UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

INSTITUTO DE POSTGRADO

TÍTULO

CONECTANDO MODELOS DE MADUREZ EN CIBERSEGURIDAD CON HACKING ÉTICO Y ANÁLISIS DE VULNERABILIDADES PARA MEDIR DE FORMA MÁS PRECISA EL NIVEL DE PREPARACIÓN DE UNA ORGANIZACIÓN FRENTE A CIBERATAQUES

AUTOR

Mora Filian, Elmer Javier

TRABAJO DE TITULACIÓN

Previo a la obtención del grado académico en
MAGÍSTER EN CIBERSEGURIDAD

TUTORA

Álvarez Galarza, María Daniela

Santa Elena, Ecuador

Año 2025

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TRIBUNAL DE SUSTENTACIÓN

Firmado electrónicamente por:
ALICIA GERMANIA ANDRADE VERA
Validar únicamente con FirmaEC

Ing. Alicia Andrade Vera, Mgtr.
COORDINADORA DEL PROGRAMA

Firmado electrónicamente por:
MARIA DANIELA ALVAREZ GALARZA
Validar únicamente con FirmaEC

Ing. María Álvarez Galarza, Mgtr.
TUTORA

Firmado electrónicamente por:
JAIME BENJAMIN OROZCO IGUASNIA
Validar únicamente con FirmaEC

Ing. Jaime Orozco Iguasnia, Mgtr.
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
DANIEL IVAN QUIRUMBAY YAGUAL
Validar únicamente con FirmaEC

Lic. Daniel Quirumbay Yagual, Mgtr.
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
MARIA MARGARITA RIVERA GONZALEZ
Validar únicamente con FirmaEC

Abg. María Rivera González, Mgtr.
SECRETARIA GENERAL
UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por Elmer Javier Mora Filian, como requerimiento para la obtención del título de Magíster en Ciberseguridad.

TUTORA

Firmado electrónicamente por:
MARIA DANIELA ALVAREZ GALARZA
Validar únicamente con FirmaEC

Ing. María Daniela Álvarez Galarza, Mgtr.

Santa Elena, 16 de octubre de 2025

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO
DECLARACIÓN DE RESPONSABILIDAD

Yo, Elmer Javier Mora Filian

DECLARO QUE:

El trabajo de Titulación, Conectando modelos de madurez en ciberseguridad con hacking ético y análisis de vulnerabilidades para medir de forma más precisa el nivel de preparación de una organización frente a ciberataques, previo a la obtención del título en Magíster en Ciberseguridad, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Santa Elena, 16 de octubre de 2025

EL AUTOR

Firmado electrónicamente por:
ELMER JAVIER MORA FILIAN
Validar únicamente con FirmaEC

Elmer Javier Mora Filian

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado CONECTANDO MODELOS DE MADUREZ EN CIBERSEGURIDAD CON HACKING ÉTICO Y ANÁLISIS DE VULNERABILIDADES PARA MEDIR DE FORMA MÁS PRECISA EL NIVEL DE PREPARACIÓN DE UNA ORGANIZACIÓN FRENTE A CIBERATAQUES., presentado por el estudiante, Elmer Javier Mora Filian fue enviado al Sistema Antiplagio COMPILATIO, presentando un porcentaje de similitud correspondiente al 3%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.


CERTIFICADO DE ANÁLISIS
magister

Tesis Modelos de Madurez-Javier Mora

3% Textos sospechosos

1% Similitudes
0 % similitudes entre comillas
< 1 % entre las fuentes mencionadas
2% Idiomas no reconocidos
40% Textos potencialmente generados por la IA (ignorado)

Nombre del documento: Tesis Modelos de Madurez-Javier Mora.pdf
ID del documento: 467727b84805e86993373d6a0dce0f2292c94e13
Tamaño del documento original: 1,33 MB

Depositante: MARÍA DANIELA ÁLVAREZ GALARZA
Fecha de depósito: 16/10/2025
Tipo de carga: interface
fecha de fin de análisis: 16/10/2025

Número de palabras: 27.226
Número de caracteres: 218.592

TUTORA

Firmado electrónicamente por:
MARIA DANIELA ALVAREZ GALARZA
Validar únicamente con FirmaEC

Ing. María Daniela Álvarez Galarza, Mgtr.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

AUTORIZACIÓN

Yo, **Elmer Javier Mora Filian**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de esta propuesta metodológica y tecnológica avanzada con fines de difusión pública, además apruebo la reproducción de esta propuesta metodológica y tecnológica avanzada dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, 16 de octubre de 2025

EL AUTOR

Firmado electrónicamente por:
ELMER JAVIER MORA FILIAN
Validar únicamente con FirmaEC

Elmer Javier Mora Filian

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

GLOSARIO DE TÉRMINOS

TÉRMINO	DEFINICIÓN
Alfa de Cronbach	Coeficiente estadístico que mide la consistencia interna de un cuestionario o instrumento. En el MHMC-EG se usa para validar la fiabilidad de la herramienta de evaluación.
Análisis de vulnerabilidades	Proceso que identifica, clasifica y prioriza debilidades técnicas en sistemas, redes o aplicaciones que pueden ser explotadas. Forma parte de la dimensión técnica del MHMC-EG.
AppLocker	Herramienta de seguridad de Windows que permite crear listas blancas de aplicaciones, evitando la ejecución no autorizada de software.
ATT&CK (MITRE ATT&CK Framework)	Base de conocimiento global sobre tácticas y técnicas utilizadas por atacantes. En el MHMC-EG se emplea para mapear vulnerabilidades con escenarios reales de ataque.
Backup (Copia de seguridad)	Duplicado de información crítica que permite restaurar datos en caso de pérdida o incidente. Evaluado en el dominio de *Recuperación y Continuidad*.
Blue Team / Red Team	Equipos que evalúan la seguridad: el *Blue Team* defiende y el *Red Team* simula ataques para medir la eficacia de los controles.
C2M2 (Cybersecurity Capability Maturity Model)	Modelo de madurez de ciberseguridad con diez dominios, desarrollado por el Departamento de Energía de EE. UU. Influyó en la estructura del MHMC-EG.
CMMC (Cybersecurity Maturity Model Certification)	Modelo de certificación de madurez del Departamento de Defensa de EE. UU. que define niveles progresivos de ciberseguridad. Referencia central en el MHMC-EG.
Control de acceso	Mecanismos técnicos y administrativos que limitan el acceso a sistemas e información solo a usuarios autorizados.
CSET (Cybersecurity Evaluation Tool)	Herramienta gratuita de CISA (EE. UU.) que permite evaluar la ciberseguridad institucional usando marcos como NIST CSF y CMMC. Base de recolección de datos en el MHMC-EG.
EGSI (Esquema Gubernamental de Seguridad de la Información)	Norma ecuatoriana que define las políticas mínimas de seguridad en el sector público. El MHMC-EG se alinea con el EGSI v3.0 para diagnóstico y mejora.
Endpoint Detection and Response (EDR)	Tecnología que detecta y responde a amenazas en equipos terminales mediante monitoreo y aislamiento automático.
Firewall (Cortafuegos)	Sistema que regula el tráfico de red según políticas predefinidas de seguridad.
Gobernanza de la ciberseguridad	Conjunto de políticas, procesos y estructuras organizacionales que garantizan la gestión y control estratégico de la seguridad de la información.
Hardening (Endurecimiento)	Proceso de configuración segura que reduce la superficie de ataque de sistemas mediante eliminación de servicios innecesarios y aplicación de parches.
KPI / KRI	Indicadores clave de desempeño (KPI) y de riesgo (KRI) usados para medir la efectividad de los controles y procesos de seguridad.
Madurez cibernética	Grado de desarrollo alcanzado por una organización en la implementación efectiva de sus controles de ciberseguridad, expresado en cinco niveles (Inicial a Optimizado).
MFA (Autenticación Multifactor)	Método de autenticación que requiere más de un factor (algo que sabes, tienes o eres) para verificar la identidad del usuario.

MITRE	Organización estadounidense sin fines de lucro dedicada a la investigación en defensa y seguridad. Creadora del marco ATT&CK y del sistema CVE.
NIST CSF (Cybersecurity Framework)	Marco del Instituto Nacional de Estándares y Tecnología de EE. UU. que organiza la gestión del riesgo en cinco funciones: Identificar, Proteger, Detectar, Responder y Recuperar.
Phishing	Técnica de engaño mediante correos o mensajes falsos que buscan obtener credenciales o información confidencial.
Plan de Continuidad Operativa (BCP)	Conjunto de acciones que aseguran la restauración de servicios críticos tras incidentes o desastres.
Plan de Respuesta a Incidentes (PRI)	Documento que define los pasos a seguir ante un incidente de ciberseguridad. Parte del dominio *Respuesta a Incidentes*.
Rúbrica de evaluación híbrida	Sistema de puntuación del MHMC-EG que pondera tres variables: madurez documental (wMD=0,5), cobertura técnica (wTC=0,3) y capacidad de respuesta (wRR=0,2).
SIEM (Security Information and Event Management)	Plataforma que recopila, analiza y correlaciona eventos de seguridad en tiempo real, permitiendo detectar incidentes.
Threat Intelligence (Inteligencia de amenazas)	Actividad que analiza tendencias y comportamientos de ataques para anticipar ciberamenazas.
Vulnerabilidad	Debilidad en un sistema o proceso que puede ser explotada para afectar la confidencialidad, integridad o disponibilidad de la información.

RESUMEN

La propuesta investigativa, conforme al **Modelo Híbrido de Madurez Cibernética para Entidades Gubernamentales (MHMC-EG),** tiene un enfoque evaluativo orientado a fortalecer la madurez institucional en ciberseguridad y seguridad informática mediante la integración de normas y marcos de trabajo reconocidos internacionalmente. El modelo articula herramientas y metodologías como la **Herramienta de Evaluación de Ciberseguridad (Cybersecurity Evaluation Tool, CSET), el Modelo de Certificación de Madurez en Ciberseguridad (Cybersecurity Maturity Model Certification, CMMC)** y el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología **(NIST Cybersecurity Framework, NIST CSF)**, junto con las evidencias derivadas de la base de conocimiento MITRE ATT&CK. Este esquema integral permite medir la existencia y la efectividad práctica de los controles frente a amenazas reales, combinando la gestión normativa con la verificación técnica. La metodología del modelo se basa en una evaluación híbrida ponderada, asignando un 50% al cumplimiento documental, un 30% a la cobertura técnica y un 20% a la capacidad de respuesta operativa.

Los resultados obtenidos en el entorno simulado evidencian que la incorporación de herramientas como el escaneo de vulnerabilidades, las simulaciones de ataque y las validaciones basadas en MITRE ATT&CK ofrecen una valoración más precisa de la madurez cibernética institucional, reduciendo la brecha entre el cumplimiento teórico y la efectividad real de los controles. El MHMC-EG se presenta como un modelo replicable, adaptable y compatible con el Esquema Gubernamental de Seguridad de la Información (EGSI v3.0), aportando una herramienta metodológica práctica para las instituciones del sector ecuatoriano que buscan fortalecer su resiliencia digital y cumplir los lineamientos nacionales de ciberseguridad. Además, representa un aporte académico original que integra la gestión del riesgo, la evidencia técnica y la mejora continua dentro de un mismo marco de evaluación.

Palabras clave:
Ciberseguridad, madurez organizacional, modelo híbrido, MITRE ATT&CK, CMMC, NIST CSF, CSET, EGSI, sector público, resiliencia digital.

ABSTRACT

The research proposal,the Hybrid Cybersecurity Maturity Model for Governmental Entities The proposed research and work, based on the Hybrid Cyber Maturity Model for Government Entitie (MHMC-EG), adopts an evaluative approach aimed at strengthening institutional maturity in cybersecurity and information security through the integration of internationally recognized standards and frameworks. The model articulates tools and methodologies such as the Cybersecurity Evaluation Tool (CSET), the Cybersecurity Maturity Model Certification (CMMC), and the National Institute of Standards and Technology Cybersecurity Framework (NIST Cybersecurity Framework, NIST CSF), along with evidence derived from the MITRE ATT&CK knowledge base. This comprehensive framework allows measuring the existence and practical effectiveness of controls against real threats, combining regulatory management with technical verification. The model's methodology is based on a weighted hybrid assessment, assigning 50% to documentary compliance, 30% to technical coverage, and 20% to operational response capacity.

The results obtained in the simulated environment show that the incorporation of tools such as vulnerability scanning, attack simulations, and MITRE ATT&CK-based validations offer a more accurate assessment of institutional cyber maturity, narrowing the gap between theoretical compliance and the actual effectiveness of controls. The MHMC-EG is presented as a replicable, adaptable, and compatible model with the Government Information Security Framework (EGSI v3.0), providing a practical methodological tool for institutions in the Ecuadorian cybersecurity sector seeking to strengthen their digital resilience and comply with national cybersecurity guidelines. Furthermore, it represents an original academic contribution that integrates risk management, technical evidence, and continuous improvement within a single assessment framework..

Keywords:
Cybersecurity, maturity model, hybrid framework, MITRE ATT&CK, CMMC, NIST CSF, CSET, EGSI, public sector, digital resilience.

INTRODUCCIÓN

En el escenario digital contemporáneo, la ciberseguridad se ha consolidado como un pilar estratégico en la sostenibilidad operativa de las organizaciones, trascendiendo su antigua concepción como un asunto meramente técnico. La expansión de las amenazas informáticas, la creciente sofisticación de los ciberataques y la interconexión global de los servicios públicos y privados han expuesto con claridad la vulnerabilidad de los sistemas digitales y la urgente necesidad de fortalecer su protección. Lo que antes se consideraba un ámbito reservado a especialistas en redes y sistemas, hoy constituye una dimensión transversal que compromete la gestión institucional, la confianza ciudadana y la estabilidad económica de las naciones. (MINTEL, 2022; PATIÑO OROZCO, 2019)

La digitalización acelerada de los últimos años ha transformado profundamente la manera en que se conciben los riesgos organizacionales. La protección de los activos de información no depende únicamente de herramientas tecnológicas, sino de la articulación entre gobernanza, procesos, cultura institucional y responsabilidad compartida respecto a los datos críticos. (estudiapuntes, 2025; MELO, 2024). Aun así, el panorama global revela brechas estructurales: los ataques de ransomware y phishing continúan en aumento, la inteligencia artificial se usa con fines ofensivos y las capacidades técnicas entre regiones permanecen desiguales. En América Latina, los gobiernos locales enfrentan mayores desafíos debido a la escasez de talento especializado y las limitaciones presupuestarias, lo que compromete la continuidad operativa y el cumplimiento normativo (PATIÑO OROZCO, 2019; CROWDSTRIKE, 2025; FORTINET, 2025; Maldonado, 2021).

En este contexto, los **modelos de madurez en ciberseguridad** emergen como herramientas metodológicas que permiten evaluar de manera progresiva el grado de preparación de una organización frente a incidentes cibernéticos y amenazas internas y externas. Estos modelos no solo miden el cumplimiento de controles o políticas, sino también el nivel de integración, optimización y mejora continua de los procesos de seguridad. En particular, **el CSET (Cybersecurity Evaluation Tool)** desarrollado por la *Cybersecurity and Infrastructure Security Agency (CISA)*, **el CMMC (Cybersecurity Maturity Model Certification)** impulsado por el *Departamento de Defensa de los Estados Unidos*, y **el NIST Cybersecurity Framework (CSF)** constituyen tres referentes esenciales para establecer estructuras comparables y escalables de madurez institucional.

A pesar de los avances logrados en materia de regulación y normalización, el análisis crítico de la práctica institucional y académica revela una brecha considerable entre el cumplimiento normativo y la eficacia técnica en la protección de los sistemas de información. Cumplir con los requisitos de un marco internacional o alcanzar una certificación no equivale necesariamente a contar con una postura sólida frente a amenazas sofisticadas ni con una capacidad real de mitigación de riesgos. Esta desconexión se origina, en gran medida, porque los modelos tradicionales se centran en el cumplimiento documental —políticas, procedimientos, controles formales—, dejando en segundo plano la verificación técnica basada en pruebas prácticas, ejercicios de simulación o escenarios de ataque controlado que reflejan de manera más realista la exposición de los activos de información. En consecuencia, se hace cada vez más evidente la necesidad de complementar la evaluación normativa con metodologías empíricas, tales como el hacking ético, el análisis de vulnerabilidades y la simulación de incidentes cibernéticos, que permitan obtener una visión objetiva y verificable del nivel de preparación institucional.

Desde esta perspectiva, el hacking ético no debe entenderse como una intromisión controlada, sino como una práctica científica y estructurada que reproduce con rigor las tácticas y procedimientos utilizados por adversarios reales. Su aplicación sistemática, mediante metodologías reconocidas a nivel internacional, permite identificar debilidades técnicas, humanas y organizacionales, al tiempo que evalúa la efectividad de las respuestas ante situaciones críticas. Paralelamente, los análisis de vulnerabilidades ofrecen una radiografía precisa del entorno tecnológico, priorizando los riesgos según su impacto y facilitando una gestión proactiva de los recursos de seguridad. Ambos enfoques comparten una premisa central: aquello que no se prueba, no se mide y no se somete a condiciones reales de verificación tiende a generar una falsa sensación de protección, exponiendo a las organizaciones a fallos estructurales cuando los controles no cumplen su función. El marco MITRE ATT&CK permite estructurar estas prácticas al mapear las tácticas y técnicas de adversarios reales, aportando una visión conductual que complementa los modelos de madurez organizacional.

Bajo esta comprensión, se configura el problema científico que da origen a la presente investigación: la falta de integración entre los modelos de madurez sustentados en el cumplimiento normativo y la evidencia empírica derivada de pruebas técnicas. Esta desconexión produce diagnósticos incompletos, subjetivos y de difícil replicabilidad, los cuales pueden certificar una supuesta “confiabilidad

documental" sin demostrar la verdadera resiliencia tecnológica ante ataques dirigidos. Así, mientras una aproximación exclusivamente normativa enfatiza el cumplimiento formal, una visión únicamente técnica suele generar intervenciones aisladas, sin conexión con la estrategia organizacional, la cultura institucional o los objetivos de largo plazo.

En respuesta a esta problemática, la hipótesis central sostiene que la combinación de los modelos **CSET, CMMC y CSF,** articulados con el marco **MITRE ATT&CK** y la integración de evidencias técnicas obtenidas mediante prácticas de hacking ético, análisis de vulnerabilidades y simulaciones controladas, permite evaluar con mayor precisión, objetividad y consistencia el nivel real de preparación de una organización frente a ciberataques. Este enfoque híbrido, que conjuga los ámbitos formales y técnicos, busca desarrollar indicadores sintéticos de madurez cibernética, capaces de reflejar la evolución institucional a lo largo del tiempo y de facilitar la comparación entre distintas entidades del mismo sector, con el propósito de fortalecer la gestión pública y la confianza digital.

La justificación de este trabajo es multidimensional: desde una perspectiva científica, la propuesta robustece la literatura en modelos de madurez adaptados a contextos latinoamericanos, aportando una visión crítica y superadora de las dicotomías tradicionales entre evaluación formal y evidencia técnica. (Rea Guamán y otros) Institucionalmente, responde a la exigencia del sector público ecuatoriano de alinearse con la Estrategia Nacional de Ciberseguridad, que exige tanto el cumplimiento normativo como la mejora efectiva de la resiliencia operacional y la reducción de la superficie de ataque. (MINTEL, 2022) La relevancia metodológica reside en la posibilidad de establecer un procedimiento sistemático y repetible para la operacionalización de variables en evaluaciones de seguridad, articulando dimensiones de madurez con métricas técnicas, de modo que los resultados generen valor tanto para la alta dirección como para los responsables de los equipos técnicos y de cumplimiento (INCIBE, 2020; (UNAD), 2024). Finalmente, desde el punto de vista práctico, el modelo híbrido ofrece a los gestores públicos y privados una herramienta aplicable a su realidad, capaz de generar diagnósticos fieles, planos de acción ajustados, y de incentivar una cultura de mejora continua, más allá de la obtención de certificaciones o "checklists" regulatorios. (Maldonado, 2021; INCIBE, 2020)

Conviene precisar que el modelo híbrido aquí propuesto se plantea como una guía teórica y metodológica. En esta fase, el trabajo se limita a la formulación y documentación del modelo, sin una

aplicación inmediata en una entidad pública ecuatoriana específica. El objetivo es que este documento sirva de base teórica y metodológica para futuras implementaciones, donde el modelo podrá aplicarse en entornos reales y específicos. De este modo, la propuesta aquí desarrollada se concibe como un marco de referencia que, en etapas posteriores, podrá ser adaptado y validado en el contexto del GAD de Baba o en otras organizaciones similares.

El desarrollo metódico de este trabajo incluirá, además de la construcción conceptual del modelo híbrido y su aplicación práctica, la elaboración de una matriz de operacionalización de variables y la definición de instrumentos de evaluación (cuestionarios, guías de entrevistas, plantillas de scoring), que permitan a los futuros investigadores y profesionales adaptar la metodología propuesta a sus propios entornos institucionales. Tales recursos metodológicos se adjuntan en los anexos, abundando en ejemplos, escalas de valoración y recomendaciones para el diseño de evaluaciones cruzadas entre modelos de madurez y resultados técnicos.

1. Planteamiento del problema

pesar del avance notable en la conceptualización y aplicación de los modelos de madurez en ciberseguridad, la mayoría de las organizaciones continúa enfrentando dificultades estructurales y operativas para medir de manera precisa y útil su nivel de preparación frente a ciberataques. Modelos como la **Herramienta de Evaluación de Ciberseguridad (Cybersecurity Evaluation Tool, CSET)** desarrollada por la **Agencia de Seguridad de Infraestructura y Ciberseguridad (Cybersecurity and Infrastructure Security Agency, CISA)**; la **Certificación de Madurez en Ciberseguridad (Cybersecurity Maturity Model Certification, CMMC)** del **Departamento de Defensa de los Estados Unidos (Department of Defense, DoD)**; y el **Marco de Ciberseguridad (Cybersecurity Framework, CSF)** del **Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, NIST)**, proporcionan esquemas estructurados para la evaluación de controles y la gestión del riesgo. Sin embargo, en la práctica, su aplicación tiende a centrarse principalmente en el **cumplimiento documental** de políticas, estándares y procedimientos, relegando la **verificación técnica de los controles** o la consideración de los **comportamientos reales de los adversarios**.

En contraste, las metodologías empíricas como el hacking ético y el análisis de vulnerabilidades ofrecen una visión práctica y actualizada del estado de la seguridad, al poner a prueba los sistemas bajo condiciones comparables a las de un ataque real. No obstante, estas evidencias técnicas rara vez se integran metodológicamente dentro de los modelos de madurez, lo que genera evaluaciones parciales y desconectadas de la realidad operativa. Esta separación entre la visión normativa y la evidencia empírica produce interpretaciones incompletas y un "falso sentido de seguridad" institucional, especialmente cuando los resultados de auditorías formales no reflejan la exposición real ante amenazas avanzadas.

La carencia de métodos estandarizados para articular modelos de madurez con marcos técnicos de comportamiento adversario —como el **MITRE ATT&CK,** que clasifica tácticas, técnicas y procedimientos utilizados por atacantes reales— ha limitado la capacidad de las organizaciones para obtener métricas observables, objetivas y replicables de su resiliencia cibernética. Esta falta de integración impide priorizar inversiones de manera estratégica, monitorear avances de madurez con base en datos verificables y transferir conocimiento entre sectores que enfrentan amenazas comunes. En consecuencia, surge la necesidad de desarrollar un modelo híbrido que combine la estructura formal de los marcos de madurez con la evidencia técnica y comportamental derivada de metodologías empíricas, con el fin de alcanzar evaluaciones más completas, reproducibles y útiles para la toma de decisiones institucionales.

2. Justificación

Desde el punto de vista científico, esta tesis busca superar el reduccionismo que ha caracterizado las evaluaciones tradicionales de ciberseguridad, integrando dos paradigmas históricamente separados: el **enfoque normativo de los modelos de madurez** y el **enfoque técnico-empírico de la validación práctica**. El desarrollo de un **modelo híbrido de madurez**, fundamentado en la integración de los modelos **CSET**, **CMMC** y **CSF** con el marco **MITRE ATT&CK**, responde a la necesidad de disponer de instrumentos diagnósticos más completos, verificables y alineados con la realidad operativa de las organizaciones contemporáneas. Este modelo no solo pretende medir el grado de cumplimiento de controles, sino también evaluar la capacidad efectiva de detección, respuesta y aprendizaje ante tácticas y técnicas adversarias.

En el plano institucional, la propuesta se enmarca en un momento de consolidación de las políticas nacionales de ciberseguridad, evidenciado por la implementación de la **Estrategia Nacional de Ciberseguridad 2022–2025** (MINTEL, 2022)**.**Sin embargo, persiste una brecha significativa entre la formulación de políticas y la reducción tangible de riesgos técnicos dentro de las entidades públicas. En este contexto, la investigación aporta una metodología **transferible y replicable**, que permite fundamentar las decisiones de inversión en ciberseguridad con base en indicadores cuantitativos y cualitativos derivados de una evaluación empírica de la madurez. Así, la propuesta contribuye a fortalecer la capacidad institucional del sector público para priorizar recursos y mejorar su postura de defensa digital frente a un entorno de amenazas en constante evolución.

Desde una perspectiva metodológica, la operacionalización de variables híbridas —que combinan métricas normativas y resultados técnicos— permitirá a los equipos de auditoría, cumplimiento y seguridad aplicar protocolos homogéneos y transparentes, favoreciendo la trazabilidad de los resultados y la comunicación con los niveles directivos. Además, el modelo facilitará la comparación transversal de niveles de madurez entre entidades con características similares, aportando un marco común de referencia para la gestión del riesgo digital.

Finalmente, el aporte práctico de esta investigación radica en su capacidad para generar informes de diagnóstico accionables, establecer rutas de madurez progresiva y promover una cultura de mejora continua orientada a la resiliencia cibernética. Al articular modelos de madurez consolidados con marcos de análisis de comportamiento adversario, esta tesis propone un modelo aplicable y adaptable que contribuye al fortalecimiento de la ciberseguridad en organizaciones públicas y privadas del contexto latinoamericano.

3 Formulación del problema de investigación

Tomando en cuenta los anteriores razonamientos, la pregunta central que orienta esta tesis es la siguiente:

¿En qué medida la integración de modelos de madurez consolidados —como el CSET, el CMMC y el CSF— con el marco de comportamiento adversario MITRE ATT&CK permite diseñar un modelo híbrido capaz de medir de forma más objetiva, precisa y replicable el nivel de preparación de una organización frente a ciberataques, en comparación con las aproximaciones convencionales basadas únicamente en el cumplimiento normativo?

Esta formulación refleja el núcleo del problema: la falta de un mecanismo integrador que articule los dominios de los modelos de madurez con la evidencia técnica y táctica de los comportamientos de ataque. La investigación, por tanto, busca desarrollar un modelo metodológico que permita superar las limitaciones de las evaluaciones formales, generando una visión unificada del estado de madurez cibernética institucional.

4. Objetivo general

Desarrollar y validar un **modelo híbrido de evaluación de la madurez en ciberseguridad**, que articule los componentes estructurales de los modelos **CSET**, **CMMC** y **CSF** con las tácticas, técnicas y procedimientos definidos por el marco **MITRE ATT&CK**, con el fin de medir de forma más objetiva y replicable el nivel de preparación de las organizaciones frente a ciberataques, fortaleciendo así su resiliencia operativa y su capacidad de respuesta ante amenazas reales.

4.1 Objetivos específicos

- Analizar comparativamente los modelos de madurez CSET, CMMC y CSF, identificando sus principios, dominios, niveles y métricas más relevantes para la medición del grado de madurez en ciberseguridad organizacional.
- Examinar el marco MITRE ATT&CK como herramienta de comprensión y clasificación del comportamiento adversario, determinando su aplicabilidad como complemento técnico en la evaluación de madurez.
- Diseñar un modelo híbrido de madurez, integrando los dominios de los modelos CSET, CMMC y CSF con las categorías tácticas del MITRE ATT&CK, mediante la definición de ponderaciones, relaciones y escalas de valoración estandarizadas.
- Validar el modelo híbrido propuesto a través de una aplicación controlada en un entorno institucional simulado, verificando su capacidad para generar indicadores objetivos y reproducibles del nivel de preparación frente a amenazas cibernéticas.
- Formular lineamientos y recomendaciones para la adopción del modelo híbrido en organizaciones públicas y privadas, promoviendo una cultura de mejora continua basada en la integración entre gestión normativa y evaluación técnica.

5. Planteamiento hipotético: Preguntas científicas

- ¿Hasta qué punto el uso de indicadores híbridos (normativos y técnicos) impacta positivamente en la objetividad y replicabilidad de las evaluaciones de madurez en ciberseguridad aplicadas a organizaciones públicas ecuatorianas?
- ¿Qué relación existe entre la cobertura documental de controles normativos y la evidencia práctica de fallos técnicos identificados mediante ejercicios de hacking ético y análisis de vulnerabilidades?
- ¿Cuáles son los factores facilitadores e inhibidores para la implementación de modelos híbridos de evaluación de la madurez cibernética en el contexto institucional ecuatoriano?
- ¿En qué grado los informes sustentados en evidencias técnicas promueven una mejora más sostenida de la resiliencia organizacional frente a los riesgos cibernéticos, en comparación con los informes centrados únicamente en el cumplimiento?
- ¿Cómo varían los resultados y la percepción de la alta dirección, los responsables de TI y los equipos de cumplimiento en función de la metodología de evaluación aplicada (normativa, técnica, híbrida)?
- ¿Cuáles son los retos operativos, éticos y organizacionales ligados a la adopción de modelos híbridos y qué recomendaciones emergen para su replicabilidad sectorial y escalabilidad nacional?

CAPÍTULO I

1. MARCO TEÓRICO REFERENCIAL

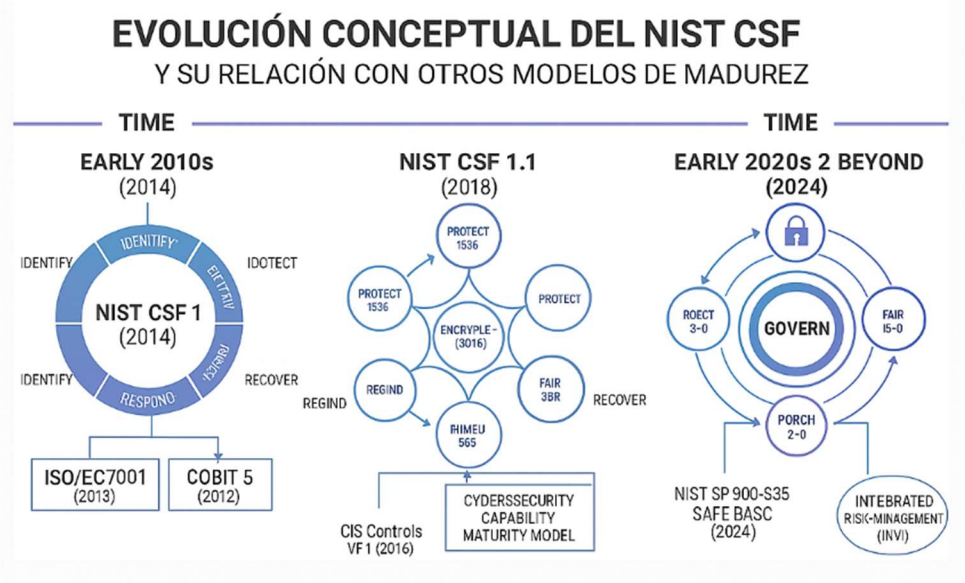
1.1. Revisión de literatura

1.2.1 Modelos de Madurez en Ciberseguridad

En el ámbito de la ciberseguridad, los modelos de madurez constituyen herramientas metodológicas diseñadas para evaluar la capacidad de una organización de proteger, detectar, responder y recuperarse ante incidentes digitales. Estos modelos, derivados del concepto de **Capability Maturity Model (CMM)**, proporcionan una estructura progresiva que permite medir el grado de avance en la implementación de controles, políticas y procesos de seguridad, identificando brechas y priorizando la mejora continua. (Marc Levesque, 2020). Un mayor nivel de madurez implica que la gestión de la seguridad se encuentra integrada en la cultura organizacional, respaldada por procesos documentados, roles definidos y decisiones basadas en datos verificables.

Ejemplos de modelos de madurez ampliamente adoptados incluyen el **NIST Cybersecurity Framework (CSF)**, desarrollado inicialmente en 2014 por el *National Institute of Standards and Technology (NIST)*. Este marco provee un lenguaje común y una metodología sistemática para gestionar el riesgo digital en organizaciones de todos los sectores. Aunque el NIST CSF no define niveles de madurez explícitos, introduce los *tiers* de implementación —**Parcial, Riesgo Informado, Repetible y Adaptativo**— que permiten evaluar el progreso desde un enfoque reactivo hasta una postura proactiva y optimizada de la seguridad (NIST, 2023). La **versión 2.0 del CSF**, publicada en 2024, amplía su alcance a todo tipo de organizaciones y agrega la función **Govern (Gobernar)**, que refuerza la importancia de la gobernanza y la rendición de cuentas en el nivel directivo. Este marco constituye una base fundamental para la articulación con otros modelos de madurez como **CSET** y **CMMC**, y con marcos técnicos como **MITRE ATT&CK**, que aportan la dimensión táctica de los comportamientos adversarios.

Figura 1. línea de tiempo de la evolución de modelos de madurez



Fuente: Autor, 2025

Diversos marcos internacionales han adoptado el enfoque de madurez como mecanismo para evaluar y mejorar la gestión de la ciberseguridad. Entre ellos, el NIST Cybersecurity Framework (CSF) se destaca por ofrecer un conjunto estructurado de resultados de seguridad que pueden adaptarse a organizaciones de cualquier tamaño o sector. Aunque el CSF no define niveles de madurez formales, introduce el concepto de tiers de implementación, que representan grados progresivos de gestión del riesgo, desde un enfoque parcial y reactivo hasta uno adaptativo y optimizado (NIST.GOV, 2022).

Este principio de evolución progresiva ha inspirado otros modelos de madurez, como el CSET (Cybersecurity Evaluation Tool) y el CMMC (Cybersecurity Maturity Model Certification), orientados a evaluar la preparación técnica e institucional mediante indicadores medibles. En conjunto, estos modelos aportan una visión integral para fortalecer la resiliencia cibernética de las organizaciones contemporáneas.

En esta línea, el **MITRE ATT&CK Framework** aporta una dimensión complementaria centrada en el **comportamiento de los adversarios**, proporcionando un conocimiento empírico sobre las tácticas, técnicas y procedimientos (TTPs) empleados en ataques reales. Su integración con los modelos de

madurez permite evaluar no solo la existencia de controles, sino también su eficacia frente a escenarios de ataque concretos, fortaleciendo así la perspectiva técnica y práctica de la evaluación.

En síntesis, la madurez en ciberseguridad se concibe como la capacidad institucional para gestionar la seguridad de manera **proactiva, medible y en mejora continua**. Alcanzar niveles elevados de madurez implica institucionalizar procesos, establecer métricas verificables y fomentar una cultura de seguridad transversal. Diversos estudios y marcos contemporáneos (NIST.GOV, 2022; DODCIO, s.f.; CISA, s.f.; ATTACK.MITRE, s.f.), coinciden en que una organización madura no solo implementa controles, sino que aprende, adapta y optimiza sus defensas frente a la evolución constante de las amenazas cibernéticas.

1.2.2 Gestión del Riesgo Digital

Constituye un componente esencial dentro de los modelos de madurez en ciberseguridad, al proporcionar la base estratégica para priorizar controles y optimizar la respuesta institucional frente a amenazas emergentes. En el contexto de la madurez cibernética, gestionar el riesgo implica no solo identificar vulnerabilidades y amenazas, sino también evaluar de manera estructurada la capacidad organizacional para anticipar, mitigar y recuperarse de incidentes, manteniendo la continuidad operativa dentro de niveles tolerables.

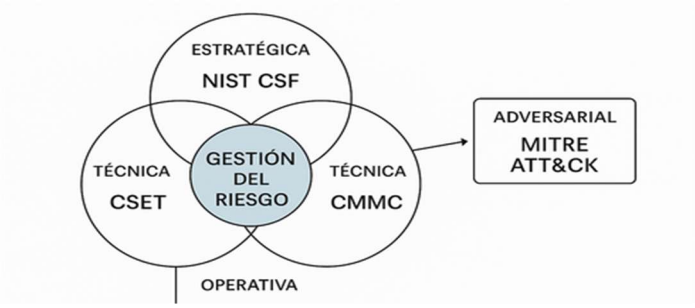
En el marco del **NIST Cybersecurity Framework (CSF)**, la gestión del riesgo es el eje articulador de las cinco funciones principales —Identificar, proteger, detectar y responder ("**Identify, Protect, Detect, Respond y Recover")**—, y se refuerza en su versión 2.0 con la incorporación de la función de Gobierno ("**Govern")**, orientada a integrar el riesgo en las decisiones estratégicas de negocio (NIST, 2024). Este enfoque promueve una visión dinámica y evolutiva del riesgo, vinculando directamente los resultados de las evaluaciones técnicas con la madurez institucional alcanzada.

De forma complementaria, el **CSET Herramienta de evaluación de ciberseguridad (Cybersecurity Evaluation Tool)** evalúa la madurez de la gestión del riesgo mediante cuestionarios estructurados que miden la existencia, implementación y eficacia de políticas, controles y procedimientos. Sus resultados permiten identificar brechas críticas y generar planes de acción priorizados según impacto y probabilidad.

Por su parte, el **CMMC Certificación del Modelo de Madurez en Ciberseguridad (Cybersecurity Maturity Model Certification)** incorpora la gestión del riesgo como un componente transversal de sus cinco niveles de madurez, evaluando tanto la documentación formal de políticas como la evidencia técnica de su aplicación. Este modelo traduce la gestión del riesgo en prácticas verificables que reflejan la capacidad real de la organización para prevenir, detectar y responder ante amenazas.

Finalmente, el **MITRE ATT&CK Framework** complementa la gestión del riesgo desde una perspectiva operacional, al proporcionar un repositorio empírico de tácticas, técnicas y procedimientos utilizados por adversarios reales. Su integración en los modelos de madurez permite vincular el riesgo teórico con escenarios prácticos de ataque, fortaleciendo la correlación entre vulnerabilidades, controles implementados y capacidad de defensa efectiva.

Figura 2. Integración de la gestión del riesgo digital en los modelos de madurez



Fuente: Autor, 2025

En conjunto, la gestión del riesgo digital en los modelos de madurez contemporáneos se concibe como un proceso **iterativo, medible y de mejora continua**, que no solo busca reducir la probabilidad e impacto de los incidentes, sino también incrementar la resiliencia organizacional mediante la retroalimentación constante entre la evaluación técnica y la gobernanza estratégica (NIST, 2024; CISA, s.f.; DODCIO, s.f.; ATTACK.MITRE, s.f.)

1.2.3 Mejora Continua

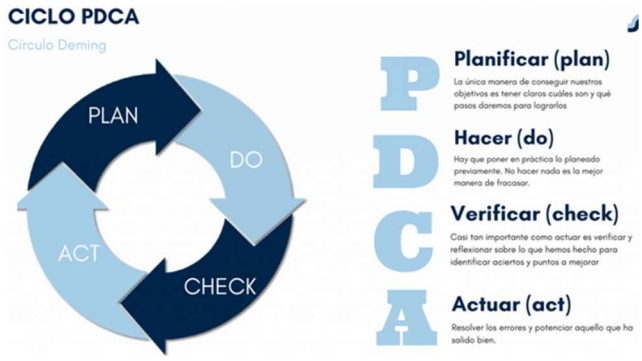
La mejora continua constituye un principio esencial dentro de los modelos de madurez en ciberseguridad, ya que garantiza que las organizaciones evolucionen de manera constante frente a la

dinámica cambiante de las amenazas digitales. No basta con implementar controles una sola vez; la sostenibilidad de la seguridad depende de establecer un ciclo iterativo de evaluación, aprendizaje y perfeccionamiento, en el que cada revisión fortalezca la capacidad de prevención, detección y respuesta ante incidentes.

En el marco del **NIST Cybersecurity Framework (CSF),** la mejora continua se materializa en las funciones de "Identify" y "Recover", que promueven la retroalimentación constante del programa de seguridad a partir de los incidentes gestionados, lecciones aprendidas y nuevas condiciones de riesgo. La versión 2.0 del CSF incorpora, además, la función de Gobierno (**"Govern"),** que refuerza la importancia de revisar y ajustar regularmente las estrategias de ciberseguridad en coherencia con los objetivos de negocio. (NIST, 2024)

De forma complementaria, el **CSET Herramienta de evaluación de ciberseguridad (Cybersecurity Evaluation Tool),** desarrollado por CISA, facilita la mejora continua mediante evaluaciones periódicas de madurez técnica y organizacional. Este enfoque permite a las instituciones monitorear sus avances, comparar resultados históricos y establecer planes de acción progresivos para cerrar brechas identificadas durante auditorías o pruebas de vulnerabilidad.

Figura 3.Ciclo PDCA aplicado a la seguridad de la información



Fuente: stocklogistic

En el **CMMC (Cybersecurity Maturity Model Certification**), la mejora continua se integra de manera estructural en sus cinco niveles de madurez. Cada nivel representa un estadio más avanzado de gestión, desde la aplicación inicial de prácticas básicas hasta la institucionalización de procesos de

mejora sistemática. Así, una organización madura no solo mantiene controles efectivos, sino que evalúa, documenta y refina su postura de seguridad de forma sostenida.

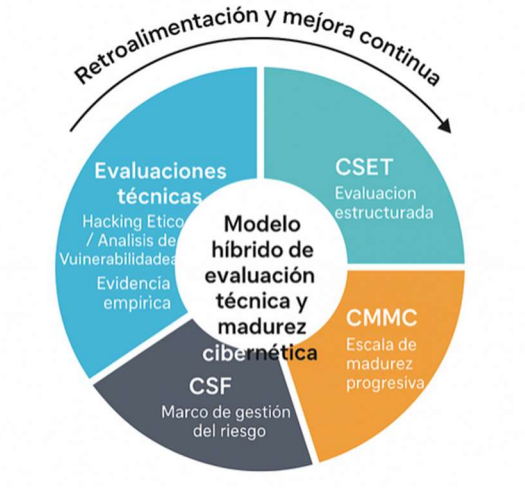
Finalmente, el **MITRE ATT&CK Framework** introduce una dimensión práctica de mejora continua al permitir que las organizaciones actualicen sus defensas conforme se documentan nuevas tácticas, técnicas y procedimientos (TTPs) de adversarios reales. De esta manera, la retroalimentación del entorno de amenazas se convierte en un insumo estratégico para fortalecer controles, ajustar políticas y priorizar inversiones.

En conjunto, los modelos de madurez **CSET, CMMC, CSF y MITRE ATT&CK** establecen un enfoque integral de mejora continua, donde la seguridad se concibe como un proceso vivo y adaptable. Este ciclo de evaluación constante asegura que las organizaciones mantengan su resiliencia, anticipen los cambios tecnológicos y operativos, y optimicen su capacidad de defensa frente a un ecosistema de ciberamenazas en permanente evolución (CISA, s.f.; DODCIO, s.f.; ATTACK.MITRE, s.f.)

1.2.4 Marco metodológico para evaluaciones técnicas: Hacking Ético y Análisis de Vulnerabilidades

La construcción de un marco metodológico robusto para la evaluación técnica en ciberseguridad es fundamental para medir y evolucionar la madurez organizacional frente a las amenazas actuales. En este contexto, el hacking ético y el análisis de vulnerabilidades representan dos pilares esenciales como fuentes de evidencia empírica. Ambos se integran en modelos híbridos de madurez adaptados a los marcos internacionales de referencia, tales como el **Cyber Security Evaluation Tool (CSET)**, el **Cybersecurity Maturity Model Certification (CMMC), el Cybersecurity Framework (CSF) del NIST**, y el mapeo de hallazgos mediante el **MITRE ATT&CK**. Esta integración no solo permite cuantificar técnicamente el riesgo y la postura de seguridad, sino también establecer un mecanismo de retroalimentación cíclica que refuerza la mejora continua y la trazabilidad ética de los procesos de evaluación.

Figura 4. Retroalimentación y mejora continua



Fuente: Autor, 2025 (basado en NIST, CISA, MITRE Y DoD)

El hacking ético se define como la práctica de evaluar activamente la seguridad de los sistemas informáticos y redes, mediante simulaciones controladas de ataques reales, con el consentimiento explícito de la organización y con el objetivo de prevenir incidentes de seguridad antes de que sean explotados por actores maliciosos (SOFTWARELAB, 2023; CAMPUSCIBERSEGURIDAD, s.f.; MALWAREBYTES, s.f.; NETPROVIDERS, 2025)A diferencia del hacking malicioso, implica un compromiso ético y legal, subrayado por principios de autorización, confidencialidad, no daño, responsabilidad, transparencia y cumplimiento normativo. (CAMPUSCIBERSEGURIDAD, s.f.; MALWAREBYTES, s.f.)

Las fases del hacking ético siguen una estructura metódica que maximiza la efectividad y minimiza el riesgo operativo.

- **Planificación:** Definición de objetivos, alcance y autorizaciones legales.
- **Reconocimiento ("Footprinting"):** Recopilación pasiva y activa de información sobre el objetivo.
- **Escaneo y enumeración:** Identificación de puertos, servicios, dispositivos y sistemas operativos.
- **Obtención de acceso:** Explotación de vulnerabilidades mediante técnicas avanzadas.
- **Mantenimiento del acceso:** Persistencia simulada en el sistema.

- **Eliminación de rastros:** Borrado y ocultamiento de pruebas para evaluar la eficacia de monitoreo.
- **Reporte:** Elaboración y comunicación de hallazgos, riesgos, metodologías utilizadas y recomendaciones.

Estas fases permiten abordar el ciclo completo de un ciberataque de forma controlada y documentada, resaltando la importancia de la trazabilidad y la justificación ética en cada una de las acciones,

1.2.4.1 Definición y características del análisis de vulnerabilidades

El **análisis de vulnerabilidades** es un proceso estructurado orientado a identificar, clasificar y priorizar debilidades técnicas en sistemas, aplicaciones, redes o procesos que pueden ser explotadas por amenazas para causar daño, interrumpir servicios o comprometer la confidencialidad, integridad y disponibilidad de los activos de información. Es una práctica crítica en la gestión del riesgo corporativo y la resiliencia operativa. (IBM, 2023; CAMPUSCIBERSEGURIDAD, s.f.; SOFTWARELAB, 2023; NETPROVIDERS, 2025; MCMTECHCO, 2025).

Sus características clave incluyen:

- **Evaluación proactiva y continua**: Incorpora chequeos regulares, tanto automatizados como manuales, durante todo el ciclo de vida tecnológico. (SOFTWARELAB, 2023)
- **Cobertura integral**: Se aplican escaneos sobre infraestructuras, aplicaciones, sistemas operativos, dispositivos IoT y políticas de seguridad.
- **Categorización y priorización**: Las vulnerabilidades se clasifican usando métricas como el Sistema de puntuación de vulnerabilidad común (“**Common Vulnerability Scoring System”) (CVSS)** y se atienden según su impacto y probabilidad de explotación. (MCMTECHCO, 2025)
- **Informe técnico**: La entrega de reportes ejecutivos y técnicos permite tanto acciones operativas como decisiones estratégicas.
- **Ciclo de remediación y verificación**: Tras la corrección se aplican retests y auditorías para validar el cierre de cada hallazgo.

- **Trazabilidad**: Cada vulnerabilidad, su origen, impacto y respuesta queda documentada para auditoría, aprendizaje y cumplimiento normativo.

Cabe destacar la diferencia entre el análisis de vulnerabilidades y el pentesting: mientras el primero identifica exhaustivamente debilidades conocidas, el segundo busca explotar selectivamente puntos críticos para medir el impacto real sanitario. (CAMPUSCIBERSEGURIDAD, s.f.; TUCONSULTORTI, s.f.)

1.2.4.2 Descripción del CSET como herramienta de evaluación técnica

El **Cyber Security Evaluation Tool (CSET)**, desarrollado por el Departamento de Seguridad Nacional de los Estados Unidos, es una herramienta de software diseñada para asistir a organizaciones en la autoevaluación de su postura de ciberseguridad frente a estándares reconocidos como NIST, ISO, NERC y CIS. (CISA, s.f.; CCN-CERT.CNI, s.f.)

CSET guía a los usuarios a través de un cuestionario adaptativo, basado en el marco normativo elegido y el nivel de seguridad objetivo. Los resultados producen:

- **Diagnóstico técnico exhaustivo**, alineado a controles internacionales.
- **Lista priorizada de recomendaciones de mejora**, con justificaciones claras.
- **Métricas objetivas y repetibles** para monitorear el progreso y comparar las evaluaciones a lo largo del tiempo.
- **Facilitación de la discusión interna sobre riesgos, cultura de ciberseguridad y mejoramiento continuo**.

El principal valor de CSET es su capacidad para objetivar, normalizar y documentar la evidencia técnica, constituyendo un insumo estructural para correlacionar la madurez medida con los modelos CMMC y CSF. (CCN-CERT.CNI, s.f.)

1.2.4.3 Modelo CMMC y sus niveles de madurez

El **Cybersecurity Maturity Model Certification (CMMC)** es un marco normativo de madurez diseñado para incrementar progresivamente la capacidad de gestión de la ciberseguridad en las

organizaciones, especialmente aquellas que manipulan información crítica en cadenas de suministro como la defensa estadounidense. (MICROSOFT, 2022; FLORES MIRANDA, 2024; DODCIO, s.f.; VISURESOLUTIONS, s.f.; CONTINUUMGRC, 2025; KEYSIGHT, 2024), **CMMC 2.0** simplifica el modelo a tres niveles, alineando cada uno con estándares específicos del NIST:

- **Nivel 1 – Fundacional (Foundational)**: Implementación de controles básicos de higiene cibernética para la protección de información contractual federal (FCI). Requiere autoevaluaciones anuales con 17 prácticas clave.
- **Nivel 2 – Avanzado (Advanced)**: Equivalente al cumplimiento total de los 110 controles de NIST SP 800-171 para proteger información controlada no clasificada (CUI), con evaluaciones periódicas realizadas por terceros.
- **Nivel 3 – Experto (Expert)**: Basado en NIST SP 800-172, enfocado en la mitigación ante amenazas avanzadas persistentes (APT), con controles adicionales y auditorías dirigidas por el gobierno federal.

Los **dominios del CMMC** abarcan aspectos como control de acceso, concienciación y formación, auditoría, gestión de la configuración, identificación, respuesta a incidentes, protección de la información y mejora continua. (VISURESOLUTIONS, s.f.) (DODCIO, s.f.)

1.2.4.4 Correlación de resultados técnicos con niveles de CMMC

La evidencia empírica generada por los ejercicios de hacking ético y análisis de vulnerabilidades alimenta de manera determinante la evaluación de la madurez según el CMMC (CONTINUUMGRC, 2025; TITANIA, s.f.; KEYSIGHT, 2024). Esta correlación se da en varios planos:

- **Hallazgos técnicos**: Cada vulnerabilidad o brecha identificada puede mapearse a controles específicos del CMMC. Por ejemplo, una falla en la gestión de contraseñas impacta el dominio de control de acceso (Access Control).
- **Gap Analysis**: Los resultados del CSET y los informes de pentesting son insumos clave para realizar análisis de brecha (gap analysis) entre el estado actual y el nivel de madurez objetivo (Carrasco & Rivera, 2023).

- **Priorización de remediación**: Los informes priorizan acciones correctivas alineadas a los requerimientos del nivel de madurez que la organización busca alcanzar.
- **Revalidación y mejora continua**: El proceso de remediación requiere reanálisis técnico para validar el cierre, generando nueva evidencia y retroalimentando la gestión de madurez.
- **Tracking y reporting**: La trazabilidad de los hallazgos, la documentación de la corrección y la actualización de políticas/processos contribuyen a la justificación y defensa en auditorías de certificación o cumplimiento.

De esta manera, la correlación entre los resultados técnicos y los niveles del CMMC es directa y funcional al objetivo de incrementar la resiliencia organizacional.

1.2.4.5 Uso del MITRE ATT&CK para mapear hallazgos técnicos

El **MITRE ATT&CK** es una base de conocimiento global sobre tácticas, técnicas y procedimientos adversarios (TTPs) observados en incidentes reales, que proporciona una taxonomía común para mapear y entender el ciclo de vida de los ataques. (ATTACK.MITRE, s.f.; TRENDMICRO, s.f.; CIBERSEGURIDAD, s.f.)

Su aplicación en el modelo metodológico incluye:

- **Clasificación de hallazgos**: Cada vulnerabilidad o brecha técnica identificada durante el hacking ético o el análisis de vulnerabilidades puede mapearse a una o varias técnicas de ATT&CK. Por ejemplo, una exposición a RDP en internet corresponde a la táctica de "Acceso Inicial" mediante "Explotación de Servicio Remoto".
- **Análisis de cobertura**: El mapeo permite visualizar la cobertura de controles existentes frente a las tácticas y técnicas adversarias más relevantes para la organización.
- **Priorización y remediación efectiva**: Al mapear los hallazgos a las matrices ATT&CK, es posible priorizar la corrección en función del riesgo real asociado a las TTPs más frecuentes o de mayor impacto en el sector.
- **Entrenamiento y concientización**: ATT&CK permite entrenar Red y Blue Teams en escenarios de simulación basados en amenazas reales, alineando pruebas técnicas con los riesgos más probables y las capacidades de defensa requeridas.

La integración de ATT&CK convierte los hallazgos empíricos en inteligencia de amenazas accionable, fortaleciendo la defensa proactiva y ajustando la estrategia organizacional a las técnicas empleadas por los adversarios vigentes. (TRENDMICRO, s.f.; ATTACK.MITRE, s.f.)

1.2.4.6 Modelo híbrido de madurez: Integrando CSET, CMMC y CSF

El enfoque metodológico propuesto es híbrido e integrador: utiliza herramientas y marcos complementarios para obtener una visión holística de la madurez en ciberseguridad:

- **CSET**: Genera evidencia técnica estructurada, normativizada y priorizada.
- **CMMC**: Proporciona una hoja de ruta progresiva para incrementar la madurez organizacional, integrando prácticas técnicas y procesos institucionales.
- **CSF del NIST**: Ofrece un marco flexible y ampliamente aceptado para gestionar riesgos, basado en funciones clave: Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar. (IBM, 2023; NIST.GOV, 2022; TSAPPS.NIST, 2024; DELTAPROTECT, 2025)

El modelo híbrido resulta en:

- **Un proceso iterativo y cíclico** en el cual los hallazgos técnicos alimentan el análisis de brecha, la planeación de mejoras y la validación de avances de madurez.
- **Una alineación entre los informes técnicos (CSET, pentesting) y las métricas de cumplimiento de modelos como CMMC y CSF.**
- Una base para integrar otras fuentes de inteligencia

En conclusión, el modelo híbrido propuesto articula las fortalezas de tres enfoques complementarios: la capacidad evaluativa del CSET, la progresión estructurada del CMMC y la flexibilidad del CSF, bajo una capa empírica proporcionada por las pruebas técnicas y el mapeo MITRE ATT&CK. Este marco permite medir la madurez de manera integral —combinando evidencia técnica y gestión estratégica—, ofreciendo un instrumento adaptable, verificable y alineado con las mejores prácticas internacionales en ciberseguridad (NIST, 2024; CISA, s.f.; ATTACK.MITRE, s.f.).

CAPÍTULO II

2. METODOLOGÍA

2.1 Contexto de la investigación

En el panorama actual de amenazas cibernéticas, las organizaciones públicas y privadas enfrentan ataques cada vez más sofisticados que explotan tanto vulnerabilidades técnicas como deficiencias en procesos y personas (PUBS.NARUC, 2020).. Esto ha llevado a un creciente interés en modelos de madurez de ciberseguridad que permitan evaluar y mejorar la **preparación institucional frente a ciberataques**. Un modelo de madurez de ciberseguridad proporciona un marco estructurado para identificar brechas en las capacidades de defensa y priorizar mejoras, lo que resulta esencial dado que la mera implementación de controles aislados no garantiza un nivel de seguridad adecuado (PUBS.NARUC, 2020). En este contexto, la investigación se orienta a construir un **modelo híbrido de evaluación de madurez cibernética** que combine fortalezas de múltiples marcos existentes con pruebas técnicas realistas, alineándose con la necesidad de una defensa proactiva y adaptativa.

Existen diversos **marcos de referencia y modelos de madurez** ampliamente aceptados. La Certificación del Modelo de Madurez en Ciberseguridad **("Cybersecurity Maturity Model Certification")** (CMMC), por ejemplo, es un modelo de madurez creado por el Departamento de Defensa de EE.UU. que define **tres niveles escalonados** de prácticas de seguridad para proteger información sensible gubernamental (FLEXENTIAL, 2025). CMMC 2.0 incorpora 15 controles básicos en el Nivel 1 (protección de información federal contractual básica), 110 controles en el Nivel 2 alineados con NIST SP 800-171 (protección de información CUI) y controles avanzados en el Nivel 3 derivados de NIST SP 800-172 para contrarrestar amenazas APT (DODCIO, s.f.). Estos controles se agrupan en dominios o familias que abarcan desde control de accesos y capacitación en seguridad, hasta protección física, gestión de configuraciones, respuesta a incidentes y evaluación de riesgos (ISIDEFENSE, 2024). Por su parte, el NIST Cybersecurity Framework (CSF) ofrece un enfoque voluntario y flexible, estructurado en **cinco funciones fundamentales** – Identificar, Proteger, Detectar, Responder y Recuperar – que describen en términos generales los pasos para lograr resiliencia cibernética (ISACA, 2024). El NIST CSF no impone controles específicos, sino que sirve como marco de alto nivel para gestionar el riesgo adaptándose a cualquier sector (ISACA, 2024). Otros modelos complementarios, como el Modelo de madurez de la capacidad de ciberseguridad

("Cybersecurity Capability Maturity Model") (C2M2) orientado a infraestructuras críticas, definen dominios detallados (10 dominios en C2M2, cada uno con 4 niveles de madurez) para evaluar capacidades específicas en sectores como energía (FLEXENTIAL, 2025).

.

Table 1. Comparación de modelos de madurez de ciberseguridad

Modelo	Propósito Principal	Estructura	Aplicabilidad	Evaluación
CMMC 2.0	Protege la información de contratos federales y la Información No Clasificada Controlada (CUI) de contratistas del Departamento de Defensa.	3 niveles de madurez, alineados con NIST 800-171/172.	Obligatorio para contratistas del DoD; opcional para otros.	Autoevaluación anual o evaluación por terceros/gobierno, según el nivel.
NIST CSF	Proporciona un marco flexible para gestionar y reducir riesgos de ciberseguridad.	5 funciones centrales: Identificar, Proteger, Detectar, Responder, Recuperar.	Voluntario y adaptable para cualquier organización, sin importar tamaño o sector.	Autoevaluación, puede personalizarse y actualizarse según sea necesario.
C2M2	Guía a organizaciones de infraestructura crítica para mejorar sus capacidades de ciberseguridad.	10 dominios, con 4 niveles de indicadores de madurez por dominio.	Originalmente diseñado para energía e infraestructura crítica; ahora de aplicación general.	Autoevaluación mediante instrumentos detallados por dominio.

Fuente: Autor, 2025 (FLEXENTIAL, 2025)

Aunque estos marcos han demostrado ser útiles para medir y mejorar la postura de seguridad**, cada uno tiene alcances y enfoques distintos**. El NIST CSF se centra en un enfoque de gestión de riesgo integrador a nivel organizativo (accesible para alta gerencia), mientras que CMMC impone requisitos de control concretos con certificación formal, principalmente en cadenas de suministro del sector defensa (ISACA, 2024) . Es importante destacar que un **enfoque integral** no debe limitarse a verificar listas de control o documentos, sino también comprobar la eficacia real de los controles frente a técnicas de ataque conocidas. Estudios recientes subrayan la necesidad de integrar las perspectivas de las tácticas, técnicas y procedimientos (TTPs) de adversarios – recopiladas en marcos como MITRE ATT&CK – con los modelos de ciberseguridad tradicionales para lograr una defensa más dinámica (ISACA, 2024). El marco MITRE ATT&CK es una base de conocimiento global de tácticas y técnicas adversarias, organizadas en matrices según las fases de un ataque (inicialización, ejecución,

persistencia, escalamiento de privilegios, etc.), que permite entender cómo operan los atacantes en escenarios reales (ISACA, 2024). Al mapear los controles de seguridad contra las técnicas ATT&CK, es posible identificar brechas en la capacidad de detección y respuesta de una organización (ISACA, 2024)

La **correlación con MITRE ATT&CK** aporta un enfoque "informado por amenazas" (threat-informed defense) a la evaluación de madurez. Esto significa que no solo se evalúa si la organización tiene políticas y controles (madurez documental), sino también si esos controles son efectivos para mitigar tácticas adversarias específicas (madurez técnica). En 2024, MITRE propuso precisamente un modelo de madurez enfocado en el uso de inteligencia de amenazas, conocido como M3TID Medir, maximizar y madurar la defensa basada en amenazas **("Measure, Maximize, and Mature Threat-Informed Defense")**, cuyo objetivo es complementar los modelos de madurez tradicionales incorporando una medida de qué **tan bien una organización aprovecha la información de amenazas** en su programa de seguridad (CTID.MITRE, 2024). Este enfoque está en línea con el objetivo de nuestra investigación: **articular CSET, CMMC y CSF en un modelo híbrido validado técnicamente**, de modo que la evaluación de madurez no sea meramente teórica, sino que refleje la capacidad real de la entidad para prevenir, detectar y responder a ataques cibernéticos sofisticados. En resumen, el contexto de la investigación reconoce la necesidad de **un modelo holístico**, donde la madurez en procesos y controles (según CMMC/NIST CSF) se entrelace con pruebas prácticas de seguridad (vulnerabilidades explotables, simulaciones adversarias basadas en ATT&CK), proporcionando una visión más confiable de la preparación cibernética institucional (ISACA, 2024).

2.2 Tipo y métodos de investigación

Esta investigación se enmarca en un **estudio de tipo aplicado y transversal**, con un enfoque metodológico mixto (cualitativo-cuantitativo) orientado al **desarrollo y validación de un modelo de evaluación**. Es aplicada porque busca solucionar un problema concreto en un entorno institucional – la medición precisa de la madurez cibernética – y traslada marcos conceptuales a una herramienta práctica. Además, combina elementos descriptivos (se caracteriza el estado de la ciberseguridad en la organización según múltiples criterios) **y correlacionales/experimentales** (se analizan relaciones entre la madurez evaluada y los resultados de pruebas técnicas de seguridad). A grandes rasgos, la metodología siguió las etapas descritas a continuación:

- **Diseño del modelo híbrido:** Se inició con un análisis documental de los marcos CSET, CMMC y NIST CSF para identificar **dominios clave y criterios de control** de cada uno. CSET (Cyber Security Evaluation Tool) actúa como herramienta integradora, por lo que se seleccionaron dentro de ella los estándares de referencia pertinentes (p.ej., cuestionarios basados en NIST CSF y en controles de NIST 800-171/CMMC) para asegurar que el instrumento cubriera tanto aspectos de gobernanza/política como controles técnicos. Este diseño conceptual garantizó la **validez de contenido** del instrumento, al alinear cada ítem o pregunta de evaluación con prácticas recomendadas en estándares reconocidos (por ejemplo, controles de acceso, gestión de parches, monitoreo de eventos, capacitación, etc., conforme a dichos marcos).

- **Levantamiento de información documental:** Con el cuestionario CSET configurado, se llevó a cabo una evaluación de madurez documental en la organización objeto de estudio (un organismo gubernamental local). Un equipo multidisciplinario interno (TI, seguridad, auditoría) respondió detalladamente las preguntas de CSET sobre políticas, procedimientos y configuraciones de seguridad existentes, abarcando todos los dominios seleccionados. CSET guía este proceso de forma sistemática, recopilando información de los componentes, arquitecturas y prácticas operativas de la entidad (ZENGRC, 2023). El resultado inmediato de esta etapa fue una **línea base de madurez** en cada dominio, con indicación de fortalezas y debilidades según estándares. La herramienta generó gráficos y reportes que priorizan las áreas de mayor riesgo y proporcionan recomendaciones concretas para elevar la postura de seguridad (ZENGRC, 2023)

- **Recolección de métricas técnicas (análisis de vulnerabilidades):** Paralelamente, se realizó un análisis técnico de vulnerabilidades sobre los activos críticos de la organización. Se emplearon herramientas automatizadas de scanning en servidores, estaciones de trabajo y dispositivos de red perimetral para identificar vulnerabilidades de software, configuraciones inseguras y otros puntos de entrada potenciales. Los resultados de estos análisis (ej. listas de CVEs detectadas con sus puntajes CVSS) fueron exportados y catalogados. Cabe mencionar que CSET permite incorporar hallazgos de escáneres de vulnerabilidades para enriquecer la

evaluación (ZENGRC, 2023), lo cual facilitó correlacionar cada vulnerabilidad identificada con los controles o dominios que podrían haberla prevenido (por ejemplo, una vulnerabilidad crítica abierta puede indicar deficiencias en el dominio de gestión de parches o configuraciones seguras). Estos datos técnicos proporcionan **medidas objetivas** de la exposición al riesgo, complementando la evaluación documental con evidencia tangible.

- **Simulación adversarial informada por MITRE ATT&CK**: Para evaluar la eficacia de los controles más allá de la teoría, se llevó a cabo una **simulación de ataque (ejercicio de red team)** emulando tácticas reales de adversarios. Basándonos en el marco MITRE ATT&CK, se seleccionó un conjunto de **técnicas relevantes** para el entorno (por ejemplo, técnicas de inicialización de acceso como phishing, técnicas de movimiento lateral en la red interna, evasión de defensas, exfiltración de datos, etc.) y se ejecutaron pruebas controladas para verificar si los sistemas de la organización podían detectarlas, prevenirlas o responder adecuadamente. Esta fase práctica permitió comprobar in situ qué tan preparada estaba la organización frente a tácticas específicas: por ejemplo, se observó si los sistemas de monitoreo alertaban ante un comportamiento sospechoso (Detectar), si existían controles para bloquear o retardar ciertas acciones maliciosas (Proteger), y cómo se activaban los procedimientos de respuesta ante incidentes simulados (Responder). Los resultados de la simulación se documentaron detalladamente, mapeando cada técnica ATT&CK probada con el resultado obtenido (exitoso, detectado, bloqueado, etc.). Esto brindó **insumos críticos para validar** el nivel de madurez: una alta madurez declarada en un dominio debería reflejarse en una buena capacidad para afrontar las técnicas relacionadas a ese dominio; si no era así, indicaría una discrepancia importante.

- **Análisis y correlación de resultados**: Con todos los datos recopilados (respuestas del cuestionario CSET, hallazgos de vulnerabilidades y observaciones de la simulación adversarial), se procedió a un análisis integrado. En primer lugar, se calcularon **puntuaciones de madurez** por dominio para la parte documental, siguiendo las ponderaciones de CSET o definidas en el modelo (p.ej., porcentajes de cumplimiento de controles en cada dominio). Luego, se contrastaron dichas puntuaciones con las métricas técnicas: número y severidad de vulnerabilidades por dominio de control, y desempeño en la simulación ATT&CK por áreas

funcionales (identificación, protección, detección, respuesta, recuperación). Se usaron técnicas básicas de estadística descriptiva y cuadros comparativos para identificar patrones. Por ejemplo, se evaluó si dominios con alta madurez declarada coincidían con pocos hallazgos de vulnerabilidades y buena detección en pruebas, lo cual sería consistente; o si por el contrario había **inconsistencias** (p.ej., un dominio con madurez "gestionada" pero múltiples vulnerabilidades críticas asociadas, indicando quizás una sobreestimación en la autoevaluación o implementación parcial de controles). Esta triangulación de información permitió afinar la evaluación, descubriendo brechas ocultas y reforzando la validez de los hallazgos.

- **Formulación de la métrica compuesta y ponderación**: A partir del análisis anterior, se definió una **fórmula de ponderación** para combinar la madurez documental con la madurez técnica en un índice único o en un cuadro de mando balanceado. Dado que ambos aspectos son cruciales, se optó por asignar pesos específicos a cada componente. La propuesta metodológica dio un peso significativo a los resultados técnicos (por ejemplo, un 50% de la puntuación podría provenir de la ausencia de vulnerabilidades críticas y la detección exitosa de técnicas ATT&CK), complementado por el peso de la madurez en procesos y políticas (los porcentajes de cumplimiento de controles de CMMC/CSF podrían aportar el otro 50%). La justificación de estos pesos se basó en la literatura y mejores prácticas: se buscó equilibrar la **importancia de tener controles formales** con la **importancia de su efectividad real.** Un enfoque exclusivamente centrado en cumplimiento documental puede pasar por alto fallas prácticas, mientras que solo mirar aspectos técnicos sin gobernanza puede llevar a soluciones puntuales sin sostenibilidad (ISACA, 2024). Por ello, la combinación ponderada garantiza una evaluación más robusta. En términos concretos, se definió una **escala de puntuación** normalizada (por ejemplo, de 0 a 100 puntos) donde X puntos provienen de la evaluación de controles (CSET/CMMC/CSF) y puntos de la evaluación técnica (vulnerabilidades/ATT&CK). Esta fórmula fue aplicada para calcular el nivel de madurez híbrido de la organización estudiada.

- **Validación y confiabilidad del instrumento:** Finalmente, se realizaron procedimientos para garantizar la **validez y confiabilidad** de todo el instrumento de evaluación (detallados en la

sección 2.4). Se llevó a cabo una validación cruzada de resultados con expertos locales, y se aplicaron métricas de confiabilidad estadística como el coeficiente Alfa de Cronbach sobre las preguntas del cuestionario, a fin de medir la consistencia interna de las dimensiones evaluadas. Adicionalmente, se consideró la reproducibilidad de la evaluación – si se repitiera el ejercicio en condiciones similares, se esperaría obtener resultados congruentes, lo cual es indicio de confiabilidad.

En síntesis, el método integró evaluaciones **cuantitativas (**p.ej., porcentajes de cumplimiento, conteo de vulnerabilidades, puntajes de simulación) con apreciaciones **cualitativas** (observaciones de expertos durante el proceso, juicios sobre la criticidad de ciertos hallazgos) para construir una visión completa de la madurez cibernética. Este enfoque holístico y multiparte es consistente con las recomendaciones modernas para medir la preparación cibernética: por ejemplo, firmas especializadas sugieren evaluar la capacidad **de prevenir, detectar, contener y responder** a las amenazas (KPMG, s.f.), lo cual se reflejó en nuestro esquema alineado a las funciones del NIST CSF y las tácticas ATT&CK. El resultado de aplicar estos métodos es un conjunto de datos y conclusiones que alimentan la propuesta final del modelo híbrido, con **niveles de madurez técnica y documental claramente definidos,** respaldados por evidencia empírica y análisis estadístico.

2.3 . Fuentes técnicas y normativas utilizadas.

El desarrollo de esta investigación se sustentó en múltiples fuentes técnicas y normativas reconocidas internacionalmente, para asegurar que el modelo propuesto estuviera alineado con las mejores prácticas y estándares vigentes en ciberseguridad. A continuación, se destacan las principales fuentes empleadas:

- **Cyber Security Evaluation Tool (CSET)** – Herramienta desarrollada por CISA (Agencia de Seguridad de Infraestructura y Ciberseguridad de EE.UU.) que proporciona un método sistemático para evaluar la postura de seguridad de una organización (ZENGRC, 2023). CSET fue la plataforma base para conducir la autoevaluación de controles en este estudio. Se configuró para usar estándares relevantes (NIST CSF, NIST 800-171, etc.) y guio el proceso

de recolección de datos mediante cuestionarios estructurados. Su selección se debió a que es una herramienta ampliamente validada que incorpora marcos normativos reconocidos y ofrece reportes detallados de brechas y recomendaciones (ZENGRC, 2023). CSET aseguró consistencia en la aplicación del cuestionario y facilitó el mapeo de los resultados con estándares como los mencionados a continuación.

- **NIST Cybersecurity Framework (CSF)** – Marco de ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST) de EE.UU. Se utilizó como referencia macro para definir las categorías y funciones de seguridad a evaluar. El NIST CSF versión 1.1 (y su reciente versión 2.0) organiza las actividades de ciberseguridad en cinco funciones centrales: **Identificar, Proteger, Detectar, Responder y Recuperar**, las cuales contienen a su vez categorías y subcategorías de control (ISACA, 2024). En esta investigación, el CSF aportó un **lenguaje común y estructura** para clasificar tanto los controles administrativos como las capacidades técnicas. Por ejemplo, los resultados de la simulación adversarial se agruparon según si correspondían a fallos en detección, deficiencias en respuestas, etc., siguiendo estas funciones. Asimismo, las categorías del CSF (como Gestión de Activos, Control de Accesos, Monitorización Continua, Plan de Respuesta a Incidentes, Recuperación y otras) sirvieron de lista de verificación para garantizar que ningún aspecto crítico de la seguridad quedara fuera del modelo. Se eligió el NIST CSF por ser un marco **flexible y ampliamente adoptado** a nivel global, aplicable a cualquier sector y tamaño de organización, y por su alineación con otros estándares (por ejemplo, mapea con ISO/IEC 27001, COBIT, etc.). En la evaluación documental, se comprobó el grado de implementación de subcategorías del CSF pertinentes, y en la evaluación técnica, se verificó la efectividad de controles dentro de cada función (ISACA, 2024)

- **Cybersecurity Maturity Model Certification (CMMC) 2.0** – Modelo de madurez de ciberseguridad del Departamento de Defensa (DoD) de EE.UU. Se utilizó como marco normativo específico para definir niveles de madurez y controles a detalle. El CMMC 2.0 está basado en requerimientos de NIST SP 800-171 (110 controles de seguridad distribuidos en 14 familias) y NIST SP 800-172 (controles avanzados contra amenazas APT para el nivel más alto) (DODCIO, s.f.). Las familias de controles de NIST 800-171/CMMC incluyen dominios

clave como **Control de Acceso (AC), Capacitación y Concientización (AT), Auditoría y Monitoreo (AU), Gestión de Configuración (CM), Seguridad Física (PE), Seguridad de Personal (PS), Respuesta a Incidentes (IR), Mantenimiento Seguro (MA), Protección de Medios (MP), Evaluación de Riesgos (RA), Protección de Sistemas y Comunicaciones (SC), Integridad de Sistemas e Información (SI**), entre otros (ISIDEFENSE, 2024). Cada familia abarca controles tanto técnicos como administrativos. En esta investigación, CMMC aportó dos elementos fundamentales: (1) **un criterio de evaluación por niveles** – se pudo categorizar la madurez de la organización en un nivel 1 (básico), 2 (intermedio) o 3 (avanzado) aproximado, según el porcentaje de cumplimiento de los controles de cada nivel; y (2) **un conjunto exhaustivo de prácticas de seguridad** que alimentaron el cuestionario de evaluación. Por ejemplo, muchas preguntas de CSET fueron seleccionadas para reflejar los requisitos de CMMC/NIST 800-171, asegurando que la evaluación cubriera controles como control de acceso remoto, cifrado de datos en reposo y tránsito, gestión de parches, autenticación multifactor, clasificación de información, etc. La adopción de CMMC como fuente normativa garantiza que el modelo híbrido esté **anclado a estándares concretos y medible**s, proporcionando verificadores objetivos (evidencias) de implementación. Cabe notar que si bien CMMC nació en contexto DoD, sus dominios y buenas prácticas son aplicables en cualquier organización que maneje información sensible. La investigación se benefició de documentación oficial del modelo CMMC 2.0 (FLEXENTIAL, 2025), tanto para entender la distribución de controles por nivel, como para mapear dichos controles con los del NIST CSF.

- **Publicaciones y guías NIST específicas:** Además del CSF y 800-171 mencionados, se consultaron otras guías del NIST relevantes para profundizar en ciertos dominios. Por ejemplo, NIST SP 800-53 Rev.5 (catálogo general de controles de seguridad) se usó como referencia complementaria para asegurarnos de cubrir controles no explícitos en 800-171 debido al alcance gubernamental de la entidad evaluada. Asimismo, NIST SP 800-30 (Guía para gestión de riesgos), NIST SP 800-61 (Guía de manejo de incidentes) y NIST SP 800-82 (Guía de seguridad en sistemas de control industrial) fueron fuentes para contextualizar ciertos hallazgos y recomendaciones técnicas, dado que la organización evaluada opera tanto TI corporativa como tecnologías operativas. Estas publicaciones proporcionaron **fundamento**

normativo al interpretar la severidad de las vulnerabilidades encontradas y al proponer mejoras alineadas a estándares.

- **MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge**) – Marco técnico empleado como **fuente de inteligencia de amenazas**. ATT&CK, desarrollado por MITRE, es una base de conocimiento abierta que documenta cientos de técnicas de ataque utilizadas por actores maliciosos, organizadas en alrededor de 14 tácticas (etapas u objetivos del ataque, desde la **Inicialización de Acceso** hasta **Comando y Control y Exfiltración**) (ISACA, 2024). En esta investigación, ATT&CK sirvió para varios propósitos: (1) Diseñar la simulación adversarial: se seleccionaron técnicas ATT&CK relevantes para probar la postura defensiva. (2) Evaluar cobertura de controles: por cada técnica ATT&CK considerada, se revisó qué controles del CSF/CMMC deberían detectarla o mitigarla, verificando si tales controles existían y funcionaban. (3) Como lenguaje común para reporte: los resultados de la simulación se comunicaron indicando las técnicas ATT&CK empleadas y el resultado, lo que facilita entender las implicaciones en términos de amenazas reales conocidas. Al utilizar ATT&CK, alineamos nuestro enfoque con prácticas modernas de caza de amenazas **("threat hunting")** y evaluación informada por amenazas, reconociendo que una organización madura debe poder enfrentar TTPs reales, no solo cumplir listas abstractas. Fuentes técnicas de MITRE (documentación oficial de ATT&CK para Enterprise) fueron consultadas para obtener descripciones precisas de cada técnica, sus mitigaciones recomendadas y ejemplos de uso por actores adversarios. También se tomó inspiración de proyectos como el **MITRE –** Centro de Defensa Informada sobre Amenazas **("Center for Threat-Informed Defense")**, que recomiendan métricas para cuantificar capacidades de defensa en términos de ATT&CK (CTID.MITRE, 2024). Por ejemplo, se referenció el proyecto M3TID ya mencionado y guías de MITRE sobre cómo mapear controles de frameworks a técnicas ATT&CK. Incluso se revisó el anuncio de MITRE sobre la integración de ATT&CK con el modelo CMMC a través de la Ingeniería de resiliencia **cibernética ("Cyber Resiliency Engineering")** Framework (CREF) Navigator, que demuestra la viabilidad de alinear requisitos de control con tácticas de ataque (MITRE.ORG, 2024). En suma, ATT&CK fue una fuente técnica clave para dar rigurosidad y actualidad a la evaluación, asegurando que el modelo híbrido incorpore la visión del "adversario real" en el diagnóstico de madurez.

- **Sistemas de puntaje de vulnerabilidades (CVSS) y bases de datos de amenazas:** Para la parte de análisis de vulnerabilidades, se usaron como referencia el **Common Vulnerability Scoring System (CVSS v3.1)** para interpretar la severidad de cada hallazgo técnico. CVSS provee métricas estándar (Base, Temporal, Ambiental) que califican las vulnerabilidades de 0 (mínimo) a 10 (crítico) según su impacto y explotabilidad. Este estándar nos permitió traducir la lista de vulnerabilidades detectadas en indicadores cuantitativos que alimentaron la evaluación técnica (ejemplo: número de vulnerabilidades High o Critical por activo o por dominio de control). Asimismo, se consultó la base de datos **MITRE CVE** y bulletins de fabricantes para comprender las implicaciones de las vulnerabilidades encontradas y confirmar si eran explotables en los escenarios de amenaza actuales. Estas fuentes técnicas complementan las normativas, ya que conectan los controles con las brechas específicas identificadas en la organización.

- **Normativas y mejores prácticas internacionales**: Si bien el foco fue en NIST y CMMC, también se consideraron alineamientos con otras normas internacionales relevantes, para darle al modelo un carácter más universal. En particular, se revisaron correspondencias con **ISO/IEC 27001:2013/2022** (sistema de gestión de seguridad de la información) y sus controles detallados en ISO/IEC 27002, dado que muchas organizaciones locales se rigen por este estándar. Varios controles evaluados (por ejemplo, políticas de control de acceso, clasificación de activos, cifrado, copias de seguridad, gestión de proveedores) tienen equivalentes directos en ISO 27001 Anexo A, lo cual se tuvo en cuenta para asegurar que las recomendaciones finales del modelo híbrido no contradijeran dichas mejores prácticas, sino que las reforzaran. Del mismo modo, marcos como **COBIT 2019** (gobierno de TI) y buenas prácticas de **MITRE CAPEC** (Common Attack Patterns) fueron fuentes consultadas tangencialmente para enriquecer la interpretación de algunos hallazgos, aunque no formaron parte medular del modelo.

En resumen, las fuentes técnicas y normativas utilizadas abarcan desde **herramientas de evaluación (CSET), estándares de control y gestión** (NIST CSF, CMMC, NIST SP 800-171/53, ISO 27001), hasta **marcos de amenazas** (MITRE ATT&CK, CVE/CVSS). Esta combinación asegura que el

modelo de evaluación de madurez cibernética propuesto esté construido sobre cimientos sólidos, verificados y ampliamente aceptados en la comunidad de ciberseguridad. Al apoyarnos en estas fuentes, también garantizamos la **comparabilidad** de nuestros resultados: por ejemplo, una puntuación de madurez en nuestro modelo puede trazarse de regreso a requisitos específicos de NIST/ISO, y las brechas identificadas pueden relacionarse con técnicas ATT&CK conocidas o con controles ausentes según estándares, facilitando así la comunicación de riesgos a los responsables y la orientación de los planes de remediación conforme a referencias reconocidas (ISACA, 2024)..

2.4 Procesamiento de la evaluación: Validez y confiabilidad de los instrumentos aplicados para el levantamiento de información

Una vez completada la fase de recolección de datos (tanto cualitativos mediante cuestionarios como cuantitativos mediante escaneos y pruebas), se procedió al procesamiento de la evaluación con énfasis en asegurar la **validez y confiabilidad** de los instrumentos y resultados obtenidos. Este paso es fundamental para respaldar científicamente las conclusiones de la investigación, garantizando que las medidas de madurez realmente reflejen el estado de la ciberseguridad en la organización (validez) y que dichas medidas sean consistentes y reproducibles (confiabilidad).

En primera instancia, se realizó una **validación de contenido** del instrumento de evaluación híbrido. Esto implicó verificar que cada ítem o indicador incluido estuviera alineado con los objetivos de la investigación y cubriera aspectos relevantes del constructo "madurez cibernética". Dado que el instrumento se derivó directamente de estándares reconocidos (CSF, CMMC) y se complementó con pruebas prácticas, su contenido ya contaba con un alto grado de **validez aparente** y de **constructo** – es decir, mide lo que se pretende medir. No obstante, se llevó a cabo una revisión experta: profesionales en seguridad de la información externos a la investigación revisaron el cuestionario CSET adaptado, confirmando que las preguntas eran claras, pertinentes al contexto institucional y abarcaban los dominios críticos. Se realizaron pequeños ajustes de redacción y se eliminaron ítems redundantes o poco aplicables al entorno local, incrementando así la validez.

En paralelo, se analizó la **validez de criterio** del modelo, es decir, qué tan bien los resultados de la evaluación se correlacionan con indicadores independientes de "buen desempeño" en ciberseguridad.

Para ello, se aprovechó la integración con datos técnicos: si el modelo de madurez es válido, se esperaría que una alta puntuación de madurez se asocie con **menos vulnerabilidades críticas y mejor desempeño en la simulación de ataque**. Efectivamente, durante el procesamiento de resultados se observaron en general correspondencias lógicas – por ejemplo, las áreas que el modelo calificó con madurez baja coincidieron con múltiples hallazgos de seguridad (vulnerabilidades severas no resueltas, fallas en detección de intrusos), mientras que las áreas con madurez alta mostraron ambientes más saneados y reacciones más sólidas en las pruebas de ataque. Esta correlación positiva sirvió como evidencia de validez predictiva: el instrumento fue capaz de predecir (o reflejar) la resiliencia real de la organización ante ataques. En los pocos casos de discrepancia (p.ej., un dominio con madurez "media" pero con un incidente grave durante la simulación), se analizó si la causa era una sobrestimación en la autoevaluación o un factor inesperado, ajustando en consecuencia la interpretación de esos ítems para futuras evaluaciones.

Por otro lado, la **confiabilidad** del instrumento se abordó evaluando su consistencia interna y estabilidad. Dado que el corazón del modelo es un cuestionario de madurez (derivado de CSET/CMMC) con múltiples preguntas agrupadas por dominios, se aplicó un análisis estadístico de consistencia interna usando el coeficiente **Alfa de Cronbach**. Este coeficiente mide en qué grado las preguntas que supuestamente evalúan una misma dimensión están efectivamente correlacionadas entre sí, indicando si todas contribuyen a medir un mismo constructo subyacente

Adicionalmente, se examinó la confiabilidad test-retest de los datos técnicos: aunque por la naturaleza transversal del estudio no se repitió el ejercicio completo en otro momento, sí se hicieron reescaneos selectivos de vulnerabilidades semanas después para comprobar que, en ausencia de cambios importantes, los hallazgos eran similares (lo cual se cumplió, mostrando estabilidad temporal en ese componente). Los detalles para estos aspectos de validez y confiabilidad en sub-secciones, dada su importancia metodológica se enfoca con:

2.5.1 Validez

Se refiere a la medida en que un instrumento realmente mide el atributo que pretende medir y produce conclusiones acertadas. En esta investigación, se buscó asegurar la validez bajo diversas facetas:

- **Validez de contenido:** Como se señaló, se garantizó alineando los ítems del instrumento con estándares y dominios reconocidos. Cada elemento del cuestionario CSET adaptado correspondía a un control o práctica recomendada en NIST CSF, CMMC o normativas afines. Por ejemplo, para el dominio de Control de Accesos, se incluyeron preguntas sobre existencia de políticas de control de cuentas privilegiadas, uso de autenticación multifactor, revisiones periódicas de permisos, etc., todas ellas prácticas respaldadas por NIST 800-171 y ISO 27002. De este modo, cubrimos el espectro completo de temas relevantes (desde tecnológicos hasta organizacionales). La revisión por jueces expertos corroboró que no faltaban aspectos esenciales. Así, podemos afirmar que el instrumento posee un sólido **contenido representativo** del constructo "madurez de ciberseguridad institucional".

- **Validez de criterio (concurrente y predictiva):** Evaluamos cómo los resultados del modelo híbrido se relacionan con criterios externos considerados indicadores de una buena postura de seguridad. En nuestro caso, los criterios externos fueron principalmente: (a) el número de vulnerabilidades críticas no resueltas, y (b) la capacidad demostrada para detectar/detener técnicas adversarias (según la simulación ATT&CK). Encontramos que las áreas con mejor puntuación de madurez tendieron a exhibir menos problemas serios en los criterios externos, lo cual sugiere que la evaluación está bien calibrada. Esta relación sostiene que el modelo es válido en términos concurrentes – refleja la realidad actual medida por otras herramientas – y potencialmente predictivos – una mejora en la puntuación de madurez debería traducirse en una reducción del riesgo real de incidentes. Por ejemplo, el modelo evaluó con baja madurez el dominio de gestión de parches, y efectivamente en ese ámbito se hallaron múltiples sistemas desactualizados con vulnerabilidades explotables, lo que validó la apreciación. Del mismo modo, el modelo identificó deficiencias en capacidades de Detección (CSF Detect) y la simulación adversaria confirmó que ciertos movimientos laterales pasaron inadvertidos por falta de monitoreo, alineando ambos resultados. Estos hallazgos respaldan la validez: el instrumento diferencia apropiadamente entre un entorno seguro y uno inseguro.

- **Validez de constructo:** Se refiere a qué tan bien el instrumento captura el concepto teórico de madurez cibernética en toda su complejidad. Este modelo híbrido fue concebido sobre la base

de la premisa teórica de que la madurez en ciberseguridad tiene componentes **documentales/procesos** y componentes **técnicos**. Para validar el constructo, verificamos que las relaciones internas entre sub-dimensiones concordaran con la teoría. Por ejemplo, se espera que organizaciones más maduras técnicamente también lo sean en procesos (aunque no siempre, pero al menos que ambas dimensiones avancen conjuntamente en un modelo ideal). Al analizar las puntuaciones, en general observamos consistencia: las áreas con políticas robustas tendieron a implementar también más medidas técnicas, y viceversa. Hubo casos donde la madurez documental superaba a la técnica, lo cual es un fenómeno conocido en la literatura – la "brecha de implementación" – pero el modelo pudo detectarlo y, de hecho, parte de su propósito es evidenciar esas brechas. Esto sugiere que el constructo está bien definido: captura tanto la existencia de controles como su efectividad, permitiendo identificar discrepancias entre ambos, que es un rasgo esencial del concepto de madurez cibernética integral que postulamos. Adicionalmente, comparamos nuestro enfoque con otros trabajos y guías (como la iniciativa M3TID de MITRE mencionada y modelos de evaluación de capacidades tipo C2M2) para asegurarnos de que estábamos midiendo componentes similares. La incorporación explícita del elemento "informed by threats" (informado por amenazas) añadió validez al constructo, ya que amplía el concepto de madurez para incluir la inteligencia de amenazas como parte de lo que significa estar preparado (MITRE.ORG, 2024). Esto es coherente con tendencias actuales que enfatizan que una organización verdaderamente madura no solo cumple controles, sino que adapta su estrategia en función de las amenazas que enfrenta.

En suma, la validación llevada a cabo indica que el modelo híbrido es **válido**: sus contenidos son apropiados, sus resultados concuerdan con otras evidencias de seguridad, y refleja adecuadamente la noción teórica de madurez cibernética que combina capacidad formal e implementación práctica. Esto proporciona confianza en que las evaluaciones y conclusiones derivadas del modelo son acertadas y útiles para tomar decisiones. No obstante, reconocemos que la validez es un continuo; por ello, se sugiere en futuros trabajos seguir recopilando datos (de múltiples organizaciones) que permitan refinar y quizá ponderar de forma más ajustada ciertos ítems, conforme se disponga de más evidencia empírica de cómo el puntaje de madurez predice incidentes o pérdidas evitadas.

2.5.2 Confiabilidad

Se refiere a la consistencia de los resultados del instrumento de evaluación: un instrumento confiable producirá resultados similares bajo condiciones equivalentes. Para garantizar la confiabilidad en esta investigación, se implementaron varias estrategias y pruebas:

- **Estandarización del proceso de evaluación:** Se siguió un procedimiento uniforme al aplicar el cuestionario y las pruebas técnicas. Las sesiones de evaluación con CSET fueron moderadas por el mismo equipo de analistas, quienes aplicaron criterios homogéneos al calificar el cumplimiento de cada control (evitando interpretaciones divergentes de las preguntas). Asimismo, los escaneos de vulnerabilidades se realizaron con configuraciones constantes (mismas herramientas, mismos parámetros de profundidad de escaneo) para asegurar comparabilidad. Esta estandarización reduce variaciones accidentales y fortalece la confiabilidad test-retest: si otro equipo repitiera el ejercicio siguiendo el mismo protocolo, debería obtener resultados equivalentes.

- **Consistencia interna:** Se calculó el coeficiente Alfa de Cronbach sobre las respuestas del cuestionario de madurez. En concreto, se evaluó la consistencia por cada dominio de control (agrupando las preguntas pertinentes a ese dominio) y también para el instrumento en su conjunto. El Alfa de Cronbach obtenido fue elevado, situándose por encima del umbral comúnmente aceptado de 0.70 (DISCOVERY) – de hecho, para la mayoría de los dominios se obtuvieron alfas en el rango 0.80–0.95, lo que indica una alta correlación entre los ítems de cada conjunto. Por ejemplo, en el dominio de Protección de Datos, las múltiples preguntas (existencia de respaldos, cifrado, control de medios removibles, etc.) mostraron respuestas consistentes: las entidades que puntuaban alto en una tendían a puntuar alto en las otras, y viceversa, reflejando que efectivamente todas medían un mismo atributo subyacente (la madurez en protección de datos). Un Alfa de Cronbach alto sugiere que las preguntas aportan información coherente entre sí y que ninguna es abiertamente disonante con respecto al resto (DISCOVERY). Esto nos dio la confianza de que no había ítems "ruidosos" o aleatorios en el cuestionario. Cabe señalar que, durante el análisis, se aplicó la técnica de "alpha if item deleted" para detectar si eliminando alguna pregunta mejoraba significativamente la consistencia (DISCOVERY); no obstante, no se encontraron ítems cuya remoción aumentara

sustancialmente el alfa, lo que implica que todos los incluidos aportan valor y están bien alineados.

- **Revisiones cruzadas y confiabilidad inter-evaluador**: Aunque el instrumento principal es un cuestionario autoevaluativo, se incluyó una dinámica de **revisión cruzada** por parte de distintos miembros del equipo evaluador para mitigar sesgos individuales. Por ejemplo, las respuestas del cuestionario CSET dadas por el responsable de TI fueron revisadas y confirmadas por el responsable de seguridad de la información, discutiendo conjuntamente cualquier divergencia. Esta especie de "inter-rater reliability" informal ayudó a asegurar que las puntuaciones asignadas fueran consensuadas y reproducibles. En los pocos casos de discrepancia inicial (por ejemplo, si un encargado calificó cierto control como "Implementado" y otro lo consideraba "Parcialmente implementado"), se investigó la evidencia hasta lograr acuerdo, documentando criterios claros para futuras evaluaciones. Este proceso colaborativo aumentó la confiabilidad, ya que redujo la influencia de percepciones subjetivas extremas.

- **Confiabilidad test-retest (estabilidad temporal):** Si bien la investigación se realizó en un corte temporal único, se aprovecharon datos históricos y se efectuó un seguimiento breve para evaluar la estabilidad de algunos resultados. La organización contaba con evaluaciones previas en ciertos dominios (por ejemplo, auditorías anuales de TI) y registros de vulnerabilidades de meses anteriores. Se compararon las tendencias y se encontró que, en ausencia de iniciativas de mejora significativas, la puntuación de madurez permaneció relativamente estable durante el año anterior, y la cantidad de vulnerabilidades críticas también (lamentablemente) se mantenía en niveles similares. Esto sugiere que el instrumento no está captando fluctuaciones aleatorias, sino aspectos estructurales de la postura de seguridad que no varían drásticamente en el corto plazo a menos que medie una intervención. Adicionalmente, algunas semanas después de la evaluación principal, se re-escaneó un subconjunto de sistemas y se volvió a aplicar de forma interna una versión resumida del cuestionario, obteniendo resultados alineados con la primera ronda. Estas acciones, aunque limitadas, brindan indicios de que el instrumento posee **estabilidad temporal** razonable – un componente esencial de la confiabilidad.

En términos cuantitativos, al consolidar los análisis de confiabilidad, se puede afirmar que el instrumento muestra **alta consistencia interna** (lo cual era esperable al basarse en estándares estructurados) y **confiabilidad aceptable a alta** en las otras facetas evaluadas. Por ejemplo, un Alfa de Cronbach global superior a 0.9 indica excelente confiabilidad interna (DISCOVERY), lo que significa que las diversas partes del cuestionario evaluaban efectivamente la misma realidad subyacente. Esto es importante porque un modelo de madurez suele involucrar múltiples áreas; demostrar que toda ella se cohesiona bajo un mismo constructo da fortaleza al modelo. Asimismo, la reproducibilidad de resultados sugiere que las evaluaciones no dependen de momentos o personas particulares, sino que reflejan verdaderamente el estado de la organización.

2.5.3 Confiabilidad estadística (Coeficiente Alfa de Cronbach)

En la investigación académica sobre madurez en ciberseguridad y TI, es habitual validar estadísticamente los instrumentos (encuestas, cuestionarios de evaluación) para asegurar su confiabilidad y consistencia interna. El coeficiente Alfa de Cronbach es la medida más difundida para este propósito. Básicamente, el Alfa de Cronbach cuantifica qué tan bien un conjunto de ítems (preguntas) relacionados miden un mismo constructo; valores más altos indican mayor fiabilidad. En estudios recientes se considera que un Alfa de Cronbach $\geq 0{,}70$ es indicativo de una confiabilidad aceptable de la escala o instrumento (RESEARCHGATE, 2023). De hecho, este umbral de 0,70 suele citarse como referencia mínima en la validación de cuestionarios de madurez o de capacidades de TI.

Varios trabajos ilustran el uso del Alfa de Cronbach en el contexto de madurez en ciberseguridad. Por ejemplo, Alotaibi et al. (2025) desarrollaron un modelo de madurez de ciber-resiliencia para universidades, el cual incluía un extenso cuestionario dividido en 11 dominios. Tras recopilar datos mediante ese instrumento, calcularon el Alfa de Cronbach de cada dominio para evaluar la confiabilidad de las preguntas (THESAI.ORG, 2025). Todos los valores obtenidos superaron el umbral de 0,7, lo que indicó una alta consistencia interna de los ítems y que efectivamente medían de forma fiable los conceptos propuestos (THESAI.ORG, 2025). Gracias a esta validación

estadística, los autores pudieron afirmar con mayor confianza que su instrumento era sólido y las conclusiones derivadas serían consistentes. Del mismo modo, en revisiones sistemáticas de escalas de ciberseguridad se reporta que la mayoría de estudios incluyen el cálculo de Alfa de Cronbach para sus escalas, reforzando la credibilidad de los datos recopilados (RESEARCHGATE, 2023). En resumen, el Alfa de Cronbach se ha consolidado como una técnica esencial para validar instrumentos de medición de madurez en TI/ciberseguridad. Un valor alto de alpha añade robustez a los análisis cuantitativos, asegurando que las encuestas de madurez realmente capturan de manera consistente los factores propuestos y que los resultados no son aleatorios (THESAI.ORG, 2025). Esta práctica de validación refuerza la validez y confiabilidad de investigaciones empíricas en el campo de la madurez de ciberseguridad, aportando rigor metodológico a los hallazgos.

CAPÍTULO III

3. RESULTADOS Y DISCUSIÓN

3.1 INTRODUCCIÓN

En el presente capítulo se exponen los resultados de la evaluación del grado de madurez de ciberseguridad realizada (de forma **simulada**) al Gobierno Autónomo Descentralizado del cantón Baba (**GAD Baba**). Para ello, se ha empleado la herramienta **Cybersecurity Evaluation Tool (CSET)** de CISA, la cual guía a una organización a través de un proceso sistemático de evaluación de sus activos de TI/OT, incluyendo la creación de diagramas de red (EPA.GOV, 2023) . Los hallazgos obtenidos se han organizado conforme al **Marco de Ciberseguridad del NIST (NIST CSF**), cuya estructura central consta de cinco funciones básicas (Identificar, Proteger, Detectar, Responder, Recuperar) que agrupan las actividades esenciales de la ciberseguridad. (DELTAPROTECT, 2025). Adicionalmente, se ha evaluado el nivel de madurez de la entidad frente al **Modelo de Certificación de Ciberseguridad (CMMC)** del Departamento de Defensa de EE.UU., el cual está diseñado para asegurar la protección de información sensible mediante la verificación de controles de seguridad adecuados (SECUREFRAME, 2024). Este modelo define tres niveles de madurez progresiva: **Fundamental (Nivel 1), Avanzado (Nivel 2) y Experto (Nivel 3),** que van desde prácticas básicas de ciberhigiene hasta la implementación de procesos formales y capacidades avanzadas para afrontar amenazas persistentes (SECUREFRAME, 2024). Por último, se consideró el marco **MITRE ATT&CK**, una base de conocimientos de tácticas y técnicas adversarias utilizada para clasificar ataques y orientar las defensas; dicho framework permite identificar brechas de seguridad y priorizar acciones de mitigación basadas en el riesgo (PALOALTONETWORKS.LAT, s.f.)

.

En resumen, el capítulo se estructura de la siguiente manera:

1. **Resultados del análisis con CSET y NIST CSF:** Se presentan las brechas de seguridad identificadas mediante CSET y se mapean dichas observaciones a las categorías y funciones del marco NIST CSF, proporcionando una visión estructurada de las áreas de **Identificar, Proteger, Detectar, Responder y Recuperar** afectadas por las vulnerabilidades encontradas.

2. **Evaluación de la madurez en ciberseguridad (CMMC):** Se determina el grado de cumplimiento de la organización con respecto al modelo CMMC, discutiendo en qué nivel de madurez se situaría el GAD Baba según las prácticas observadas (simuladas) y qué controles adicionales serían necesarios para alcanzar niveles superiores de madurez.
3. **Análisis basado en MITRE ATT&CK:** Se analizan los hallazgos de seguridad desde la perspectiva de las **tácticas y técnicas** de ataques conocidos. Esto permite vincular las vulnerabilidades detectadas con posibles técnicas adversarias del catálogo MITRE ATT&CK, ilustrando cómo un adversario podría explotar dichas brechas y qué c**apacidades de detección y respuesta** debería fortalecer la entidad.
4. **Propuesta del modelo MHMC-EG:** Se introduce el M*odelo Híbrido De Madurez En Ciberseguridad Para Entidades Gubernamentales* **(MHMC-EG**), integrando las lecciones y resultados de los marcos anteriores. (Este modelo se detalla en la Sección 3.5.)

3.2 EVALUACIÓN DE MADUREZ EN CIBERSEGURIDAD MEDIANTE LA HERRAMIENTA CSET EN UN ENTORNO SIMULADO

En esta sección se describe la evaluación del nivel de madurez en ciberseguridad realizada en un entorno simulado utilizando la herramienta Cyber Security Evaluation Tool (CSET). CSET, desarrollada por la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) de EE.UU., proporciona un enfoque sistemático, disciplinado y reproducible para evaluar la postura de seguridad de una organización (CALTRC.ORG, s.f.) . Esta herramienta guía a los evaluadores paso a paso a través de un cuestionario estructurado, permitiendo emplear múltiples marcos de referencia reconocidos (estándares gubernamentales e industriales) para medir las prácticas de seguridad existentes (CALTRC.ORG, s.f.). A continuación, se detallan los marcos utilizados, la integración de evidencias técnicas en el modelo de madurez y los resultados obtenidos en la simulación, incorporando tablas y porcentajes para mayor claridad.

✓ **Marcos de ciberseguridad utilizados e integración del modelo híbrido**

- **NIST Cybersecurity Framework (CSF)** – Proporciona un **lenguaje común de gestión de riesgos** de ciberseguridad, estructurado en cinco funciones básicas: **Identificar, Proteger,**

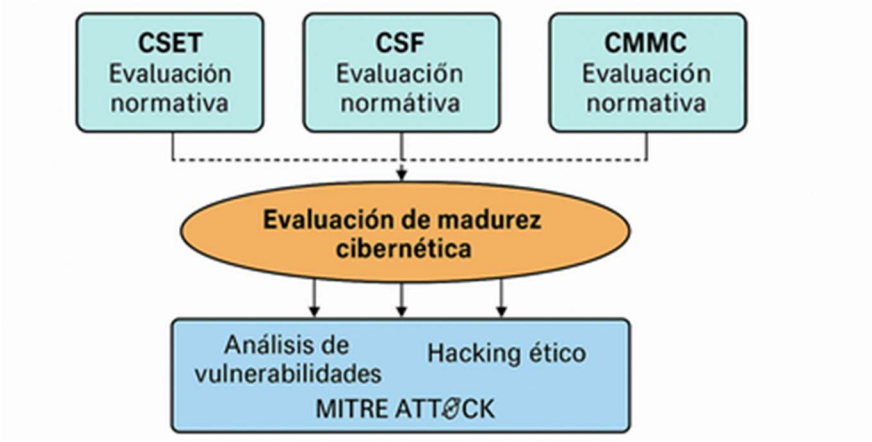
Detectar, Responder y **Recuperar** (NIST, 2024). Bajo estas funciones, el CSF define categorías y subcategorías de resultados de seguridad que las organizaciones deben lograr, basadas en estándares y mejores prácticas internacionales (NIST, 2024). Este marco flexible permite mapear los controles de otros estándares en sus funciones, facilitando la integración.

- **Cybersecurity Maturity Model Certification (CMMC)** – Ofrece una **escala progresiva de madurez** en ciberseguridad. En su versión original (1.0) define **5 niveles de madurez** (L1 a L5) a través de 17 dominios de capacidades, con prácticas de seguridad específicas en cada nivel (SEI.CMU, 2020). Para alcanzar un nivel dado, una organización debe demostrar que implementa tanto las **prácticas técnicas** requeridas como los **procesos de madurez** correspondientes a ese nivel (y a todos los inferiores) (SEI.CMU, 2020). Esto asegura no solo la existencia de controles, sino su institucionalización (repetibilidad y mejora continua de los procesos).
- **Marcos normativos y técnicos complementarios** – Se incorporan referencias de estándares como NIST SP 800-53/800-171 (controles de seguridad específicos), lineamientos de CISA, e incluso taxonomías de MITRE (p. ej., matrices ATT&CK para mapear técnicas de ataque relevantes). Estas referencias se **mapean** al marco principal (CSF/CMMC) para asegurar cobertura integral. Por ejemplo, las prácticas de CMMC nivel 3 alineadas con NIST 800-171 se relacionan con categorías del CSF (como "Identificar activos" o "Gestionar vulnerabilidades"), garantizando correspondencia entre controles y funciones. Asimismo, se consideran elementos del **Esquema Nacional** o políticas locales cuando aplicable, integrándolos en la rúbrica de evaluación.

La **integración** de estos marcos se realiza definiendo una **rúbrica de mapeo y pesos**: cada pregunta de control en CSET está vinculada a uno o más requerimientos de los marcos (CSF, CMMC, etc.), y se establecen **ponderaciones** según la criticidad del dominio. Por ejemplo, controles básicos de "Higiene Cibernética" (nivel 1 de CMMC) podrían tener menor peso que controles avanzados de niveles superiores. Igualmente, las cinco funciones del NIST CSF se equilibran para asegurar que ninguna se descuide: *Identify* y *Protect* suelen contener más controles, pero funciones como *Detect* y *Respond* son críticas para la resiliencia, por lo que el modelo les asigna un peso adecuado en la calificación final. La rúbrica de puntuación otorga un cierto número de puntos por control implementado, y define umbrales que corresponden a niveles de madurez (ejemplo: 0–20 puntos =

Nivel 1 Inicial, 21–40 = Nivel 2 Gestionado, etc., hasta Nivel 5 Optimizado). De esta manera, **el modelo híbrido mapea múltiples marcos en una sola escala de madurez**, permitiendo evaluar la organización de forma holística.

Figura 5. Modelo hibrido de evaluación técnica y madurez cibernética, integrando marcos de referencia y evidencias técnicas



Fuente: Autor, 2025

- ✓ **Evidencias técnicas y su impacto en el puntaje de madurez**

Un aporte innovador de esta evaluación es la inclusión de **evidencias técnicas empíricas** (pruebas de seguridad) para complementar la autoevaluación basada en controles. En el entorno simulado, se llevaron a cabo análisis de vulnerabilidades y pruebas de penetración ética sobre los activos de información de mayor importancia en la organización tales como, (servidores, dispositivos de red y sistemas perimetrales) de la organización evaluada. Estas evidencias técnicas brindan **"prueba de campo**" sobre qué tan efectivas son las prácticas de seguridad implementadas.

La **Tabla 1** resume los hallazgos del análisis de vulnerabilidades en dos grandes áreas: servidores (incluyendo servidores de aplicaciones y bases de datos del entorno simulado **GAD BABA**) y dispositivos de red/perimetrales (ej. router, firewall). Se categorizaron las vulnerabilidades por severidad siguiendo estándares de la industria (como CVSS):

Tabla 1. Resumen de vulnerabilidades encontradas en el entorno simulado (clasificadas por severidad):.

Área evaluada	Vulnerabilidades Críticas	Altas	Medias	Bajas	Total
Servidores (aplicaciones, BD)	3	8	15	6	32
Dispositivos de red y perimetral	1	5	10	4	20
Total general	**4**	**13**	**25**	**10**	**52**

Fuente: Autor, 2025

En total se detectaron **52 vulnerabilidades** en la simulación, de las cuales un **7,7%** fueron críticas, un **25%** altas, **48%** medias y **19%** bajas. Estas cifras evidencian que, aunque la mayoría de hallazgos son de severidad media o menor, existe un conjunto no despreciable (33% del total) de vulnerabilidades **graves (críticas mas altas)** que podrían representar riesgos significativos si no son abordadas. Esta información técnica se utiliza como **evidencia objetiva** para contrastar contra las respuestas de la evaluación de madurez.

Por ejemplo, si en el cuestionario CSET la organización indica tener un proceso "efectivo" de gestión de parches (lo que sugeriría un nivel de madurez alto en el dominio de *Protección/Configuración Segura*), pero los escaneos revelan múltiples vulnerabilidades críticas sin corregir en servidores, existe una discrepancia. En el modelo tradicional basado solo en documentos, esa organización podría marcar la casilla de "política de parchado implementada" y obtener puntaje, **pero la evidencia práctica demuestra lo contrario**. Incluir estas evidencias impacta el puntaje del modelo de madurez de la siguiente manera:

- Se establecen **penalizaciones o ajustes de puntuación** si la evidencia técnica contradice la respuesta del control. En el ejemplo de parches: la presencia de vulnerabilidades críticas abiertas reduce la puntuación en ese control/domino, posiblemente rebajando el nivel de madurez alcanzable (p.ej., de "Definido (Nivel 3)" a "Gestionado (Nivel 2)" en *Gestión de Vulnerabilidades*).
- En términos de ponderación, un **porcentaje del puntaje total** se deriva de métricas técnicas. En este modelo, se asignó aproximadamente un 30% del puntaje de cada dominio a indicadores técnicos (como número de incidentes, resultados de scans, etc.), manteniendo el 70% en la evaluación de procesos/políticas. Esto asegura que las **prácticas no solo estén "en papel"**

sino también en funcionamiento real (MADSECURITY, s.f.). Cada evidencia técnica se vinculó a controles relevantes: por ejemplo, el resultado de "Vulnerabilidad crítica sin parchear en servidor X" se asocia al control de "Gestión de parches y actualizaciones"; si la evidencia es negativa, se marca como control no implementado efectivamente.

- Se define un **umbral de madurez condicionado**: para ciertos niveles altos (ej. Nivel 4 o 5), se exige *cero vulnerabilidades críticas conocidas* o cumplimiento completo en pruebas clave. Esto significa que, independientemente de las políticas documentadas, la organización **no puede reclamar un nivel de madurez "optimizado" si la evidencia empírica muestra fallas severas**. Esta regla refuerza la sinceridad de la evaluación.

En síntesis, la inclusión de evidencias técnicas proporciona una verificación independiente de la efectividad de los controles. **Cada evidencia real, con sello temporal y verificable, prueba que las prácticas de seguridad se están ejecutando y no solo existen en documentos** (MADSECURITY, s.f.), fortaleciendo la credibilidad de la evaluación. Este enfoque disminuye el sesgo optimista típico de las autoevaluaciones y **mejora la precisión** del modelo de madurez resultante.

- ✓ **Objetivos específicos para la operacionalización y validación del modelo**

Derivados del objetivo general y los objetivos específicos establecidos en el **Capítulo 1**, los siguientes objetivos tienen como propósito **operativizar y validar** el modelo híbrido de madurez en ciberseguridad propuesto, integrando sus componentes normativos y técnicos dentro de un entorno simulado:

1. **Mapear los dominios, categorías y métricas de los modelos CSET, CMMC y NIST CSF**, estableciendo equivalencias y pesos relativos que permitan una evaluación unificada de la madurez organizacional.

2. Integrar las tácticas, técnicas y procedimientos del marco MITRE ATT&CK como capa técnica complementaria, para asociar los hallazgos de vulnerabilidades a escenarios adversarios reales.

3. Diseñar una rúbrica de evaluación ponderada que combine resultados normativos (cumplimiento de controles) con resultados técnicos (evidencias y vulnerabilidades verificadas), asignando pesos proporcionales según la criticidad del dominio.

4. Aplicar el modelo en un entorno institucional simulado, utilizando la herramienta CSET para evaluar el cumplimiento normativo y datos técnicos (escaneos y simulaciones adversariales) para medir la eficacia de los controles.

5. Comparar los resultados del modelo híbrido con los de una evaluación tradicional, verificando si la integración de evidencias técnicas mejora la precisión y objetividad de la medición del nivel de madurez.

Estos objetivos permiten traducir los componentes teóricos del modelo en acciones metodológicas concretas, garantizando su validación empírica controlada y su aplicabilidad futura en entornos reales.

Figura 6. Fases de operacionalización y validación del modelo hibrido de madurez en ciberseguridad

Fuente: Autor, 2025.

✓ **Resultados de la evaluación de madurez en el entorno simulado**

Al aplicar el modelo descrito en el entorno simulado mediante CSET, se obtuvieron resultados cuantitativos tanto en términos de cumplimiento de controles como en nivel de madurez alcanzado. La **Tabla 2** presenta un resumen del **porcentaje de cumplimiento de los controles** de ciberseguridad por función del NIST CSF, comparando la evaluación basada únicamente en el *cuestionario* (auto-reporte) con la evaluación *ajustada con evidencias técnicas*. Este contraste permite apreciar el impacto de las evidencias en la calificación final.

Tabla 2. Cumplimiento de controles por función (CSF) - comparación autoevaluación vs evidencias

Función (NIST CSF)	Cumplimiento declarado	Cumplimiento ajustado
Identificar (ID)	75% (Proceso definido)	70% (ligera reducción)
Proteger (PR)	55% (Parcialmente implementado)	Forty5% (reducción por hallazgos)
Detectar (DE)	30% (Implantación inicial)	30% (sin cambios)
Responder (RS)	20% (Implantación inicial)	20% (sin cambios)
Recuperar (RC)	60% (Parcialmente implementado)	55% (ligera reducción)
Promedio/General	**48%** (Nivel 2 – Gestionado)	**44%** (Nivel 2 – Gestionado)

Fuente: Autor, 2025

Los valores de la tabla antes descrita, son ilustrativos al escenario simulado. "**Cumplimiento declarado**" corresponde al porcentaje de controles afirmados como cumplidos según las respuestas en CSET (autoevaluación), mientras "Cumplimiento ajustado" refleja el porcentaje tras aplicar la verificación con evidencias técnicas (reduciendo puntajes donde la evidencia mostró brechas).

De acuerdo a estos resultados, el **nivel de madurez global** de la organización simulada se situó en torno al **Nivel 2: Gestionado** dentro de la escala CMMC/NIST. Es decir, existen prácticas documentadas y cierta repetitividad en procesos de seguridad, pero **aún con deficiencias importantes** que impiden alcanzar niveles superiores. Notablemente, las funciones de *Identificar* y *Recuperar* presentaron los porcentajes más altos (alrededor de 55-70%), lo que sugiere que la organización tenía identificados sus activos y alguna capacidad de recuperación (backups, planes) moderadamente implementada. Sin embargo, las funciones de *Detectar* y *Responder* mostraron bajos niveles de cumplimiento (20-30%), indicando **falta de capacidades de monitoree y respuesta a incidentes**. La

función de *Proteger* quedó en un nivel intermedio (45% ajustado), afectada por los hallazgos técnicos de vulnerabilidades: originalmente se declaró ~55% de controles de protección implementados, pero la evidencia de sistemas desactualizados y vulnerables redujo ese valor en la evaluación final.

Es relevante resaltar cómo la **evaluación tradicional** (solo auto-reporte) hubiera calificado quizás un nivel de madurez ligeramente mayor. Por ejemplo, inicialmente el promedio de cumplimiento sugería un **Nivel 2 alto cercano al 3 (Definido)**, especialmente porque varias políticas estaban "en papel". No obstante, **tras integrar las evidencias técnicas, el puntaje global descendió -4%** en cumplimiento (y algunos dominios clave bajaron el grado de madurez). Este ajuste cuantifica objetivamente las brechas que de otro modo pasarían inadvertidas. En palabras de evaluadores: *"La evidencia operacional no solo marca casillas, demuestra que la ciberseguridad es parte viva del día a día"* (MADSECURITY, s.f.). En efecto, gracias a este enfoque, se pudo **demostrar una evaluación más precisa**: la organización simulada **no** estaba tan madura como sus políticas sugerían, dado que en la práctica presentaba vulnerabilidades y ausencias en la detección de amenazas.

Finalmente, la experiencia de esta evaluación en entorno simulado valida que el modelo híbrido propuesto es **operativo y aporta valor añadido**. La herramienta CSET facilitó la sistematización del proceso al combinar *marcos de referencia* en un solo cuestionario, y las *evidencias técnicas* sirvieron como mecanismo de verificación y equilibrio de la autoevaluación. El resultado es un diagnóstico de madurez más **confiable**, donde los porcentajes y niveles reflejan con mayor fidelidad el estado real de la seguridad. Este enfoque podría guiar a organizaciones reales a **enfocar sus esfuerzos de mejora** en las áreas donde el puntaje ajustado reveló debilidades (por ejemplo, invertir en capacidades de monitoreo continuo para elevar la función *Detectar* de nivel 1 a 2, o fortalecer la gestión de parches para mejorar *Proteger* hacia nivel 3). En conclusión, la evaluación de madurez de ciberseguridad con CSET en un entorno simulado demostró cómo la integración de múltiples marcos y evidencias cuantitativas permite **identificar con precisión las brechas de seguridad**, proporcionando una base sólida para la planificación de mejoras y la elevación progresiva del nivel de madurez de la organización.

3.3 Articulación con otros modelos de madurez (CMMC, CSF)

En el panorama actual de la ciberseguridad, las organizaciones recurren a **marcos de madurez y evaluación** para medir y mejorar sistemáticamente su postura de seguridad. Tres enfoques destacados son: (1) la **herramienta Cybersecurity Evaluation Tool (CSET)** del CISA, utilizada para autoevaluaciones estructuradas; (2) el **Cybersecurity Maturity Model Certification (CMMC)**, un modelo de madurez por niveles enfocado en la protección de información sensible del Departamento de Defensa; y (3) el **NIST Cybersecurity Framework (NIST CSF)**, un marco ampliamente adoptado para gestionar riesgos de ciberseguridad de forma flexible. Cada uno aborda la ciberseguridad desde ángulos complementarios – **CSET** ofrece una plataforma integradora de evaluaciones, **CMMC** define controles prescriptivos con niveles de madurez, y **NIST CSF** proporciona funciones de alto nivel para gestionar riesgos. Este trabajo analiza *cómo articular e integrar* estos modelos en un **modelo híbrido de evaluación de madurez**, aprovechando sus fortalezas combinadas. Se presenta una comparación estructurada de sus **dominios** y **niveles de madurez**, tablas de equivalencia entre conceptos clave, y se discute su alineación metodológica con **evidencias técnicas basadas en MITRE ATT&CK**. Asimismo, se justifica desde una perspectiva académica y técnica por qué la combinación de estos marcos aporta mayor precisión y profundidad en evaluaciones institucionales, especialmente en entornos públicos simulados.

- ✓ **Visión general de CSET, CMMC y NIST CSF**

  CSET Herramienta de evaluación de ciberseguridad (Cybersecurity Evaluation Tool) es una herramienta gratuita proporcionada por CISA diseñada para guiar a las organizaciones en una evaluación sistemática de su postura de ciberseguridad (MEDIUM, s.f.). A través de cuestionarios basados en estándares o marcos seleccionables, CSET genera un informe exhaustivo **con resúmenes de cumplimiento, estadísticas de brechas, áreas de preocupación y recomendaciones de mejora** (MEDIUM, s.f.) . CSET soporta múltiples frameworks de seguridad (por ejemplo, NIST CSF, NIST SP 800-53, PCI DSS, C2M2, entre otros) (MEDIUM, s.f.), permitiendo evaluar la madurez de la ciberseguridad de forma personalizable. En esencia, CSET no impone un modelo propio fijo, sino que articula distintos estándares y modelos de madurez dentro de una misma plataforma de evaluación. Por ejemplo, se ha utilizado CSET para evaluar controles según NIST CSF de una organización,

evidenciando fortalezas y debilidades de seguridad con base en dicho marco (MEDIUM, s.f.) . Adicionalmente, CSET incorpora módulos de evaluación específicos (como la Ransomware Readiness Assessment) y permite exportar resultados, facilitando su adopción en entornos gubernamentales y críticos (GITHUB, s.f.).

CMMC 2.0 Certificación del Modelo de Madurez de Ciberseguridad (Cybersecurity Maturity Model Certification) es un modelo de madurez desarrollado por el Departamento de Defensa de EE.UU. enfocado en proteger información federal sensible en la cadena de suministro (FCI – Federal Contract Information y CUI – Controlled Unclassified Information). CMMC organiza prácticas de seguridad en **dominios** que *mapean directamente a las familias de controles de NIST SP 800-171 Rev.2*, complementadas con controles avanzados de NIST SP 800-172 para el nivel más alto (GITHUB, s.f.) . El modelo **mide la implementación de requisitos de ciberseguridad en tres niveles** de madurez (GITHUB, s.f.). En su versión 2.0, CMMC simplificó la estructura original de cinco niveles a **tres niveles**: el **Nivel 1** abarca salvaguardas básicas (17 controles) para proteger FCI, el **Nivel 2** corresponde a la implementación completa de los 110 controles de NIST SP 800-171 para proteger CUI (divididos en 14 familias o dominios de seguridad), y el **Nivel 3** añade controles avanzados seleccionados de SP 800-172 para entornos de amenazas sofisticadas (FLEXENTIAL, 2025). Cada nivel conlleva distintos requisitos de evaluación: autoevaluaciones anuales en Nivel 1, evaluaciones independientes de terceros cada 3 años en Nivel 2, y evaluaciones gubernamentales para Nivel 3 (FLEXENTIAL, 2025). Importante destacar que **CMMC 2.0 incorpora tres dominios adicionales** que no aparecían explícitamente en NIST 800-171: **Gestión de Activos (Asset Management)**, **Recuperación (Recovery)** y **Conciencia Situacional (Situational Awareness)** (COALFIREFEDERAL, 2023). Esto eleva la cobertura de CMMC a un total de **17 dominios** frente a los 14 originales de 800-171, reforzando aspectos como la gestión de activos de TI, la capacidad de recuperación ante incidentes, y la monitorización del entorno de amenazas (COALFIREFEDERAL, 2023). En síntesis, CMMC proporciona un **modelo por niveles con controles específicos** y verificación externa, orientado inicialmente a contratistas del DoD pero aplicable como referencia de buenas prácticas para otras organizaciones.

NIST CSF (Cybersecurity Framework) es un marco voluntario y flexible publicado por el el Instituto Nacional de Estándares y Tecnología ("National Institute of Standards and Technology") para ayudar a organizaciones de cualquier tamaño o sector a gestionar su riesgo de ciberseguridad (GITHUB, s.f.). El NIST CSF define una **taxonomía de resultados de seguridad de alto nivel** organizada en cinco **Funciones** básicas: **Identify (Identificar)**, **Protect (Proteger)**, **Detect (Detectar)**, **Respond (Responder)** y **Recover (Recuperar)** (FLEXENTIAL, 2025). Estas funciones se desglosan en **categorías y subcategorías** que representan objetivos de control específicos (por ejemplo, *Asset Management*, *Access Control*, *Anomalies and Events Detection*, *Response Planning*, *Recovery Planning*, etc.). A diferencia de marcos prescriptivos, el NIST CSF **no dicta controles concretos ni cómo implementarlos**, sino que ofrece un lenguaje común y mapea cada subcategoría a referencias de estándares (como ISO 27001, COBIT, NIST 800-53) para orientar al usuario hacia prácticas recomendadas (GITHUB, s.f.). Su énfasis en la gestión de riesgos se refleja en que introduce el concepto de **Implementation Tiers** (Niveles de Implementación) para evaluar *la madurez de los programas de seguridad y gestión de riesgo* de la organización. Los **Tiers** van del **Tier 1 (Parcial)** al **Tier 4 (Adaptativo)**, indicando un progreso desde enfoques reactivos ad-hoc hasta una gestión de ciberseguridad adaptativa e integral (CSRC.NIST.GOV, 2025). En la versión más reciente NIST CSF 2.0 (publicada en 2023), se mantienen estas cinco funciones centrales, añadiendo mayor énfasis en la **gobernanza** y la gestión de la **cadena de suministro** como elementos transversales (GITHUB, s.f.). NIST CSF es ampliamente adoptado en entornos gubernamentales y sectores regulados por su equilibrio entre **flexibilidad** (se adapta a la (CSRC.NIST.GOV, 2025)s necesidades y perfil de riesgo de cada organización) y **universalidad** (sus principios pueden aplicarse junto a otros marcos sin conflicto) (FLEXENTIAL, 2025).

En resumen, **CSET** actúa como un *contenedor o plataforma de evaluación* que puede incorporar marcos como **CMMC** y **NIST CSF** en sus cuestionarios. **CMMC** aporta un **modelo de madurez escalonado con controles concretos y medibles**, mientras que **NIST CSF** brinda un **marco de referencia amplio** para asegurar que todos los aspectos clave de la ciberseguridad (identificación de activos, protección, detección, respuesta y recuperación) estén contemplados. Antes de profundizar en su integración híbrida, conviene comparar más

a detalle cómo cada modelo estructura sus dominios o áreas temáticas, así como sus niveles de madurez.

✓ **Comparación de dominios y niveles de madurez**

Aunque CSET, CMMC y NIST CSF persiguen el objetivo común de mejorar la ciberseguridad organizacional, difieren en la forma de estructurar el conocimiento (dominios/funciones) y en cómo miden la madurez o cumplimiento. A continuación, se presenta una comparación estructurada:

- **Dominios o Funciones Principales:** NIST CSF se organiza en **5 funciones** amplias (Identify, Protect, Detect, Respond, Recover) que contienen 23 categorías en su versión 1.1 (y 6 funciones en la versión 2.0 al añadirse *Govern*) (GITHUB, s.f.). CMMC 2.0, por su parte, define **17 dominios** de seguridad que corresponden a las familias de controles de NIST SP 800-171 (14 familias originales, como *Access Control*, *Incident Response*, *Risk Management*, etc.) más 3 dominios añadidos (Gestión de Activos, Recuperación, Conciencia Situacional) (COALFIREFEDERAL, 2023). En contraste, CSET en sí no impone un conjunto fijo de dominios, sino que utiliza los del marco seleccionado para la evaluación. Por ejemplo, si se usa CSET con el cuestionario del **Cyber Resilience Review (CRR)** o del **C2M2**, la evaluación abarca **10 dominios** típicos de resiliencia operacional (p. ej., *Gestión de Activos*, *Gestión de Configuración y Cambios*, *Gestión de Vulnerabilidades*, *Respuesta a Incidentes*, *Continuidad del Servicio*, *Gestión de Riesgos*, *Dependencias Externas*, *Conciencia Situacional*, *Capacitación y Concientización*, etc.) (DC3.MIL, s.f.). Precisamente, la reciente herramienta **Cyber Resilience Analysis (CRA)** del DoD integra 10 dominios alineados con **NIST CSF, NIST 800-171 y CMMC** – evidenciando considerable solapamiento temático entre estos marcos_(DC3.MIL, s.f.)l. La siguiente tabla resume algunos **dominios equivalentes** entre CMMC, NIST CSF y marcos de madurez empleados en CSET:

Tabla 3 Equivalencias ilustrativas entre dominios de CMMC 2.0, categorías del NIST CSF y dominios típicos en modelos de madurez integrados en CSET (como CRR o C2M2).

Dominio CMMC (v2.0)	Categoría/Función NIST CSF	Dominio típico en CSET (CRR/C2M2)
Control de accesos a sistemas e información.	Control de acceso dentro de la función "Proteger"	Incluido en *Gestión de Controles de Seguridad* (p. ej., control de acceso lógico/físico) dentro de dominios de resiliencia.
Respuesta a incidentes de seguridad.	Todas las categorías de la función "Responder" (RS.RP Planificación de respuesta, RS.CO Comunicaciones,	Dominio *Gestión de Incidentes* (CRR) – evalúa planificación, análisis, gestión y aprendizaje de incidentes de ciberseguridad.

	RS.AN Análisis, RS.MI Mitigación, RS.IM Improvements) tratan la respuesta a incidentes.	
Gestión de riesgos de seguridad	Categoría de gestión de riesgos dentro de "Identificar"), en CSF 2.0.	Dominio *Gestión de Riesgos* – evalúa la identificación, análisis y tratamiento de riesgos en procesos críticos.
Inventario y gestión de activos (dominio agregado en CMMC 2.0).	Categoría fundamental del NIST CSF para identificar activos, datos, software y recursos por proteger.	Dominio *Gestión de Activos* – pilar inicial en CRR/C2M2, asegurando conocimiento y control sobre activos de información, personas, tecnologías y instalaciones críticas.
Conciencia situacional de ciberamenazas (dominio agregado).	Relacionado con categorías del CSF orientadas a monitorear eventos de seguridad y fuentes de inteligencia para detección temprana.	Dominio *Conciencia Situacional* – presente en CRR, evalúa la recolección y uso de inteligencia de amenazas, monitoreo activo de redes y el conocimiento del entorno de amenaza por parte de la organización.
Recuperación tras incidentes (dominio agregado).	La función "Recuperar" del NIST CSF (RC) abarca la planificación y ejecución de la restauración de sistemas y operaciones tras incidentes (RC.RP Planes de recuperación, RC.IM Mejoras).	Parte del dominio *Continuidad del Servicio* o *Gestión de la Continuidad* – que en modelos de resiliencia cubre planes de contingencia, backup, recuperación y continuidad operativa luego de interrupciones.
Capacitación y concientización en ciberseguridad.	Categoría que asegura formación de usuarios y proveedores en seguridad.	Dominio *Capacitación y Concientización* – evalúa programas de formación, entrenamientos especializados, ejercicios de concientización (frecuentemente incluido en CRR/C2M2).
Mantenimiento seguro de sistemas.	Controles para realizar mantenimiento con seguridad (ej. restricciones a herramientas de mantenimiento, supervisión).	Usualmente cubierto bajo *Gestión de Configuración y Cambios* – abordando mantenimiento de sistemas, aplicaciones de parches, control de cambios en el entorno técnico.
Seguridad física de instalaciones.	Pueden englobar consideraciones de seguridad física en CSF (no hay categoría específica, pero la protección de infraestructura física está implícita).	Incluido en dominios de *Gestión de Activos* (identificación de instalaciones críticas) y *Controles de Seguridad* (control de acceso físico) en evaluaciones de madurez operacional.

Fuente: Autor, 2025

Como se observa, existe una correspondencia significativa entre los **temas cubiertos** por CMMC y NIST CSF – no en vano CMMC se construyó tomando los controles de NIST SP 800-171, los cuales a su vez derivan de controles NIST 800-53 que fueron considerados en la elaboración del NIST CSFverveindustrial.comverveindustrial.com. Por ejemplo, el dominio **Access Control** de CMMC equivale a garantizar *identificación y control de accesos* (usuarios, dispositivos, sesiones) según NIST CSF, mientras que **Incident Response** se alinea completamente con la función "Responder" del CSF. Ciertas áreas de NIST CSF (como *Governance* en ID.GV, o *Business Environment* ID.BE) no tienen un dominio explícito en CMMC, ya que CMMC se enfocó en controles operativos más que en gestión corporativa; sin embargo, pueden incorporarse vía CSET/CRR bajo prácticas de gobernanza y gestión de riesgo organizacional. **CSET**, al permitir seleccionar múltiples estándares, puede servir de *puente* para **mapear** estos marcos entre sí. Esto facilita que una organización al realizar un **autodiagnóstico con CSET/CRA** conozca su posicionamiento simultáneamente frente a *múltiples marcos*: recibe un

informe que indica el grado de cumplimiento de prácticas CMMC y, a la vez, el estado de sus funciones NIST CSF, todo a partir del mismo set de respuestas.

En cuanto a los **niveles de madurez**: CMMC 2.0 emplea un **modelo de madurez por niveles discretos (1 a 3)**, donde cada nivel añade requisitos más exigentes y presume la implementación de todos los controles de niveles inferiores. Por ejemplo, una organización Nivel 2 debe implementar los controles Nivel 1 (básicos) más todos los de Nivel 2 (equivalentes a 800-171) (COALFIREFEDERAL, 2023). NIST CSF, en lugar de niveles de madurez escalonados por control, propone los **Tiers de Implementación (1 al 4)** que evalúan *cuán institucionalizada* está la gestión de ciberseguridad y riesgo (CSRC.NIST.GOV, 2025). Un **Tier 1 (Parcial)** en NIST CSF indica que la gestión de riesgo es ad-hoc y reactiva, mientras que **Tier 4 (Adaptativo)** implica que la organización no solo gestiona proactivamente el riesgo sino que adapta continuamente sus prácticas con base en lecciones aprendidas y cambios en el entorno de amenazas (CSRC.NIST.GOV, 2025; SPRINTO, 2024). Estos tiers son análogos a evaluar la madurez de procesos (inspirado en modelos CMMI), más que el grado de cumplimiento de controles individuales. Finalmente, CSET frecuentemente incorpora **modelos de madurez por dominio** como el **CRR (Cyber Resilience Review)** o el **C2M2**. Por ejemplo, el **C2M2 (Cybersecurity Capability Maturity Model)** desarrollado para el sector eléctrico define 10 dominios y utiliza **4 niveles de madurez por dominio (MIL0 a MIL3)** (FLEXENTIAL, 2025). El **CRR**, base de la evaluación de resiliencia de CISA, emplea **6 niveles de madurez (MIL0 a MIL5)** para calificar cada dominio, desde *Incompleto (MIL0)* hasta *Gestionado y Sostenible (MIL5)* (CENTRALEYES, s.f.)Estos niveles se centran en la *institucionalización* de las prácticas: por ejemplo, para alcanzar MIL3 en un dominio de CRR, no basta con realizar las prácticas (MIL1) y planificarlas/pautarlas (MIL2), sino que deben gestionarse activamente con los recursos adecuados, medirse y revisarse regularmente (CENTRALEYES, s.f.) .

Figura 1. Comparación resumida entre CMMC 2.0, NIST CSF y C2M2 (estructura de niveles, propósito y aplicabilidad) (FLEXENTIAL, 2025; COALFIREFEDERAL, 2023). CMMC es obligatorio para proveedores del DoD y exige certificación de terceros en niveles altos, mientras NIST CSF es voluntario y adaptable para cualquier organización. Modelos como C2M2 (implementados vía CSET) ofrecen evaluaciones detalladas por dominio con indicadores de madurez MIL.

En suma, **CMMC** aporta la concreción de *qué* controles deben existir a cada nivel de madurez, **NIST CSF** aporta una visión holística de *qué áreas funcionales* cubrir y *cómo mejorar continuamente*, y **los modelos tipo CSET/CRR/C2M2** aportan la medición de *qué tan bien* están implementados e institucionalizados esos controles/procesos en cada dominio. Esta complementariedad sienta las bases para un **modelo híbrido**, como se detalla a continuación.

- ✓ **Alineación con evidencias de MITRE ATT&CK**

Un componente clave para robustecer metodológicamente el modelo híbrido es la integración de **evidencias técnicas basadas en el marco MITRE ATT&CK**. MITRE ATT&CK es una base de conocimiento que clasifica las **tácticas, técnicas y procedimientos (TTPs)** adversarios conocidos, ofreciendo un lenguaje común para describir *cómo* atacantes reales operan (DEV.TO, 2024). Mientras que CMMC y NIST CSF delinean *qué se debe hacer* (controles, procesos) y los modelos de madurez miden *qué tan bien se hace*, **MITRE ATT&CK aporta el contexto de la amenaza**: permite validar si las defensas de la organización cubren las técnicas efectivamente empleadas por los ciberdelincuentes. La integración se logra mediante **mapeos entre controles y técnicas ATT&CK** – un enfoque promovido por iniciativas de *Threat-Informed Defense*. Por ejemplo, en 2022 el Center for Threat-Informed Defense de MITRE publicó un mapeo completo de **controles NIST SP 800-53 a técnicas ATT&CK**, con más de 6.300 vinculaciones (CTID.MITRE, 2024). Dado que NIST 800-171 (y por ende CMMC) es un subconjunto de 800-53, estos mapeos ofrecen un recurso valioso para evaluar **qué tan cubiertas están las técnicas adversarias por los controles implementados** (CTID.MITRE, 2024). En otras palabras, una organización puede tomar sus resultados de cumplimiento (ej. mediante CSET/CMMC) y cruzarlos con ATT&CK para identificar brechas desde la perspectiva de amenazas: si ciertos TTPs críticos no están siendo mitigados o detectados por ninguno de los controles implementados, se evidencia un vacío de seguridad a pesar de que *en papel* se cumplan controles.

Metodológicamente, la alineación con ATT&CK se puede realizar en varios niveles: (1) **Mapeo estático de controles a técnicas**: Por ejemplo, un control de "auditoría de registros" (NIST AC-2(4) o CMMC AU.2.042) se puede mapear a la técnica ATT&CK *T1003: Credential Dumping*, indicando que dicha práctica contribuye a detectar o mitigar esa técnica (SIKICH, 2025). Si la organización no tiene implementado eficazmente el control de auditoría, ATT&CK sugiere que es probable que la

técnica T1003 no pueda ser detectada, lo cual representa un riesgo concreto. (2) **Evaluaciones dinámicas tipo *purple teaming***: usando ATT&CK como guía, se simulan técnicas específicas (ej.: phishing, movimiento lateral, exfiltración de datos) para recolectar evidencia de cómo responden los controles y procesos de la organización. Los resultados de estas simulaciones proveen **evidencia empírica** de la madurez: por ejemplo, si ante un *ataque simulado* de ransomware la organización logra detectar la intrusión (Detect), activar su plan de respuesta (Respond) y restaurar sistemas desde respaldos (Recover), se demuestra en la práctica un nivel de madurez consistente con lo que los documentos y políticas indicaban. En cambio, si falla alguna etapa, se revelan **brechas ocultas** que quizá no se hubieran advertido solo con una revisión documental.

Combinar **NIST CSF y MITRE ATT&CK** crea un vínculo valioso entre la gestión de riesgos estratégica y la inteligencia táctica de amenazas. El NIST CSF proporciona los objetivos de alto nivel (ej. "mejorar capacidades de detección"), mientras que ATT&CK detalla *qué debe saber detectar* el sistema de monitoreo (ej. técnicas de *privilege escalation*, *lateral movement*, etc.) (DEV.TO, 2024). Como señala CloudDefense.AI, *"la sinergia de usar NIST CSF junto con MITRE ATT&CK permite una estrategia integral: el CSF establece los objetivos y estructura de gobierno, mientras ATT&CK proporciona los pasos detallados para lograr esos objetivos"* (DEV.TO, 2024). Esta alineación **metodológica** garantiza que el modelo híbrido no se quede en el nivel teórico de controles, sino que baje al nivel práctico de comprobar su eficacia frente a amenazas reales. Desde una perspectiva de madurez, incorporar evidencias ATT&CK impulsa a la organización hacia niveles superiores (Tier 4 del CSF, o MIL4/5 en resiliencia), ya que promueve la retroalimentación continua: identificar dónde **no hay visibilidad** o **no hay capacidad de respuesta** ante ciertas tácticas adversarias lleva a mejorar controles, procedimientos y entrenamiento de forma dirigida. Un caso documentado mostró que centrar mejoras en TTPs concretas (como *credential dumping*) permitió a una empresa elevar sus puntajes de madurez NIST CSF en categorías de Protección (PR.AC) y Detección (DE.CM) en un año (SIKICH, 2025), evidenciando el impacto positivo de integrar ATT&CK en las evaluaciones de riesgo. Además, ATT&CK ayuda a **priorizar**: de un universo de decenas de controles, la organización puede focalizar primero en aquellos que mitigan técnicas activas contra su industria, logrando una mejora más *precisa* de su postura de seguridad.

En la práctica, existen herramientas y proyectos que ya unen estos mundos. Por ejemplo, la plataforma CSET ha ido incorporando referencias a MITRE ATT&CK en ciertos módulos (como el Ransomware Readiness Assessment, que mapea defensas contra técnicas comunes de ransomware). También se han propuesto extensiones al NIST CSF para incluir consideraciones de amenazas – por caso, **NIST CSF 2.0** incorpora subcategorías referidas a analizar escenarios de adversario e inteligencia de amenazas (ej. ID.RA-6 en el borrador CSF 2.0 enfatiza evaluar escenarios de amenaza)verveindustrial.com. Todo esto refuerza la idea de que un **marco híbrido CSET + CMMC + NIST CSF** alcanza su máximo potencial al enlazarse con **ATT&CK**, asegurando que la evaluación de madurez considere no solo *si la organización cumple controles*, sino *si esos controles funcionan contra las tácticas enemigas conocidas*. En términos académicos, esto se alinea con el enfoque de *"threat-informed defense"*, donde la defensa se evalúa y mejora con base en conocimientos de amenazas actuales (CTID.MITRE, 2024).

- ✓ **Beneficios de un enfoque híbrido y justificación técnico-académica**

Combinar CSET, CMMC y NIST CSF dentro de un modelo híbrido de evaluación de madurez brinda **mayor precisión y profundidad** por varias razones fundamentadas tanto técnicamente como en la literatura académica/industrial reciente:

- **Cobertura integral de dimensiones de ciberseguridad:** Ningún marco individual cubre por completo todas las facetas requeridas para una defensa cibernética sólida. NIST CSF entrega la **cobertura holística** de cinco funciones amplias (incluyendo aspectos de identificación de activos y recuperación, a veces subestimados en enfoques de cumplimiento) (FLEXENTIAL, 2025). CMMC aporta **rigurosidad** y detalle a nivel de controles específicos (ej. requisitos técnicos como cifrado, gestión de claves, control de accesos con múltiples factores, etc.), asegurando que se atiendan medidas concretas de protección de datos sensibles (COALFIREFEDERAL, 2023). Los modelos de madurez tipo CRR/C2M2 (facilitados por CSET) incorporan la **variable procesal y cultural**: evalúan si la organización tiene políticas, asignación de recursos, monitoreo y mejora continua en cada área, más allá de la mera existencia de tecnología o documentos (CENTRALEYES, s.f.). Al combinarse, el modelo híbrido obliga a mirar cada dominio desde *distintas perspectivas complementarias*: p.ej., en

"Respuesta a Incidentes" se verifica que existan procedimientos formales y personal capacitado (madurez de proceso, CRR), que cumplan con controles específicos como notificación y análisis forense (CMMC/800-171), y que cubran efectivamente las amenazas relevantes (ATT&CK – capacidad de responder a ransomware, robos de credenciales, etc.). Esta triangulación elimina puntos ciegos y brinda una evaluación **multidimensional** de la capacidad de ciberseguridad institucional (DEV.TO, 2024).

- **Alineación entre cumplimiento y riesgo real:** Uno de los desafíos conocidos en ciberseguridad es que cumplir con marcos de referencia (compliance) no siempre se traduce en estar protegido contra amenazas reales. El enfoque híbrido mitiga esto al *fusionar el lente del cumplimiento (CMMC/NIST SP 800-171)* con el *lente de la gestión de riesgo continua (NIST CSF)* y con el *lente de inteligencia de amenazas (MITRE ATT&CK)*. Desde una postura académica de gestión de riesgos, este enfoque coincide con principios de **gestión adaptativa** y **defensa en profundidad informada por amenazas** (DEV.TO, 2024; MITRE.ORG, 2024). La precisión mejora porque cualquier discrepancia entre "lo que se pide" y "lo que realmente se necesita" sale a la luz: por ejemplo, CMMC puede requerir un antivirus actualizado (control específico), pero ATT&CK evidenciará si ese antivirus detecta las técnicas actuales de ataque; NIST CSF por su parte exigirá que exista un proceso de mejora si repetidamente alguna amenaza elude las defensas (Tier de mayor madurez). Así, la combinación fuerza una **coherencia** entre las políticas/controles formales y la efectividad práctica, alineando la seguridad con las *necesidades reales de defensa* de la institución (SIKICH, 2025; DEV.TO, 2024).
- **Profundidad en la evaluación y priorización de mejoras:** Academicamente, los modelos de madurez se valoran porque permiten identificar *no solo qué falta*, sino *qué tan bueno es lo que hay*. CMMC por sí solo indicaría faltantes de controles (por ejemplo, si no se tiene un registro de accesos fallidos, no cumples tal práctica). Pero al añadir la escala de madurez CRR/C2M2 vía CSET, incluso si un control existe, se puede puntuar bajo si está pobremente documentado o sostenido. Esto da una **gradación más fina** para priorizar mejoras: quizás una organización cumple todos los controles CMMC Nivel 2, pero su puntuación de madurez CRR revela debilidades en *medición y gestión* en varios dominios (MIL1 o 2 de 5). Por ende, el informe híbrido señalará no solo "qué controles faltan" sino también "en qué controles/procesos se debe mejorar la eficacia o consistencia" (CENTRALEYES, s.f.). Además, al incorporar

métricas de ATT&CK (p. ej. porcentaje de técnicas de una determinada táctica que la organización puede detectar), se priorizan inversiones donde el riesgo es tangible. Esto va en línea con hallazgos de investigaciones que sugieren complementar los **frameworks de control con evaluaciones de amenazas** para lograr mejoras más substanciales en la postura de seguridad (CTID.MITRE, 2024; SIKICH, 2025)

- **Rigurosidad y confianza para entornos institucionales:** En entornos públicos o gubernamentales, a menudo existe el mandato de seguir marcos como NIST CSF (por su reconocimiento internacional) y ahora CMMC para ciertas entidades o proveedores. Un modelo híbrido permite cumplir con estas obligaciones de una forma **integrada**, evitando duplicación de esfuerzos. Por ejemplo, una entidad pública puede ejecutar una sola evaluación con CSET que simultáneamente le genere *perfil NIST CSF*, *scoring CMMC* y *reporte de madurez CRR*, ahorrando recursos y facilitando la comunicación de resultados a diferentes audiencias (directivos estratégicos entenderán el nivel CSF, auditores de cumplimiento verán el nivel CMMC, equipos técnicos accionarán sobre hallazgos ATT&CK). Desde la perspectiva académica de administración pública, esto aporta **eficiencia** y **transparencia** al proceso de evaluación de la ciberseguridad institucional. Adicionalmente, la profundidad extra del enfoque híbrido fortalece la **justificación técnica** ante terceros: por ejemplo, ante órganos de control o financiadores, la institución puede demostrar con evidencia que no solo cumple cierta normativa, sino que ha testeado sus capacidades contra escenarios de ciberataque realistas – lo cual tiende a generar mayor confianza en la resiliencia reportada.

En conjunto, las sinergias entre los marcos quedan respaldadas por iniciativas recientes. El **Departamento de Defensa de EE.UU.** con su programa **Análisis de resiliencia cibernética (CRA)** en 2024 adoptó explícitamente un enfoque unificado: su herramienta CRA evalúa 10 dominios que *"se alinean con NIST CSF, NIST 800-171 y CMMC"*, proporcionando resultados cruzados (DC3.MIL, s.f.). Esto fue diseñado para ayudar a las empresas del DIB (Defense Industrial Base) a *"llevar su ciber resiliencia al siguiente nivel"* (DC3.MIL, s.f.), combinando requisitos de cumplimiento con resiliencia operativa. Asimismo, organizaciones asesoras en ciberseguridad recomiendan **mapear CMMC con NIST CSF** para enriquecer el entendimiento de ambos (VERVEINDUSTRIAL, 2019), e incluso **extender NIST CSF con controles de 800-171B** para cubrir escenarios avanzados no descritos originalmente en

CMMCverveindustrial.comverveindustrial.com. Toda esta convergencia conceptual sugiere que la comunidad profesional y de investigación reconoce el valor de **combinar marcos** en vez de usarlos de forma aislada. El enfoque híbrido CSET–CMMC–CSF–ATT&CK se alinea con las mejores prácticas emergentes de evaluar la ciberseguridad de manera *integral, basada en riesgo y evidencia*, superando la visión siloed de cumplimiento puro.

- ✓ **Aplicación del modelo híbrido en entornos públicos simulados**

Consideremos cómo implementar este modelo híbrido en un **entorno institucional público** (por ejemplo, un ministerio, una empresa pública o una universidad estatal) mediante un ejercicio simulado:

1. **Selección y personalización del marco híbrido:** La institución escoge adoptar el **NIST CSF** como marco madre para organizar su programa de seguridad (dado que es reconocido en políticas públicas). A la vez, si está en la órbita del sector defensa o maneja información sensible, decide que debe alcanzar **CMMC Nivel 2** para ciertas áreas. Con apoyo de CSET, configura una evaluación que incluya el **cuestionario de CMMC** y adicionalmente active la opción de **mapeo a NIST CSF** y/o use el **cuestionario de CRA/CRR** para medir madurez por dominio. Este paso equivale a definir el "perfil híbrido" a medir.

2. **Ejecución de la evaluación simulada:** Se realiza un **ejercicio de autoevaluación** en un contexto simulado (por ejemplo, durante un **ciber simulacro** o *table-top exercise* institucional). Los responsables de cada área responden a las preguntas de CSET, proporcionando evidencia de sus prácticas. Por ejemplo, el área de TI responde si tiene control de cuentas privilegiadas (CMMC AC.1.001), el área de capacitación indica si hay programas regulares de concientización (CMMC AT.2.056), etc. CSET recopila y al final genera un **informe multi-marca**. Gracias al mapeo interno, el informe podría indicar: "Dominio CMMC: Access Control = 70% implementado, corresponde a función **Protect** del NIST CSF la cual está 'Parcialmente Implementada' (Tier 2) en subcategoría PR.AC; Madurez CRR en *Controles de Acceso* = MIL2 (Planificado pero no completamente gestionado)". De esta

manera, los directivos obtienen un cuadro claro de *dónde se encuentran* en la escala de madurez.

3. **Incorporación de escenarios ATT&CK:** Como parte del ejercicio, el equipo rojo/azul de la institución simula uno o dos escenarios de ataque relevantes mapeados en MITRE ATT&CK (por ejemplo, un ataque de phishing que conduce a ejecución de malware de cifrado). Se observa cómo responden los controles existentes: ¿El SOC detectó la intrusión (DE?CM)? ¿Se bloqueó la ejecución maliciosa (PR?PT)? ¿Se siguió el plan de respuesta a incidentes (RS.RP)? Los hallazgos de esta simulación se correlacionan con las puntuaciones de la evaluación. Quizá la evaluación CMMC indicó que había un antivirus actual (control SI.3.219) – pero la simulación revela que no detuvo la técnica T1059 (command-line scripting) usada por el malware. Esto generará una *recomendación específica* en el informe: mejorar el control X o implementar una capacidad adicional (ej. EDR, monitoreo de scripting). Este paso añade realismo a la simulación y entrena a la organización en manejar incidentes, a la vez que valida o refuta supuestos de la autoevaluación.

4. **Plan de mejora híbrido:** Con los resultados, la institución elabora un **plan de acción** priorizado. Las **brechas de cumplimiento CMMC** (controles "No Implementados") se abordan para alcanzar el nivel requerido – esto asegura *cumplimiento normativo*. Las **brechas de madurez** identificadas (dominios con bajo MIL o Tier) se traducen en proyectos de fortalecimiento de procesos: por ejemplo, formalizar la gestión de parches (si Vulnerability Management salió en MIL1), o instituir métricas e informes periódicos de seguridad a la alta gerencia (si Governance salió Tier 1). Finalmente, las **brechas de amenaza** (técnicas ATT&CK no mitigadas) se abordan implementando contramedidas concretas: quizá mejorar reglas SIEM para detectar movimiento lateral, o invertir en capacitación contra phishing dirigido si se evidenció debilidad allí. Gracias a la estructura híbrida, el plan de mejora queda **trazable** a objetivos de alto nivel (funciones CSF), a requisitos concretos (controles CMMC) y a escenarios de riesgo (ATT&CK), lo cual facilita su justificación ante autoridades y su comprensión por todo el personal involucrado.

5. **Reevaluación y ciclo continuo:** Tras un periodo (6-12 meses), se repite la evaluación simulada para medir progreso. Idealmente, la institución verá elevarse su madurez en varios dominios (p. ej. pasar de MIL2 a MIL3 en *Respuesta a Incidentes* gracias a la institucionalización de lecciones aprendidas) (CENTRALEYES, s.f.), acercándose quizás a Tier 3 del NIST CSF (procesos *repeatable* y gestionados) (SPRINTO, 2024). Asimismo, al haber cerrado brechas críticas, las simulaciones ATT&CK mostrarán menos impactos no contenidos. Esto refuerza un **ciclo de mejora continua** – principio rector tanto del NIST CSF como de los modelos de calidad/madurez en los que se basa CSET.

En un entorno público real, este enfoque híbrido permite **simular el cumplimiento de múltiples exigencias** (por ejemplo, una agencia gubernamental puede autoevaluarse para estándares nacionales equivalentes a NIST CSF, y simultáneamente verificar si cumpliría con CMMC en caso de aspirar a contratos federales). También facilita comunicar resultados a distintos stakeholders: se puede reportar un *score* de madurez global al gobierno central usando el lenguaje NIST CSF (e.j. "estamos Tier 2 acercándonos a Tier 3" en gestión de riesgo), mientras internamente los equipos técnicos trabajan con el detalle de controles CMMC a implementar o mejorar, y los equipos de monitoreo usan ATT&CK para afinar detecciones. Dado que el modelo híbrido está soportado por herramientas como CSET, su implementación es viable sin necesidad de desarrollar metodologías desde cero; al contrario, **consolida las mejores prácticas existentes** en una sola evaluación coherente.

La articulación conjunta de CSET, CMMC y NIST CSF – potenciada con la alineación a MITRE ATT&CK – proporciona un **modelo híbrido de evaluación de madurez en ciberseguridad** sumamente robusto. A través de este enfoque, una organización puede **mapear su posición actual** en términos de gobierno de seguridad (NIST CSF), **cumplimiento de controles fundamentales** (CMMC/NIST 800-171) y **madurez de implementación** (CRR/C2M2 via CSET), todo mientras comprueba su eficacia contra **escenarios de amenaza reales** (ATT&CK). La comparación estructurada entre marcos mostró que existen claras sinergias: CMMC y NIST CSF comparten muchos dominios/funciones equivalentes, y CSET permite integrar evaluaciones multi-marco sinérgicas. Las tablas de equivalencia presentadas evidencian cómo los dominios clave se relacionan unos con otros, facilitando *traducciones* entre el lenguaje de gestión de riesgos y el lenguaje de cumplimiento técnico. Desde una perspectiva académica y técnica, combinar estos marcos atiende las

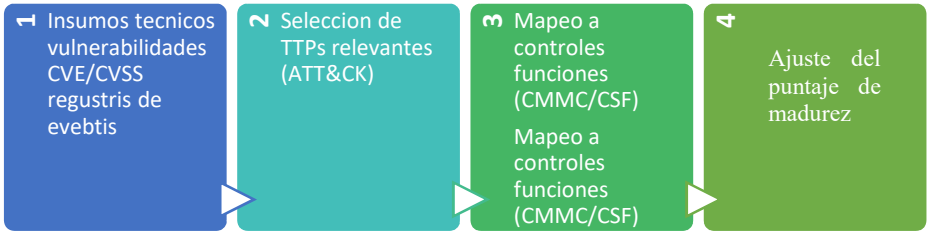
críticas habituales de cada uno por separado – se evita que NIST CSF quede demasiado *alto nivel* o teórico al vincularlo con controles concretos de CMMC; se evita que CMMC sea una mera *lista de verificación* al incorporarle la dimensión de madurez de procesos y la adaptación a riesgos cambiantes promulgada por CSF; y se trasciende el enfoque *estático* de cualquier marco al introducir la dinámica de amenazas reales vía ATT&CK. El resultado es una evaluación más **precisa** (porque refleja fielmente las capacidades y brechas reales, no solo documentos) y más **profunda** (porque indaga en la calidad y efectividad de cada control/proceso, no solo en su existencia). Esto redunda en recomendaciones más acertadas y en una mejora continua más dirigida.

Para instituciones públicas o entornos gubernamentales, un modelo híbrido así orientado ofrece un camino práctico para **fortalecer la ciberseguridad institucional** de forma integral. Permite cumplir con lineamientos normativos (ej. marcos nacionales basados en NIST CSF o exigencias tipo CMMC) al mismo tiempo que garantiza que esas inversiones se traduzcan en **resiliencia tangible** contra las ciberamenazas que enfrentan. Además, en simulaciones o evaluaciones periódicas, provee un instrumento pedagógico: al involucrar múltiples áreas (riesgos, TI, operaciones, alta gerencia) bajo un mismo paraguas evaluativo, fomenta una *cultura de ciberseguridad* más madura y compartida.

3.4 INTEGRACIÓN CON EL MARCO MITRE ATT&CK Y ANÁLISIS TÉCNICO

Esta sección integra el marco **MITRE ATT&CK** al análisis técnico de la evaluación, con el fin **de conectar los resultados de madurez** (documentales) con **evidencia empírica** sobre cómo se comportan los adversarios en escenarios reales. El enfoque es **informado por amenazas** (threat-informed defense): no basta declarar que un control existe; es necesario verificar qué tácticas y técnicas (TTPs) cubre, qué detecta y qué mitiga. Todo el ejercicio se plantea en entorno simulado, tal como exige el alcance del estudio y las indicaciones de la tutora.

Figura 7. Conducción de Integración



Fuente: Autor, 2025

3.4.1 Selección de tácticas y técnicas relevantes (ATT&CK)

Para el entorno institucional simulado se definió un **perfil de amenaza** sintético A partir de ese perfil se seleccionó un subconjunto de **tácticas** y **técnicas** de ATT&CK con mayor probabilidad/impacto en entidades públicas:

- **Acceso inicial (Initial Access):** Técnica T1566 – Suplantación o fraude por correo electrónico (Phishing) y T1190 – Explotación de aplicaciones expuestas al público (Exploitation for Public-Facing Application).
- **Ejecución (Execution):** Técnica T1059 – Intérprete de comandos y secuencias de ejecución (Command and Scripting Interpreter).
- **Persistencia / Evasión de defensas (Persistence / Defense Evasion):** Técnicas T1547 – Ejecución automática en el arranque o inicio de sesión (Boot or Logon Autostart Execution) y T1070 – Eliminación de indicadores (Indicator Removal).
- **Descubrimiento y movimiento lateral (Discovery / Lateral Movement):** Técnicas T1087 – Descubrimiento de cuentas (Account Discovery) y T1021 – Uso de servicios remotos (Remote Services).
- **Exfiltración / Comando y control (Exfiltration / Command and Control):** Técnicas T1041 – Exfiltración de datos a través del canal de comando y control (Exfiltration Over C2 Channel) y T1071 – Uso del protocolo de capa de aplicación.

3.4.2 Matriz de cobertura y detección (plantilla)

Para cada técnica seleccionada se elaboró una **matriz de cobertura** que relaciona: (a) **detección** (si existen reglas, telemetría o alertas), (b) **prevención/mitigación** (controles efectivos), y (c) **respuesta** (procedimientos y tiempos). La matriz permite calcular indicadores de **cobertura técnica** y **capacidad de respuesta**.

Tabla 4 Matriz de cobertura ATT&CK

Táctica	Técnica (ID)	¿Detecta? (S/N)	Evidencia de detección (fuente)	¿Previene/Mitiga? (S/N)	Control asociado	¿Procedimiento de respuesta? (S/N)	Tiempo estimado de respuesta
Acceso Inicial	T1566 Phishing	Si	Correo/SEG/SIEM	Si	Filtro antiphishing n + SEG + MFA	S	< 4 h
Ejecución	T1059 Scripting	N	—	Parcial	Políticas restrictivas	N	—
Movimiento Lateral	T1021 Remote Services	No	—	No	Fortalecimiento (Hardening) + RBAC + cierre de puertos	Parcial	> 24 h

Fuente: Autor, 2025

- ✓ **Phishing (T1566):** Se *detecta* porque el SEG marca y el SIEM correlaciona eventos sospechosos; se *mitiga* combinando SEG + **MFA** (aun si cae el usuario, el acceso no se completa). Existe **procedimiento** (aislación del buzón, bloqueo del remitente, notificación a usuarios) con SLA **< 4 h**.
- ✓ **Ejecución por scripting (T1059):** No se *detecta* (no hay alertas en SIEM/EDR); la *mitigación* es **parcial** (existen reglas de AppLocker/EDR, pero no uniformes); **no** hay **procedimiento** formal para contención/verificación forense.
- ✓ **Servicios remotos (T1021):** No se *detecta* (no hay monitoreo de intentos RDP/SMB anómalos); **no** se *mitiga* de forma consistente (faltan MFA, listas de control de acceso estrictas y telemetría); hay un *procedimiento parcial* (desconexión de sesión / restablecimiento de credenciales), con SLA **> 24 h** por falta de automatización.

- **Cobertura de técnicas** (Techique Coverage, TC);

$$\boldsymbol{TC} = \frac{\#\ tecnicas\ con\ detección = Si}{\#\ tecnicas\ evaluadas}$$

- **Capacidad de respuesta** (Response Readiness, RR);

$$\boldsymbol{TC} = \frac{\#\ tecnicas\ de\ Procedimiento = Si}{\#\ tecnicas\ evaluadas}$$

3.4.3 Rúbrica y ponderación: impacto técnico en el puntaje de madurez

Para integrar objetivamente la evidencia técnica al **puntaje de madurez**, se utiliza una **rúbrica ponderada**. Se proponen tres componentes:

1. **Madurez documental** (MD) – resultado de CSET/CMMC/CSF por dominio.
2. **Cobertura técnica** (TC) – proporción de técnicas evaluadas con *detección efectiva*.
3. **Capacidad de respuesta** (RR) – proporción de técnicas con *procedimiento y tiempos* definidos.

Fórmula de puntaje híbrido por dominio (PH):

$$PH_D = \omega_{MD} * MD_d + \omega_{TC} * TC_d + \omega_{RR} * RR_d$$

Con pesos recomendados para entornos institucionales:

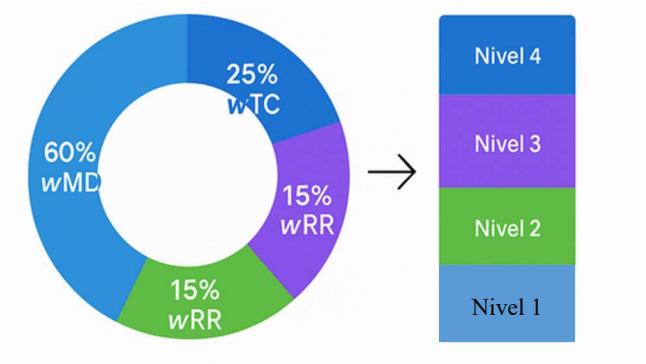
- ω MD=0.5w_{MD}=0.5wMD=0.5 (cumplimiento y procesos importan)
- ω TC=0.3w_{TC}=0.3wTC=0.3 (detección real pesa)
- ω RR=0.2w_{RR}=0.2wRR=0.2 (capacidad de respuesta operativa)

Reglas de cautela (umbral): para **Nivel alto** no debe haber *técnicas críticas sin detección* ni *vulnerabilidades críticas abiertas* (condición bloqueante).

Conversión a niveles de madurez (escala 1–5):

- **Nivel 1 (Inicial):** PH < 0,30
- **Nivel 2 (Gestionado):** 0,30 ≤ PH < 0,50
- **Nivel 3 (Definido):** 0,50 ≤ PH < 0,70
- **Nivel 4 (Medido):** 0,70 ≤ PH < 0,85 y sin bloqueos
- **Nivel 5 (Optimizado):** PH ≥ 0,85 y sin bloqueos

Figura 8. Esquema de Rubricas y pesos



Fuente: Autor, 2025

Nivel 4– Azul oscuro → corresponde a *wMD 60%* (mayor madurez documental).

Nivel 3 – Morado → estandarización de procesos.

Nivel 2 – Verde → capacidades básicas / respuesta inicial (*wRR 15%*).

Nivel 1 – Azul medio → transición a validación técnica (*wTC 25%*).

3.4.4 Procedimiento en entorno simulado

Para cumplir el alcance metodológico:

- **Sin impacto en producción**: todo se ejecuta en laboratorio (clon/VM).
- **Autorización académica**: documentación de alcance y control de evidencias.

- **Trazabilidad**: cada hallazgo técnico se etiqueta con *fecha, activo simulado, técnica ATT&CK, control CSF/CMMC asociado*.
- **Reporte**: matriz ATT&CK (3.4-B), *cross-walk* (3.4-C) y PH por dominio.

Tabla 5 Checklist de ejecución segura

Ítem	Descripción
Autorización	Se cuenta con la debida autorización para simular evaluaciones técnicas
Alcance	Se define el ámbito y limites de pruebas de la integración propuestas
Dataset Simulado	Se alimenta el modelo exclusivamente con vulnerabilidades simuladas
Control de Logs	Los registros de eventos (logs) son gestionados y supervisados adecuadamente
Descarte seguro	Se eliminan los datos generados por la ejecución tras su análisis

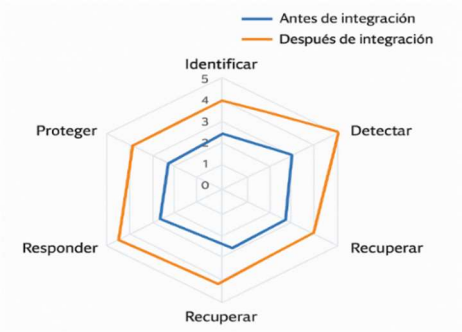
Fuente: Autor, 2025

3.4.5 Discusión y valor añadido en el contexto institucional

La integración con ATT&CK aporta tres **beneficios prácticos** al diagnóstico de madurez:

- ✓ **Reduce el sesgo de auto-reporte**: evidencia empírica corrige sobre-estimaciones documentales.
- ✓ **Prioriza inversiones**: mapea brechas a TTPs con impacto demostrado en el sector público
- ✓ **Cierra el ciclo de mejora continua**: los déficits en *Detectar/Responder* se traducen en proyectos concretos (reglas SIEM/EDR, procedimientos, capacitación), elevando el nivel de madurez de forma **medible**

Figura 9. Radar de integración de MITRE ATT&CK



Fuente: Autor, 2025

3.5 PROPUESTA METODOLÓGICA DEL MODELO HÍBRIDO DE MADUREZ EN CIBERSEGURIDAD: INTEGRACIÓN NORMATIVA Y TÉCNICA

En esta sección se presenta la propuesta central del presente trabajo de investigación, correspondiente al Modelo Híbrido de Madurez Cibernética para Entidades Gubernamentales (MHMC-EG). Este modelo integra los resultados de los marcos normativos y técnicos analizados en los apartados anteriores **(CSET, CMMC, NIST CSF y MITRE ATT&CK)** con el propósito de establecer una metodología unificada y medible para evaluar la madurez en ciberseguridad institucional.

El MHMC-EG constituye un instrumento metodológico de diagnóstico y mejora continua, diseñado específicamente para entornos gubernamentales, en los cuales se busca trascender el cumplimiento formal y avanzar hacia una gestión basada en evidencia técnica. La propuesta combina la dimensión normativa (orientada al cumplimiento y la gobernanza) con la dimensión técnica (centrada en la verificación empírica de los controles), garantizando que los resultados obtenidos reflejen la realidad operativa y la capacidad de respuesta de la organización frente a amenazas cibernéticas. A continuación, se detallan los fundamentos conceptuales, la arquitectura metodológica y las fases operativas que estructuran el modelo MHMC-EG, como contribución académica y práctica para la evaluación integral de la madurez cibernética en instituciones públicas.

3.5.1 Fundamentación general del modelo MHMC-EG

El modelo **MHMC-EG** organiza la madurez cibernética en cinco niveles progresivos (Inicial, Gestionado, Definido, Medido y Optimizado) y seis dominios de evaluación, derivados de la correlación entre **CSET, NIST CSF y CMMC 2.0.**

Cada dominio agrupa un conjunto de preguntas guía que permiten medir tanto el cumplimiento documental como la eficacia técnica; se presenta una matriz general del modelo con sus niveles, dominios y ejemplos de indicadores evaluables.

Tabla 6. Matriz general del modelo MHMC-EG: niveles, dominios y preguntas guía

Dominio / Dimensión	Descripción del dominio	Ejemplo de preguntas guía	Nivel 1: Inicial	Nivel 2: Gestionado	Nivel 3: Definido	Nivel 4: Medido	Nivel 5: Optimizado
1. Gobernanza y Gestión de Riesgos	Define políticas, roles y responsabilidades para la gestión de la ciberseguridad.	¿Existen políticas de seguridad formalmente aprobadas? ¿Se evalúan los riesgos anualmente?	No hay políticas documentadas.	Políticas básicas sin revisión periódica.	Políticas aprobadas, con roles asignados.	Políticas revisadas con métricas.	Gobernanza integral basada en riesgo continuo.
2. Protección de Activos e Infraestructura	Incluye controles técnicos para proteger sistemas, redes y datos.	¿Se gestionan parches y respaldos de forma programada?	Controles ad-hoc.	Inventario parcial de activos y respaldos semanales.	Gestión formal de parches y backups.	Controles automatizados.	Controles basados en riesgo y auditorías trimestrales.
3. Detección y Monitoreo	Evaluación de la capacidad de identificar incidentes.	¿Existen sistemas de monitoreo (SIEM, alertas)?	No hay monitoreo formal.	Monitoreo parcial sin métricas.	SIEM activo con revisiones diarias.	Análisis de tendencias y correlaciones.	Detección predictiva basada en inteligencia de amenazas.
4. Respuesta a Incidentes	Mide la capacidad de actuar frente a eventos de seguridad.	¿Existe un plan de respuesta y personal entrenado?	Reacción ad-hoc.	Procedimiento básico, no probado.	Plan documentado y roles definidos.	Pruebas regulares y métricas de respuesta.	Simulaciones periódicas tipo Red/Blue Team.
5. Recuperación y Continuidad	Evalúa la capacidad para restaurar operaciones tras incidentes.	¿Se dispone de un plan de recuperación ante desastres?	No existen copias formales.	Respaldos sin prueba de restauración.	Plan de recuperación documentado.	Pruebas anuales exitosas.	Continuidad integrada con resiliencia organizacional.
6. Conciencia y Capacitación	Considera la cultura organizacional y el factor humano.	¿Se realizan campañas de sensibilización?	No se capacita al personal.	Capacitaciones esporádicas.	Plan anual de formación en seguridad.	Seguimiento de efectividad (encuestas, KPI).	Cultura institucionalizada de seguridad.

Fuente: Autor, 2025 - basada en la integración de CSET, CMMC 2.0, NIST CSF 2.0 y MITRE ATT&CK (2025).

El MHMC-EG combina ambos mundos:

1. **La dimensión normativa y de gestión**, sustentada en marcos consolidados (CSET, CMMC 2.0 y NIST CSF 2.0).
2. **La dimensión técnica y empírica**, sustentada en evidencias reales obtenidas mediante metodologías informadas por amenazas (MITRE ATT&CK, análisis de vulnerabilidades y ejercicios de simulación controlada).

Esta convergencia permite que las evaluaciones de madurez no se limiten a la "existencia" de políticas o procedimientos, sino que reflejen **la efectividad práctica** de los controles frente a tácticas adversarias observadas.

El modelo se estructura como un **sistema modular** adaptable a distintos organismos públicos, integrando los siguientes componentes:

Tabla 7. Sistema Modular

Componente	Marco de referencia	Propósito en el modelo MHMC-EG
CSET	CISA – herramienta de evaluación	Plataforma base para recolectar evidencias normativas y técnicas.
CMMC 2.0	DoD / NIST 800-171	Define niveles de madurez y controles verificables.
NIST CSF 2.0	NIST	Proporciona las funciones macro (*Identify, Protect, Detect, Respond, Recover*).
MITRE ATT&CK	MITRE CTID	Traduce las amenazas reales en tácticas/técnicas medibles y mapeables.
Evidencia empírica	Análisis de vulnerabilidades, pentesting ético	Contrasta la efectividad de los controles y alimenta la puntuación técnica.

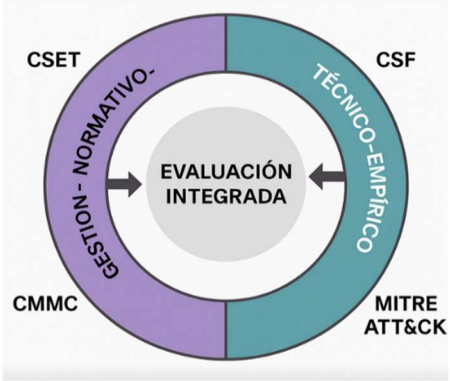
Fuente: Autor,2025

El principio rector del MHMC-EG es la **correlación entre el cumplimiento formal y la evidencia empírica**. De esta manera, la madurez organizacional se calcula ponderando la coherencia entre ambos tipos de evidencia.

3.5.2 Arquitectura metodológica del modelo

El modelo MHMC-EG adopta el ciclo PDCA (Planificar, Hacer, Verificar, Actuar) como enfoque metodológico de mejora continua. Este ciclo guía la aplicación del modelo en iteraciones anuales o semestrales, donde se planifica la evaluación, se ejecuta la medición, se verifican los resultados y se actúa corrigiendo o fortaleciendo controles. En la **Figura 10** se muestra cómo las dos dimensiones del modelo (Normativa–Gestión y Técnica–Empírica) se integran dentro de este ciclo de mejora continua.

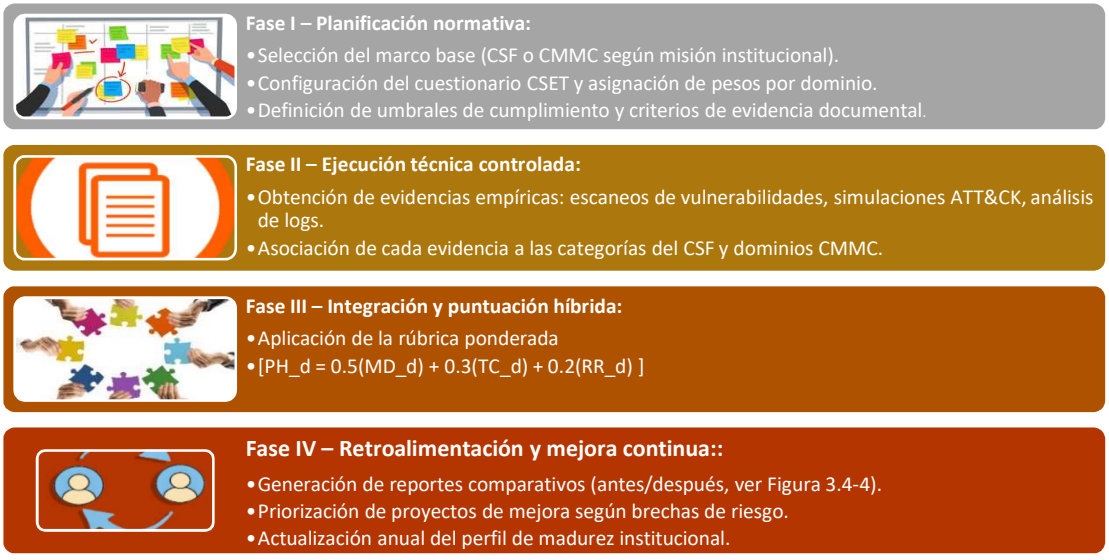
Figura 10. Integración de las dimensiones Normativa y Técnica del modelo MHMC-EG dentro del ciclo PDCA de mejora continua.



Fuente: Autor, 2025

Nota: El ciclo PDCA no sustituye los modelos de madurez (CSET, CMMC, CSF o ATT&CK), sino que proporciona la estructura metodológica que orienta su aplicación y revisión continua en cada iteración del modelo MHMC-EG.

Figura 11. Fases de ciclo de madurez MHMC - EG



Fuente: Autor 2025

3.5.3 Dimensión normativa y gestión (CSET + CMMC + CSF)

La primera dimensión del modelo corresponde al **componente normativo**, que define la estructura de referencia para medir el grado de implementación de políticas, procedimientos y controles administrativos.

- **CSET** actúa como instrumento de levantamiento y mapeo cruzado entre marcos.
- **CMMC** aporta los niveles de madurez progresiva (1–3 para entornos públicos) y las prácticas verificables.
- **NIST CSF** organiza la información por funciones y categorías, garantizando trazabilidad con estándares internacionales.

El resultado de esta dimensión es una **puntuación documental (MD)** que cuantifica la existencia, aplicabilidad y actualización de controles de seguridad institucional.

3.5.4 Dimensión técnica y evidencia empírica (MITRE ATT&CK)

La segunda dimensión incorpora el factor técnico-operativo: las pruebas de efectividad de los controles mediante mapeo a tácticas y técnicas ATT&CK. Cada técnica relevante se evalúa según tres criterios: detección, mitigación y respuesta. Los resultados se traducen en los índices TC y RR integrados en la fórmula anterior.

Este componente valida si las capacidades declaradas en políticas realmente **detectan y mitigan técnicas adversarias**. Su peso del 30 % (*TC*) y 20 % (*RR*) responde a la necesidad de reflejar la eficacia práctica sin desbalancear la importancia de la gobernanza.

3.5.5 Niveles y criterios de madurez

La evaluación de madurez del modelo MHMC-EG se estructura en **cinco niveles progresivos**, que reflejan la evolución institucional desde una gestión reactiva y desorganizada hasta una madurez optimizada basada en mejora continua.

Cada nivel combina **controles técnicos, procedimientos administrativos y capacidades operativas** alineadas a los marcos CMMC y NIST CSF. A continuación, se detallan los niveles, con ejemplos específicos de controles, políticas y prácticas asociadas.

Tabla 8. Niveles de criterios de madurez MHMC - EG

Nivel	Denominación	Características principales
1	Inicial	Controles ad-hoc, sin planificación ni documentación formal. No existe inventario de activos ni clasificación de información. La seguridad depende de acciones reactivas del personal técnico ante incidentes. Ejemplo: respuesta informal ante malware o caídas de red; ausencia de SOC (Centro de Operaciones de Seguridad), CSIRT (Equipo de Respuesta a Incidentes) o CERT institucional.
2	Gestionado	Se implementan políticas básicas de seguridad sin evaluación técnica formal. Ejemplos: política de contraseñas, respaldo manual de información, acceso restringido por usuario, control de uso de dispositivos USB, y antivirus instalado. No se validan métricas de efectividad ni simulaciones de ataque.
3	Definido	Se establecen procesos y procedimientos estandarizados para gestionar la seguridad. Ejemplos: plan de respuesta a incidentes, gestión de parches, clasificación de datos, uso de SIEM (Security Information and Event Management) para monitoreo básico, y evidencia parcial de eficacia de controles.
4	Medido	Los controles y procesos son validados técnica y documentalmente. Existen indicadores de desempeño (KPI/KRI) y monitoreo continuo. Ejemplos: escaneos periódicos de vulnerabilidades, pruebas de penetración anuales, correlación activa de eventos, auditorías internas, métricas de cumplimiento.
5	Optimizado	La mejora continua está institucionalizada mediante análisis de amenazas, lecciones aprendidas y simulaciones avanzadas. Ejemplos: ejercicios de Red Team / Blue Team, automatización de respuesta a incidentes, inteligencia de amenazas (Threat Intelligence), y ciclos PDCA aplicados en la gestión de seguridad.

Fuente: Autor, 2025 con base en CMMC 2.0, NIST CSF 2.0, CSET y MITRE ATT&CK (2025).

Los niveles del MHMC-EG no solo describen el grado de cumplimiento documental, sino también la capacidad práctica de la organización para anticipar, detectar y responder ante incidentes cibernéticos.

A diferencia de modelos puramente normativos, este enfoque incorpora validaciones técnicas derivadas de los ejercicios ATT&CK y los resultados de escaneos de vulnerabilidades, lo que permite que la madurez refleje evidencia comprobable y no percepción declarativa.

En entornos institucionales, alcanzar un nivel 4 o 5 implica la existencia de capacidades formales de monitoreo, respuesta y mejora continua, respaldadas por roles definidos y métricas objetivas.

3.5.6 Validación y aplicabilidad institucional

El MHMC-EG está diseñado para ser **replicable y auditable** en distintas entidades públicas del Ecuador o de la región. puede aplicarse:

- Como **autoevaluación interna**, usando CSET con el perfil híbrido configurado.
- Como **evaluación externa**, dirigida por auditores o el Comité de Seguridad de la Información.
- Como **instrumento de seguimiento** del cumplimiento del **EGSI v3.0**, ya que su lógica de mejora continua y verificación técnica complementa las exigencias de dicho esquema.

El modelo se valida a través de:

1. **Pruebas de consistencia interna** (coeficiente α de Cronbach ≥ 0.70 en cuestionarios).
2. **Comparación longitudinal** (evolución del puntaje híbrido PH entre ciclos).
3. **Revisión por pares técnicos** (verificación cruzada de evidencias por expertos).

3.5.7 Discusión final

El MHMC-EG ofrece a los gobiernos locales un marco **escalable, medible y adaptable**, permitiendo pasar de diagnósticos declarativos a **evaluaciones basadas en evidencia**. Integra la lógica del **cumplimiento normativo (qué debe existir)** con la **verificación empírica (qué realmente funciona)**. Su estructura modular facilita futuras extensiones.

Desde la perspectiva académica, el modelo constituye una **propuesta metodológica original** que unifica los principios de la gestión de riesgos (NIST CSF), los niveles de madurez procesal

(CMMC/C2M2), la verificación empírica (ATT&CK) y la medición cuantitativa (rúbrica ponderada), articulando teoría, práctica y evaluación estadística.

En términos prácticos, su adopción permitiría a entidades como el GAD Municipal de Baba medir objetivamente su progreso anual en seguridad de la información, priorizar recursos y alinear sus planes de mejora con estándares internacionales y requerimientos nacionales.

CONCLUSIONES

- El Modelo Hibrido de Madurez Cibernética es un método completo y flexible para superar las limitaciones del modelo tradicional de ciberseguridad. La combinación de reglas (CSET, CMMC, NIST CSF) con pruebas tecnológicas (MITRE ATT&CK, verificación de vulnerabilidad) permite medir qué tan madura es una institución, tanto siguiendo las reglas como qué tan bien funcionan los controles en la realidad.

- Las evaluaciones gubernamentales generalmente verifican el papeleo, pero el Modelo Híbrido de Madurez Cibernética para las Entidades Gubernamentales ofrece una forma más clara y justa de verificarlo, al incorporar métricas de desempeño técnico y evidencia simulada de ataque/defensa, el modelo promueve la responsabilidad y prioriza las inversiones en seguridad.

- Esta ponderación prioriza la madurez documental, pero aún valora la detección y la respuesta operativa. La fórmula híbrida hace que la evaluación sea más objetiva y menos subjetiva que las autoevaluaciones.

- Puede aplicarse en diversos sectores públicos o privados, ajustando la complejidad del análisis al tamaño e importancia de la institución. Los resultados se verifican con pruebas de consistencia interna (Alfa de Cronbach) y se realiza un seguimiento del progreso a lo largo del tiempo.

- El modelo ofrece una forma nueva y repetible para futuras investigaciones sobre la madurez de la ciberseguridad. El Modelo Hibrido de Madurez Cibernética ofrece una combinación equilibrada de cumplimiento, riesgo y pruebas técnicas, lo que ayuda a elaborar políticas nacionales de ciberseguridad y refuerza marcos como EGSI v3.

RECOMENDACIONES

- Aplicar los inicios del Modelo Híbrido de Madurez Cibernética en modo piloto en áreas clave (como infraestructura tecnológica o privacidad de datos), para verificar la usabilidad y ajustar los pesos de las rúbricas para que coincidan con las operaciones del mundo real de cada entidad

- Para la correcta aplicación del modelo, es fundamental que tanto los gestores TIC como los funcionarios administrativos comprendan los marcos de referencia utilizados (CSET, CMMC, CSF, ATT&CK) y su interrelación. La formación dual (normativa y técnica) aumenta la coherencia y la fiabilidad de la evaluación.

- La metodología propuesta puede incorporarse como una herramienta complementaria dentro del proceso de cumplimiento de EGSI, fortaleciendo el componente de mejora continua y la validación empírica de los controles definidos en dicho esquema

- Fomentar el registro voluntario de los resultados de madurez en las organizaciones en formato estándar, permitiendo comparaciones sectoriales y regionales

- MITRE ATT&CK- Las simulaciones y entornos virtuales deben ser parte de las evaluaciones anuales Esto ayuda a detectar puntos débiles temprano y mantener fuerte la defensa

- Utilizar el Modelo Híbrido de Madurez Cibernética utilizado para diseñar un marco nacional de madurez en ciberseguridad, unificando criterios de evaluación, mejorando la interoperabilidad y fortaleciendo las organizaciones sirviendo como guía estatal de ciberresiliencia.

REFERENCIAS

(UNAD), U. N. (17 de 06 de 2024). *https://selloeditorial.unad.edu.co.* HYPERLINK "https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Guia_para_la_valoraci%C3%B3n_y_evaluaci%C3%B3n_de_riesgos_de_ciberseguridad__Pag_publicado.pdf" \t "_blank" https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Guia_para_la_valoraci%C3%B3n_y_evaluaci%C3%B3n_de_riesgos_de_ciberseguridad__Pag_publicado.pdf

ATTACK.CLOUDFALL.CN. (s.f.). *https://attack.cloudfall.cn/.* HYPERLINK "https://attack.cloudfall.cn/techniques/T1046/" \l ":~:text=Network%20intrusion%20detection%20systems%20can,network%20flows%20to" \t "_blank" https://attack.cloudfall.cn/techniques/T1046/#:~:text=Network%20intrusion%20detection%20systems%20can,network%20flows%20to

ATTACK.MITRE. (s.f.). *https://attack.mitre.org/.* HYPERLINK "https://attack.mitre.org/" \l ":~:text=MITRE%20ATT%26CK%C2%AE%20is%20a%20globally,cybersecurity%20product%20and%20service%20community" \t "_blank" https://attack.mitre.org/#:~:text=MITRE%20ATT%26CK%C2%AE%20is%20a%20globally,cybersecurity%20product%20and%20service%20community

ATTACK.MITRE.ORG. (s.f.). *https://attack.mitre.org/techniques/T1046/#:~:text=Tactic%3A%20Discovery*. HYPERLINK "https://attack.mitre.org/techniques/T1046/" \l ":~:text=Tactic%3A%20Discovery" \t "_blank" https://attack.mitre.org/techniques/T1046/#:~:text=Tactic%3A%20Discovery

CALTRC.ORG. (s.f.). *https://caltrc.org/.* HYPERLINK "https://caltrc.org/news/cyber-security-evaluation-tool-cset-assess-your-practice/" \l ":~:text=The%20Cyber%20Security%20Evaluation%20Tool,and%20industry%20standards%20and%20recommendations" \t "_blank" https://caltrc.org/news/cyber-security-evaluation-tool-cset-assess-your-

practice/#:~:text=The%20Cyber%20Security%20Evaluation%20Tool,and%20industry%20standards%20and%20recommendations

CAMPUSCIBERSEGURIDAD. (s.f.). *https://www.campusciberseguridad.com*. HYPERLINK "https://www.campusciberseguridad.com/blog/guia-completa-de-wireshark-para-analisis-y-monitoreo-de-redes/" \l ":~:text=Wireshark%20se%20utiliza%20para%20capturar,botella%2C%20vulnerabilidades%20y%20comportamientos%20an%C3%B3malos" \t "_blank" https://www.campusciberseguridad.com/blog/guia-completa-de-wireshark-para-analisis-y-monitoreo-de-redes/#:~:text=Wireshark%20se%20utiliza%20para%20capturar,botella%2C%20vulnerabilidades%20y%20comportamientos%20an%C3%B3malos

CARALLI, R. A., ALLEN, J. H., & WHITE, D. W. (2016). *https://www.sei.cmu.edu.* HYPERLINK "https://www.sei.cmu.edu/library/cert-resilience-management-model-a-maturity-model-for-managing-operational-resilience/" \l ":~:text=CERT%20Resilience%20Management%20Model%20%28CERT,achieve%20strategic%20resilience%20management%20goals" \t "_blank" https://www.sei.cmu.edu/library/cert-resilience-management-model-a-maturity-model-for-managing-operational-resilience/#:~:text=CERT%20Resilience%20Management%20Model%20%28CERT,achieve%20strategic%20resilience%20management%20goals

CCN-CERT.CNI. (s.f.). *https://www.ccn-cert.cni.es/*. HYPERLINK "https://www.ccn-cert.cni.es/es/soluciones-seguridad/elena.html?view=article&id=910:cset-nueva-herrmienta-para-aumentar-la-ciberseguridad&catid=23" \t "_blank" https://www.ccn-cert.cni.es/es/soluciones-seguridad/elena.html?view=article&id=910:cset-nueva-herrmienta-para-aumentar-la-ciberseguridad&catid=23

CENTRALEYES. (s.f.). *https://www.centraleyes.com/*. HYPERLINK "https://www.centraleyes.com/cyber-resilience-review-crr/" \l ":~:text=MIL0%20Incomplete%20,MIL5%20Defined" \t "_blank"

https://www.centraleyes.com/cyber-resilience-review-crr/#:~:text=MIL0%20Incomplete%20,MIL5%20Defined

CIBERSEGURIDAD. (s.f.). *https://ciberseguridad.com/*. HYPERLINK "https://ciberseguridad.com/herramientas/marco-mitre-att-ck/" \t "_blank" https://ciberseguridad.com/herramientas/marco-mitre-att-ck/

Ciberseguridadyhackingetico. (s.f.). *https://www.ciberseguridadyhackingetico.com/*. HYPERLINK "https://www.ciberseguridadyhackingetico.com/servicios/evaluacion-de-vulnerabilidades/" \l ":~:text=Prevenci%C3%B3n%20Proactiva%20de%20Brechas%20de,Seguridad" \t "_blank" https://www.ciberseguridadyhackingetico.com/servicios/evaluacion-de-vulnerabilidades/#:~:text=Prevenci%C3%B3n%20Proactiva%20de%20Brechas%20de,Seguridad

CISA. (s.f.). *https://www.cisa.gov/*. HYPERLINK "https://www.cisa.gov/resources-tools/services/cyber-security-evaluation-tool-cset" \l ":~:text=The%20Cyber%20Security%20Evaluation%20Tool,evaluating%20an%20organization%27s%20security%20posture" \t "_blank" https://www.cisa.gov/resources-tools/services/cyber-security-evaluation-tool-cset#:~:text=The%20Cyber%20Security%20Evaluation%20Tool,evaluating%20an%20organization%27s%20security%20posture

COALFIREFEDERAL. (27 de Octubre de 2023). *https://coalfirefederal.com*. HYPERLINK "https://coalfirefederal.com/resource/cmmc-vs-nist-800-171/" \l ":~:text=face%20and%20their%20potential%20impact,iii%29%20Situational%20awareness" \t "_blank" https://coalfirefederal.com/resource/cmmc-vs-nist-800-171/#:~:text=face%20and%20their%20potential%20impact,iii%29%20Situational%20awareness

CONCEPTO. (s.f.). *https://concepto.de/*. HYPERLINK "https://concepto.de/investigacion-no-experimental/" \t "_blank" https://concepto.de/investigacion-no-experimental/

CONTINUUMGRC. (26 de SEPTIEMBRE de 2025). *https://continuumgrc.com/*. HYPERLINK "https://continuumgrc.com/es/cmmc-2-0-and-level-3-maturity/" \t "_blank" https://continuumgrc.com/es/cmmc-2-0-and-level-3-maturity/

CROWDSTRIKE. (2025). *https://www.crowdstrike.com.* HYPERLINK "https://www.crowdstrike.com/explore/2025-global-threat-report-es-es?utm_medium=dir" \t "_blank" https://www.crowdstrike.com/explore/2025-global-threat-report-es-es?utm_medium=dir

CSRC.NIST.GOV. (1 de Octubre de 2025). *https://csrc.nist.gov/.* HYPERLINK "https://csrc.nist.gov/glossary/term/csf_tier" \l ":~:text=CSF%20Tier%20,About" \t "_blank" https://csrc.nist.gov/glossary/term/csf_tier#:~:text=CSF%20Tier%20,About

CSWP, N. (26 de Febrero de 2024). *https://nvlpubs.nist.gov.* HYPERLINK "https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf" \l ":~:text=government%20agencies%2C%20and%20other%20organizations,prescribe%20how%20outcomes%20should%20be" \t "_blank" https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf#:~:text=government%20agencies%2C%20and%20other%20organizations,prescribe%20how%20outcomes%20should%20be

CTID.MITRE. (10 de Abril de 2024). *https://ctid.mitre.org/.* HYPERLINK "https://ctid.mitre.org/projects/measure-maximize-and-mature-threat-informed-defense-m3tid/" \l ":~:text=M3TID%20leverages%20threat%20understanding%20to,well%20threat%20information%20is%20leveraged" \t "_blank" https://ctid.mitre.org/projects/measure-maximize-and-mature-threat-informed-defense-m3tid/#:~:text=M3TID%20leverages%20threat%20understanding%20to,well%20threat%20information%20is%20leveraged

CYBERSAINT. (s.f.). *https://www.cybersaint.io/.* HYPERLINK "https://www.cybersaint.io/cybersecurity/frameworks-and-standards/nist/glossary/nist-csf-to-cmmc-control-mapping" \t "_blank" https://www.cybersaint.io/cybersecurity/frameworks-and-standards/nist/glossary/nist-csf-to-cmmc-control-mapping

DC3.MIL. (s.f.). *https://www.dc3.mil/.* HYPERLINK "https://www.dc3.mil/Missions/DIB-Cybersecurity/DIB-Cybersecurity-DCISE/" \l ":~:text=Analysis%20%28CRA%29%20is%20your%20mission,Are%20you%20ready%20t

o%20defend" \t "_blank" https://www.dc3.mil/Missions/DIB-Cybersecurity/DIB-Cybersecurity-DCISE/#:~:text=Analysis%20%28CRA%29%20is%20your%20mission,Are%20you%20ready%20to%20defend

Dekra-certification. (08 de 2025). *https://www.dekra-certification.es.* HYPERLINK "https://www.dekra-certification.es/es/iso27001-gestion-riesgos-ciberseguridad/" \t "_blank" https://www.dekra-certification.es/es/iso27001-gestion-riesgos-ciberseguridad/

DELTAPROTECT. (21 de Mayo de 2025). *https://www.deltaprotect.com/.* HYPERLINK "https://www.deltaprotect.com/blog/marco-ciberseguridad-nist" \t "_blank" https://www.deltaprotect.com/blog/marco-ciberseguridad-nist

DEV.TO. (27 de Julio de 2024). *https://dev.to/.* HYPERLINK "https://dev.to/clouddefenseai/mitre-attck-vs-nist-csf-a-comprehensive-guide-to-cybersecurity-frameworks-4805" \l ":~:text=Understanding%20the%20MITRE%20ATT%26CK%20Framework" \t "_blank" https://dev.to/clouddefenseai/mitre-attck-vs-nist-csf-a-comprehensive-guide-to-cybersecurity-frameworks-4805#:~:text=Understanding%20the%20MITRE%20ATT%26CK%20Framework

DISCOVERY. (s.f.). *https://discovery.ucl.ac.uk/.* HYPERLINK "https://discovery.ucl.ac.uk/id/eprint/10120863/1/bcp.14744.pdf" \l ":~:text=equal%20value%20to%20the%20questionnaire,89%20in%20the" \t "_blank" https://discovery.ucl.ac.uk/id/eprint/10120863/1/bcp.14744.pdf#:~:text=equal%20value%20to%20the%20questionnaire,89%20in%20the

DODCIO. (s.f.). *https://dodcio.defense.gov/.* HYPERLINK "https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview.pdf" \t "_blank" https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview.pdf

EPA.GOV. (03 de 2023). *https://www.epa.gov/.* HYPERLINK "https://www.epa.gov/system/files/documents/2023-06/230228_Cyber%20SS%20Guidance_508c.docx_en-US_es-419%20%281%29.pdf" \l ":~:text=diagram,creaci%C3%B3n%20de%20diagramas%20de%20red" \t "_blank" https://www.epa.gov/system/files/documents/2023-

06/230228_Cyber%20SS%20Guidance_508c.docx_en-US_es-419%20%281%29.pdf#:~:text=diagram,creaci%C3%B3n%20de%20diagramas%20de%20red

ESPINOZA SALDAÑA, N., LARA ZAMBRANO, W. O., RUIZ JARA, J. A., & ZAMORA MAYORGA, D. J. (2025). Ciberseguridad en gobierno electrónico: percepción del sector público en El Empalme . *Revista Científica Ciencia y Método (RCyM) , 110*, 13. HYPERLINK "https://doi.org/https://doi.org/10.55813/gaea/rcym/v3/n3/62%20" \t "_blank" https://doi.org/https://doi.org/10.55813/gaea/rcym/v3/n3/62

Estudiapuntes. (8 de Julio de 2025). *https://www.estudiapuntes.com*. HYPERLINK "https://www.estudiapuntes.com/evolucion-de-la-ciberseguridad-hitos-historicos-y-modelos-clave.html" \t "_blank" https://www.estudiapuntes.com/evolucion-de-la-ciberseguridad-hitos-historicos-y-modelos-clave.html

FASTERCAPITAL. (30 de ABRIL de 2025). *https://fastercapital.com*. HYPERLINK "https://fastercapital.com/es/contenido/Hacking-etico--Como-utilizar-tecnicas-de-hacking-etico-para-probar-y-mejorar-tu-ciberseguridad.html" \t "_blank" https://fastercapital.com/es/contenido/Hacking-etico--Como-utilizar-tecnicas-de-hacking-etico-para-probar-y-mejorar-tu-ciberseguridad.html

FLEXENTIAL. (07 de Julio de 2025). *https://www.flexential.com/resources/blog/cybersecurity-maturity-models#:~:text=CMMC%202,level%20structure*. HYPERLINK "https://www.flexential.com/resources/blog/cybersecurity-maturity-models" \l ":~:text=CMMC%202,level%20structure" \t "_blank" https://www.flexential.com/resources/blog/cybersecurity-maturity-models#:~:text=CMMC%202,level%20structure

FLORES MIRANDA, M. (18 de Maro de 2024). *https://www.deletetechnology.com/blog/cmmc-gu%C3%ADa-de-cumplimiento-para-certificaci%C3%B3n-del-modelo-de-madurez-de-ciberseguridad*. HYPERLINK "https://www.deletetechnology.com/blog/cmmc-gu%C3%ADa-de-cumplimiento-para-certificaci%C3%B3n-del-modelo-de-madurez-de-ciberseguridad" \t "_blank" https://www.deletetechnology.com/blog/cmmc-gu%C3%ADa-de-cumplimiento-para-certificaci%C3%B3n-del-modelo-de-madurez-de-ciberseguridad

FORTINET. (2025). *https://www.fortinet.com.* HYPERLINK "https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/es_la/threat-landscape-report-2025.pdf" \t "_blank" https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/es_la/threat-landscape-report-2025.pdf

FTC. (s.f.). *https://www.ftc.gov/es/.* HYPERLINK "https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist" \l ":~:text=Usted%20puede%20implementar%20el%20Marco,protecci%C3%B3n%2C%20detecci%C3%B3n%2C%20respuesta%20y%20recuperaci%C3%B3n" \t "_blank" https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist#:~:text=Usted%20puede%20implementar%20el%20Marco,protecci%C3%B3n%2C%20detecci%C3%B3n%2C%20respuesta%20y%20recuperaci%C3%B3n

GITHUB. (s.f.). *https://github.com/.* HYPERLINK "https://github.com/cisagov/cset/releases" \t "_blank" https://github.com/cisagov/cset/releases

IBM. (15 de Diciembre de 2023). *https://www.ibm.com/.* HYPERLINK "https://www.ibm.com/mx-es/think/topics/vulnerability-scanning" \t "_blank" https://www.ibm.com/mx-es/think/topics/vulnerability-scanning

INCIBE. (05 de 2020). *https://www.incibe.es.* HYPERLINK "https://www.incibe.es/sites/default/files/contenidos/guias/IMC/imc_01_metodologia-evaluacion.pdf" \t "_blank" https://www.incibe.es/sites/default/files/contenidos/guias/IMC/imc_01_metodologia-evaluacion.pdf

ISACA. (17 de Octubre de 2024). *https://www.isaca.org/resources/news-and-trends/industry-news/2024/comparing-the-mitre-attck-and-nist-cybersecurity-frameworks#:~:text=landscape*. HYPERLINK "https://www.isaca.org/resources/news-and-trends/industry-news/2024/comparing-the-mitre-attck-and-nist-cybersecurity-frameworks" \l ":~:text=landscape" \t "_blank" https://www.isaca.org/resources/news-and-trends/industry-news/2024/comparing-the-mitre-attck-and-nist-cybersecurity-frameworks#:~:text=landscape

ISIDEFENSE. (04 de Noviembre de 2024). *https://isidefense.com/*. HYPERLINK "https://isidefense.com/blog/how-to-be-nist-800-171-compliant-defense-contractors" \l ":~:text=Understanding%20NIST%20800,best%20practices%2C%20and%20details%20how" \t "_blank" https://isidefense.com/blog/how-to-be-nist-800-171-compliant-defense-contractors#:~:text=Understanding%20NIST%20800,best%20practices%2C%20and%20details%20how

KEYSIGHT. (18 de Noviembre de 2024). *https://www.keysight.com*. HYPERLINK "https://www.keysight.com/blogs/en/tech/nwvs/2024/11/18/fast-track-cmmc-with-these-five-game-changing-tools" \t "_blank" https://www.keysight.com/blogs/en/tech/nwvs/2024/11/18/fast-track-cmmc-with-these-five-game-changing-tools

KPMG. (s.f.). *https://kpmg.com/*. HYPERLINK "https://kpmg.com/nz/en/home/services/advisory/risk-consulting/cyber-security/strategy-and-governance/cyber-maturity-assessment.html" \l ":~:text=Cyber%20Maturity%20Assessment%20,contain%20and%20respond%20to%20threats" \t "_blank" https://kpmg.com/nz/en/home/services/advisory/risk-consulting/cyber-security/strategy-and-governance/cyber-maturity-assessment.html#:~:text=Cyber%20Maturity%20Assessment%20,contain%20and%20respond%20to%20threats

MADSECURITY. (s.f.). *https://madsecurity.com/*. HYPERLINK "https://madsecurity.com/madsecurity-blog/cmmc-assessment-preparation-using-soc-data" \l ":~:text=Each%20SOC%20output%20provides%20real,not%20just%20documented%20on%20paper" \t "_blank" https://madsecurity.com/madsecurity-blog/cmmc-assessment-preparation-using-soc-data#:~:text=Each%20SOC%20output%20provides%20real,not%20just%20documented%20on%20paper

Maldonado, M. (04 de 2021). *https://dspace.ups.edu.ec.* HYPERLINK "https://dspace.ups.edu.ec/bitstream/123456789/20243/1/UPS-GT003204.pdf" \t "_blank" https://dspace.ups.edu.ec/bitstream/123456789/20243/1/UPS-GT003204.pdf

MALWAREBYTES. (s.f.). *https://www.malwarebytes.com/es/cybersecurity/basics/what-is-ethical-hacking*. HYPERLINK "https://www.malwarebytes.com/es/cybersecurity/basics/what-is-ethical-hacking" \t "_blank" https://www.malwarebytes.com/es/cybersecurity/basics/what-is-ethical-hacking

Marc Levesque, N. A. (Septiembre de 2020). *https://pubs.naruc.org*. HYPERLINK "https://pubs.naruc.org/pub.cfm?id=287AC0D5-155D-0A36-311A-67F7847F17F4" \l ":~:text=Page%2013%20%E2%80%A2%20It%20provides,maturity%20level%20of%20a%20utility" \t "_blank" https://pubs.naruc.org/pub.cfm?id=287AC0D5-155D-0A36-311A-67F7847F17F4#:~:text=Page%2013%20%E2%80%A2%20It%20provides,maturity%20level%20of%20a%20utility

Maturitylab. (s.f.). *https://maturitylab.com/*. HYPERLINK "https://maturitylab.com/es/modelo-de-madurez-de-ciberseguridad-del-nist-una-guia-para-la-mejora-continua-y-la-resiliencia-cibernetica/" \t "_blank" https://maturitylab.com/es/modelo-de-madurez-de-ciberseguridad-del-nist-una-guia-para-la-mejora-continua-y-la-resiliencia-cibernetica/

MCMTECHCO. (Enero de 2025). *https://blog.mcmtechco.com/analisis-de-vulnerabilidad*. HYPERLINK "https://blog.mcmtechco.com/analisis-de-vulnerabilidad" \t "_blank" https://blog.mcmtechco.com/analisis-de-vulnerabilidad

MEDIUM. (s.f.). *https://medium.com/*. HYPERLINK "https://medium.com/@martinnorris23/cybersecurity-evaluation-tool-cset-in-relation-to-nist-csf-ce247a3c7cad" \l ":~:text=The%20tool%20is%20clearly%20mapped,of%20concern%20and%20security%20recommendations" \t "_blank" https://medium.com/@martinnorris23/cybersecurity-evaluation-tool-cset-in-relation-to-nist-csf-ce247a3c7cad#:~:text=The%20tool%20is%20clearly%20mapped,of%20concern%20and%20security%20recommendations

MELO, J. A. (2024). *https://repositorio.uchile.cl*. HYPERLINK "https://repositorio.uchile.cl/bitstream/handle/2250/205366/Tesis%20-%20JOSE%20ANTONIO%20LAGOS%20MELO.docx.pdf?sequence=1" \t "_blank"

https://repositorio.uchile.cl/bitstream/handle/2250/205366/Tesis%20-%20JOSE%20ANTONIO%20LAGOS%20MELO.docx.pdf?sequence=1

MICROSOFT. (2022). *Microsoft Technical Reference Guide for CMMC Reference Guide for CMMC.*

MINTEL. (2022). *https://gobiernoelectronico.gob.ec/.* HYPERLINK "https://gobiernoelectronico.gob.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-2022.pdf" \t "_blank" https://gobiernoelectronico.gob.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-2022.pdf

MITRE.ORG. (25 de Abril de 2024). *https://www.mitre.org/.* HYPERLINK "https://www.mitre.org/news-insights/news-release/mitres-cyber-resiliency-engineering-framework-navigator" \l ":~:text=MITRE%20in%20partnership%20with%20NIST,for%20cyber%20threat%20modeling" \t "_blank" https://www.mitre.org/news-insights/news-release/mitres-cyber-resiliency-engineering-framework-navigator#:~:text=MITRE%20in%20partnership%20with%20NIST,for%20cyber%20threat%20modeling

NACIONAL, A. (26 de Mayo de 2021). *https://www.finanzaspopulares.gob.ec/.* HYPERLINK "https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf" \t "_blank" https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

NETPROVIDERS. (21 de Mayo de 2025). *https://www.netprovider.com/.* HYPERLINK "https://www.netprovider.com/post/ethical-hacking-como-detectar-vulnerabilidades-antes-de-ser-atacado" \t "_blank" https://www.netprovider.com/post/ethical-hacking-como-detectar-vulnerabilidades-antes-de-ser-atacado

NIST. (2024). NIST Cybersecurity Framework 2.0: Quick-Start Guide for Using . *5.* HYPERLINK "https://doi.org/https://doi.org/10.6028/NIST.SP.1302" \t "_blank" https://doi.org/https://doi.org/10.6028/NIST.SP.1302

NIST.GOV. (2022). *https://www.nist.gov/.* HYPERLINK "https://www.nist.gov/system/files/documents/2023/04/03/2023-01-19%20Deploy-securely_508_redacted.pdf" \l ":~:text=and%20that%20your%20procedures%20are,DAST%2C%20IAST%2C%20and%20SCA%20tools" \t "_blank" https://www.nist.gov/system/files/documents/2023/04/03/2023-01-19%20Deploy-securely_508_redacted.pdf#:~:text=and%20that%20your%20procedures%20are,DAST%2C%20IAST%2C%20and%20SCA%20tools

OROZCO, G. A. (10 de 2019). *https://repositorioinstitucional.uabc.mx.* HYPERLINK "https://repositorioinstitucional.uabc.mx/server/api/core/bitstreams/c5111146-3383-427f-8ee8-0356ebe23ed4/content" \t "_blank" https://repositorioinstitucional.uabc.mx/server/api/core/bitstreams/c5111146-3383-427f-8ee8-0356ebe23ed4/content

PALOALTONETWORKS.LAT. (s.f.). *https://www.paloaltonetworks.lat*. HYPERLINK "https://www.paloaltonetworks.lat/cyberpedia/what-is-mitre-attack-framework" \l ":~:text=El%20marco%20MITRE%20ATT%26CK%C2%AE%20es,mitigaci%C3%B3n%20basadas%20en%20el%20riesgo" \t "_blank" https://www.paloaltonetworks.lat/cyberpedia/what-is-mitre-attack-framework#:~:text=El%20marco%20MITRE%20ATT%26CK%C2%AE%20es,mitigaci%C3%B3n%20basadas%20en%20el%20riesgo

PATIÑO OROZCO, G. A. (Octubre de 2019). *https://repositorioinstitucional.uabc.mx.* HYPERLINK "https://repositorioinstitucional.uabc.mx/server/api/core/bitstreams/c5111146-3383-427f-8ee8-0356ebe23ed4/content" \t "_blank" https://repositorioinstitucional.uabc.mx/server/api/core/bitstreams/c5111146-3383-427f-8ee8-0356ebe23ed4/content

PIRANIRISK. (s.f.). *https://www.piranirisk.com*. HYPERLINK "https://www.piranirisk.com/es/academia/especiales/iso-27001-controles-y-como-implementarlos-correctamente" \l ":~:text=ISO%2027001%3A%20Controles%20y%20c%C3%B3mo,10" \t "_blank"

https://www.piranirisk.com/es/academia/especiales/iso-27001-controles-y-como-implementarlos-correctamente#:~:text=ISO%2027001%3A%20Controles%20y%20c%C3%B3mo,10

PUBS.NARUC. (Septiembre de 2020). *https://pubs.naruc.org/*. HYPERLINK "https://pubs.naruc.org/pub.cfm?id=287AC0D5-155D-0A36-311A-67F7847F17F4" \l ":~:text=and%20application%20software%20vulnerabilities,supply%20chains%2C%20operations%2C%20and%20logistics" \t "_blank" https://pubs.naruc.org/pub.cfm?id=287AC0D5-155D-0A36-311A-67F7847F17F4#:~:text=and%20application%20software%20vulnerabilities,supply%20chains%2C%20operations%2C%20and%20logistics

Rea Guamán, Á. M., ánchez García, ,. I., San Feliu Gilabert, T., & Calvo-Manzano Villalón, J. A. (s.f.). *https://oa.upm.es*. HYPERLINK "https://oa.upm.es/48746/" \t "_blank" https://oa.upm.es/48746/

REDZONE. (s.f.). *https://www.redeszone.net/*. HYPERLINK "https://www.redeszone.net/tutoriales/redes-cable/wireshark-capturar-analizar-trafico-red/" \t "_blank" https://www.redeszone.net/tutoriales/redes-cable/wireshark-capturar-analizar-trafico-red/

RESEARCHGATE. (MARZO de 2023). *https://www.researchgate.net/publication/369027581_A_systematic_literature_review_of_cybersecurity_scales_assessing_information_security_awareness#:~:text=evaluated%20based%20on%20Cronbach%E2%80%99s%20alpha,48%5D.%20An*. HYPERLINK "https://www.researchgate.net/publication/369027581_A_systematic_literature_review_of_cybersecurity_scales_assessing_information_security_awareness" \l ":~:text=evaluated%20based%20on%20Cronbach%E2%80%99s%20alpha,48%5D.%20An" \t "_blank" https://www.researchgate.net/publication/369027581_A_systematic_literature_review_of_cybersecurity_scales_assessing_information_security_awareness#:~:text=evaluated%20based%20on%20Cronbach%E2%80%99s%20alpha,48%5D.%20An

SECUREFRAME. (11 de Junio de 2024). *https://secureframe.com/*. HYPERLINK "https://secureframe.com/es-es/blog/cmmc" \t "_blank" https://secureframe.com/es-es/blog/cmmc

SEI.CMU. (Marzo de 2020). *https://www.sei.cmu.edu/*. HYPERLINK "https://www.sei.cmu.edu/blog/an-introduction-to-the-cybersecurity-maturity-model-certification-cmmc/" \l ":~:text=A%20total%20of%20171%20technical,receive%20a%20Level%202%20certification" \t "_blank" https://www.sei.cmu.edu/blog/an-introduction-to-the-cybersecurity-maturity-model-certification-cmmc/#:~:text=A%20total%20of%20171%20technical,receive%20a%20Level%202%20certification

SIKICH. (20 de 06 de 2025). *https://www.sikich.com/*. HYPERLINK "https://www.sikich.com/insight/going-beyond-the-basics-using-mitre-attck-to-enhance-your-risk-assessments-and-security-policies/" \l ":~:text=,02%3A%20Threat%20monitoring%20requirements" \t "_blank" https://www.sikich.com/insight/going-beyond-the-basics-using-mitre-attck-to-enhance-your-risk-assessments-and-security-policies/#:~:text=,02%3A%20Threat%20monitoring%20requirements

SOFTWARELAB. (2023). *https://softwarelab.org/*. HYPERLINK "https://softwarelab.org/es/blog/que-es-el-hacking-etico/" \t "_blank" https://softwarelab.org/es/blog/que-es-el-hacking-etico/

SPRINTO. (01 de Octubre de 2024). *https://sprinto.com*. HYPERLINK "https://sprinto.com/blog/nist-implementation-tiers/" \l ":~:text=Nist%20Implementation%20Tiers%20101%3A%20All,%C2%B7%20Tier%204%20%E2%80%93%20Adaptive" \t "_blank" https://sprinto.com/blog/nist-implementation-tiers/#:~:text=Nist%20Implementation%20Tiers%20101%3A%20All,%C2%B7%20Tier%204%20%E2%80%93%20Adaptive

TELECOMUNICACIONES, M. D. (2022). *https://www.telecomunicaciones.gob.ec/*. HYPERLINK "https://www.telecomunicaciones.gob.ec/wp-

content/uploads/2023/05/DIAGNO%CC%81STICO-DE-LAS-CAPACIDADES-DE-CIBERSEGURIDAD-Ecuador-Diciembre-2022_compressed.pdf" \t "_blank" https://www.telecomunicaciones.gob.ec/wp-content/uploads/2023/05/DIAGNO%CC%81STICO-DE-LAS-CAPACIDADES-DE-CIBERSEGURIDAD-Ecuador-Diciembre-2022_compressed.pdf

THESAI.ORG. (2025). *https://thesai.org/*. HYPERLINK "https://thesai.org/Downloads/Volume16No5/Paper_10-Building_Cyber_Resilient_Universities.pdf" \l ":~:text=For%20the%20quantitative%20part%2C%20reliability,more%20weight%20on%20the%20reliability" \t "_blank" https://thesai.org/Downloads/Volume16No5/Paper_10-Building_Cyber_Resilient_Universities.pdf#:~:text=For%20the%20quantitative%20part%2C%20reliability,more%20weight%20on%20the%20reliability

TITANIA. (s.f.). *https://www.titania.com/*. HYPERLINK "https://www.titania.com/resources/compliance/cmmc-mapping-document" \t "_blank" https://www.titania.com/resources/compliance/cmmc-mapping-document

TRENDMICRO. (s.f.). *https://www.trendmicro.com/*. HYPERLINK "https://www.trendmicro.com/es_es/what-is/cyber-attack/mitre-attack-framework.html" \t "_blank" https://www.trendmicro.com/es_es/what-is/cyber-attack/mitre-attack-framework.html

TSAPPS.NIST. (26 de Febrero de 2024). *https://tsapps.nist.gov/*. HYPERLINK "https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=958048" \t "_blank" https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=958048

TUCONSULTORTI. (s.f.). *https://www.tuconsultorti.com/*. HYPERLINK "https://www.tuconsultorti.com/ciberseguridad/pentesting-en-el-ciclo-de-vida-del-desarrollo-de-software/" \t "_blank" https://www.tuconsultorti.com/ciberseguridad/pentesting-en-el-ciclo-de-vida-del-desarrollo-de-software/

VERVEINDUSTRIAL. (18 de Septiembre de 2019). *https://verveindustrial.com/*. HYPERLINK "https://verveindustrial.com/resources/blog/extending-nist-csf-and-dod-cmmc-by-reference-to-the-nist-sp-800-171bdraft/" \t "_blank"

https://verveindustrial.com/resources/blog/extending-nist-csf-and-dod-cmmc-by-reference-to-the-nist-sp-800-171bdraft/

VISURESOLUTIONS. (s.f.). *https://visuresolutions.com/*. HYPERLINK "https://visuresolutions.com/es/gu%C3%ADa-de-limosna/cmmc/" \t "_blank" https://visuresolutions.com/es/gu%C3%ADa-de-limosna/cmmc/

ZENGRC. (26 de Mayo de 2023). *https://www.zengrc.com/*. HYPERLINK "https://www.zengrc.com/blog/what-you-should-know-about-the-new-cyber-security-evaluation-tool-model/" \l ":~:text=How%20Does%20CSET%20Work%3F" \t "_blank" https://www.zengrc.com/blog/what-you-should-know-about-the-new-cyber-security-evaluation-tool-model/#:~:text=How%20Does%20CSET%20Work%3F