INVESTIGACIÓN

Diagnóstico de Madurez en Seguridad Digital para servicios de consultoría

Digital Security Maturity Assessment for Consulting Services

M. Sc. Noel Emilio Rojas Martos [1*], M. Sc. Liban de Armas Granado [2]

Recibido: 01/2026 | Aceptado: 03/2026 | Publicado: 07/2026

Resumen

Este estudio presentó un modelo metodológico de Diagnóstico de Madurez en Seguridad Digital, orientado a instituciones con estructuras organizativas diversas. El objetivo fue desarrollar una herramienta capaz de identificar brechas, priorizar acciones y alinear la seguridad digital con los objetivos institucionales y de la política para la transformación digital, la agenda digital cubana y la estrategia de inteligencia artificial. El enfoque combinó una matriz de evaluación modular, entrevistas estratégicas y una hoja de ruta personalizada. La propuesta se estructuró en nueve dimensiones: liderazgo digital, puesto de trabajo digital, tecnologías, información y comunicación, políticas y estrategias de seguridad digital, operaciones digitales, cultura y clima digital, migración a la nube, marcos legales y regulatorios, y habilidades digitales. Se aplicaron técnicas cualitativas y escalas ordinales para

[1*] M. Sc. Ingeniero. Especialista Comercial, Departamento de Proyectos, Dirección de Consultoría. DCCH. noel.rojas@etecsa.cu

[2] M. Sc. Ingeniero. Jefe Departamento de Proyectos, Dirección de Consultoría. DCCH. liban.dearmas@etecsa.cu

construir perfiles de madurez contextualizados, activando procesos de reflexión interna y planificación estratégica. Los resultados que se obtengan con su aplicación pueden evidenciar patrones de vulnerabilidad, como la ausencia de políticas formales, baja cultura de reporte y dependencia de actores individuales. Al mismo tiempo, se identificaron oportunidades de mejora sostenibles, alcanzables sin requerimientos técnicos complejos. La hoja de ruta permitió visualizar acciones escalonadas, adaptables a cada contexto institucional. El modelo demostró capacidad no solo para diagnosticar, sino para habilitar procesos de transformación organizacional. Su aplicación puede favorecer el fortalecimiento institucional, la preparación para auditorías externas y la integración de la seguridad digital como componente estratégico. Se propone su incorporación como fase fundacional en procesos de mejora continua y transformación digital.

Palabras clave: Diagnóstico, dimensiones, modelo, transformación, seguridad

Abstract

This study presented a methodological model for assessing digital security maturity, aimed at institutions with diverse organizational structures. Its objective was to develop a tool capable of identifying gaps, prioritizing actions, and aligning digital security with institutional goals as well as with the Digital Transformation Policy, the Cuban Digital Agenda, and the Artificial Intelligence Strategy. The approach combined a modular evaluation matrix, strategic interviews, and a customized roadmap. The model was structured around nine dimensions: Digital Leadership, Digital Workstation, Technologies, Information and Communication, Digital Security Policies and Strategies, Digital Operations, Digital Culture and Climate, Cloud Migration, Legal and Regulatory Frameworks, and Digital Skills. Qualitative techniques and ordinal scales were applied to build contextualized maturity profiles, activating internal reflection and strategic planning processes. Results obtained through its application may reveal vulnerability patterns such as the absence of formal policies, low reporting culture, and reliance on individual actors. At the same time, sustainable improvement opportunities were identified,

achievable without complex technical requirements. The roadmap enabled the visualization of phased actions, adaptable to each institutional context. The model proved capable not only of diagnosing but also of enabling organizational transformation processes. Its application may support institutional strengthening, preparation for external audits, and the integration of digital security as a strategic component. Its incorporation is proposed as a foundational phase in continuous improvement and digital transformation initiatives.

Keywords: *Diagnosis; dimensions, model, transformation, security*

Introducción

Este estudio propuesto tuvo como objetivo desarrollar un modelo metodológico de Diagnóstico de Madurez en Seguridad Digital orientado a instituciones con estructuras organizativas diversas, para facilitar la identificación de brechas, priorizar acciones, apoyar procesos de transformación digital segura, priorizar acciones de mejora en función del nivel de madurez institucional, facilitar la alineación con marcos regulatorios y estándares internacionales y alinear la seguridad digital con los objetivos institucionales, en consonancia con la política para la transformación digital, la agenda digital cubana y la estrategia nacional de inteligencia artificial.

La evolución de la seguridad digital a nivel internacional ha dado lugar a una serie de conceptos clave que trascienden la protección técnica de sistemas y datos, y que hoy constituyen pilares para la evaluación de la madurez institucional (Von Solms & Van Niekerk, 2013). Dentro de esos conceptos destacamos los más relevantes para el diseño y aplicación de modelos de diagnósticos:

1. Resiliencia cibernética: capacidad de una organización para anticipar, resistir, recuperarse y adaptarse ante incidentes cibernéticos. Aplicación en el modelo: Se incorpora mediante indicadores de continuidad operativa, gestión de crisis, aprendizaje organizacional y flexibilidad adaptativa.

2. Seguridad digital como capacidad nacional: La seguridad digital es una capacidad estratégica que involucra legislación, infraestructura, educación, cooperación y gobernanza. Marco de referencia: Global

Cybersecurity Index (UIT). Aplicación en el modelo: Permite mapear el alineamiento institucional con políticas nacionales, estrategias sectoriales y marcos regulatorios.

3. Enfoque sociotécnico: La seguridad digital es un fenómeno que combina tecnología, personas, procesos y cultura. Aplicación en el modelo: Justifica la inclusión de dimensiones como liderazgo, cultura organizacional, percepción del riesgo y comunicación interna.

4. Gobernanza multinivel: La seguridad digital requiere articulación entre actores locales, nacionales e internacionales, públicos y privados. Aplicación en el modelo: Se evalúa la participación institucional en redes colaborativas, la interoperabilidad normativa y la capacidad de coordinación interinstitucional.

5. Madurez digital y seguridad por diseño La seguridad debe estar integrada desde la fase de diseño de procesos, sistemas y políticas. Aplicación en el modelo: Se diagnostica si la seguridad está incorporada estructuralmente o si responde a una lógica reactiva.

La incorporación de estos conceptos permite que el modelo diagnóstico trascienda la auditoría técnica y se convierta en una herramienta estratégica para la transformación institucional. Al evaluar las nueve dimensiones que abarcan el diagnóstico objeto de estudio: Liderazgo Digital, Puesto de Trabajo Digital, Tecnologías, Información y Comunicación, Políticas y Estrategias de Seguridad Digital, Operaciones Digitales, Cultura y Clima Digital, Migración a la Nube, Marcos Legales y Regulatorios, y Habilidades Digitales, este se posiciona como un instrumento alineado con las mejores prácticas internacionales y adaptable a contextos nacionales. Las dimensiones se estructuraron con técnicas cualitativas y escalas ordinales para construir perfiles de madurez contextualizados, activando procesos de reflexión interna y planificación estratégica.

La investigación se fundamentó en aportes teóricos y metodológicos de autores como Von Solms y Van Niekerk, quienes ampliaron el concepto de seguridad digital más allá de lo técnico; Siponen y Pahnila, que abordaron la adherencia organizacional a políticas de seguridad, las normativas cubanas Decreto-Ley 78/2023 «Sobre la

seguridad y protección de la información clasificada y limitada»; Decreto 104/2024 «Reglamento de la seguridad y protección de la información clasificada y limitada»; Decreto 360/2019 «Sobre la seguridad de las TIC y la defensa del Ciberespacio Nacional»; Resolución 128/2019 «Reglamento de Seguridad de las TIC»; Resolución 105/2021«Reglamento sobre el Modelo de Actuación Nacional para la Respuesta a Incidentes de Ciberseguridad» y los marcos internacionales como el NIST Cybersecurity Framework (National Institute of Standards and Technology [NIST], 2018); las ISO/IEC 27001 y 27002 y CIS Controls. El diagnóstico propuesto permite también habilitar procesos de transformación organizacional mediante una hoja de ruta escalonada, adaptable y orientada a la acción.

Materiales y métodos

El Diagnóstico de Madurez en Seguridad Digital ha sido desarrollado con el propósito de evaluar de forma estructurada el estado actual de las capacidades, políticas y prácticas institucionales vinculadas a la gestión segura de la información y los sistemas digitales. Su aplicación permite identificar fortalezas, brechas y oportunidades de mejora, contribuyendo a la toma de decisiones estratégicas orientadas a la resiliencia organizacional y al cumplimiento normativo.

En el artículo de investigación propone un Diagnóstico de Madurez en Seguridad Digital para los servicios consultivos enfocado a la transformación digital. Para ello, fue necesario realizar un acercamiento al marco teórico y al estado del arte de los conceptos y modelos principales asociados a la ciberseguridad, así como el análisis de las regulaciones, normativas y recomendaciones de publicaciones de la UIT, empresas de ciberseguridad, las normativas cubanas relacionadas con el tema de investigación, de las tendencias y buenas prácticas identificadas. La investigación se ha sustentado en fuentes bibliográficas de una amplia gama de actores (reguladores, operadores, consultores, académicos).

Mediante el diagnóstico se pretende facilitar la identificación y vulnerabilidades asociadas a la seguridad digital y otras capacidades intangibles de los sectores presupuestado, empresarial y de otros actores económicos interesados en el proceso de la transformación digital.

Brinda la posibilidad de diagnosticar el Nivel de Madurez en Seguridad Digital, de trazar una hoja de ruta estratégica para la mejora cualitativa y cuantitativa de su gestión y de incrementar sus resultados. El diagnóstico tiene implicaciones prácticas porque constituye uno de los pilares del proyecto de diseño e implementación de los servicios de consultoría en la Empresa de Telecomunicaciones de Cuba. S.A. (ETECSA), para hacer una contribución a la sociedad cubana, a partir de las buenas prácticas implementadas; y puede tener un impacto positivo en el proceso de transformación digital del país. El beneficio económico está estimado sobre la base del ahorro por sustitución de importaciones, por concepto de diseño propio de la empresa y el valor para la protección de la información, sin necesidad de servicios consultivos externos.

En el desarrollo de esta investigación se combinaron métodos teóricos y estadísticos-matemáticos. Desde el punto de vista teórico, se procedió con la búsqueda, identificación y revisión de la literatura relacionada con el tema para recopilar la información de interés. Se utilizó el análisis y síntesis de toda la información consultada en la literatura especializada, proveniente de estudiosos del tema, empresas de ciberseguridad, casas consultoras, y organismos internacionales, entre otros.

Se trabajó el enfoque en sistema para garantizar la integración, interrelación, interdependencia y sinergia de las dimensiones que tributan al diagnóstico en su conjunto. Se implementó el método de ascenso de lo abstracto a lo complejo elaborando un sistema de abstracciones conceptuales con cada una de las dimensiones, así como los planos de análisis que posibilitaron el estudio de lo general a lo particular para obtener una imagen integral del proceso. Mediante el método histórico-lógico se logró enmarcar el proceso que es objeto de estudio en la historia y evolución, desde que aparece la ciberseguridad como ciencia hasta la actualidad.

Fueron utilizados métodos empíricos como la consulta bibliográfica, mediante la cual se acumuló una amplia bibliografía relacionada con el objetivo propuesto, y se procedió con la selección, revisión crítica y resumen para arribar a conclusiones. La observación científica fue utilizada para estudiar la experiencia práctica de diferentes diagnósticos de

ciberseguridad y los resultados de su implementación, a través de lo cual fue posible elaborar la formulación del problema, la comprobación de la hipótesis y proyectar la repercusión social de la solución a partir de la generalización del diagnóstico.

La investigación permitió el desarrollo de un test (tipo lista de chequeo) específico como instrumento para medir el Nivel de Madurez en Seguridad Digital como herramienta para diagnosticar el estado actual de organismos, empresas y organizaciones.

Resultados y discusión

El Diagnóstico de Madurez en Seguridad Digital está fundamentado en las buenas prácticas sobre el Índice Mundial de Ciberseguridad (Global Cybersecurity Index (GCI) 2020. Geneva: ITU. publicado por la Unión Internacional de Telecomunicaciones (International Telecommunication Union [ITU], 2020); forma parte de la tecnología TETR4DIG (Modelo de Gestión enfocado a la Transformación Digital. De Armas Granado, L., Díaz Monjiotti,2022) (Figura 1); evalúa el compromiso de las organizaciones (organismos y empresas) en materia de Seguridad Digital de acuerdo con los cinco pilares de la Agenda sobre Ciberseguridad Global (medidas jurídicas, técnicas, organizativas, capacitación y cooperación [Center for Internet Security (CIS), 2021] y está en correspondencia con los ocho ejes estratégicos de la Política para la Transformación Digital, la Agenda Digital Cubana y la Estrategia de Inteligencia Artificial. Está elaborado en forma de *test* (encuesta tipo lista de chequeo) para cada una de las dimensiones.

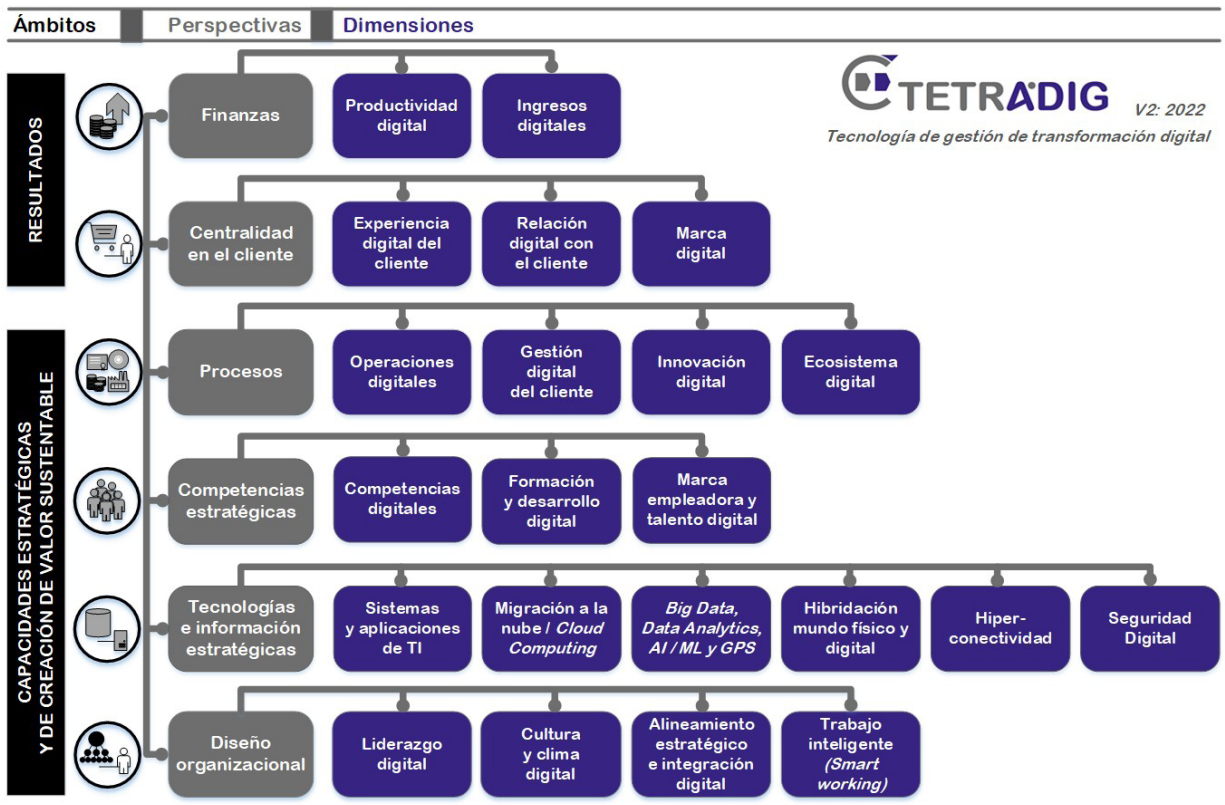


Figura 1. TETR4DIG: Modelo de gestión del cambio organizacional enfocado a la transformación digital (de Armas Granado, Liban; Díaz Monjiotti, Ela. 2022)

Sus objetivos son identificar fortalezas y debilidades en la infraestructura de la organización; identificar riesgos y vulnerabilidades; crear un plan de acción para mejorar la madurez en Seguridad Digital, incluyendo objetivos a corto, mediano y largo plazo, fomentar la conciencia y cultura de Seguridad Digital y preparar a la organización para el cumplimiento de las normas y políticas aprobadas a nivel de país.

Para la realización del diagnóstico se identificaron nueve dimensiones que forman parte del Modelo de Seguridad Digital (Figura 2) presentado durante los eventos «Ciberseguridad en las Telecomunicaciones» (ETECSA, 2023) y «XVI Seminario Iberoamericano de Seguridad en las Tecnologías de la Información» (Palacio de las Convenciones 2024).



Figura 2. Modelo de Seguridad Digital basado en la tecnología TETR4DIG. (Rojas Martos, Noel E. 2024)

Estructura del modelo y definición de las dimensiones

A partir de la fundamentación del diagnóstico, de una revisión de las normativas cubanas y de los marcos internacionales y de la conceptualización de la tecnología TETR4DIG, se diseñó una herramienta evaluativa compuesta por nueve dimensiones estratégicas que permiten valorar el grado de avance, integración y sostenibilidad de la seguridad digital en entornos institucionales.

Estas dimensiones no se conciben como elementos aislados, sino como componentes interdependientes que configuran un ecosistema

digital seguro, resiliente y orientado al desarrollo. La representación gráfica del modelo (centrada en el concepto de Seguridad Digital como núcleo articulador) permite visualizar la relación sistémica entre liderazgo, políticas, tecnología, cultura, habilidades y marcos regulatorios.

Cada dimensión responde a criterios específicos de evaluación y se vincula directamente con los ejes estratégicos de la Política Cubana de Transformación Digital, lo que garantiza la pertinencia contextual del instrumento y su capacidad para orientar procesos de mejora continua, planificación estratégica y cumplimiento normativo. Cada una representa un componente estratégico que contribuye al fortalecimiento de la seguridad digital institucional y su evaluación permite identificar el nivel de madurez, integración y alineación con los ejes de la Política Cubana de *Transformación Digital*. A continuación, se describe el significado y alcance de cada dimensión evaluada en el *test*:

Liderazgo Digital: evalúa el compromiso de la alta dirección con la seguridad digital como eje transversal de la transformación institucional. Incluye la existencia de políticas claras, asignación de responsabilidades, y capacidad de decisión estratégica. Un liderazgo maduro impulsa la gobernanza digital y promueve una cultura organizacional orientada a la resiliencia.

Políticas y Estrategias de Seguridad Digital: analiza la presencia, actualización y aplicación de políticas institucionales relacionadas con la ciberseguridad, protección de datos y gestión de riesgos. Considera si estas políticas están alineadas con marcos normativos nacionales e internacionales, y si se integran en la planificación estratégica de la organización.

Puesto de Trabajo Digital: valora el grado de digitalización de los entornos laborales, incluyendo el uso de herramientas tecnológicas, automatización de procesos y acceso seguro a plataformas digitales. También contempla la capacitación del personal en el uso responsable y seguro de los recursos digitales.

Tecnologías de la Información y la Comunicación (TIC): examina la infraestructura tecnológica disponible, su nivel de interoperabilidad, conectividad, y capacidad para habilitar servicios digitales seguros.

Incluye la gestión de activos tecnológicos, la actualización de sistemas y la implementación de soluciones innovadoras.

Cultura y Clima Digital: mide el nivel de conciencia, participación y confianza de los actores institucionales en el entorno digital. Evalúa la existencia de campañas de sensibilización, prácticas inclusivas, y mecanismos para fomentar valores digitales como la responsabilidad, la ética y la colaboración.

Marcos Legales y Regulatorios: determina el grado de cumplimiento de la organización con las normativas vigentes en materia de protección de datos, identidad digital, ciberseguridad e inteligencia artificial. Incluye la existencia de mecanismos de auditoría, control legal y adaptación normativa.

Migración a la Nube: explora el uso de tecnologías emergentes, especialmente la computación en la nube, como estrategia para mejorar la eficiencia, escalabilidad y seguridad de los servicios digitales. Considera aspectos como la gestión de proveedores, la protección de datos en entornos virtuales y la continuidad operativa.

Operaciones Digitales: evalúa la transformación de procesos internos y servicios públicos mediante plataformas digitales, trámites en línea y ventanillas únicas. Mide la eficiencia operativa, la experiencia del usuario y la capacidad de respuesta institucional en entornos digitales.

Habilidades Digitales: analiza la formación, actualización y desarrollo de competencias digitales en el personal institucional. Incluye conocimientos en TIC, ciberseguridad, inteligencia artificial y gestión de datos, así como la existencia de programas de capacitación continua.

Los análisis obtenidos a través del *test* de Diagnóstico de Madurez en Seguridad Digital evidencian una estructura institucional que, si bien ha avanzado en la adopción de tecnologías y políticas digitales, aún enfrenta desafíos en la integración sistémica de la seguridad como eje transversal. La matriz analítica y el modelo dimensional permiten identificar fortalezas en áreas como infraestructura TIC y operaciones digitales, así como brechas en liderazgo estratégico, cultura organizacional y habilidades digitales.

La correspondencia entre las dimensiones evaluadas y los ejes estratégicos de la *Política Cubana de Transformación Digital* valida la pertinencia contextual del modelo, posicionándolo como una herramienta metodológica capaz de orientar procesos de mejora continua, planificación institucional y cumplimiento normativo. Además, al incorporar enfoques sociotécnicos y principios de gobernanza digital, el diagnóstico trasciende la auditoría técnica y se convierte en un instrumento de transformación organizacional. Este análisis no solo permite caracterizar el estado actual de la seguridad digital en las instituciones evaluadas, sino que también ofrece insumos concretos para la formulación de estrategias, la toma de decisiones y el fortalecimiento de capacidades, en función de una transformación digital segura, inclusiva y sostenible.

Articulación del modelo diagnóstico con la *Política Cubana de Transformación Digital*

Los resultados del Diagnóstico de Madurez en Seguridad Digital se organizaron en una matriz que vincula cada dimensión evaluada con los ejes estratégicos definidos en la *Política Cubana de Transformación Digital*. Esta articulación permite validar la pertinencia del modelo en el contexto nacional y evidenciar su capacidad para operacionalizar los principios rectores de la política pública. La matriz revela una correspondencia directa entre las dimensiones del modelo y los componentes estratégicos de la política, como se muestra a continuación (Tabla 1):

Tabla 1. Vinculación de las dimensiones con la Política para la Transformación Digital, la Agenda Digital Cubana y la Estrategia de Inteligencia Artificial y sus ocho ejes estratégicos.
Fuente: elaboración propia

Dimensión del Diagnóstico de Seguridad Digital	Vinculación con la Política Cubana	Ejes Estratégicos	Fundamentación
Liderazgo Digital	La política establece que el Estado lidera la transformación digital como "proceso transversal, estratégico y urgente" (p. 6), con un enfoque de gobernanza digital y participación multisectorial.	Marco Normativo, Gobierno Digital	El liderazgo impulsa la adopción de marcos legales, políticas públicas y gobernanza digital dentro de la organización.

Dimensión del Diagnóstico de Seguridad Digital	Vinculación con la Política Cubana	Ejes Estratégicos	Fundamentación
Puesto de Trabajo Digital	Se promueve la digitalización de procesos laborales, automatización y uso de herramientas digitales en sectores como salud, educación y administración pública (p. 12).	Economía Digital, Educación y Cultura Digital	Moderniza los entornos laborales, fomenta la productividad digital y promueve la alfabetización tecnológica del personal.
Tecnologías, Información y Comunicación (TIC)	Se prioriza el desarrollo de infraestructura digital, conectividad, interoperabilidad de sistemas y servicios digitales accesibles (p. 9).	Economía Digital, Gobierno Digital, Innovación	Las tecnologías habilitan servicios digitales, interoperabilidad, automatización y desarrollo de nuevos modelos de negocio.
Políticas y Estrategias de Seguridad Digital	Se reconoce la necesidad de una Estrategia Nacional de Ciberseguridad, protección de datos personales y resiliencia ante amenazas digitales (p. 10).	Ciberseguridad, Marco Normativo	Refuerza la protección de datos, la gestión de riesgos y el cumplimiento normativo en entornos digitales.
Operaciones Digitales	Se impulsa la transformación de servicios públicos, trámites en línea, plataformas de gobierno electrónico y ventanillas únicas digitales (p. 13).	Gobierno Digital, Economía Digital	Digitaliza procesos internos y servicios públicos, mejora la eficiencia y la experiencia del usuario.
Cultura y Clima Digital	Se promueve una cultura digital inclusiva, con énfasis en la alfabetización digital, participación ciudadana y confianza en el entorno digital (p. 11).	Educación y Cultura Digital, Contenidos Digitales	Promueve valores digitales, participación ciudadana y generación de contenidos digitales inclusivos.
Migración a la Nube	Se menciona la adopción de tecnologías emergentes como la computación en la nube para mejorar la eficiencia y seguridad de los servicios digitales (p. 14).	Innovación, Ciberseguridad	Facilita la escalabilidad, flexibilidad y seguridad de los servicios digitales mediante tecnologías emergentes.
Marcos Legales y Regulatorios	Se plantea la actualización del marco legal para regular la protección de datos, identidad digital, ciberseguridad e inteligencia artificial (p. 15).	Marco Normativo, Ciberseguridad	Asegura que la organización cumpla con leyes sobre protección de datos, identidad digital e IA.
Habilidades Digitales	Se prioriza la formación de talento digital, capacitación en IA, TIC y competencias digitales para todos los sectores (p. 16).	Educación y Cultura Digital, Innovación	Desarrolla capacidades en TIC, IA y ciberseguridad, alineadas con la formación continua y la innovación.

La correspondencia entre las dimensiones del modelo y los ejes estratégicos de la política cubana permite afirmar que el diagnóstico no solo evalúa el estado actual de la seguridad digital institucional, sino que también orienta su alineación con los objetivos nacionales. Esta validación contextual refuerza la utilidad del modelo como herramienta de planificación estratégica, mejora continua y rendición de cuentas.

Además, la matriz evidencia que la seguridad digital no se limita a aspectos técnicos, sino que abarca liderazgo, cultura, habilidades, normativas y procesos, en consonancia con los enfoques sociotécnicos y de gobernanza multinivel promovidos internacionalmente. En este sentido, el modelo contribuye a posicionar la seguridad digital como eje transversal de la transformación institucional.

Requisitos que mide el *test* por cada dimensión

Con el objetivo de operacionalizar el modelo de Diagnóstico de Madurez en Seguridad Digital, se diseñó un conjunto de 160 ítems distribuidos en las nueve dimensiones estratégicas. Cada ítem representa un requisito específico que permite evaluar el grado de cumplimiento, integración y sostenibilidad de prácticas, políticas y capacidades institucionales en materia de seguridad digital. Estos requisitos fueron formulados a partir de una revisión crítica de las normativas cubanas y de los marcos internacionales expuestos anteriormente, principios de gobernanza digital, y lineamientos de la *Política Cubana de Transformación Digital*. Asimismo, se incorporaron criterios sociotécnicos, organizacionales y normativos que permiten capturar la complejidad del entorno digital institucional.

La estructura del test responde a una lógica modular, donde cada dimensión agrupa requisitos que abarcan desde aspectos técnicos y normativos hasta factores culturales, operativos y estratégicos. Esta organización facilita la aplicación del instrumento en distintos tipos de instituciones, permite identificar brechas específicas y orienta la formulación de planes de mejora contextualizados. A continuación, se presentan los requisitos evaluados por cada dimensión, acompañados de una breve descripción que justifica su inclusión y relevancia diagnóstica (Tabla 2).

Tabla 2. Requisitos evaluados por cada dimensión, acompañados de una breve descripción que justifica su inclusión y relevancia diagnóstica. Fuente: elaboración propia

Nº	Dimensión	Objetivo de los Ítems	Criterios Evaluados (Resumen)	Ítems Evaluados
1	**Liderazgo Digital**	Identificar estructuras de liderazgo, asignación de responsabilidades y visión institucional.	Políticas aprobadas, responsables designados, planificación estratégica, cultura de seguridad, recursos asignados.	24
2	**Políticas y Estrategias de Seguridad Digital**	Verificar coherencia normativa, actualización y efectividad de las políticas.	Existencia, alineación legal, difusión, auditoría, protocolos de respuesta, participación institucional.	26
3	**Puesto de Trabajo Digital**	Determinar condiciones técnicas, uso seguro de tecnologías y capacitación del personal.	Herramientas digitales, protección de dispositivos, automatización, gestión de accesos, respaldo.	13
4	**TIC (Tecnologías de la Información y la Comunicación)**	Evaluar robustez, interoperabilidad y actualización de sistemas.	Infraestructura, interoperabilidad, monitoreo, escalabilidad, integración externa.	20
5	**Cultura y Clima Digital**	Identificar valores, prácticas y percepciones que favorecen la seguridad digital.	Sensibilización, percepción del riesgo, ética digital, participación, retroalimentación.	12
6	**Marcos Legales y Regulatorios**	Verificar alineación legal, auditoría y adaptación normativa.	Legislación vigente, estándares internacionales, auditoría, capacitación jurídica.	20
7	**Migración a la Nube**	Evaluar planificación, gestión de proveedores y protección de datos en la nube.	Estrategia de adopción, seguridad virtual, continuidad operativa, autenticación.	19
8	**Operaciones Digitales**	Determinar eficiencia operativa y experiencia del usuario.	Digitalización, automatización, interoperabilidad, monitoreo, retroalimentación ciudadana.	14
9	**Habilidades Digitales**	Identificar preparación técnica, programas formativos y alineación institucional.	Diagnóstico de competencias, formación continua, certificaciones, redes de aprendizaje.	21

La siguiente tabla tabla 3 sintetiza los principales componentes del test, donde cada dimensión agrupa un conjunto de ítems que permiten evaluar prácticas, capacidades y políticas institucionales vinculadas a la seguridad digital. Además del número de ítems evaluados, se incluyen recomendaciones clave que orientan la interpretación de los resultados y la formulación de acciones de mejora según el nivel de madurez identificado.

Tabla 3. Tabla resumen que sintetiza las nueve dimensiones del test de Diagnóstico de Madurez en Seguridad Digital, el número de ítems evaluados en cada una, y las recomendaciones clave según los resultados esperados. Fuente: elaboración propia

Nº	Dimensión	Ítems Evaluados	Recomendaciones según resultados esperados
1	**Liderazgo Digital**	24	Fortalecer el compromiso directivo, asignar responsables, integrar la seguridad en la planificación estratégica.
2	**Políticas y Estrategias de Seguridad Digital**	26	Formalizar y actualizar políticas, alinearlas con marcos normativos, garantizar su difusión y aplicación efectiva.
3	**Puesto de Trabajo Digital**	13	Digitalizar procesos laborales, proteger dispositivos, capacitar al personal en el uso seguro de tecnologías.
4	**Tecnologías de la Información y la Comunicación (TIC)**	20	Modernizar infraestructura, asegurar interoperabilidad, implementar mecanismos de monitoreo y actualización tecnológica.
5	**Cultura y Clima Digital**	12	Promover campañas de sensibilización, fomentar valores digitales, medir percepción y participación institucional.
6	**Marcos Legales y Regulatorios**	20	Asegurar cumplimiento normativo, capacitar en legislación vigente, participar en procesos regulatorios.
7	**Migración a la Nube**	19	Diseñar estrategias de adopción, seleccionar proveedores seguros, proteger datos y garantizar continuidad operativa.
8	**Operaciones Digitales**	14	Automatizar trámites, mejorar experiencia del usuario, integrar plataformas y evaluar desempeño operativo.
9	**Habilidades Digitales**	21	Implementar programas de formación continua, diagnosticar competencias, incentivar el desarrollo profesional.

Aplicación e Interpretación del Test

El *test* de Diagnóstico de Madurez en Seguridad Digital se puede aplicar mediante una combinación de entrevistas semiestructuradas, revisión documental y observación directa, adaptado a las características organizativas de cada institución evaluada. Los 160 ítems distribuidos en las nueve dimensiones permiten una evaluación modular, flexible y contextualizada, facilitando la identificación de fortalezas, brechas y oportunidades de mejora.

Cada ítem se valora en una escala ordinal que refleja el grado de cumplimiento institucional, permitiendo clasificar los resultados en cuatro niveles de madurez, utilizando como referencia el sistema de evaluación que propone la tecnología TETR4DIG:

Básico: procesos de seguridad digital sin documentar, en cambio constante, dispuestos especialmente para un fin de forma reactiva.

Inicial: procesos de seguridad digital que siempre se ejecutan igual, con resultados constantes. Iniciada la implementación de medidas de seguridad digital en algunas áreas de la entidad.

Estratégico (procesos de seguridad digital de integración estratégica. Implementando hoja de ruta de seguridad digital de forma holística e integrada, con orientación centrada en los recursos de la empresa y los clientes, procesos estandarizados, definidos y documentados que sufren algún tipo de revisión en el tiempo).

Innovador-disruptivo: procesos de seguridad digital para la protección de los datos y la información al nivel del estado del arte, liderazgo digitales, mejora continua de la eficacia de los procesos mediante cambios e innovación tecnológica, procesos ágiles, innovadores, flexibles, conectados, colaborativos, abiertos, con uso de datos relevantes con protección en más de un soporte tecnológico. Se adaptan de forma continua a los cambios.

Esta clasificación permite construir perfiles de madurez por dimensión, identificar patrones comunes entre instituciones, y orientar la formulación de planes de mejora específicos. Además, facilita la comparación longitudinal y la evaluación del impacto de intervenciones estratégicas en seguridad digital.

Conclusiones

El presente artículo ha propuesto y validado un modelo de Diagnóstico de Madurez en Seguridad Digital diseñado específicamente para servicios de consultoría institucional. A partir de un enfoque sociotécnico e interdisciplinario, el modelo permite evaluar el grado de integración, sostenibilidad y alineación estratégica de la seguridad digital en organizaciones públicas y privadas, en consonancia con los ejes de la *Política Cubana de Transformación Digital* y los marcos internacionales de referencia (ISO/IEC 27001, NIST, UIT).

La estructura modular del diagnóstico (compuesta por nueve dimensiones estratégicas y 160 ítems evaluativos) facilita una caracterización integral del entorno digital institucional, abarcando desde el liderazgo y la cultura organizacional hasta la infraestructura tecnológica, las políticas normativas y las habilidades del personal. Esta amplitud permite identificar brechas específicas, orientar planes de mejora y fortalecer capacidades organizativas en función de una transformación digital segura, inclusiva y resiliente.

Los resultados obtenidos evidencian que la seguridad digital no puede abordarse como un componente técnico aislado, sino como un proceso transversal que exige liderazgo comprometido, gobernanza efectiva, formación continua y articulación normativa. En este sentido, el modelo se posiciona como una herramienta metodológica útil para consultores, gestores y responsables institucionales que buscan integrar la seguridad digital en sus procesos de planificación, evaluación y toma de decisiones.

Su aplicación no sustituye los servicios de Ciberseguridad que hoy están en la cartera de servicios de la Dirección de Consultoría, sino que puede identificar debilidades y oportunidades para que estos puedan ser contratados por quienes realicen el diagnóstico.

Finalmente, se destaca el potencial del diagnóstico como instrumento de monitoreo longitudinal, adaptable a distintos contextos sectoriales y escalable en función de los avances tecnológicos y regulatorios. Su aplicación sistemática puede contribuir al fortalecimiento de la cultura de seguridad, la mejora de la calidad institucional y el cumplimiento de los objetivos estratégicos de transformación digital en Cuba y otros entornos similares.

Bibliografía

De Armas Granado, L., Díaz Monjiotti, E., & Tito Bertor, A. (2021). *De la ciberseguridad a la seguridad digital en los servicios de consultoría de la Empresa de Telecomunicaciones de Cuba S.A*. En III Taller de Ciberseguridad “Bienestar para todos”. La Habana: ETECSA.

D’Antonio, G., & Olías de Lima, P. M. (2019). *Digital security en la nueva era de transformación digital*. Madrid: Real Instituto Elcano.

Decreto 104/2024. (2024). *Reglamento de la seguridad y protección de la información clasificada y limitada*. Gaceta Oficial de la República de Cuba.

Decreto 360/2019. (2019). *Sobre la seguridad de las TIC y la defensa del Ciberespacio Nacional*. Gaceta Oficial de la República de Cuba.

Decreto-Ley 78/2023. (2023). *Sobre la seguridad y protección de la información clasificada y limitada*. Gaceta Oficial de la República de Cuba.

ISO/IEC 27001. (2013). Information technology – Security techniques – Information security management systems – Requirements. Geneva: International Organization for Standardization.

ISO/IEC 27002. (2013). Information technology – Security techniques – Code of practice for information security controls. Geneva: International Organization for Standardization.

National Institute of Standards and Technology (NIST). (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). Gaithersburg, MD: U.S. Department of Commerce.

Observatorio de la Ciberseguridad. (s.f.). *Indicador de madurez en ciberseguridad*. Recuperado de https://observatoriociberseguridad.org

Política para la Transformación Digital, la Agenda Digital Cubana y la Estrategia de Inteligencia Artificial (2024).

Resolución 105/2021. (2021). *Reglamento sobre el Modelo de Actuación Nacional para la Respuesta a Incidentes de Ciberseguridad*. Gaceta Oficial de la República de Cuba.

Resolución 128/2019. (2019). *Reglamento de Seguridad de las TIC. Gaceta Oficial de la República de Cuba*.

13. Rojas Martos, Noel E. *Modelo de Seguridad Digital basado en la tecnología TETR4DIG. III Taller de Ciberseguridad*. La Habana: ETECSA. XVI Seminario Iberoamericano de Seguridad en las Tecnologías de la Información" (Palacio de las Convenciones. Cuba. 2024).

Siponen, M., & Pahnila, S. (2018). Hacia un modelo unificado de cumplimiento de la política de seguridad de la información. *Revista de Seguridad Informática, 34* (2), 45–62.

Solms, B. von, & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102.