MÉXICO

IMC 2025

Índice de Madurez en Ciberseguridad de las IES Iberoamericanas

metared by universia

Secretaría General Iberoamericana
Secretaria-Geral Ibero-Americana

Realización
MetaRed by Universia - Fundación Universia

Dirección
Jesús Martínez Martínez

Equipo técnico
Jesús Martínez Martínez
Patricia Pandrini
Paula Venosa
Gastón Zamorano Seguel
Daniel Felipe Genta García
Ricardo Estévez Serrano

Edición
MetaRed by Universia - Fundación Universia

Diseño
María Moraleja Vicente

MÉXICO

IMC 2025

Índice de Madurez en Ciberseguridad de las IES Iberoamericanas

metared by universia

Secretaría General Iberoamericana
Secretaria-Geral Ibero-Americana

Contenidos IMC 2025.

Prólogo

En un momento en el que la transformación digital está redefiniendo la universidad, en MetaRed tenemos la firme convicción de que la ciberseguridad ha dejado de ser un asunto técnico para convertirse en un pilar estratégico sin el cual no hay futuro digital posible. Proteger lo que somos y lo que construimos es hoy indispensable para mantener la confianza y asegurar que nuestras instituciones puedan avanzar sin miedo.

Esta realidad es la que nos impulsa a fortalecer la colaboración y el apoyo mutuo. Ninguna universidad puede recorrer este camino sola, y ahí MetaRed cobra sentido: **conectar talento, compartir experiencias y construir soluciones comunes para retos que también son comunes.**

Con esa ambición nació en 2024 el Índice de Madurez en Ciberseguridad (IMC). Lo que comenzó como una iniciativa modesta se ha convertido en un año en una herramienta clave para la región. La edición 2025 lo demuestra: 308 instituciones y un proyecto que pasa de 7 a 9 países con la incorporación de Brasil y Perú. Más que cifras, son señales de confianza y de un proyecto que ya no es piloto, sino un instrumento real para orientar la mejora institucional.

Pero el valor del IMC no reside solo en los datos, sino en lo que posibilita como comunidad: **aprender, compararnos, mejorar y decidir con mayor claridad.** Cada indicador y cada análisis de este informe es una invitación a avanzar de forma conjunta y a reforzar nuestras capacidades.

Desde MetaRed mantenemos el compromiso claro de **seguir construyendo un ecosistema universitario iberoamericano más fuerte, más seguro y mejor preparado**. La ciberseguridad no es un desafío que se supere en un año; es un camino y recorrerlo acompañados marca toda la diferencia.

Vamos en la dirección correcta.

Sigamos empujando.

Rafael Hernández

Vicepresidente de Fundación Universia

Presentación

La digitalización avanza a un ritmo vertiginoso y con ella crece también la exposición de las instituciones a nuevas amenazas. En este escenario, la ciberseguridad ya no es solo una cuestión tecnológica: es un eje estratégico para garantizar la confianza, la continuidad y la resiliencia de nuestras universidades.

El **Índice de Madurez en Ciberseguridad de IES iberoamericanas (IMC)** nació en 2024 con un propósito claro: ofrecer a las instituciones un marco de referencia que les permita conocer su situación, compararse con pares y orientar sus esfuerzos de mejora. Sin embargo, su verdadero valor se aprecia al repetir el ejercicio año tras año, porque solo así es posible medir la evolución, identificar tendencias y aprender colectivamente.

La edición 2025 marca un paso decisivo en este camino: **308 Instituciones de Educación Superior han participado, ampliando la base de 7 a 9 países con la incorporación de Brasil y Perú.** Este crecimiento refuerza la representatividad del informe y consolida al IMC como la principal herramienta de diagnóstico y seguimiento de la madurez en ciberseguridad universitaria en Iberoamérica.

Medir no es suficiente si no se convierte en aprendizaje. Por eso, el **IMC 2025** no solo presenta resultados, sino que **muestra cómo cada institución evoluciona frente a los desafíos de la seguridad digital,** cómo se fortalecen las capacidades compartidas y cómo se construye, paso a paso, un ecosistema universitario iberoamericano más seguro, conectado y resiliente.

MetaRed TIC México

Héctor Bonola

Universidad Veracruzana

Dirección de Servicios de Red e Infraestructura Tecnológica

MetaRed TIC México

Roger Arturo Sunción Campos

Universidad Peruana Cayetano Heredia

Director de TI

1.

Conclusiones

- Un ecosistema en plena evolución
- Los motores del cambio: Inversión y Talento como factores decisivos
- Radiografía de la madurez
- Conclusiones estratégicas

El Índice de Madurez en Ciberseguridad (IMC) 2025 marca un hito en la evaluación de la seguridad digital en el sector de la educación superior iberoamericano.

Esta segunda edición no solo ofrece una instantánea actualizada del estado de la ciberseguridad, sino que, por primera vez, permite un análisis evolutivo riguroso para medir el progreso y las tendencias en la región. El notable crecimiento en la participación, que alcanza **308 Instituciones de Educación Superior de 9 países,** consolida al IMC como la principal herramienta de diagnóstico y seguimiento estratégico a nivel regional. Este informe revela un hallazgo fundamental: el ecosistema universitario iberoamericano ha dado un salto cualitativo, avanzando de forma colectiva hacia un nuevo y más robusto nivel de madurez.

El modelo mantiene la coherencia con el estudio previo y se basa en la versión 2.0 del **Cybersecurity Framework** del *National Institute of Standards and Technology (NIST)* de los Estados Unidos. Asimismo, integra prácticas y controles de estándares internacionales como **ISO/IEC 27001:2022, ISO/IEC 27002:2022 y el Esquema Nacional de Seguridad (ENS) de España,** garantizando una cobertura completa y actualizada de los aspectos clave de la seguridad de la información.

Aumento en la participación:
308 IES
9 países.

Una novedad en 2025 es la incorporación de cuestiones relacionadas con el **uso de herramientas de inteligencia artificial (IA)** y sus implicaciones en la ciberseguridad. Este enfoque híbrido, que combina marcos internacionales consolidados con nuevas dimensiones tecnológicas, ofrece un modelo robusto, contextualizado y alineado con los desafíos actuales de la región.

En suma, el IMC 2025 continúa la senda iniciada en 2024, consolidando un marco de referencia sólido y efectivo para la evaluación y la mejora de la madurez en ciberseguridad en las IES de Iberoamérica.

El IMC se actualiza:
incorporación de cuestiones sobre el uso de herramientas de IA.

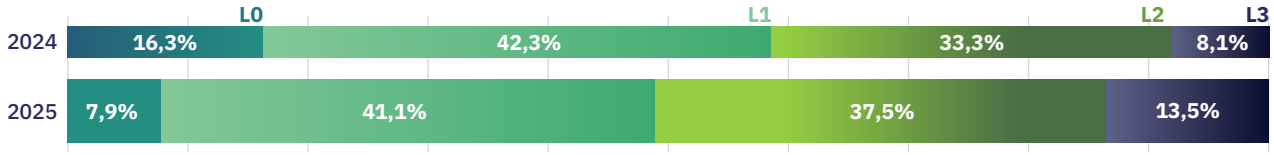
Un ecosistema en plena evolución

El IMC Iberoamericano global ha avanzado de 1,37 (Nivel Básico - L1) en 2024 a 1,51 (Nivel Intermedio - L2) en 2025. Este avance representa un hito estratégico. En términos prácticos, evidencia un cambio fundamental hacia un "uso más extendido de prácticas avanzadas, la definición y documentación de políticas y procedimientos, y la asignación de recursos adecuados para respaldar los procesos".

Esta evolución se manifiesta claramente en la distribución de las instituciones por niveles de madurez, donde se observa un desplazamiento significativo hacia los estadios más avanzados:

De básico a intermedio:
un salto cualitativo para la región.

Gráfico 1: Comparativa niveles de madurez. Evolución 2024-2025.



El análisis de esta transición revela dos tendencias clave: una **reducción drástica de las instituciones en el nivel inicial (L0), que cae 8,4 puntos porcentuales,** y un **crecimiento notable en los niveles intermedio y avanzado (L2 y L3), que en conjunto aumentan su representación en más de 9,6 puntos porcentuales.**

Este avance general se sustenta en factores determinantes como la asignación de presupuestos específicos y la creciente especialización de los equipos, que actúan como verdaderos motores del cambio.

Iberoamérica avanza hacia un nuevo nivel de madurez.

Los motores del cambio: Inversión y Talento como factores decisivos

Una lectura transversal del informe revela dos factores que explican de manera contundente las diferencias de madurez entre instituciones: la existencia de un presupuesto formal de ciberseguridad y la disponibilidad de equipos especializados.

INVERTIR ES PROGRESAR: EL PRESUPUESTO COMO PALANCA DE MADUREZ

Los datos muestran una correlación inequívoca entre inversión y madurez. **Las universidades que invierten un 5% o más de su presupuesto de TI en ciberseguridad alcanzan niveles de madurez significativamente superiores.**

Los patrones de tendencia encontrados son los siguientes:

- **Intervalo de inversión:** El tramo del **5-10% del presupuesto de TI** no solo logra el IMC más alto (1,79), sino que también experimenta el mayor salto de madurez (+0,23 puntos) respecto al año anterior. Este dato sugiere que el 5-10% representa el umbral de inversión más eficiente, donde los recursos son suficientes para habilitar un ecosistema de seguridad integral (personas, procesos y tecnología).
- **El riesgo de la inacción:** El dato más preocupante es que **una de cada tres instituciones (33,4%) aún carece de presupuesto.** Este grupo no solo no mejora, sino que retrocede en su madurez, pasando de un IMC de 1,34 a 1,13. Este retroceso es el principal motor que frena un avance regional aún más rápido y alimenta directamente el grupo de IES rezagadas en el Nivel Básico (L1), ampliando la brecha de madurez en lugar de cerrarla.
- **Tendencia a la formalización:** Se observa una evolución positiva hacia la institucionalización del gasto. Aumentan las **partidas específicas dentro de TI (+4,0 puntos)** y los **presupuestos diferenciados (+1,5 puntos),** mientras descienden las asignaciones generales no específicas.

El ajuste de la inversión y la formalización del presupuesto son condiciones indispensables para planificar, medir y sostener las capacidades de ciberseguridad. Este recurso financiero es el que permite habilitar el otro pilar fundamental: el capital humano.

EL FACTOR HUMANO: EQUIPOS ESPECIALIZADOS COMO ACELERADORES DEL CAMBIO

Al igual que IMC 2024, el análisis de los datos de 2025 refleja que la **dimensión de los equipos de ciberseguridad es el factor más determinante de la madurez.**

La disponibilidad de personal dedicado y especializado tiene un impacto directo y masivo en el IMC de una institución.

- **Liderazgo consolidado:** Las IES con equipos de **más de 5 personas** lideran con un IMC de 1,93, muy por encima de la media regional (1,51).
- **Alto riesgo:** En el extremo opuesto, aquellas **sin personal especializado** apenas alcanzan un IMC de 1,03, un nivel de madurez básico e insuficiente para afrontar el panorama de amenazas actual.
- **Punto de inflexión:** El salto cualitativo más significativo se produce al consolidar equipos de **3 a 5 personas,** que mejoran su IMC de 1,60 a 1,80 en un solo año, demostrando ser el umbral que acelera la institucionalización de las prácticas de seguridad.

La brecha entre las universidades con equipos grandes y las que carecen de ellos supera las nueve décimas de IMC, marcando una diferencia estructural. Esta evidencia subraya que invertir en talento no es un gasto, sino el principal acelerador del cambio.

La dimensión de los equipos de ciberseguridad es el factor más determinante de la madurez.

Radiografía de la madurez: fortalezas, debilidades y el gran reto pendiente

Si bien la región muestra una mejora generalizada, el análisis detallado por dominios revela un patrón de desarrollo claro y consistente. Las instituciones iberoamericanas han logrado una fuerte consolidación de sus capacidades de prevención y vigilancia, pero enfrentan una debilidad persistente en su capacidad de respuesta ante incidentes. Este patrón de desarrollo asimétrico revela una estrategia regional centrada en la prevención, pero con una peligrosa falta de preparación para el "día después". Aunque se están construyendo muros más altos, no existen planes de respuesta y recuperación eficaces, lo que podría dejar a las instituciones en un estado de falsa seguridad.

FORTALEZAS CONSOLIDADAS

El progreso regional se concentra en tres dominios clave que forman el núcleo de las capacidades preventivas:

- El dominio **Proteger (PR)** se mantiene como el más sólido en términos absolutos, alcanzando un IMC de 1,68. Esto confirma que la implementación de controles técnicos sigue siendo la principal prioridad para las IES.
- Los dominios **Identificar (ID) y Detectar (DE),** con 1,51 y 1,64 respectivamente, son los que experimentan el mayor crecimiento, con aumentos de +0,19 y +0,17 puntos respectivamente.

Esta evolución indica que las IES iberoamericanas están mejorando de forma decidida su capacidad para conocer sus activos, gestionar riesgos e implementar controles de monitoreo continuo, sentando las bases de una defensa más proactiva.

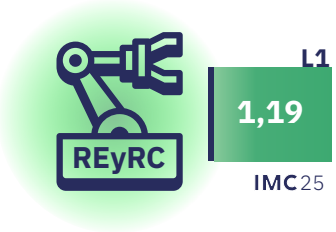
Avances en identificación, protección y detención

PRINCIPALES DEBILIDADES

El informe identifica de manera inequívoca al dominio **Responder y Recuperar (REyRC)** como la principal debilidad estructural de la región. Con un IMC de solo **1,19** y un avance mínimo de +0,09 puntos, este dominio permanece anclado en un nivel básico.

Las implicaciones de esta debilidad son estratégicas: sin una capacidad de respuesta y recuperación eficaz, la resiliencia global de las instituciones permanece limitada, sin importar cuánto mejoren en prevención y detección. Esta sigue siendo la "principal tarea pendiente para las IES iberoamericanas".

La respuesta y la recuperación siguen siendo la tarea pendiente



RETOS

HETEROGENEIDAD

El promedio iberoamericano de 1,51 oculta un mosaico de realidades muy diversas. El análisis de las diferencias por país y por tipo de institución es fundamental para comprender las brechas existentes y diseñar estrategias de mejora efectivas y contextualizadas, reconociendo que no existe un único camino hacia la madurez.

Múltiples realidades en la ciberseguridad universitaria.

UN AVANCE A MÚLTIPLES VELOCIDADES

El progreso en ciberseguridad no es uniforme en toda la región, con países que lideran la adopción de prácticas avanzadas y otros que avanzan a un ritmo más moderado.

Líderes por encima de la media: España (1,88), Colombia (1,75), Perú (1,59) y Brasil (1,55) se consolidan como los países con mayor nivel de madurez, superando el promedio regional (1,51).

El mayor crecimiento: Ecuador destaca como el país con el mayor incremento anual, mejorando su IMC en **+0,37** puntos y reduciendo significativamente su brecha con la media.

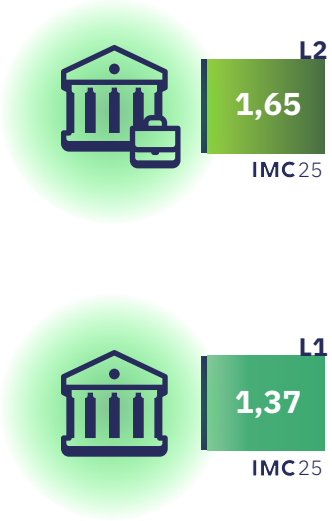
Progreso Sostenido: Argentina y España también muestran un avance notable, con un incremento de +0,15 puntos cada uno.

Ritmo Moderado: México, Chile y Portugal presentan un crecimiento más lento en el último año.

BRECHA PÚBLICO-PRIVADA

La tipología de la institución es otro factor diferenciador clave. Los datos de 2025 confirman y amplían una tendencia ya observada:

- Las **instituciones privadas (IMC 1,65)** muestran, en promedio, un nivel de madurez superior a las **instituciones públicas (IMC 1,37).**
- La brecha entre ambos tipos de institución aumenta en el último año. Las privadas mejoraron a un ritmo casi doble (+0,15) que las públicas (+0,09), lo que sugiere mayor agilidad en la asignación de recursos y la toma de decisiones.
- Esta tendencia no es universal. Existen excepciones notables: **en Colombia y Portugal, las universidades públicas superan a las privadas, mientras que en España ambos sectores han alcanzado la paridad,** demostrando un desarrollo equilibrado.



EL ROL DE LA INTELIGENCIA ARTIFICIAL

Por primera vez, el IMC 2025 analiza el uso de la IA como capacidad emergente en la ciberseguridad universitaria. Los resultados revelan un despliegue incipiente y desigual, con patrones de adopción claros que apuntan su potencial como herramienta de defensa.

El uso de la IA en ciberseguridad se caracteriza actualmente por los siguientes rasgos:

- **Concentración Operativa:** El uso de IA se enfoca en los dominios más técnicos. El 38,3% de las IES la aplica en tareas de **Proteger** y el 32,5% en **Detectar,** sobre todo para automatizar vigilancia y analizar amenazas.
- **Ausencia Estratégica:** Presencia mínima en **Gobernar (10,1%) y Responder y Recuperar (11,0%),** lo que indica que aún no se ha integrado en la toma de decisiones estratégicas.

Despliegue incipiente y desigual

- **Adopción Heterogénea:** El despliegue es desigual entre países. **Brasil, Chile y Ecuador** están a la cabeza de la adopción. Otros países muestran un uso más prudente y contenido.

La IA, tal como se usa hoy, refuerza la capacidad defensiva, pero no resuelve la debilidad estructural de la región: identificar antes no implica responder mejor. Si no se acompaña de estructuras de respuesta maduras, la brecha entre alerta y actuación puede incluso ampliarse.

Conclusiones estratégicas

IMC 2025 confirma que el ecosistema universitario iberoamericano ha dado un paso firme hacia la madurez, reflejando un esfuerzo colectivo y un compromiso creciente con la ciberseguridad. Sin embargo, este progreso generalizado saca a la luz tres imperativos estratégicos que serán determinantes para alcanzar un estado de resiliencia sostenible.

Institucionalizar la inversión: Es imperativo superar la dependencia de asignaciones generales y formalizar presupuestos específicos para ciberseguridad. La evidencia es clara: sin inversión planificada, no hay avance sostenido.

Invertir en talento: La dimensión y especialización de los equipos de ciberseguridad es el factor crítico de éxito. Las instituciones deben priorizar la atracción y retención de talento como el principal acelerador de la madurez.

Superar la asignatura pendiente: La región debe centrar sus esfuerzos en **fortalecer las capacidades de respuesta y recuperación.** Una defensa robusta es incompleta si no se cuenta con planes eficaces para gestionar y recuperarse de los incidentes.

Hacia una ciberseguridad resiliente e integrada

En síntesis, IMC funciona como un **predictor sólido del comportamiento real** frente a ciberamenazas. Invertir en madurez —tanto en estructura organizativa como en procesos y capacidades técnicas— se refleja directamente en una reducción del riesgo y del número de incidentes que afectan al funcionamiento de las instituciones de educación superior.

El futuro de la universidad digitalmente robusta y resiliente no pasa únicamente por la adquisición de tecnología, sino de la decisión de sus líderes de institucionalizar la inversión, profesionalizar el talento y dominar la capacidad de respuesta.

2.

IMC México

MÉX

L0 L1 L2 L3

IMC24 1,27 L1

IMC25 1,33 L1

IMC MÉXICO
1,33

2024-2025 EVOLUCIÓN
+0,06

IMC IBE DIFERENCIA
-0,18

TIPO DE IES
*evolución sobre IMC IES MÉX.

PÚBLICAS 1,57 (+0,16)

PRIVADAS 1,28 (+0,04)

DOMINIOS
*evolución sobre IMC dominios IBE

PROTEGER 1,49 (-0,19)

IDENTIFICAR 1,40 (-0,11)

GOBERNAR 1,36 (-0,19)

DETECTAR 1,35 (-0,29)

RESPONDER 1,10 (-0,09)

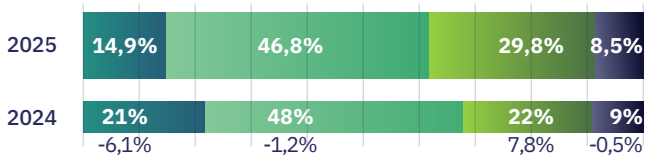
TOP 3
PROTEGER
IDENTIFICAR
GOBERNAR

Ninguno de los dominios supera el IMC25 (1,51).

Proteger (1,49) e Identificar (1,40) obtienen la mejor puntuación.

Responder y Recuperar (1,10), Detectar (1,35) y Gobernar (1,36) tienen los valores más bajos y alejados de las medias, luego de Argentina.

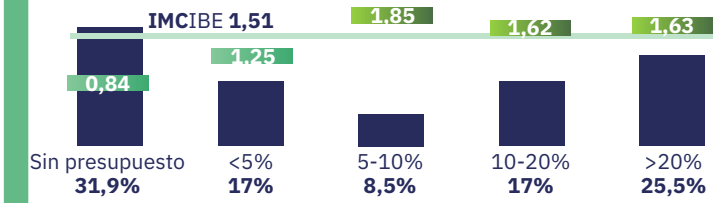
DISTRIBUCIÓN SEGÚN IMC



Se reduce un 6,1% las IES en el nivel más bajo (Inicial, L0).

6 de cada 10 IES mexicanas se encuentran por debajo del nivel intermedio (L2).

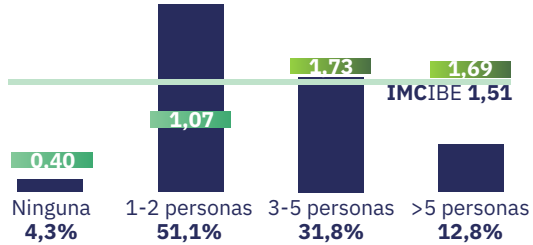
PRESUPUESTO



Una tercera parte de las IES **no cuentan con presupuesto específico.**

El rango de asignación presupuestaria 5-10% marca la diferencia entre las IES que superan la media iberoamericana y las que no.

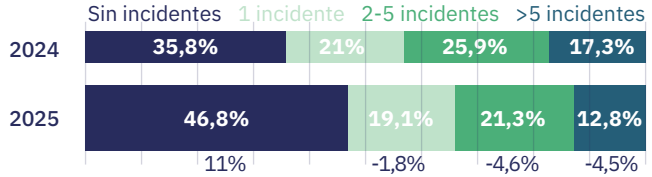
EQUIPOS DE CIBERSEGURIDAD



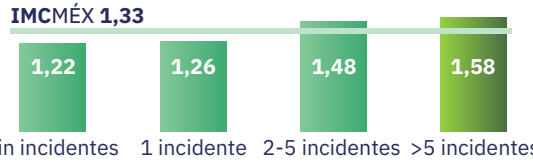
8 de cada 10 equipos están compuestos por menos de 5 personas. Se observa una relación directa entre el tamaño de los equipos de seguridad y el nivel de madurez, excepto en los equipos de más de 5 personas, en los que el IMC parece descender, aunque no significativamente.

CIBERINCIDENTES

DISTRIBUCIÓN DE LOS INCIDENTES



EVOLUCIÓN DEL IMC SEGÚN Nº DE INCIDENTES



Más de la mitad de las instituciones mexicanas han sufrido al menos un incidente considerado crítico en el último año.

3.

Resumen Ejecutivo

RESUMEN EJECUTIVO MÉXICO

México alcanza un IMC de 1,33 en 2025 y mantiene un avance progresivo, aunque por debajo de la media regional.

México obtiene en 2025 un I**MC de 1,33,** lo que lo sitúa dentro del nivel básico (L1), aunque próximo al umbral del nivel intermedio. Este resultado muestra un crecimiento respecto a 2024, cuando el país registró un IMC de 1,27. El avance, aunque moderado (+0,06), confirma una tendencia sostenida de mejora.

Aun así, México se mantiene por debajo del promedio iberoamericano de 2025 (1,51). Esto indica que, pese a su progresión, el país continúa enfrentando desafíos estructurales para avanzar hacia un nivel intermedio consolidado. La brecha con la media regional se ha mantenido relativamente estable, lo que sugiere que, aunque México mejora, otros países avanzan a ritmos similares o superiores.

El comportamiento del país refleja un sistema de educación superior con capacidades técnicas relevantes, pero con debilidades persistentes en gobernanza, documentación, procedimientos y capacidad de respuesta, dimensiones que continúan condicionando su avance hacia niveles superiores de madurez.

BRECHA ENTRE INSTITUCIONES PÚBLICAS Y PRIVADAS

El análisis por tipo de institución revela diferencias claras de madurez. En 2025, las IES privadas alcanzan un IMC promedio de **1,57,** mientras que las públicas se sitúan en **1,28,** generando una brecha significativa. Esta diferencia es una de las más amplias entre países de la región, y evidencia desigualdades en la capacidad de organización, planificación y aplicación de políticas internas.

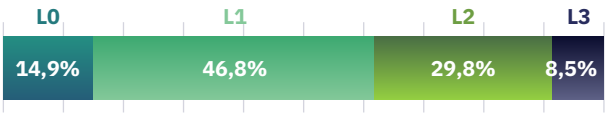
Las IES privadas muestran mejores resultados en prácticamente todos los subdominios de Gobernar: estrategia, normativa, procedimientos y asignación de presupuesto. Por el contrario, las IES públicas presentan déficits más marcados en presupuesto, documentación técnica y definición de roles, tres elementos que afectan de manera directa su capacidad para sostener un programa de ciberseguridad estable.

Sin embargo, las IES públicas destacan en algunos subdominios técnicos, como infraestructura y comunicaciones, con resultados competitivos. Esto refleja que, aunque existen brechas organizativas, varias universidades públicas cuentan con activos tecnológicos relevantes, aún sin una estructura de gestión que permita maximizar su impacto.

Mayoría de IES en nivel básico, pero ligera mejoría hacia nivel intermedio.

DISTRIBUCIÓN DE NIVELES DE MADUREZ

La distribución nacional de las IES mexicanas en los niveles del modelo muestra un panorama de transición:



En comparación con 2024, cuando el país tenía 21% en L0 y 21% en L2, el avance es claro: se reduce el grupo de instituciones incipientes y aumenta el nivel intermedio. La proporción de universidades en L3 se mantiene estable en torno al 8–10%, lo que indica la presencia de un grupo reducido de instituciones con capacidades consolidadas.

No obstante, más del 60% del sistema sigue concentrado en L0–L1, lo que evidencia que México enfrenta un reto estructural: elevar el piso mínimo de madurez, de manera que el desarrollo no dependa de un conjunto acotado de instituciones con mejores capacidades organizativas y presupuestarias.

DESEMPEÑO POR DOMINIOS

Fortalezas en Infraestructura y Comunicaciones,

debilidades en Gobernanza y Respuesta.

El perfil de México en los dominios del IMC muestra un país con importantes fortalezas técnicas, pero con brechas claras en aspectos de planificación, procedimientos y gestión de incidentes. En 2025, los valores por dominio son los siguientes: **Gobernar (GB): 1,36, Identificar (ID): 1,40, Proteger (PR): 1,49, Detectar (DE): 1,35, Responder (RE): 1,10.**

Los subdominios técnicos destacan especialmente. **Infraestructura (2,35), Comunicaciones (1,83), Externos (1,62) y Servicios (1,49)** alcanzan niveles comparables a los de países más avanzados, evidenciando inversiones sostenidas en capacidades defensivas. Asimismo, **Información (1,59) y Continuidad (1,19)** muestran progresos respecto a 2024.

Sin embargo, México enfrenta dificultades en áreas clave de gobernanza y gestión operativa. El subdominio **Procedimientos (1,17)** continúa siendo bajo, lo que revela carencias en formalización, documentación y estandarización. **Responsabilidad (1,09) y Presupuesto (1,15)** también presentan valores limitados, indicando que muchas instituciones aún operan sin roles claros ni recursos dedicados a la ciberseguridad.

El dominio **Responder y Recuperar** constituye el desafío más crítico, con debilidades en **Gestión de Incidentes (1,04), Mitigación (1,13) y Recuperación (1,13).** Aunque el país ha mejorado levemente en esta área, el nivel de preparación para enfrentar incidentes sigue siendo insuficiente en gran parte del sistema.

IMPACTO DEL TAMAÑO DEL EQUIPO DE CIBERSEGURIDAD

El tamaño del equipo especializado vuelve a ser uno de los factores que más explica la diferencia de madurez entre instituciones. Los datos de México son especialmente ilustrativos:

- IES con **ningún profesional dedicado: IMC 0,40**, uno de los niveles más bajos de toda la región.
- IES con **1–2 personas: IMC 1,27,** mostrando limitaciones claras.
- IES con **3–5 personas: IMC 1,73,** avanzando hacia el nivel intermedio.
- IES con **más de 5 personas: IMC 1,69,** perfil ya cercano al nivel intermedio-alto.

El salto de madurez entre los equipos de 1–2 personas y los de 3–5 es especialmente significativo. Esto confirma que la estructura mínima necesaria para operar capacidades de seguridad modernas en México se sitúa en

equipos de al menos tres profesionales especializados. Las instituciones sin personal dedicado presentan carencias sistémicas en todos los dominios, especialmente en gobernanza y respuesta.

INFLUENCIA DEL PRESUPUESTO EN LA MADUREZ

El análisis del presupuesto asignado a ciberseguridad muestra una tendencia clara: las IES que destinan un porcentaje mayor de su presupuesto de TI a seguridad presentan niveles de madurez sensiblemente superiores. En México:

- IES **sin presupuesto asignado: IMC 0,84**
- IES con **menos del 5%: IMC 1,25**
- IES con **5–10%: IMC 1,85**
- IES con **10–20%: IMC 1,62**
- IES con **más del 20%: IMC 1,63**

Estos datos ponen de manifiesto que la asignación de presupuestos en el rango del 5-10 % del presupuesto del área de TI consolida niveles de madurez intermedios (L2), con valores promedio de 1,85. Esto sitúa a estas IES por encima de la media iberoamericana.

Estos resultados consolidan la tendencia detectada en 2024, donde ya se observaba la misma situación: el rango del 5-10 % marcaba un salto significativo en los niveles de madurez, situando el promedio en 1,58 puntos, frente al IMC mexicano de 2024, que se encontraba en 1,27.

Aunque este patrón no debe interpretarse de manera causal estricta —es posible que las instituciones más maduras asignen más presupuesto precisamente porque ya poseen capacidades más desarrolladas—, sí es evidente que la disponibilidad de recursos facilita la adopción de controles, la contratación de personal especializado y la institucionalización de procesos.

Las instituciones con presupuestos bajos reflejan también **valores muy reducidos en Gobernanza, Accesos, Mitigación y Procedimientos,** lo que muestra que la sostenibilidad operativa está directamente condicionada por la inversión.

INCIDENTES DE SEGURIDAD: EVOLUCIÓN Y RELACIÓN CON LA MADUREZ

Un factor crítico que evidencia diferencias profundas en resiliencia

México presenta uno de los perfiles de incidentes más altos de la región. En 2025, el **35,8%** de las IES no reportó incidentes, pero el resto sí lo hizo en distintos niveles:

- **1 incidente: 21%**
- **2 a 5 incidentes: 25,9%**
- **Más de 5 incidentes: 17,3%**

Además, el número promedio de incidentes entre las instituciones que reportaron al menos uno sigue siendo elevado, pasando **de 7,31 en 2024 a 6,57 en 2025**. Aunque hay una ligera mejora, los valores siguen siendo altos, lo que sugiere una exposición significativa y una capacidad limitada para prevenir o contener incidentes críticos.

El análisis del IMC según incidentes muestra diferencias muy marcadas. Las instituciones sin incidentes presentan un IMC de **1,22,** similar al nivel básico; sin embargo, **las instituciones con más de 5 incidentes alcanzan un IMC de 1,58,** lo que podría interpretarse de forma superficial como un “mejor desempeño”. No obstante, este

resultado exige una lectura cuidadosa: es probable que las instituciones más complejas y con mayor actividad reporten más incidentes porque **tienen mayor capacidad de detección,** no porque sufran más fallos estructurales. Aun así, los datos muestran patrones preocupantes:

- Las IES con más incidentes presentan **valores más bajos en Responsabilidad, Presupuesto, Continuidad y Mitigación.**
- Los subdominios más afectados entre las instituciones con incidentes recurrentes son **Procedimientos, Análisis de riesgos, Gestión de incidentes y Recuperación.**
- Las instituciones con pocos recursos y sin equipos dedicados muestran mayor impacto operativo frente a incidentes.

En conjunto, los incidentes revelan una **resiliencia desigual** dentro del sistema mexicano: mientras algunas instituciones cuentan con mecanismos de detección y respuesta relativamente más maduros, un número significativo de universidades permanece vulnerable y carece de procesos sólidos para prevenir, contener y recuperarse ante amenazas.

USO DE LA INTELIGENCIA ARTIFICIAL EN CIBERSEGURIDAD

El uso de IA en México muestra una **adopción mayor** que en muchos países de la región, especialmente en los dominios **Proteger (34%), Detectar (29,8%) e Identificar (23,4%).** Sin embargo, sigue siendo **minoritario en Gobernar (8,5%), Responder (14,9%) y Formación (6,4%).**

Las instituciones que declaran utilizar IA presentan, en promedio, **niveles de madurez significativamente más altos (IMC 2,23)** frente a las que no la usan (IMC 1,25). Esto ocurre de manera consistente en prácticamente todos los dominios, incluidos los más técnicos como Proteger e Identificar, y también en los organizativos como Gobernar.

No obstante, esta diferencia debe interpretarse con prudencia. Es probable que las instituciones que han empezado a experimentar con IA sean también aquellas con **mayor disponibilidad de recursos, equipos más amplios y procesos más consolidados**, lo que puede explicar buena parte de la brecha observada. Con un porcentaje reducido de IES que han adoptado IA en 2025, cualquier variación individual puede influir notablemente en los promedios.

Aun así, los datos sugieren que la IA está siendo utilizada sobre todo como **complemento a capacidades ya existentes,** en áreas donde México presenta fortalezas técnicas —infraestructura, comunicaciones, vigilancia, análisis de anomalías—. La adopción aún no es homogénea ni suficiente para generar efectos estructurales en el conjunto del sistema, pero sí anticipa un posible cambio de tendencia a medida que las instituciones más avanzadas consoliden su experiencia y el resto del ecosistema observe su evolución.

MÉXICO

IMC 2025

Índice de Madurez en Ciberseguridad de las IES Iberoamericanas

metared by universia

Secretaría General Iberoamericana
Secretaria-Geral Ibero-Americana