UNIVERSIDAD NACIONAL DEL SANTA

FACULTAD DE INGENIERIA

Escuela Profesional de Ingeniería de Sistemas e Informática

==========

“Análisis de los controles CIS alineados a los pilares de Zero Trust para medir el nivel de madurez de ciberseguridad en empresas latinas”

==========

Tesis para Optar el Título Profesional de Ingeniero de Sistemas e Informática

Autores:

Bach. Aranda Timaná, Nancy Lorena

Bach. Loncarich Manrique, Yelko Andrej

Asesor:

Dr. Sánchez Chávez, Juan Pablo

Nuevo Chimbote – Perú

2025

UNIVERSIDAD NACIONAL DEL SANTA

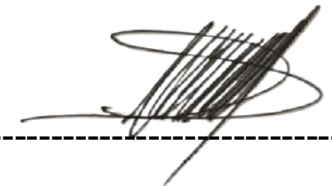
FACULTAD DE INGENIERIA

Escuela Profesional de Ingeniería de Sistemas e Informática

"Análisis de los controles CIS alineados a los pilares de Zero Trust para medir el nivel de madurez de ciberseguridad en empresas latinas"

Tesis para Optar el Título Profesional de Ingeniero de Sistemas e Informática

Revisado y Aprobado por el Asesor:



Dr. Sánchez Chávez, Juan Pablo
DNI: 17808722
Cód: ORCID: 0000-0002-3521-7037
ASESOR

UNIVERSIDAD NACIONAL DEL SANTA

FACULTAD DE INGENIERIA

Escuela Profesional de Ingeniería de Sistemas e Informática

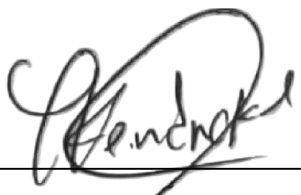
"Análisis de los controles CIS alineados a los pilares de Zero Trust para medir el nivel de madurez de ciberseguridad en empresas latinas"

Tesis para Optar el Título Profesional de Ingeniero de Sistemas e Informática

Revisado y Aprobado por el Jurado Evaluador:

Ms. Mirko Martin Manrique Ronceros
DNI: 32965599
Cód. ORCID: 0000-0002-0364-4237
PRESIDENTE

Dr. Juan Pablo Sánchez Chávez
DNI: 17808722
Cód. ORCID: 0000-0002-3521-7037
SECRETARIO



Ms. Whinston Kendrick Borja Reyna
DNI: 44939310
Cód. ORCID: 0000-0002-5966-3859
INTEGRANTE

ACTA DE SUSTENTACIÓN DE LA TESIS

FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL INGENIERÍA DE SISTEMAS E INFORMÁTICA

ACTA DE SUSTENTACIÓN INFORME FINAL DE TESIS

A los nueve días del mes de octubre del año dos mil veinticinco, siendo las 11:00 am. En el aula S-2 del Pabellón de la Escuela Profesional de Ingeniería Sistema e Informática-FI-UNS, se instaló el Jurado Evaluador designado mediante Resolución 622-2024-UNS-CFI, y de expedito según Resolución Decanal N° 688-2025-UNS-FI integrado por los docentes: Ms. Mirko Martin Manrique Ronceros **(presidente),** Dr. Juan Pablo Sánchez Chávez **(secretario) y el** Ms. Whiston Kendrick Borja Reyna **(Integrante)**, para dar inicio a la sustentación de la Tesis intitulada **"ANALISIS DE LOS CONTROLES CIS ALINEADOS A LOS PILARES DE ZERO TRUST PARA MEDIR EL NIVEL DE MADUREZ DE CIBERSEGURIDAD EN EMPRESAS LATINAS"**, perteneciente a los Bachilleres: ARANDA TIMANA NACY LORENA, con código de matrícula N° 0201714058 y LONCARICH MANRIQUE YELKO ANDREJ con código de matrícula N°0201714021, quienes fueron asesorado por el Dr. Juan Pablo Sánchez Chávez , según T/R. D. N°059-2024-UNS-FI.

El Jurado Evaluador, después de deliberar sobre aspectos relacionados con el trabajo, contenido y sustentación del mismo, y con las sugerencias pertinentes en concordancia con el Reglamento General de Grados y Títulos, vigente, declaran aprobar:

BACHILLER	PROMEDIO VIGESIMAL	PONDERACIÓN
ARANDA TIMANA NACY LORENA	17	BUENO

Siendo las 12pm del mismo día, se dio por terminado el acto de sustentación, firmando la presente acta en señal de conformidad.

Nuevo Chimbote,09 octubre de 2025

Ms. Mirko Martin Manrique Ronceros
PRESIDENTE

Dr. Juan Pablo Sánchez Chávez
SECRETARIO

Ms. Whiston Kendrick Borja Reyna
INTEGRANTE

ACTA DE SUSTENTACIÓN DE LA TESIS

FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL INGENIERÍA DE SISTEMAS E INFORMÁTICA

ACTA DE SUSTENTACIÓN INFORME FINAL DE TESIS

A los nueve días del mes de octubre del año dos mil veinticinco, siendo las 11:00 am. En el aula S-2 del Pabellón de la Escuela Profesional de Ingeniería Sistema e Informática-FI-UNS, se instaló el Jurado Evaluador designado mediante Resolución 622-2024-UNS-CFI, y de expedito según Resolución Decanal N° 688-2025-UNS-FI integrado por los docentes: Ms. Mirko Martin Manrique Ronceros **(presidente),** Dr. Juan Pablo Sánchez Chávez **(secretario) y el** Ms. Whiston Kendrick Borja Reyna **(Integrante)**, para dar inicio a la sustentación de la Tesis intitulada **"ANALISIS DE LOS CONTROLES CIS ALINEADOS A LOS PILARES DE ZERO TRUST PARA MEDIR EL NIVEL DE MADUREZ DE CIBERSEGURIDAD EN EMPRESAS LATINAS"**, perteneciente a los Bachilleres: ARANDA TIMANA NACY LORENA, con código de matrícula N° 0201714058 y LONCARICH MANRIQUE YELKO ANDREJ con código de matrícula N°0201714021, quienes fueron asesorado por el Dr. Juan Pablo Sánchez Chávez , según T/R. D. N°059-2024-UNS-FI.

El Jurado Evaluador, después de deliberar sobre aspectos relacionados con el trabajo, contenido y sustentación del mismo, y con las sugerencias pertinentes en concordancia con el Reglamento General de Grados y Títulos, vigente, declaran aprobar:

BACHILLER	PROMEDIO VIGESIMAL	PONDERACIÓN
LONCARICH MANRIQUE YELKO ANDREJ	17	BUENO

Siendo las 12pm del mismo día, se dio por terminado el acto de sustentación, firmando la presente acta en señal de conformidad.

Nuevo Chimbote,09 octubre de 2025

Ms. Mirko Martin Manrique Ronceros
PRESIDENTE

Dr. Juan Pablo Sánchez Chávez
SECRETARIO

Ms. Whiston Kendrick Borja Reyna
INTEGRANTE

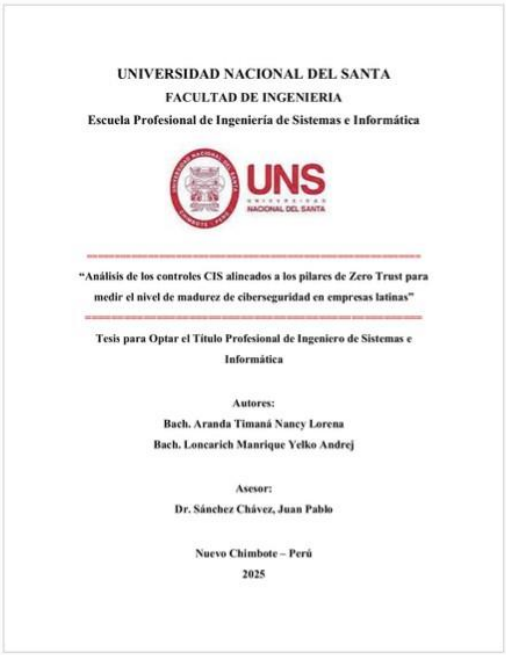
turnitin

Recibo digital

Este recibo confirma quesu trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega:	Nancy Aranda
Título del ejercicio:	TESIS
Título de la entrega:	Análisis de los controles CIS alineados a los pilares de Zero Tru...
Nombre del archivo:	Aranda-Loncarich_-_Tesis.docx
Tamaño del archivo:	5.01M
Total páginas:	123
Total de palabras:	24,219
Total de caracteres:	141,489
Fecha de entrega:	23-sept-2025 10:03a. m. (UTC-0500)
Identificador de la entrega:	2759739144



UNIVERSIDAD NACIONAL DEL SANTA
FACULTAD DE INGENIERIA
Escuela Profesional de Ingeniería de Sistemas e Informática

"Análisis de los controles CIS alineados a los pilares de Zero Trust para medir el nivel de madurez de ciberseguridad en empresas latinas"

Tesis para Optar el Título Profesional de Ingeniero de Sistemas e Informática

Autores:
Bach. Aranda Timaná Nancy Lorena
Bach. Loncarich Manrique Yelko Andrej

Asesor:
Dr. Sánchez Chávez, Juan Pablo

Nuevo Chimbote – Perú
2025

Análisis de los controles CIS alineados a los pilares de Zero Trust para medir el nivel de madurez de ciberseguridad en empresas latinas

INFORME DE ORIGINALIDAD

15%	14%	0%	8%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	2%
2	repositorio.uns.edu.pe Fuente de Internet	1%
3	upc.aws.openrepository.com Fuente de Internet	1%
4	repository.unad.edu.co Fuente de Internet	1%
5	Submitted to Universidad Tecnica De Ambato-Direccion de Investigacion y Desarrollo , DIDE Trabajo del estudiante	1%
6	diplomadociberseguridad.com Fuente de Internet	1%
7	repositorio.usil.edu.pe Fuente de Internet	1%

DEDICATORIA

Dedico este trabajo a mi madre, quien, con su dedicación, amor incondicional y su fortaleza me dio el valor y la motivación para seguir adelante y cumplir mis objetivos.

A mi familia, por enseñarme que el camino hacia el éxito se construye con esfuerzo, dedicación y perseverancia.

A mi compañero de tesis, por ser parte de este camino de crecimiento profesional.

Nancy Lorena Aranda Timaná

DEDICATORIA

Dedico este trabajo a mi familia, que con su apoyo incondicional y enseñanzas han sido la base de mi formación tanto personal como profesional. Gracias por demostrarme que con esfuerzo es posible alcanzar cualquier meta.

A mi camino académico, que me ha desafiado y fortalecido, dándome las herramientas necesarias para crecer y superarme cada día.

Yelko Andrej Loncarich Marique

AGRADECIMIENTO

En primer lugar, agradecemos a nuestras familias, quienes con su apoyo incondicional y confianza en nosotros nos brindaron la motivación necesaria para seguir adelante en nuestro camino profesional y cumplir nuestras metas.

En segundo lugar, expresamos nuestro sincero agradecimiento a los docentes de la especialidad de Ingeniería de Sistemas e Informática, por compartir con nosotros los conocimientos y herramientas necesarias para nuestro desarrollo profesional. En especial, queremos agradecer al ingeniero Sánchez, nuestro asesor, por su valiosa orientación y dedicación, que nos permitió completar este trabajo de manera exitosa.

Atentamente;

Nancy Lorena Aranda Timaná
Yelko Andrej Loncarich Manrique

ÍNDICE

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

La ciberseguridad se ha vuelto crítica en América Latina ante el aumento de amenazas cibernéticas y la limitada adopción de medidas preventivas en muchas organizaciones. Mediante el presente estudio, se evaluó el nivel de madurez en ciberseguridad de más de 150 empresas de 16 países de la región, aplicando un análisis estructurado de los Controles CIS alineados a los pilares del modelo Zero Trust. Bajo un enfoque deductivo, descriptivo y aplicado, se diseñó un cuestionario para clasificar a las organizaciones en cuatro niveles de madurez: básico, tradicional, avanzado y optimizado. Los resultados evidenciaron que la mayoría de las empresas se ubican en el nivel "tradicional", con brechas notorias en pilares como Datos y Dispositivos. En contraste, los pilares de Redes y Aplicaciones mostraron mayor avance. El análisis también reveló que sectores como el financiero e industrial presentan mayores niveles de madurez, mientras que el sector público y empresas de otros rubros reflejan rezagos importantes. Los subcontroles más débiles están relacionados con la gestión del acceso a datos sensibles, accesos privilegiados y la respuesta a incidentes. El estudio se desarrolló con el acompañamiento técnico de la consultora Exypnos, lo que permitió una mejor recolección de datos y validación de resultados en campo. A partir de los hallazgos, se formularon recomendaciones prácticas por subcontrol, combinando estrategias técnicas y de proceso. La metodología empleada no solo aporta un diagnóstico replicable, sino también conocimiento clave para políticas públicas y empresariales que fortalezcan la ciberseguridad en la región.

Palabras Clave: *Ciberseguridad, Zero Trust, Controles CIS, Madurez de seguridad, América Latina.*

ABSTRACT

Cybersecurity has become critical in Latin America due to the rise in cyber threats and the limited adoption of preventive measures by many organizations. This study evaluated the cybersecurity maturity level of over 150 companies across 16 countries in the region, applying a structured analysis based on CIS Controls aligned with the pillars of the Zero Trust model. Using a deductive, descriptive, and applied approach, a questionnaire was designed to classify organizations into four maturity levels: basic, traditional, advanced, and optimized. The results showed that most companies fall into the "traditional" level, with significant gaps in pillars such as Data and Devices. In contrast, the Networks and Applications pillars showed great progress. The analysis also revealed that sectors such as finance and industry exhibit higher levels of maturity, while the public sector and other business areas show a notable lag. The weakest sub-controls were related to the management of access to sensitive data, privileged access, and incident response. The study was carried out with the technical support of the consultancy Exypnos, which contributed to more effective data collection and validation in the field. Based on the findings, practical recommendations were developed for each sub-control, combining technical and procedural strategies. The methodology used not only provides a replicable diagnostic framework but also offers valuable insights for public policy and business strategies aimed at strengthening cybersecurity across the region.

Keywords: *Cybersecurity, Zero Trust, CIS Controls, security maturity, Latin America.*

PRESENTACIÓN

Señores miembros del Jurado Evaluador:

En cumplimiento a lo dispuesto en el Reglamento General de Grados y Títulos de la Universidad Nacional del Santa, ponemos a vuestra consideración el presente Proyecto de Tesis intitulado: **"ANÁLISIS DE LOS CONTROLES CIS ALINEADOS A LOS PILARES DE ZERO TRUST PARA MEDIR EL NIVEL DE MADUREZ DE CIBERSEGURIDAD EN EMPRESAS LATINAS"** que es, requisito previo para optar el Título Profesional de Ingeniero de Sistemas e Informática.

El presente Proyecto de Tesis, es gracias al esfuerzo, dedicación y aplicación de los conocimientos logrados a través de nuestra formación profesional, que refleja el carácter empeñado de nuestra capacidad y la iniciativa por la investigación de cada uno de sus egresados inculcados en esta casa superior de estudios.

Por lo expuesto, a ustedes señores miembros del jurado evaluador, teniendo en cuenta las limitaciones propias de este proyecto, dejamos a vuestro criterio y consideración, su revisión con el deseo de que cumpla con los requisitos mínimos para su correspondiente aprobación.

Atentamente,

Bach. Nancy Lorena Aranda Timaná

Bach. Yelko Andrej Loncarich Manrique

CAPÍTULO I: INTRODUCCIÓN

1.1. TÍTULO DEL PROYECTO

ANÁLISIS DE LOS CONTROLES CIS ALINEADOS A LOS PILARES DE ZERO TRUST PARA MEDIR EL NIVEL DE MADUREZ DE CIBERSEGURIDAD EN EMPRESAS LATINAS.

1.2. PERSONAL INVESTIGADOR

- Bach. Nancy Lorena Aranda Timaná
- Bach. Yelko Andrej Loncarich Manrique

1.3. ASESOR

- Dr. Juan Pablo Sánchez Chávez

1.4. TIPO DE INVESTIGACIÓN

1.4.1. SEGÚN SU NATURALEZA

La presente investigación es de tipo descriptiva y se enfoca en esclarecer el estado de madurez en ciberseguridad de las empresas latinas. Este proceso se lleva a cabo mediante la recopilación de datos directamente de profesionales de TI, tales como arquitectos cloud, líderes de ciberseguridad, jefes de infraestructura, entre otros. El propósito de esta investigación es diagnosticar de manera precisa los desafíos y oportunidades en ciberseguridad que enfrentan estas empresas. Se trabajará con dos variables: la variable dependiente es la madurez de ciberseguridad, y la variable independiente es la alineación de los controles CIS con los pilares de Zero Trust. Utilizando estos dos conceptos, se obtendrá un nivel de madurez de ciberseguridad para cada empresa, y, por extensión, para cada región, sector y tamaño de empresa, entre otras categorías evaluadas. El objetivo final es proporcionar recomendaciones estratégicas para elevar la madurez de ciberseguridad en el sector empresarial de Latinoamérica, contribuyendo así a un entorno digital más seguro y resiliente.

1.4.2. SEGÚN SU FIN O PROPÓSITO

Esta investigación se enfoca en el ámbito aplicado, con el objetivo de explicar el nivel de madurez de ciberseguridad de las empresas latinas, proporcionando una visión clara sobre cómo se gestiona la ciberseguridad en la región. Este estudio busca generar mejoras significativas en los procesos de seguridad de las empresas estudiadas. Para medir el nivel de madurez, se utilizan las teorías y principios de los controles CIS y la metodología de Zero Trust. Mediante una exhaustiva investigación y correlación de estos enfoques, se desarrolla un esquema para medir cuantitativamente la implementación de estos principios y determinar el nivel de madurez de cada empresa. Asimismo, este trabajo aspira a generar conocimiento aplicable a corto y mediano plazo para resolver problemas reales, con el objetivo de contribuir al ámbito académico, empresarial e investigador de la ciberseguridad

1.5. MÉTODO DE INVESTIGACIÓN

Este estudio se enmarca en un método de investigación deductivo, partiendo de teorías y marcos teóricos establecidos sobre los controles CIS y los pilares de Zero Trust para evaluar la madurez de ciberseguridad de las empresas latinas. Utilizando un enfoque deductivo, partimos de generalizaciones previas para aplicar conceptos relacionados a las variables pertinentes. Este proceso nos permitirá formular hipótesis específicas sobre cómo la integración de estos controles y pilares puede ayudar a medir el nivel de madurez en ciberseguridad en las organizaciones de Latinoamérica. Posteriormente, validaremos estas hipótesis mediante la recopilación y análisis de datos obtenidos de profesionales de TI de diversas empresas y sectores en la región. Esto permitirá describir la puntuación obtenida por cada empresa de la región y ofrecer conclusiones basadas en los hallazgos encontrados durante la investigación. Este enfoque asegura que la investigación no solo se apoye en la teoría existente, sino que también contribuya a la práctica, ofreciendo soluciones basadas en evidencias para enfrentar los desafíos de ciberseguridad en el contexto latinoamericano.

1.6. RÉGIMEN DE INVESTIGACIÓN

El régimen de esta investigación es orientado, ya que la iniciativa para realizar el estudio sobre el “Análisis de los controles CIS alineados a los pilares de Zero Trust para medir el

nivel de madurez de ciberseguridad en empresas latinas" proviene de una necesidad específica identificada por la empresa Exypnos. Este enfoque se centra en comprender el estado actual del nivel de madurez de la ciberseguridad dentro del entorno empresarial latinoamericano. Así, la investigación está dirigida a abordar preguntas prácticas y operativas relevantes, proponiendo soluciones basadas en evidencias que respondan a los desafíos de ciberseguridad enfrentados por las organizaciones en América Latina.

1.7. ÁREA DE DESARROLLO DEL PROYECTO

1.7.1. LOCALIDAD

El proyecto se desarrollará en 16 países de América Latina, incluyendo Argentina, Brasil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, México, Panamá, Paraguay, Perú, Puerto Rico, República Dominicana y Uruguay.

Figura 1: Mapa de América Latina.

Fuente: Página Web: maps.com.

1.7.2. DELIMITACIÓN DEL ESTUDIO

Este estudio se enfoca en el análisis de los controles CIS alineados a los pilares de Zero Trust para evaluar el nivel de madurez de ciberseguridad, concentrándose en empresas latinoamericanas que colaboran con la empresa de consultoría, Exypnos. La delimitación se establece en base a la disponibilidad de datos proporcionados por Exypnos, obtenidos de organizaciones latinas interesadas en conocer y optimizar su madurez en ciberseguridad. Esta colaboración facilita un acceso privilegiado a información verídica y relevante, permitiendo un análisis profundo y específico del estado actual de la ciberseguridad en el ámbito empresarial latinoamericano. Así, nuestro estudio se circunscribe a aquellos datos y hallazgos proporcionados por Exypnos, lo que asegura que los hallazgos y recomendaciones sean directamente aplicables y beneficiosos para las empresas participantes y otras en contextos similares dentro de la región.

1.7.3. ACTIVIDAD DE LA EMPRESA

Exypnos es una empresa de consultoría dedicada a la ciberseguridad con presencia en Colombia, Chile y Estados Unidos. Especializados en realizar evaluaciones estratégicas basadas en el modelo de Zero Trust, ofrecen soporte multilingüe en español, inglés y portugués para satisfacer las necesidades globales de sus clientes. Como miembros destacados del Microsoft Solution Assessment Program y Partners Selectos en Cybersecurity Assessment, disponen de Itametrix, una solución innovadora propia. Dada su posición privilegiada y su compromiso con la excelencia en seguridad digital, Exypnos está interesado en determinar el nivel de madurez en ciberseguridad de las empresas latinoamericanas. Este interés se orienta hacia la recomendación y provisión de soluciones estratégicas personalizadas que respondan eficazmente a los retos específicos en materia de ciberseguridad que enfrentan sus clientes.

Figura 2. Logo de Exypnos.

Fuente: Página Web de Exypnos.

1.8. REALIDAD PROBLEMÁTICA

Actualmente, la ciberseguridad es fundamental en las empresas del mundo, ya que estamos en una era digital donde dependemos de tecnologías para realizar nuestra labor cotidiana, lo cual nos mantiene expuestos a sofisticados ciberataques que tienen impactos significativos en el entorno laboral. En ese orden de ideas, es importante resaltar que en el estudio de (Schwartz, y otros, 2023) se menciona que, los tipos de ciberataques más comunes son los de phishing, ransomware y software malicioso o malware.

Del mismo modo, es necesario reconocer como los ciberataques y la cantidad de ciberdelincuentes han incrementado y evolucionado de manera acelerada en la sociedad. Según los datos del Informe de Protección Digital de Microsoft 2023, realizado desde julio del 2022 a junio del 2023, se observa que la cantidad de ataques de ransomware ha incrementado al triple en comparación al año anterior, además mencionan que, desde noviembre del 2022, se han duplicado las posibles instancias de exfiltración de datos (robo, movimiento o eliminación no autorizada de datos desde un dispositivo). De la misma manera, el informe indica que la frecuencia de los ataques de compromiso de email empresarial se ha disparado a más de 156 mil por día.

Por otro lado, en el estudio sobre el Panorama de Amenazas 2023 publicado por Kaspersky, se indica que en América Latina se registraron 1.8 millones de intentos de infección por malware durante el periodo de julio del 2022 a julio del 2023, además de un incremento del 617% en ataques de phishing en el último año con un promedio de 544 ataques por minuto. Adicionalmente, se menciona que otro de los ataques más comunes en este periodo es el de troyanos bancarios, con un registro de 7160 ataques diarios.

Luego de revisar estas alarmantes cifras, surge la siguiente interrogante: Si la tecnología evoluciona día a día, ¿Por qué los ciberataques no se controlan de la misma manera y siguen incrementando exponencialmente en la región de Latinoamérica? Para responder a esta pregunta, es necesario observar el panorama completo de la problemática. Uno de los grandes factores es la inversión y el interés que tienen las empresas para la ciberseguridad.

El informe sobre Perspectivas de Ciberseguridad de los Líderes de la Industria 2023 elaborado por LATAM CISO, indica que el presupuesto dedicado a la ciberseguridad del

31% de las empresas encuestadas es inferior a USD 50 mil, mientras que el 59% restante menciona que tienen un presupuesto inferior a USD 500 mil.

Por otro lado, comparando estas cifras con el estudio realizado por IBM en el 2023 llamado Cost of a Data Breach, se menciona que el costo de una filtración de datos en Latinoamérica equivale a USD 3.69 millones. Por lo tanto, un presupuesto inferior a USD 500 mil, mencionado en el párrafo anterior, representa menos del 15% del equivalente del costo de una filtración de datos. Por eso es necesario que más organizaciones planeen estrategias de inversión para evitar los ciberataques y responder ante ellos rápidamente y evitar impactos significativos en las empresas.

Se debe considerar el involucramiento de los entes gubernamentales y privados con respecto a las estrategias de ciberseguridad aplicadas en la región. Según el informe de Perspectivas de Ciberseguridad de los Líderes de la Industria 2023 elaborado por LATAM CISO, la capacidad de trabajar en conjunto con las agencias gubernamentales luego de un ciberataque es fundamental para prevenir delitos similares, pero esta premisa no va de acuerdo con la realidad, ya que, a pesar de que la mayoría de las organizaciones conocen el procedimiento de comunicarse con dichas agencias, el 32% de las empresas no saben a quién contactar y cómo hacerlo. En ese mismo orden de ideas, el 35% de las organizaciones en Latinoamérica tienen una confianza moderadamente baja en agencias nacionales de aplicación de la ley y su CERT (Equipo de respuesta a emergencias informáticas) nacional.

Cabe mencionar que los gobiernos de algunos países tienen mayor interés en mejorar el nivel de madurez en ciberseguridad, tal es el caso República Dominicana, porque de acuerdo con el ranking mundial de ciberseguridad elaborado por e-Governance Academy 2023, se encuentra en el puesto 29 de 161 países evaluados, obteniendo una puntuación de 71.43% con respecto a las capacidades de seguridad cibernética que son implementadas por los gobiernos centrales y 45.21% de cumplimiento del índice de las TIC y el índice de preparación en red. Asimismo, tenemos a Paraguay, Argentina, Perú y Chile, en los puestos 47, 51, 53 y 56 respectivamente.

Finalmente, como resultado del diagnóstico realizado, se llegaron a considerar los siguientes subproblemas relacionados al nivel de madurez de ciberseguridad dentro de la región de Latinoamérica:

1. Evolución constante de las amenazas cibernéticas y ciberdelincuentes en la sociedad actual.
2. Falta de un modelo estructurado que permita medir cuantitativamente el nivel de madurez en ciberseguridad en empresas latinoamericanas.
3. Falta de análisis sobre patrones o tendencias comunes de madurez en ciberseguridad, lo cual limita la capacidad de diseñar estrategias regionales coherentes.
4. Presupuesto limitado y falta de interés para el área de ciberseguridad dentro de las organizaciones.
5. Falta de compromiso por parte de entidades gubernamentales y privadas para establecer líneas base de estrategias de ciberseguridad dentro de los países de Latinoamérica.

1.9. FORMULACIÓN DEL PROBLEMA

Luego de haber realizado el análisis de la problemática actual de la ciberseguridad de las empresas en Latinoamérica, se logra plasmar la realidad en la siguiente pregunta:

¿De qué manera se debe llevar a cabo el análisis de los controles CIS alineados a los pilares de Zero Trust para lograr medir el nivel de madurez de ciberseguridad en las Empresas Latinas en el año 2023?

1.10. OBJETIVOS

1.10.1. Objetivo General

Aplicar el análisis de los controles CIS alineados a los pilares de Zero Trust para lograr medir el nivel de madurez de ciberseguridad en las Empresas Latinas en el año 2023.

1.10.2. Objetivos Específicos

- Desarrollar una correlación entre 36 controles CIS y 6 pilares de la metodología Zero Trust que permita proporcionar un valor cuantitativo del nivel de madurez de ciberseguridad en las empresas de la región de Latinoamérica.
- Determinar y analizar cuáles son los pilares de la metodología Zero Trust que presentan los niveles más altos y bajos de madurez en las empresas evaluadas, diferenciando los resultados según el sector al que pertenecen.

- Identificar el sector empresarial que presenta los niveles más altos de madurez en ciberseguridad, a través de un análisis comparativo entre industrias para evidenciar cuáles muestran un mayor avance en la implementación de una estrategia de ciberseguridad.
- Analizar las tendencias de madurez en ciberseguridad desde la perspectiva de los pilares del modelo Zero Trust, con el propósito de identificar patrones comunes de fortalezas y debilidades que orienten el diseño de estrategias regionales más efectivas.
- Evaluar el nivel de madurez de ciberseguridad en empresas latinas mediante el análisis de los controles CIS alineados a los pilares de Zero Trust, para proponer recomendaciones y mejoras con el fin de fortalecer la ciberseguridad y contrarrestar los efectos de la evolución constante de las amenazas cibernéticas y ciberdelincuentes.
- Contribuir al campo académico mediante una metodología replicable, que sirva como referencia para investigaciones futuras en ciberseguridad y madurez organizacional en la región.

1.11. HIPÓTESIS

El análisis pertinente de los controles CIS alineados a los pilares de Zero Trust permiten medir el nivel de madurez de ciberseguridad en las Empresas Latinas en el año 2023.

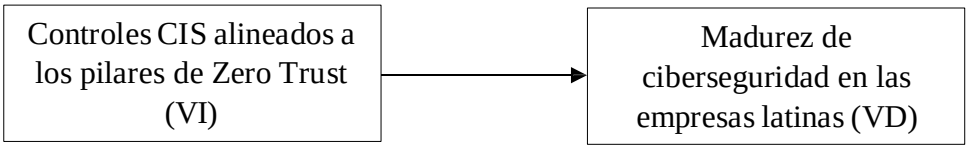
1.12. IDENTIFICACIÓN DE VARIABLES

Variable Independiente (Causa):

Controles CIS alineados a los pilares de Zero Trust.

Variable Dependiente (Efecto):

Madurez de ciberseguridad en las empresas latinas.



1.13. OPERACIONALIZACIÓN DE LAS VARIABLES

1.13.1. Variable Independiente

Controles CIS alineados a los pilares de Zero Trust.

1.13.1.1. Definición Conceptual

Conjunto de buenas prácticas y recomendaciones de seguridad que se integran con el modelo de seguridad Zero Trust. Estos controles buscan implementar y reforzar un enfoque de seguridad que no confía automáticamente en ningún usuario, dispositivo o red, ya sea interna o externa a la organización. Se centran en la verificación continua, la mínima concesión de privilegios y la segmentación de recursos para proteger los activos de la organización.

1.13.1.2. Definición Operacional

Los controles CIS alineados a los pilares de Zero Trust se implementan mediante la configuración y monitoreo de mecanismos específicos, como la autenticación multifactor (MFA), el control de acceso basado en roles (RBAC), la segmentación de la red, y la verificación continua de identidad para usuarios y dispositivos. Estos controles son evaluados y aplicados utilizando herramientas automatizadas de gestión de identidades, firewalls de próxima generación, y sistemas de detección de intrusiones, asegurando

que cada acceso sea autorizado y auditado según los criterios establecidos por la política de Zero Trust de la organización.

1.13.1.3. Dimensiones

- Seguridad de Aplicaciones.
- Protección de Datos.
- Gestión de Dispositivos.
- Control de Acceso y Autenticación.
- Gestión de Infraestructura
- Monitoreo de Redes.

1.13.2. Variable Dependiente

Madurez de ciberseguridad en las empresas latinas.

1.13.2.1. Definición Conceptual

El nivel de madurez en ciberseguridad se entiende como el grado de desarrollo, efectividad y consistencia con el que una organización implementa políticas, procesos y controles orientados a proteger sus activos digitales frente a amenazas cibernéticas. En este estudio, se concibe como una expresión de la efectividad operativa en ciberseguridad, evaluada en términos de la capacidad de aplicar prácticas alineadas al modelo Zero Trust y marcos como los controles CIS v8, en el contexto de empresas latinoamericanas.

1.13.2.2. Definición Operacional

La madurez de ciberseguridad se operacionaliza como un indicador compuesto que refleja la efectividad operativa en la implementación de controles de seguridad. Este nivel se obtiene a partir del promedio de los niveles de implementación reportados en los seis pilares del modelo Zero Trust: Dispositivos, Identidad, Aplicaciones, Redes, Infraestructura y Datos. Cada pilar es evaluado mediante ítems que reflejan prácticas

extraídas de los controles CIS, calificados en una escala ordinal del 1 al 4 (Básico a Optimizado). El valor final es tratado como una variable cuantitativa continua.

1.13.2.3. Dimensiones

- Efectividad operativa en ciberseguridad.

1.13.3. Cuadro de Operacionalización de Variables

Tabla 1. Cuadro de Operacionalización de Variables.

VARIABLE	DIMENSIONES	INDICADOR	TIPO DE VARIABLE
VI: Controles CIS alineados a los pilares de Zero Trust	Seguridad de Aplicaciones	Control de acceso, uso de aplicaciones autorizadas, monitoreo	Cuantitativa ordinal
	Protección de Datos	Clasificación, cifrado, control de acceso, DLP	Cuantitativa ordinal
	Gestión de Dispositivos	Controles aplicados para gestión de dispositivos (MDM, MFA, inventario)	Cuantitativa ordinal
	Control de Acceso y Autenticación	Controles para autenticación, privilegios, IAM, revisión de logs	Cuantitativa ordinal
	Gestión de Infraestructura	Control de servidores, monitoreo, privilegios	Cuantitativa ordinal
	Monitoreo de redes	Segmentación, cifrado, monitoreo de tráfico	Cuantitativa ordinal
VD: Madurez de ciberseguridad en las empresas latinas	Efectividad operativa en ciberseguridad	Promedio de niveles de implementación de controles por pilar Zero Trust	Cuantitativa continua

Fuente: Elaboración Propia

1.14. JUSTIFICACIÓN

La presente investigación se justifica en los siguientes aspectos:

1.14.1. Justificación Operativa

Desde una perspectiva operativa, este estudio aborda directamente el desafío de optimizar los procesos de ciberseguridad en las empresas latinoamericanas. Al evaluar la eficacia de los controles CIS alineados con los principios de Zero Trust, la investigación proporciona una base empírica para que las empresas adopten prácticas y estrategias que mejoren su capacidad de respuestas ante ciber amenazas. Esta optimización de recursos no solo aumenta la eficiencia en la gestión de la seguridad de la información, sino que también establece un marco para la adopción de nuevas tecnologías de protección de manera más efectiva.

1.14.2. Justificación Académica

Desde el punto de vista académico, este proyecto aporta un valioso conocimiento al campo de estudio de la ciberseguridad, llenando un vacío en la investigación sobre la aplicación de controles CIS y Zero Trust en el contexto empresarial latinoamericano. Al combinar análisis empíricos con teorías de seguridad de la información, esta investigación enriquece el diálogo académico en torno a las mejores prácticas de ciberseguridad, ofreciendo una base sólida para futuras investigaciones. Además, al analizar datos reales de empresas, proporciona casos de estudio y ejemplos prácticos que pueden ser utilizados en contextos educativos para ilustrar los desafíos y soluciones en la gestión de la ciberseguridad.

1.14.3. Justificación Tecnológica

La justificación tecnológica de este proyecto radica en su enfoque en evaluar y aplicar metodologías avanzadas de ciberseguridad, como los controles CIS y el modelo de Zero Trust, dentro del contexto específico de las empresas latinoamericanas. Al proporcionar un análisis detallado de cómo estas tecnologías pueden ser implementadas eficazmente, la investigación contribuye al avance del conocimiento técnico en el campo de la ciberseguridad. Este estudio no solo destaca las capacidades y limitaciones de las tecnologías existentes, sino que también

sugiere direcciones futuras para el desarrollo tecnológico, promoviendo así la innovación en la protección contra ciber amenazas.

1.15. IMPORTANCIA DE LA INVESTIGACIÓN

La importancia de esta investigación reside en su capacidad para abordar una de las preocupaciones más críticas en el ámbito de las tecnologías de la información: la seguridad cibernética en el entorno empresarial latinoamericano. En una era donde la digitalización empresarial avanza a pasos agigantados, la vulnerabilidad a las ciber amenazas se ha incrementado exponencialmente, lo que hace imperativo el desarrollo de estrategias de seguridad robustas y eficaces. Al centrarse en la aplicación de los controles CIS y los pilares de Zero Trust, este estudio ofrece un enfoque novedoso y específico para evaluar y mejorar la ciberseguridad, adaptándose a las particularidades y desafíos que enfrentan las empresas en Latinoamérica. Esta investigación no solo proporciona una metodología detallada para la evaluación de la madurez en ciberseguridad, sino que también establece un precedente para la implementación práctica de soluciones basadas en estándares reconocidos a nivel mundial.

Además, el estudio es crucial para fortalecer la resiliencia cibernética de las empresas latinoamericanas, contribuyendo a proteger activos críticos y datos sensibles. La implementación efectiva de los controles CIS alineados con los principios de Zero Trust se presenta como una solución estratégica para enfrentar las amenazas cibernéticas, permitiendo a las organizaciones anticiparse a posibles vulnerabilidades. Al entender las prácticas de seguridad actuales y sus áreas de mejora, la investigación empodera a los líderes empresariales y a los profesionales de TI para tomar decisiones informadas, promoviendo una cultura de seguridad esencial en el entorno digital de hoy.

Finalmente, la relevancia de esta investigación trasciende el ámbito empresarial, impactando positivamente en la sociedad al garantizar la integridad y confidencialidad de la información de los usuarios. En un momento en que la confianza digital se ha convertido en un valor indispensable para las interacciones en línea. Así, este estudio no solo aborda una necesidad inmediata de las empresas latinoamericanas, sino que también sienta las bases para un futuro más seguro y resiliente frente a las ciber amenazas globales.

CAPÍTULO II: MARCO TEÓRICO

2.1. ANTEDEDENTES DEL PROBLEMA

2.1.1. Antecedentes Internacionales

2.1.1.1. Antecedente Internacional 1

Autor **:** Jani Kujo

Tesis **: "**Implementación de la arquitectura de Zero Trust para identidades y puntos finales con herramientas de Microsoft"

Institución **:** Jamk University of Applied Sciences – Jyväskylä – Finlandia

Año 2023

Grado **:** Máster en Tecnología de la Información y Ciberseguridad.

Resumen y Resultados:

Durante los últimos años, ha sido una tendencia para los empleados trabajar desde casa. Esto se debe principalmente a la pandemia del COVID-19, pero también intervienen otros factores. Este cambio desde el trabajo perimetral en oficinas e instalaciones de organizaciones ha traído consigo nuevos problemas en el paisaje cibernético en constante cambio. La exposición de identidades y puntos finales está aumentando, y las organizaciones son más vulnerables.

Esta investigación describe métodos eficientes que ayudan a las organizaciones a protegerse de los ataques cibernéticos contra identidades y

puntos finales con la Arquitectura de Zero Trust y discute las posibilidades de desarrollar una estrategia cibernética general.

Los resultados muestran que, con las políticas adecuadas y la configuración, las organizaciones pueden desviar ciertos tipos de ataques y amenazas, y que la postura de seguridad puede mejorar con cambios relativamente pequeños. En esta investigación, esto se demuestra con casos de uso de amenazas y creando políticas de ejemplo para protegerse.

Los hallazgos de esta investigación son que los mecanismos de protección de identidades y puntos finales son actualmente inadecuados contra vectores de ataque muy grandes, y las organizaciones deberían tener esto en cuenta.

Relación con nuestra investigación:

Este antecedente se relaciona con nuestro estudio, ya que propuso un marco de trabajo práctico y demuestra cómo ajustes estratégicos en la arquitectura de seguridad pueden mejorar significativamente la protección contra ataques, especialmente en identidades y puntos finales. Sus hallazgos subrayan la necesidad de adoptar modelos de seguridad avanzados, como Zero Trust, proporcionando una base relevante para desarrollar estrategias de ciberseguridad más robustas y efectivas.

2.1.1.2. Antecedente Internacional 2

Autor **:** Jorge Luis Gaitan Baquero

Tesis **:** **“**Análisis del modelo de seguridad Zero Trust y las consideraciones generales aplicables a cualquier organización pública en Colombia.”

Institución **:** Universidad Nacional Abierta y a Distancia UNAD de Colombia – Fusagasugá – Colombia

Año 2022

Título **:** Título de Especialista en Seguridad Informática.

Resumen y Resultados:

El presente trabajo pretende hacer una revisión documental sobre el modelo de seguridad de “Zero Trust” y las consideraciones de su posible implementación en las organizaciones públicas colombianas, permitiendo de esta forma brindar una perspectiva general sobre la importancia de contar con el conjunto de medidas óptimas que minimicen el riesgo de un ataque informático y el impacto que pueda tener en la estructura de negocio para una organización.

Por lo tanto, el modelo de seguridad de “Zero Trust”, se define como las estrategias que se encargan de la identificación, verificación y automatización de los lineamientos de seguridad al interior de una organización que serán aplicados en los recursos tecnológicos y fundamentalmente a los usuarios. Para llevar a cabo este propósito, el modelo presenta tres pilares; verificar y asegurar, accesos limitados y el monitoreo constante.

Para la elaboración de este trabajo se establecerán como fases de investigación la construcción del estado del arte acerca de modelos de seguridad, una revisión contextual sobre el enfoque de seguridad de las organizaciones en Colombia, un consolidado documental sobre los componentes y principales características de “Zero Trust” y de esta manera finalizar, con la presentación de las consideraciones requeridas para utilizar un esquema de “Zero Trust” en las organizaciones colombianas, enfocado a la seguridad informática y el cumplimiento normativo.

Relación con nuestra investigación:

Este antecedente es crucial para nuestro estudio al detallar cómo el modelo Zero Trust, mediante estrategias como la identificación y verificación, se adapta a necesidades específicas de organizaciones públicas, reduciendo el riesgo de ciberataques. Resalta la importancia de un enfoque de seguridad personalizado y dinámico, ofreciendo perspectivas clave para fortalecer la ciberseguridad y evaluar la madurez de ciberseguridad en empresas. Su análisis subraya la necesidad de adaptabilidad en las prácticas de seguridad, enriqueciendo así nuestra comprensión y estrategias para mejorar la ciberseguridad en el contexto latinoamericano.

2.1.1.3. Antecedente Internacional 3

Autor **:** Patrik Svensberg

Tesis **: "**Arquitectura de red de Zero Trust definida por software: Evolución desde el modelo Purdue networking."

Institución **:** University of Turku – Turku – Finlandia

Año 2023

Grado **:** Maestría en Ciberseguridad

Resumen y Resultados:

La digitalización ha traído muchos desarrollos tecnológicos que mejoran las operaciones comerciales en muchas industrias. En los últimos años, el impulso hacia soluciones basadas en servicios ha superado a las soluciones gestionadas localmente hacia soluciones gestionadas por proveedores que se administran a través de Internet. Desafortunadamente, la arquitectura y la infraestructura en la que se basa no han evolucionado al mismo ritmo. Esto ha llevado a las organizaciones a socavar la arquitectura y las políticas

diseñadas para ella. Por lo tanto, se necesita una arquitectura moderna con capacidad para soportar estas tecnologías emergentes. El objetivo de esta tesis fue averiguar si el modelo de Purdue funciona como una arquitectura de referencia válida para construir redes según los estándares actuales, y si necesita ser reemplazado, cuáles serían las alternativas.

Para responder a la pregunta de investigación, primero se investigó si el modelo de Purdue puede ser utilizado para la arquitectura de redes modernas. Después de eso, se realizó una revisión bibliográfica para ver cuáles son algunas de las recomendaciones actuales y modernas. La revisión bibliográfica también incluyó investigaciones sobre cuáles son algunas de las amenazas actuales para las plataformas digitales y cómo se diseñan la ciberseguridad.

Se descubrió que la arquitectura de Zero Trust y las soluciones definidas por software mejoran la seguridad y la gestión general de los entornos operativos. La tesis concluye con una arquitectura de referencia lógica para redes como solución sugerida. La solución sugerida es una nueva arquitectura de red que implementa los elementos de Zero Trust y utiliza la definición de redes por software para gestionar la infraestructura subyacente.

Relación con nuestra investigación:

Este antecedente se relaciona con nuestro estudio, ya que subraya cómo las arquitecturas tradicionales, como el modelo de Purdue, pueden no ser suficientes para las demandas de seguridad de las operaciones comerciales digitalizadas y cómo la adopción de una arquitectura Zero Trust definida por software representa una alternativa viable y más segura. Al ofrecer una solución que integra los principios de Zero Trust con tecnologías de red definidas por software, esta tesis aporta un marco de referencia actualizado que puede servir de base para mejorar la madurez de ciberseguridad en

empresas latinoamericanas, enfatizando la importancia de estructuras flexibles y adaptativas en la protección contra amenazas emergentes.

2.1.2. Antecedentes Nacionales

2.1.2.1. Antecedente Nacional 1

Autor **:** Roger Alonso Paredes Gutierrez, Fernando David Perez Valencia

Tesis : "Controles del Centro de Seguridad de Internet para la defensa cibernética que minimizan las vulnerabilidades"

Institución **:** Universidad San Ignacio de Loyola – Lima

Año 2022

Título **:** Título Profesional de Ingeniero Informático y de Sistemas

Resumen y Resultados:

Esta investigación consiste en encontrar brechas de seguridad en el dominio público de cualquier entidad. Dicha información se encuentra públicamente en el alcance a todo usuario que navega en el Internet.

El método de la investigación se resume en que el tipo de investigación es aplicada. Por consecuente, el nivel de investigación es descriptivo con el fin de identificar el estado actual del acceso a la información pública de alguna entidad. A la vez, el enfoque de investigación es cualitativo ya que nos permite analizar y recabar los resultados obtenidos de la encuesta realizada a los exempleados de una entidad aleatoria. Por último, el diseño de la investigación será no experimental debido a que no se realizará manipulación de la información sensible disponible del dominio público de alguna entidad.

Se realizó un análisis en el dominio público de una entidad usando las herramientas de la fase Reconocimiento del Hacking Ético: DNSdumpster, Whois, Google Hacking. Dichas herramientas no realizan intrusión de fuerza bruta al sistema del dominio público. Gracias a ello, se tomó la decisión de aplicar los Controles de Seguridad de Internet (CIS) debido a que proponen una serie de estrategias específicas para cada tipo de vulnerabilidad encontrada en el dominio público de cualquier entidad.

Relación con nuestra investigación:

El antecedente se relaciona con nuestra investigación, ya que comparte el objetivo de fortalecer las defensas de las organizaciones contra posibles amenazas cibernéticas. Asimismo, esta investigación tiene un enfoque práctico, que permite identificar vulnerabilidades específicas en la seguridad de las empresas y ofrecer recomendaciones para mejorarlas. Gracias a este antecedente, se puede lograr una comprensión más completa de como las empresas pueden proteger sus activos cibernéticos y tener una mayor resiliencia ante ciber amenazas.

2.1.2.2. Antecedente Nacional 2

Autor **:** Alan Pierre Salinas Tomapasca

Tesis **:** **“**Modelo de Ciberseguridad para Cajas Municipales en tiempos de Transformación Digital – Un nuevo enfoque”

Institución **:** Universidad Privada del Norte – Trujillo

Año 2020

Grado **:** Maestro en Ingeniería de Sistemas con mención en Gerencia de Sistemas de Información

Resumen y Resultados:

El objetivo del presente estudio fue elaborar la propuesta para un modelo de ciberseguridad con nuevo enfoque para cajas municipales, en tiempo de transformación digital, que incluya características de integridad, confidencialidad y disponibilidad, y que pueda servir para adaptarse a las exigencias actuales de la transformación digital y hacerles frente a los nuevos tipos de amenaza y ataques informáticos que evolucionan constantemente.

Dentro de los resultados, se desarrolló la propuesta, utilizando el modelo de ciberseguridad "Zero Trust", basado en el marco de gestión de ciberseguridad NIST. Así mismo, se diseñó un modelo organizacional basado en un esquema de niveles Estratégicos, Operacionales y Tácticos en forma de pirámide, que permitirá una mejor gestión de ciberseguridad y una comunicación constante entre todos los departamentos de la organización. Se modificó el organigrama

del departamento de seguridad de la información; así como también, se elaboró la estructura de una nueva sección dentro del departamento de Tecnologías de Información llamada "Seguridad informática"; ambas, con sus respectivas macro funciones. Se elaboró el diseño de arquitectura de seguridad que protege y monitorea tanto el perímetro como lo que se encuentra fuera de él (internet). Se diseñó una matriz para el uso de 20 controles de seguridad CIS y acciones para crear una cultura robusta en ciberseguridad en toda la organización.

Como conclusión, se logró identificar los modelos de ciberseguridad: "Defensa en Profundidad", "Modelo Perimetral", Modelo Zero Trust" y "Modelo Thin Security" a través de una matriz de priorización validada por expertos en ciberseguridad. Así mismo, se evaluaron estos modelos a través de una matriz de comparación de características; se determinaron las características que debe utilizar el modelo y fueron validadas a través de una lista de cotejo de usuarios potenciales. En base a lo anterior, se elaboró la

propuesta utilizando el modelo de ciberseguridad Zero Trust basado en el marco NIST, el diseño de una nueva estructura organizacional de seguridad, la creación de una matriz de soporte de controles de seguridad CIS, el diseño de una arquitectura de ciberseguridad y los pasos para la creación de cultura en ciberseguridad en la organización. Finalmente, se validó la pertinencia, relevancia y claridad de la propuesta a través de una evaluación de Juicio de Expertos realizada a los usuarios potenciales.

Relación con nuestra investigación:

El antecedente será importante para nuestro estudio, ya que presenta un modelo de ciberseguridad innovador diseñado para satisfacer las necesidades de la transformación digital actualmente. Este estudio se fundamenta en la arquitectura Zero Trust y en el marco de gestión de ciberseguridad NIST, estableciendo una conexión relevante con nuestra investigación, centrada en analizar los controles CIS en el contexto de Zero Trust. Por otro lado, el estudio propone modificaciones en la estructura organizacional y en el departamento de seguridad de la información, además de la implementación de una cultura robusta en ciberseguridad en toda la organización. Estas propuestas ofrecen un caso de uso concreto de cómo fortalecer la ciberseguridad en un entorno empresarial.

2.1.2.3. Antecedente Nacional 3

Autor **:** Marcos Cesar Davila Fernandez, Jhonathan Muñoz Huaman

Tesis **: "**Diseño de controles de ciberseguridad para reducir los ciberataques en empresas distribuidoras de productos digitales basados en CIS control V8"

Institución **:** Universidad Peruana de Ciencias Aplicadas – Lima

Año 2023

Título **:** Título profesional de Ingeniero de Redes y Comunicaciones

Resumen y Resultados:

Los controles de seguridad CIS desempeñan un papel crítico en la protección de las empresas contra ciberataques. En un mundo cada vez más digitalizado, donde la información y los activos empresariales son vulnerables a amenazas cibernéticas constantes, implementar medidas de seguridad sólidas se ha vuelto esencial. Los controles de seguridad CIS ofrecen un conjunto de directrices que ayudan a las organizaciones a fortalecer su postura de SI.

En primer lugar, brindan un marco sólido para identificar y mitigar las vulnerabilidades en la infraestructura de TI y las aplicaciones. Siguiendo estas pautas, las empresas pueden asegurarse de que sus sistemas estén debidamente parcheados y actualizados, lo que reduce la

superficie de ataque disponible para los ciberdelincuentes.

La importancia de estos controles radica en su enfoque en la prevención de ciberataques. Al adoptar una mentalidad proactiva, las empresas pueden evitar problemas antes de que ocurran en lugar de simplemente reaccionar a incidentes. Además, estos controles permiten una mejor gestión de incidentes, lo que significa que, si ocurre un ciberataque, la empresa estará mejor preparada para responder efectivamente y minimizar el daño.

En resumen, los controles de seguridad CIS son esenciales para proteger a las empresas contra ciberataques. Proporcionan una base sólida para la prevención y mitigación de amenazas, ayudan a establecer políticas de acceso adecuadas y se adaptan a las amenazas en constante evolución. Al seguir estas directrices, las empresas pueden fortalecer su postura de seguridad, proteger sus activos y mantener la confianza de sus clientes y socios comerciales.

Relación con nuestra investigación:

El antecedente nos ayuda a entender la importancia y el papel crítico de los controles de seguridad CIS en la protección de las empresas contra ciberataques. Además, se destaca especialmente en la aplicación de lineamientos de defensa en profundidad como un enfoque estratégico en ciberseguridad, que busca implementar múltiples capas de seguridad en la infraestructura tecnológica. Por lo tanto, esta iniciativa no solo beneficia a las empresas del sector identificados, sino que también contribuye a mejorar su reputación frente a la competencia en el mercado. Entonces, estas acciones están alineadas con los objetivos propuestos en nuestra investigación.

2.2. BASES TEÓRICAS

2.2.1. Fundamentos de los controles CIS

2.2.1.1. Principios

En la versión 8 de su documento, (Center for Internet Security, 2021) nos expone los siguientes principios:

- *Ofensiva informa a la defensa:* Los controles del CIS se seleccionan, descartan y priorizan en función de los datos y del conocimiento específico del comportamiento de los atacantes y de cómo detenerlo.
- *Objetivo:* Ayudar a los defensores a identificar los puntos críticos que hay que abordar para detener los ataques más importantes.
- *Factibilidad:* Cada recomendación individual debe ser específica y práctica de aplicar.
- *Métricas:* Los controles CIS, especialmente para el grupo de implementación, deben ser medibles.
- *Adaptado:* Crear y demostrar una coexistencia pacífica con otros esquemas, marcos y estructuras de gobierno, regulación y gestión de procesos.

2.2.1.2. Estructura

(Center for Internet Security, 2021), nos menciona que la estructura de un control está conformada por los siguientes elementos:

- Resumen.
- ¿Por qué es crítico este Control?
- Procedimientos y Herramientas.
- Salvaguardas.

2.2.1.3. Perfiles

Los perfiles de los Controles CIS, conocidos como Grupos de Implementación (IGs), son esquemas diseñados para ayudar a las organizaciones a priorizar y adaptar la implementación de los controles de ciberseguridad en función de su nivel de riesgo y recursos disponibles. Estos perfiles facilitan un enfoque de implementación personalizado, que permite a cada empresa abordar las medidas de seguridad más críticas y adecuadas para su contexto operativo. Los IGs representan una estructura horizontal a través de los Controles CIS, adaptada a las necesidades de diferentes tipos de empresas.

- *IG1:* Las empresas IG1 son generalmente pequeñas a medianas con limitada experiencia en TI y ciberseguridad, centradas en mantener operaciones continuas.
- *IG2 (Incluye IG1):* Las empresas IG2 cuentan con personal especializado en gestionar y proteger la infraestructura de TI, y operan con múltiples departamentos que varían en riesgo según su función y misión.
- *IG3 (Incluye IG1 y IG2):* Las empresas IG3 cuentan con expertos en seguridad especializados en diversas áreas como gestión de riesgos, pruebas de penetración y seguridad de aplicaciones.

2.2.2. Fundamentos de Zero Trust

2.2.2.1. Origen de Zero Trust

El concepto de Zero Trust fue introducido por primera vez por John Kindervag en el año 2010, durante su rol como Principal Analyst en Forrester Research. Kindervag, que actualmente es Senior VP of Cibersecurity Strategy en ON2IT y anteriormente fue CTO en Palo Alto Networks, desarrolló este modelo en respuesta a las limitaciones de las estrategias tradicionales sobre la seguridad de la red.

Kindervag, durante una entrevista en el año 2023, llamada, "Creator of Zero Trust Gives You a 30 Second Elevator Pitch", explica que el origen de Zero Trust se remota a la experiencia de instalación de firewalls para proteger los dispositivos conectados a las redes. Tradicionalmente, los firewalls operaban bajo un modelo de confianza implícita, donde las interfaces de red internas se consideraban confiables, con un valor de confianza de 100, y las externas no confiables, con un valor de 0. Las DMZ o zonas intermedias, recibían valores de confianza arbitrarios entre 1 y 99, que dictaban las políticas de tráfico.

Este enfoque supuso que el tráfico interno era seguro y no requería reglas adicionales, mientras que el tráfico exterior, considerado poco fiable, necesitaba una regulación minuciosa. Sin embargo, esta suposición resultó peligrosa, ya que los ataques podían originarse desde dentro de la red interna, supuestamente confiable, algo que la política inicial no tenía en cuenta.

John Kindervag desafió esa mentalidad proponiendo que la confianza no debería ser un atributo implícito de ninguna entidad dentro de la red. Según el modelo Zero Trust, todos los elementos, internos o externos, deben ser continuamente autenticados y autorizados, independientemente de su origen. Esto implica que cada paquete de datos debe ser validado, garantizando que realice solo las acciones permitidas.

Kindervag también enfatizó que las personas no "residen" en la red; en cambio, las máquinas y dispositivos que usan interactúan y se autentican en ella. Por lo tanto, Zero Trust no se centra en la confianza de los usuarios, sino en la verificación continua de los dispositivos y paquetes de datos.

La idea detrás de Zero Trust se basa en cuestionar y verificar todos los aspectos del acceso a la red, respondiendo a preguntas fundamentales como quién, qué, cuándo, dónde, por qué y cómo ocurre cada interacción. Esto permite la creación de políticas de seguridad claras y comprensibles, que determinan quién puede acceder a qué recursos, a través de qué aplicaciones, desde qué ubicaciones y en qué condiciones de tiempo y motivo.

Por lo tanto, Zero Trust se configura como un conjunto de reglas granulares diseñadas para minimizar los riesgos, permitiendo solo las interacciones estrictamente necesarias y específicas. Este enfoque granular es muy importante porque los ataques más dañinos suelen ocurrir dentro de reglas de acceso amplias. Al hacer que estas reglas sean lo más pequeñas y específicas posible, se mejora significativamente la seguridad de la red.

2.2.2.2. ¿Qué es Zero Trust?

Según (Kindervag, 2010) Zero Trust es un modelo de seguridad de la información que establece que los profesionales de seguridad deben abandonar la idea de confiar en los paquetes como si fueran personas, en su lugar, se propone que ninguna red, ya sea interna o externa, debe ser considerada intrínsecamente confiable. En el enfoque Zero Trust, todo el tráfico de red no es confiable, por lo tanto, los profesionales de seguridad deben adoptar una postura de verificación continua y protección exhaustiva para todos los recursos. Asimismo, se consideran tres conceptos fundamentales que aseguran que el modelo Zero Trust proteja la infraestructura de TI:

- Hay que asegurar de que todos los recursos sean accedidos de forma segura, independientemente de la ubicación.

- Adoptar una estrategia de privilegio mínimo y aplicar el control de acceso.
- Inspeccionar y registrar todo el tráfico.

Por otro lado, según (CISCO, s.f.), Zero Trust no es un producto, sino un enfoque para una seguridad mejorada, que establece y verifica la confianza para cada solicitud de acceso, sin importar de dónde provenga. Con este método, la confianza no es fija, sino que evoluciona con las empresas, lo que garantiza que solo los usuarios y dispositivos correctos obtengan acceso cuando lo necesiten, y que las amenazas no recorran la red.

Asimismo, (IBM, ¿Qué es Zero Trust?, s.f.) menciona que Zero Trust es una infraestructura basada en la premisa de que la seguridad de redes complejas siempre está en riesgo por amenazas externas e internas. Esto nos permite organizar y desarrollar estrategias para contrarrestar estas amenazas.

Para finalizar, (Microsoft, What is Zero Trust?, 2024) nos explica que Zero Trust es un enfoque creado para diseñar e implementar unos principios, en los que debemos comprobar explícitamente las autenticaciones y autorizaciones de los usuarios según los datos disponibles. Además, debemos considerar el uso de acceso con privilegios mínimos para reducir el nivel de riesgo y aumentar la protección de los datos. Por último, como se menciona en los puntos anteriores, debemos dar por hecho que nuestros sistemas siempre tendrán intrusiones. Para Microsoft este es el núcleo de Zero Trust, en lugar de creer que todo lo que protegemos es seguro, debemos creer que siempre existirá una brecha, por este motivo, Zero Trust, nos enseña a nunca confiar.

2.2.2.3. Principios

Según la documentación de (Microsoft, What is Zero Trust?, 2024), Zero Trust es un enfoque para diseñar y aplicar los siguientes principios de seguridad:

- Verificar explícitamente.
- Utilizar el acceso con menos privilegios.
- Asumir una brecha.

Es importante mencionar que Zero Trust es una estrategia para incrementar la seguridad y la productividad de los equipos de TI y Ciberseguridad dentro de las empresas.

2.2.2.4. Pilares

De acuerdo con lo publicado por (Microsoft, 2024), se implementan los principios de Zero Trust en las infraestructuras de TI mediante la aplicación de controles y tecnologías específicas en seis pilares fundamentales. Dichos pilares, actúan como fuentes de señal, planos de control para la aplicación, y recursos críticos para ser defendidos. Cada pilar que recopila señales y brinda visibilidad para incidentes de seguridad, además de facilitar la automatización y orquestación para responder y mitigar las amenazas de ciberseguridad.

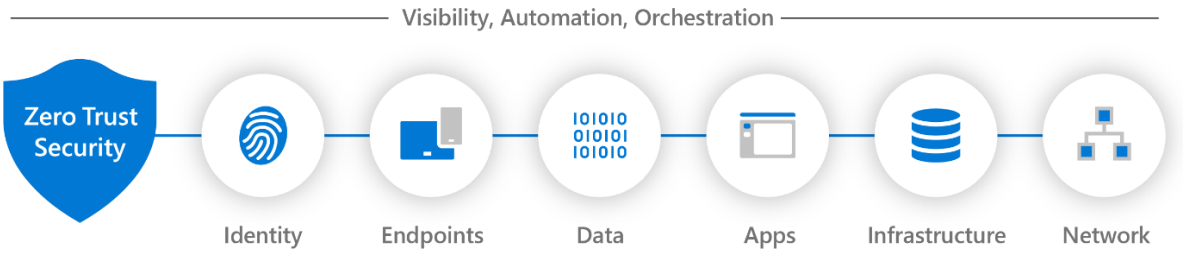


Figura 3. Pilares de Zero Trust.

Fuente: (Microsoft, Zero Trust deployment for technology pillars, 2024)

A continuación, se explicarán cada uno de los seis pilares de Zero Trust:

- *Identidad:* Representa a personas, servicios y dispositivos IoT. Este pilar define el plano de control de Zero Trust. Cada vez que una identidad intenta acceder a un recurso, es necesario verificar dicha

identidad mediante autenticación robusta y asegurar que el acceso solicitado es conforme y típico para esa identidad.

- *Dispositivos:* Representa desde los dispositivos de IoT y smartphones hasta dispositivos BYOD (personales), cargas locales y servidores en la nube. Este pilar es crítico una vez que la identidad ha sido verificada. Es importante monitorear constantemente el estado de los dispositivos y asegurar el cumplimiento de las políticas de seguridad establecidas. Esto garantiza el acceso seguro a los recursos de la red.
- *Datos:* Durante los últimos años, los equipos de seguridad han incrementado sus esfuerzos para proteger los datos. Esto, porque es fundamental que los datos permanezcan seguros cuando salen del ámbito de los dispositivos, aplicaciones, infraestructura y redes controladas por la empresa.
- *Aplicaciones:* Abarca a las cargas de trabajo locales, sistemas heredados, cargas de trabajo en la nube o aplicaciones SaaS modernas. Las aplicaciones y las API son los puntos de acceso a los datos, lo que las convierte en un componente crítico a proteger. Es importante aplicar controles y tecnologías para descubrir y mitigar shadow IT (uso no autorizado de software, hardware, u otros sistemas y servicios dentro de una organización). Asimismo, se deben garantizar los permisos adecuados en las aplicaciones, aplicar controles de acceso en tiempo real basados en análisis, supervisar comportamientos anómalos, controlar las acciones de los usuarios y validar configuraciones seguras.
- *Infraestructura:* Incluye a los servidores locales, máquinas virtuales en la nube, contenedores, microservicios, entre otros. Para lograr asegurar este vector, es importante evaluar continuamente la versión, configuración y acceso Justo a Tiempo (JIT) para robustecer la defensa. Además, se puede utilizar la telemetría para detectar ataques y anomalías en tiempo real.
- *Redes:* Este pilar es fundamental por el cual se accede a todos los datos. Controlar la infraestructura de red proporciona controles críticos para

mejorar la visibilidad y prevenir que los atacantes se muevan lateralmente a través de la red. Es importante segmentar/ microsegmentar las redes para implementar protección contra amenazas en tiempo real, cifrado de extremo a extremo, sistemas de monitoreo y análisis avanzado.

2.2.2.5. Implementación

(IBM, ¿Qué es Zero Trust?, s.f.) indica que, para tener una implementación exitosa de Zero Trust, las empresas deben integrar la información de todos los dominios de seguridad. De la misma manera, el equipo de seguridad de la empresa debe estar de acuerdo sobre las prioridades y coordinar las políticas de acceso.

Con la misma idea, en relación con los pilares de Zero Trust, deben protegerse según una estrategia y hoja de ruta planificadas para implementar e integrar las herramientas de seguridad para lograr resultados que beneficien al negocio y sus objetivos.

Es importante mencionar que un modelo de Zero Trust requiere contexto. De acuerdo con (IBM, ¿Qué es Zero Trust?, s.f.) los principios para obtener un modelo de gobierno que facilite el intercambio de contexto entre las herramientas de seguridad son los siguientes:

- Definir el contexto.
- Verificar e Implementar.
- Resolver incidencias.
- Analizar y mejorar.

Por otro lado, (Olufon & Ber, 2024), analistas en Forrester Research, mencionan que, al planear una implementación exitosa de Zero Trust, los lideres de seguridad deben evitar los siguientes problemas comunes:

- No estar alineados con los objetivos del negocio ni explicar los casos del negocio.
- Operar en silos, con puntos de vista desalineados sobre los objetivos de implementación de Zero Trust.
- Olvidarse de definir y medir los beneficios que puede entender el negocio.

Finalmente, es importante destacar que la implementación de Zero Trust requiere integrar la información de todos los dominios de seguridad y coordinar efectivamente las políticas de acceso. Basado en los principios mencionados, es esencial protegerse con una estrategia bien planificada, definir un contexto claro para usuarios y recursos, verificar y validar activamente las solicitudes de acceso, y mejorar continuamente las políticas de seguridad para adaptarse a nuevas amenazas.

2.2.3. Alineación de los Controles CIS con Zero Trust

2.2.3.1. Fundamentos de alineación

Según (Tenable, 2023) los principios de Zero Trust se alinean directamente con 0los controles CIS, ya que estos últimos son ampliamente utilizados para la higiene cibernética básica. A continuación, detallaremos cada principio por separado para demostrar la fácil adaptabilidad de Zero Trust en las empresas.

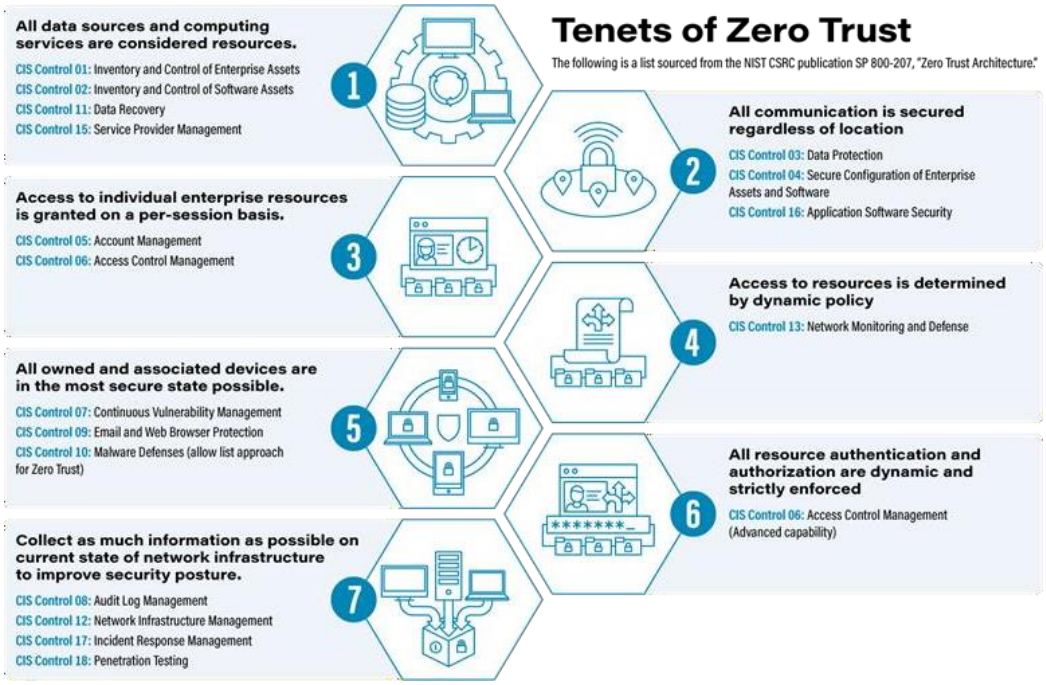


Figura 4. Mapeo de los Controles CIS v8 con los Principios de Zero Trust de NIST SP 800-207.

Fuente: (Moriarty, 2021)

- *Todas las fuentes de datos y los servicios de cómputo se consideran recursos.* Esto implica que todo lo que se encuentra dentro de una empresa es un recurso o activo. Este principio se basa en un dicho común en el mundo de la seguridad "No se puede proteger lo que no se ve". Por tanto, es crucial que las organizaciones creen y mantengan inventarios exhaustivos de sus activos, así se obtiene una visión clara y detallada de los recursos dentro y fuera del entorno de la compañía. Esto permite a los equipos de seguridad cuenten con una hoja de ruta clara para reducir su superficie de ataque y aplicar las acciones necesarias de manera efectiva.
- *Todas las comunicaciones están protegidas independientemente de su ubicación.* Es importante recordar que, según el enfoque de Zero Trust, las empresas deben asumir que siempre están en riesgo y no deben confiar de manera predeterminada. Por esta razón, es fundamental proteger la comunicación digital a través de

configuraciones robustas de hardware y software. Al asegurar las comunicaciones de la empresa, se obtiene como resultado la protección de los datos transferidos mediante mensajes, llamadas, archivos y otros medios. Del mismo modo, es esencial evitar el acceso no autorizado al sistema, ya que cualquier intrusión podría llevar a configuraciones que comprometan la seguridad de la organización.

- *El acceso a los recursos individuales de la empresa se otorga por sesión.* Este principio exige que los usuarios solo deben tener acceso a lo estrictamente necesario para realizar su trabajo y únicamente durante un tiempo predefinido. Es crucial que las empresas adopten este principio para evitar ataques como el ransomware, donde un infiltrado podría permanecer en el entorno durante más tiempo de imaginado. Por este motivo, es importante contar con soluciones que detecten errores de configuración en los sistemas de control de acceso y monitoreen los cambios en tiempo real. Al tener las configuraciones adecuadas, se pueden generar alertas oportunas que otorguen más tiempo a la organización para identificar y eliminar amenazas que podrían persistir durante meses o incluso años.
- *El acceso a los recursos queda determinado por una política dinámica y todas las autenticaciones y autorizaciones de recursos son dinámicas y se aplican de manera estricta.* Estos principios exigen una evaluación constantemente de las políticas y autorizaciones configuradas para acceder a los recursos. Un motor de políticas es un componente muy importante en la arquitectura de Zero Trust, dando soporte para dar acceso a los recursos. Del mismo modo es crucial que el motor central de políticas se mantenga informado para ajustar dinámicamente las políticas y comprender los riesgos asociados a cada usuario y activo. Convertir la priorización de recursos en un motor de políticas dinámico es una estrategia vital para la modernización de la seguridad informática, ya que las amenazas activas evolucionan constantemente en el ámbito tecnológico.

- *Todos los dispositivos propios y asociados están en el estado más seguro posible*. Es indispensable que los dispositivos de una red empresarial estén correctamente configurados y seguros mediante la supervisión y evaluación constante. Asimismo, la implementación y el uso de una solución de gestión de vulnerabilidades ayuda a cerrar proactivamente las brechas que los atacantes podrían explotar. Al realizar escaneos de vulnerabilidades programados de manera periódica, el equipo de seguridad obtiene la información necesaria para reducir el riesgo de amenazas y priorizar las vulnerabilidades a corregir.
- *Recopile toda la información que sea posible sobre el estado actual de la infraestructura de red para mejorar la postura de seguridad*. Este principio se refiere básicamente a tener un conocimiento detallado y actualizado sobre el estado de la infraestructura de la empresa. Comprender la condición de la infraestructura permite informar adecuadamente a las soluciones de seguridad utilizadas por la organización. Asimismo, este control incluye la auditoría de registros, la respuesta ante incidentes y las pruebas de penetración. Esta información es crítica, ya que es importante que cada cambio, ya sea accidental o malintencionado, sea conocido por la empresa. De esta manera, se pueden desarrollar y evaluar eficazmente las estrategias de seguridad implementadas.

Finalmente, (Rose, Borchert, Mitchell, & Connelly, 2020) mencionan que, es importante reconocer que estos principios representan un objetivo ideal, aunque no todos pueden aplicarse plenamente en una estrategia de seguridad. Además, estos principios intentan ser agnósticos respecto a la tecnología, ya que buscan brindar flexibilidad y adaptabilidad en la integración de diversas tecnologías, permitiendo así una mejor respuesta a la evolución de amenazas.

2.2.3.2. Análisis de los controles CIS en el Marco de Zero Trust

Según (Charfoos, y otros, 2024) en su guía para definir la ciberseguridad razonable, se indica cómo un marco, los controles CIS, puede ser implementado de manera prescriptiva. Este enfoque permite a todos aquellos que usan y dependen del ecosistema tecnológico evaluar si se han tomado medidas razonables de ciberseguridad, siguiendo el principio de Zero Trust, "Nunca confíes, siempre verifica".

A continuación, se presentará parte de la implementación de los 18 controles CIS, junto con la descripción de las actividades prescriptivas y priorizadas que las organizaciones deben considerar para defender su empresa:

- ***CIS Control 01: Inventario y Control de los Activos Empresariales:*** Consiste en identificar todos los dispositivos conectados a la red, registrar su información esencial (como direcciones, propietario y estado), y emplear herramientas de descubrimiento para detectar activos no autorizados, asegurando visibilidad total de la infraestructura.
- ***CIS Control 02: Inventario y Control de Activos de Software:*** Implica mantener un inventario completo y actualizado del software instalado, incluyendo su propósito y versión, además de establecer listas de software permitido y herramientas para automatizar la detección de programas no autorizados.
- ***CIS Control 03: Protección de los Datos:*** Requiere clasificar los datos sensibles, definir políticas de acceso, retención y eliminación, así como cifrar la información en tránsito y en reposo. También se recomienda mapear los flujos de datos y controlar el uso de medios extraíbles.
- ***CIS Control 04: Configuración Segura de Activos y Software Empresarial:*** Consiste en aplicar configuraciones estándar seguras desde la instalación de sistemas, eliminando servicios innecesarios, deshabilitando cuentas por defecto y asegurando funcionalidades como el bloqueo por inactividad y el borrado remoto.

- ***CIS Control 05: Administración de Cuentas:*** Implica mantener un registro detallado de todas las cuentas (usuario y servicio), revisar su validez regularmente, eliminar las inactivas y documentar claramente su propósito y responsable.
- ***CIS Control 06: Gestión de Control de Accesos:*** Se enfoca en identificar los accesos a aplicaciones y sistemas, aplicar autenticación multifactor, restringir privilegios innecesarios, y asegurar que solo usuarios autorizados puedan acceder a recursos críticos.
- ***CIS Control 07: Gestión Continua de Vulnerabilidades:*** Requiere implementar herramientas de escaneo para detectar vulnerabilidades, aplicar parches de manera oportuna y mantener actualizado el software. También se deben identificar activos que no estén cubiertos por estas herramientas.
- ***CIS Control 08: Gestión de Registros de Auditoría:*** Consiste en recopilar y almacenar registros de eventos relevantes (logs), sincronizar tiempos, y utilizar herramientas de agregación para mantener un historial útil para auditorías e investigaciones.
- ***CIS Control 09: Protección del Correo Electrónico y Navegador Web:*** Establece controles sobre navegadores y clientes de correo, utilizando filtrado de DNS, restricciones de plugins y políticas de uso seguro para reducir vectores comunes de ataque como el phishing.
- ***CIS Control 10: Defensas contra Malware:*** Incluye la implementación de software antimalware actualizado en todos los dispositivos, su configuración automática y la detección basada en comportamiento para enfrentar amenazas avanzadas.
- ***CIS Control 11: Recuperación de Datos:*** e basa en realizar respaldos automáticos y cifrados, validar su integridad, y almacenar copias en ubicaciones aisladas para garantizar la continuidad operativa ante incidentes.
- ***CIS Control 12: Gestión de la Infraestructura de Red:*** Abarca el control de dispositivos y servicios de red mediante sesiones cifradas,

uso de protocolos autorizados, segmentación de red, autenticación fuerte y monitoreo de accesos remotos.

- ***CIS Control 13: Monitoreo y Defensa de la red:*** Requiere desplegar soluciones de detección y prevención de intrusos, registrar eventos de red, monitorear segmentos críticos y proteger los límites del entorno mediante filtrado y autenticación.
- ***CIS Control 14: Concientización en Seguridad y Formación de Habilidades:*** Implica capacitar al personal sobre buenas prácticas, ingeniería social, manejo de información sensible y respuesta ante incidentes, ajustando los contenidos a los roles específicos.
- ***CIS Control 15: Gestión de Proveedores de Servicios:*** Incluye mantener un inventario de proveedores, definir requisitos de seguridad en contratos, evaluar su cumplimiento y monitorear permanentemente los servicios tercerizados.
- ***CIS Control 16: Seguridad en el Software de Aplicación:*** Promueve el uso de buenas prácticas de codificación, separación de entornos, inventario de componentes externos, plantillas de configuración seguras y pruebas de seguridad como modelado de amenazas y pentesting.
- ***CIS Control 17: Gestión de Respuesta a Incidentes:*** Establece un plan formal de respuesta ante incidentes, define responsables, canales de comunicación, procedimientos post-incidente y ejercicios de simulación para preparar al equipo.
- ***CIS Control 18: Pruebas de Penetración:*** Consiste en realizar evaluaciones periódicas que simulen ataques reales, documentar los hallazgos, corregir vulnerabilidades y validar las mejoras implementadas.

Finalmente, luego de haber explicado parte de la implementación de los 18 controles CIS, se puede concluir que este marco, siendo agnóstico, no solo permite a las organizaciones proteger eficazmente sus activos tecnológicos,

sino también brinda un método robusto para evaluar si se tomaron las medidas adecuadas para la seguridad cibernética.

2.2.3.3. Desafíos y Soluciones

De acuerdo con lo investigado por (Newton, 2022) en una encuesta desarrollada por Fortinet, la implementación de Zero Trust puede ser más fácil de decir que de hacer.

Las organizaciones evaluadas respondieron sobre la dificultad de implementar Zero Trust en sus empresas, donde más el 80 % sentían que la implementación de Zero Trust a través de una red extendida no sería fácil. La mayoría de ellos, el 60 %, reportaron que sería moderadamente difícil, y otro 21 % dijeron que sería extremadamente difícil.

A pesar de esto, la gran mayoría entendían cuál era la importancia de la integración de Zero Trust a su estrategia de protección de los activos. A continuación, se muestra el resultado de cuáles son los desafíos más significantes al construir una estrategia de Zero Trust.

Figura 5. El reto más importante de crear una estrategia de Zero Trust.

Fuente: (Newton, 2022)

Como se puede ver en la imagen, el 24% de los encuestados identificaron como el desafío más significativo la falta de proveedores calificados que ofrezcan una solución completa. Este fue seguido por la falta de presupuesto para implementar cambios en ese momento, con un 19%. Finalmente, se observa que la resistencia organizacional dentro de los equipos de TI representa otro desafío, mencionado por el 7% de los encuestados.

Por otro lado, (Tadmor, 2023) menciona que la aplicación de Zero Trust exige considerables recursos financieros y personal calificado, lo que resulta en dificultades para muchas organizaciones. Según su investigación, los tres desafíos más comunes son los siguientes:

- La complejidad de la red hibrida y problemas de interoperabilidad ya que, al tener sistemas locales heredados, se requiere de ayuda para adaptarse a los protocolos de seguridad, además de recursos adicionales, modificaciones o actualizaciones para garantizar la compatibilidad.
- Los recursos limitados y las limitaciones presupuestarias pueden dificultar la implementación y gestión de los principios de Zero Trust.
- La visibilidad y supervisión de datos, debido a que los recursos se distribuyen en diferentes ubicaciones y entornos de nube, lo que hace que la recopilación y análisis de datos sea un reto.

Asimismo, según (Nordic Defender, 2023), existe un gran desafío relacionado con la implementación de los controles CIS en una empresa debido al creciente número de ciberataques y las nuevas técnicas que los hackers usan para penetrar en los sistemas de TI. Por lo tanto, los dos desafíos comunes al implementar la lista de controles CIS son los siguientes:

- Presupuesto limitado que muchas organizaciones asignan para el área de ciberseguridad, priorizando otras áreas dentro del negocio.

- Falta de expertos profesionales en ciberseguridad para trabajar en la implementación adecuada de los controles CIS.

Luego de comprender cada uno de los desafíos expuestos anteriormente, se presentarán algunas soluciones planteadas por (Terranova Security, 2023) que ofrecen apoyo para establecer una base sólida en la implementación de Zero Trust y los Controles CIS.

- Adoptar una implementación por fases para realizar una adecuada gestión de la complejidad.
- Realizar un presupuesto y análisis del retorno sobre la inversión (ROI) para comparar los beneficios a largo plazo de implementar Zero Trust en la empresa.
- Utilizar herramientas de integración para cerrar la brecha entre los sistemas heredados y el modelo de Zero Trust.
- Capacitar a los empleados con regularidad para comunicar e instruir claramente lo que establece el modelo de Zero Trust y los Controles CIS.

Del mismo modo, (Shea & Turpitka, 2022) mencionan en su investigación que Zero Trust es la postura preferida para las empresas conscientes de la seguridad, por este motivo, para mitigar los riesgos inherentes, es necesario realizar lo siguiente:

- Ejecutar pruebas de Zero Trust antes de implementar la implementación completa. Esto proporciona a los usuarios experiencia utilizando y administrando este tipo de sistemas.
- Iniciar poco a poco y una vez que se tenga éxito, escalar lentamente el despliegue de la implementación.
- Es clave no solo tener el personal adecuado a cargo de los despliegues y la gestión, sino también adaptar la cultura del lugar de trabajo.

2.2.4. Factores que Influyen en la Madurez de Ciberseguridad

(Friel, 2021) menciona que el factor humano representa un riesgo significativo en la ciberseguridad, ya que los ciberdelincuentes lo explotan para obtener accesos no autorizados, robar credenciales e infectar sistemas informáticos y puntos finales con malware. Además, identifica tres vectores principales que involucran a una persona en algún punto de la cadena de ataque: *Phishing, Escaneo y Explotación y el Uso no autorizado de las Credenciales.*

Por otro lado, según lo señalado por (Esteban, y otros, 2024) en el IV Indicador de madurez en ciberseguridad del Observatorio de la Ciberseguridad en España, en donde se contó con la participación de 45 organizaciones que operan en el ámbito nacional. Esta muestra abarca tanto a empresas multinacionales como nacionales y excluye la información recopilada de empresas proveedoras de servicios de ciberseguridad.

De acuerdo con los resultados obtenidos, el 100% de los encuestados mencionaron que las nuevas herramientas de Inteligencia Artificial (IA) y servicios de explotación generan nuevas amenazas de seguridad. Del mismo modo, dos tercios de los encuestados perciben un aumento en los riesgos internos durante una crisis económica. Esto se atribuye a la desesperación financiera, insatisfacción laboral, aumento de la vulnerabilidad interna y una mayor dependencia de proveedores externos.

Del mismo modo, según el informe del Índice de Inteligencia de Amenazas de (IBM, 2024), el aumento del malware diseñado para robar información, conocido como "infostealer malware", ha fortalecido el mercado de credenciales robadas en la dark web, proporcionando a los ciberdelincuentes acceso a los sistemas. Además, el informe señala que la adopción de la IA en las operaciones empresariales presenta un riesgo crítico, ya que muchos trabajadores no están adecuadamente capacitados para entender y aplicar estas nuevas capacidades de manera segura.

Adicionalmente, los errores de configuración de seguridad en aplicaciones web son factores cruciales que afectan el nivel de ciberseguridad. Un problema destacado es

permitir múltiples sesiones de usuario simultáneas en la aplicación, lo que debilita la autenticación multifactor al facilitar el secuestro de sesiones.

Según el Informe de Amenazas Internas de (Cybersecurity Insiders, 2024), se realizó una encuesta en diciembre del 2023 que recopiló las respuestas de 467 profesionales de la ciberseguridad de diversos sectores. El objetivo de esta encuesta es descubrir la naturaleza de los desafíos de amenazas internas que enfrentan las organizaciones, centrándose en comprender los factores que impulsan estas amenazas, las complejidades de su detección y mitigación, y la efectividad de los programas de amenazas internas. El informe busca proporcionar información sobre cómo las organizaciones están adaptando sus estrategias y soluciones para contrarrestar eficazmente estos riesgos de seguridad interna en evolución.

Por lo tanto, algunos de los principales impulsores y facilitadores detrás del aumento de ataques internos son los siguientes:

- Falta de Capacitación y Conciencia (37%).
- Complejidad Global y Tecnológica (34%).
- Medidas de Seguridad Inadecuadas (29%).
- Entorno de TI Complejo (27%).
- Empleados o Contratistas Descontentos (24%).

Finalmente, es muy importante reconocer los factores que influyen en la madurez de la ciberseguridad, ya que permite planificar una guía para aplicar buenas prácticas en las organizaciones, asegurando los activos y manteniendo una ciberseguridad robusta.

2.2.5. Medición de la Madurez de Ciberseguridad

En su última versión del C2M2 (Cybersecurity Capability Maturity Model), el (U.S. Department of Energy, 2022) incluye 356 prácticas de ciberseguridad, agrupadas en diez dominios. Estas prácticas representan las actividades que una empresa puede realizar para establecer y madurar su capacidad en cada dominio.

Dentro de cada dominio, las prácticas se organizan en objetivos que representan logros específicos que apoyan el dominio. Además, dentro de cada objetivo, las prácticas están ordenadas por niveles de indicadores de madurez (MILs).

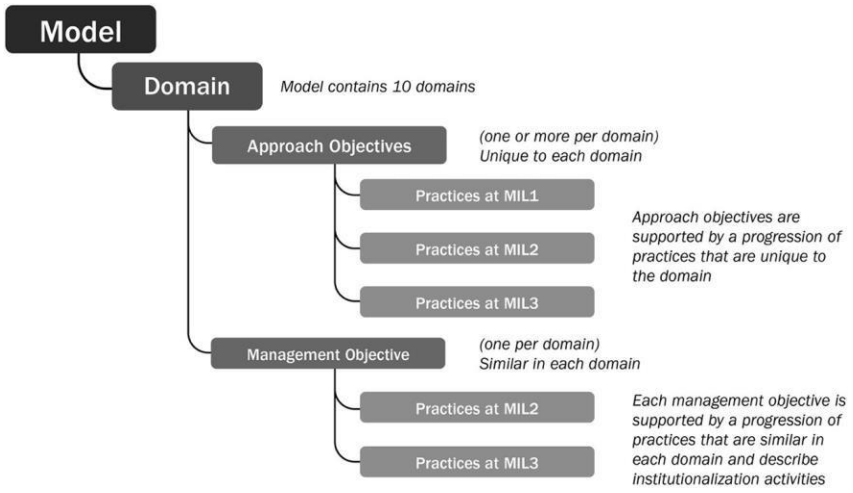


Figura 6.Elementos del Modelo y Dominio de C2M2.

Fuente: (U.S. Department of Energy, 2022)

Existen cuatro aspectos de los niveles de indicadores de madurez (MILs) que son importantes para entender y aplicar el modelo:

- Los MILs se aplican de forma independiente a cada dominio. Por ejemplo, una organización podría estar operando en MIL1 en un dominio, MIL2 en otro dominio y MIL3 en un tercer dominio.
- Los MIL, desde MIL0 hasta MIL3, son acumulativos dentro de cada dominio. Para obtener un MIL en un dominio determinado, una organización debe llevar a cabo todas las prácticas en ese nivel y en el nivel anterior.
- Establecer un MIL objetivo para cada dominio es una estrategia efectiva para utilizar el modelo para guiar la mejora del programa de ciberseguridad.
- El desempeño de la práctica y el logro del MIL deben alinearse con los objetivos comerciales y la estrategia del programa de ciberseguridad de la organización.

En la siguiente tabla se resumen las características de cada MIL:

Tabla 2. Resumen de las características de los Niveles de Indicadores de Madurez (MIL).

NIVEL	CARACTERÍSTICAS
MIL0	Las prácticas no se llevan a cabo.
MIL1	Se realizan prácticas iniciales, pero pueden ser ad hoc.
MIL2	Características de gestión: • Las prácticas están documentadas. • Se proporcionan recursos adecuados para apoyar el proceso Característica del enfoque: • Las prácticas son más completas o avanzadas que en MIL1
MIL3	Características de gestión: • Las actividades están guiadas por políticas u otras directivas organizativas. • Se asignan responsabilidad, rendición de cuentas y autoridad para realizar las prácticas. • El personal que realiza las prácticas tiene habilidades y conocimientos adecuados. • Se evalúa y sigue la eficacia de las actividades Característica del enfoque: • Las prácticas son más completas o avanzadas que en MIL2.

Fuente: Elaboración propia a partir de (U.S. Department of Energy, 2022).

Adicionalmente, los diez dominios evaluados son los siguientes:

- Gestión de activos, cambios y configuraciones.
- Gestión de amenazas y vulnerabilidades.
- Gestión de riesgos.
- Gestión de identidad y acceso.
- Conocimiento de la situación.
- Respuesta ante incidentes y eventos, continuidad de las operaciones.
- Gestión de riesgos de terceros.
- Gestión de la fuerza laboral.
- Arquitectura de Ciberseguridad.
- Gestión de Programas de Ciberseguridad. ciberseguridad de la organización.

Por otro lado, el (National Institute of Standards and Technology , 2024) describe a los Perfiles Organizacionales de CSF (Framework de Ciberseguridad del NIST) como la postura actual y/u objetivo de ciberseguridad de una organización en términos de los resultados del Núcleo. Los Perfiles Organizacionales se utilizan para comprender, adaptar, evaluar, priorizar y comunicar los resultados del Núcleo, considerando los objetivos de la misión de la organización, las expectativas de los interesados, el panorama de amenazas y los requisitos. Cada Perfil Organizacional incluye uno o ambos de los siguientes:

- *Perfil Actual:* Especifica los resultados del Núcleo que una organización está logrando actualmente (o intenta lograr) y caracteriza cómo o en qué medida se está logrando cada resultado.
- *Perfil Objetivo:* Especifica los resultados deseados que una organización ha seleccionado y priorizado para lograr sus objetivos de gestión del riesgo cibernético.

De esta manera, una organización puede optar por usar niveles para definir sus perfiles actuales y objetivos. Estos niveles caracterizan el rigor de las prácticas de gestión y gobernanza de riesgos de ciberseguridad de la empresa, y proporcionan un contexto sobre cómo se perciben los riesgos de ciberseguridad y los procesos establecidos para gestionarlos. Los cuatro niveles se detallan en la tabla a continuación:

Tabla 3. Ilustración teórica de los niveles del CSF.

NIVEL	CIBERSEGURIDAD GOBERNANZA DE RIESGOS	CIBERSEGURIDAD GESTIÓN DE RIESGOS
Nivel 1: Parcial	La aplicación de la estrategia de riesgo de ciberseguridad institucional se gestiona de manera ad hoc.	Existe un conocimiento limitado de los riesgos de ciberseguridad a nivel organizacional.
Nivel2: Informado sobre los Riesgos	Las prácticas de gestión de riesgos son aprobadas por la dirección,	El proyecto de tesis es una investigación descriptiva y aplicada, y su método es

	pero no pueden establecerse como política de toda la organización.	Inductivo–Deductivo, pretende proponer la aplicación de las TIC en una institución educativa, lo que permitirá mejorar la gestión educativa de la institución en estudio.
Nivel 3: Repetible	Las prácticas de gestión de riesgos de la organización se aprueban oficialmente y se expresan como políticas.	Existe un enfoque a nivel de toda la organización para gestionar los riesgos de ciberseguridad.
Nivel 4: Adaptable	Existe un enfoque a nivel de toda la organización para gestionar los riesgos de ciberseguridad que utiliza políticas, procesos y procedimientos basados en riesgos para abordar posibles eventos de ciberseguridad.	La organización adapta sus prácticas de ciberseguridad en función de las actividades de ciberseguridad anteriores y actuales, incluidas las lecciones aprendidas y los indicadores predictivos.

Fuente: Elaboración propia a partir de (National Institute of Standards and Technology , 2024).

Cabe mencionar que seleccionar niveles ayuda a establecer el enfoque general de cómo una entidad gestionará sus riesgos de ciberseguridad. Los niveles se pueden utilizar como referencia interna para un enfoque integral de gestión de riesgos de ciberseguridad en toda la organización. También, se recomienda avanzar a niveles superiores cuando los riesgos o mandatos sean mayores, o cuando un análisis de costo-beneficio indique que es factible y rentable reducir los riesgos negativos de ciberseguridad.

Finalmente, (L&Co Staff Auditors, 2023) indican que existen diferentes modelos de madurez de seguridad y capacidades que se pueden utilizar para evaluar y analizar el progreso de una empresa, pero hay cinco niveles comunes que aparecen en algún aspecto de cada modelo de madurez de ciberseguridad. A continuación, se presentan los niveles típicos utilizados para definir la madurez de las capacidades de una empresa:

- *Nivel 1 (No estructurado y desorganizado):* Se está iniciando con los procesos de seguridad de la información y definiendo cómo se ven esos procesos.
- *Nivel 2 (Repetible):* Los procesos de seguridad están documentados para que las acciones y respuestas puedan ser repetidas por diferentes miembros de un equipo específico.
- *Nivel 3 (Estandarizado):* Los procesos y procedimientos están estandarizados en toda la organización. Se proporciona orientación sobre procedimientos y políticas de seguridad a nivel organizacional y el liderazgo comunica la cultura de respuestas proactivas a la seguridad.
- *Nivel 4 (Gestionado y Monitoreado):* Los controles de seguridad son monitoreados y pueden ser medidos por la organización. Se implementan herramientas analíticas para informar estadísticas cuantitativas relacionadas con controles y eventos de seguridad.
- *Nivel 5 (Optimizado):* Los procesos de seguridad de la información son continuamente analizados y mejorados.

2.3. BASES CONCEPTUALES

2.3.1. Importancia de la Ciberseguridad en LATAM

(Hanwa Vision, 2023) indica que la ciberseguridad es un pilar fundamental en la era actual, ya que está relacionada con el desarrollo y la estabilidad de las naciones. Adicionalmente, indica que, aunque Latinoamérica está adoptando rápidamente las tecnologías digitales, la región también enfrenta diversos ciberataques constantemente.

Para enfrentar estos desafíos, los gobiernos, las empresas y la sociedad en general deben invertir en medidas de ciberseguridad. Según estudios, aproximadamente el 70% de las empresas en Latinoamérica planean aumentar sus inversiones en ciberseguridad en los próximos dos años.

Por otro lado, (Contreras, y otros, 2024), en su informe "Preparación Cibernética en los Sectores Públicos de América Latina: Lecciones de la Primera Línea", realizado en colaboración con la Alianza Digi Americas, la Red LATAM CISO y

la Universidad de Duke, indican que la región está avanzando en el desarrollo de medidas de ciberseguridad. Para comprender el panorama de ciberseguridad en la región, se encuestó a 150 CISOs (Chief Information Security Officer) y otros profesionales de alto nivel, lo que proporcionó una visión general sobre la gestión de riesgos de ciberseguridad (RMF) y el uso de infraestructura de ciberseguridad basada en la nube pública para mitigar el riesgo, entre otros temas.

Según el 72% de los encuestados, habían implementado un RMF en su estrategia de ciberseguridad. De estos, el 40% afirmó que fue muy eficaz, mientras que el 30% mencionó que tuvo una eficacia limitada. Estos hallazgos demuestran la adopción generalizada de RMF en los países latinoamericanos para mitigar riesgos y posibles ataques.

Del mismo modo, (Robledo Hoecker, 2023) señala que la evolución de la ciberseguridad en América Latina y el Caribe ha avanzado mientras estos países se integran en la economía global, en un contexto de grandes avances tecnológicos y mayor desigualdad producida por la globalización. La mayoría de los países en la región están desarrollando iniciativas de ciberseguridad, y algunos ya están implementando medidas concretas en los últimos cuatro años.

Por ejemplo, en América Central, el Sistema de Integración Centroamericana (Sica) adoptó la Estrategia Regional Digital para el desarrollo de la sociedad de la información y el conocimiento. Por otro lado, el Mercosur (Mercado Común del Sur) lanzó en 2017 el Grupo Agenda Digital, que en 2018 aprobó su primer plan de acción, incluyendo compromisos sobre infraestructura digital, conectividad, seguridad y confianza en el entorno digital, habilidades digitales, además de aspectos técnicos y regulatorios.

Por lo tanto, se puede concluir que la ciberseguridad en Latinoamérica está en constante evolución, buscando responder adecuadamente a la creciente adopción de tecnologías digitales al aumento de los ciberataques. Asimismo, la inversión en medidas de ciberseguridad por parte de gobiernos y empresas es esencial para proteger la estabilidad y el desarrollo de la región. Los informes y estudios indican que, aunque existen avances significativos, aún se tienen desafíos por superar, como

la necesidad de una mayor estandarización y eficacia en la implementación de marcos de gestión de riesgos de ciberseguridad (RMF).

Del mismo modo, la colaboración entre los países de la región y la adopción de mejores prácticas globales serán esenciales para enfrentar las amenazas cibernéticas y asegurar un entorno digital seguro y confiable para todos los ciudadanos.

2.3.2. Desafíos de Ciberseguridad Específicos de LATAM

De acuerdo con lo mencionado por (Unidad Latina, 2024), la ciberseguridad en América Latina ha cobrado relevancia en los últimos años debido al aumento de la conectividad y el uso de dispositivos inteligentes en la región. Esto ha incrementado las amenazas cibernéticas que ponen en riesgo la privacidad, la seguridad y la estabilidad económica de las empresas. Algunos de los desafíos y vulnerabilidades identificados incluyen:

- Infraestructura obsoleta en muchos países de la región.
- Falta de conciencia y capacitación sobre la importancia de la ciberseguridad dentro de las empresas.
- Recursos limitados, tanto humanos como financieros.
- Marcos legales inadecuados en materia de ciberseguridad.

Asimismo, (Ruiz, s.f.) señala que, con la creciente dependencia de la tecnología, surgen nuevos desafíos que exigen que las empresas ajusten sus estrategias de ciberseguridad para poder enfrentarlos. Entre estos desafíos se encuentran:

- Expansión de la superficie de ataque cibernético.
- El teletrabajo.
- Ataques cibernéticos a infraestructuras criticas dentro de las organizaciones.
- Falta de desarrollo de capacidades locales en ciberseguridad.

Del mismo modo, (EY, 2023) en su investigación que recopila las perspectivas de más de 500 líderes de ciberseguridad de diferentes industrias en América Latina, encontró que el 62 % de las empresas evaluadas sufrieron alguna filtración de datos.

Además, el 91 % de estas compañías han experimentado incidentes de ciberseguridad, lo que subraya los desafíos que enfrenta la región en este ámbito.

A continuación, se presenta una gráfica con los hallazgos obtenidos de esta encuesta.

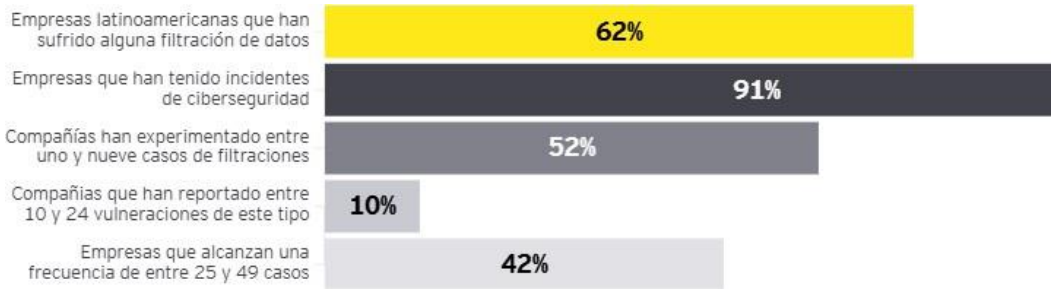


Figura 7. Cantidad de empresas que sufrieron incidentes de ciberseguridad en el 2023.

Fuente: (EY, 2023)

Además, se indica que las tecnologías que presentan mayores riesgos tanto para las empresas en Latinoamérica como a nivel global son: la nube a escala, IoT, inteligencia artificial y machine learning, computación cuántica y el metaverso. Por lo tanto, es crucial que las compañías de la región fortalezcan sus estrategias de ciberseguridad con un enfoque holístico, priorizando la automatización y simplificación de los sistemas.

Adicionalmente, la (Organización de los Estados Americanos, 2023) señala que los eventos de ciberseguridad afectan severamente a las compañías, generando una serie de implicaciones colaterales que provocan incertidumbre y confrontación entre los colaboradores de una empresa. Algunos ejemplos de incidentes de ciberseguridad comunes en Latinoamérica incluyen:

- Extorsión con datos.
- Falta de comprensión de los controles de seguridad para los servicios técnicos.
- Baja higiene informática.
- Confianza ingenua en los medios y tecnologías disponibles.
- Aumento de productos y servicios digitales.

Finalmente, los aspectos actuales de la criminalidad digital se caracterizan por:

- El máximo anonimato con la mínima evidencia.
- La máxima ambigüedad jurídica con el mínimo conocimiento tecnológico disponible.
- La máxima efectividad de sus acciones con el mínimo esfuerzo.

En resumen, tras enumerar los distintos incidentes de ciberseguridad comunes en América Latina, se puede concluir que los agresores tienen un escenario ideal para movilizarse y llevar a cabo sus acciones y planes con poco margen de detección si no se tienen estrategias adecuadas de ciberseguridad.

2.3.3. Tendencias y Futuro de la Ciberseguridad en LATAM

(Contreras, 2024) en su artículo, menciona recomendaciones importantes para que los países Latinoamericanos logren fortalecer sus medidas de ciberseguridad. A continuación, se describen dichas recomendaciones:

- Inversión en capital humano.
- Establecimiento de un marco voluntario de gestión de riesgos.
- Inversión estratégica en infraestructura y tecnologías de ciberseguridad.
- Sistemas centralizados de gestión y notificación de la ciberseguridad.

Del mismo modo, los investigadores (Ramírez Cuenca, Gutiérrez Amaya, & González Cuautle, 2024), en un informe de We Live Security, una editorial de noticias, opiniones y análisis de seguridad en Internet de ESET, señalan que la implementación de la inteligencia artificial (IA) será una tendencia clave en las futuras estrategias de ciberseguridad en América Latina. Entre los usos de la IA para mitigar riesgos y mejorar la eficiencia en la respuesta a incidentes se destacan los siguientes:

- Respuesta rápida a consultas de seguridad.
- Generación automática de informes.

- Procesamiento de grandes volúmenes de datos.
- Capacitación de equipos de seguridad.
- Detección y análisis de vulnerabilidades.

Adicionalmente, (Gartner, 2024) identifica nueve tendencias principales en ciberseguridad para 2024, distribuidas en dos grupos: optimización para la resiliencia y optimización para el rendimiento.

- ***Tendencias de la optimización para la resiliencia:***
  - Gestión continua de la exposición a amenazas (CTEM).
  - Ampliación del valor de la Gestión de Identidad y Acceso (IAM).
  - Gestión de riesgos de ciberseguridad de terceros.
  - Desacoplamiento de aplicaciones y de datos impulsado por la privacidad

- ***Tendencias de la optimización para el renacimiento:***
  - IA generativa.
  - Programas de comportamiento y cultura de la ciberseguridad.
  - Métricas de ciberseguridad basadas en resultados.
  - Evolución de los modelos operativos de ciberseguridad.
  - Mejora de las competencias en ciberseguridad.

En conclusión, las tendencias y el futuro de la ciberseguridad en Lationamérica se enfocan en la inversión en capital humano, la modernización de infraestructuras tecnológicas y la adopción de tecnologías avanzadas como la IA para mitigar riesgos y mejorar la respuesta a incidentes. Estas medidas fortalecen la resiliencia ante las ciberamenazas, optimizan el rendimiento de las estrategias de ciberseguridad, permitiendo así una respuesta más rápida y efectiva a un entorno de amenazas en constante cambio. La colaboración regional y la adopción de mejores prácticas globales jugarán un papel fundamental en la garantía de un entorno digital seguro y confiable en América Latina.

CAPÍTULO III: DESARROLLO DE LA INVESTIGACIÓN

3.1. PROCEDIMIENTO PARA LA RECOLECCIÓN DE DATOS

Para el proceso de recolección de datos, se obtuvo la información de diversas asesorías realizadas en el año fiscal 2023, comprendido entre julio de 2022 y junio de 2023, por la empresa consultora de ciberseguridad Exypnos.

Es importante destacar que las empresas que recibieron estas asesorías lo hicieron por iniciativa propia, buscando mejorar su nivel de ciberseguridad. Estas organizaciones deseaban conocer su situación actual y recibir recomendaciones para que sus equipos de TI, ciberseguridad, redes, o cualquier otro responsable de la seguridad informática, puedan reforzar sus estrategias contra posibles vulnerabilidades.

En primer lugar, se llevó a cabo una reunión inicial con las partes interesadas de la empresa para explicarles el propósito de la asesoría sobre análisis de postura de seguridad. Se presentó el enfoque de Exypnos y los elementos clave involucrados en la asesoría. Asimismo, se detallaron los entregables finales, que incluían un informe con visualizaciones significativas en Power BI y una presentación ejecutiva en PowerPoint para la toma de decisiones.

Durante esta reunión, se discutieron aspectos básicos para comprender el contexto del cliente, tales como el sector de la empresa, su tamaño y algunas tecnologías en uso. Posteriormente, se explicó la metodología, dividida en cuatro etapas: planeación, evaluación, análisis y acción, con una duración aproximada de tres semanas. Una vez explicada la metodología, se especificaron los informes necesarios para un análisis adecuado, los participantes involucrados y las reuniones posteriores para la obtención de la información requerida.

La información utilizada para esta investigación se recopiló durante una sesión denominada “Taller de Evaluación de Madurez de Zero Trust”. Esta sesión tenía una duración de entre

una hora y media a dos horas e incluía la explicación del modelo de seguridad Zero Trust y la evaluación de la madurez de ciberseguridad a través de una encuesta con 36 preguntas. Estas preguntas se basaron en 36 subcontroles CIS seleccionados y divididos en seis partes, correspondientes a los seis pilares de Zero Trust.

En resumen, el proceso de recolección de datos para esta investigación se basó en asesorías realizadas a empresas latinas interesadas en mejorar su nivel de ciberseguridad. A través de una metodología ágil estructurada, se llevaron a cabo reuniones iniciales y talleres específicos para recopilar datos valiosos. Este enfoque sistemático y detallado garantiza que la información obtenida sea relevante y verídica, proporcionando una base sólida para evaluar la madurez de ciberseguridad en las empresas de la región y ofrecer recomendaciones estrategias basadas en evidencia.

3.2. CORRELACIÓN DE SUBCONTROLES CIS Y PILARES DE ZERO TRUST

El procedimiento realizado para correlacionar de los 36 subcontroles CIS con los seis pilares de la metodología Zero Trust se divide en los siguientes pasos:

- *Paso1: Identificar los Pilares:*

  Como se explicó previamente en el Capítulo III: Marco Teórico, Zero Trust se compone de seis pilares fundamentales: Aplicaciones, Datos, Dispositivos, Identidad, Infraestructura y Redes.

- *Paso 2: Identificar los Subcontroles por Pilar:*

  Del mismo modo, como se detalló previamente en el Capítulo III: Marco Teórico, la versión 8 de los controles CIS comprende 18 controles principales y 153 salvaguardas o subcontroles. Luego de un análisis exhaustivo, se seleccionaron 36 subcontroles relevantes, cada uno alineado con los pilares de Zero Trust.

  A continuación, se presentará una tabla que muestra los 36 controles CIS relacionados con sus respectivos pilares de Zero Trust.

Tabla 4. Correlación de Subcontroles CIS y Pilares de Zero Trust.

PILAR	SUBCONTROLES CIS ASOCIADOS
Aplicaciones	***Subctrl CIS 2.3 –*** *Atender periódicamente el software no autorizado detectado.*
	Subctrl CIS 6.8 – *Definir y mantener un control de acceso basado en roles a los recursos empresariales.*
	Subctrl CIS 13.10 – *Realizar filtrado de contenido en la capa de aplicación.*
	Subctrl CIS 2.5 – *Limite el uso de software y/o acceso a servicios autorizados.*
Datos	***Subctrl CIS 3.1 –*** *Establecer y mantener un proceso de gobierno de datos.*
	Subctrl CIS 3.10 – *Encriptar información sensible en tránsito.*
	Subctrl CIS 3.11 – *Encriptar información sensible en reposo.*
	Subctrl CIS 3.13 – *Implementar una solución DLP (Data Loss Prevention).*
	Subctrl CIS 3.14 – *Registrar y controlar acceso a datos sensibles (incluyendo cambios y eliminaciones).*
	Subctrl CIS 3.7 – *Establecer y mantener un esquema de clasificación de datos.*
Dispositivos	***Subctrl CIS 1.1 –*** *Mantener un inventario de activos detallado y actualizado.*
	Subctrl CIS 4.1 – *Establecer y mantener un proceso de configuraciones seguras.*
	Subctrl CIS 16.7 – *Usar plantillas de seguridad (Hardening) para configuraciones estándares.*
	Subctrl CIS 1.2 – *Identificar y remover activos no autorizados.*
	Subctrl CIS 4.11 – *Forzar reseteo remoto (Wipe) para dispositivos portátiles de usuarios finales.*
	Subctrl CIS 4.12 – *Separar ambiente empresarial en dispositivos móviles.*
	Subctrl CIS 13.5 – *Gestione y controle acceso por condiciones para activos conectados remotamente.*
	Subctrl CIS 10.5 – *Usar tecnologías anti-explotación basadas en análisis de datos y comportamiento (p.e. EDR).*
Identidad	***Subctrl CIS 6.7 –*** *Centralizar el control de acceso a todos los activos tecnológicos.*
	Subctrl CIS 5.6 – *Gestión de cuentas centralizada mediante servicio de identidad o directorio.*
	Subctrl CIS 6.4 – *Requerir autenticación multi-factor para todo acceso remoto.*

	Subctrl CIS 6.5 – *Requerir autenticación multi-factor para accesos administrativos (privilegiados).*
	Subctrl CIS 4.7 – *Gestione o desactive las cuentas por defecto en los sistemas empresariales.*
	Subctrl CIS 8.11 – *Revisar periódicamente logs de auditoría para detectar eventos sospechosos.*
Infraestructura	***Subctrl CIS 5.4 –*** *Restringir privilegios administrativos exclusivamente para cuentas dedicadas administrativas.*
	Subctrl CIS 12.5 – *Centralizar autenticación, autorización y auditoría (AAA) en la red.*
	Subctrl CIS 12.2 – *Establecer y mantener una arquitectura de red segura.*
	Subctrl CIS 16.10 – *Aplicar principios de diseño seguro en arquitectura de aplicaciones.*
	Subctrl CIS 17.7 – *Realizar ejercicios periódicos de respuesta ante incidentes.*
	Subctrl CIS 4.6 – *Gestionar activos y cargas empresariales con configuraciones seguras.*
	Subctrl CIS 10.7 – *Usar soluciones basadas en analítica del comportamiento.*
	Subctrl CIS 13.1 – *Centralizar la alerta de eventos de seguridad (p.e. SIEM o Log Analytics).*
Redes	***Subctrl CIS 13.4 –*** *Realizar filtrado de tráfico entre segmentos de red.*
	Subctrl CIS 12.3 – *Gestionar la seguridad de la infraestructura de red.*
	Subctrl CIS 9.3 – *Mantener y forzar filtrado de URL a nivel de red.*
	Subctrl CIS 9.7 – *Implementar y mantener protección antimalware a nivel de correo.*

Fuente: Elaboración propia a partir de información brindada por Exypnos.

Esta correlación se convierte posteriormente en una encuesta que se revisa durante la sesión "Taller de Evaluación de Madurez de Zero Trust", con el fin de recolectar datos cuantitativos y lograr determinar un valor numérico que refleje el nivel de madurez de ciberseguridad de cada empresa evaluada.

- *Paso 3: Valoración por Puntación Obtenida:*

  Es importante mencionar que el alcance de esta evaluación se fundamenta en las tecnologías, procesos y documentación empleados por la empresa asesorada. A continuación, se presenta una tabla que describe cada uno de estos elementos:

Tabla 5. Criterios Base para la Evaluación.

TECNOLOGÍAS	• Supervisión y Operaciones Unificadas
	• SIEM (Administración de Eventos e Información de Seguridad) & SOAR (Orquestación, Automatización y Respuesta de Seguridad)
	• Seguridad de la Red & Firewall de Aplicación Web
	• MDM (Gestión de Dispositivos Móviles) & MAM (Gestión de Aplicaciones Móviles)
	• UEM (Gestión Unificada de Puntos Finales)
	• IAM (Gestión de Identidades y Accesos)
	• EPP (Plataforma de Protección de Puntos Finales) & EDR (Detección y Respuesta de Puntos Finales)
	• Protección de Cargas & XDR (Detección y Respuesta Ampliadas)
	• Seguridad de Datos & CASB (Agente de Seguridad de Acceso a la Nube)
PROCESOS	• Gestión de Aplicaciones
	• Respuesta ante Incidentes
	• Gestión de Datos
DOCUMENTACIÓN	• Línea Base de Seguridad

Fuente: Elaboración propia a partir de información brindada por Exypnos.

Asimismo, cada una de las entidades enumeradas en la tabla anterior se relaciona con los 36 subcontroles CIS seleccionados. A continuación, se presenta una tabla que muestra la relación de cada uno de ellos.

Tabla 6. Correlación de Subcontroles Evaluados y Entidades.

PILAR	SUBCONTROLES CIS	ENTIDAD
Aplicaciones	Subctrl CIS 2.3	Línea Base de Seguridad
	Subctrl CIS 6.8	IAM (Gestión de Identidades y Accesos)
	Subctrl CIS 13.10	Seguridad de la Red & Firewall de Aplicación Web
	Subctrl CIS 2.5	Seguridad de Datos & CASB (Agente de Seguridad de Acceso a la Nube)
Datos	Subctrl CIS 3.1	Gestión de Datos
	Subctrl CIS 3.10	Seguridad de Datos & CASB (Agente de Seguridad de Acceso a la Nube)

	Subctrl CIS 3.11	Seguridad de Datos & CASB (Agente de Seguridad de Acceso a la Nube)
	Subctrl CIS 3.13	Seguridad de Datos & CASB (Agente de Seguridad de Acceso a la Nube)
	Subctrl CIS 3.14	Seguridad de Datos & CASB (Agente de Seguridad de Acceso a la Nube)
	Subctrl CIS 3.7	Gestión de Datos
Dispositivos	Subctrl CIS 1.1	UEM (Gestión Unificada de Puntos Finales)
	Subctrl CIS 4.1	UEM (Gestión Unificada de Puntos Finales)
	Subctrl CIS 16.7	Línea Base de Seguridad
	Subctrl CIS 1.2	Respuesta ante Incidentes
	Subctrl CIS 4.11	MDM (Gestión de Dispositivos Móviles) & MAM (Gestión de Aplicaciones Móviles)
	Subctrl CIS 4.12	MDM (Gestión de Dispositivos Móviles) & MAM (Gestión de Aplicaciones Móviles)
	Subctrl CIS 13.5	IAM (Gestión de Identidades y Accesos)
	Subctrl CIS 10.5	EPP (Plataforma de Protección de Puntos Finales) & EDR (Detección y Respuesta de Puntos Finales)
Identidad	Subctrl CIS 6.7	IAM (Gestión de Identidades y Accesos)
	Subctrl CIS 5.6	IAM (Gestión de Identidades y Accesos)
	Subctrl CIS 6.4	IAM (Gestión de Identidades y Accesos)
	Subctrl CIS 6.5	IAM (Gestión de Identidades y Accesos)
	Subctrl CIS 4.7	Línea Base de Seguridad
	Subctrl CIS 8.11	Respuesta ante Incidentes
Infraestructura	Subctrl CIS 5.4	IAM (Gestión de Identidades y Accesos)
	Subctrl CIS 12.5	Supervisión y Operaciones Unificadas
	Subctrl CIS 12.2	Supervisión y Operaciones Unificadas
	Subctrl CIS 16.10	Protección de Cargas & XDR (Detección y Respuesta Ampliadas)
	Subctrl CIS 17.7	Respuesta ante Incidentes
	Subctrl CIS 4.6	Supervisión y Operaciones Unificadas

	Subctrl CIS 10.7	Protección de Cargas & XDR (Detección y Respuesta Ampliadas)
	Subctrl CIS 13.1	SIEM (Administración de Eventos e Información de Seguridad) & SOAR (Orquestación, Automatización y Respuesta de Seguridad)
Redes	Subctrl CIS 13.4	Seguridad de la Red & Firewall de Aplicación Web
	Subctrl CIS 12.3	Supervisión y Operaciones Unificadas
	Subctrl CIS 9.3	Seguridad de la Red & Firewall de Aplicación Web
	Subctrl CIS 9.7	Protección de Cargas & XDR (Detección y Respuesta Ampliadas)

Fuente: Elaboración propia a partir de información brindada por Exypnos.

Finalmente, el esquema utilizado para asignar la puntuación a cada una de las preguntas de la encuesta es el siguiente:

Tabla 7. Criterios de Puntuación.

#	NIVEL	DOCUMENTACIÓN	PROCESOS	TECNOLOGÍA
1	**Básico**	No hay documentación	No hay proceso formal	No hay solución
2	**Tradicional**	Documentación parcial	Actividades dependen de personas	Tecnología parcial
3	**Avanzado**	Documentación formal (excepciones documentadas)	Procesos formales (excepciones aceptadas)	Tecnología aprovechada
4	**Optimizado**	Programa de Ciberseguridad con gestión centralizada	Procesos estándares con respuesta automática	Tecnologías modernas con analítica e IA

Fuente: Elaboración propia a partir de información brindada por Exypnos.

3.2.1. Procesamiento de Datos

Para desarrollar el modelo de datos en Power BI, se llevó a cabo un proceso ETL (Extract, Transform & Load) utilizando datos de asesorías realizadas entre julio de 2022 y junio de 2023. La información se recopiló desde archivos de Excel y reportes previos en Power BI, que contenían datos detallados de cada asesoría por empresa.

Como primer paso, se realizó la extracción de datos recopilando y consolidando la información disponible en Excel y Power BI. Estos datos incluían detalles específicos de cada asesoría, organizados por empresa.

Por otro lado, durante la fase de transformación, los datos se ordenaron y limpiaron en un nuevo archivo de Excel, creando las siguientes entidades para estructurar el modelo de datos: Cliente, Sector, Región, Tamaño, Pilares, Controles, Subcontroles y Madurez. Se optó por un modelo de estrella debido a su equilibrio entre eficiencia en el rendimiento y flexibilidad en el análisis, lo que facilita un entorno de reporte robusto y accesible.

En el mismo orden de ideas, la tabla de hechos principal, denominada "Maturity" o Madurez, contiene los niveles de madurez de ciberseguridad obtenidos en cada asesoría. Las demás entidades se estructuraron como dimensiones, proporcionando contexto y detalle adicional para el análisis.

Finalmente, para la carga de los datos al modelo de Power BI no se requirió una limpieza adicional con Power Query, ya que esta etapa se completó previamente en Excel. Los datos limpios se cargaron directamente en Power BI, donde se implementaron funciones DAX (Data Analysis Expressions) para crear los gráficos y visualizaciones necesarios. Adicionalmente, se creó una tabla de calendario para habilitar el análisis temporal detallado, mejorar la eficiencia y garantizar la consistencia en el manejo de fechas.

Por lo tanto, el resultado final fue un modelo de datos que permite analizar el nivel de madurez de ciberseguridad en las empresas latinoamericanas. Este modelo facilita el análisis detallado y la elaboración de informes alineados con los objetivos del estudio, proporcionando una visión clara de los controles CIS alineados a los

pilares de Zero Trust. A continuación, se describen detalladamente las tablas utilizadas y su contribución al análisis:

- ***Tabla de Hechos:***

Tabla 8. Tabla de Hechos "MATURITY".

MATURITY
• ID_MATURITY: Identificador único de la madurez. (PK) • ID_CLIENT: Identificador único del cliente. (FK) • ID_SUBCTRL: Identificador único del subcontrol. (FK) • DATE: Fecha de la medición de madurez. (FK) • PUNCTUATION: Puntuación de Madurez obtenida.

Fuente: Elaboración propia.

- ***Tablas de Dimensiones:***

Tabla 9. Tabla Dimensión "CLIENT".

CLIENT
• ID_CLIENT: Identificador único del cliente. (PK) • ID_REGION: Identificador único de la región. (FK) • ID_SECTOR: Identificador único del sector. (FK) • ID_SIZESTAND: Identificador único del tamaño de la empresa. (FK) • NAME: Nombre del cliente. • SIZE: Tamaño de la empresa.

Fuente: Elaboración propia.

Tabla 10. Tabla Dimensión "SECTOR".

SECTOR
• ID_SECTOR: Identificador único del sector. (PK) • SECTOR: Nombre del sector.

Fuente: Elaboración propia.

Tabla 11. Tabla Dimensión "REGION".

REGION
• ID_REGION: Identificador único de la región. (PK) • REGION: Identificador único de la región.

Fuente: Elaboración propia.

Tabla 12. Tabla Dimensión "SIZE".

SIZE
• ID_SIZESTAND: Identificador único del tamaño de la empresa. (PK) • SIZE: Descripción del tamaño de la empresa.

Fuente: Elaboración propia.

Tabla 13. Tabla Dimensión "PILARS".

PILARS
• ID_PILAR: Identificador único del pilar. (PK) • PILARS: Nombre del pilar.

Fuente: Elaboración propia.

Tabla 14. Tabla Dimensión "CONTROLS".

CONTROLS
• ID_CTRL: Identificador único del control. (PK) • DESC_CTRL: Descripción del control.

Fuente: Elaboración propia.

Tabla 15. Tabla Dimensión "SUBCONTROL".

SUBCONTROL
• ID_SUBCTRL: Identificador único del subcontrol. (PK) • ID_CTRL: Identificador único del cliente. (FK) • ID_PILAR: Identificador único del pilar. (FK) • DESC_SUBCTRL: Descripción del subcontrol. • NUM_SUBCTRL: Número del subcontrol.

Fuente: Elaboración propia.

Tabla 16. Tabla Dimensión "CALENDAR".

CALENDAR
• #Month: Número del mes. • #Quarter: Número del trimestre. • Month: Nombre del mes. • MonthYear: Nombre del mes y año. • Quarter: Nombre del trimestre. • Year: Número del año. • ShortMonth: Nombre corto del mes. • YearQuarter: Nombre del año y trimestre. • YearShortMonth: Nombre del año y mes corto.

Fuente: Elaboración propia.

Del mismo modo, se describen las relaciones entre las tablas del modelo de datos, las cuales están definidas como relaciones de uno a muchos.

- **CLIENT -> REGION:**

  CLIENT[ID_REGION] -> REGION[ID_REGION]

- **CLIENT -> SECTOR:**

  CLIENT[ID_SECTOR] -> SECTOR[ID_SECTOR]

- **CLIENT -> SIZE:**
  CLIENT[ID_SIZESTAND] -> SIZE[ID_SIZESTAND]

- **MATURITY -> CLIENT:**
  MATURITY2[ID_CLIENT] -> CLIENT[ID_CLIENT]

- **MATURITY -> SUBCONTROL:**
  MATURITY[ID_SUBCTRL] -> SUBCONTROL[ID_SUBCTRL]

- **SUBCONTROL -> CONTROLS:**
  SUBCONTROL[ID_CTRL] -> CONTROLS[ID_CTRL]

- **SUBCONTROL -> PILARS:**
  SUBCONTROL[ID_PILAR] -> PILARS[ID_PILAR]

- **MATURITY -> CALENDAR:**
  MATURITY2[DATE] -> CALENDAR[DATE]

Finalmente, el modelo entidad-relación se estructuró considerando las diversas entidades y sus interacciones. A continuación, se detalla el modelo final, que refleja cómo se relacionan las distintas tablas entre sí, incluyendo las claves primarias y foráneas, así como las cardinalidades de las relaciones. El modelo resultante ofrece una representación clara y coherente de los datos, lo que facilita su análisis y comprensión. El esquema entidad-relación se ilustra en la siguiente página:

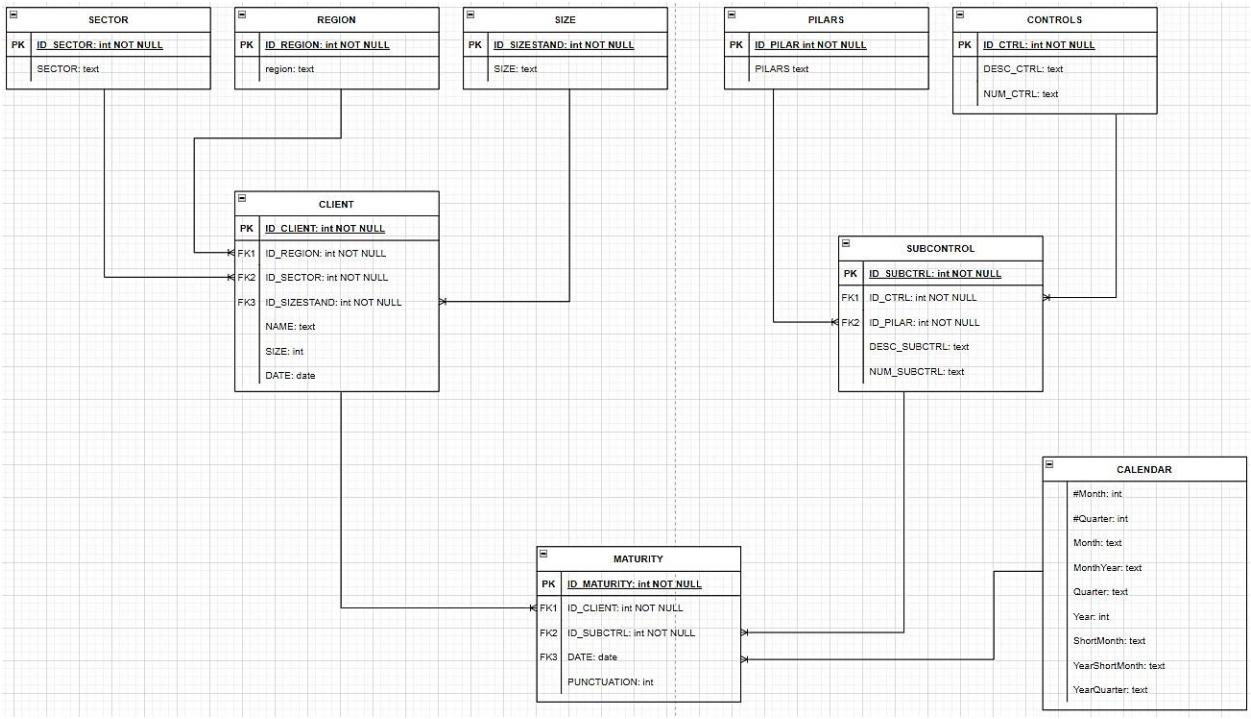


Figura 8. Modelo Entidad-Relación.

Fuente: Elaboración Propia.

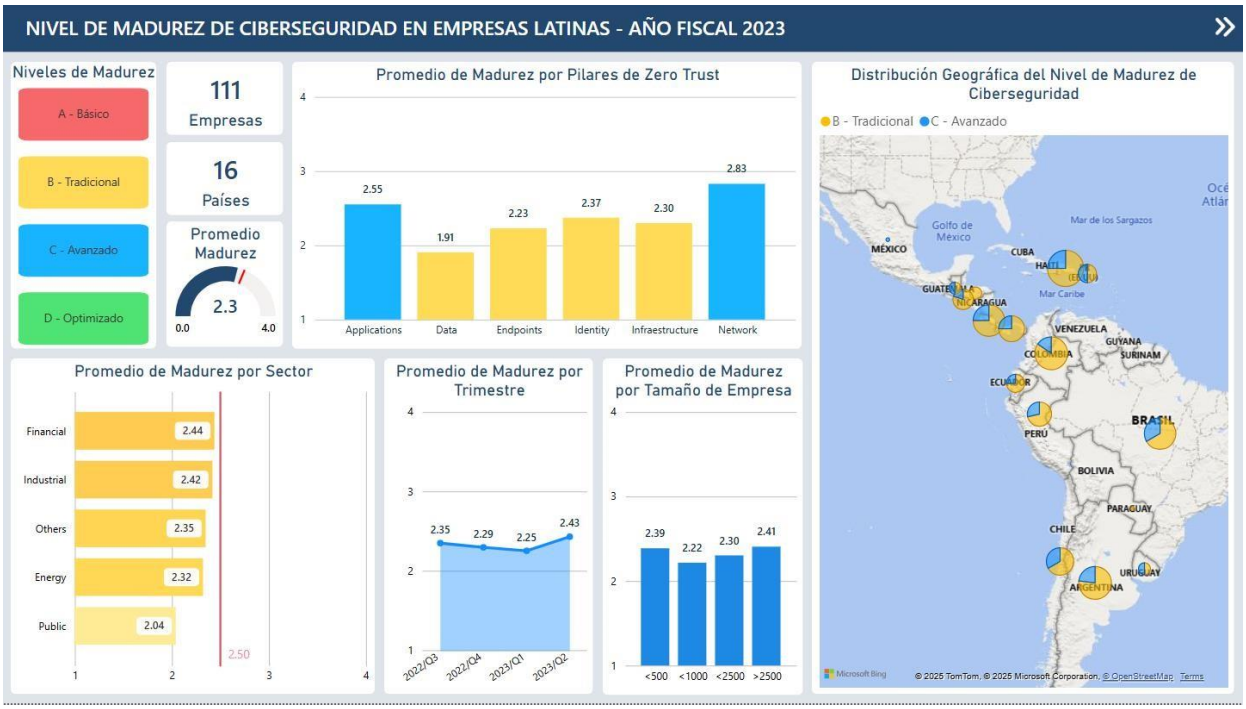


Figura 9. Dashboard en Power BI sobre datos Generales de la Investigación.

Fuente: Elaboración Propia.

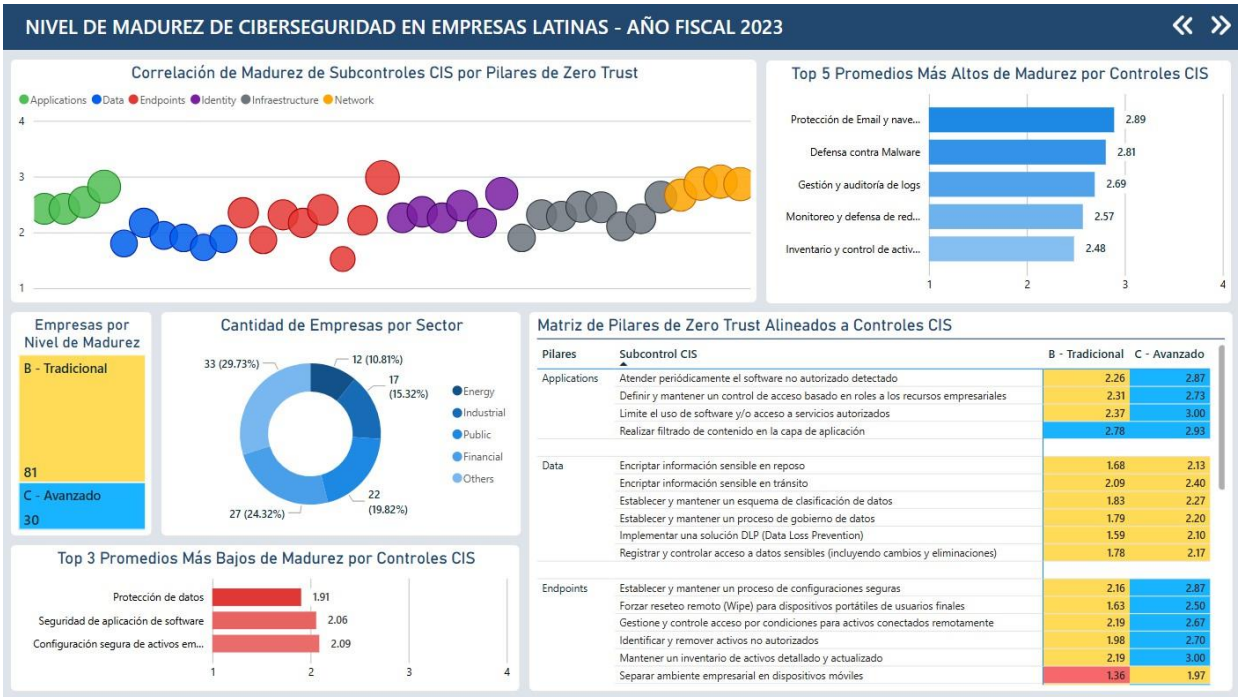


Figura 10. Dashboard en Power BI sobre los Subcontroles Usados para la Investigación

Fuente: Elaboración Propia.

3.2.2. Estrategias dirigidas a optimizar los pilares con menor desempeño en el enfoque Zero Trust

A continuación, se presentan las estrategias propuestas para el fortalecimiento de los pilares del modelo Zero Trust que evidenciaron menores niveles de madurez, con el propósito de orientar acciones de mejora en la ciberseguridad organizacional.

- **Subcontrol 2.3 – Atender periódicamente el software no autorizado detectado**
  - ***Pilar:*** Aplicaciones – AP1
  - ***Recomendación técnica:*** Implementar soluciones de monitoreo automatizado que detecten y eliminen software no autorizado en los endpoints, como Microsoft Defender, Tanium o CrowdStrike. Estas herramientas deben integrarse con scripts automatizados para remediar sin intervención manual constante, reduciendo así el tiempo de exposición a posibles amenazas.

- ***Recomendación de proceso:*** Establecer auditorías mensuales obligatorias de software instalado. Las excepciones deben estar documentadas y aprobadas por el área de seguridad. Además, se recomienda difundir una política clara sobre el uso aceptado de software en la organización, para concientizar a los empleados y fomentar la cultura de cumplimiento.
- ***Soluciones o estrategias del mercado:*** IBM BigFix, ManageEngine Endpoint Central, SentinelOne. Estas plataformas ofrecen inventario de software en tiempo real, remoción remota y alertas automáticas. Integrar este control con una estrategia de Zero Trust fortalece la visibilidad y reduce la superficie de ataque.

- **Subcontrol 3.14 – Registrar y controlar acceso a datos sensibles (incluyendo cambios y eliminaciones)**
  - ***Pilar:*** Datos – DA6
  - ***Recomendación técnica:*** Utilizar soluciones SIEM (como Splunk o Microsoft Sentinel) y sistemas IAM que registren detalladamente quién accede, modifica o elimina datos sensibles. Se deben activar alertas ante accesos inusuales o intentos de alteración no autorizada.
  - ***Recomendación de proceso:*** Definir procedimientos regulares de revisión de logs por parte de personal designado. Realizar auditorías de privilegios y accesos sensibles, asegurando que los usuarios solo tengan acceso a lo estrictamente necesario (principio de mínimo privilegio).
  - ***Soluciones o estrategias del mercado:*** Splunk, IBM QRadar, Google Chronicle. Todas permiten correlación de eventos, generación de reportes e integración con plataformas de detección de amenazas. Su aplicación ayuda a mantener la integridad de la información más crítica de la empresa.

- **Subcontrol 1.2 – Identificar y remover activos no autorizados**
  - ***Pilar:*** Dispositivos – DI4
  - ***Recomendación técnica:*** Implementar tecnologías de descubrimiento continuo de activos, como EDR (CrowdStrike), NDR (Darktrace) o

escaneos automáticos de red que alerten ante dispositivos no reconocidos conectados a la red corporativa.

- ***Recomendación de proceso:*** Establecer revisiones semanales del inventario de activos. Crear protocolos claros para poner en cuarentena, bloquear o eliminar cualquier dispositivo no autorizado detectado. Este proceso debe estar integrado con políticas de onboarding de dispositivos y validación de identidad.
- ***Soluciones o estrategias del mercado:*** Cisco ISE, Microsoft Defender for Endpoint, Rapid7 InsightVM. Estas soluciones proporcionan visibilidad completa de dispositivos en red, categorizan activos y aplican controles de acceso. Es un paso clave para reducir riesgos derivados del shadow IT.

- **Subcontrol 5.6 – Gestión de cuentas centralizada mediante servicio de identidad o directorio**
  - ***Pilar:*** Identidad – ID2
  - ***Recomendación técnica:*** Utilizar plataformas de identidad como Azure Active Directory, Okta o JumpCloud para centralizar la administración de cuentas. Esto permite tener un control único sobre el ciclo de vida de las credenciales y reduce la posibilidad de cuentas huérfanas o no gestionadas.
  - ***Recomendación de proceso:*** Establecer políticas claras para el alta, modificación y baja de cuentas, bajo el modelo de control de acceso basado en roles (RBAC). Estas políticas deben estar documentadas y automatizadas siempre que sea posible.
  - ***Soluciones o estrategias del mercado:*** OneLogin, ForgeRock, soluciones IAM empresariales. Además de centralizar el control, estas herramientas ofrecen funciones de autenticación multifactor, control de sesiones y alertas ante accesos sospechosos, alineándose con prácticas de Zero Trust.

- **Subcontrol 17.7 – Realizar ejercicios periódicos de respuesta ante incidentes**
  - ***Pilar:*** Infraestructura – IN6
  - ***Recomendación técnica:*** Ejecutar simulacros realistas de ciberataques (phishing, ransomware, denegación de servicio) para evaluar la respuesta del equipo de seguridad y de las áreas involucradas. Medir tiempos de detección, contención y recuperación. Utilizar plataformas de orquestación de respuesta (SOAR).
  - ***Recomendación de proceso:*** Diseñar un plan formal de respuesta a incidentes, con roles bien definidos, comunicación clara y procesos de escalamiento. Estos ejercicios deben realizarse al menos una vez al año e incluir lecciones aprendidas.
  - ***Soluciones o estrategias del mercado:*** IBM Resilient, Splunk SOAR, simuladores BAS como AttackIQ. Ayudan a preparar a la organización para responder a amenazas reales, fortaleciendo la resiliencia cibernética y promoviendo una cultura de prevención proactiva.

CAPÍTULO IV: MATERIALES Y MÉTODOS

4.1. DISEÑO DE CONTRASTACIÓN DE LA HIPÓTESIS

El diseño de contrastación de la hipótesis es descriptivo, de tipo preexperimental con recolección de datos única y post-test.

Esquema del Diseño:

GE (01) ---------- VI ----------M1

Donde:

GE (01) = Grupo Experimental

VI = Controles CIS alineados a los pilares de Zero Trust.

M1 = Madurez de ciberseguridad en las empresas latinas

4.2. POBLACIÓN

Según (Vara Horna, 2008), la población se puede definir como un conjunto de todos los individuos que el investigador o investigadores desean estudiar. Además, estos individuos tienen una o varias características en común como, por ejemplo, el espacio, el territorio, la edad, entre otras.

En esta investigación, la población objetivo está constituida por empresas latinoamericanas de diferentes sectores, específicamente seleccionadas para evaluar su nivel de madurez en ciberseguridad mediante la implementación de Zero Trust alineados a los controles CIS. Los sectores considerados en esta población incluyen financiero, industrial, energía, públicos y otros. Estas empresas varían en cuanto a la cantidad de empleados y otros factores demográficos, lo que proporciona una visión comprensiva de la ciberseguridad en distintos contextos organizacionales.

4.3. MUESTRA

Como se indica en el estudio de (Vara Horna, 2008), la muestra es un conjunto de casos que se extraen de la población. Para seleccionar a la muestra existen diversos métodos que se pueden aplicar, pueden ser probabilísticos y no probabilísticos. Asimismo, al utilizar una muestra se logra ahorrar tiempo, reducir costos y tener una mayor exactitud y profundidad en los resultados del estudio.

Para esta investigación, que se enfoca en evaluar el nivel de madurez en ciberseguridad utilizando la implementación de Zero Trust alineados a los controles CIS en empresas latinoamericanas de diferentes sectores, se calculará la muestra utilizando un método de muestreo probabilístico estratificado. La fórmula utilizada para determinar el tamaño de la muestra en poblaciones finitas es la siguiente:

$$n = \frac{z^2_{1-\frac{\propto}{2}} pqN}{z^2_{1-\frac{\propto}{2}} pq + E^2(N-1)}$$

Donde:

z: Valor tabular asociado a un nivel de confianza.

p: Proporción de éxito.

q: Proporción de fracaso => q = 1 – p

E: Error de estimación.

N: Tamaño de la población.

Ahora, asignaremos un nivel de confianza para la investigación del 95%, por lo tanto, el valor de:

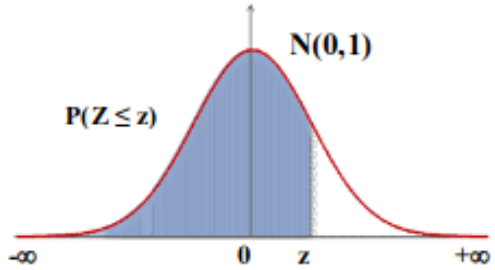
$$\propto = 1 - 0.95 => 0.05$$

Además, reemplazando:

$$1 - \frac{\propto}{2} => 1 - (0.05/2) = 1 - 0.025 => 0.975$$

Por lo tanto, en el momento de reemplazar en la tabla de distribución normal, obtendremos el valor de Z = 1.96.

FUNCIÓN DE DISTRIBUCIÓN NORMAL N(0,1)



z	0,00	0,01	0,02	0,03	0,04	0,05	0,06	0,07	0,08	0,09
0,0	0,5000	0,5040	0,5080	0,5120	0,5160	0,5199	0,5239	0,5279	0,5319	0,5359
0,1	0,5398	0,5438	0,5478	0,5517	0,5557	0,5596	0,5636	0,5675	0,5714	0,5753
0,2	0,5793	0,5832	0,5871	0,5910	0,5948	0,5987	0,6026	0,6064	0,6103	0,6141
0,3	0,6179	0,6217	0,6255	0,6293	0,6331	0,6368	0,6406	0,6443	0,6480	0,6517
0,4	0,6554	0,6591	0,6628	0,6664	0,6700	0,6736	0,6772	0,6808	0,6844	0,6879
0,5	0,6915	0,6950	0,6985	0,7019	0,7054	0,7088	0,7123	0,7157	0,7190	0,7224
0,6	0,7257	0,7291	0,7324	0,7357	0,7389	0,7422	0,7454	0,7486	0,7517	0,7549
0,7	0,7580	0,7611	0,7642	0,7673	0,7704	0,7734	0,7764	0,7794	0,7823	0,7852
0,8	0,7881	0,7910	0,7939	0,7967	0,7995	0,8023	0,8051	0,8078	0,8106	0,8133
0,9	0,8159	0,8186	0,8212	0,8238	0,8264	0,8289	0,8315	0,8340	0,8365	0,8389
1,0	0,8413	0,8438	0,8461	0,8485	0,8508	0,8531	0,8554	0,8577	0,8599	0,8621
1,1	0,8643	0,8665	0,8686	0,8708	0,8729	0,8749	0,8770	0,8790	0,8810	0,8830
1,2	0,8849	0,8869	0,8888	0,8907	0,8925	0,8944	0,8962	0,8980	0,8997	0,9015
1,3	0,9032	0,9049	0,9066	0,9082	0,9099	0,9115	0,9131	0,9147	0,9162	0,9177
1,4	0,9192	0,9207	0,9222	0,9236	0,9251	0,9265	0,9279	0,9292	0,9306	0,9319
1,5	0,9332	0,9345	0,9357	0,9370	0,9382	0,9394	0,9406	0,9418	0,9429	0,9441
1,6	0,9452	0,9463	0,9474	0,9484	0,9495	0,9505	0,9515	0,9525	0,9535	0,9545
1,7	0,9554	0,9564	0,9573	0,9582	0,9591	0,9599	0,9608	0,9616	0,9625	0,9633
1,8	0,9641	0,9649	0,9656	0,9664	0,9671	0,9678	0,9686	0,9693	0,9699	0,9706
1,9	0,9713	0,9719	0,9726	0,9732	0,9738	0,9744	0,9750	0,9756	0,9761	0,9767
2,0	0,9772	0,9778	0,9783	0,9788	0,9793	0,9798	0,9803	0,9808	0,9812	0,9817

Figura 11.Función de Distribución Normal.

Luego de definir el valor de Z, se asignará a "p", o proporción de éxito, un valor de 50%, basándose en la falta de conocimiento previo sobre la proporción exacta de empresas que implementan los controles CIS y los pilares de Zero Trust. Este valor maximiza la variabilidad y proporciona un tamaño de muestra conservador. El 50% restante corresponde a "q", o proporción de fracaso, dado que "q" = 1 - "p".

Por otra parte, el valor para "E" o el error muestral será del 5% o de 0.05 y el tamaño de la población es de 156 empresas.

Entonces, los datos que se deben reemplazar en la fórmula serán los siguientes:

z = 1.96

p = 0.50

q = 0.50

E = 0.05

N = 156

Ahora, reemplazando en la fórmula, se obtendrá el siguiente resultado:

$$n = \frac{(1.96)^2 \; x \; 0.50 \; x \; 0.50 \; x \; 156}{[(1.96)^2 \; x \; 0.50 \; x \; 0.50] + \; [(0.05)^2 \; x \; (156 - 1)]}$$

$$n = 111{,}15 \; \approx 111$$

En consecuencia, se calculó que se tendrá una muestra de 111 para la presente investigación.

4.4. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

4.4.1. Técnicas

4.4.1.1. De Campo

Para recopilar datos primarios directamente del entorno de estudio, se emplearon diversas técnicas de campo. Específicamente, se realizaron encuestas y cuestionarios dirigidos a varias empresas latinas que participaron en las asesorías proporcionadas por la empresa de consultoría Exypnos. La información obtenida a través de estas encuestas y cuestionarios permitió recolectar datos actuales y específicos del contexto de cada empresa. La interacción directa con los participantes facilitó una comprensión detallada y precisa de sus prácticas y desafíos de ciberseguridad.

4.4.1.2. De Gabinete

Para obtener una comprensión integral de la madurez de ciberseguridad, se emplearon diversas técnicas de gabinete. Esto incluyó la revisión exhaustiva de la literatura existente realizada por otros investigadores e instituciones. Además, hizo un análisis documental y de contenido, lo que permitió recopilar una amplia gama de información y antecedentes sobre el tema. Estas técnicas proporcionaron un contexto teórico y empírico esencial para el análisis de los controles CIS y los pilares de Zero Trust.

4.4.2. Instrumentos

4.4.2.1. Encuestas

Las encuestas se utilizan para obtener una visión general amplia sobre las características de las empresas asesoradas, como el tamaño, el sector, la ubicación y otra información relevante.

4.4.2.2. Cuestionarios

Los cuestionarios se emplean para recopilar respuestas directas a preguntas específicas. Son útiles para el análisis cuantitativo y para comparar las respuestas entre diferentes empresas. Por ejemplo, se puede evaluar el puntaje de madurez de ciberseguridad obtenido por una empresa del sector energético.

4.4.2.3. Escala Ordinal

La escala ordinal se utiliza para clasificar elementos en un orden específico según ciertos criterios. En este caso, se emplea para medir el nivel de madurez de ciberseguridad según las respuestas de la encuesta, utilizando categorías como: Básico, Tradicional, Avanzado y Optimizado.

CAPÍTULO V: RESULTADOS Y DISCUSIÓN

5.1. INTRODUCCIÓN

En este capítulo se presentan los resultados obtenidos a partir del análisis de madurez en ciberseguridad de las empresas evaluadas, considerando el enfoque del modelo Zero Trust. La evaluación se ha basado en los seis pilares fundamentales de Zero Trust: Dispositivos, Identidad, Aplicaciones, Redes, Infraestructura y Datos, los cuales han sido alineados con 36 Controles CIS para proporcionar una medición estructurada del nivel de madurez en la región de Latinoamérica.

El diseño metodológico de esta investigación es de tipo descriptivo y preexperimental, con recolección de datos única. Es decir, no se cuenta con mediciones previas ni grupo de control, ya que el objetivo principal es identificar el estado actual de la ciberseguridad en las organizaciones y generar una base para recomendaciones estratégicas futuras.

La información recopilada se presenta de forma estructurada y comparativa, a través de análisis generales, por sector y correlaciones entre pilares.

5.2. ENFOQUE METODOLÓGICO DE LA PRESENTACIÓN DE RESULTADOS

Los resultados se han organizado por dimensiones clave que permiten abordar el tema desde diferentes perspectivas:

- Nivel de madurez por pilar.
- Distribución porcentual por niveles de madurez.
- Análisis detallado de cada pilar (por subcontrol).
- Comparación entre sectores industriales.
- Correlación entre pilares.

Cada sección contiene tanto análisis cuantitativo como visualizaciones para facilitar la comprensión de los patrones encontrados.

5.3. NIVEL GENERAL DE MADUREZ EN CIBERSEGURIDAD

Esta sección ofrece una visión consolidada del nivel de madurez alcanzado de ciberseguridad, considerando los seis pilares evaluados. Se presentan a continuación los resultados en una tabla, con el fin de facilitar el análisis integral del estado actual

Tabla 17. Promedio de Madurez por Pilar

Promedio de madurez por pilar		
Pilar	**Promedio**	**Desviación Estándar**
Dispositivos	2.23	0.89
Identidad	2.37	0.77
Redes	2.83	0.63
Aplicaciones	2.55	0.75
Infraestructura	2.30	0.74
Datos	1.91	0.64

Fuente: Elaboración propia

El análisis muestra que el pilar con mayor madurez es **Redes**, con un promedio de **2.83**, lo que lo sitúa cerca del nivel **Avanzado**. Le siguen **Aplicaciones (2.55)** e **Identidad (2.37),** ambas dentro del rango **Tradicional a Avanzado**. En contraste, el pilar **Datos** presenta el menor promedio **(1.91)**, evidenciando una brecha significativa en la implementación de controles asociados, con predominancia de niveles **Básico a Tradicional**. La mayor variabilidad se observa en **Dispositivos** (desviación estándar de 0.89), lo que indica una adopción más desigual entre las organizaciones evaluadas.

5.4. DISTRIBUCIÓN DE MADUREZ POR NIVEL

En esta sección se presentan los porcentajes correspondientes a cada nivel de madurez alcanzado. La figura a continuación permite visualizar cómo se distribuyen los resultados a lo largo de los distintos niveles evaluados, facilitando la identificación de áreas con mayor desarrollo y aquellas que requieren fortalecimiento.

Promedio de madurez de pilares por sector						
Sector	**Aplicaciones**	**Datos**	**Dispositivos**	**Identidad**	**Infraestructura**	**Redes**
Energia	2.46	1.86	2.28	2.42	2.35	2.75
Financiero	2.67	2.02	2.36	2.46	2.49	2.86
Industrial	2.74	1.92	2.34	2.51	2.34	3.03
Publico	2.53	1.99	2.24	2.43	2.33	2.82
Otros	2.35	1.64	1.93	2.04	1.97	2.69

Figura 12. Mapa de Calor de la Distribución de Madurez de Pilares por Sector

Fuente: Elaboración Propia.

El sector **industrial** presenta los niveles más altos de madurez en la mayoría de los pilares, alcanzando valores cercanos al nivel **Avanzado** en **Redes (3.03)** y **Aplicaciones (2.74)**. Le sigue el sector **financiero**, con un desempeño sólido y consistente, situado en su mayoría dentro del rango **Tradicional a Avanzado**. En contraste, el grupo **"Otros"** registra los promedios más bajos, manteniéndose en niveles **Básico o apenas Tradicional**, especialmente en **Datos (1.64)** y **Dispositivos (1.93)**, lo que evidencia una menor adopción de controles de ciberseguridad en dicho segmento.

5.5. ANÁLISIS DETALLADO POR PILAR

En esta sección se examina cada pilar de forma individual, considerando el desempeño alcanzado en cada uno de sus subcontroles. Se incluyen tablas que detallan la distribución del nivel de madurez por subcontrol, así como gráficos de barras que muestran el nivel de madurez alcanzado por cada uno de los seis pilares.

5.5.1. Dispositivos

Tabla 18. Distribución Porcentual de Empresas según Nivel de Madurez en el Pilar de Dispositivos

Dispositivos						
Nº	**Descripción**	**Básico**	**Tradicional**	**Avanzado**	**Optimizado**	**Total**
DI-1	Establecer y mantener un proceso de configuraciones seguras	4.98%	42.15%	39.08%	13.79%	100%
DI-2	Forzar reseteo remoto (Wipe) para dispositivos portátiles de usuarios finales	27.32%	21.46%	33.66%	17.56%	100%
DI-3	Gestione y controle acceso por condiciones para activos conectados remotamente	0.78%	59.92%	31.52%	7.78%	100%
DI-4	Identificar y remover activos no autorizados	7.05%	56.43%	19.92%	16.60%	100%
DI-5	Mantener un inventario de activos detallado y actualizado	5.24%	39.70%	32.58%	22.47%	100%
DI-6	Separar ambiente empresarial en dispositivos móviles	42.01%	28.40%	24.85%	4.73%	100%
DI-7	Usar plantillas de seguridad (Hardening) para configuraciones estándares	5.28%	53.66%	32.93%	8.13%	100%
DI-8	Usar tecnologías anti-explotación basadas en análisis de datos y comportamiento (p.e. EDR)	0.30%	16.92%	48.94%	33.84%	100%
Total		9.46%	39.76%	33.99%	16.79%	100%

Fuente: Elaboración Propia.

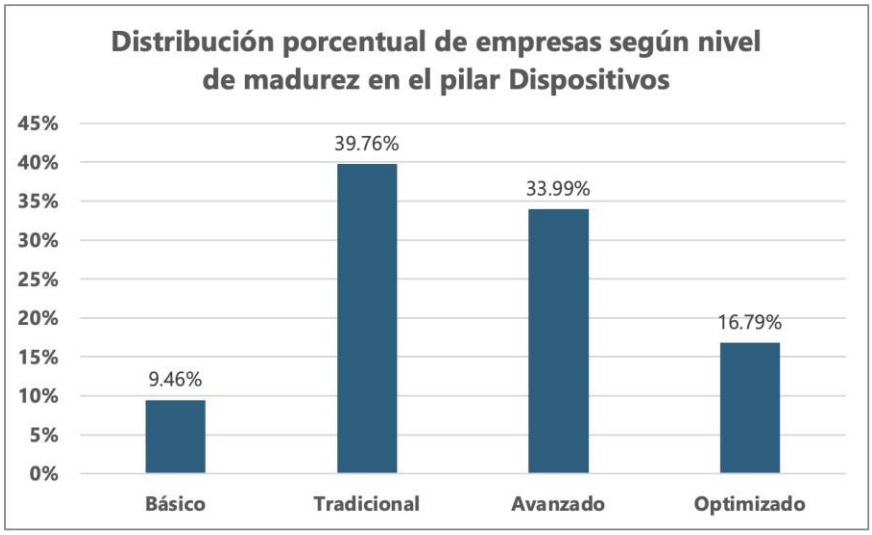


Figura 13. Gráfico de Barras de la Distribución Porcentual de Empresas según Nivel de Madurez en el Pilar de Dispositivos

Fuente: Elaboración Propia.

En el pilar **Dispositivos**, la mayoría de las empresas se ubica en niveles **Tradicional (39.76%)** y **Avanzado (33.99%)**, con menor presencia en **Optimizado (16.79%)**. A nivel de subcontroles, **D1.2 y D1.6** presentan los mayores porcentajes en nivel **Básico**, lo que evidencia brechas en el uso seguro de acceso remoto y segmentación de entornos. Por el contrario, **D1.5 y D1.8** destacan por su mayor madurez, con más del **50%** de empresas en niveles **Avanzado u Optimizado**, reflejando una mejor adopción de inventariado actualizado y tecnologías anti-exploit.

5.5.2. Identidad

Tabla 19. Distribución Porcentual de Empresas según Nivel de Madurez en el Pilar de Identidad

Identidad						
N°	Descripción	Básico	Tradicional	Avanzado	Optimizado	Total
ID-1	Centralizar el control de acceso a todos los activos tecnológicos	2.79%	57.37%	33.47%	6.37%	100%
ID-2	Gestión de cuentas centralizada mediante servicio de identidad o directorio	0.76%	53.23%	39.92%	6.08%	100%
ID-3	Gestione o desactive las cuentas por defecto en los sistemas empresariales	4.78%	49.40%	39.44%	6.37%	100%
ID-4	Requerir autenticación multi-factor para accesos administrativos (privilegiados)	3.27%	32.00%	58.91%	5.82%	100%
ID-5	Requerir autenticación multi-factor para todo acceso remoto	9.96%	38.17%	48.55%	3.32%	100%
ID-6	Revisar periodicamente logs de auditoría para detectar eventos sospechosos	4.01%	29.43%	21.07%	45.48%	100%
Total		4.18%	42.78%	39.87%	13.16%	100%

Fuente: Elaboración Propia.

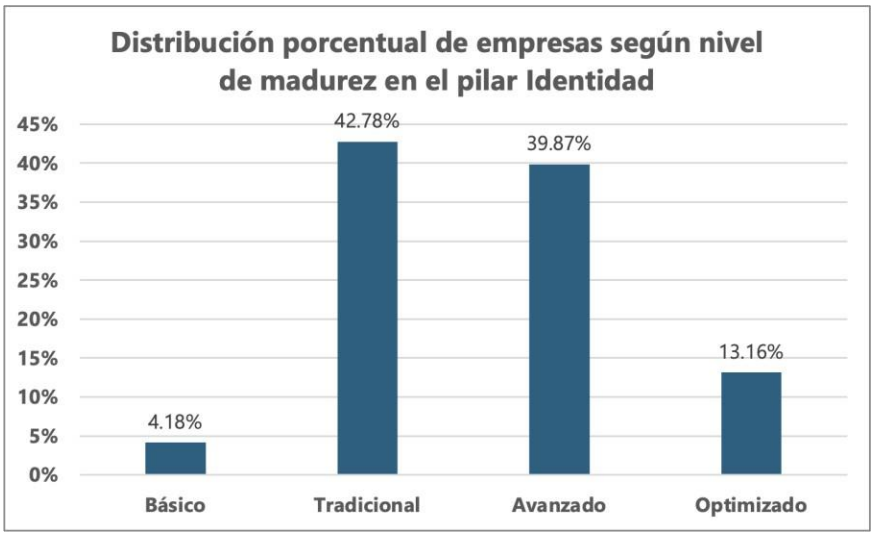


Figura 14. Gráfico de Barras de la Distribución Porcentual de Empresas según Nivel de Madurez en el Pilar de Identidad

Fuente: Elaboración Propia.

En el pilar **Identidad**, la mayoría de las empresas se concentra en los niveles **Tradicional (42.78%)** y **Avanzado (39.87%)**, reflejando una implementación progresiva de controles de acceso. Los subcontroles **ID-4** (autenticación multi-factor administrativa) e **ID-2/ID-3** (gestión de cuentas y control de cuentas por defecto) destacan con más del **39%** de empresas en nivel **Avanzado**, aunque su adopción en **Optimizado** aún es limitada. En contraste, el subcontrol **ID-5** muestra un 9.96% en **Básico**, lo que evidencia rezago en el uso de autenticación fuerte para accesos remotos. Por su parte, **ID-6** presenta una madurez más distribuida, con un 45.48% en **Optimizado**, lo que indica una mejor práctica en la revisión de logs de auditoría.

5.5.3. Aplicaciones

Tabla 20. Distribución Porcentual de Empresas según Nivel de Madurez en el Pilar de Aplicaciones

Aplicaciones						
N°	**Descripción**	**Básico**	**Tradicional**	**Avanzado**	**Optimizado**	**Total**
AP-1	Atender periodicamente el software no autorizado detectado	2.60%	46.10%	33.46%	17.84%	100%
AP-2	Definir y mantener un control de acceso basado en roles a los recursos empresariales	1.49%	46.84%	41.26%	10.41%	100%
AP-3	Limite el uso de software y/o acceso a servicios autorizados	2.13%	34.75%	48.94%	14.18%	100%
AP-4	Realizar filtrado de contenido en la capa de aplicación	0.96%	21.73%	51.76%	25.56%	100%
Total		1.77%	36.72%	44.22%	17.30%	100%

Fuente: Elaboración Propia.

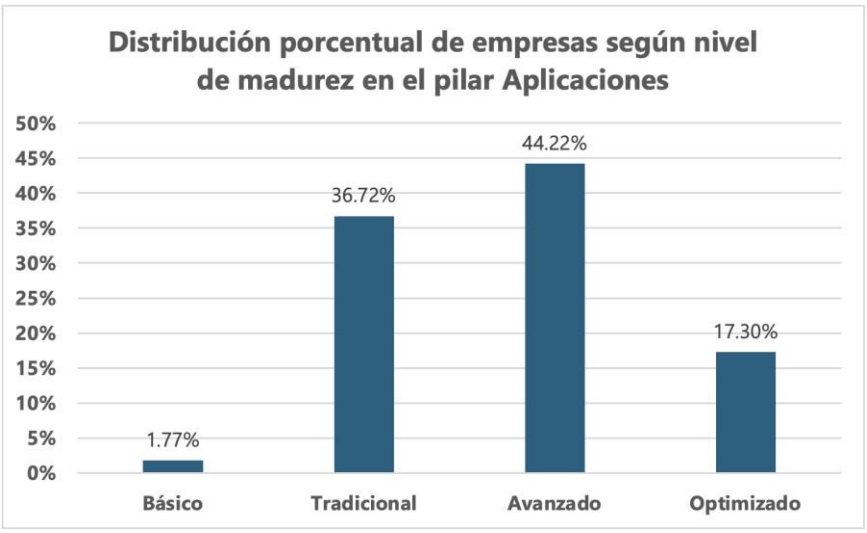


Figura 15. Gráfico de Barras de la Distribución Porcentual de Empresas según Nivel de Madurez en el Pilar de Aplicaciones

Fuente: Elaboración Propia.

En el pilar **Aplicaciones**, la mayoría de las empresas se sitúa en los niveles **Avanzado (44.22%)** y **Tradicional (36.72%)**, lo que indica un grado de madurez medio-alto en la implementación de controles asociados. El subcontrol **AP-4** destaca con el mayor porcentaje en **Avanzado (51.76%)**, seguido por **AP-3** con **48.94%**, evidenciando un enfoque sólido en filtrado a nivel de aplicación y control sobre software autorizado. Por su parte, **AP-1** presenta una distribución más equilibrada entre niveles Tradicional y Avanzado, mientras que **AP-2** muestra la mayor concentración en nivel Tradicional (46.84%) con menor adopción en Optimizado (10.41%). En conjunto, el pilar refleja un avance importante, aunque con oportunidades de mejora en automatización y optimización de controles.

5.5.4. Redes

Tabla 21. Distribución Porcentual de Empresas según Nivel de Madurez en el Pilar de Redes

Redes						
Nº	**Descripción**	**Básico**	**Tradicional**	**Avanzado**	**Optimizado**	**Total**
RE-1	Gestionar la seguridad de la infraestructura de red	0.00%	26.35%	70.95%	2.70%	100%
RE-2	Implementar y mantener protección antimalware a nivel de correo	0.00%	20.06%	57.37%	22.57%	100%
RE-3	Mantener y forzar filtrado de URL a nivel de red	0.00%	21.05%	49.23%	29.72%	100%
RE-4	Realizar filtrado de tráfico entre segmentos de red	0.00%	16.98%	67.92%	15.09%	100%
Total		0.00%	21.02%	61.15%	17.83%	100%

Fuente: Elaboración Propia.

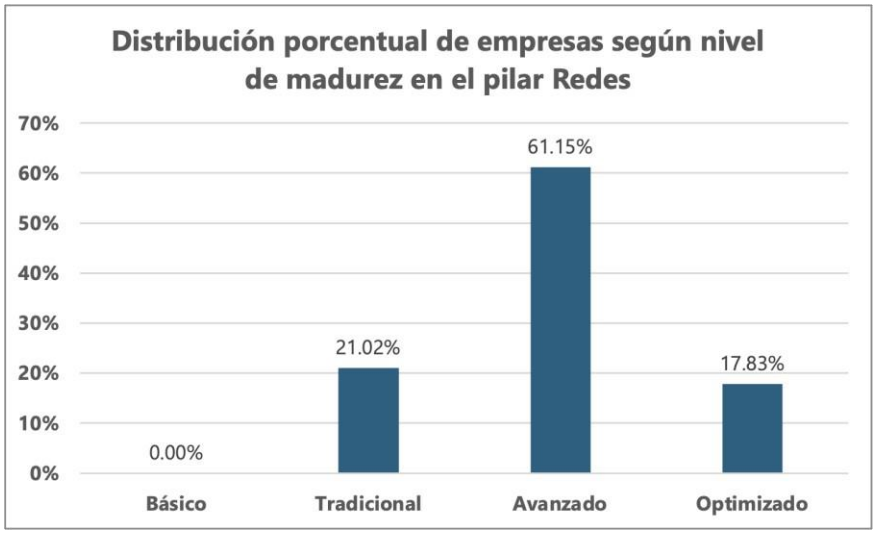


Figura 16. Gráfico de Barras de la Distribución Porcentual de Empresas según Nivel de Madurez en el Pilar de Redes

Fuente: Elaboración Propia.

El pilar **Redes** presenta uno de los niveles de madurez más altos, con una concentración del **61.15%** en **Avanzado** y **17.83%** en **Optimizado**, sin presencia en nivel Básico. El subcontrol **RE-1**, relacionado con la gestión de seguridad en infraestructura de red, lidera con **70.95%** en **Avanzado**, reflejando un control ampliamente adoptado. Asimismo, **RE-2** y **RE-3** muestran una distribución favorable, con más del 50% en Avanzado y valores significativos en Optimizado (**22.57%** y **29.72%**, respectivamente). Aunque el nivel de madurez es alto en general, el menor porcentaje en Optimizado sugiere que aún hay espacio para mejorar en automatización y monitoreo continuo de políticas de red.

5.5.5. Infraestructura

Tabla 22. Distribución Porcentual de Empresas según Nivel de Madurez en el Pilar de Infraestructura

Infraestructura						
N°	Descripción	Básico	Tradicional	Avanzado	Optimizado	Total
IN-1	Aplicar principios de diseño seguro en arquitectura de aplicaciones	11.37%	71.09%	15.64%	1.90%	100%
IN-2	Centralizar autenticación, autorización y auditoría (AAA) en la red	2.72%	52.14%	37.35%	7.78%	100%
IN-3	Centralizar la alerta de eventos de seguridad (p.e. SIEM o Log Analytics)	9.45%	29.13%	51.97%	9.45%	100%
IN-4	Establecer y mantener una arquitectura de red segura	0.73%	43.96%	49.45%	5.86%	100%
IN-5	Gestionar activos y cargas empresariales con configuraciones seguras	3.31%	37.50%	47.43%	11.76%	100%
IN-6	Realizar ejercicios periódicos de respuesta ante incidentes	7.69%	58.12%	25.64%	8.55%	100%
IN-7	Restringir privilegios administrativos exclusivamente para cuentas dedicadas administrativas	4.82%	53.82%	30.12%	11.24%	100%
IN-8	Usar soluciones basadas en analítica del comportamiento	1.37%	30.82%	51.37%	16.44%	100%
Total		4.90%	46.03%	39.67%	9.40%	100%

Fuente: Elaboración Propia.

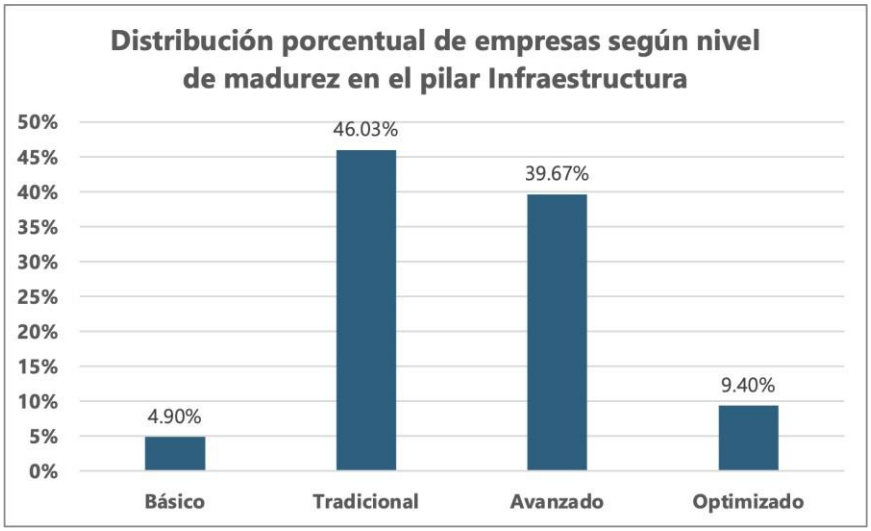


Figura 17. Gráfico de Barras de la Distribución Porcentual de Empresas según Nivel de Madurez en el Pilar de Infraestructura

Fuente: Elaboración Propia.

El pilar **Infraestructura** presenta una distribución centrada en el nivel **Tradicional (46.03%)**, seguido de **Avanzado (39.67%)**, con una menor proporción en **Optimizado (9.40%)**. Destaca el subcontrol **IN-3**, con **51.97%** en **Avanzado**, reflejando una adopción significativa de soluciones de monitoreo como SIEM. Asimismo, **IN-5** e **IN-8** se aproximan al 50% en niveles medio-altos, evidenciando buenas prácticas en configuraciones seguras y análisis del comportamiento. En contraste, IN-1 presenta el mayor rezago, con **11.37%** en **Básico** y solo **1.90%** en **Optimizado**, lo que indica desafíos en la implementación de diseño seguro en

arquitecturas. En general, este pilar muestra una adopción moderada de controles, con potencial de mejora en automatización y consolidación de prácticas avanzadas.

5.5.6. Datos

Tabla 23. Distribución Porcentual de Empresas según Nivel de Madurez en el Pilar de Datos

Datos						
N°	Descripción	Básico	Tradicional	Avanzado	Optimizado	Total
DA-1	Encriptar información sensible en reposo	17.00%	66.00%	15.00%	2.00%	100%
DA-2	Encriptar información sensible en tránsito	3.73%	63.07%	29.88%	3.32%	100%
DA-3	Establecer y mantener un esquema de clasificación de datos	13.43%	55.56%	29.17%	1.85%	100%
DA-4	Establecer y mantener un proceso de gobierno de datos	13.74%	61.61%	22.75%	1.90%	100%
DA-5	Implementar una solución DLP (Data Loss Prevention)	20.83%	63.54%	15.63%	0.00%	100%
DA-6	Registrar y controlar acceso a datos sensibles (incluyendo cambios y eliminaciones)	12.44%	68.90%	18.66%	0.00%	100%
Total		13.16%	63.04%	22.22%	1.58%	100%

Fuente: Elaboración Propia.

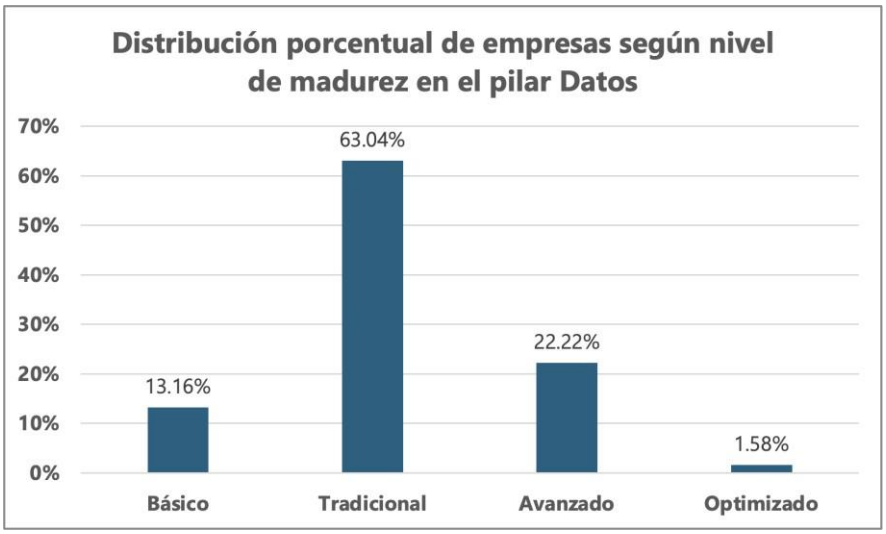


Figura 18. Gráfico de Barras de la Distribución Porcentual de Empresas según Nivel de Madurez en el Pilar de Datos

Fuente: Elaboración Propia.

El pilar **Datos** presenta el nivel de madurez más bajo del modelo, con una fuerte concentración en el nivel **Tradicional (63.04%)** y baja presencia en **Avanzado (22.22%)** y **Optimizado (1.58%)**. Destacan **DA-1** y **DA-5** con los porcentajes más altos de clientes en nivel **Básico (17% y 20.83%)**, evidenciando rezagos importantes en la protección de datos en reposo y la implementación de soluciones DLP. Asimismo, DA-6 refleja una limitada madurez con **68.90%** en **Tradicional** y **0%** en **Optimizado**, indicando carencias en el control de accesos a datos

sensibles. En general, este pilar muestra un estado inicial de adopción de controles, con oportunidades claras de mejora en automatización, clasificación de datos y gobierno efectivo de la información.

5.6. CORRELACIÓN ENTRE PILARES

Esta sección analiza la relación estadística entre los distintos pilares evaluados, utilizando el coeficiente de correlación de Pearson como método de medición.

Correlación entre pilares						
Pilar	**Identidad**	**Dispositivos**	**Aplicaciones**	**Redes**	**Infraestructura**	**Datos**
Identidad	1.00	0.66	0.50	0.48	0.68	0.53
Dispositivos	0.66	1.00	0.55	0.48	0.73	0.49
Aplicaciones	0.50	0.55	1.00	0.47	0.54	0.38
Redes	0.48	0.48	0.47	1.00	0.51	0.30
Infraestructura	0.68	0.73	0.54	0.51	1.00	0.59
Datos	0.53	0.49	0.38	0.30	0.59	1.00

Figura 19. Mapa de Calor de la Correlación entre Pilares

Fuente: Elaboración Propia.

El análisis de correlación entre pilares muestra asociaciones relevantes en el desarrollo de capacidades de ciberseguridad. La relación más fuerte se observa entre **Dispositivos e Infraestructura (0.73)**, seguida por **Identidad e Infraestructura (0.68)** e **Identidad–Dispositivos (0.66)**, lo que indica que las organizaciones que invierten en gestión de infraestructura y control de accesos tienden a desarrollar capacidades de manera conjunta en estas áreas.

En contraste, el pilar **Datos** presenta las correlaciones más bajas con el resto, especialmente con **Redes (0.30)** y **Aplicaciones (0.38)**, lo que sugiere que su madurez avanza de manera más aislada o independiente. Esto refuerza la necesidad de **integrar prácticas de protección de datos** dentro de estrategias más amplias de seguridad.

En general, los pilares presentan correlaciones moderadas, reflejando un grado de interdependencia en la implementación de controles, aunque aún con oportunidades de mejora en la articulación entre dominios estratégicos.

5.7. HALLAZGOS RELEVANTES

Se evidencia diferencias significativas entre pilares, sectores y prácticas específicas. A nivel general, los pilares **Redes y Aplicaciones** presentan mayores niveles de madurez, mientras que **Datos** y **Dispositivos** muestran rezagos importantes, especialmente en la adopción de controles avanzados y automatizados.

El pilar **Datos** es el más crítico, ya que, tiene niveles **Básico** y **Tradicional** en la mayoría de subcontroles, lo que refleja una débil gestión en protección, clasificación y monitoreo de información sensible. En contraste, **Redes** destaca como el pilar más fortalecido, con altos porcentajes en niveles **Avanzado**, evidenciando un enfoque prioritario en la protección de la conectividad e infraestructura técnica.

Al analizar por sector, se observa que los rubros **financiero** e **industrial** alcanzan los mayores promedios de madurez, lo que indica un enfoque más robusto en gestión de riesgos digitales. Por otro lado, el grupo **"Otros"** presenta los niveles más bajos, con valores cercanos a **Básico**, reflejando una menor capacidad o prioridad en ciberseguridad.

La correlación entre pilares revela relaciones fuertes y consistentes entre **Infraestructura**, **Dispositivos** e **Identidad**, lo que sugiere que el fortalecimiento de uno de estos dominios tiende a estar acompañado por avances en los otros. Sin embargo, el pilar **Datos** nuevamente se presenta como el más débilmente correlacionado, lo que indica que su evolución no necesariamente avanza en sincronía con el resto de los componentes.

En conjunto, los hallazgos evidencian que, si bien existen avances importantes en ciertos dominios, persisten **brechas estructurales** que deben ser abordadas, particularmente en la protección de datos y la integración transversal de controles de seguridad.

5.8. CONTRASTACIÓN DE LA HIPÓTESIS

Los resultados del estudio permiten **confirmar la hipótesis**, al demostrar que el análisis de controles CIS alineados a los pilares de Zero Trust es una herramienta válida para medir la madurez de ciberseguridad en empresas latinoamericanas. La evaluación permitió identificar diferencias claras entre pilares, subcontroles y sectores, reflejando la efectividad del modelo propuesto para diagnosticar niveles de madurez de forma estructurada y comparativa.

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

- Se logró establecer una correlación efectiva entre los 36 controles del marco CIS y los 6 pilares del modelo Zero Trust, obteniendo en una herramienta cuantitativa clara para evaluar el nivel de madurez de ciberseguridad. Esta correlación facilitó el diseño de indicadores precisos por pilar, adaptables a distintas industrias de Latinoamérica.

- Se evidenció diferencias notables en la distribución de niveles de madurez. Redes destaca como el pilar más avanzado, con un 61 % de las empresas en nivel avanzado y un 17 % en optimizado, seguido por Aplicaciones, donde el 44 % se ubica en avanzado y 17 % en optimizado. Estos resultados indican progreso en aspectos relacionados con conectividad y seguridad del software. En contraste, pilares como Datos presentan una alta concentración en niveles medios y bajos, con un 63 % de las empresas en nivel tradicional y un 13 % en básico, mientras que Dispositivos muestra también una distribución baja, con 39 % en tradicional y 9 % en básico, lo que evidencia áreas críticas que aún requieren fortalecimiento en estrategias de ciberseguridad.

- Se evidenció que los sectores con mayor madurez en ciberseguridad fueron aquellos relacionados con servicios financieros e industriales, mostrando mayores puntajes en niveles avanzados y optimizados. Por el contrario, sectores públicos y educativos presentaron niveles básicos o tradicionales, revelando una brecha preocupante en monitoreo de dispositivos y protección de datos sensibles.

- Se identificaron patrones comunes entre los pilares analizados. Por ejemplo, se observa una tendencia en niveles de madurez “básicos” en controles relacionados con la implementación de soluciones DLP y la autenticación MFA, mientras que se registran

avances hacia niveles “optimizados” en controles como el filtrado de contenido en la capa de aplicación y el filtrado de URL a nivel de red. Estos resultados demuestran que muchas organizaciones priorizan medidas más visibles de protección perimetral, mientras que aún presentan brechas importantes en protección de datos sensibles y gestión de identidad, lo cual pone en evidencia una madurez parcial y desbalanceada que puede comprometer la ciberseguridad de sus entornos.

- El análisis cuantitativo del nivel de madurez permitió proponer mejorar para fortalecer la resiliencia ante amenazas modernas como ransomware, filtraciones de datos y suplantación de identidad, los cuales son problemas en aumento en la región.

- Se confirmó la hipótesis inicial luego de hallar los resultados de la investigación. El análisis estructurado de los controles CIS alineados a los pilares del modelo Zero Trust demostró ser una metodología efectiva para medir el nivel de madurez de ciberseguridad en empresas latinoamericanas durante el año 2023. Esta metodología permitió cuantificar la madurez de forma clara y replicable, aportando valor tanto al ámbito organizacional como académico.

6.2. RECOMENDACIONES

- Las empresas latinoamericanas deben migrar hacia una arquitectura de Zero Trust, priorizando pilares más rezagados como Datos y Dispositivos. Esta adopción debe ser gradual, comenzando por controles críticos relacionados a controlar el acceso a los datos sensibles y separar el ambiente empresarial de dispositivos móviles.

- Se sugiere establecer iniciativas regionales que promuevan la inversión en ciberseguridad en sectores públicos y educativos, mediante políticas públicas, alianzas estratégicas y cooperación internacional.

- Invertir en soluciones automatizadas y entrenamiento especializado. Las recomendaciones técnicas incluyen el uso de SIEM (Control de logs), EDR

(Dispositivos), IAM (Identidad) y SOAR (Respuesta ante incidentes) para aumentar la eficiencia de respuesta y control. Del mismo modo, es importante capacitar al personal en el uso de estas herramientas y promover la sensibilización organizacional sobre ciberseguridad.

- Las empresas deben implementar ciclos de revisión y mejora de sus controles CIS alineados a Zero Trust. Esto incluye auditorías periódicas, revisión de logs, pruebas de penetración y simulacros internos.

- Fomentar el uso de la metodología propuesta para futuras investigaciones en diferentes contextos regionales, sectores y tamaños empresariales, contribuyendo a una cultura de ciberseguridad más sólida y basada en evidencia.

CAPÍTULO VII: REFERENCIAS BIBLIOGRÁFICAS

Akami. (s.f.). *Modelo de seguridad Zero Trust: ¿Qué es Zero Trust?* Obtenido de https://www.akamai.com/es/glossary/what-is-zero-trust

Almagro, L., Oliveira, L., August Treppel, A., Barrett, K.-A., Garcés, O., Moreno, D., . . . Venugopal, V. (2023). *Reporte sobre el desarrollo de la Fuerza Laboral de Ciberseguridad en una era de escasez de talento y habilidades.* Organización de los Estados Americanos.

Center for Internet Security. (20 de Octubre de 2021). CIS Critical Security Controls Version 8.

Charfoos, A., Cronin, C., de Vallance, B., Dukes, C., Herath, K., Lee, P., . . . Victor, I. (2024). *A Guide to Defining Reasonable Cybersecurity.* Mayo: Center for Internet Security.

CISCO. (s.f.). *Cómo Cisco habilita Zero Trust Security*. Obtenido de https://www.cisco.com/site/mx/es/solutions/security/zero-trust/index.html#accordion-1eed8426ac-item-ed17d9d080

Contreras, B. (2 de Mayo de 2024). *Lecciones de ciberseguridad de la batalla de América Latina contra las amenazas de ransomware*. Obtenido de https://es.weforum.org/agenda/2024/05/lecciones-de-ciberseguridad-de-la-batalla-de-america-latina-contra-las-amenazas-de-ransomware/

Contreras, B., Steffaro, A., Jordan-Zoob, I., Hoffman, D., Herrera, C., Bermúdez, L., . . . González Castellanos, H. (2024). *PREPARACIÓN CIBERNÉTICA EN LOS SECTORES PÚBLICOS DE AMÉRICA LATINA: LECCIONES DE LA PRIMERA LÍNEA.*

Cybersecurity Insiders. (2024). *2024 Insider Threat Report Trends, Challenges, and Solutions.*

Esteban, D., García, D., Llorente, D., Sánchez, I., Forné, O., Sánchez, Ó., . . . García, T. (2024). *IV Indicador de madurez en ciberseguridad del Observatorio de la Ciberseguridad.* Barcelona.

EY. (09 de Octubre de 2023). *Panorama de ciberseguridad en Latinoamérica: ¿qué riesgos enfrentan las empresas?* Obtenido de https://www.ey.com/es_py/cybersecurity/panorama-ciberseguridad-latinoamerica-riesgos-enfrentan-empresas

Fortinet. (s.f.). *¿Qué es Confianza Cero modelo Zero Trust?* Obtenido de https://www.fortinet.com/lat/resources/cyberglossary/what-is-the-zero-trust-network-security-model

Friel, D. (9 de Agosto de 2021). *Riesgos de ciberseguridad: ¿Factores humanos o fallos humanos?* Obtenido de https://www.metacompliance.com/es/blog/cyber-security-awareness/cyber-security-risk?_gl=1*1b01qx7*_up*MQ..*_ga*NTEyMTg5NjUxLjE3MTc0NzIyNjM.*_ga_YM5NQGCDCJ*MTcxNzQ3MjI2My4xLjEuMTcxNzQ3MjI5OS4wLjAuMA..

Gartner. (2024). *Las 9 principales tendencias en ciberseguridad para 2024.*

Hanwa Vision. (24 de Febrero de 2023). *La Importancia de la Ciberseguridad en Latinoamérica*. Obtenido de https://hanwhavisionlatam.com/blog/la-importancia-de-la-ciberseguridad-en-latinoamerica/#:~:text=La%20ciberseguridad%20no%20solo%20es,estabilidad%20y%20la%20seguridad%20nacional.

IBM. (s.f.). *¿Qué es Zero Trust?* Obtenido de https://www.ibm.com/es-es/topics/zero-trust

IBM. (2024). *X-Force Threat Intelligence Index 2024.* Madrid.

ISO (International Organization for Standardization). (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* Ginebra.

Kindervag, J. (14 de Septiembre de 2010). *No More Chewy Centers: Introducing The Zero Trust Model Of Information Security.*

Kindervag, J. (21 de Junio de 2023). Creator of Zero Trust Gives You a 30 Second Elevator Pitch | John Kindervag & Kevin Bocek, Venafi. (K. Bocek, Entrevistador)

L&Co Staff Auditors. (4 de Enero de 2023). *Security Maturity Models: Common Levels of Maturity & How They're Evaluated*. Obtenido de https://linfordco.com/blog/security-maturity-models/#:~:text=What%20is%20the%20Security%20Maturity,compliance%20framework%20suggestions%20or%20requirements

Microsoft. (31 de Julio de 2023). *Overview of Microsoft cloud security benchmark (v1)*. Obtenido de https://learn.microsoft.com/en-us/security/benchmark/azure/overview

Microsoft. (30 de Enero de 2024). *Introduction to the Microsoft cloud security benchmark*. Obtenido de https://learn.microsoft.com/en-us/security/benchmark/azure/introduction

Microsoft. (12 de Abril de 2024). *What is Zero Trust?* Obtenido de https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview

Microsoft. (12 de Abril de 2024). *Zero Trust deployment for technology pillars*. Obtenido de https://learn.microsoft.com/en-us/security/zero-trust/deploy/overview

Moriarty, K. (27 de Julio de 2021). *Center for Internet Security.* Obtenido de https://www.cisecurity.org/insights/blog/prioritizing-a-zero-trust-journey-using-cis-controls-v8

National Institute of Standards and Technology . (26 de Febrero de 2024). The NIST Cybersecurity Framework (CSF) 2.0. Estados Unidos.

Newton, P. (12 de Enero de 2022). *Survey Reveals Challenges of Zero Trust Implementation*. Obtenido de https://www.fortinet.com/blog/business-and-technology/fortinet-zero-trust-survey-indicates-gaps-in-implementation

Nordic Defender. (3 de Abril de 2023). *The Benefits and Challenges of Implementing the CIS Controls*. Obtenido de https://nordicdefender.com/blog/benefits-and-challenges-of-cis-controls

Olufon, T., & Ber, Z. (11 de Abril de 2024). *Building A Zero Trust Roadmap: A Practical Guide*. Obtenido de https://www.forrester.com/blogs/building-a-zero-trust-roadmap-a-practical-guide/?ref_search=0_1716164296681

Organización de los Estados Americanos. (2022). *National Cybersecurity Strategies: Lessons Learned and Reflections from the Americas and Other Regions.*

Organización de los Estados Americanos. (2023). *Retos y Estrategias: Las consideraciones de los ataques de ransmware en las Américas.*

Ramírez Cuenca, F., Gutiérrez Amaya, C., & González Cuautle, D. (2024). *TENDENCIAS EN CIBERSEGURIDAD PARA EL 2024.*

Robledo Hoecker, M. (2023). *AMÉRICA LATINA Y LA GOBERNANZA GLOBAL Y REGIONAL SOBRE CIBERSEGURIDAD.* Bogotá.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture.* National Institute of Standards and Technology.

Ruiz, R. (s.f.). *Ciberseguridad en LatAm: nuevos desafíos en la era digital*. Obtenido de https://cibergestion.com/2024/02/14/ciberseguridad-en-latam-nuevos-desafios-en-la-era-digital/

Schwartz, A., Contreras, B., Botting, A., Hoffman, D., Rodríguez Maffioli, D., Kotz, A., . . . Reeves, S. (2023). *Perspectivas de Ciberseguridad de los Líderes de la Industria*. LATAM CISO.

Shea, S., & Turpitka, D. (11 de Octubre de 2022). *What is the zero-trust security model?* Obtenido de https://www.techtarget.com/searchsecurity/tip/Top-risks-of-deploying-zero-trust-cybersecurity-model

Tadmor, E. (26 de Diciembre de 2023). *3 Common Challenges and Solutions when Implementing Zero Trust Networking Policies*. Obtenido de https://www.tufin.com/blog/3-challenges-and-solutions-implementing-zero-trust

Tenable. (2023). *EVALUACIÓN CONSTANTE DE CIS PARA UN MUNDO DE ZERO TRUST.*

Terranova Security. (30 de Octubre de 2023). *The Limitations of Zero Trust Architecture and How to Overcome Them.* Obtenido de https://www.terranovasecurity.com/blog/limitations-of-zero-trust-architecture#:~:text=Here's%20where%20most%20security%20professionals,%2C%20access%20control%2C%20and%20monitoring.

U.S. Department of Energy. (Junio de 2022). Cybersecurity Capability Maturity Model (C2M2) Version 2.1. Estados Unidos.

Unidad Latina. (13 de Abril de 2024). *Ciberseguridad en América Latina*. Obtenido de https://unidadlatina.org/tecnologia/ciberseguridad-en-america-latina/#Casos_representativos_de_ciberseguridad_en_America_Latina

Vara Horna, A. A. (2008). *La tesis de maestría en educación. Una guía efectiva para obtener el grado de maestro y no desistir en el intento. Tomo I. El proyecto de tesis.* Lima: Depósito Legal en la Biblioteca Nacional del Perú.

ANEXOS

ANEXO A

SUBPROBLEMAS:

- **DEFICIENCIA 1:** EVOLUCIÓN CONSTANTE DE LAS AMENAZAS CIBERNÉTICAS Y CIBERDELINCUENTES EN LA SOCIEDAD ACTUAL.

  Formulación del Subproblema 1:

  ¿De qué manera el análisis de los controles CIS alineados a los pilares de Zero Trust enfrentará los efectos de la evolución constante de las amenazas cibernéticas y ciberdelincuentes en la sociedad actual?

  Objetivo Específico 1:

  Analizar y evaluar el nivel de madurez de ciberseguridad en empresas latinas mediante el análisis de los controles CIS alineados a los pilares de Zero Trust, para proponer recomendaciones y mejoras con el fin de fortalecer la ciberseguridad y contrarrestar los efectos de la evolución constante de las amenazas cibernéticas y ciberdelincuentes.

- **DEFICIENCIA 2:** PRESUPUESTO LIMITADO Y FALTA DE INTERÉS PARA EL ÁREA DE CIBERSEGURIDAD DENTRO DE LAS ORGANIZACIONES.

  Formulación del Subproblema 2:

  ¿De qué manera análisis de los controles CIS alineados a los pilares de Zero Trust brindará estrategias efectivas para incentivar el aumento del presupuesto y el interés para el área de ciberseguridad dentro de las organizaciones?

  Objetivo Específico 2:

  Evaluar y proponer estrategias concretas fundamentadas en el análisis de los controles CIS alineados a los pilares de Zero Trust. para incentivar el aumento del presupuesto y el interés para el área de ciberseguridad dentro de las organizaciones.

- **DEFICIENCIA 3:** CAMBIO EN LA FORMA DE TRABAJAR, DE PRESENCIAL A REMOTO, DESDE LA PANDEMIA DEL COVID-19 INICIADA EN EL AÑO 2020.

  Formulación del Subproblema 3:

  ¿Cómo el análisis de los controles CIS alineados a los pilares de Zero Trust permitirá comprender el impacto en la ciberseguridad causado por el cambio en la forma de trabajar, de presencial a remoto, desde la pandemia del COVID-19 iniciada en el año 2020?

  Objetivo Específico 3:

  Identificar vulnerabilidades y proponer estrategias efectivas basadas en el análisis de los controles CIS alineados a los pilares de Zero Trust para fortalecer la ciberseguridad y garantizar una transición segura y eficiente al trabajo remoto frente al cambio en la forma de trabajar desde la pandemia del COVID-19.

- **DEFICIENCIA 4:** CARENCIA DE PROFESIONALES CAPACITADOS Y SENSIBILIZADOS FRENTE A ATAQUES CIBERNÉTICOS, ADEMÁS DE LA ALTA DEMANDA EN PUESTOS DE CIBERSEGURIDAD.

  Formulación del Subproblema 4:

  ¿De qué manera el análisis de los controles CIS alineados a los pilares de Zero Trust demostrará el efecto negativo resultante de la carencia de profesionales capacitados y sensibilizados frente a los ataques cibernéticos, sumado a la alta demanda en puestos de ciberseguridad?

  Objetivo Específico 4:

  Realizar un diagnóstico de la situación actual de profesionales capacitados y sensibilizados frente a ataques cibernéticos, así como de la demanda en puestos de ciberseguridad en empresas latinas, teniendo como punto de partida los resultados del análisis de los controles CIS alineados a los pilares de Zero Trust.

- **DEFICIENCIA 5:** FALTA DE COMPROMISO POR PARTE DE ENTIDADES GUBERNAMENTALES Y PRIVADAS PARA ESTABLECER LÍNEAS BASE DE ESTRATEGIAS DE CIBERSEGURIDAD DENTRO DE LOS PAÍSES DE LATINOAMÉRICA.

  Formulación del Subproblema 5:

  ¿Cómo el análisis de los controles CIS alineados a los pilares de Zero Trust fomentará el compromiso por parte de entidades gubernamentales y privadas para establecer líneas base de estrategias de ciberseguridad en países de Latinoamérica?

  Objetivo Específico 5:

  Evaluar el nivel de compromiso de entidades gubernamentales y privadas en países de Latinoamérica respecto a la ciberseguridad, para proponer recomendaciones y acciones específicas que impulsen la colaboración entre estos actores y se fomente la implementación del análisis de los controles CIS alineados a los pilares de Zero2 Trust.

ANEXO B

ENCUESTA DE ENTENDIMIENTO INICIAL:

1. ¿Cómo están organizados sus equipos de Seguridad e Infraestructura?
    a. Gestión Centralizada
    b. Servicios Compartidos
    c. Multinacional
    d. Gestión Descentralizada

2. ¿Cuánto ha progresado su transformación digital?
    a. Menos del 25%
    b. Entre el 25% al 50%
    c. Entre el 50% al 75%
    d. Más del 75%

3. ¿Cuán sensibles son sus datos?
    a. Información de Identificación Personal (PII)
    b. Propiedad Intelectual (IP)
    c. Información Financiera
    d. Información de Salud

4. ¿A qué sector pertenece?
    a. Comunicación
    b. Bienes y Consumo
    c. Educación
    d. Energía
    e. Entretenimiento
    f. Financiero
    g. Salud
    h. Hostelería
    i. Industrial
    j. Medios
    k. Farmacéutico
    l. Público
    m. Investigación y Desarrollo
    n. Retail
    o. Servicios
    p. Tecnológico
    q. Transporte

ANEXO C

CUESTIONARIO DEL TALLER DE EVALUACIÓN DE MADUREZ DE ZERO TRUST:

Identidad:

ID-1. ¿Los usuarios cuentan con una única identidad para acceder a sus aplicaciones?

a. Básico
b. Tradicional
c. Avanzado
d. Optimizado

ID-2. ¿Cuenta con una gestión de identidades centralizada que incluya usuarios y recursos empresariales (Dispositivos y aplicaciones)?

a. Básico
b. Tradicional
c. Avanzado
d. Optimizado

Dispositivos:

DI-1. ¿Cuenta con una gestión unificada para sus dispositivos Pcs y móviles?

a. Básico
b. Tradicional
c. Avanzado
d. Optimizado

DI-2. ¿Se cuenta con un proceso para monitorear la configuración segura en sus dispositivos?

a. Básico
b. Tradicional
c. Avanzado
d. Optimizado

Aplicaciones:

AP-1. ¿Se monitorea periódicamente el software ejecutado para garantizar seguridad y cumplimiento?

a. Básico
b. Tradicional
c. Avanzado
d. Optimizado

AP-2. ¿Cuenta con controles de acceso basado en roles para sus aplicaciones?

a. Básico

b. Tradicional
c. Avanzado
d. Optimizado

Redes:

RE-1. ¿Se aplica filtrado según reglas de negocio al tráfico entre segmentos de red?
a. Básico
b. Tradicional
c. Avanzado
d. Optimizado

RE-2. ¿Se cuenta con controles para que el tráfico de la red sea seguro? (SSH, HTTPS)
a. Básico
b. Tradicional
c. Avanzado
d. Optimizado

Infraestructura:

IN-1. ¿Se controla el otorgamiento de privilegios administrativos exclusivamente a cuentas administrativas?
a. Básico
b. Tradicional
c. Avanzado
d. Optimizado

IN-2. ¿Se aplican políticas centralizadas para verificar la identidad, autorizar accesos determinados y registrar las actividades?
a. Básico
b. Tradicional
c. Avanzado
d. Optimizado

Datos:

DA-1. ¿Cuenta con un proceso para determinar la sensibilidad de sus datos?

a. Básico
b. Tradicional
c. Avanzado
d. Optimizado

DA-2. ¿Aplica cifrado a los datos sensibles en tránsito?

a. Básico
b. Tradicional
c. Avanzado
d. Optimizado