INVESTIGACIÓN

Estudio piloto de evaluación de madurez de la seguridad digital en organizaciones cubanas

Pilot study to evaluate the maturity of digital security in Cuban organizations

Libán de Armas Granado[1*]

Recibido: 06/2023 | Aceptado: 09/2023 | Publicado: 12/2023

Resumen

La disrupción digital impacta en todas las dimensiones económicas, sociales y medioambientales, dando lugar a un nuevo sistema digitalmente entrelazado de la economía tradicional con la economía digital. La expansión de dispositivos conectados y la aceleración de aplicaciones de IoT, blockchain, 5G, cuántica y otras tecnologías, incrementa la superficie de ataque, genera mayores riesgos de seguridad cibernética, datos y privacidad, y desafía los programas de riesgo tradicionales. Este artículo tiene como objetivo analizar los resultados de la autoevaluación de madurez de la seguridad digital, del estudio piloto realizado en organismos de la Administración Central del Estado y empresas cubanas, en el período comprendido entre el 30 de agosto de 2022 y el 7 de junio de 2023. En el proceso de investigación se combinaron métodos teóricos, empíricos y estadísticos matemáticos, con un enfoque mixto. La aplicación del modelo y el test estructurado de evaluación preliminar de madurez digital, de la tecnología de gestión de transformación digital TETR4DIG, permitió un análisis con enfoque sistémico y holístico, como demanda la economía global hiperconectada. El índice de madurez digital en la dimensión de seguridad

1* Dirección de Consultoría. DCCH. Empresa de Telecomunicaciones de Cuba, S.A., ETECSA, Playa, La Habana, Cuba. liban.dearmas@etecsa.cu

digital fue de un 50,0%, equivalente a un nivel de madurez "inicial". El estudio tiene relevancia social e implicación práctica, por su aporte como herramienta de autodiagnóstico y guía, proporcionando información útil para la toma de decisiones en el proceso de elaboración e implementación de la Política de Transformación Digital y la Agenda Digital 2030 en Cuba, y para la estrategia y enfoque digital de cada organización.

Palabras clave: Seguridad digital; transformación digital; madurez digital.

Abstract

Digital disruption impacts all economic, social and environmental dimensions, giving rise to a new digitally intertwined system of the traditional economy with the digital economy. The expansion of connected devices and the acceleration of applications of IoT, blockchain, 5G, quantum and other technologies increases the attack surface, generates greater cybersecurity, data and privacy risks, and challenges traditional risk programs. This article aims to analyze the results of the digital security maturity self-assessment, of the pilot study carried out in organizations of the Central State Administration and Cuban companies, in the period between August 30, 2022 and June 7 2023. In the research process, theoretical, empirical and mathematical statistical methods were combined, with a mixed approach. The application of the model and the structured preliminary evaluation of digital maturity test, of the TETR4DIG digital transformation management technology, it allowed an analysis with a systemic and holistic approach, as demanded by the hyperconnected global economy. The digital maturity index in the digital security dimension was 50.0%, equivalent to an "initial" maturity level. The study has social relevance and practical implication, due to its contribution as a self-diagnosis tool and guide, providing useful information for decision-making in the process of elaboration and implementation of the Digital Transformation Policy and the 2030 Digital Agenda in Cuba, and for the digital strategy and approach of each organization.

Keywords: *Digital security; Digital transformation; Digital maturity.*

Introducción

La disrupción digital impacta en todas las dimensiones económicas, sociales y medioambientales, dando lugar a un nuevo sistema digitalmente entrelazado de la economía tradicional con la economía digital (CEPAL, 2021), (OIT/ILO, 2022). La expansión de dispositivos conectados y la aceleración de aplicaciones de IoT, blockchain, 5G, cuántica y otras tecnologías, incrementa la superficie de ataque, genera mayores riesgos de seguridad cibernética, datos y privacidad, y desafía los programas de riesgo tradicionales. La seguridad en la actualidad no sólo se refiere a la necesidad de proteger la red, el perímetro o los dispositivos, sino que también abarca la protección de todos los elementos que componen el entorno de trabajo, que incluye aplicaciones críticas para el negocio, infraestructura de mensajería y colaboración, servicios en la nube, comercio electrónico y aplicaciones de fabricación, plantas de producción, y muchos otros elementos, llegando hasta los empleados y la necesidad inminente de formarlos en este ámbito (Foro IT Digital Security, 2023).

La ciberseguridad debe analizarse más allá de la dimensión tecnológica. Debe ser abordada con una visión holística integrada, con un modelo multidimensional, y caracterizada como un proceso sistemático. En la dimensión relacionada con el talento, uno de los principales desafíos es el desarrollo de competencias por medio de programas flexibles y ágiles, que permitan responder a las amenazas que se hacen más sofisticadas de forma exponencial. En la dimensión cultural, se requiere cambios de conducta efectivos y concretos en todos los usuarios digitales; tanto en el contexto laboral, como también en los contextos digitales personales y ciudadanos. Esto requiere desarrollar estrategias y campañas comunicacionales que permitan un alcance a escala nacional; y revisar la conducta y la alineación de la estrategia y visión de negocios con la identidad y comportamiento digital de las instituciones. (Global Cyber Security Capacity Centre, 2016), (Centro de Innovación UC Anacleto Angelini, 2022) y (McKinsey & Company, 2023).

Este artículo tiene como objetivo exponer los resultados del estudio piloto de evaluación de madurez digital, realizado en organismos de la Administración Central del Estado y empresas cubanas, centrando el análisis en

la dimensión de capacidades tecnológicas de Seguridad Digital, y las relaciones con otras dimensiones de diseño organizacional y competencias estratégicas. La relevancia social e implicación práctica se vincula al impacto positivo que tiene, al proporcionar información útil para la toma de decisiones en la elaboración de la estrategia digital de cada organización; y para la implementación de la Política de Transformación Digital de Cuba y su Agenda Digital 2030. El estudio aporta un marco de medición referencial, que facilita diagnosticar de forma preliminar, el punto de partida o estado actual, y medir posteriormente el avance de la implementación.

Materiales y métodos

En esta investigación se combinaron métodos teóricos, empíricos y estadísticos matemáticos, con un enfoque mixto. La evaluación de madurez digital se basa en el modelo y la versión reducida del test estructurado, de la tecnología de gestión de transformación digital TETR4DIG, descrita en (de Armas Granado, Díaz Monjiotti, & Reyes León, 2022). La metodología del estudio piloto se desarrolló en las fases siguientes:

1) Selección y preparación de la herramienta de soporte para la recolección de la información: la encuesta estructurada se aplicó generalmente de forma *online*, soportada mediante la plataforma empresarial Moodle. También se aplicó de forma *offline* con una plantilla de Excel,

2) Preparación teórica del personal encargado de realizar la autoevaluación: alta dirección de cada organización.

3) Aplicación del test o encuesta estructurada: consta de 23 indicadores, uno de ellos específico para la Seguridad Digital, que se valoran de acuerdo a una escala ordinal de 5 criterios de puntuación, entre cero (0) y cuatro (4) puntos, según el nivel de implementación de cada requisito o iniciativa digital. La decisión se toma a partir de un proceso de discusión colectiva, buscando el consenso de los participantes.

4) Análisis de resultados y determinación de los índices de madurez: procesamiento estadístico para calcular los grados relativos de madurez digital global, por ámbitos, por perspectivas y por dimensiones, así como el nivel de madurez correspondiente. Los resultados se clasifican en cuatro niveles de madurez: Básico (0% a= 25%), Inicial (25% a = 50%), Estratégico (50% a = 75%) e Innovador Disruptivo (75% a = 100%).

5) Elaboración del informe de madurez digital, e información de resultados.

Las autoevaluaciones se realizaron en el período comprendido entre el 30 de agosto de 2022 y el 7 de junio de 2023. Las organizaciones que participaron en el estudio fueron las siguientes: Banco Central de Cuba (BCC); Centro de Ingeniería Genética y Biotecnología (CIGB); Empresa de Telecomunicaciones de Cuba, S.A. (ETECSA); Instituto Cubano de Radio y Televisión (ICRT); Instituto Nacional de Deporte y Recreación (INDER); Ministerio de Ciencia, Tecnología y Medio Ambiente (CITMA); Ministerio de Economía y Planificación (MEP); Ministerio de Educación (MINED); Ministerio de Justicia (MINJUS); Ministerio de Trabajo y Seguridad Social (MTSS); y el Ministerio de la Construcción (MICONS).

Resultados y discusión

Del total de organizaciones que participaron en el estudio piloto de madurez digital, el 54,5 % valoró que se encuentra habilitando requisitos e iniciativas digitales relacionadas con la dimensión de Seguridad Digital (ver tabla 1). Este indicador se refiere a las capacidades o disposición estratégica de tecnologías de ciberseguridad, que son necesarias para respaldar los procesos internos críticos asociados a la nueva propuesta de valor digital.

Seguridad Digital: Dispone/prevé inversiones de tecnologías de ciberseguridad: anti-fraude, anti-malware, auditoría técnica, contingencia/continuidad, control acceso/autenticación, inteligencia de seguridad, y de protección de comunicaciones, que fortalecen resiliencia.

Escala ordinal para evaluar requisitos e iniciativas digitales — Autoevaluación

Valor	Categoría	Descripción	Cantidad de entidades	Porciento (%)
0	No existente	Aún no se han adoptado actividades o iniciativas digitales disruptivas. Predominan enfoques o tecnologías analógicas y tradicionales *(legacy)*.	0	0.0
1	Iniciando	Se han iniciado actividades o iniciativas digitales que responden a necesidades o ideas aisladas. Aún no forman parte de la estrategia de la organización o de un plan de digitalización.	3	27.3

2	Habili-tando	Con actividades o iniciativas digitales incorpora-das a la estrategia de la organización, o en etapa de planificación, o de inversiones. Se realizan pruebas, proyectos piloto o de experimentación y ajuste.	6	54.5
3	Opera-cional	Con actividades o iniciativas digitales en etapa de puesta en marcha o generalización (se imple-menta en las operaciones diarias).	1	9.1
4	Opti-miza-do	Las actividades o iniciativas digitales están en etapa de optimización y mejora continua. Se aplica la I+D+i para incrementar la eficiencia y eficacia de la gestión.	1	9.1
TOTAL			11	100

Tabla 1. Resumen de las autoevaluaciones de la dimensión de Seguridad Digital.
Fuente: elaboración propia.

El Índice de madurez digital de la dimensión (IMDD) de Seguridad Digital promedio de las once organizaciones que se autoevaluaron fue de 50,00 %, y equivale a un nivel “inicial” de madurez digital (ver figura 1). De las 22 dimensiones autoevaluadas en el diagnóstico preliminar, esta fue la que mayor índice de madurez promedio alcanzó. En la figura 2 se muestra la distribución de los niveles de madurez alcanzados por las once organizaciones.

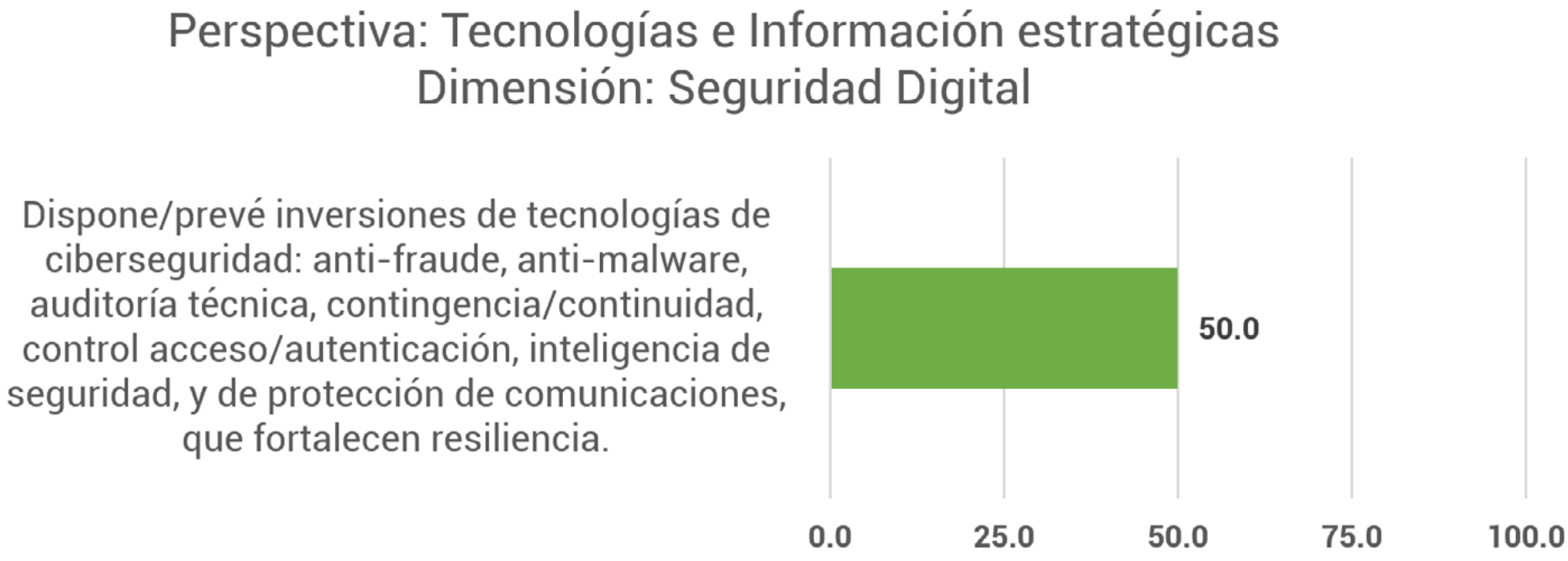

Figura 1. Índice de madurez digital de dimensión (IMDD) de Seguridad Digital.
Fuente: elaboración propia.

Para realizar un análisis holístico e integral, se debe analizar también el resultado de las autoevaluaciones de otras dimensiones de las perspectivas de diseño organizacional y competencias estratégicas, que influyen en la seguridad digital. Por ejemplo, algunos de los índi-

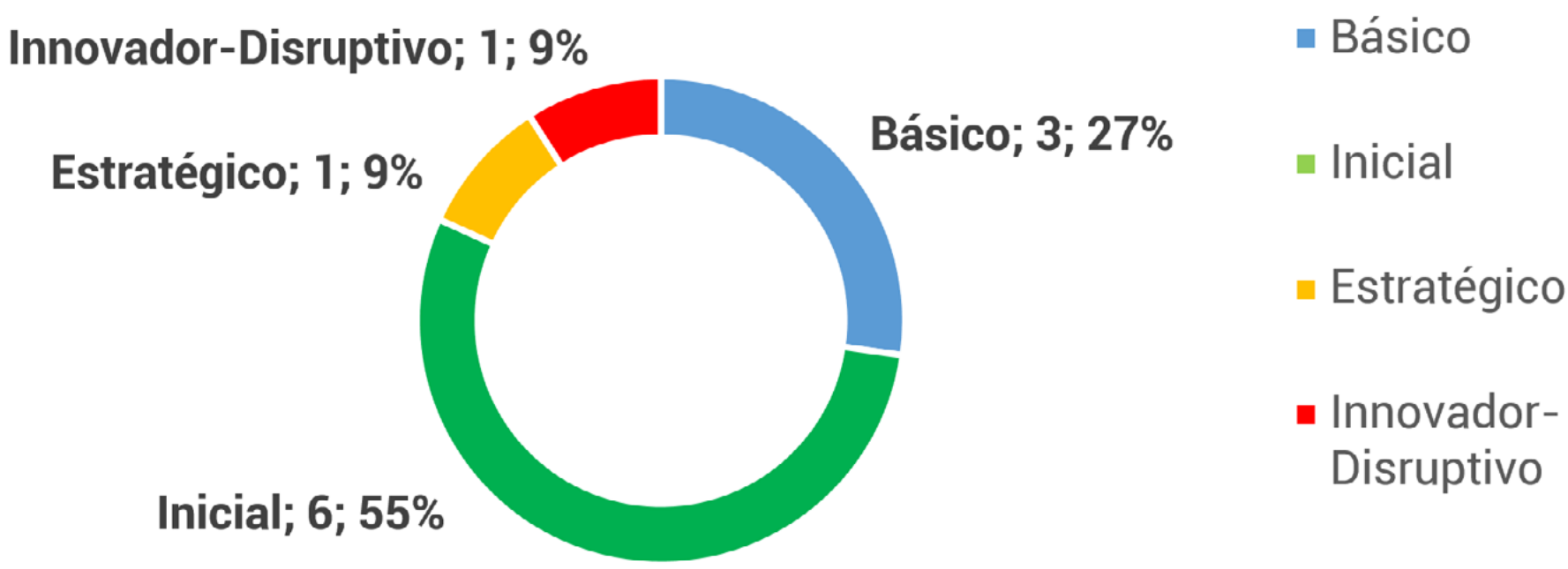

Figura 2. Cantidad de organizaciones por niveles de madurez digital de dimensión (IMDD) de Seguridad Digital.
Fuente: elaboración propia.

ces de madurez digital promedio de dimensiones (IMDD) fueron los siguientes: Liderazgo digital, 35.2%; mientras que Cultura y clima digital, Competencias digitales y Formación y desarrollo digital, obtuvieron un 20.5% cada una. La tendencia resultante de la evaluación de estas dimensiones, a partir de las once organizaciones estudiadas, se puede apreciar en la figura 3.

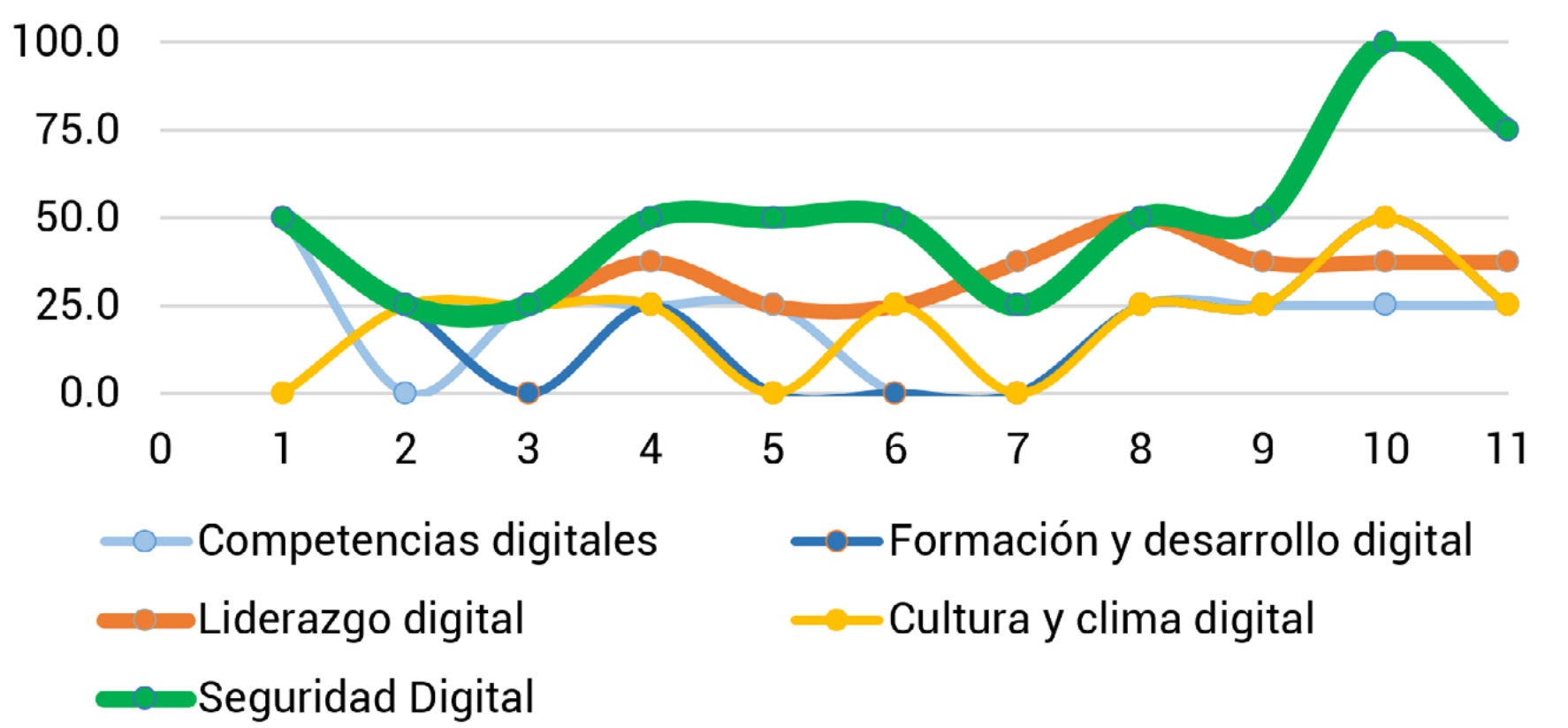

Figura 3. Gráfico de dispersión de índices de madurez digital de dimensiones (IMDD) relacionadas con la Seguridad Digital, para las once organizaciones del estudio piloto. Fuente: elaboración propia.

Exceptuando el resultado de la organización número siete, en todos los demás casos, la dimensión tecnológica de Seguridad digital fue la de mayor autoevaluación de madurez digital (ver figuras 3 y 4). Todas

estas dimensiones inciden de una forma u otra, en la seguridad digital, por lo que se puede inferir que existen otras brechas de capacidades estratégicas en materia de seguridad digital, no asociadas a los elementos tecnológicos, sino organizacionales, y culturales.

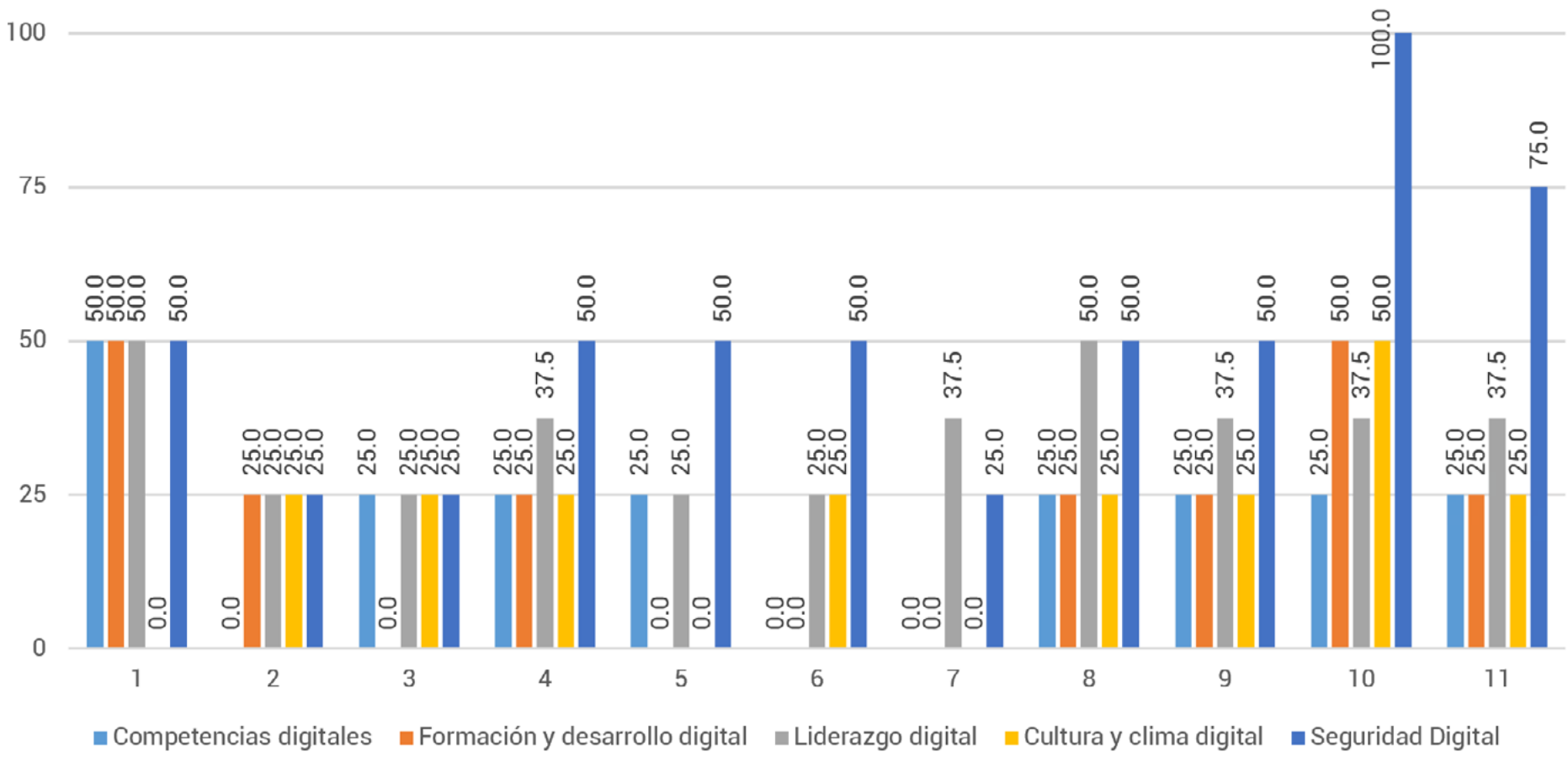

Figura 4. Cantidad de organizaciones por niveles de madurez digital de dimensión (IMDD) de Seguridad Digital.
Fuente: elaboración propia.

Conclusiones

El estudio piloto de modelo de madurez digital proporciona información útil preliminar para la toma de decisiones, en el proceso de elaboración de la estrategia digital de cada organización, y en particular, para el análisis de la Seguridad Digital con un enfoque holístico e integrado. Su aplicación en los organismos de la Administración Central del Estado y empresas, facilita la identificación de mejores prácticas nacionales, que puedan ser generalizadas, y detectar las mayores problemáticas respecto al aprovechamiento de capacidades tecnológicas disruptivas y otros intangibles, o respecto a la medición de los resultados de la transformación digital, y brinda insumos útiles para acelerar la implementación de la Política de Transformación Digital y la Agenda Digital 2030 en Cuba.

Se continúa la investigación en las líneas de desarrollo de la metodología para el diseño del *framework* de Seguridad Digital, y el test estructurado avanzado, que permita realizar una evaluación con mayor precisión. También se proyectan acciones de mejora en la automatización y acceso en línea de la herramienta.

Referencias

Centro de Innovación UC Anacleto Angelini. (2022). *Hoja de Ruta de Ciberseguridad: Iniciativa impulsada por Microsoft y el Centro de Innovación UC. Primera edición*. Centro de Innovación UC Anacleto Angelini. Obtenido de https://centrodeinnovacion.uc.cl/hoja-de-ruta-de-ciberseguridad/

CEPAL. (2021). *Tecnologías digitales para un nuevo futuro (LC/TS.2021/43)*. Santiago: Naciones Unidas. Recuperado el 12 de Septiembre de 2023, de https://www.cepal.org/es/publicaciones/46816-tecnologias-digitales-un-nuevo-futuro

de Armas Granado, L., Díaz Monjiotti, E., & Reyes León, G. E. (julio-septiembre de 2022). Evaluación de madurez de la transformación digital basada en el modelo TETR4DIG. *Revista Cubana de Transformación Digital*, 3(3), e177. Obtenido de https://rctd.uic.cu/rctd/article/download/177/89/1245

Foro IT Digital Security. (2023). *Estrategias de Ciberseguridad Inteligentes: hoja de ruta y mejores prácticas*. Foro IT Digital Security. Obtenido de https://ciberseguridadinteligente-foroitds.it-events.es/?s=PBOD

Global Cyber Security Capacity Centre. (2016). *Modelo de Madurez de Capacidades de Ciberseguridad para Naciones (CMM). Edición revisada*. University of Oxford. Oxford: The Global Cyber Security Capacity Centre. .

McKinsey & Company. (3 de April de 2023). *What is cybersecurity?* Obtenido de McKinsey & Company Web site: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-cybersecurity#:~:text=It's%20what%20organizations%20do%20to,%22%20%22

OIT/ILO. (2022). *Informe Regional Productividad. Transición digital, cambio tecnológico y políticas de desarrollo productivo en ALC: desafíos y oportunidades*. (Primera ed.). Ginebra: Oficina Internacional del Trabajo. Recuperado el 12 de Septiembre de 2023, de https://www.ilo.org/americas/publicaciones/WCMS_847153/lang-es/index.htm