# ECUADOR

# 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

# ECUADOR

# 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 5

Presentación 6

1. Conclusiones 7

2. IMC Ecuador 16

3. Resumen Ejecutivo 18

- 3.1 Brecha entre universidades públicas y privadas 19
- 3.2 Distribución de niveles de madurez 19
- 3.3 Desempeño por dominios 19
- 3.4 Impacto del tamaño del equipo de ciberseguridad 20
- 3.5 Influencia del presupuesto en ciberseguridad 20
- 3.6 Incidentes de seguridad: evolución y relación con la madurez 20
- 3.7 Uso de la Inteligencia Artificial en ciberseguridad 21

# 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 Ecuador

**Carlos Gabriel Córdova Erreis**

Universidad Técnica Particular de Loja

Gerente TI

MetaRed TIC Ecuador

**Julia Alexandra Pineda Arévalo**

Universidad Técnica Particular de Loja

Coordinadora de Seguridad y Riesgos

# 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.

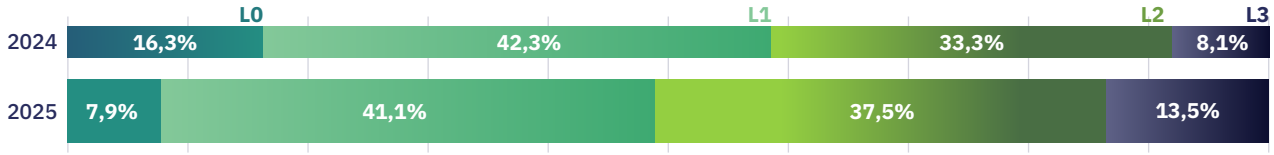
# Un ecosistema en plena evolución

**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

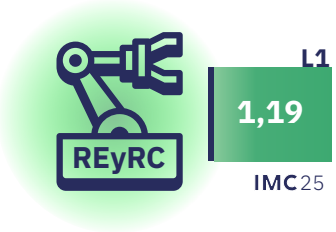


## PRINCIPALES DEBILIDADES

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.

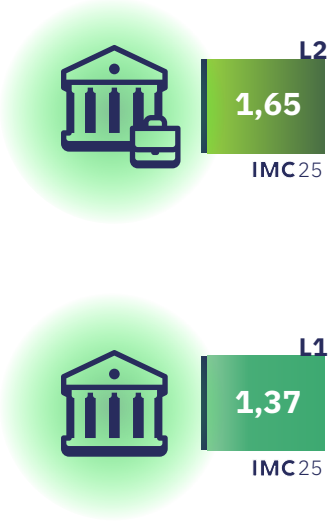
**Progreso Sostenido: Argentina y España** también muestran un avance notable, con un incremento de +0,15 puntos cada uno.

**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 Ecuador

# ECU

L0 L1 L2 L3

IMC24 0,99 L1
1,36 L1
IMC25

## IMC ECUADOR
1,36

## 2024-2025 EVOLUCIÓN
+0,37

## IMC IBE DIFERENCIA
-0,15

## TIPO DE IES
*evolución sobre IMC IES ECU.

**PÚBLICAS** 1,32 (+0,51)

**PRIVADAS** 1,43 (+0,13)

## DOMINIOS
*evolución sobre IMC dominios IBE

**DETECTAR** 1,60 (-0,04)

**PROTEGER** 1,56 (-0,12)

**GOBERNAR** 1,38 (-0,17)

**IDENTIFICAR** 1,35 (-0,16)

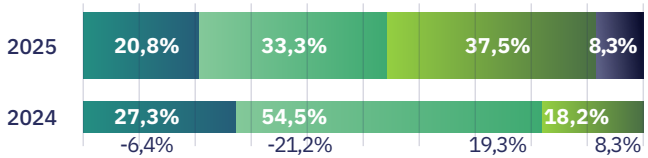
**RESPONDER** 0,93 (-0,26)

**TOP 3**
DETECTAR
PROTEGER
GOBERNAR

**Detectar y Proteger obtienen la mejor puntuación y superan IMC25 (1,51).**

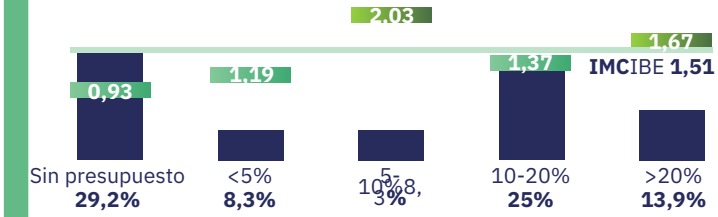
Gobernar e Identificar tienen valores más bajos y alejados de la media, pero Responder y Recuperar es el que más se aleja (0,58 puntos).

## DISTRIBUCIÓN SEGÚN IMC




Bajada importante del número de IES en nivel inicial (L0) y básico (L1) y fuerte incremento del número de IES en nivel intermedio (+19,3%) y avanzado (+8,3)

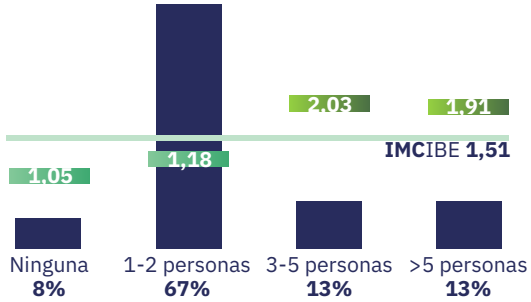
## PRESUPUESTO




**Casi el 30%** de las IES **no cuentan con presupuesto específico.**

El nivel de madurez de las IES con presupuesto del 5-10% duplica a las que no tienen importe asignado.

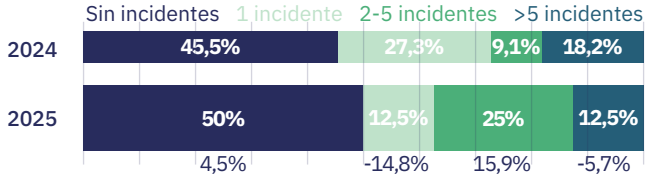
## EQUIPOS DE CIBERSEGURIDAD



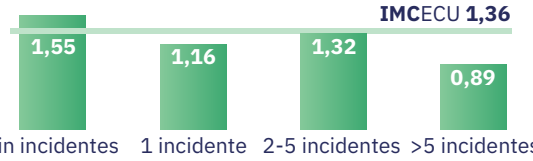

La gran mayoría de IES ecuatorianas (66%) cuentan con equipos de ciberseguridad pequeños, compuestos por 1-2 personas.

## CIBERINCIDENTES

### DISTRIBUCIÓN DE LOS INCIDENTES




### EVOLUCIÓN DEL IMC SEGÚN Nº DE INCIDENTES




5 de cada 10 IES ecuatorianas han sufrido algún ciberincidente en el último año.

# 3.

# Resumen Ejecutivo


3.1 Brecha entre universidades públicas y privadas

3.2 Distribución de niveles de madurez

3.3 Desempeño por dominios

3.4 Impacto del tamaño del equipo de ciberseguridad

3.5 Influencia del presupuesto en ciberseguridad

3.6 Incidentes de seguridad: evolución y relación con la madurez

3.7 Uso de la Inteligencia Artificial en ciberseguridad

## RESUMEN EJECUTIVO ECUADOR

# Ecuador avanza con fuerza hacia el nivel intermedio, aunque por debajo de la media regional.

Ecuador ha obtenido un **IMC 2025 de 1,36,** ubicándose en el nivel básico (L1), pero notablemente más cercano al umbral intermedio que en 2024, cuando registró un IMC de 0,99. El incremento de **+0,37** puntos es uno de los avances más altos de la región y supera ampliamente el crecimiento medio de Iberoamérica (+0,14). Esto sugiere que las instituciones de educación superior ecuatorianas han desplegado esfuerzos consistentes para fortalecer sus capacidades de ciberseguridad durante el último año.

Pese a esta mejora, Ecuador permanece todavía 0,15 puntos por debajo del promedio regional registrado en 2025 (1,51). No obstante, el ritmo de crecimiento observado indica que el país podría cerrar parte de esta brecha en los próximos años si mantiene la tendencia actual, especialmente en dominios técnicos y de identificación, donde los avances han sido más marcados.

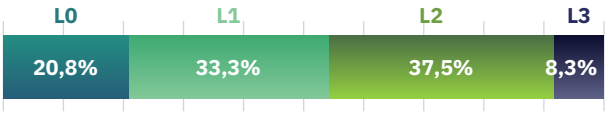
## BRECHA ENTRE UNIVERSIDADES PÚBLICAS Y PRIVADAS

La comparación entre instituciones públicas y privadas muestra una diferencia moderada, aunque persistente, en el nivel de madurez. En 2025, las IES privadas alcanzan un IMC medio de **1,43,** mientras que las públicas se sitúan en **1,32.** Aunque la brecha es menor que la observada en países como Argentina o Chile, sí refleja que las instituciones privadas disponen de estructuras más formalizadas en ciertos ámbitos, especialmente en políticas internas, identificación de activos y gestión técnica de la infraestructura.

Las universidades públicas, por su parte, presentan rezagos visibles en subdominios como **presupuesto, responsabilidad y respuesta a incidentes,** lo que podría explicar parte de la diferencia. Aun así, ambos sectores muestran una mejora respecto al año anterior, lo que sugiere un avance transversal del sistema, aunque no completamente homogéneo.

## DISTRIBUCIÓN DE NIVELES DE MADUREZ

La distribución de las IES por niveles de madurez muestra un desplazamiento positivo respecto a 2024. En 2025, la situación del país es la siguiente:




En 2024, Ecuador contaba todavía con 27,3% de instituciones en L0 y ninguna en nivel avanzado. El hecho de que en 2025 exista ya un grupo —aunque pequeño— en L3 indica la aparición de instituciones con capacidades consolidadas, especialmente en dominios técnicos. También destaca el crecimiento del nivel intermedio (L2), que ahora abarca más de un tercio del sistema.

Aun así, existe una proporción significativa (≈54%) de IES en niveles básicos o incipientes, lo que muestra que el desarrollo del ecosistema aún es desigual y necesita elevar el piso mínimo de madurez.

## DESEMPEÑO POR DOMINIOS

El perfil de Ecuador evidencia avances importantes en capacidades técnicas, aunque persisten debilidades en aspectos organizativos y, especialmente, en la respuesta a incidentes. Los valores nacionales de 2025 son Gobernar (GB) 1,38, Identificar (ID) 1,35, Detectar (DE): 1,60, Proteger (PR) 1,56, Responder y Recuperar (REyRC) 0,93.

Las fortalezas del país se concentran en los dominios Proteger y Detectar, que se sitúan cerca del nivel intermedio. Subdominios como **Infraestructura (2,55), Comunicaciones (1,77) y**

**Servicios (1,65)** alcanzan niveles elevados y reflejan una clara priorización de medidas técnicas de seguridad. Asimismo, **Identificar** muestra avances notables, especialmente en **Inventario de Activos (1,46) y Análisis de Impacto (1,42),** que se encuentran cerca de superar el nivel básico.

En contraste, **Responder y Recuperar** continúa siendo el dominio más rezagado, con valores bajos en **Mitigación (0,75) y Recuperación (0,88).** Estas cifras ponen de manifiesto la falta de procedimientos sólidos para enfrentar incidentes, un patrón que se repite también en **Continuidad (0,96) y en Presupuesto (1,13)** dentro del dominio Gobernar. El perfil resultante es similar al de otros países que están en transición hacia niveles intermedios: fuertes capacidades técnicas, pero carencias claras en arquitectura institucional y gestión de incidentes.

## IMPACTO DEL TAMAÑO DEL EQUIPO DE CIBERSEGURIDAD

El tamaño del equipo de ciberseguridad vuelve a ser determinante. Las IES con **3–5 personas** dedicadas alcanzan un IMC cercano a **2,03,** mientras que aquellas con **1–2 personas** apenas llegan a **1,18.** Las pocas universidades con **más de 5 personas** mantienen niveles comparables (≈1,91), lo que confirma que la presencia de equipos especializados permite sostener procesos continuos de gestión, monitoreo y mejora.

Por el contrario, las IES que no cuentan con personal específico siguen situándose en niveles básicos (≈1,05). Este patrón sugiere que la disponibilidad de talento humano especializado es uno de los principales condicionantes para que Ecuador pueda acelerar su transición hacia niveles intermedios consolidados.

## INFLUENCIA DEL PRESUPUESTO EN CIBERSEGURIDAD

El presupuesto específico destinado a ciberseguridad sigue siendo un punto débil. Aunque el país muestra mejoras respecto a 2024, el subdominio **Presupuesto (1,13)** continúa en los valores más bajos del modelo. Las IES que asignan recursos más altos tienen mejores resultados en dominios como **Gobernar, Proteger y Detectar,** mientras que aquellas con presupuesto reducido enfrentan dificultades para sostener prácticas avanzadas y fortalecer sus capacidades organizativas.

La relación entre inversión y madurez aparece de forma recurrente en los datos, aunque no puede interpretarse de manera estrictamente causal: es probable que las IES más maduras sean también las que destinan más presupuesto, no necesariamente al revés. Aun así, el patrón muestra que la disponibilidad de recursos continúa condicionando el ritmo de avance de las IES ecuatorianas. En concreto, se observa un gran incremento de la madurez , de 0,93 para aquellas IES sin presupuesto asignado, a valores de 2,03 en aquellas IES que afirman contar con partidas entre 5-10% del presupuesto del área IT.

## INCIDENTES DE SEGURIDAD: EVOLUCIÓN Y RELACIÓN CON LA MADUREZ

El análisis de los incidentes reportados por las IES ecuatorianas en 2025 muestra un patrón similar al observado en otros países de la región: **las instituciones con menor nivel de madurez tienden a reportar más incidentes o experimentar impactos más significativos,** especialmente en ámbitos relacionados con disponibilidad, continuidad operativa y afectación de servicios esenciales. Aunque los datos no permiten establecer una relación causal estricta, sí revelan que la capacidad de anticipación, contención y recuperación es considerablemente menor en aquellas instituciones que aún se sitúan en niveles básicos del modelo.

Las IES con valores más bajos en los dominios **Gobernar, Responder y Recuperar y algunos subdominios clave —como Mitigación, Recuperación, Continuidad y Responsabilidad—** muestran **mayores dificultades** para gestionar incidentes cuando estos ocurren. En particular, la

debilidad del subdominio **Mitigación (0,75)** indica que muchas IES carecen de procedimientos claros para contener y reducir el impacto de un incidente. Esto se refleja también en **Recuperación (0,88),** donde la capacidad de restaurar servicios tras una interrupción es limitada y depende en gran medida de esfuerzos manuales o acciones reactivas.

Asimismo, los incidentes reportados evidencian carencias en la documentación, la coordinación interna y la comunicación durante situaciones de crisis. El bajo desempeño del subdominio **Responsabilidad (1,17)** sugiere que, en varias instituciones, todavía no existe un rol claramente definido para liderar incidentes ni protocolos formales que faciliten la toma de decisiones. Esta falta de claridad organizativa aumenta el tiempo de respuesta y, en algunos casos, prolonga el impacto operativo de los incidentes.

Otro aspecto relevante es la influencia del tamaño del equipo y la disponibilidad de recursos. Las IES con personal específico en ciberseguridad o con más presupuesto tienden a manejar los incidentes con más eficacia, mostrando una recuperación más rápida y menor afectación a servicios críticos. En cambio, las IES sin equipos dedicados —o muy pequeños— suelen presentar demoras claves en identificación de la causa raíz, contención y restauración de la normalidad operativa.

En conjunto, los incidentes de seguridad en las IES ecuatorianas revelan una **madurez operativa aún incipiente en la gestión de crisis.** Aunque se ha avanzado en dominios técnicos como infraestructura y comunicaciones, la capacidad para gestionar incidentes de forma integral sigue siendo un desafío pendiente. Fortalecer la gobernanza, definir roles claros, invertir en formación y consolidar procedimientos formales será fundamental para reducir la exposición y mejorar la resiliencia institucional frente a futuros incidentes.

## USO DE LA INTELIGENCIA ARTIFICIAL EN CIBERSEGURIDAD

El uso de Inteligencia Artificial (IA) en ciberseguridad en Ecuador es todavía muy moderado. Los datos muestran que solo **una baja proporción de IES declara utilizar IA** en alguno de los dominios del modelo, con porcentajes que se mantienen por debajo del 33% en todas las áreas, con la excepción de **Proteger,** que registra un 41,7% de uso. Esto sugiere que la IA se encuentra aún en fase inicial dentro del ecosistema universitario ecuatoriano.

### Adopción limitada y resultados aún difíciles de interpretar en las IES ecuatorianas.

Al comparar los niveles de madurez entre IES que usan IA y las que no, se observan diferencias ligeras en algunos dominios, pero no existe un patrón uniforme. En ciertos casos, las que afirman utilizar IA muestran valores algo superiores, especialmente en aspectos técnicos como **Identificación, Detección o Protección.** Sin embargo, en **Gobernanza** la diferencia es mínima, lo que invita a una lectura prudente de los resultados.

Es probable que las IES que están iniciándose en el uso de IA sean también las que ya contaban con mayor capacidad técnica, equipos más desarrollados o procesos más maduros, factores que explicarían parte de las diferencias de madurez observadas. Con un número limitado de IES declarando uso de IA, cualquier variación individual influye de manera significativa en los promedios.

En conjunto, el caso ecuatoriano refleja un interés inicial por explorar herramientas de IA, pero aún **no existen evidencias suficientes para afirmar que su uso esté generando mejoras directas y generalizadas en el IMC.** La IA podría convertirse en un elemento diferenciador en los próximos años, especialmente en ámbitos como la detección de anomalías y la automatización de análisis, pero su impacto real dependerá de la consolidación previa de capacidades organizativas y técnicas en las instituciones.

# ECUADOR

# IMC 2025

Índice de Madurez en Ciberseguridad de las IES Iberoamericanas

metared by universia

Secretaría General Iberoamericana
Secretaria-Geral Ibero-Americana