Asegurar el valor, la calidad de los entregables del proyecto y maximizar su contribución a las carteras y programas establecidos.
O33	Gestionar los problemas	Incrementar la disponibilidad, mejorar los niveles de servicio, reduzca los costos y satisfacer mejor las necesidades y la satisfacción del cliente al reducir la cantidad de problemas operativos, con la identificación de la causa raíz como parte de la resolución de problemas.
O34	Gestionar la continuidad	En caso de una interrupción importante (p. ej., ciber amenaza), adaptarse rápidamente a las operaciones comerciales en curso y mantener la disponibilidad de recursos e información a niveles aceptables para el negocio.
O35	Gestionar los servicios de seguridad	Reducir el impacto comercial de las brechas de seguridad de la información y los incidentes operativos.

O36	Gestionar los controles de los procesos de negocio	Mantener la seguridad y la integridad de la información y los activos manejados dentro de los procesos de operaciones comerciales internas o subcontratadas de la empresa.
O37	Gestionar la monitorización del rendimiento y la conformidad	Proporcionar información transparente sobre el desempeño y el cumplimiento e impulsar el logro de los objetivos.
O38	Gestionar el sistema de control interno	Proporcionar información transparente a las partes interesadas clave sobre la adecuación del sistema de control interno, brindando confiabilidad operativa, confianza en el logro de los objetivos de la empresa y una buena comprensión de los riesgos residuales.
O39	Gestionar el cumplimiento de los requerimientos externos	Asegurarse de que la empresa cumpla con todos los requisitos externos aplicables.
O40	Gestionar el aseguramiento	Facilitar el diseño y desarrollo de programas efectivos y eficientes utilizando una hoja de ruta basada en estándares aclamados, brindando orientación sobre la planificación, el alcance, la ejecución y el seguimiento.

Nota. Adaptado de "Guía de diseño COBIT 2019: Diseño de una solución de Gobierno de Información y Tecnología", por ISACA, 2018 (<https://www.isaca.org/>)

Muchos procesos están directamente relacionados con los componentes del sistema de gobierno, como la estructura organizativa, las políticas y los procedimientos, la cultura, la seguridad industrial y la infraestructura y las aplicaciones del entorno industrial.

Para esta primera secuencia se han definido 9 factores de diseño, las cuales se describen a continuación:

5.1.1 Estrategia empresarial:

Cada empresa tiene una estrategia comercial diferente según la categoría en la que se encuentran. Generalmente hay una estrategia primaria y una estrategia secundaria.

Tabla 7*Factor de diseño: Estrategia empresarial*

Estrategia empresarial	Descripción
Crecimiento / Adquisición	Se enfoca en el crecimiento económico.
Innovación / Diferenciación	Se enfoca en empresas que ofrecen productos y servicios diferentes y/o innovadores a sus clientes.
Liderazgo en costos	Se centra en la minimización de costos a corto plazo.
Servicio al cliente / Estabilidad	Se enfoca en brindar un servicio estable y orientado al cliente.

5.1.2 Metas empresariales:

Son las que aportan al logro de la estrategia empresarial.

Tabla 8*Factor de diseño: Metas empresariales*

Dimensiones del cuadro de mando integral	Meta empresarial
Finanzas	Portafolio competitivo de productos y servicios
Finanzas	Gestión de riesgo empresariales
Finanzas	Cumplir con las leyes y regulaciones externas
Finanzas	Calidad de la información financiera
Cliente	Cultura de servicio centrada cliente
Cliente	Continuidad y disponibilidad del servicio comercial
Cliente	Gestión de la calidad de la información
Interno	Funciones para optimizar los procesos comerciales internos
Interno	Optimización de costes de los procesos de negocio
Interno	Habilidades, Motivación y Productividad de los Empleados
Interno	Cumplir con las políticas internas
Crecimiento	Gestión de iniciativas de transformación digital
Crecimiento	Innovación de productos y negocios

Nota. Adaptado de "Guía de diseño COBIT 2019: Diseño de una solución de Gobierno de Información y Tecnología", por ISACA, 2018 (<https://www.isaca.org/>)

5.1.3 Perfil de riesgo:

Se identifican todos los tipos de riesgos en ciberseguridad industrial a los que se encuentran expuestas las empresas.

Tabla 9

Factor de diseño: Perfil de riesgo

Categoría de riesgo	Ejemplos de escenarios de riesgo
Toma de decisiones de inversión en ciberseguridad industrial, definición y mantenimiento de portafolio	<p>A. Los programas elegidos para su implementación no están alineados con la estrategia y las prioridades de la empresa.</p> <p>B. Las inversiones relacionadas con la ciberseguridad industrial no logran respaldar la estructura operativa de la empresa.</p> <p>C. Opciones incorrectas de adquisición e implementación de soluciones de ciberseguridad (en términos de costo, rendimiento, funcionalidad, compatibilidad, redundancia, etc.)</p> <p>D. Elección incorrecta de la infraestructura para su implementación (en términos de costo, rendimiento, características, compatibilidad, etc.)</p> <p>E. Existe una duplicación o superposición sustancial entre los diversos programas de inversión.</p> <p>F. Asignación de recursos, gestión y/o competencia ineficientes que no se alinean con las prioridades del negocio.</p>
Gestión del ciclo de vida de programas y proyectos	<p>A. La alta dirección no completa los proyectos fallidos (debido al costo, retrasos excesivos, pérdida del control del alcance, cambios en las prioridades comerciales).</p> <p>B. Falta de presupuesto para programas de ciberseguridad industrial.</p> <p>C. Problemas de calidad de los proyectos de ciberseguridad industrial.</p> <p>D. Retraso en la entrega de proyectos de ciberseguridad industrial.</p> <p>E. El proveedor subcontratado no entregó el proyecto según el acuerdo contractual (cualquier combinación de sobrecostos presupuestarios, problemas de calidad, falta de funcionalidad, entrega tardía).</p>
Coste y supervisión de ciberseguridad industrial	<p>A. Dependencia y uso excesivo de aplicaciones y soluciones ad hoc creadas, definidas y mantenidas por los usuarios.</p> <p>B. Los acuerdos de nivel de servicio (SLA) son inválidos debido a requisitos insuficientes.</p> <p>C. Falta de inversión en capital relacionado con la ciberseguridad industrial.</p>
Comportamiento, habilidades y conocimiento de ciberseguridad industrial	<p>A. Falta o incompatibilidad de habilidades relacionadas con la ciberseguridad dentro del campo (p. ej., debido a nuevas tecnologías, métodos de trabajo, amenazas emergentes).</p> <p>B. La falta de conocimiento empresarial entre el personal de ciberseguridad industrial afecta la calidad de los servicios/proyectos proporcionados.</p> <p>C. Incapacidad para contratar y retener personal de ciberseguridad industrial.</p> <p>D. Perfiles de reclutamiento insuficientes debido a la falta de debida diligencia durante el proceso de reclutamiento.</p> <p>E. Falta de formación en ciberseguridad industrial.</p>

	F. Dependencia excesiva en personal clave para proporcionar servicios de ciberseguridad industrial.
Arquitectura empresarial / ciberseguridad industrial	<p>A. La estructura empresarial es compleja e inflexible, lo que dificulta su evolución y expansión, lo que genera la pérdida de oportunidades comerciales.</p> <p>B. Carencia de adopción y uso de nueva infraestructura o abandono de infraestructura obsoleta.</p> <p>C. No adoptar y aprovechar nuevas soluciones de ciberseguridad industrial (características, optimizaciones, etc.) o abandonar procesos obsoletos.</p> <p>D. Arquitectura empresarial no documentada, lo que genera ineficiencias y duplicación.</p> <p>E. Hay demasiadas excepciones a los estándares de arquitectura empresarial.</p>
Incidentes de infraestructura operativa de ciberseguridad industrial	<p>A. Daños accidentales al equipo.</p> <p>B. Errores del personal de ciberseguridad industrial (configuración de red insuficiente, instalación de actualizaciones no verificadas, programa de mantenimiento inadecuado, etc.).</p> <p>C. El personal de ciberseguridad industrial o los usuarios del sistema ingresan información incorrecta.</p> <p>D. Interrupción del Centro de Control de Seguridad Cibernética por parte del personal interno (sabotaje, etc.).</p> <p>E. Robo de dispositivos con datos confidenciales.</p> <p>F. Robo de dispositivos con datos confidenciales.</p> <p>G. Componentes de hardware mal configurados.</p> <p>H. Manipulación intencional de hardware (equipo de monitoreo, etc.).</p> <p>I. Abuso de la función preferida de acceso a la infraestructura de acceso.</p> <p>J. Falta de examen de la eficacia de las soluciones de ciberseguridad industrial.</p> <p>K. Pérdida de la integridad de los datos del servicio en la nube.</p> <p>L. Pérdida de Disponibilidad del Servicio en la Nube.</p>
Acciones no autorizadas	<p>A. Manipulación del software.</p> <p>B. Modificar o manipular intencionalmente el software para causar una brecha de seguridad.</p> <p>C. Modificar o manipular intencionalmente el software para provocar un comportamiento fraudulento.</p> <p>D. Modificación accidental del software que resulta en resultados inexactos.</p> <p>E. Errores no intencionales en la gestión de la configuración.</p>
Problemas de adopción/Uso	<p>A. Resistir cambios en los procesos debido a la implementación de nuevas soluciones de ciberseguridad industrial.</p> <p>B. Un Proceso de Ciberseguridad Industrial Inadecuado o Incumplimiento.</p>
Incidentes de Hardware	<p>A. Inestabilidad de ICS (SCADA, PLC, DCS) cuando se instala una nueva infraestructura, lo que provoca fallas operativas (p. ej., actualización de la plataforma).</p> <p>B. Cuando aumenta el número de usuarios, ICS no puede procesar el volumen de transacciones.</p> <p>C. ICS no puede manejar la carga del sistema al implementar nuevas aplicaciones o programas.</p> <p>D. Falla del servicio (telecomunicaciones, electricidad).</p>

- E. Falla del hardware debido a sobrecalentamiento y/u otras condiciones ambientales como la humedad.
- F. Corrupción de datos debido a daños internos en componentes de hardware.
- G. Pérdida/divulgación de medios portátiles (CD, unidades USB, unidades de memoria USB, etc.) que contienen datos confidenciales.
- H. Aumentar el tiempo para resolver o dar soporte a las demoras en caso de un evento de hardware.
- Fallos de Software
- A. Incapacidad para usar el software para alcanzar los resultados esperados (p. ej., no realizar los cambios necesarios en el modelo comercial o cambios organizacionales).
- B. Implementación de software inmaduro (primeros usuarios, errores, etc.).
- C. Fallas operativas cuando se pone en funcionamiento un nuevo software.
- D. Errores generales de funcionamiento del software para aplicaciones críticas.
- E. Software de aplicación desactualizado (p. ej., tecnología heredada, mal documentado, costoso de mantener, no escalable, no integrado en la arquitectura actual, etc.).
- F. La nueva versión tiene problemas de funcionamiento y no puede volver a la versión anterior.
- G. Corrupción de la base de datos debido a que el software pierde acceso a los datos.
- Exposición a Ciberataques
- A. Una persona interna no autorizada intenta ingresar al sistema.
- B. Interrupción del servicio debido a un ataque de denegación de servicio (DoS).
- C. Ataque de malware.
- D. Espionaje industrial.
- E. Hacktivismo.
- F. Los empleados descontentos implementan malware de cuenta regresiva, lo que resulta en la pérdida de datos.
- G. Acceso no autorizado a datos de la empresa mediante ataques de phishing.
- H. Ataques a sistemas críticos por parte de gobiernos extranjeros.
- Incidentes de terceros/Proveedores
- A. Rendimiento deficiente del proveedor en acuerdos de subcontratación a largo plazo y a gran escala (por ejemplo, debido a la falta de diligencia debida del proveedor sobre la viabilidad financiera, la capacidad de entrega y la sostenibilidad de los servicios del proveedor).
- B. Los proveedores de ciberseguridad aceptan términos comerciales poco razonables.
- C. Soporte y servicio insuficientes de proveedores que no cumplen con los SLA.
- D. Incumplimiento del Acuerdo de Competencia de Soluciones de Ciberseguridad.
- E. La funcionalidad no se puede transferir a un proveedor alternativo debido a una dependencia excesiva del proveedor actual.
- F. Múltiples adquisiciones de soluciones de ciberseguridad (especialmente servicios en la nube) sin consultoría/participación en ciberseguridad, lo que resulta en la incapacidad de integrar los servicios con los servicios internos.
- G. No cumplimiento del Acuerdo de Nivel de Servicio (SLA) o incumplimiento para obtener el servicio acordado y penalización por incumplimiento.

Incumplimiento	<p>A. El incumplimiento de las normas nacionales o internacionales (por ejemplo, medio ambiente, seguridad industrial, privacidad, etc.).</p> <p>B. Falta de conocimiento sobre los cambios regulatorios que pueden impactar el negocio.</p> <p>C. Obstáculos comerciales causados por regulaciones.</p> <p>D. Incumplimiento de los procedimientos internos.</p>
Problemas Geopolíticos	<p>A. Inaccesible debido a eventos disruptivos en otras instalaciones.</p> <p>B. El impacto de la intervención del gobierno y las políticas nacionales en las empresas.</p> <p>C. Acciones dirigidas por grupos u organismos financiados por el gobierno.</p>
Acción Sindical	<p>A. Instalaciones y edificios inaccesibles por huelgas sindicales.</p> <p>B. El tercero no puede prestar servicios debido a una huelga.</p> <p>C. El personal clave no está disponible debido a la acción del sindicato, como una huelga de transporte o servicios públicos.</p>
Desastres Naturales	<p>A. Terremotos que destruyan o dañen infraestructura crítica.</p> <p>B. El tsunami destruyó edificios importantes.</p> <p>C. Grandes tormentas y ciclones tropicales o tornados que dañan infraestructura crítica.</p> <p>D. Grandes incendios forestales.</p> <p>E. Inundación.</p> <p>F. Los niveles de las aguas subterráneas inutilizan los lugares críticos.</p> <p>G. Las altas temperaturas hacen que sea antieconómico mantener en funcionamiento los lugares críticos.</p>
Innovación Tecnológica	<p>A. Falta de identificación de nuevas tendencias tecnológicas importantes.</p> <p>B. No aprovechar el valor y el potencial de las tecnologías actuales y futuras en a ptimizacin de recursos.</p> <p>C. Falta de adopción y uso de nueva infraestructura de manera oportuna (funcionalidad, optimización de procesos, etc.).</p> <p>D. No brindar soporte técnico para nuevos modelos de negocios.</p>
Medio Ambiente	<p>A. Equipos no ecológicos (por ejemplo, consumo de energía).</p>
Gestión de información y datos	<p>A. El personal no autorizado descubre información confidencial debido a la retención/archivo/eliminación de información ineficiente.</p> <p>B. Cambio intencional, ilegal o malicioso de datos.</p> <p>C. Compartir información confidencial sin autorización a través de correo electrónico o redes sociales.</p> <p>D. Pérdida de propiedad intelectual (PI) y/o compartir de información competitiva.</p>

Nota. Adaptado de "Guía de diseño COBIT 2019: Diseño de una solución de Gobierno de Información y Tecnología", por ISACA, 2018 (<https://www.isaca.org/>)

5.1.4 Problemas relacionados con la ciberseguridad industrial:

Son los problemas relacionados con ciberseguridad industrial, en otras palabras, son los riesgos que se han llegado a materializar.

Tabla 10

Factor de diseño: Problemas relacionados con la ciberseguridad industrial

Problema	Descripción
P1	Frustración entre los diferentes departamentos de ciberseguridad industrial de una organización debido a la percepción de una baja contribución al valor comercial.
P2	Frustración entre diferentes partes de la empresa (p. ej., clientes de ciberseguridad industrial) y el sector de la ciberseguridad industrial por el fracaso del programa o la baja contribución al valor comercial.
P3	Principales incidentes relacionados con la ciberseguridad industrial, como pérdida de datos, brechas de seguridad, fallas en proyectos, errores de aplicación, etc. Relacionados con la ciberseguridad industrial.
P4	Problemas de ejecución de servicios para subcontratistas de ciberseguridad industrial.
P5	Incumplimiento de requisitos normativos o contractuales relacionados con la ciberseguridad industrial.
P6	Resultados de auditorías periódicas u otros informes de evaluación de desempeño deficiente de ciberseguridad industrial o problemas de calidad y servicio de ciberseguridad industrial.
P7	Gasto encubierto y la falsificación de inversiones en ciberseguridad industrial por parte de sectores usuarios que operan al margen de los procesos habituales de toma de decisiones y presupuestos aprobados.
P8	Duplicación o superposición de iniciativas u otras formas de desperdicio de recursos.
P9	Recursos insuficientes en ciberseguridad industrial, personal poco capacitado y agotamiento/insatisfacción del personal.
P10	Los cambios o proyectos facilitados por la ciberseguridad industrial a menudo no cumplen con las necesidades comerciales y la ejecución se retrasa o se excede del presupuesto.
P11	Los miembros de la junta, los ejecutivos o la alta dirección muestran resistencia a participar en la ciberseguridad industrial o carecen de un compromiso con el patrocinio corporativo.
P12	Modelos operativos complejos en ciberseguridad industrial y/o mecanismos confusos para la toma de decisiones relacionadas con la ciberseguridad industrial.
P13	La ciberseguridad industrial tiene costos excesivos.
P14	Implementación bloqueada o fallida de nuevas iniciativas o innovaciones debido a las arquitecturas y sistemas de ciberseguridad industrial actuales.
P15	Brechas entre el conocimiento técnico y comercial, lo que resulta en usuarios comerciales y/o expertos en ciberseguridad industrial que hablan diferentes idiomas.
P16	Problemas generales de calidad de datos e integración de datos de fuentes dispares.
P17	Alto nivel de cómputo por parte de los usuarios finales, lo que resulta (entre otros problemas) en la falta de monitoreo y control de calidad sobre las aplicaciones desarrolladas e implementadas.
P18	Las áreas implementan sus propias soluciones de ciberseguridad, con poca o ninguna participación de los departamentos corporativos de ciberseguridad

industrial, a menudo debido a la insatisfacción con las soluciones y servicios de ciberseguridad industrial.

P19 Desconocimiento y/o vulneración de la normativa de protección de datos.

P20 Incapacidad para aprovechar las nuevas tecnologías o innovar en ciberseguridad industrial.

Nota. Adaptado de "Guía de diseño COBIT 2019: Diseño de una solución de Gobierno de Información y Tecnología", por ISACA, 2018 (<https://www.isaca.org/>)

5.1.5 Escenarios de amenazas:

Corresponde a los escenarios de amenaza operados por la empresa y se clasifica en normal y alta.

Tabla 11

Factor de diseño: Escenario de amenazas

Escenario de amenazas	Explicación
Normal	La empresa opera a niveles normales de amenaza.
Alta	Debido a su ubicación geopolítica y sector industrial, la empresa opera en un entorno de alta amenaza.

5.1.6 Requisitos de cumplimiento:

Son aquellos requisitos que las empresas deben cumplir.

Tabla 12

Factor de diseño: Requisitos de cumplimiento

Entornos regulatorios	Explicación
Requerimientos de cumplimiento bajo	Los requisitos mínimos de cumplimiento de la empresa están por debajo del promedio.
Requerimientos de cumplimiento normal	Las compañías deben cumplir con diversos requisitos de conformidad que son compartidos en distintas industrias.
Requerimientos de cumplimiento alto	La empresa debe cumplir con requisitos de conformidad más exigentes de lo habitual, que están vinculados principalmente al sector industrial y las condiciones geopolíticas.

5.1.7 Rol de ciberseguridad:

Los roles de ciberseguridad se clasifican de acuerdo con la criticidad del giro de negocio.

Tabla 13*Factor de diseño: Rol de Ciberseguridad*

Rol de ciberseguridad	Explicación
Soporte	La ciberseguridad industrial no es crítica para el funcionamiento y la continuidad de los procesos y servicios comerciales o sus innovaciones.
Fábrica	La falla de una solución de ciberseguridad impacta directamente en la operación y continuidad de los procesos y servicios de negocio. A pesar de esto, la ciberseguridad no es el impulsor principal de la innovación en servicios y procesos comerciales.
Cambio	La ciberseguridad se considera un impulsor de la innovación de servicios y procesos comerciales. No obstante, actualmente existe poca confianza en que la ciberseguridad pueda garantizar una operación continua y una continuidad adecuada en los procesos y servicios comerciales.
Estratégico	El correcto funcionamiento e innovación en los procesos y servicios comerciales de una organización dependen fundamentalmente de la ciberseguridad.

5.1.8 Modelo de compra de proveedores para ciberseguridad industrial:

El modelo de abastecimiento de proveedores utilizado por una empresa para prestar servicios.

Tabla 14*Factor de diseño: Modelo de abastecimiento de proveedores para ciberseguridad industrial*

Modelo de abastecimiento de proveedores	Explicación
Externalización (outsourcing)	La empresa necesita los servicios de un tercero para prestar servicios de ciberseguridad.
Nube	La empresa maximiza el uso de la nube para brindar a los usuarios servicios de ciberseguridad.
Personal interno (Insourced)	La empresa proporciona su propio personal y servicios de ciberseguridad.

5.1.9 Estrategia de adopción de tecnología:

La estrategia de adopción de nuevas tecnologías depende de cada empresa y en función de sus necesidades.

Tabla 15

Factor de diseño: Estrategias de adopción de tecnología

Estrategia de adopción de tecnología	Explicación
Primero en reaccionar (First mover)	Las empresas suelen adoptar nuevas tecnologías lo más rápido posible y se esfuerzan por obtener una ventaja competitiva.
Seguidor (Follower)	Por lo general, la empresa espera que una nueva tecnología se implemente y pruebe ampliamente antes de adoptarla.
Adoptadores lentos (Slow adopter)	A la empresa le llevará mucho tiempo adoptar nuevas tecnologías.

Para la segunda etapa, se plantearán los requerimientos de ciberseguridad industrial considerando los Requerimientos Funcionales de la norma IEC 62443 en el cual se establecen los principales controles que toda empresa del sector industrial debe desarrollar. Estos proporcionan requisitos técnicos detallados del sistema de control asociados con los siete requisitos fundamentales descritos en ISA-62443-2-1 para la capacidad del sistema de control.

5.1.10 Requisitos de ciberseguridad:

Cada uno de los 7 requerimientos funcionales serán evaluados en los 5 niveles de seguridad, tal como se describen:

- SL 0: No se requieren requisitos específicos ni protección de seguridad
- SL 1: Protección contra la infracción casual o coincidente
- SL 3: Protección contra las violaciones intencionales utilizando medios sofisticados con los recursos apropiados, habilidades específicas de IACS y motivación apropiada.

- SL 4: Protección contra la violación intencionales utilizando medios sofisticados con recursos ampliados, habilidades específicas de IACS y alta motivación.

Tabla 16*Requisitos de ciberseguridad*

Control de identificación y autenticación	
FR1	Identificación y autenticación de usuarios humanos
	Proceso de software e identificación y autenticación de dispositivos
	Administración de cuentas
	Gestión de identificadores
	Gestión de autenticadores
	Gestión de acceso inalámbrico
	Fortaleza de la autenticación basada en contraseña
	Certificado de infraestructura de clave pública (PKI)
	Intensidad de autenticación de clave pública
	Retroalimentación del autenticador
	Intentos de acceso fallido
	Notificación de uso del sistema
Acceso a través de una red no confiable	
Control de uso	
FR2	Cumplimiento de la autorización
	Control de uso inalámbrico
	Control de uso para dispositivos portátiles y móviles
	Código móvil
	Bloqueo de sesión
	Terminación de sesión remota
	Control de sesiones concurrentes
	Eventos auditables
	Capacidad de almacenamiento de auditoría
	Respuesta a falla de procesamiento de auditoría
	Marca de tiempo
No repudio	
Integridad del sistema	
FR3	Integridad de la comunicación
	Protección de código malicioso
	Verificar las características de seguridad
	Integridad de la información software y software
	Validación de entrada
	Salida de estado predeterminado
Manejo de errores	

	Integridad de la sesión
	Protección de la información de auditoría
	Confidencialidad de los datos
FR4	Confidencialidad de la información
	Persistencia de la información
	Uso de criptografía
	Flujo de datos restringido
FR5	Segmentación de la red
	Protección de límites de zona
	Restricciones de comunicación de persona a persona de propósito general
	Partición de aplicaciones
	Respuesta oportuna a eventos
FR6	Accesibilidad del registro de auditoría
	Monitoreo continuo
	Disponibilidad de recursos
	Protección de denegación de servicio
	Gestión de recursos
	Respaldo del sistema de control
FR7	Recuperación y reconstitución del sistema de control
	Energía de emergencia
	Ajustes de configuración de red y seguridad
	Funcionalidad mínima
	Inventario de componentes del sistema de control

5.2 Fases de la implementación

5.2.1 *Análisis de artículos de investigación*

En el Capítulo III, en el desarrollo del Estado del Arte observamos que los investigadores planteaban soluciones a problemas similares al nuestro, proporcionando una línea base de cómo abordar el problema, qué investigar y qué conocimientos aplican a problemas similares al nuestro permitiendo dar el primer paso para la solución.

5.2.2 *Benchmarking de estándares aplicables al sector industrial*

Del análisis anterior, se obtuvo un alcance del proceso que realizaban los investigadores para lograr una solución a los problemas que planteaban, la cual consistía en revisar marcos de trabajo, buenas prácticas y estándares que fueron fundamentales para brindar bases para la formulación de los lineamientos de los problemas. Partiendo de ello,

se procede a la revisión de distintos marcos, normas, estándares y buenas prácticas en materia de gobierno y ciberseguridad que apliquen o se puedan adaptar al sector industrial.

5.2.3 Adaptación de COBIT a ciberseguridad industrial en base a ISA/IEC 62443-2-1

Desde el marco COBIT, se adapta cada uno de los 40 objetivos de gobierno y gestión, originalmente orientados al mundo de TI pero adaptados y redefinidos para el entorno de ciberseguridad industrial.

5.2.4 Creación de los factores de diseño

5.2.4.1 Factor de Diseño 1 - Estrategia de Negocios:

Para el cálculo de los factores de diseño se debe realizar un cálculo matricial a partir de los valores ingresados para la estrategia de negocio y la tabla de asignación del factor de diseño 1, Tabla 15, para puntuar cada objetivo de Gobierno y Gestión.

$$FD1_{i,j} = \sum_{k=1}^{40} \frac{TPFD1_{i,k} EE_{k,j}}{4}$$

donde: FD140x1 matriz resultante del factor de diseño 1

TPFD140x4 matriz de la tabla de puntuación del factor de diseño 1

EE4x1 matriz de estrategia empresarial

Tabla 17*Tabla asignación Factor de diseño 1*

FD1	Estrategia empresarial				
	Crecimiento/ Adquisición	Innovación/ Diferenciación	Liderazgo en costos	Servicio al cliente/ estabilidad	
O1	1	1	1.5	1.5	
O2	1.5	1	2	3.5	
O3	1	1	1	2	
O4	1.5	1	4	1	
O5	1.5	1.5	1	2	
O6	1	1	1	1	
O7	3.5	3.5	1.5	1	
O8	4	2	1	1	
O9	1	4	1	1	
O10	3.5	4	2.5	1	
O11	1.5	1	4	1	
O12	2.5	1.5	1.5	1.5	
O13	1	1.5	1	3.5	
O14	1	1	1.5	4	
O15	1	1	3.5	1.5	
O16	1	1	1	4	
O17	1	1.5	1	2.5	
O18	1	1	1	2.5	
O19	1	1	1	1	
O20	4	2	1.5	1.5	
O21	1	1	1.5	1	
O22	1	1	1.5	1	
O23	1	1	1	3	
O24	4	2	1	1.5	
O25	2	2	1	1.5	
O26	1.5	2	1	1.5	
O27	1	3.5	1	1	
O28	1	1	1	1	
O29	1	1	1	1	
O30	3.5	3	1.5	1	
O31	1	1	1	1.5	
O32	1	1	1	4	
O33	1	1	1	3	
O34	1	1	1	4	
O35	1	1	1	2.5	
O36	1	1	1	1.5	
O37	1	1	1	1	
O38	1	1	1	1	
O39	1	1	1	1	
O40	1	1	1	1	

5.2.4.2 Factor de diseño 2 – Metas empresariales

Para el cálculo de los factores de diseño se debe realizar un cálculo de doble matriz en base a los valores ingresados para el objetivo de negocio, la tabla de asignación entre el objetivo de negocio y el objetivo de asignación, ver Tabla 16.

$$RP_{i,j} = \sum_{k=1}^{13} \frac{ME_{i,k} TPMEA_{k,j}}{4}$$

donde:	RP1x13	matriz Resultante Parcial
	ME1x13	matriz de metas empresariales
	TPMEA13x13	matriz de la tabla de puntuación entre Metas empresariales y asignación

Con base en los resultados del primer cálculo de RP1, realizamos un cálculo de matriz utilizando la tabla de asignación entre las metas de asignación y la tabla de puntuación para el factor de diseño 2, consulte la Tabla 17, para obtener una puntuación de referencia para cada objetivo de Gobierno y Gestión.

$$FD2_{i,j} = \sum_{k=1}^{13} \frac{RP_{i,k} TPMEA_{k,j}}{4}$$

donde:	FD2 _{1x40}	Matriz Factor de Diseño 2
	RP _{1x13}	Matriz Resultante Parcial
	TPFD2 _{13x40}	Matriz de la tabla de puntuación factor de diseño 2.

Tabla 18*Tabla puntuación de Metas empresariales y de alineamiento*

	FD2:1	Metas de Alineamiento												
		MA1	MA2	MA3	MA4	MA5	MA6	MA7	MA8	MA9	MA10	MA11	MA12	MA13
Metas Empresariales	ME1			S		P	P		P	P				P
	ME2	S	P	S		P	P	P	P	P		S		P
	ME3	P	P					P				P		S
	ME4	P			P						P	P		S
	ME5				P						P			
	ME6			S	P	S	S		P	S	P		S	
	ME7			S	P	S	S		P	S	P		S	
	ME8			S	P	S	S		S	S	P			
	ME9			S	P	S	S		S	S	S			
	ME10			S	P				S	S	S		P	
	ME11	S							S			P	P	
	ME12	S		P		S	S		P	P		P		S
	ME13			P		S	S		S	S				P

Tabla 19*Tabla de puntuación Factor de Diseño 2*

FD2:2	Metas de Alineamiento												
	MA1	MA2	MA3	MA4	MA5	MA6	MA7	MA8	MA9	MA10	MA11	MA12	MA13
O1	P	S	P					S			S		
O2			P		S	S		S					S
O3	S	P					P				S		
O4			S		S	S		S	P			S	S
O5				S						P	S		
O6	S	S	P		S		S	S	S	S	P		
O7			S		S	S		P				S	P
O8			S		S	P	S	P					
O9			S			P		S				S	
O10			P		P	S		S	S				
O11			S	P					S	P			
O12			P		P				P			P	P
O13			S		P	P		S	S			P	P
O14					P			S					
O15					P	S			S				
O16			S	S	S				P	P			
O17		P					P						
O18	S	S					P						
O19	S	S		S			S			P			
O20			P			S		S	P				
O21			S		P	P		S	P			S	
O22			S		P	P		S	P				
O23					P		S		S				

Objetivos Empresariales

O24			P		S	S		P	P			S	
O25		S			S			P	S				
O26		S						P				S	
O27			S					S		S			P P
O28				P								S	
O29					S		P						
O30			P		S	P					P		
O31					P				S				
O32		S			P			S					
O33		S			P			S					
O34		S			P			P					
O35	S	P			S		P					S	
O36		S			S		S	P				S	
O37	S		S		P					S	P	S	
O38	S	S		S	S		S			S	S	P	
O39	P											S	
O40	S	S		S	S		S				S	P	

5.2.4.3 Factor de diseño 3 – Riesgos de ciberseguridad:

Para calcular el factor de diseño, se debe realizar un cálculo matricial con base en el valor de riesgo de ciberseguridad ingresado y la tabla de asignación para el factor de diseño 3, Tabla 18, para puntuar cada objetivo de Gobierno y Gestión.

$$FD3_{i,j} = \sum_{k=1}^{19} \frac{TPFD3_{i,k} RC_{k,j}}{4}$$

donde: $FD_{3 \times 40}$ Matriz del factor de diseño 3

$TPFD_{3 \times 40 \times 19}$ Matriz para la tabla de puntuación del factor de diseño 3

$RC_{19 \times 1}$ Matriz de riesgos de ciberseguridad

Tabla 20

Tabla de puntuación Factor de diseño 3

FD3	Riesgo de Ciberseguridad																		
	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14	R15	R16	R17	R18	R19
O1	3	2	3	0	0	0	2	0	0	0	0	0	3	2	0	0	2	2	2
O2	3	2	0	0	2	0	0	0	0	0	0	0	1	0	0	0	3	1	3
O3	2	2	0	0	0	0	0	0	0	1	2	0	3	3	0	0	0	2	3
O4	3	0	4	3	2	0	0	0	0	0	0	2	1	0	2	0	0	2	3
O5	3	1	3	0	0	0	2	0	0	1	0	1	3	3	0	0	0	2	2
O6	2	3	2	0	2	2	4	2	0	2	3	3	3	0	0	0	3	2	3
O7	2	0	0	0	3	0	0	2	1	0	1	2	0	0	0	0	2	2	1
O8	2	0	0	0	4	0	0	2	0	2	2	2	0	0	0	0	2	0	3
O9	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	4	0	0
O10	4	2	2	0	2	0	0	2	2	0	0	0	0	0	0	0	2	0	0
O11	2	3	4	0	0	0	0	0	0	0	0	2	0	2	0	0	2	2	0
O12	0	0	0	4	0	2	3	3	0	0	2	0	0	2	4	0	2	2	0
O13	0	0	0	2	2	0	0	4	0	0	2	2	0	0	0	0	3	0	2
O14	0	0	2	0	0	0	2	3	0	1	2	3	0	0	0	0	0	0	0
O15	0	2	3	0	0	0	2	2	3	2	2	4	2	2	0	0	0	0	0
O16	0	3	0	0	0	0	0	2	0	4	0	0	0	0	0	0	0	0	2
O17	0	0	0	0	0	0	3	0	0	2	3	0	0	0	0	2	0	0	0
O18	0	0	0	0	0	0	4	0	0	0	4	0	3	0	0	0	0	0	0

O19	0	0	0	0	0	0	3	2	0	0	2	0	3	0	2	4	2	0	4
O20	0	4	0	0	2	0	0	3	0	0	0	0	0	0	0	0	0	0	0
O21	2	2	0	0	2	0	0	3	0	2	2	0	0	0	0	0	0	0	0
O22	0	3	0	0	2	0	0	2	0	3	3	0	0	0	0	0	0	0	0
O23	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
O24	0	2	0	2	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0
O25	0	0	0	0	0	3	4	0	0	2	3	0	0	0	0	0	0	0	3
O26	0	0	0	0	0	2	3	2	0	4	2	0	0	0	0	0	0	0	0
O27	0	0	0	2	0	3	0	3	0	3	0	0	0	0	2	0	0	0	2
O28	0	0	0	0	0	1	3	0	0	0	0	0	0	0	0	0	0	0	0
O29	0	0	0	0	0	2	4	0	0	2	3	0	0	0	0	0	0	0	0
O30	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
O31	0	0	0	0	0	4	3	0	4	0	2	0	0	0	0	0	0	2	0
O32	0	0	0	0	0	3	2	3	2	2	4	0	0	0	0	0	0	0	0
O33	0	0	0	0	0	3	1	4	0	3	1	0	0	0	0	0	0	0	0
O34	0	0	0	0	0	3	3	0	3	0	4	0	2	0	3	4	0	0	2
O35	0	0	0	0	0	3	4	0	2	0	4	0	3	0	3	2	0	0	3
O36	0	0	0	0	0	3	4	2	0	0	2	0	2	0	0	0	0	0	3
O37	1	2	2	0	0	2	2	0	0	2	3	2	2	2	0	2	0	0	2
O38	1	2	2	0	0	3	3	0	0	2	3	2	2	3	0	2	0	0	2
O39	0	1	0	0	0	1	2	0	0	0	3	2	4	2	0	0	0	0	2
O40	1	2	0	0	0	0	3	0	0	2	3	2	2	4	0	2	2	0	2

5.2.4.4 Factor de diseño 4 - Problemas relacionados con IACS:

Para calcular los factores de diseño, se debe realizar un cálculo matricial para calificar cada objetivo de diseño con base en los valores ingresados para los problemas relacionados con IACS y la tabla de asignación para el factor de diseño 4, Tabla 19. Resultando en un puntaje para cada objetivo de Gobierno y Gestión para el Factor de diseño 4.

$$FD4_{i,j} = \sum_{k=1}^{20} TPF4_{i,k} PR_{k,j}$$

donde: $FD4_{40 \times 1}$ Matriz del factor de diseño 4

$TPFD4_{40 \times 20}$ Matriz para la tabla de puntuación del factor de diseño 4

$PR_{20 \times 1}$ Matriz de problemas relacionadas con el IACS

Tabla 21

Tabla puntuación Factor de diseño 4

FD4		Problemas Relacionados con Ciberseguridad																			
		P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20
Objetivos Empresariales	O1	3	3	1	1	2	2	2	1	1	1	3	3.5	1	1	1	1	2	3	1.5	1
	O2	2.5	3	1	1	1.5	2.5	2	1.5	0.5	2.5	1.5	1	3	2	1	1	2	2	1	2.5
	O3	1	1	2	1	2	2	1	1	0	0.5	1	0	1	1.5	1	2	1	1	2.5	1
	O4	1	1	1	1	1	2	3	3.5	3.5	1	1.5	0	4	2	1	1.5	2	2.5	0	1
	O5	1	1	1	1	1.5	2	1	1	0	1	3	1.5	1.5	0.5	0	0.5	1	1	1	0
	O6	2	1	2	1	2	2	1	1	0	0.5	1.5	4	1	2	1	1	1.5	2	0.5	1
	O7	1.5	1.5	1.5	1	1	1.5	1	1	0	1	2.5	0.5	0.5	1.5	1.5	0.5	2	2	0	2.5
	O8	1	1.5	1	1.5	0.5	1.5	2	1.5	1	3.5	0.5	0.5	1	4	1	3.5	2	3	0	2
	O9	1	1	1	2	0.5	0.5	0.5	0.5	0	0	0.5	1	0.5	2	1	0	0.5	0.5	0	4
	O10	3	3	1	1	2	2	1.5	3.5	0.5	2	2	1.5	2	1	0.5	0	2.5	2.5	0	2
	O11	3.5	2	1	1.5	1.5	2	4	3	1	2	1	1.5	4	0	0	0	1	2	0	0
	O12	2	1.5	1.5	2	1.5	2	2.5	2.5	4	1.5	0.5	0.5	1.5	0.5	4	0.5	1	1	2	1.5
	O13	2.5	2	1	1	1.5	1	2.5	2	1.5	1	3	1	0.5	1	4	1	3	3.5	0	0.5
	O14	2	1.5	2	2.5	1	2.5	1.5	2	0.5	1	0	0	1	0	0	0	1	1.5	0	0

O15	1	1	2	4	1.5	1.5	1.5	0	1.5	1	0	0	1	0	0	0	0.5	2	1	0
O16	1	1	3	4	1	3	0	0	0	2	0	0	0	0.5	0.5	3	2	2	0	1
O17	1	0.5	2.5	1.5	2	2	1	1	0.5	1	1	1	1	1	1	2	1	1.5	2.5	1
O18	0	0	3.5	1.5	2	1	0	1	0	0.5	0	0	0	0	0	1.5	2	1	2	1
O19	1	1.5	3	1	2.5	1.5	1	1.5	0	1.5	0	0	0.5	2.5	0.5	4	2.5	2	3	0.5
O20	0	1	1.5	1	0	0	0	3	1	3.5	0	0	1.5	0.5	1	0	1.5	2	0	1
O21	0	3	0	0	0.5	2	0	2	0	3.5	0	1	1	2	2	1.5	2.5	3	0.5	1
O22	1	2	2	0	0	2	0	1	0	3	0	0.5	1	1	1	0.5	2	2	1	0.5
O23	0.5	0	2	0	0	2	0	0	0	0	0	0	0.5	0	0	1	1	1	0	0.5
O24	1	3	0	3	0	0	0	0.5	0	3	1	0	0	0.5	2	0	0.5	1.5	0	1
O25	0	0	2.5	0	0.5	1.5	0	1	0	1.5	0	1	0.5	1	0.5	2	2	2	1	1
O26	0	1	2	3	0.5	1.5	0	0.5	0	2	0	1	0	1	0.5	2	2	2	0	1
O27	0	0	0	2	0.5	0.5	0	1	2	0.5	0	0.5	0	1	3	2	1	1.5	0	0.5
O28	0.5	0.5	1	1.5	0	0	2	2	0	0	0	0	2	1	0	0	1	1.5	0	0
O29	0	0	2.5	0	0.5	0	0	0.5	0	0	0	0	1	1.5	0	1.5	1	2	0	0
O30	1	2	2.5	2	0	0	2	3	1	4	0	0	1.5	2	0.5	0	1	1.5	0	0.5
O31	0	0	2.5	0	1	2	0	0.5	0	0	0	0	1	0	0	1.5	1	2	0	0
O32	1	1	4	2	1	2.5	0	0	0	0	0	0	1	0	0	1	1	1	0	0
O33	0	1	3	3	0	3	0	0	0	0	0	0	0	1	1.5	1	1	1	0	0
O34	0	0	3	3	2	0	0	0	0	0	0	0	0	0	0	1.5	1	2	0	0
O35	0	0	4	1	2	0	0	0	0	0	0	0	0	0	0	1.5	1	2	2	0
O36	0	1	0.5	2	3	0.5	0	0	0	1	0	0	0	0	1.5	2.5	1.5	1	2	0
O37	1	1.5	2	0	2.5	3	1	2	1.5	1	1	1	2	1	1	1	1.5	1	2.5	1
O38	0	0	2	2	2.5	2	2	0	0.5	2	1	1	1.5	1	0	2	1	1	2.5	0
O39	0	0	2	2	4	0.5	0	0	0	0	0	0	0	0	0	2	0	0	4	0
O40	1	1	3	1.5	3	4	2	1	1	0.5	1	1	1.5	0	1	1	1	1	2.5	1

5.2.4.5 Factor de diseño 5 – Escenario de amenaza:

Para calcular el factor de diseño se debe realizar un cálculo matricial a partir de los valores ingresados para el escenario de amenaza y la tabla de asignación para el factor de diseño 5, Tabla 20, para puntuar cada objetivo de Gobierno y la Gestión del factor de diseño 5.

$$FD5_{i,j} = \sum_{k=1}^2 TPF5_{i,k} EA_{k,j}$$

donde: FD540x1 Matriz de factor de diseño 5
 TPF540x2 Matriz para la tabla de puntuación del factor de diseño 5
 EA2x1 Matriz de escenario de amenazas

Tabla 22

Tabla puntuación Factor de diseño 5

FD5	Escenario de Amenaza	
	Alto	Normal
O1	3	1
O2	1	1
O3	4	1
O4	1	1
O5	2	1
O6	3	1
O7	1	1
O8	3	1
O9	1	1
O10	1	1
O11	1	1
O12	2	1
O13	1	1
O14	2	1
O15	3	1
O16	2	1
O17	4	1
O18	4	1
O19	3	1
O20	1	1
O21	1	1
O22	1	1
O23	2	1

Objetivos Empresariales

O24	1	1
O25	3	1
O26	1	1
O27	1	1
O28	1	1
O29	3	1
O30	1	1
O31	1	1
O32	3	1
O33	2	1
O34	4	1
O35	3	1
O36	3	1
O37	3	1
O38	2	1
O39	3	1
O40	3	1

5.2.4.6 Factor de diseño 6 - Requisitos de cumplimiento:

Para el cálculo del Factor de Diseño se debe realizar un cálculo matricial en base a los valores ingresados para los requisitos de cumplimiento y la tabla de Asignación del Factor de Diseño 6, Tabla 21, para puntuar cada objetivo de Gobierno y Gestión del Factor de Diseño 6.

$$FD6_{i,j} = \sum_{k=1}^3 TPF6_{i,k} RC_{k,j}$$

donde: FD640x1 Matriz de factor de diseño 6

 TPF640x3 Matriz para la tabla de puntuación del factor de diseño 6

 RC3x1 Matriz de requisitos de cumplimiento

Tabla 23*Tabla de puntuación Factor diseño 6*

FD6	Requisitos de Cumplimiento		
	Alto	Normal	Baja
O1	3	2	1
O2	1	1	1
O3	4	2	1
O4	1	1	1
O5	1.5	1	1
O6	2	1.5	1
O7	1	1	1
O8	1	1	1
O9	1	1	1
O10	1	1	1
O11	1	1	1
O12	1.5	1.5	1.5
O13	1	1	1
O14	1	1	1
O15	1.5	1	1
O16	1	1	1
O17	4	2	1
O18	1.5	1	1
O19	2	1.5	1
O20	1	1	1
O21	1	1	1
O22	1	1	1
O23	1	1	1
O24	1	1	1
O25	1	1	1
O26	1	1	1
O27	1	1	1
O28	1	1	1
O29	1	1	1
O30	1	1	1
O31	1	1	1
O32	1	1	1
O33	1	1	1
O34	1.5	1	1
O35	2	1	1
O36	1	1	1
O37	1	1	1
O38	1	1	1
O39	4	2	1
O40	3.5	2	1

Objetivos Empresariales

5.2.4.7 Factor de diseño 7 - Rol de ciberseguridad:

Para calcular el factor de diseño se debe realizar un cálculo matricial a partir de los valores ingresados para el rol de ciberseguridad y la tabla de asignación para el factor de diseño 7, Tabla 22, para puntuar cada objetivo de Gobierno y Gestión del Factor de Diseño 7.

$$FD7_{i,j} = \sum_{k=1}^4 TPF7_{i,k} RCI_{k,j}$$

donde: FD740x1 Matriz de factor de diseño 7
 TPF740x4 Matriz para la tabla de puntuación del factor de diseño 7
 RCI4x1 Matriz de Rol de ciberseguridad

Tabla 24

Tabla puntuación Factor de diseño 7

FD7	Rol de Ciberseguridad			
	Soporte	Fábrica	Cambio	Estratégico
O1	1	2	1.5	4
O2	1	1	2.5	3
O3	1	3	1	3
O4	1	1	1	2
O5	1	1	1	2
O6	1	1.5	1.5	2.5
O7	1	1	3	3
O8	1	1	2	2
O9	0.5	1	3.5	4
O10	1	1	2.5	3
O11	1	1	1	2
O12	1.5	1.5	1.5	2
O13	1	1	2	2.5
O14	1	2	1.5	2
O15	1	2.5	1.5	2
O16	1	1.5	1.5	2
O17	1	2.5	1	3
O18	1	2	1.5	3
O19	1	1.5	1.5	2.5
O20	1	1	2	2.5
O21	1	1	3	3
O22	1	1	3	3

O23	1	2.5	1.5	2
O24	1	1	1	2
O25	1	2.5	1	2
O26	1	1	2	2
O27	1	1	1	2
O28	1	1	1	2
O29	1	1.5	1	2
O30	1	1	2	2
O31	1	3.5	1	3
O32	1	3	1.5	3
O33	1	3	1.5	3.5
O34	1	3	1.5	3.5
O35	1.5	2.5	1.5	3.5
O36	1	1	1	2.5
O37	1	1	1	2
O38	1	1	1	2
O39	1	1	1	1.5
O40	1	1	1	2

5.2.4.8 Factor de diseño 8 - Modelo de abastecimiento de proveedores:

Para el cálculo del factor de diseño se debe realizar un cálculo matricial a partir de los valores ingresados para el modelo de contratación de proveedores, donde la tabla de asignación para el factor de diseño 8, Tabla 23, para puntuar cada objetivo de Gobierno y Gestión del Factor de Diseño 8.

$$FD8_{i,j} = \sum_{k=1}^2 TPF8_{i,k} AP_{k,j}$$

donde: FD840x1 Matriz de factor de diseño 8
 TPF840x3 Matriz para la tabla de puntuación del factor de diseño 8
 AP3x1 Matriz de Modelo de abastecimiento de proveedores

Tabla 25

Tabla puntuación Factor de diseño 8

FD8		Modelo de Abastecimiento de Proveedores		
		Externalización	Nube	Personal interno
Objetivos	O1	1	1	1
	O2	1	1	1
	O3	1	2	1

O4	1	1	1
O5	1	1	1
O6	1	1	1
O7	1	1	1
O8	1	1	1
O9	1	1	1
O10	1	1	1
O11	1	1	1
O12	1	1	1
O13	1	1	1
O14	4	4	1
O15	4	4	1
O16	1	1	1
O17	2	2	1
O18	1	1	1
O19	1	1	1
O20	1	1	1
O21	1	1	1
O22	1	1	1
O23	1	1	1
O24	1	1	1
O25	1	1	1
O26	1	1	1
O27	1	1	1
O28	1	1	1
O29	1	1	1
O30	1	1	1
O31	1	1	1
O32	1	1	1
O33	1	1	1
O34	1	1	1
O35	1	1	1
O36	1	1	1
O37	3	3	1
O38	1	1	1
O39	1	1	1
O40	1	1	1

5.2.4.9 Factor de diseño 9 - Estrategia de adopción de tecnología:

Para el cálculo del factor de diseño se debe realizar un cálculo matricial a partir de los valores ingresados para el modelo de contratación de proveedores, donde la tabla de asignación para el factor de diseño 9, Tabla 24, para puntuar cada objetivo de Gobierno y Gestión del Factor de Diseño 9.

$$FD9_{i,j} = \sum_{k=1}^3 TPF9_{i,k} \cdot AT_{k,j}$$

donde: FD940x1 Matriz de factor de diseño 9
 TPF940x3 Matriz para la tabla de puntuación del factor de diseño 9
 AT3x1 Matriz de Estrategia de adopción de tecnologías

Tabla 26

Tabla de puntuación de Factor de diseño 9

FD9	Estrategia de adopción de tecnología		
	Adoptadores pioneros	Seguidor	Adoptador lento
O1	3.5	2.5	1.5
O2	4	2.5	1.5
O3	1.5	1	1
O4	2.5	2	1.5
O5	1.5	1	1
O6	2.5	1.5	1
O7	4	3	1.5
O8	2	1	1
O9	4	3	1
O10	4	2.5	1
O11	1	1.5	1
O12	3	2.5	1.5
O13	3	1.5	1
O14	1.5	1.5	1
O15	2.5	1.5	1
O16	1.5	1.5	1
O17	2	1.5	1
O18	1	1	1
O19	2.5	2	1
O20	4	3	1.5
O21	3.5	2.5	1
O22	4	2.5	1
O23	1.5	1.5	1
O24	3	2	1
O25	2.5	2	1
O26	3.5	2.5	1
O27	1.5	1	1
O28	1	1	1
O29	1.5	1	1
O30	3.5	2.5	1
O31	1	1	1
O32	1	1	1

O33	1.5	1	1
O34	1.5	1	1
O35	1.5	1	1
O36	1	1	1
O37	3	2	1
O38	1	1	1
O39	1	1	1
O40	1	1	1

5.2.5 Ejecución del marco de trabajo

El área usuaria y/o encargado de ciberseguridad industrial debe de responder los cuestionarios de los 9 Factores de diseño, en cada uno de ellos deberá responder sobre la situación actual y el contexto en el que se encuentra su empresa. Una vez que se hayan resuelto los nueve cuestionarios, la herramienta agregará todos los factores de diseño para cada gobierno y objetivo regulatorio.

$$RFD_{i,j} = \sum_{n=1}^9 FDN_{i,j}$$

donde: RFD40x1 matriz resultante de los factores de diseño
 FDN 40x1 matriz del factor de diseño “n”
 n corresponde al número de factor de diseño

Finalmente, de la matriz resultante se procederá a ordenar descendientemente a fin de ubicar los 6 primeros objetivos con mayor puntaje que serán los Objetivos priorizados para el gobierno y gestión de ciberseguridad y que servirá para que el área usuaria y/o encargado defina en su Comité si abordarán todos ellos o parcialmente de acuerdo con la recomendación que brinda la herramienta.

En la segunda parte de los cuestionarios, Requisitos de Ciberseguridad, el área usuaria y/o encargado de ciberseguridad industrial deberá responder a cada uno de los Requerimientos de Seguridad (SR) puntuando sobre la situación actual que tiene en cada uno de ellos y también sobre el nivel Objetivo al cual aspira la empresa, la herramienta le proporcionará el listado de Controles que debe de cumplir para su nivel actual,

permitiéndole sincerar si está puntuado correctamente o aún le hace falta la implementación de algún control para llegar a su nivel actual. También, se le otorgará un listado de controles que deberá implementar en un siguiente paso para así lograr el nivel objetivo. Con todo ello, la herramienta finalmente le otorgará el porcentaje de Controles que hacen falta implementar para que pueda tener una métrica porcentual para medir su desempeño en Implementación de los Controles de Ciberseguridad Industrial.

Capítulo VI. Protocolo de Validación

En este capítulo se realiza el protocolo de validación del artefacto, para ello las organizaciones emplearán la herramienta diseñada, responderán los cuestionarios lo cual permitirá el desarrollo de los factores de diseño para obtener una lista priorizada de objetivos.

6.1 Proceso de validación del artefacto

Para realizar el proceso de validación del artefacto, la herramienta brinda una serie de cuestionarios en base a los factores de diseño que serán puntuados de acuerdo con la realidad de cada organización.

6.1.1 Estrategia empresarial:

Esto permite traducir las políticas definidas por la organización en puntajes de prioridad para los objetivos de gobierno y gestión. Las asignaciones para cada posible valor establecido en la Tabla 7 se clasifican en una escala de uno (0) a cuatro (4): 4 es MUY ALTA y 0 es MUY BAJA.

Tabla 27

Niveles de prioridad de estrategias empresariales

Niveles de prioridad	
Muy Alta	4
Alta	3
Media	2
Baja	1
Muy baja	0

6.1.2 Metas empresariales:

Una vez evaluada la estrategia de negocio de la organización, existe una base para realizar un análisis de las metas empresariales en los siguientes factores de diseño, los cuales definen un conjunto de 13 metas empresariales genéricas identificados en la Tabla 8, los cuales deben ser priorizados de acuerdo con lo establecido. estrategia considerar

Los valores se asignan en base a los siguientes criterios de puntuación: 4 indica la MUY ALTA y 0 indica MUY BAJA.

Tabla 28

Niveles de prioridad de metas empresariales

Niveles de prioridad	
Muy Alta	4
Alta	3
Media	2
Baja	1
Muy baja	0

6.1.3 Perfil de riesgo:

Este factor de diseño determinará el riesgo al que está expuesta la empresa. Se plantean una serie de escenarios que en el sector industrial se encuentran presentes y las organizaciones deberán medir su nivel de riesgo.

Tabla 29

Mapa de calor de la matriz de riesgo

Impacto/ Riesgo	1	2	3	4	5
1	BAJO	BAJO	BAJO	NORMAL	NORMAL
2	BAJO	NORMAL	NORMAL	NORMAL	ALTO
3	BAJO	NORMAL	ALTO	ALTO	MUY ALTO
4	NORMAL	NORMAL	ALTO	MUY ALTO	MUY ALTO
5	NORMAL	ALTO	MUY ALTO	MUY ALTO	MUY ALTO

Tabla 30

Relación impacto / riesgo

Nivel de Riesgo	Puntuación
BAJO	<4
NORMAL	<9
ALTO	<13
MUY ALTO	>13




De acuerdo a los escenarios establecidos en la herramienta mediante la Tabla 9, cada responsable debe ver su impacto y probabilidad de ocurrencia para definir su nivel de riesgo.

6.1.4 Problemas relacionados con la ciberseguridad

Para proporcionar un análisis de los problemas relacionados a ciberseguridad que la organización experimenta, se definen un conjunto de 20 problemas relacionados, de acuerdo con lo mostrado en la Tabla 10, que deben priorizarse de acuerdo con los objetivos de gobierno y gestión. Para comprobar su adecuación a la situación real de la organización que está siendo analizado se define:

Tabla 31

Medición nivel existencia de problema

	La empresa no tiene problemas relacionados con ciberseguridad industrial	Ningún problema
	La empresa tiene problemas relacionados con ciberseguridad industrial	Con problema
	La empresa tiene graves problemas relacionados con ciberseguridad industrial	Problema grave

6.1.5 Escenario de amenazas

Permite determinar los valores más adecuados para las operaciones de la organización al utilizar la herramienta, teniendo en cuenta las dos opciones posibles correspondientes a este factor de diseño: ALTO y NORMAL, de acuerdo a lo definido en la Tabla 11. Los factores de diseño de escenarios de amenazas en cada categoría se clasificaron en un 100 %.

6.1.6 Requisitos de cumplimiento

Permite determinar los valores más apropiados para las políticas y su cumplimiento establecidos en la organización al utilizar la herramienta, en base a cada una de las dos posibles entradas correspondientes a este factor de diseño: ALTO,

NORMAL y BAJO, de acuerdo a lo definido en la Tabla 12. Los factores de diseño de escenarios de amenazas clasificados al 100 % en cada categoría.

6.1.7 Rol de la ciberseguridad

Este factor evalúa los cuatro posibles parámetros del Rol de ciberseguridad definidos en la Tabla 13. Considerando el estado actual de la organización, se evaluó esta matriz de factores de diseño, con un valor de escala entre cero (0) y cuatro (4): 0 es MUY BAJA y 4 es MUY ALTA.

Tabla 32

Niveles de Rol de Ciberseguridad

Niveles de prioridad	
Muy Alta	4
Alta	3
Media	2
Baja	1
Muy baja	0

6.1.8 Modelo de abastecimiento

Este factor evalúa los tres posibles modelos de abastecimiento de acuerdo a lo establecido en la Tabla 14. El análisis de cada uno de los tres valores posibles para el factor de diseño del modelo de suministro del proveedor, que tiene un valor entre 0% y 100%. La suma de los tres valores debe ser 100%.

6.1.9 Estrategia de adopción tecnológica

Este factor evalúa las 3 estrategias de adopción tecnológicas de acuerdo a lo establecido en la Tabla 15. El análisis para cada una de estas tres estrategias varía de 0% a 100%. La suma de los tres valores debe ser 100%.

6.2 Resultados de la validación

Para la puesta a prueba de la herramienta realizamos un muestreo con 3 personas de organizaciones que pertenecen al sector industrial las cuales son: Empresa 1 – Sector Hidrocarburos, Empresa 2- Sector Cementero y Empresa 3-Sector Minero. Se muestra una comparativa entre cada uno de los intervenidos mostrando su realidad frente a la ciberseguridad y al sector de la organización:

6.2.1 Estrategia empresarial:

En las tres figuras adjuntas podemos ver como se una clara diferencia en el tipo de estrategia empresarial adopta cada una de las organizaciones de muestra, en la estrategia 1 de “Crecimiento/Adquisición” es la más desarrollada, por otro lado en la estrategia 2 “Innovación/Diferenciación” es lo contrario lo cual indica que están estandarizados de forma muy similar y no buscar una mejora u optimización mediante nuevos puntos de vista no es prioridad y abordan planes ya establecidos en el mercado actual.

Figura 14

FDI Empresa 1 Hidrocarburos

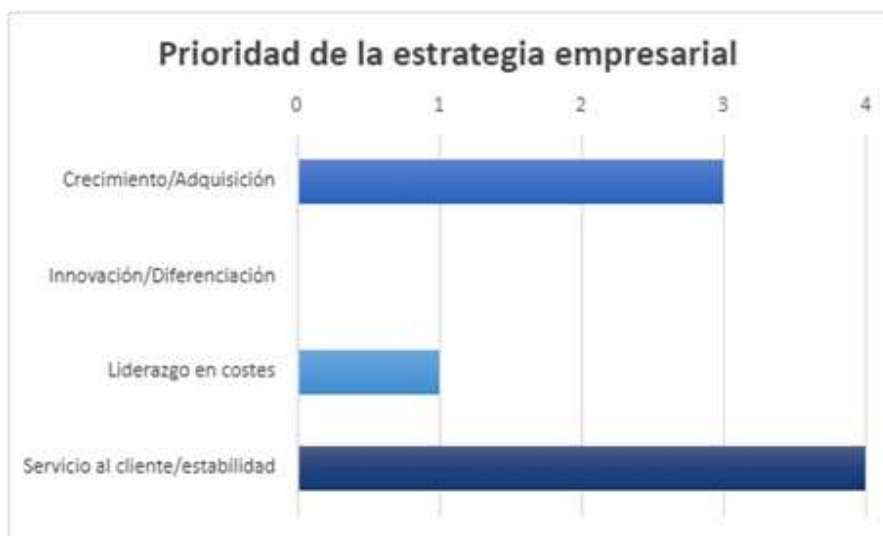


Figura 15

FDI Empresa 2 Cementera

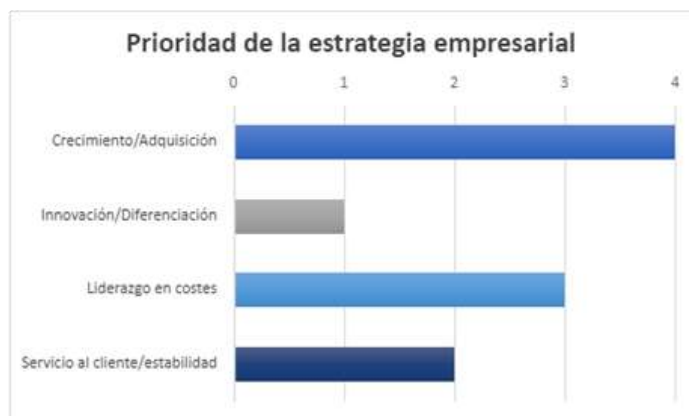
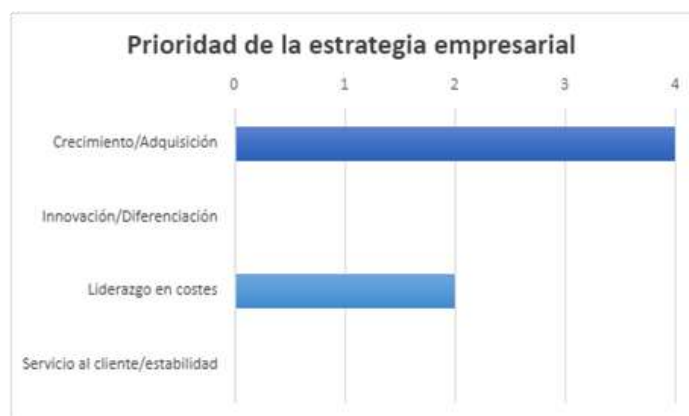


Figura 16

FD 1 Empresa 3 Minera



6.2.2 Metas empresariales:

En las 3 figuras adjuntas podemos visualizar de manera similar las metas orientadas al tipo de negocio de cada organización viendo que “Continuidad y disponibilidad del servicio del negocio”, “Cumplimiento de leyes y regulaciones externas” y “Calidad de la información financiera” como las más prioritarias a diferencia de “Gestión de riesgo del negocio”, “Optimización de la funcionalidad de los procesos internos del negocio” y “Gestión de programas de transformación digital” que tienen una prioridad de “MUY BAJA” lo cual indica que se toman en cuenta y se apuntan pero no presentan un gran impacto en las 3 organizaciones.

Figura 17

FD2 Empresa 1 Hidrocarburos



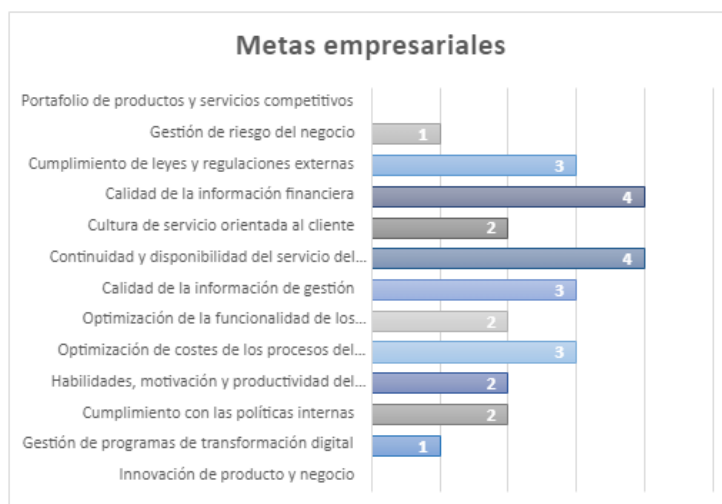
Figura 18

FD2 Empresa 2 Cementera



Figura 19

FD2 Empresa 3 Minera



6.2.3 Perfil de riesgo:

Las 3 figuras adjuntas presentan grandes diferencias en base a los lineamientos de la organización, para la organización del sector minero el más definido es el de “Problemas geopolíticos” esto se debe a que van de la mano no solo de la aceptación de los poblados cercanos si no también del cumplimiento de las políticas establecidas por el gobiernos y debido a esa políticas presentan controles mucho más definidos para la mitigación de incidentes ya sea en ciberseguridad o seguridad ocupacional, en cambio las otras 2 empresas que están orientados a la industria de producción y distribución definen un riesgo más altos para los escenarios “Incidentes de infraestructura operativa de ciberseguridad industrial”, “Incidentes de terceros/proveedores” y “Acciones no autorizadas” que están más orientados a la producción y distribución.

Figura 20

FD3 Empresa 1 Hidrocarburos

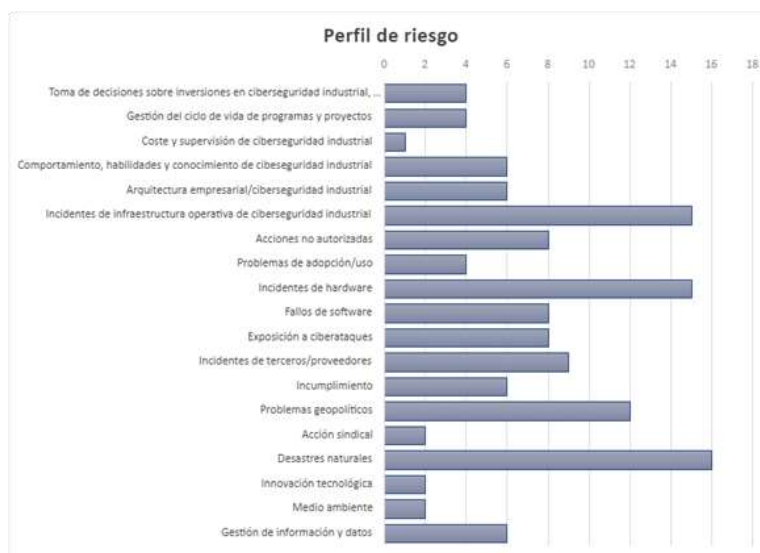


Figura 21

FD3 Empresa 2 Cementera

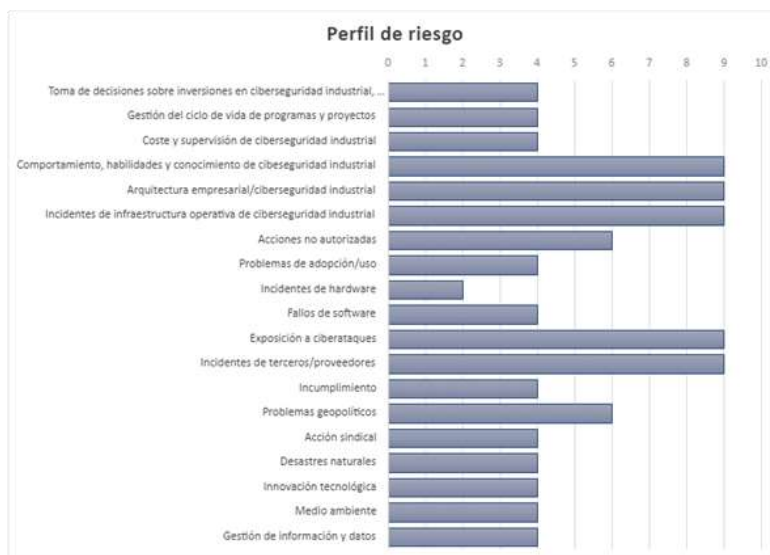
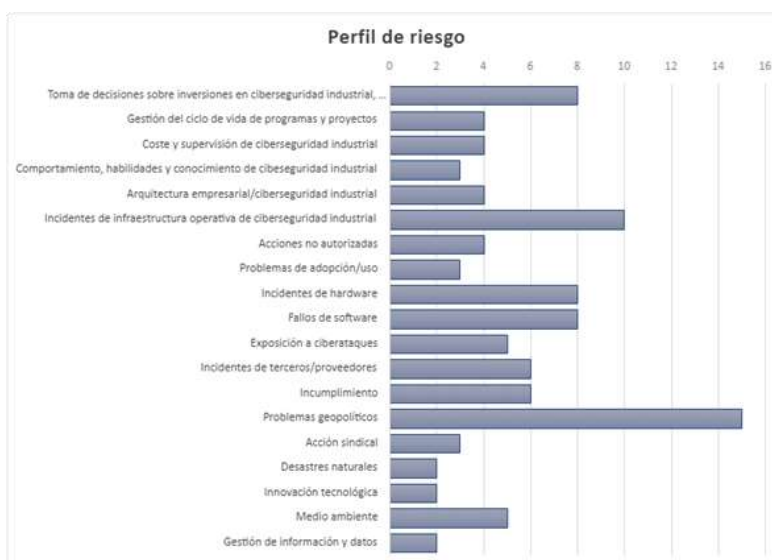


Figura 22

FD3 Empresa 3 Minera



6.2.4 Problemas relacionados con la ciberseguridad:

En las figuras adjuntas podemos ver problemas bastante remarcados los cuales serían P1, P9, P11, P13 y P20 lo cual demuestra que la poca conciencia en ciberseguridad que presentan las 3 organizaciones no solo por la parte administrativa sino también por los departamentos encargados de la infraestructura tecnológica que no brindaron la información y concientización de la importancia de estar protegidos y de nuevas tecnologías.

Figura 23

FD4 Empresa 1 Hidrocarburos

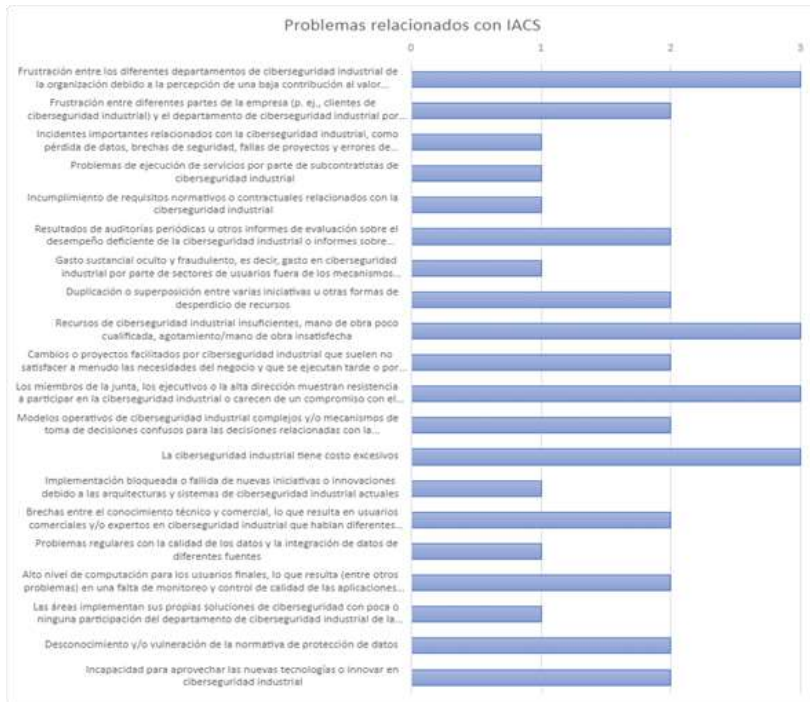


Figura 24

FD4 Empresa 2 Cementera

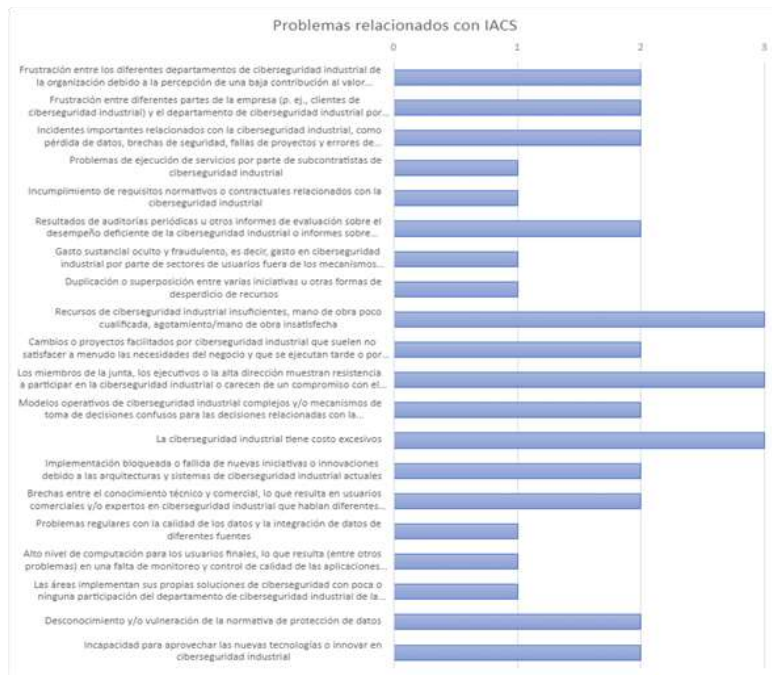


Figura 25

FD4 Empresa 3 Minera



6.2.5 Escenario de amenazas:

En las figuras adjuntas se mostró como las 3 organizaciones operan y clasifican los escenarios de amenaza alto o normal siendo la empresa del sector minero la que presenta en menor porcentaje un entorno de amenaza alta demostrando controles o procedimiento más desarrollados para mitigar el impacto cuando se presente ese escenario.

Figura 26

FD5 Empresa 1 Hidrocarburos

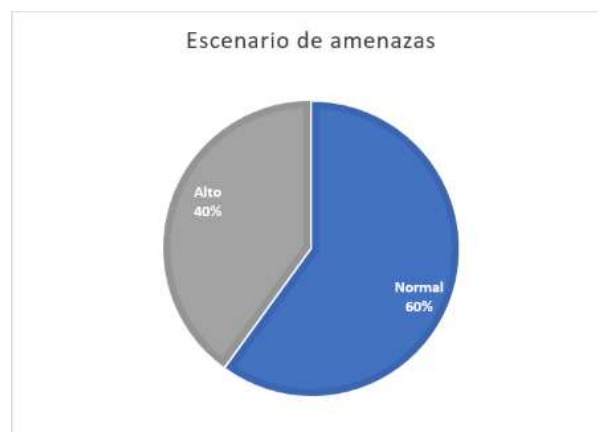
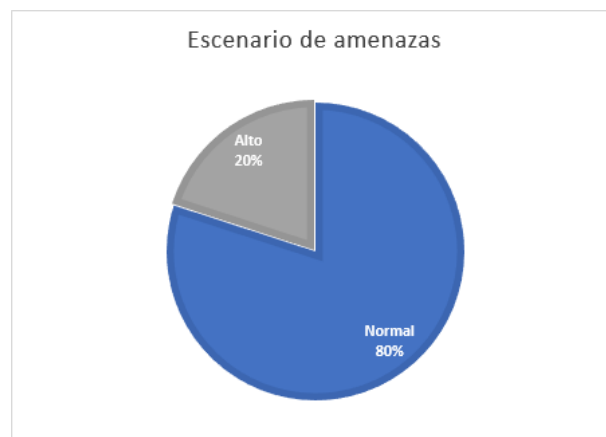


Figura 27*FD5 Empresa 2 Cementera***Figura 28***FD5 Empresa 3 Minera*

6.2.6 Requisitos de cumplimiento:

En las figuras adjuntas podemos observar un comportamiento más negligente frente al cumplimiento de los requisitos para la segunda organización, un escenario totalmente opuesto la tercera organización que demuestra los requerimientos comunes establecidos para el sector minero, la segunda organización demuestra un cumplimiento progresivo de los requisitos lo cual demuestra que apunta a un mejoramiento continuo.

Figura 29*FD6 Empresa 1 Hidrocarburos*

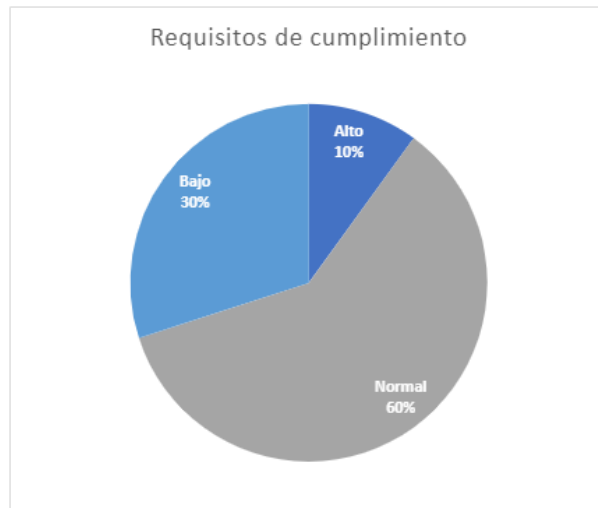


Figura 30

FD6 Empresa 2 Cementera

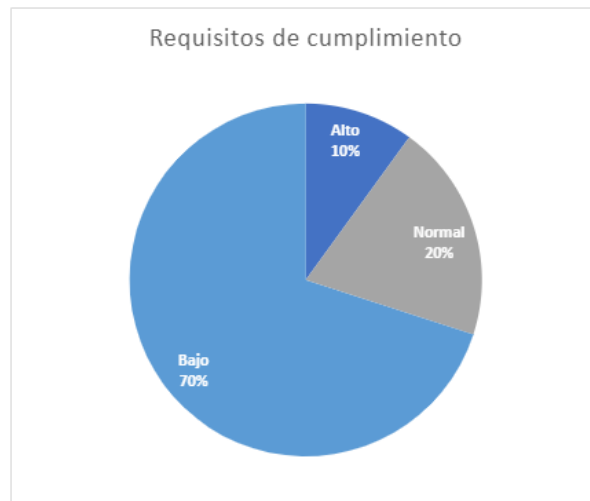


Figura 31

FD6 Empresa 3 Minera



6.2.7 Rol de la ciberseguridad

En las figuras adjuntas las 3 organizaciones le dan un nivel de criticidad muy alto al rol de “SOPORTE” y en segundo lugar el rol de “FABRICA” ya que son los roles de los cuales depende la continuidad operacional, de igual manera se percibe que los factores de innovación presentado en los roles de “CAMBIO” y “ESTRATEGICO” en las 3 organizaciones están presentes, pero no representan un nivel de criticidad adecuado.

Figura 32

FD7 Empresa 1 Hidrocarburos

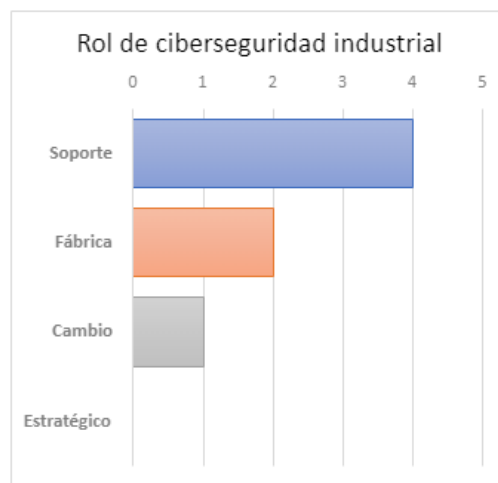


Figura 33

FD7 Empresa 2 Cementera

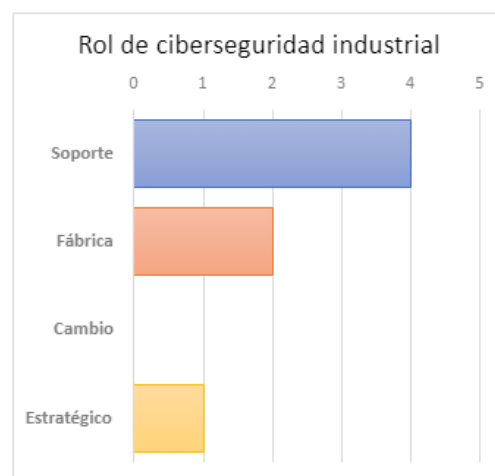
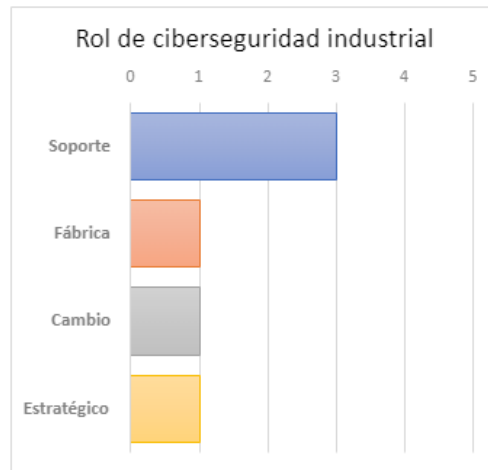


Figura 34

FD7 Empresa 3 Minera



6.2.8 Modelo de abastecimiento:

En las figuras adjuntas se demostró que la organización del sector minero es la única que optó por un enfoque en servicios en la nube, lo contrario a las otras organizaciones.

El enfoque mostrado para la organización del sector hidrocarburos es el de implementar sus propios controles internos en ciberseguridad a diferencia de la organización del sector cementero que optó por dejar las políticas de ciberseguridad a proveedores externos lo cual permite menor carga de responsabilidad, pero representa un riesgo en el desarrollo de estrategias internas.

Figura 35

FD8 Empresa 1 Hidrocarburos

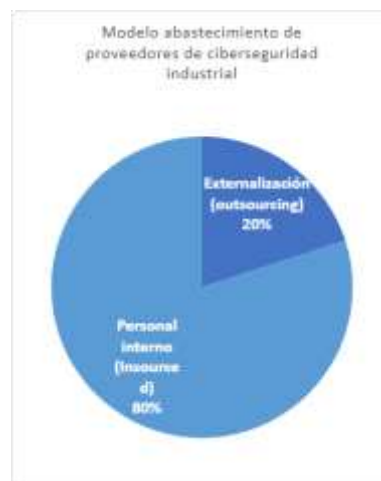
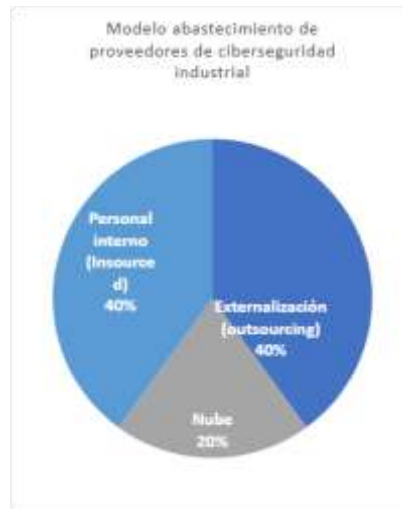
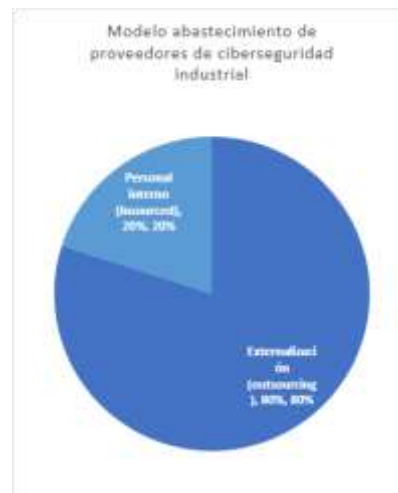


Figura 36*FD8 Empresa 2 Cementera***Figura 37***FD8 Empresa 3 Minera*

6.2.9 Estrategia de adopción tecnológica

En las 3 figuras adjuntas podemos visualizar que las organizaciones han optado por una postura muy desfasada frente las nuevas tecnologías, lo cual ha demostrado poco interés en la adquisición de estas por ende un retraso en las políticas de ciberseguridad.

Figura 38*FD9 Empresa 1 Hidrocarburos*



Figura 39

FD9 Empresa 2 Cementera



Figura 40

FD9 Empresa 3 Minera



En base a la información recopilada a través de la herramienta, se obtuvieron objetivos prioritarios de gobierno y gestión para cada solución de gobierno, como se muestra en la Tabla 21. Se observa en las 3 organizaciones similitudes en los 6 objetivos prioritarios, principalmente en el objetivo “Gestionar el marco de gestión de

ciberseguridad industrial” y solo en la empresa minera busca “Asegurar el establecimiento y mantenimiento de un marco de gobierno” lo cual demuestra la falta de controles en ciberseguridad a diferencia de la empresa 1 y 2.

Tabla 33

Objetivos priorizados por cada empresa

Empresa 1 - Hidrocarburos		Empresa 2 - Cementera		Empresa 3 -Minera	
Nº	Objetivo	Nº	Objetivo	Nº	Objetivo
1	Gestionar el marco de gestión de ciberseguridad industrial	1	Gestionar los recursos humanos	1	Gestionar el marco de gestión de ciberseguridad industrial
2	Gestionar los recursos humanos	2	Gestionar el marco de gestión de ciberseguridad industrial	2	Asegurar el establecimiento y mantenimiento de un marco de gobierno
3	Gestionar la monitorización del rendimiento y la conformidad	3	Asegurar la optimización de recursos	3	Gestionar los recursos humanos
4	Gestionar el aseguramiento	4	Gestionar la monitorización del rendimiento y la conformidad	4	Gestionar el aseguramiento
5	Asegurar el establecimiento y mantenimiento de un marco de gobierno	5	Asegurar el establecimiento y mantenimiento de un marco de gobierno	5	Gestionar la monitorización del rendimiento y la conformidad
6	Gestionar el sistema de control interno	6	Gestionar las relaciones	6	Gestionar el presupuesto y los costes

Con la lista de objetivos priorizados de cada organización se logró validar la cantidad de controles establecidos, así como los controles que se recomiendan implementar para el logro del nivel objetivo de acuerdo a lo mostrado en las tablas 34, 35 y 36 para el cumplimiento del marco de gobierno de ciberseguridad industrial y su posterior mantenimiento y optimización.

Tabla 34

Definición de controles Empresa 1 Hidrocarburos

Número de controles actuales	Número de controles objetivo	Porcentaje para alcanzar el nivel objetivo
60	83	22.89%

Tabla 35*Definición de controles Empresa 2 Cementera*

Número de controles actuales	Número de controles objetivo	Porcentaje para alcanzar el nivel objetivo
63	94	32.97%

Tabla 36*Definición de controles Empresa 3 Minera*

Número de controles actuales	Número de controles objetivo	Porcentaje para alcanzar el nivel objetivo
56	76	26.31%

Capítulo VII. Conclusiones y Recomendaciones

7.1 Conclusiones

- Mediante la síntesis de los trabajos de investigación explorados se obtuvo un proceso general y una línea base de los estándares y marcos de trabajo que pudieron formar parte de la solución al problema planteado, los cuales fueron analizados en una segunda instancia para seleccionar los más adecuados, a través de la adaptación de estos se crearon los factores de diseño y se proporcionan las listas de controles que son los componentes de la solución de gobierno, de esta manera se brindan los lineamientos base para el gobierno de ciberseguridad en el sector industrial.
- Entre los diversos estándares y marcos disponibles se eligieron los más adecuados en base a aquellos que permitan el desarrollo de gobierno y estén alineados a las necesidades del sector industrial, estos al ser adaptados permiten resolver el problema planteado en el estudio.
- Los lineamientos que proporciona el estándar ISA/IEC 62443-2-1 nos permitió adaptar lo propuesto en COBIT 2019 en base a las necesidades particulares que tiene el sector industrial y crear los factores de diseño de ciberseguridad industrial.
- La herramienta de medición al ser aplicada en 3 empresas del sector industrial permitió en cada una de ellas los objetivos priorizados y controles que deben ser abordados en el gobierno de ciberseguridad industrial. De los resultados obtenidos se aprecian similitudes entre estos que son debido al contexto en el que se encuentran, pero existen puntos particulares en cada una de las soluciones de gobierno.

7.2 Recomendaciones

- Crear una interfaz que permita a la herramienta ser consumida de manera sencilla y ser distribuida de una manera segura y masiva para que los interesados puedan obtener los beneficios de esta, ejemplo: interfaz web responsiva.
- Asociar los controles resultantes con ejemplos de tecnologías utilizadas para cumplir con las listas de controles planteadas.
- Crear un cuestionario de preguntas de perfilamiento de riesgo similar al de FFIEC para obtener el nivel objetivo de ciberseguridad mínimo y máximo con el que se debe contar.
- Se plantea la difusión a través de los canales de la Sociedad Nacional de Industrias (SIN) y/o la Sociedad Nacional de Minería, Petróleo y Energía (SNMPE) para que puedan adoptar el marco obteniendo los beneficios de este y mediante la cooperación retroalimentarlo para la mejora continua.

Referencias

- Brown, M. A., Zhou, S., & Ahmadi, M. (2018). Smart grid governance: An international review of evolving policy issues and innovations. *WIREs Energy and Environment*, 7(5). <https://doi.org/10.1002/wene.290>
- ISA. (2007). *ANSI/ISA-62443-1-1 Security for Industrial Automation and Control Systems Part 1-1 Terminology, Concepts, and Models*. American National Standards Institute.
- ISA. (2009). *ANSI/ISA-62443-2-1 Security for Industrial Automation and Control Systems Part 2-1 Establishing an Industrial Automation and Control Systems Security Program*. International Society of Automation.
- ISA. (2013). *ANSI/ISA-62443-3-3 Security for Industrial Automation and Control Systems Part 3-3 System security requirements and security levels*.
- Lara, C. M., Frieiro, R., Garcia, X., Bravo, A., Pedriza, A., Espósito, N., Santos, J. A., & D'Antonio, G. (2019). *Las preocupaciones del CISO El estado de la ciberseguridad en el 2019*.
- Seguridad industrial 2019 en cifras | INCIBE-CERT*. (n.d.). Retrieved January 3, 2022, from <https://www.incibe-cert.es/blog/seguridad-industrial-2019-cifras>
- Setiawan, A. B., Syamsudin, A., & Sastrosubroto, A. S. (2016). Information security governance on national cyber physical systems. *2016 International Conference on Information Technology Systems and Innovation (ICITSI)*, 1–6. <https://doi.org/10.1109/ICITSI.2016.7858210>
- Zhu, P., & Liyanage, J. P. (2021). Cybersecurity of Offshore Oil and Gas Production Assets Under Trending Asset Digitalization Contexts: A Specific Review of Issues and Challenges in Safety Instrumented Systems. *European Journal for Security Research*. <https://doi.org/10.1007/s41125-021-00076-2>