ESPAÑA

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

ESPAÑA 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.

Crue Digitalización, España

Francisco José Sampalo Lainz

Universidad Politécnica de Cartagena

Responsable de Seguridad

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.

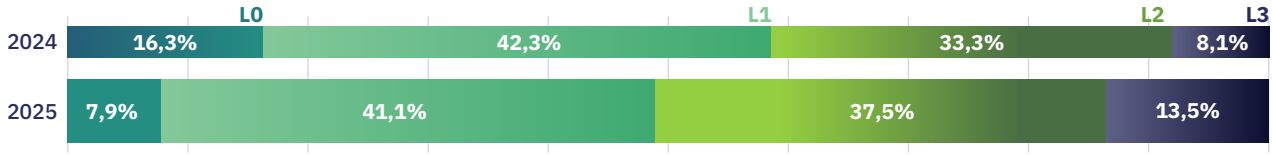
Un ecosistema en plena evolución

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.

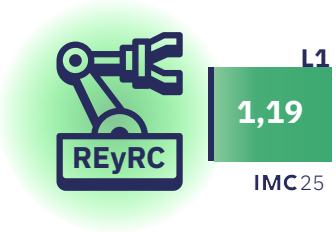
Avances en identificación, protección y detención

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.

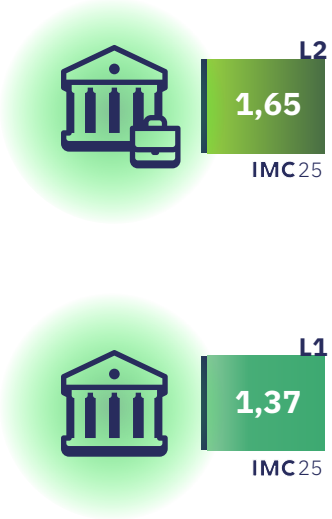
Progreso Sostenido: Argentina y España también muestran un avance notable, con un incremento de +0,15 puntos cada uno.

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

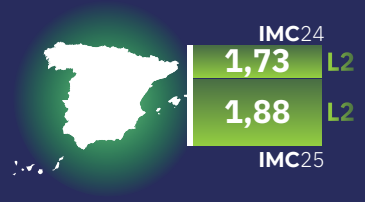
En síntesis, IMC funciona como un **predictor sólido del comportamiento real** frente a ciberamenazas. Invertir en madurez —tanto en estructura organizativa como en procesos y capacidades técnicas— se refleja directamente en una reducción del riesgo y del número de incidentes que afectan al funcionamiento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

ESP



IMC ESPAÑA

1,88

2024-2025 EVOLUCIÓN

+0,15

IMC IBE DIFERENCIA

+0,37

L0 L1 L2 L3

TIPO DE IES

*evolución sobre IMC IES ESP.

PÚBLICAS
1,88 (+0,06)

PRIVADAS
1,88 (+0,16)

DOMINIOS

*evolución sobre IMC dominios IBE

DETECTAR
2,11 (+0,47)

GOBERNAR
2,07 (+0,52)

PROTEGER
1,92 (+0,26)

IDENTIFICAR
1,84 (+0,33)

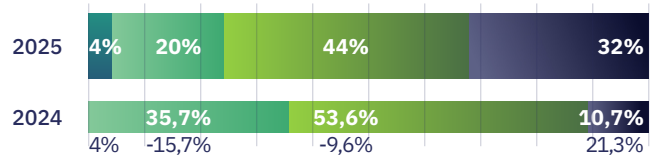
RESPONDER
1,48 (+0,39)

TOP 3
DETECTAR
GOBERNAR
PROTEGER

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

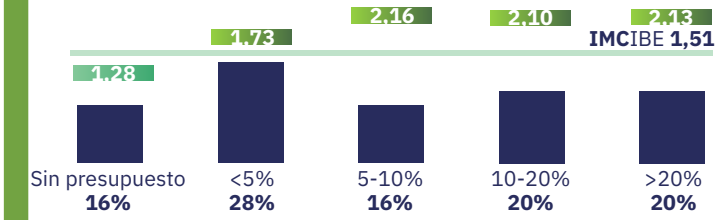
Responder y Recuperar (1,48), se encuentra a tan solo 3 décimas de superarla.

DISTRIBUCIÓN SEGÚN IMC



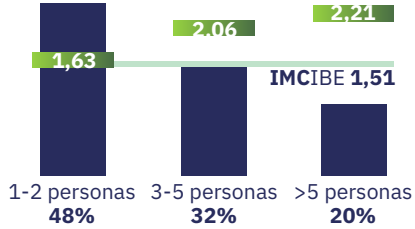
Crecen un 21% las IES del nivel más alto (avanzado, L3).
7 de cada 10 IES españolas se encuentran en niveles intermedio (L2) o avanzado (L3).

PRESUPUESTO



El 84% de las IES españolas cuentan con presupuesto de ciberseguridad.
El nivel de madurez de las IES con el 10-20% del presupuesto casi dobla al de las que no tienen ninguno.
Las que cuentan con presupuesto para ciberseguridad, aunque sea pequeño, alcanzan un nivel L2.

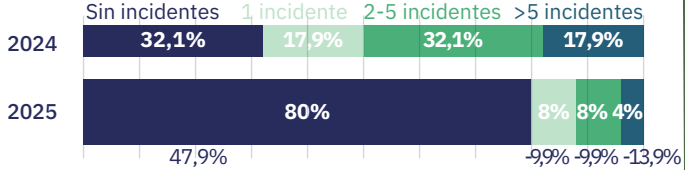
EQUIPOS DE CIBERSEGURIDAD



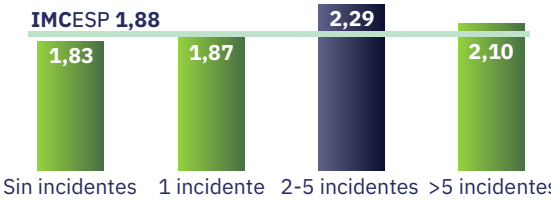
Cerca del 50% están compuestos por 1 o 2 personas.
Clara tendencia alcista en el nivel de madurez de aquellas IES con equipos de mayor tamaño.

CIBERINCIDENTES

DISTRIBUCIÓN DE LOS INCIDENTES



EVOLUCIÓN DEL IMC SEGÚN Nº DE INCIDENTES



7 de cada 10 IES españolas han sufrido algún ciberincidente el último año.
Las IES que han reportado entre 2 y 5 incidentes presentan un índice de madurez mayor (2,29), seguidas por aquéllas que han sufrido más de 5 incidentes (2,10).

3.

Resumen Ejecutivo

RESUMEN EJECUTIVO ESPAÑA

España consolida un nivel intermedio alto en ciberseguridad.

España ha obtenido un **IMC 2025 de 1,88,** lo que la ubica sólidamente en el nivel **intermedio (L2)** de madurez en ciberseguridad. En promedio, las instituciones de educación superior españolas han desarrollado capacidades cercanas a etapas intermedias-avanzadas, aunque aún sin alcanzar la madurez plena. Este valor **supera ampliamente el promedio iberoamericano,** situado en 1,51, quedando España **0,37 puntos por encima de la media regional.** En 2024 ya mantenía una ventaja similar (IMC 1,73 frente a 1,37 de la región), y el incremento nacional de +0,15 puntos en el último año supera levemente el ritmo de mejora iberoamericano (~+0,14). En síntesis, España **consolida su posición** como uno de los países más maduros de la región, afianzada en un nivel L2 alto y **manteniendo su ventaja relativa,** aunque sin acortar todavía la distancia hacia el nivel avanzado (L3).

BRECHA ENTRE UNIVERSIDADES PÚBLICAS Y PRIVADAS

La madurez de las universidades públicas y privadas se equilibra

A diferencia de otros países, España **ha prácticamente cerrado la brecha de madurez** entre sus universidades privadas y públicas. En 2024 las privadas mostraban un IMC medio ligeramente superior (≈1,82 vs. 1,72 en públicas), una diferencia modesta de 0,10 puntos. Para 2025, ambas alcanzan **prácticamente el mismo nivel:** alrededor de **1,88** de IMC en promedio. Es decir, **no se observa una distancia significativa** entre sectores: las instituciones públicas han acelerado su desarrollo y **alcanzado a las privadas en madurez.**

Conviene destacar que las universidades públicas mejoraron más su IMC (+0,16) que las privadas (+0,06) de 2024 a 2025, convergiendo en el mismo valor. Este resultado sugiere que **no hay un rezago estructural marcado** entre sectores en España; ambos tipos de IES han logrado niveles intermedios altos. En la comparación es importante matizar que **no se trata de competir, sino de elevar conjuntamente** la ciberseguridad académica: la paridad alcanzada indica un avance cohesionado. Aun así, persisten diferencias internas en aspectos concretos (por ejemplo, las privadas siguen destinando más presupuesto específico a seguridad), pero en el global **el perfil de madurez es ahora muy similar,** lo cual reduce posibles brechas de vulnerabilidad entre los dos subsectores.

DISTRIBUCIÓN DE NIVELES DE MADUREZ

La distribución del nivel de madurez de las IES españolas entre 2024 y 2025 **evidencia un marcado desplazamiento hacia niveles más altos**. El año 2024 no registraba prácticamente instituciones en nivel L0 (incipiente/inexistente, 0%), con la mayoría en L1 (básico, 35,7%) o L2 (intermedio,~53,6%) y apenas un 10,7% en L3 (avanzado).

En 2025, aunque aparece un pequeño **4% en L0** (posiblemente nuevas IES incorporadas con capacidades incipientes), **disminuye de manera drástica L1** a solo 20% de las instituciones, **aumenta L2 a 44%** y, sobre todo, **se triplica la proporción en L3 (32% de las IES).** En conjunto, **tres de cada cuatro universidades (76%)** alcanzan al menos un nivel intermedio (L2–L3),

frente a 64% el año anterior, lo que refleja un **notable fortalecimiento del perfil de madurez.**

Muchas IES que en 2024 se encontraban en nivel básico han progresado a niveles intermedios o avanzados en 2025, elevando el "techo" nacional de ciberseguridad. Este panorama indica que España ha logrado **ensanchar la cúspide de madurez:** casi un tercio del sistema ya opera en un estado avanzado, cuando antes eso era un grupo muy reducido.

El **reto a futuro** será continuar empujando el piso hacia arriba (reducir ese 20% restante en nivel básico) y seguir incorporando a las rezagadas –incluidas las pocas en L0– de modo que la madurez sea más homogénea y ninguna institución quede expuesta por falta de capacidades mínimas.

Fortalezas técnico-operativas y debilidades en respuesta e inversión.

DESEMPEÑO POR DOMINIOS

El perfil por dominios del modelo IMC revela en España **áreas de fortaleza en controles técnicos y de gestión, frente a brechas en respuesta a incidentes y recursos.** Entre los cinco dominios principales, el mejor desempeño en 2025 se observa en **Detectar (DE)** con valor promedio **2,11,** seguido de cerca por **Gobernar (GB, 2,07)** y luego **Proteger (PR, 1,92).** Estos niveles indican que las IES españolas han implantado con éxito mecanismos de monitoreo, vigilancia y gobierno de la seguridad, situándose incluso cerca del nivel avanzado en detección de amenazas. Por el contrario, el dominio **Responder y Recuperar (REyRC)** es el más rezagado con solo **1,48** (nivel básico), incluso ligeramente **inferior al año previo** (1,51 en 2024).

Asimismo, **Identificar (ID),** aunque mejora notablemente de 1,46 a **1,84,** se mantiene por detrás de los dominios líderes. En conjunto, **España exhibe un perfil equilibrado hacia arriba en prevención y gestión, pero adolece de preparación reactiva:** las capacidades de respuesta a incidentes no han avanzado al mismo ritmo e **imponen un cuello de botella** en la madurez general.

A nivel de **subdominios específicos,** sobresalen **fortalezas muy notorias en la dimensión tecnológica.** Por ejemplo, el subdominio **Infraestructura (seguridad de redes, sistemas y centros de datos)** alcanza en 2025 un nivel promedio de **IMC ≈2,75,** cercano al avanzado completo. Este valor extraordinario sugiere que la protección de la infraestructura TI en muchas universidades españolas es bastante madura, probablemente gracias a la adopción generalizada de **buenas prácticas técnicas, herramientas robustas (*firewalls*, IDS/IPS, etc.) y arquitecturas seguras.** También destaca **Comunicaciones** (seguridad en redes y comunicaciones) con un desempeño alto (IMC ~2,22). Igualmente, la **monitorización de actividad de usuarios** se sitúa en niveles avanzados (IMC >2,3 en promedio); indicio de que las IES con mayor madurez han implementado **Sistemas de Información de Seguridad (SIEM), detección de anomalías y registros de auditoría** efectivos.

En el **lado opuesto, persisten brechas preocupantes** en subdominios relacionados con gobernanza y respuesta. El subdominio **Continuidad** (planes de continuidad de negocio/operaciones) apenas alcanza **IMC ~1,0 en 2025,** manteniéndose en estado incipiente a pesar de una ligera mejora. De forma similar, **Recuperación ante desastres/incidentes** promedia solo **1,12,** revelando que la mayoría de universidades carece de procedimientos sólidos para restaurar sistemas tras un ataque. Otro punto débil es el **Presupuesto** dedicado: aunque mejoró a **1,44** en 2025, sigue siendo de los valores más bajos, particularmente en el sector público (muchas IES públicas declaran

financiamiento muy limitado para seguridad). Estas brechas indican que, si bien España ha **fortalecido sobremanera sus medidas técnicas, aún adolece de madurez en dimensiones organizativas y de respuesta:** faltan planes integrales de continuidad, asignación adecuada de recursos financieros y procesos formales de gestión de incidentes.

En resumen, el desempeño por dominios es **dispar –sobresaliente en prevención/detección, pero débil en reacción e inversión–** lo cual sugiere focalizar esfuerzos en fortalecer los cimientos institucionales (planificación, procedimientos y recursos) para equilibrar el perfil de madurez nacional.

Más personal especializado impulsa la madurez.

IMPACTO DEL TAMAÑO DEL EQUIPO DE CIBERSEGURIDAD

Los datos de España **confirman claramente la correlación positiva** entre el tamaño del equipo de seguridad dedicado y el nivel de madurez de las IES, replicando el patrón observado en la región. Las instituciones con equipos más numerosos alcanzan **índices de madurez significativamente superiores** a aquellas con escaso o ningún personal especializado. En 2024, por ejemplo, las universidades con **más de 5 profesionales** en seguridad lograron un IMC promedio de **2,33** (nivel avanzado, L3), mientras que las que contaban con **3-5 personas** se quedaron en **1,75** (nivel intermedio, L2). Incluso disponer de un equipo pequeño **(1-2 personas)** marcaba una diferencia considerable (IMC 1,55 en 2024). En 2025 esta brecha persiste: las IES con **equipos de 3-5 integrantes** promedian IMC ≈2,06, y las pocas con **más de 5 rondan 2,21,** en tanto que las organizaciones con **solo 1-2 personas alcanzan cerca de 1,63.** Si bien la distancia extrema se redujo ligeramente, **las diferencias siguen siendo notables.**

En términos prácticos, **contar con un equipo dedicado es un factor determinante:** las IES con mayor personal pueden implementar más controles y programas de mejora continua, alcanzando niveles de madurez mucho más altos, mientras que aquellas sin equipo específico difícilmente superan el nivel básico. Este patrón se ha mantenido de 2024 a 2025, enviando un mensaje claro: **invertir en capital humano especializado en ciberseguridad resulta crucial** para avanzar en el modelo de madurez.

A mayor inversión, mayor madurez alcanzada.

INFLUENCIA DEL PRESUPUESTO EN CIBERSEGURIDAD

De forma análoga al recurso humano, la **asignación de presupuesto específico** para ciberseguridad –y su **peso relativo dentro del gasto de TI**– tiene un impacto directo en el nivel de madurez de las IES. Las instituciones que **destinan una proporción elevada de su presupuesto de TI a seguridad** exhiben índices de madurez muy superiores a las que invierten poco o nada. En la región se observa que aquellas sin partida dedicada (0%) permanecen en niveles en niveles básicos (1,28), mientras que las que canalizan **más del 20%** alcanzan madurez cercana al nivel avanzado (IMC 2,13). Incluso **pequeñas inversiones** marcan diferencia: por ejemplo, pasar de no asignar nada a invertir **aunque sea <5%** puede elevar el IMC promedio desde 1,28 hasta 1,73.

En el caso de **España,** la mayoría de IES **sí cuenta con algún presupuesto para seguridad,** pero los valores del subdominio Presupuesto (IMC 1,44 en

2025) indican que **suele ser limitado.** Se infiere que solo **una minoría de universidades españolas invierte porcentajes altos** en ciberseguridad (posiblemente las más maduras, que destinan >10-20% del presupuesto TI), mientras que otras mantienen partidas modestas.

La tendencia general, no obstante, es clara: las IES que **incorporan la seguridad como prioridad presupuestaria** logran implementar mejores controles, herramientas y personal, reflejándose en niveles de madurez mayores, en tanto que quienes **no asignan recursos suficientes quedan rezagadas.**

Este **factor presupuestario, junto al tamaño del equipo, conforma un eje crítico de mejora:** para que una universidad transite del nivel básico al intermedio-avanzado, necesita respaldar sus políticas con **financiamiento adecuado y sostenido** en seguridad digital. España deberá seguir trabajando en esta línea, fomentando que más IES destinen un porcentaje creciente de sus presupuestos de TI a ciberseguridad, cerrando así la brecha que aún separa a las instituciones más rezagadas de las líderes en madurez.

Menos casos y una relación más sana con el nivel de madurez.

INCIDENTES DE SEGURIDAD: EVOLUCIÓN Y RELACIÓN CON LA MADUREZ

El panorama de ciberincidentes en las IES españolas sugiere **mejoras tanto en la reducción de casos como en su relación con la madurez alcanzada.** En el último año analizado, **disminuyó la frecuencia de incidentes graves:** se estima que en 2025 aumentó el porcentaje de universidades que **no sufrieron ningún incidente,** superando la mitad del total (en 2024 era alrededor del 32%, subiendo a 80% sin incidentes en 2025, según las tendencias regionales). Además, las que sí enfrentaron ataques registraron, en promedio, menos incidentes exitosos gracias a mejores controles de prevención y detección.

La relación entre incidentes y madurez también experimentó un cambio significativo. En **2024** se observaba un patrón paradójico: las IES con **más incidentes reportados tendían a tener un IMC más alto.** Por ejemplo, aquellas con >5 incidentes promediaban IMC ~1,87, comparado con 1,52 de las que no tuvieron ninguno. Esto podía interpretarse así: las universidades más grandes o avanzadas detectaban y reportaban más incidentes (por su mayor exposición y mejores mecanismos), mientras que las menos maduras quizá no registraban incidentes – ya fuera por su menor tamaño o por falta de capacidad de detección.

Sin embargo, **en 2025 la dinámica cambia.** Los datos muestran que las instituciones sin **incidentes alcanzaron una madurez equiparable o superior** a las más atacadas. De hecho, las IES sin ningún incidente en el año promedian un IMC 1,83, prácticamente al nivel –e incluso acercándose– de aquellas con >5 incidentes (IMC 2,10). Llama la atención que el grupo con **2 a 5 incidentes** presenta el IMC más alto (2,29), indicando que cierto grado de exposición controlada coincide con capacidades muy desarrolladas.

En conjunto, conforme las universidades **elevan su madurez, logran prevenir y resistir mejor los ataques,** rompiendo la correlación positiva previa entre incidentes y madurez. **Las instituciones más maduras ahora pueden incluso no sufrir ningún incidente significativo en el año,** evidenciando mayor resiliencia.

En conclusión, **2025 trae buenas noticias:** se reducen los ciberincidentes en el sector universitario español y **la vulnerabilidad ya no es signo de avance** (antes los más maduros reportaban más incidentes; ahora logran contenerlos). Esto realza la importancia de seguir elevando el nivel de madurez en todas las IES como vía para **minimizar el impacto de los incidentes** y alcanzar un ecosistema académico más seguro.

USO DE LA INTELIGENCIA ARTIFICIAL EN CIBERSEGURIDAD

Primeros pasos con alto potencial en las IES españolas.

El uso de **inteligencia artificial (IA)** en las labores de ciberseguridad universitarias es **aún incipiente en España,** pero los pocos casos de adopción temprana **muestran una madurez notablemente superior.**

Según los datos, solamente una **minoría muy reducida** de IES (apenas uno o dos centros pioneros) declararon emplear herramientas de IA para reforzar su seguridad –por ejemplo, algoritmos de detección de amenazas, análisis automatizado de eventos o respuesta asistida–. Estas instituciones que **usan IA alcanzaron un IMC promedio de 2,55,** frente a apenas 1,85 en aquellas que **no utilizan IA.** La diferencia es contundente (≈+0,7 puntos de madurez) y sugiere que **la adopción de IA está asociada a estrategias de ciberseguridad más avanzadas** y a una mayor sofisticación en capacidades.

Probablemente las universidades que incorporan IA sean las que ya tenían un alto nivel de madurez y recursos, **posiblemente grandes instituciones o algunas privadas líderes,** aunque el conjunto de datos es muy pequeño para generalizar por sector. En cualquier caso, **no se observan aún diferencias sectoriales amplias** en el uso de IA, simplemente porque la gran mayoría (≈95% o más) de las IES españolas **aún no la han implementado** en 2025. Esto indica que la IA en ciberseguridad se encuentra **en fase exploratoria** en el ámbito académico: solo unos pioneros la están probando y cosechando sus beneficios, mientras que el resto observa su evolución.

De cara al futuro, esta tecnología podría convertirse en **un factor diferenciador importante** –acelerando la detección de amenazas, reduciendo tiempos de respuesta y optimizando la gestión de riesgos– por lo que **se espera un crecimiento** en su adopción conforme las universidades vayan fortaleciendo sus cimientos de ciberseguridad. En suma, **el uso de IA es todavía limitado pero promete alto impacto:** las IES que logren integrarla eficazmente podrían obtener **una ventaja considerable en su nivel de madurez y protección** frente a amenazas cada vez más avanzadas.

ESPAÑA IMC 2025

Índice de Madurez en Ciberseguridad de las IES Iberoamericanas

metared by universia

Secretaría General Iberoamericana
Secretaria-Geral Ibero-Americana