COLOMBIA

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

COLOMBIA

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 Colombia
Maritza Giraldo Agudelo
Universidad Pontificia Bolivariana
Directora de Infraestructura Tecnológica Multicampus

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.

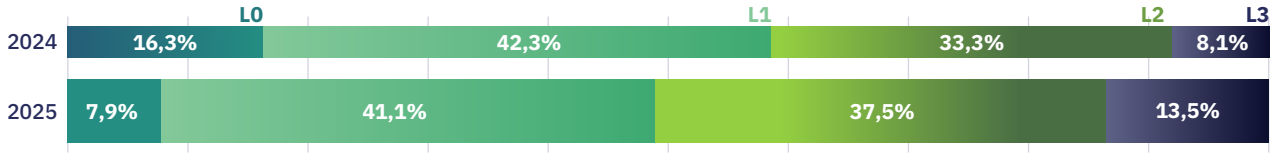
Un ecosistema en plena evolución

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.

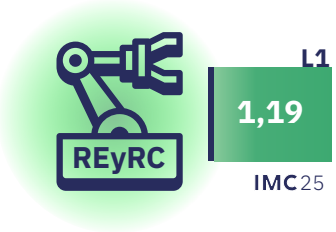
Esta evolución indica que las IES iberoamericanas están mejorando de forma decidida su capacidad para conocer sus activos, gestionar riesgos e implementar controles de monitoreo continuo, sentando las bases de una defensa más proactiva.

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

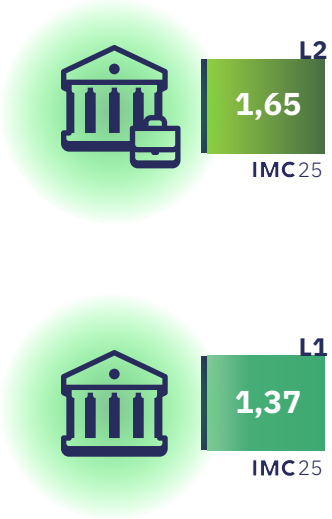
El progreso en ciberseguridad no es uniforme en toda la región, con países que lideran la adopción de prácticas avanzadas y otros que avanzan a un ritmo más moderado.

- **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 Colombia

COL

L0 L1 L2 L3

IMC24 1,62 L2

IMC25 1,75 L2

IMC COLOMBIA
1,75

2024-2025 EVOLUCIÓN
+0,13

IMC IBE DIFERENCIA
+0,24

TIPO DE IES
*evolución sobre IMC IES COL.

PÚBLICAS
1,86 (+0,07)

PRIVADAS
1,72 (+0,11)

DOMINIOS
*evolución sobre IMC dominios IBE

PROTEGER
2,00 (+0,32)

GOBERNAR
1,90 (+0,35)

DETECTAR
1,89 (+0,25)

IDENTIFICAR
1,77 (+0,26)

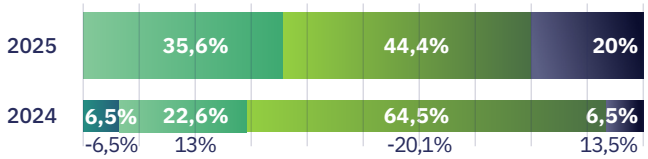
RESPONDER
1,19 (0,00)

TOP 3
PROTEGER
GOBERNAR
DETECTAR

Todos los dominios analizados, salvo Responder y Recuperar, superan la media de Iberoamérica (1,51).

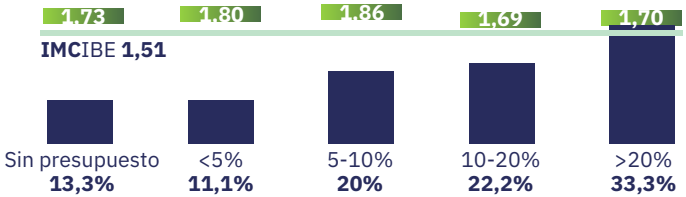
Responder y Recuperar (1,19), presenta el mismo valor que la media iberoamericana para este dominio.

DISTRIBUCIÓN SEGÚN IMC



Un ecosistema colombiano en crecimiento: en 2025 no hay IES en nivel inicial (L0). Aumentan un 13% las de nivel básico (L1), caen un 20,1% las de nivel intermedio (L2) y crecen hasta el 20% las de nivel avanzado (L3).

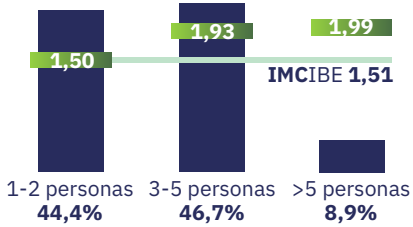
PRESUPUESTO



El 86,7% de las IES colombianas cuentan con presupuesto de ciberseguridad.

A diferencia de otros países, especialmente aquellos con madurez más baja, el presupuesto asignado a ciberseguridad es importante, pero la desviación entre los diferentes grupos es más suavizada.

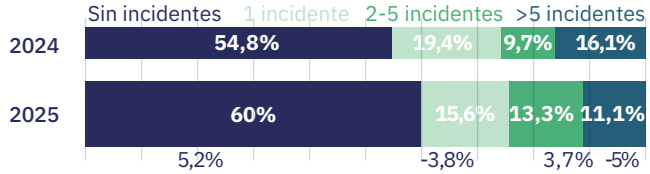
EQUIPOS DE CIBERSEGURIDAD



Más del 90% están compuestos por menos de 5 personas. Se observa una clara relación directa entre el tamaño de los equipos de seguridad y el nivel de madurez.

CIBERINCIDENTES

DISTRIBUCIÓN DE LOS INCIDENTES



EVOLUCIÓN DEL IMC SEGÚN Nº DE INCIDENTES

6 de cada 10 IES colombianas no 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 en las IES

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 COLOMBIA

Colombia ha obtenido un **IMC 2025 de 1,75,** un valor que corresponde al nivel intermedio (L2) dentro del modelo de madurez. Esto significa que, en promedio, las instituciones de educación superior (IES) colombianas han desarrollado capacidades de ciberseguridad de forma relativamente consolidada, situándose en etapas intermedias de madurez aunque aún sin alcanzar un nivel plenamente avanzado. El resultado de Colombia se ubica por encima del **promedio iberoamericano** que en 2025 fue de 1,51, manteniendo una ventaja de 0,24 puntos sobre la media regional (similar a la brecha de 0,25 puntos observada en 2024).

A nivel de evolución anual, **Colombia ha mostrado una mejora notable frente a 2024,** cuando su IMC había sido 1,62. El incremento de +0,13 puntos indica un progreso significativo, aunque ligeramente por debajo del avance promedio iberoamericano (+0,14). En otras palabras, el país logró **elevar su índice de madurez de ciberseguridad,** conservando su posición por encima de la media regional, pero sin aumentar la distancia relativa respecto a otros países. De hecho, Colombia se mantiene en el grupo de naciones de madurez intermedia (L2) – junto con España o Brasil, por ejemplo – superando claramente a países rezagados en nivel básico (L1) como Argentina o México, y ocupando el segundo lugar entre los países participantes después de España.

En síntesis, el país ha fortalecido su índice de madurez de ciberseguridad de forma sostenida, **manteniendo un desempeño superior al promedio regional,** si bien deberá seguir acelerando sus avances para acercarse a los niveles más altos de la región.

BRECHA ENTRE UNIVERSIDADES PÚBLICAS Y PRIVADAS

Un análisis por tipo de institución revela **diferencias moderadas de madurez** en Colombia según el sector, aunque menores que en otros países de la región. En 2025, las universidades **privadas** del país alcanzaron un IMC medio de **1,86,** ligeramente superior incluso a la media iberoamericana, mientras que las **públicas** promediaron **1,72.** Esta brecha (0,14 puntos) se ha reducido respecto a 2024, cuando las privadas marcaban 1,79 vs. 1,61 en las públicas (diferencia de 0,18).

Las cifras evidencian que las IES privadas han mantenido un mayor nivel de madurez y han mejorado, pero las públicas también **han acelerado su progreso** en el último año, cerrando ligeramente la brecha. El resultado invita a una reflexión: aunque **ambos subsectores han mejorado su IMC,** las instituciones públicas – mayoritarias en número y alcance – siguen encontrando obstáculos para desarrollar sus capacidades de ciberseguridad al mismo ritmo que las privadas. Las universidades privadas suelen exhibir prácticas más formalizadas y recursos mejor aplicados, mientras que las públicas permanecen algo rezagadas en aspectos clave. Esta disparidad, lejos de fomentar rivalidad, señala la necesidad de **elevar el apoyo estructural y estratégico** en el sector público para seguir cerrando la brecha, entendiendo que la ciberseguridad en la academia debe avanzar de manera homogénea.

En particular, dominios como el **gobierno de la seguridad,** la formalización de **procedimientos y la asignación de presupuesto** presentan diferencias marcadas a favor de las privadas – las evidencias indican, por ejemplo, que muchas universidades públicas carecen de un presupuesto específico para seguridad, reflejándose en niveles de madurez más bajos (en 2025, el subdominio de presupuesto en IES públicas apenas alcanzó un valor incipiente). Por tanto, las universidades públicas requieren mayor **inversión y enfoque institucional** para no quedar vulnerables frente al creciente panorama de riesgos, consolidando un avance más parejo con sus pares privadas.

DISTRIBUCIÓN DE NIVELES DE MADUREZ EN LAS IES

La distribución del nivel de madurez entre las IES colombianas muestra **cambios importantes hacia extremos más altos,** aunque con un aumento en la proporción de instituciones en nivel básico. En 2025, **ninguna** institución se ubica ya en el nivel L0 (incipiente/inexistente), mientras que el **35,6%** de las IES aproximadamente están en nivel **L1 (básico), 44,4% en L2 (intermedio)** y alrededor de **20,0% alcanzan el L3 (avanzado).** En comparación con el año anterior, este panorama refleja **mejoras notables:** en 2024, aún un 6,5% de las IES se encontraban en L0 y solo 6,5% habían logrado L3, frente a un 64,5% en L2 y 22,6% en L1. Es decir, en el último año **se eliminó prácticamente el nivel incipiente** (pasando de 6,5% a 0% instituciones en L0) y **se cuadruplicó** la proporción de IES en nivel avanzado (de 6,5% a 20%). Consecuentemente, la categoría L2 perdió peso relativo (de 64,5% bajó a 44,4%), mientras **aumentó significativamente L1** (de 22,6% a 35,6%). Este desplazamiento sugiere que algunas IES que antes estaban en nivel intermedio, han progresado hasta el nivel avanzado, mientras que la incorporación de nuevas IES o la reevaluación de otras ha engrosado el nivel básico.

En términos generales, Colombia **ha logrado que todas sus IES alcancen al menos un nivel básico de madurez,** eliminando casos totalmente rezagados, y ha impulsado a un grupo importante hasta niveles avanzados. Sin embargo, la distribución aún **no es homogénea:** la mayoría de instituciones (80%) se concentra en los niveles básicos o intermedios (L1 o L2), y solo una quinta parte ha logrado un estadio avanzado. El reto a futuro radica en **seguir elevando el piso común de madurez** – reduciendo ese 35,6% de IES en nivel básico– de modo que más instituciones asciendan a niveles intermedios y avanzados. Si bien 2025 muestra progresos claros (ninguna IES en nivel inexistente y un aumento sustancial de L3), Colombia debe aspirar a consolidar un estado general más robusto, incrementando el porcentaje de instituciones que alcanzan los niveles L2 y L3, para fortalecer la resiliencia colectiva en ciberseguridad.

DESEMPEÑO POR DOMINIOS

El perfil de madurez de Colombia varía al examinar los dominios y subdominios del modelo IMC, revelando **fortalezas técnicas y algunas debilidades en capacidades de respuesta y recursos.** Entre los cinco dominios principales, el país se desempeña **mejor en Proteger (PR),** con un valor promedio de **1,92,** muy cercano a 2,0, que indica un nivel intermedio-alto. Le siguen **Detectar (DE) con 1,89, Gobernar (GB) con 1,90** y un poco más alejado, **Identificar (ID) con 1,77.**

Los datos sugieren que las IES colombianas avanzan significativamente en la implementación de controles de protección como seguridad de infraestructura, gestión de accesos, protección de datos; y cuentan con una gestión de seguridad gubernativa relativamente sólida, así como con mecanismos aceptables de monitoreo y detección de amenazas. Por contra, **Responder y Recuperar (REyRC)** presenta el puntaje más bajo, con un IMC de **1,19** (nivel básico/incipiente), reflejando rezagos importantes en la capacidad de respuesta a incidentes.

En síntesis, Colombia exhibe un desempeño robusto en la prevención (protección) y en la organización/gobierno de la seguridad, pero muestra **debilidad en la preparación y reacción ante incidentes.**

A nivel de **subdominios específicos,** destacan **puntos fuertes** técnicos muy notables. En particular, **Infraestructura** –seguridad de redes, sistemas y centros de datos– alcanza en 2025 un nivel avanzado (IMC combinado **≈2,8).** Este valor sobresaliente sugiere que la protección de la infraestructura TI en muchas IES colombianas es bastante madura, posiblemente gracias a la adopción de buenas prácticas, arquitecturas seguras y herramientas robustas *(firewalls,* sistemas de prevención de intrusiones, etc.). Otro subdominio bien posicionado es **Comunicaciones** (seguridad en redes y comunicaciones), con un desempeño también alto (en torno a **2,4** en 2025). Estos logros evidencian que Colombia ha priorizado las **medidas técnicas de resguardo** de sus activos digitales, alcanzando niveles competitivos en dichos aspectos.

En el lado opuesto, destacan brechas preocupantes en los subdominios relacionados con la **respuesta a incidentes y la asignación de recursos.** Dentro del dominio REyRC, el subdominio **Recuperación** –que evalúa la capacidad de restaurar sistemas tras un incidente– se sitúa en un nivel básico (IMC 1,0 en 2025). Algo similar ocurre con **Mitigación,** que mide las habilidades para contener y reducir el impacto de los ataques, con un valor medio de apenas 1,1. Estos resultados indican que muchas universidades **carecen de procedimientos sólidos de respuesta,** quedando expuestas a consecuencias graves cuando enfrentan un incidente.

Por otro lado, aunque **Gobernar** presenta una valoración general positiva, aún se observan **déficits importantes en algunos aspectos de organización.** El subdominio **Presupuesto,** por ejemplo, se mantiene como uno de los más rezagados. Pese a una ligera mejora respecto a 2024, su media nacional sigue en torno a 1,6–1,7 (nivel intermedio). El caso es más crítico en las IES públicas, que caen a **1,14,** reflejo de una **planificación financiera muy limitada** en ciberseguridad.

En conjunto, estos datos muestran que, si bien Colombia ha logrado avances técnicos relevantes, **aún presenta debilidades importantes en las dimensiones operativas e institucionales.** Faltan estrategias integrales de gestión de incidentes, planes de continuidad y presupuestos específicos que garanticen una protección sistemática.

En resumen, el perfil del país es **fuerte en prevención técnica, pero débil en respuesta y en algunos puntos de gobernanza,** por lo que será clave **reforzar los cimientos procedimentales y de recursos** para alcanzar un nivel de madurez más equilibrado y sostenible.

IMPACTO DEL TAMAÑO DEL EQUIPO DE CIBERSEGURIDAD

Los datos de 2025 refuerzan con claridad una tendencia ya observada en ediciones anteriores: **existe una correlación directa entre el tamaño del equipo de ciberseguridad y el nivel de madurez alcanzado por las instituciones.** Las universidades colombianas que cuentan con más profesionales especializados muestran una madurez significativamente superior a aquellas sin personal dedicado.

En concreto, las instituciones con **equipos medianos (de 3 a 5 personas)** han logrado un **IMC promedio de 1,93,** mientras que aquellas con **más de 5 miembros** han alcanzado un IMC medio de **1,99.** En contraste, las universidades con solo **1 o 2 profesionales** se sitúan en torno a **1,50.**

Este patrón ya era visible en 2024, cuando las IES sin equipos propios difícilmente alcanzaban el nivel básico, mientras que aquellas con estructuras más sólidas se situaban en niveles intermedios consolidados. La conclusión es clara: **tener personal específico y cualificado en ciberseguridad permite estructurar políticas, especializar funciones clave (gestión de incidentes, monitoreo, análisis de riesgos) y sostener una mejora contínua,** lo que se traduce directamente en mejores niveles de madurez institucional.

Por el contrario, las instituciones que dependen de perfiles generalistas o de servicios externos mínimos encuentran grandes dificultades para superar el nivel básico. Este resultado subraya nuevamente que **la inversión en talento humano es uno de los factores más determinantes para avanzar en ciberseguridad y no quedar rezagado en el modelo de madurez.**

INFLUENCIA DEL PRESUPUESTO EN CIBERSEGURIDAD

La asignación presupuestaria en ciberseguridad tiene un impacto directo en el nivel de madurez alcanzado por las IES, en la misma línea que ocurre con la disponibilidad de personal especializado. Los datos de Colombia evidencian esta relación pero matizada. En el caso de Colombia, el capital humano tiene un mayor peso en esta ecuación. Es decir, el presupuesto es importante para la ejecución de inversiones en ciberseguridad pero la madurez de las IES del país hace que la curva presupuesto-imc sea más suavizada que en otros países con un IMC inferior.

Esto no quiere decir que el presupuesto no sea importante, sino que en países con mayor solidez en ciberseguridad hay aspectos que tienen un mayor impacto directo en la madurez.

En 2025, la variación del nivel de madurez según el presupuesto se mantiene en un intervalo de 17 décimas para los diferentes grupos de presupuesto. En 2024, se observaba que no asignar recursos equivalía a permanecer en niveles incipientes, mientras que las instituciones con partidas superiores al 20% lograban situarse cerca del nivel intermedio-alto.

Incluso los incrementos modestos en inversión generan un impacto positivo: pasar de no asignar nada a dedicar un pequeño porcentaje (<5%) eleva sustancialmente el nivel de madurez por encima del umbral más bajo. Asignar entre un 5% y un 10% ya se traduce en IMC de entre 1,80 y 1,86.

Sin embargo, **en Colombia muchas IES aún no respaldan sus políticas de seguridad con el presupuesto necesario.** El subdominio Presupuesto se mantiene como uno de los más débiles, reflejo de que en muchas universidades, especialmente públicas, la ciberseguridad sigue sin ocupar un lugar prioritario en la planificación financiera.

En conjunto con el tamaño del equipo, el presupuesto específico forma un eje crítico de madurez. **Sin una inversión sostenida y suficiente, los esfuerzos institucionales en normativas o procedimientos difícilmente se traducen en avances reales.** La evidencia es clara: priorizar la seguridad digital en los presupuestos permite a las universidades implementar mejores tecnologías, fortalecer sus capacidades internas y avanzar hacia niveles más sólidos de madurez.

INCIDENTES DE SEGURIDAD: EVOLUCIÓN Y RELACIÓN CON LA MADUREZ

El panorama de **ciberincidentes** en las IES colombianas ofrece otro indicador importante, tanto de la exposición a amenazas como de la efectividad de las capacidades de seguridad desarrolladas.

En el último período analizado, Colombia **reporta una disminución** en la cantidad de incidentes críticos. El **promedio de incidentes** anuales por institución **bajó de 4,45 en 2024 a 3,55 en 2025.** De modo similar, entre las IES que sufrieron al menos un incidente, el promedio descendió de **10,75 a 9,18** incidentes en el año. Estas cifras sugieren que, aunque los incidentes continúan ocurriendo, su **frecuencia e intensidad se han moderado** ligeramente. Es probable que una mayor madurez esté permitiendo prevenir o contener mejor muchos ataques, reduciendo la cantidad de incidentes exitosos. Cabe destacar, además, que **más de la mitad de las IES (≈60%) lograron no registrar ningún incidente** en 2025. Si bien esto indica que una porción importante del sistema evitó brechas de seguridad reportables en el año, aún queda un **40% de IES que sufrieron uno o más incidentes,** evidenciando que la amenaza sigue presente en casi la mitad del sector.

Al explorar la relación entre el nivel de madurez y la incidencia de incidentes, emergen hallazgos reveladores. **En 2024,** a diferencia de otros países, los datos de Colombia ya sugerían la tendencia esperada: las instituciones **sin incidentes** presentaban, en promedio, un nivel de madurez más alto (IMC 1,78) que aquellas que enfrentaron varios. De hecho, las IES que sufrieron de **2 a 5 incidentes** en 2024 mostraban el IMC promedio más bajo (1,23), mientras que las pocas con **más de 5** incidentes promediaron 1,47 (aún por debajo del grupo sin incidentes). Esta dinámica se **consolida en 2025:** las IES que **no tuvieron ningún incidente** exhiben ahora el mayor nivel de madurez (IMC **1,84),** superando al de aquellas que sufrieron muchos incidentes (>5), con IMC **1,71.** Es decir, conforme **se eleva la madurez,** las universidades parecen más eficaces en **prevenir y resistir incidentes,** manteniendo a raya las brechas de seguridad. Por contra, las organizaciones con algunos incidentes reportados mantienen niveles de madurez más bajos (las que tuvieron uno o unos pocos incidentes en 2025 se ubicaron en IMC ~1,55–1,56, casi nivel básico). Posiblemente, las mejoras implementadas en las IES más avanzadas (mejores controles preventivos, detección temprana, respuesta eficaz) **están evitando que**

los ataques se materialicen en incidentes significativos, mientras que las IES menos maduras experimentan incidentes dada su mayor vulnerabilidad.

En conclusión, aunque el **panorama de incidentes en Colombia** sigue siendo delicado en casi la mitad de las IES, **se observa una reducción leve en su frecuencia** y una relación cada vez más coherente con la madurez: las IES más maduras logran **contener mejor los incidentes** (incluso evitarlos por completo), mientras que las menos maduras continúan más expuestas. Esto realza la importancia de **elevar el nivel de madurez** como vía para reducir el impacto de los incidentes de seguridad en el sector académico. Los avances de 2025 –menos incidentes en promedio y una correlación más "sana" madurez/incidentes– son alentadores, pero consolidar estos logros requerirá persistir en el fortalecimiento de las capacidades de ciberseguridad en **todas** las IES del país, de modo que el sistema universitario en su conjunto sea más **resiliente** frente a ciberamenazas.

USO DE LA INTELIGENCIA ARTIFICIAL EN CIBERSEGURIDAD

Adopción creciente, impacto heterogéneo y una lectura condicionada por la madurez previa.

El uso de inteligencia artificial (IA) en ciberseguridad en las IES colombianas muestra una adopción más extendida que en otros países, pero con patrones que varían mucho según el dominio. Mientras que Proteger (64%) y Detectar (56%) presentan un uso significativo, dominios como Gobernar, Responder o Formación se mantienen en niveles moderados o bajos, entre el 20% y el 38%. Esto configura un escenario donde la IA está presente, pero no de forma homogénea en las funciones críticas del modelo.

En cuanto a los niveles de madurez, las diferencias entre IES que usan y no usan IA son **irregulares.** En algunos dominios operativos —particularmente **Proteger y Detectar**— las instituciones con IA tienden a alcanzar valores medios algo mayores, sobre todo en aspectos como gestión de accesos, análisis de anomalías o servicios. Sin embargo, en otros dominios las diferencias se reducen o se inclinan en sentido contrario. Por ejemplo, en **Gobernar** el IMC de ambos grupos es prácticamente idéntico, e incluso en componentes estratégicos y procedimentales aparecen casos donde las IES sin IA superan ligeramente a las que sí la utilizan.

Esta variabilidad sugiere que la relación entre uso de IA y madurez no es lineal ni inmediata. Es razonable pensar que muchas de las instituciones que ya experimentan con IA cuentan previamente con **equipos consolidados, procesos estables y mayores capacidades técnicas,** lo que influye directamente en sus resultados del IMC. En ese sentido, la IA parece insertarse sobre bases que ya eran relativamente fuertes, más que generar mejoras automáticas o uniformes por sí misma.

También llama la atención que la adopción de IA se concentra en dominios donde la automatización —monitoreo, protección, vigilancia, servicios— ofrece un retorno operativo más claro. Allí sí se observan algunas ventajas en instituciones que declaran usarla, aunque estas diferencias deben interpretarse con cautela debido al peso del perfil institucional y a las variaciones internas entre grupos.

En síntesis, el caso colombiano refleja un ecosistema **más activo en la exploración de IA,** pero donde los efectos sobre la madurez son todavía difíciles de aislar. La tecnología parece alinearse con instituciones ya avanzadas en ciberseguridad, lo que sugiere que su adopción actual responde más a una estrategia incremental que a una transformación profunda. A futuro, será relevante observar si la expansión del uso de IA se traduce en mejoras consistentes y generalizables, o si sus beneficios dependerán de la capacidad organizativa previa de cada IES.

COLOMBIA

IMC 2025

Índice de Madurez en Ciberseguridad de las IES Iberoamericanas

metared by universia

Secretaría General Iberoamericana
Secretaria-Geral Ibero-Americana