2025 REPORTE DE CIBERSEGURIDAD GUATEMALA

Equipo ASEGURAR DATA

www.asegurardata.com
Email: asegurardata@asegurardata.com

ÍNDICE

Contenido

CONTEXTO

El presente documento tiene como propósito presentar los resultados obtenidos por Guatemala con base en el reporte 2025-Cybersecurity Report Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean[1] informe elaborado por el Banco Interamericano de Desarrollo – BID con el apoyo de la Organización de Estados Americanos – OEA y el Global Cybersecurity Capacity Centre University of Oxford – GCSCC.

Este estudio se basa en el Modelo CMM[2] promovido por el GCSCC de la Universidad de Oxford en su versión 2021. Este modelo es una "herramienta global diseñada para evaluar y fortalecer la **resiliencia digital** de los países. Este marco analiza la capacidad nacional a través de **cinco dimensiones críticas**, que abarcan desde la estrategia política y la cultura social hasta los marcos legales y los estándares tecnológicos. El modelo utiliza un sistema de **cinco etapas de madurez** —desde el nivel inicial hasta el dinámico."

El informe recopila la evolución de los resultados para los años 2016, 2020 y 2025, permitiendo conocer la evolución de los países de Latinoamérica en su modelo de madurez de ciberseguridad.

Desde ASEGURARDATA invitamos a todas las partes interesadas del país para que se profundice las diferentes temáticas involucradas en este resultado, se generen los respectivos debates, análisis y propuestas que sirvan de base para establecer un plan de escalamiento para fortalecer la ciberseguridad del país en todos los ámbitos.

[1] Inter American Development Bank (IDB), 2025
[2] Cybersecurity Capacity Maturity Model for Nations, 2021 Edition GCSCC Department of Computer Science, University of Oxford.

RESULTADOS GENERALES PARA AMÉRICA LATINA Y EL CARIBE

Reporte de Ciberseguridad 2025: Madurez y Desafios en Latinoamérica[3]

Este reporte elaborado conjuntamente por el Banco Interamericano de Desarrollo (BID), la Organización de los Estados Americanos (OEA) y el Global Cyber Security Capacity Centre (GCSCC) de la Universidad de Oxford, presenta un análisis detallado sobre la **madurez de las capacidades de ciberseguridad** en 30 países de América Latina y el Caribe (ALC). El informe actúa como una hoja de ruta para fortalecer la gobernanza digital y cerrar las brechas de vulnerabilidad en la región.

A continuación, se resumen los puntos clave de la fuente:

1. El Modelo de Evaluación (CMM)

El reporte utiliza el **Modelo de Madurez de la Capacidad de Ciberseguridad para Naciones (CMM)** en su edición 2021. Este modelo evalúa cinco dimensiones críticas:

- **Política y Estrategia:** Desarrollo de estrategias nacionales y respuesta a incidentes.
- **Cultura y Sociedad:** Mentalidad de seguridad y confianza en servicios en línea.
- **Conocimientos y Capacidades:** Educación, concienciación y formación profesional.
- **Marcos Legales:** Capacidad para legislar y perseguir el cibercrimen.
- **Estándares y Tecnologías:** Uso de controles técnicos y resiliencia de la infraestructura.

Cada dimensión se mide en una escala de cinco niveles: **Inicial (Start-up), Formativo, Establecido, Estratégico y Dinámico**.

2. Tendencias Regionales (2020-2025)

El análisis revela una **mejora generalizada** en la madurez de la región en comparación con el reporte de 2020.

- **Avances significativos:** El factor con mayor crecimiento fue la **Divulgación Responsable (D5.6[4])**, reflejando mejores marcos para

[3] Resumen basado en el documento original, utilizando IA NoteBookLM y verificado por el equipo de ASEGURARDATA
[4] Ver sección Marco Metodológico, página 4 a 10.

gestionar vulnerabilidades. También hubo avances en mecanismos de denuncia y ciberdefensa.

• **Capacidades consolidadas:** Los marcos legales y regulatorios (D4.1 y D4.2) siguen siendo las áreas más maduras en la mayoría de los países.

• **Debilidades persistentes:** La **Investigación e Innovación en Ciberseguridad (D3.4)** se mantiene como el factor menos desarrollado, ya que la inversión en esta área sigue siendo incipiente. Asimismo, la protección de infraestructura crítica sigue siendo un reto: solo 9 países están plenamente equipados para proteger sectores como hospitales o puertos.

3. Nuevos Desafíos: Inteligencia Artificial (IA)

El reporte destaca que la adopción masiva de la IA ha transformado el panorama de amenazas.

• **Amplificación de riesgos:** La IA permite a atacantes menos experimentados realizar ataques más sofisticados, como correos de *phishing* convincentes o generación de código malicioso.

• **Nuevas superficies de ataque:** Los propios sistemas de IA son vulnerables a ataques de "envenenamiento de datos" o manipulación de modelos.

• **Riesgos digitales amplios:** El uso de *deepfakes* para fraude y desinformación plantea retos que escapan a los marcos tradicionales de seguridad.

4. Equidad y Género en Ciberseguridad

El documento introduce conceptos fundamentales para el desarrollo inclusivo:

• **Inequidad Ciber:** Existe una brecha creciente entre las organizaciones grandes (con recursos y seguros contra ciberriesgos) y las PyMEs, que son la base económica de la región pero carecen de habilidades técnicas.

• **Perspectiva de Género:** Se resalta que las amenazas afectan de forma distinta según el género (ej. acoso en línea o filtración de datos sensibles). Solo el **25% de los profesionales** del sector son mujeres, lo que genera una falta de diversidad en la toma de decisiones estratégicas.

5. Conclusión y Llamado a la Acción

A pesar de que la mayoría de los países ya cuentan con estrategias nacionales, la **voluntad política** y el financiamiento sostenido son esenciales para pasar de la

planificación a la implementación efectiva. La ciberseguridad ya no es solo un tema técnico, sino un **pilar de la confianza para el desarrollo económico** y la estabilidad democrática.

MARCO METODOLÓGICO

El marco metodológico basado en el modelo CMM se resume a continuación:

Dimensión 1: Política y Estrategia de Ciberseguridad

Esta dimensión explora la capacidad de un país para desarrollar y entregar una estrategia nacional, así como para mejorar su resiliencia mediante la respuesta a incidentes, la ciberdefensa y la protección de infraestructuras críticas.

Tabla No 1

Factor	Alcance y Explicación
D 1.1: Estrategia Nacional	Evalúa la existencia de una agenda para priorizar la ciberseguridad, determinando responsabilidades, mandatos y asignación de recursos presupuestarios.
D 1.2: Respuesta a Incidentes y Manejo de Crisis	Revisa la capacidad sistemática para identificar incidentes nacionales, organizar la respuesta coordinada e integrarla en el marco nacional de gestión de crisis.
D 1.3: Protección de Infraestructura Crítica (CI)	Estudia la capacidad gubernamental para identificar activos críticos, establecer requisitos regulatorios específicos y asegurar que los operadores implementen buenas prácticas.
D 1.4: Ciberseguridad en Defensa y Seguridad Nacional	Explora el diseño e implementación de estrategias de ciberseguridad dentro de las fuerzas armadas y la colaboración entre entidades civiles y de defensa.

Fuente: 2025-Cybersecurity Report Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean

Dimensión 2: Cultura y Sociedad de Ciberseguridad

Esta dimensión revisa elementos de una cultura de ciberseguridad responsable, incluyendo la comprensión de riesgos, la confianza en servicios en línea y los mecanismos de denuncia.

Tabla No 2

Factor	Alcance y Explicación
D 2.1: Mentalidad de Ciberseguridad	Evalúa qué tanto se prioriza la seguridad en los valores y prácticas del gobierno, el sector privado y los usuarios en general.
D 2.2: Confianza en los Servicios en Línea	Revisa las habilidades de alfabetización digital de los usuarios, la gestión de la desinformación y el nivel de confianza en el gobierno y comercio electrónicos.
D 2.3: Comprensión de la Protección de Datos Personales	Analiza si los usuarios y las organizaciones reconocen la importancia de proteger la información personal y si son sensibles a sus derechos de privacidad.
D 2.4: Mecanismos de Denuncia	Explora la existencia de canales funcionales para que los usuarios reporten delitos como fraude, acoso, abuso infantil o violaciones de seguridad.
D 2.5: Medios y Plataformas en Línea	Revisa el papel de los medios de comunicación y redes sociales en la difusión de información y en la formación de valores y actitudes de ciberseguridad.

Fuente: 2025-Cybersecurity Report Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean

Dimensión 3: Creación de Conocimientos y Capacidades

Esta dimensión revisa la disponibilidad, calidad y adopción de programas educativos y de sensibilización para diversos grupos de interés.

Tabla No 3

Factor	Alcance y Explicación
D 3.1: Concienciación sobre Ciberseguridad	Se enfoca en programas nacionales coordinados por el gobierno, sector privado y sociedad civil para educar sobre riesgos y amenazas.
D 3.2: Educación en Ciberseguridad	Evalúa la oferta de programas académicos de alta calidad, la disponibilidad de educadores calificados y la colaboración para satisfacer la demanda nacional.
D 3.3: Formación Profesional en Ciberseguridad	Revisa la disponibilidad de formación técnica asequible para construir un cuerpo de profesionales certificados y la transferencia de habilidades dentro de las organizaciones.
D 3.4: Investigación e Innovación	Investiga la existencia de una cultura de investigación y desarrollo (I+D) con apoyo financiero, incentivos y producción de resultados utilizables en el país.

Fuente: 2025-Cybersecurity Report Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean

Dimensión 4: Marcos Legales y Regulatorios

Esta dimensión examina la capacidad del gobierno para diseñar, promulgar y hacer cumplir leyes nacionales relacionadas directa o indirectamente con la ciberseguridad.

Tabla No 4

Factor	Alcance y Explicación
D 4.1: Disposiciones Legales y Regulatorias	Aborda la legislación sobre ciberdelincuencia (sustantiva y procesal) y la realización de evaluaciones de impacto en los derechos humanos.
D 4.2: Marcos Legislativos Relacionados	Incluye leyes de protección de datos, protección infantil en línea, protección al consumidor y propiedad intelectual.
D 4.3: Capacidad Legal y Regulatoria	Estudia la capacitación y recursos de la policía para investigar, de los fiscales para presentar casos y de los tribunales para juzgar delitos informáticos.
D 4.4: Marcos de Cooperación contra el Cibercrimen	Revisa los mecanismos formales e informales de cooperación entre actores nacionales e internacionales y la colaboración público-privada.

Fuente: 2025-Cybersecurity Report Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean

Dimensión 5: Estándares y Tecnologías

Esta dimensión aborda el uso efectivo de tecnologías de ciberseguridad, la implementación de estándares internacionales y el despliegue de controles técnicos.

Tabla No 5

Factor	Alcance y Explicación
D 5.1: Adherencia a Estándares	Revisa la capacidad gubernamental para promover y monitorear el cumplimiento de estándares internacionales y buenas prácticas en adquisiciones.
D 5.2: Controles de Seguridad	Explora el despliegue de controles técnicos actualizados (como parches y respaldos) y el uso de técnicas criptográficas basadas en marcos establecidos.
D 5.3: Calidad del Software	Examina los requisitos funcionales del software y la existencia de políticas para su actualización y mantenimiento basadas en evaluaciones de riesgo.
D 5.4: Resiliencia de la Infraestructura de Internet	Aborda la confiabilidad de los servicios de infraestructura y la existencia de mecanismos de monitoreo y respuesta ante fallas o ataques.
D 5.5: Mercado de Ciberseguridad	Analiza la disponibilidad de tecnologías competitivas, servicios de consultoría, seguros contra ciber riesgos y la gestión de riesgos en la externalización (outsourcing).
D 5.6: Divulgación Responsable	Explora la existencia de marcos para recibir y difundir información sobre vulnerabilidades y las protecciones legales para quienes las reportan.

Fuente: 2025-Cybersecurity Report Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean

Para realizar las mediciones de cada factor se definen unos aspectos para facilitar la recopilación de evidencia y medición. Cada aspecto es analizado de acuerdo con las diferentes etapas de maduración. (Ver Tabla 7)

Los aspectos por factor son los siguientes:

Tabla No 6[5]

Dimensión	Factor	Aspectos [Página de referencia]
D1: Política y Estrategia de Ciberseguridad	**D 1.1: Estrategia Nacional de Ciberseguridad**	• Desarrollo de la Estrategia • Contenido • Implementación y Revisión • Compromiso Internacional • Organización.
	D 1.2: Respuesta a Incidentes y Manejo de Crisis	• Identificación y Categorización de Incidentes • Organización • Integración de la Ciberseguridad en el Manejo de Crisis Nacional • Coordinación y Modo de Operación
	D 1.3: Protección de Infraestructura Crítica (CI)	• Identificación • Requisitos Regulatorios • Práctica Operativa • Organización • Respuesta y Gestión de Riesgos.
	D 1.4: Ciberseguridad en Defensa y Seguridad Nacional	• Estrategia de Ciberseguridad de las Fuerzas de Defensa • Capacidad de Ciberseguridad de las Fuerzas de Defensa • Coordinación de Defensa Civil • Organización • Coordinación.
D2: Cultura de Ciberseguridad y Sociedad	**D 2.1: Mentalidad de Ciberseguridad**	• Conciencia de los Riesgos • Prioridad de la Seguridad • Prácticas • Gobierno • Sector Privado • Usuarios
	D 2.2: Confianza en los Servicios en Línea	• Alfabetización y Habilidades Digitales • Confianza del Usuario en la Búsqueda e Información en Línea • Desinformación • Confianza del Usuario en Servicios de Gobierno Electrónico • Confianza del Usuario en Servicios de Comercio Electrónico
	D 2.3: Comprensión del Usuario sobre Protección de Información Personal	• Protección de Información Personal en Línea
	D 2.4: Mecanismos de Denuncia	• Mecanismos de Denuncia
	D 2.5: Medios y Plataformas en Línea	• Medios de Comunicación y Redes Sociales
D3: Creación de Conocimientos y Capacidades	**D 3.1: Fomento de la Concientización en Ciberseguridad**	• Iniciativas de Concientización del Gobierno • Iniciativas de Concientización del Sector Privado • Iniciativas de Concientización de la Sociedad Civil •

[5] Para mayor precisión del nivel de madurez de los diferentes aspectos se puede revisar el documento Cybersecurity Capacity Maturity Model for Nations, 2021 Edition GCSCC Department of Computer Science, University of Oxford.

		Concientización Alta dirección pública y privada • Programas de concientización.
	D 3.2: Educación en Ciberseguridad	• Provisión • Administración
	D 3.3: Formación Profesional en Ciberseguridad	• Provisión • Adopción
	D 3.4: Investigación e Innovación en Ciberseguridad	• Investigación y Desarrollo (I+D) en Ciberseguridad
D4: Marcos Legales y Regulatorios	**D 4.1: Disposiciones Legales y Regulatorias**	• Legislación Sustantiva sobre Ciberdelincuencia • Requisitos Legales y Regulatorios para la Ciberseguridad • Legislación Procesal sobre Ciberdelincuencia • Evaluación de Impacto en los Derechos Humanos • Marcos legislativos para la seguridad de las TIC • Privacidad, libertad de expresión y otros derechos humanos en línea.
	D 4.2: Marcos Legislativos Relacionados	• Legislación de Protección de Datos • Protección Infantil en Línea • Legislación de Protección al Consumidor • Legislación de Propiedad Intelectual.
	D 4.3: Capacidad Legal y Regulatoria	• Aplicación de la Ley • Procesos Acusatorios • Tribunales • Órganos Regulatorios.
	D 4.4: Marcos de Cooperación Formal e Informal contra la Ciberdelincuencia	• Cooperación de las Fuerzas del Orden con el Sector Privado • Cooperación con Contrapartes Extranjeras de las Fuerzas del Orden • Colaboración entre el Gobierno y el Sector de Justicia Penal • Cooperación Formal • Cooperación Informal.
D5: Estándares y Tecnologías	**D 5.1: Adhesión a Estándares**	• Estándares de Seguridad TIC • Estándares en Implementación de TI • Estándares para la Implementación de Productos y Servicios digitales.
	D 5.2: Controles de Seguridad	• Controles de Seguridad Tecnológica • Controles Criptográficos.
	D 5.3: Calidad del Software	• Calidad y Garantía del Software
	D 5.4: Resiliencia de la Infraestructura de Internet y Comunicaciones	• Confiabilidad de la Infraestructura de Internet • Monitoreo y Respuesta.
	D 5.5: Oferta de Ciberseguridad	• Tecnologías de Ciberseguridad • Servicios y Competencias en Ciberseguridad • Implicaciones de

	la Externalización de la Seguridad • Ciberseguros • Seguros Cibercrimen.
D 5.6: Divulgación Responsable	• Intercambio de Información sobre Vulnerabilidades • Políticas, Procesos y Legislación para la Divulgación Responsable de Fallas de Seguridad.

Fuente: Elaboración Propia

EVOLUCIÓN MADUREZ MODELO CMM GUATEMALA 2016, 2020 Y 2025

A continuación se presentan los resultados de medición del modelo CMM de Guatemala para los años 2016, 2020 y 2025:

Tabla No 7

Dimensión / Factor	2016	2020	2025
D1: Política y Estrategia			
D1.1 Estrategia Nacional de Ciberseguridad	1	3	**3**
D1.2 Respuesta a Incidentes y Manejo de Crisis	1	2	**2**
D1.3 Protección de Infraestructura Crítica (CI)	1	1	1
D1.4 Ciberseguridad en Defensa y Seguridad Nacional	1	1	2
D2: Cultura y Sociedad			
D2.1 Mentalidad de Ciberseguridad	1	2	2
D2.2 Confianza en los Servicios en Línea	2	2	2
D2.3 Comprensión de la Protección de Datos Personales	NA	2	1
D2.4 Mecanismos de Denuncia	NA	1	1
D2.5 Medios y Plataformas en Línea	NA	2	1
D3: Conocimientos y Capacidades			
D3.1 Concienciación sobre Ciberseguridad	2	2	**2**
D3.2 Educación en Ciberseguridad	2	2	**3**
D3.3 Formación Profesional en Ciberseguridad	2	2	2
D3.4 Investigación e Innovación en Ciberseguridad	N/A	N/A	2
D4: Marcos Legales y Regulatorios			
D4.1 Disposiciones Legales y Regulatorias	2	2	2
D4.2 Marcos Legislativos Relacionados	NA	2	2
D4.3 Capacidad Legal y Regulatoria	2	2	2

Dimensión / Factor	2016	2020	2025
D4.4 Marcos de Cooperación contra el Cibercrimen	NA	2	2
D5: Estándares y Tecnologías			
D5.1 Adherencia a Estándares	1	2	2
D5.2 Controles de Seguridad	NA	2	2
D5.3 Calidad del Software	NA	2	1
D5.4 Resiliencia de la Infraestructura de Internet	NA	NA	3
D5.5 Mercado de Ciberseguridad	1	2	2
D5.6 Divulgación Responsable	NA	NA	**2**

Fuente: Elaboración Propia

Con base en la anterior tabla, la tendencia de la evolución entre el año 2016, 2020 y 2025 ha sido mínima lo cual se evidencia en el informe para el país que se encuentra en las páginas 108 y 109 del informe 2025-Cybersecurity Report Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean. El cual hemos resumido de la siguiente manera[6]:

Resumen Resultados

El informe de 2025 para **Guatemala** (páginas 108 y 109 del reporte de país) destaca un país en una fase de fortalecimiento institucional, pero que enfrenta barreras críticas, principalmente en su marco legal y en la cultura digital ciudadana.

A continuación, se presenta un resumen de las conclusiones y los puntos de fricción que han obstaculizado un progreso más ágil entre 2020 y 2025:

Conclusiones Institucionales

• **Gobernanza Fortalecida:** Se destaca la consolidación del Comité Nacional de Ciberseguridad (**CONCIBER**) y la elevación de la ciberseguridad a una **prioridad de desarrollo nacional** dentro de la Política de Gobierno 2024-2028.

• **Liderazgo Educativo:** Guatemala se mantiene como un referente regional en **educación superior**, con universidades (Galileo, del Valle, Mariano Gálvez, entre

[6] Este resumen contempla los aspectos a resaltar que se encuentran en el documento original y los cuellos de botella o puntos de fricción que enfrenta el país.

otras) que ofrecen maestrías especializadas y fortalecen el capital humano técnico.

• **Resiliencia Financiera:** El sector financiero es el más avanzado, gracias a la labor de **BanCERT** y al cumplimiento de normativas de gestión de riesgo tecnológico como la **JM-104-2021**.

Puntos de Fricción que impiden el avance (2020-2025)

A pesar de los esfuerzos, existen cuatro obstáculos principales identificados en las fuentes que han generado un "estancamiento" en ciertas dimensiones:

1. **El "Cuello de Botella" Legislativo:** Este es el punto de fricción más grave. La **Iniciativa de Ley 5254** (Ley contra la Ciberdelincuencia) ha estado bajo revisión legislativa desde **2017** sin ser aprobada definitivamente. Esta parálisis impide que el país se adhiera al **Convenio de Budapest** y debilita la capacidad procesal para perseguir delitos informáticos.

2. **Ausencia de una Campaña Nacional de Concientización:** A diferencia de sus vecinos, Guatemala carece de un esfuerzo estatal masivo y unificado para educar a la población. La mayoría de los ciudadanos sigue siendo vulnerable a ataques básicos como el *phishing* porque la **alfabetización digital** no ha crecido a la par del acceso a la tecnología.

3. **Falta de Mandatos para Infraestructura Crítica:** Si bien se alienta a los sectores esenciales a seguir buenas prácticas (como NIST), **no existe un requisito regulatorio** que obligue a los operadores de infraestructura crítica a implementar estándares de seguridad mínimos, lo que genera una protección desigual y fragmentada en el país.

4. **Capacidad Operativa en Tiempo Real:** Aunque el **CSIRT-GT** trabaja con los ministerios, todavía existe una brecha en la capacidad de **detección de amenazas en tiempo real** y en la respuesta unificada ante incidentes a nivel nacional, lo que mantiene al país en una etapa mayormente formativa en esta área.

RESULTADOS COMPARATIVOS

Con el objetivo de establecer un comparativo entre los resultados de Guatemala y cuatro países de Centroamérica (Costa Rica, Panamá, El Salvador y Honduras) para el año 2025, se presentan dos escenarios comparativos. El primero a nivel de factores y el segundo a nivel de dimensiones.[7]

Comparativo Factores

Se seleccionaron 5 factores, teniendo en cuenta que fueran los de mayor avance para el país o los más significativos para la región. Los factores seleccionados fueron:

- D1.1: Estrategia Nacional
- D1.2: Respuesta a Incidentes
- D3.2: Educación en Ciberseguridad
- D4.1: Disposiciones Legales
- D5.6: Divulgación Responsable

Para entender la tabla comparativa y el significado de cada nivel, la interpretación se puede visualizar a continuación:

Tabla No 8

Nivel	Etapa (Nombre)	Definición y Equivalencia de Capacidad
1	**Inicial (Start-up)**	La capacidad es **inexistente o embrionaria**. Puede haber discusiones iniciales, pero **no se han tomado acciones concretas** y suele haber una ausencia de evidencia observable.
2	**Formativa (Formative)**	Algunas características han comenzado a crecer y formularse, pero son **ad hoc, desorganizadas o mal definidas**. Sin embargo, la evidencia de esta actividad ya puede demostrarse claramente.
3	**Establecida (Established)**	Los indicadores están vigentes y funcionan. El aspecto es funcional y está definido, pero **no hay una consideración profunda sobre la asignación de recursos** o decisiones estratégicas de inversión.

[7] Este mismo tipo de análisis se pueden realizar para todos los factores o una combinación de ellos para ampliar así el contexto general evaluado por el modelo CMM.

Nivel	Etapa (Nombre)	Definición y Equivalencia de Capacidad
4	**Estratégica (Strategic)**	Se han tomado decisiones conscientes sobre **qué partes del aspecto son prioritarias** y cuáles no, basándose en las circunstancias particulares de la organización o de la nación.
5	**Dinámica (Dynamic)**	Existen mecanismos claros para **alterar la estrategia rápidamente** según el entorno de amenazas o cambios tecnológicos. El país demuestra **liderazgo global** y toma decisiones rápidas para reasignar recursos.

Fuente: Cybersecurity Capacity Maturity Model for Nations, 2021 Edition

Con base en los anteriores factores tomados del modelo CMM, se obtuvo el siguiente resultado:

Tabla No 9

Dimensión / Factor	Guatemala	Costa Rica	Panamá	El Salvador	Honduras
D1.1: Estrategia Nacional	Nivel 3	Nivel 4	Nivel 3	Nivel 2	Nivel 2
D1.2: Respuesta a Incidentes	Nivel 2	Nivel 3	Nivel 3	Nivel 3	Nivel 2
D3.2: Educación en Ciberseguridad	Nivel 3	Nivel 3	Nivel 3	Nivel 2	Nivel 2
D4.1: Disposiciones Legales	Nivel 2	Nivel 4	Nivel 2	Nivel 3	Nivel 1
D5.6: Divulgación Responsable	Nivel 2	Nivel 3	Nivel 3	Nivel 2	Nivel 1

Fuente: Elaboración propia

Con base en la información disponible en el informe 2025-Cybersecurity Report Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean, el comparativo de los factores analizados se puede resumir de la siguiente forma:

1. D1.1: Estrategia Nacional de Ciberseguridad

Este factor evalúa la existencia, contenido e implementación de una agenda nacional que priorice la ciberseguridad.

Guatemala (Nivel 3 - Establecido): Ha logrado avances significativos mediante el Comité Nacional de Ciberseguridad (**CONCIBER**) y la integración de la ciberseguridad en la Política de Gobierno 2024-2028.

• **Costa Rica (Nivel 4 - Estratégico):** Posee una estrategia robusta (2023-2027) con enfoque en derechos humanos y liderazgo nacional tras los ciberataques de 2022.

• **Panamá (Nivel 3 - Establecido):** Mantiene vigente su estrategia 2021-2024 bajo la Autoridad Nacional para la Innovación Gubernamental (AIG).

• **El Salvador (Nivel 2 - Formativo):** Se encuentra en una etapa de transición tras la creación de la Agencia del Estado (ACE) en 2024.

• **Honduras (Nivel 2 - Formativo):** Su estrategia nacional es esperada para el año 2025.

2. D1.2: Respuesta a Incidentes y Manejo de Crisis

Mide la capacidad del gobierno para identificar incidentes de manera sistemática y coordinar la respuesta.

• **Guatemala (Nivel 2 - Formativo):** Posee un **CSIRT-GT** activo que trabaja en protocolos de respuesta, pero aún se encuentra en fase de desarrollo de capacidades en tiempo real.

• **Costa Rica (Nivel 3 - Establecido):** Cuenta con un **SOC** (Centro de Operaciones de Seguridad) y un **CSIRT-CR** consolidados, con reporte de incidentes obligatorio en 24 horas.

• **Panamá (Nivel 3 - Establecido):** Su CSIRT nacional, activo desde 2011, tiene un rol formalizado en la protección de infraestructuras.

• **El Salvador (Nivel 3 - Establecido):** Ha implementado SOCS específicos, destacando el primer SOC para el sector financiero en la región.

• **Honduras (Nivel 2 - Formativo):** Su capacidad operativa es aún incipiente y está en proceso de formación de su equipo experto.

3. D3.2: Educación en Ciberseguridad

Revisa la disponibilidad de programas académicos de alta calidad y la formación de docentes.

• **Guatemala (Nivel 3 - Establecido):** Alcanza este nivel gracias a maestrías especializadas en universidades como Galileo, del Valle e Internaciones.

• **Costa Rica (Nivel 3 - Establecido):** Posee una oferta universitaria acreditada y está desarrollando un marco nacional de educación en ciberseguridad.

• **Panamá (Nivel 3 - Establecido):** Ofrece programas técnicos y grados académicos sólidos en la UTP y la Universidad de Panamá.

• **Honduras y El Salvador (Nivel 2 - Formativo):** Se centran en diplomados, cursos para PYMES y alianzas técnicas (como con Cisco), pero carecen de grados académicos de ciberseguridad plenamente integrados.

4. D4.1: Disposiciones Legales y Regulatorias

Aborda la legislación sobre ciberdelincuencia y la protección de los derechos humanos.

• **Guatemala (Nivel 2 - Formativo):** Presenta un **rezago normativo**, ya que sus iniciativas de ley de ciberdelincuencia y protección de datos siguen en revisión legislativa.

• **Costa Rica (Nivel 4 - Estratégico):** El país es firmante del **Convenio de Budapest** y pose marcos legales maduros alineados con estándares internacionales.

• **Panama (Nivel 2 - Formativo):** Ha desarrollado marcos normativos que están en proceso de consolidación.

• **El Salvador (Nivel 3 - Establecido):** Aprobó leyes críticas de ciberseguridad y protección de datos en 2024.

• **Honduras (Nivel 1 - Inicial):** Define delitos informáticos en su Código Penal, pero carece de normas procesales para la evidencia electrónica.

5. D5.6: Divulgación Responsable

Explora mecanismos para recibir y difundir información sobre vulnerabilidades técnicas.

• **Guatemala y El Salvador (Nivel 2 - Formativo):** Cuentan con esfuerzos sectoriales (especialmente financieros), pero carecen de un marco nacional unificado de protección legal para quien reporta incidentes.

• **Costa Rica y Panamá (Nivel 3 - Establecido):** Han institucionalizado guías y protocolos para la gestión de fallas de seguridad.

• **Honduras (Nivel 1 - Inicial):** No presenta mecanismos formales de divulgación responsable a nivel nacional

Comparativo Dimensiones

Con respecto al resultado para 2025 y comparando las 5 dimensiones para Guatemala, Panamá, Costa Rica, El Salvador y Honduras, el comportamiento de Guatemala es:

1. Posicionamiento Estratégico (Dimensión 1)

Guatemala ha alcanzado un **Nivel 3 (Establecido)** en el desarrollo de su **Estrategia Nacional**, situándose a la par de **Panamá** y por encima de **El Salvador** (Nivel 2) y **Honduras** (Nivel 1). Este avance se debe a la formalización del Comité Nacional de Ciberseguridad (**CONCIBER**) y la integración de la ciberseguridad en la Política de Gobierno 2024-2028. Sin embargo, aún se encuentra por detrás de **Costa Rica** (Nivel 4), que ha logrado un enfoque estratégico más robusto tras los graves ciberataques sufridos en 2022.

2. Fortaleza en Capital Humano y Academia (Dimensión 3)

Una de las mayores fortalezas competitivas de Guatemala es la **educación en ciberseguridad**, donde alcanza un **Nivel 3 (Establecido)**. El país supera a Honduras y El Salvador en este rubro gracias a la disponibilidad de **programas de maestría** y certificaciones técnicas ofrecidas por universidades como Galileo, del Valle y Mariano Gálvez. Esta capacidad de generar talento de alto nivel coloca a Guatemala en el mismo peldaño que Panamá, consolidándose como un **proveedor regional de profesionales especializados**.

3. El "Cuello de Botella" Legislativo (Dimensión 4)

La brecha más crítica para Guatemala se encuentra en su **marco legal**, donde permanece en un **Nivel 2 (Formativo)**. A diferencia de **Costa Rica**, que han alcanzado el Nivel 4 al adherirse a estándares internacionales como el **Convenio de Budapest**, Guatemala tiene sus principales herramientas legales (como la **Iniciativa de Ley 5254** de ciberdelincuencia y la ley de protección de datos) aún en revisión legislativa. Esta falta de un marco jurídico vigente limita la capacidad del país para procesar delitos informáticos en comparación con **El Salvador**, que ya subió al Nivel 3 con leyes aprobadas en 2024.

4. Capacidad Operativa y Respuesta (Dimensiones 1 y 5)

En cuanto a la **Respuesta a Incidentes (D1.2)** y la **Divulgación Responsable (D5.6)**, Guatemala opera en un **Nivel 2 (Formativo)**. Aunque cuenta con un **CSIRT-GT activo** y guías de riesgo para el sector financiero (JM-104-2021), todavía carece de la infraestructura técnica y los protocolos de respuesta en tiempo real que han llevado a **Costa Rica** al Nivel 4.

Cuadro Resumen por dimensiones:

Tabla No 10

Área de Comparación	Guatemala frente a la Región
Gobernanza	**Líder intermedio.** Superior a Honduras/El Salvador, pero inferior a Costa Rica.
Educación	**Avance regional.** A la par de Panamá; eje fundamental de su resiliencia.
Legislación	**Punto crítico.** Guatemala es el país con el mayor rezago normativo entre los comparados.
Infraestructura	**En desarrollo.** Posee la base (CSIRT), pero falta integración estratégica nacional.

Fuente: Elaboración propia

CONCLUSIONES

Mientras no exista un avance en los temas de ciberseguridad de los países de América Latina, estos estarán expuestos a limitaciones en su desarrollo económico, político y social. Existen diversas fuentes que han analizado esta relación entre madurez de la ciberseguridad y las capacidades para aprovechar la economía digital. Con base en un reciente estudio realizado por ASEGURARDATA, revisando diversas fuentes relacionadas con este temática, se puede resumir este tipo de análisis de la siguiente forma:

La rápida digitalización, aunque beneficiosa, ha ampliado la superficie de ataque, creando una brecha crítica entre naciones desarrolladas y países menos adelantados.

A continuación, se resumen los puntos principales de las fuentes:

1. Marcos de Evaluación y Madurez Nacional

Para medir la capacidad defensiva de un país, se utilizan principalmente dos índices:

• **Índice Global de Ciberseguridad (GCI):** Mide el compromiso de los países a través de cinco pilares: medidas legales, técnicas, organizativas, desarrollo de capacidades y cooperación.

• **Índice Nacional de Ciberseguridad (NCSI):** Se enfoca en la **preparación operativa** para gestionar incidentes. Un concepto clave es la "Diferencia" entre el nivel de digitalización y el de seguridad; si la digitalización avanza más rápido que la protección, se genera una vulnerabilidad sistémica.

2. Impacto Macroeconómico y Resiliencia

La ciberseguridad influye directamente en el **Producto Interno Bruto (PIB)**, especialmente en economías emergentes.

• **Correlación negativa:** En países de ingresos medios y bajos, un aumento del 1% en ciberincidentes se asocia con una caída del 0,0138% en el PIB per cápita.

• **Caso de estudio:** El ataque de *ransomware* en **Costa Rica (2022)** provocó una pérdida estimada de hasta el **2,4% de su PIB**, subrayando que la seguridad es vital para la continuidad del Estado.

• **Canales de riesgo:** Los ataques afectan la economía mediante la distorsión de la producción, el daño reputacional que aleja la inversión extranjera y la erosión de la confianza ciudadana.

3. Pilares de la Transformación Digital (Marco DE4A)

El Banco Mundial identifica cinco fundamentos necesarios para una economía digital segura: **infraestructura, plataformas públicas, servicios financieros, emprendimiento y habilidades digitales**. Se destaca que la baja ciberseguridad es responsable del fracaso de hasta el 80% de los proyectos de e-gobierno en países en desarrollo.

4. Desafíos Críticos: PYMES y Talento Humano

• **Inequidad Cibernética:** Las pequeñas y medianas empresas son el eslabón más débil; el 75% no sobreviviría a un ataque de *ransomware* debido a presupuestos limitados y falta de expertos.

• **Brecha de Talento:** Existe un déficit global de **4 millones de profesionales** de ciberseguridad. La crisis es más aguda en el sector público, donde casi la mitad de las organizaciones carecen de personal capacitado.

5. El Rol de la Inteligencia Artificial y el Futuro

La IA actúa como una **"paradoja"**: mientras el 72% de las organizaciones ven mayores riesgos por ataques automatizados o *deepfakes*, la mayoría de los profesionales la ven como una oportunidad para mejorar la detección temprana y la respuesta defensiva. Además, se introduce la **"Transición Gemela"**, que busca el avance simultáneo hacia una economía digital y una economía verde de cero emisiones.

6. Modelos de Éxito y Recomendaciones

Las fuentes recomiendan integrar la ciberseguridad de forma transversal en las políticas nacionales, fomentar asociaciones público-privadas y dar apoyo específico a las PYMES.

7. Fuentes Consultadas: Para aquellos que quieran ampliar los impactos de la ciberseguridad en el desarrollo económico, pueden consultar las siguientes fuentes:

1. Global Cybersecurity Index 2024 - ITU, https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

2. ITU Global Cybersecurity Index 2024: A Changing Cybersecurity Landscape - Codesealer, https://codesealer.com/blog/itu-global-cybersecurity-index-2024-a-changing-cybersecurity-landscape

3. Cybersecurity as a catalyst for digital transformation and economic development: A fuzzy system dynamics approach - CEUR-WS.org, https://ceur-ws.org/Vol-4024/paper26.pdf

4. Cybersecurity for Sustainable and Digital Economic Transformations | Asian Development Bank, https://www.adb.org/sites/default/files/institutional-document/1052731/adpr2025bp-cybersecurity-digital-economic-transformations.pdf

5. Cybersecurity Economics - World Bank, https://www.worldbank.org/en/topic/digital/publication/Cybersecurity-Economics-for-Emerging-Markets

---

Fecha de Elaboración:

7 de enero de 2026

EQUIPO ASEGURARDATA