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

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. MetaRed: La importancia de la colaboración en ciberseguridad 7
2. Conclusiones 11
3. IMC: Índice de Madurez en Ciberseguridad 20
3.1 Modelo IMC 24
3.2 Dominios 24
3.3 Niveles de madurez 26
3.4 Tipología de la muestra 28
4. IMC Iberoamericano 32
4.1 Evolución/tendencia 33
4.2 IMC por dominio de aplicación 35
4.3 Uso de la Inteligencia Artificial 77
4.4 Enfoque de las IES en torno a la ciberseguridad 78
4.5 IMC Iberoamericano por país 80
4.6 IMC Iberoamericano por tipo de institución 87
4.7 IMC Iberoamericano por tamaño 91
4.8 IMC según presupuesto asignado a ciberseguridad 100
4.9 Ciberincidentes en Iberoamérica 104
4.10 IMC Iberoamericano según la gestión interna de la ciberseguridad 108
5. Argentina 111
6. Brasil 118
7. Chile 124
8. Colombia 131
9. Ecuador 138
10. España 143
11. México 150
12. Perú 156
13.Portugal 162
Anexo 1. Ficha técnica. Descripción de la muestra 170

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.

1.

MetaRed: La importancia de la colaboración en ciberseguridad

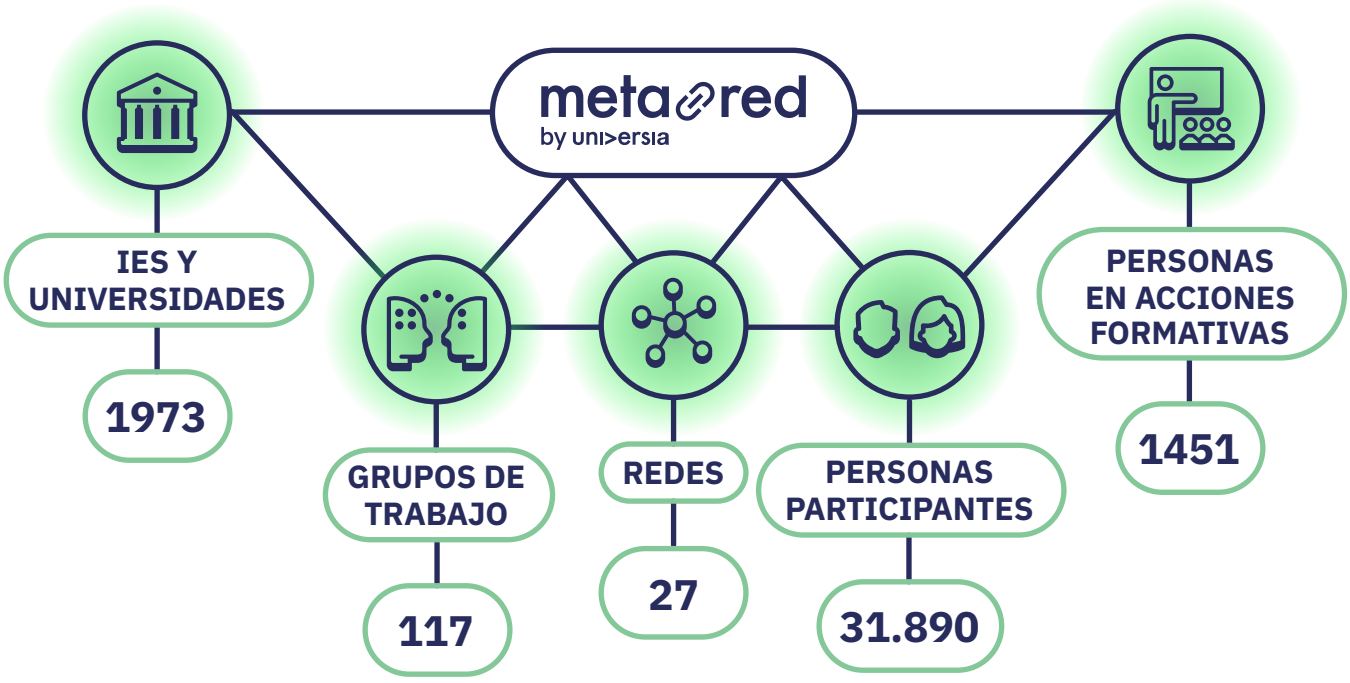
MetaRed

Grupo de Trabajo Internacional en seguridad

MetaRed es la mayor red de redes de colaboración de Instituciones de Educación Superior (IES) iberoamericanas, públicas y privadas, que impulsa la cooperación en ámbitos estratégicos como la transformación digital, el emprendimiento, la sostenibilidad y la responsabilidad social universitaria.

En el terreno de la transformación digital, **MetaRed TIC** articula un espacio de trabajo colaborativo en el que participan más de 1.973 instituciones de 15 países, representadas por sus responsables de Tecnologías de la Información y la Comunicación (TIC), un Comité Internacional de Presidentes/as y Rectores/as, así como múltiples Grupos de Trabajo de alcance nacional e internacional. Estos grupos abordan de forma específica temas como ciberseguridad, tecnologías educativas, madurez digital, relación con proveedores y la red de mujeres TIC, promoviendo la compartición de experiencias, buenas prácticas y casos de éxito.

La acelerada evolución tecnológica supone un reto común para todas las universidades. Con independencia de su tamaño o tipología, las IES se enfrentan a crecientes demandas en materia de seguridad digital, que exigen personal especializado, nuevas herramientas, procesos más robustos y marcos de referencia que faciliten la gestión. Ante este panorama, **la cooperación se convierte en un factor decisivo:** establecer alianzas y trabajar de forma conjunta multiplica la capacidad de respuesta y fortalece el ecosistema universitario iberoamericano.



En este sentido, el **Grupo de Trabajo Internacional (GTI) de Ciberseguridad** desempeña un papel fundamental. Su labor no se limita a la protección técnica frente a los ciberataques, sino que aporta una dimensión estratégica al recopilar, documentar y difundir buenas prácticas, estudios y experiencias que resultan de gran valor para las instituciones. Esta cooperación reduce costes, optimiza la operación y, sobre todo, impulsa un cambio cultural que coloca la ciberseguridad en el centro de la agenda universitaria.

El verdadero valor del GTI de Ciberseguridad reside en ser un **espacio de conocimiento compartido** capaz de inspirar y guiar a las IES en el camino hacia entornos más seguros, resilientes y preparados para afrontar los desafíos digitales del presente y del futuro.

Grupo de Trabajo Internacional en Ciberseguridad

Coordinadores y coordinadoras

MetaRed TIC Argentina

Javier Diaz

Universidad Nacional de la Plata
Secretario de Vinculación e Innovación Tecnológica

MetaRed TIC Argentina

Fernando Menzaque

Universidad Nacional de Córdoba
Director de infraestructuras y Servicios

MetaRed TIC Brasil

Domingos Sávio Alcântara Machado

Universidade Tiradentes
Vice-Presidência de Estratégia, Internacionalização e Inovação

MetaRed TIC Centroamérica y el Caribe

José Luis Regalado Menchaca

Universidad Tecnológica Centroamericana
UNITEC Honduras
CIO

1. MetaRed: La importancia de la colaboración en ciberseguridad. Grupo de Trabajo Internacional en Ciberseguridad

Crue Digitalización, España

Francisco José Sampalo Lainz

Universidad Politécnica de Cartagena

Responsable de Seguridad

MetaRed TIC Chile

Álvaro Fuentes Maldonado

Universidad Autónoma de Chile

Director corporativo de tecnologías

MetaRed TIC México

Héctor Bonola

Universidad Veracruzana

Dirección de Servicios de Red e Infraestructura Tecnológica

MetaRed TIC Colombia

Maritza Giraldo Agudelo

Universidad Pontificia Bolivariana

Directora de Infraestructura Tecnológica Multicampus

MetaRed TIC México

Roger Arturo Sunción Campos

Universidad Peruana Cayetano Heredia

Director de TI

MetaRed TIC Perú

Silvana Balarezo

Universidad Peruana de Ciencias Aplicadas

Gerente de Experiencia de Aprendizaje Digital

MetaRed TIC Ecuador

Carlos Gabriel Córdova Erreis

Universidad Técnica Particular de Loja

Gerente TI

MetaRed TIC Portugal

Carla Alexandra Santos

Politécnico de Coimbra

Departamento de Tecnologias de Informação e Comunicação

MetaRed TIC Ecuador

Julia Alexandra Pineda Arévalo

Universidad Técnica Particular de Loja

Coordinadora de Seguridad y Riesgos

MetaRed TIC Portugal

Tiago Pedrosa

Instituto Politécnico de Bragança

Profesor, CISO y Coordinador CSIRT

2.

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.

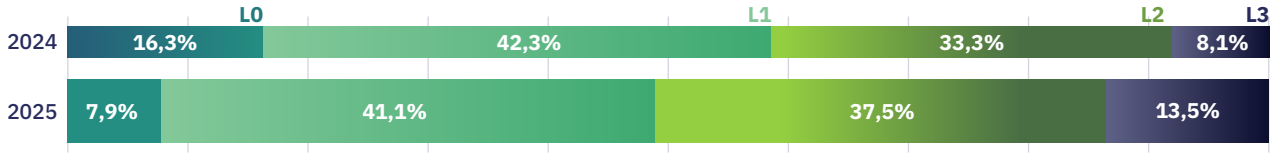
Un ecosistema en plena evolución

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.

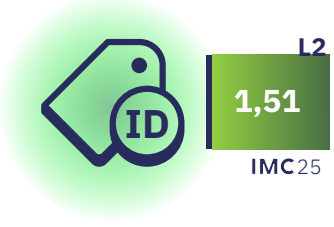
FORTALEZAS CONSOLIDADAS

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

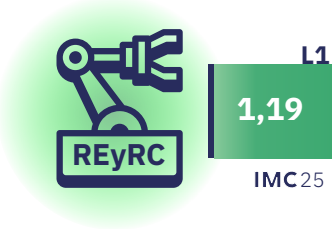


PRINCIPALES DEBILIDADES

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.

3.

IMC: Índice de Madurez en Ciberseguridad

Objetivos

Resultados esperados

Alcance

3.1 Modelo IMC

3.2 Dominios

3.3 Niveles de madurez

3.4 Tipología de la muestra

3. IMC: Índice de Madurez en Ciberseguridad

El IMC 2025, en continuidad con el IMC 2024, constituye un marco general para evaluar el estado actual de la ciberseguridad en universidades IES de Iberoamérica. Al igual que el año anterior, permite obtener una visión detallada y específica del nivel de madurez en ciberseguridad, habilitando la comparación con entidades de similar naturaleza del propio país y de la región.

Como novedad principal, esta edición **posibilita el análisis evolutivo** respecto a 2024 para las instituciones que participaron entonces, de modo que puedan apreciar el **nivel de avance** en la aplicación de prácticas de ciberseguridad. El IMC se concibe como una **herramienta para la toma de decisiones estratégicas y operativas** y para una **mejor asignación de recursos** al desarrollar iniciativas de protección de los activos de información.

Como se señaló en el informe **IMC 2024**, las universidades e IES son depositarias de **información sensible** (datos personales de estudiantes y docentes, investigaciones de vanguardia, propiedad intelectual). Su protección es un asunto **técnico y de responsabilidad social y cumplimiento normativo,** demostrando la capacidad institucional de **gobernar y gestionar** los activos de información y **preservar el valor** que generan.

En un proceso de **transformación digital irreversible,** las IES han redefinido procesos académicos y de gestión. Ello trae aparejados **riesgos asociados a las tecnologías utilizadas,** que deben **evaluarse y mitigarse** para proteger adecuadamente la información.

Si bien existen diversos marcos de evaluación de la madurez en ciberseguridad en múltiples contextos, este estudio **atiende un vacío regional** en el ámbito de la educación superior iberoamericana, **marcando tendencia** y contribuyendo a la mejora de la ciberseguridad en las IES.

El IMC 2025 está dirigido a **autoridades nacionales** vinculadas a las IES, **equipos directivos, responsables TIC y de Seguridad de la Información,** así como **equipos técnicos y académicos** involucrados en iniciativas de ciberseguridad en el ámbito universitario.

Objetivos

- **Estrategia conjunta:** Respaldar los proyectos de MetaRed mediante la definición de un plan de acciones colaborativas globales más preciso, coherente y de alto valor añadido para las instituciones participantes.
- **Diagnóstico del estado actual:** Proporcionar un marco de referencia que permita a las IES evaluar su nivel de madurez en ciberseguridad, identificar brechas y desarrollar estrategias de mejora continua, posibilitando un análisis evolutivo basado en la comparación con los resultados de años anteriores.
- **Guía para la mejora continua:** Ofrecer un análisis detallado de la situación de cada institución en materia de ciberseguridad, destacando fortalezas y áreas de mejora, y facilitando la comparación tanto con su propia evolución como con otras IES a nivel nacional y regional.
- **Fomento de la cultura de la ciberseguridad:** Impulsar la concienciación y comprensión de la ciberseguridad en las comunidades universitarias, promoviendo una cultura preventiva y una respuesta eficaz ante incidentes cibernéticos.

Resultados esperados

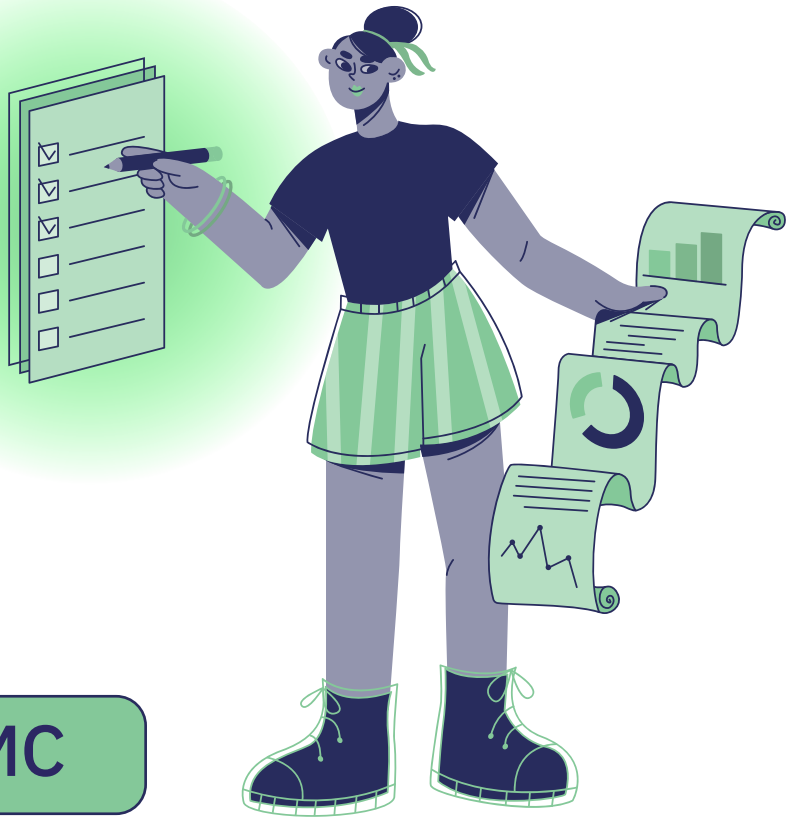
- Conocer el **estado de la ciberseguridad** en las IES de la región iberoamericana integradas en MetaRed.
- Obtener un **panorama comparativo** que les permita medir su nivel de madurez frente a otras instituciones de su país y frente al promedio regional de forma anomizada.
- Analizar su **evolución** respecto a los resultados obtenidos en el IMC 2024, siempre que hayan participado en dicho estudio.
- **Definir e implementar medidas** fundamentadas para fortalecer la ciberseguridad en sus respectivos ámbitos.

Alcance

Este informe presenta los resultados de la aplicación de la encuesta de madurez en ciberseguridad a un grupo de universidades de países de Iberoamérica que participan en forma voluntaria. La información sobre el estado actual de la ciberseguridad en cada institución que forma parte de la medición es proporcionada por personal responsable de las áreas de tecnologías de la información o de las unidades especializadas en ciberseguridad, cuando existen. Si bien esto permite identificar tendencias sólidas y calcular un Índice de Madurez (IMC) comparativo, los datos reflejan la visión interna de las instituciones y no el resultado de auditorías técnicas externas.

> Al tratarse de un muestreo basado en la participación voluntaria dentro de la red MetaRed, utilizando un muestreo no probabilístico, los resultados representan la realidad de las instituciones participantes y marcan tendencias regionales, pero no deben extrapolarse como datos censales de todo el universo de la educación superior.

La aplicación de un conjunto similar de preguntas para evaluar la madurez digital en dos años consecutivos, permite presentar resultados comparados para el total de países participantes de Iberoamérica, siempre que hubieran cumplido la cuota mínima de instituciones participantes.



3.1. Modelo IMC

Con el fin de mantener la coherencia con el estudio de 2024, **el IMC 2025 se basa en la versión 2.0 del Framework de Ciberseguridad del NIST** (Estados Unidos), publicado en febrero de 2024.

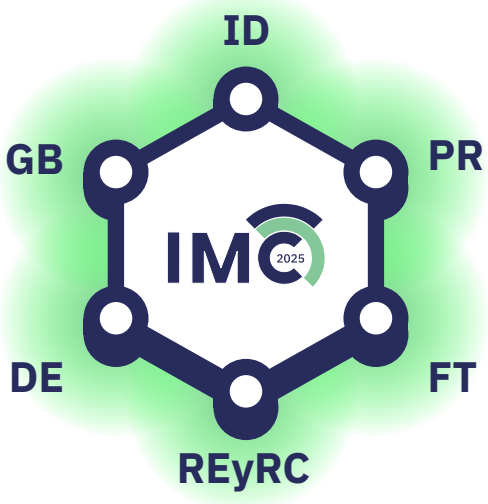
Como en la edición anterior, integra **controles y prácticas** de **ISO/IEC 27001:2022** y **ISO/IEC 27002:2022,** así como del **Esquema Nacional de Seguridad (ENS)** de España, asegurando una **cobertura completa** de los aspectos relevantes de seguridad de la información.

En esta edición se consideran también **aspectos vinculados al uso de herramientas de inteligencia artificial (IA**) y sus **implicancias para la ciberseguridad.** Este **enfoque híbrido y adaptado al contexto** combina estándares internacionales de reconocimiento con nuevas tecnologías, adecuado a la realidad iberoamericana.

En suma, se **continúa la línea** iniciada con el IMC 2024, proporcionando un **marco robusto y efectivo** para evaluar y mejorar la madurez en ciberseguridad de las IES de la región.

3.2. Dominios

Fruto del ciclo de mejora continua sobre el que se basa la evolución del modelo IMC, en esta edición se mantienen los **seis dominios** utilizados en 2024 y se incorporan **indicadores especiales para medir el uso de la IA y su impacto** vinculado a la ciberseguridad, así como se **reformularon y mejoraron** algunas preguntas relativas a la **participación de la mujer** en los grupos de ciberseguridad y a la **definición de incidente.**



Gobernar (GB)

Involucra el **establecimiento, compromiso y monitoreo** de la ciberseguridad por parte de la **dirección.** Es fundamental para integrar la ciberseguridad en el funcionamiento institucional. Incluye la **estrategia de ciberseguridad, la elaboración, mantenimiento y comunicación de políticas, el establecimiento de procesos y procedimientos, la identificación de roles y responsabilidades** y la gestión global de la función de ciberseguridad. Abarca **comprender el contexto, gestionar el riesgo en la cadena de suministro, definir roles, responsabilidades y autoridades, implementar procesos y procedimientos y supervisar** el cumplimiento de los objetivos.

Detectar (DE)

Comprende acciones para **buscar y analizar** posibles **ataques y compromisos.** Facilita el **descubrimiento y análisis oportunos de anomalías, indicadores de compromiso y otros eventos potencialmente adversos** que puedan indicar ataques o incidentes. Incluye monitoreo de red mediante fuentes internas y externas, **configuración de herramientas y análisis de eventos.**

Identificar (ID)

Implica **determinar el riesgo actual** de ciberseguridad. Requiere **conocer activos** (datos, *hardware, software,* sistemas, instalaciones, servicios y personas) y los **riesgos asociados,** para **priorizar mejoras en políticas, procesos, procedimientos y prácticas** que respaldan la gestión de la ciberseguridad. Incluye la **identificación** de dichas políticas, procesos, procedimientos y prácticas.

Responder y recuperar (REyRC)

Responder define cómo **actuar ante un incidente** detectado: **gestión, análisis, mitigación y comunicación** de incidentes y procesos vinculados. **Recuperar** comprende **restaurar activos y operaciones** afectadas, con acciones que **restablezcan oportunamente** la normalidad para **reducir y contener el impacto.** Incluye **planes de contingencia y recuperación y sus procedimientos asociados.**

Proteger (PR)

Se refiere a **implementar controles para mitigar riesgos y proteger activos,** reduciendo la **probabilidad e impacto** de eventos adversos. Incluye **concientización y entrenamiento, seguridad de datos, gestión de identidades, seguridad de la plataforma y resiliencia** de la infraestructura tecnológica.

Formación y talento (FT)

Dominio **complementario** orientado a la **formación en ciberseguridad** y a la **captación y retención de talento** en la institución, acorde con la naturaleza educativa de las IES. **No se utiliza para calcular el nivel de madurez.**

3.3 Niveles de madurez

Se definen, al igual que en el estudio del año pasado, 4 niveles de madurez de acuerdo al estado de implementación de los controles en cada dominio. Cada control, definido en los diferentes dominios, será correlacionado dentro de los niveles de madurez concretados: L0, L1, L2, L3. A continuación se muestran exactamente las características incluidas en cada nivel, manteniendo los criterios del IMC 2024:

L0

0,00 - 0,74

No se realizan prácticas de ciberseguridad.

Conciencia mínima sobre la importancia de la ciberseguridad.

Ausencia de políticas y procedimientos formales.

Uso limitado y no sistemático de tecnologías de seguridad.

Sin personal dedicado específicamente a la ciberseguridad.

Falta de procesos formales de gestión de riesgos.

L1

0,75- 1,49

Se realizan prácticas iniciales, pero pueden ser ad hoc o informales.

Establecimiento de políticas y procedimientos básicos.

Implementación inicial de tecnologías de seguridad.

Personal responsable de la ciberseguridad, aunque no especializado.

Inicio de procesos formales de identificación y evaluación de riesgos.

L2

1,50- 2,24

Las prácticas de ciberseguridad son más completas y avanzadas que en L1. Están documentadas y se proporcionan recursos adecuados para apoyar el proceso.

Políticas y procedimientos bien definidos y documentados.

Implementación avanzada de tecnologías de seguridad, incluyendo sistemas de detección de intrusos y herramientas de cifrado.

Personal de ciberseguridad dedicado y especializado.

Procesos de gestión de riesgos formalizados y regularizados.

L3

2,25 - 3,00

Las prácticas de ciberseguridad son más avanzadas que en L2. Las actividades están guiadas por políticas u otras directivas organizacionales. Se asignan responsabilidades e instancias de rendición de cuentas y de autoridad para realizar las prácticas. El personal que realiza las prácticas tiene habilidades y conocimientos adecuados. Se evalúa y realiza un seguimiento de la eficiencia de las actividades.

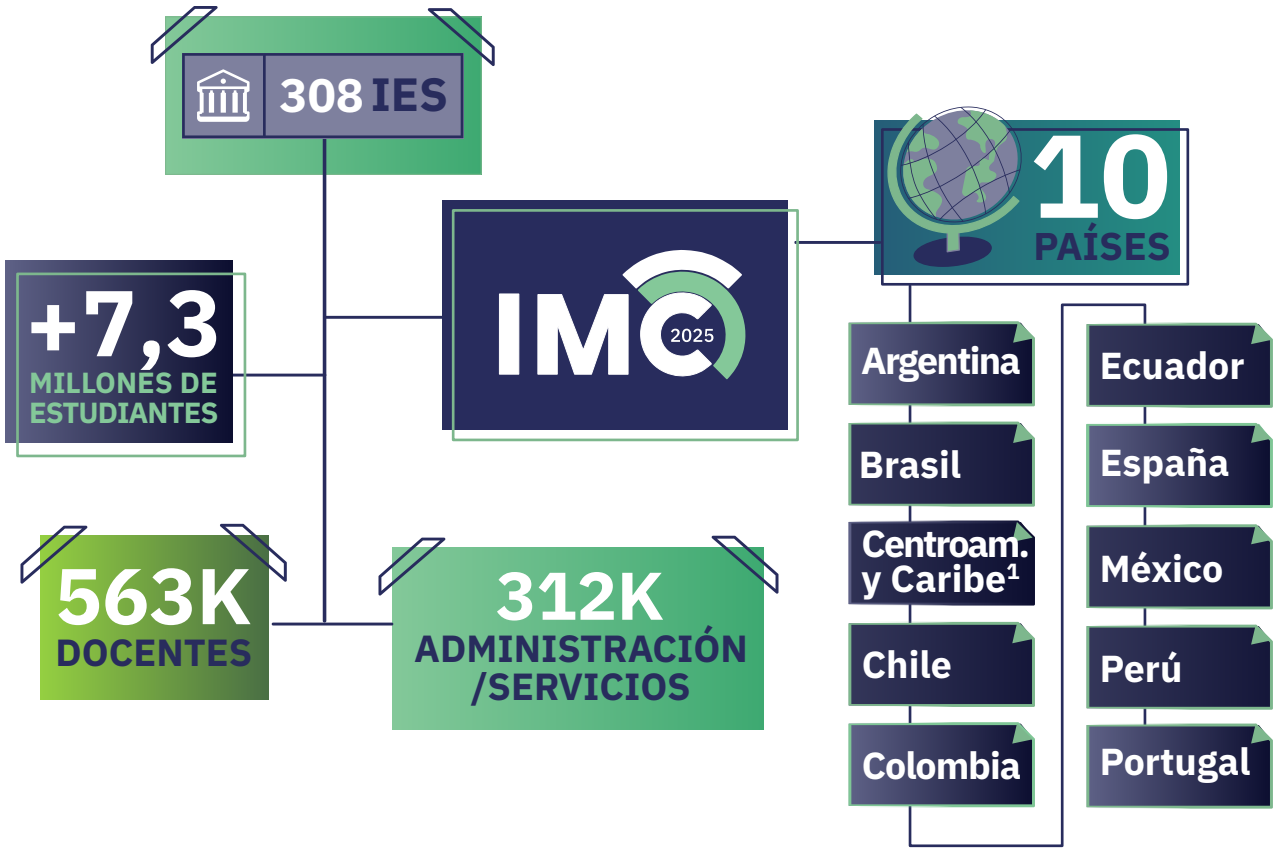
Políticas y procedimientos integrados en todas las operaciones de la institución.

Uso de tecnologías de seguridad de última generación y enfoque proactivo en la mejora continua.

Equipo de ciberseguridad altamente especializado y capacitado.

Gestión de riesgos altamente madura con un enfoque proactivo en identificación y mitigación de amenazas.

3.4 Tipología de la muestra



La mayoría de los países contaron con una participación similar al 2024, con la excepción positiva de Brasil y Perú, donde la participación ha crecido notablemente y ha permitido la creación de informes específicos de estos países.

En valor absoluto, **el número de IES participantes se ha incrementado en 61 instituciones,** un 24,7% más que en la edición de 2024. De las IES participantes en 2024, cerca del 50% ha vuelto a participar en la edición de este año.

1 Centroamérica y Caribe al no contar con el número mínimo de IES necesario para considerar la muestra como representativa de la región no tiene informe específico de país, sin embargo, la participación de sus IES si computa para el promedio iberoamericano y las IES participantes de esta zona podrán consultar sus cuadros de mando, analizar su evolución con respecto a 2024 y comparar con la media iberoamericana.

TIPOLOGÍA DE LAS IES PARTICIPANTES

A nivel global, la muestra obtenida presenta una distribución homogénea entre las instituciones públicas (51%) y privadas (49%), datos que, junto al incremento de participantes, mejoran la muestra con respecto a la edición anterior. Sin embargo, es necesario tratar estos datos con cautela debido a que la distribución cambia en función del país analizado, tal y como se puede apreciar en la siguiente gráfica.

Gráfico 2: Participación tipo de IES públicas vs. privadas.

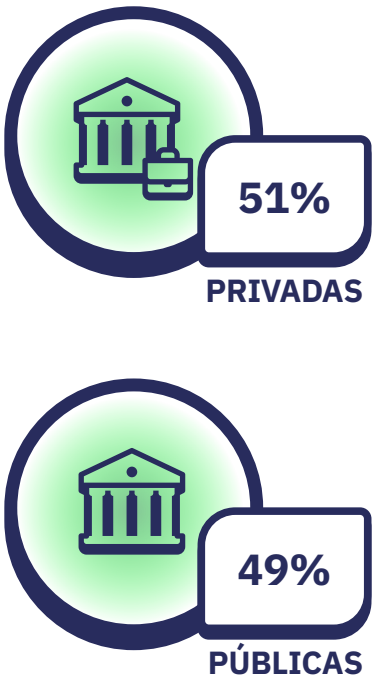
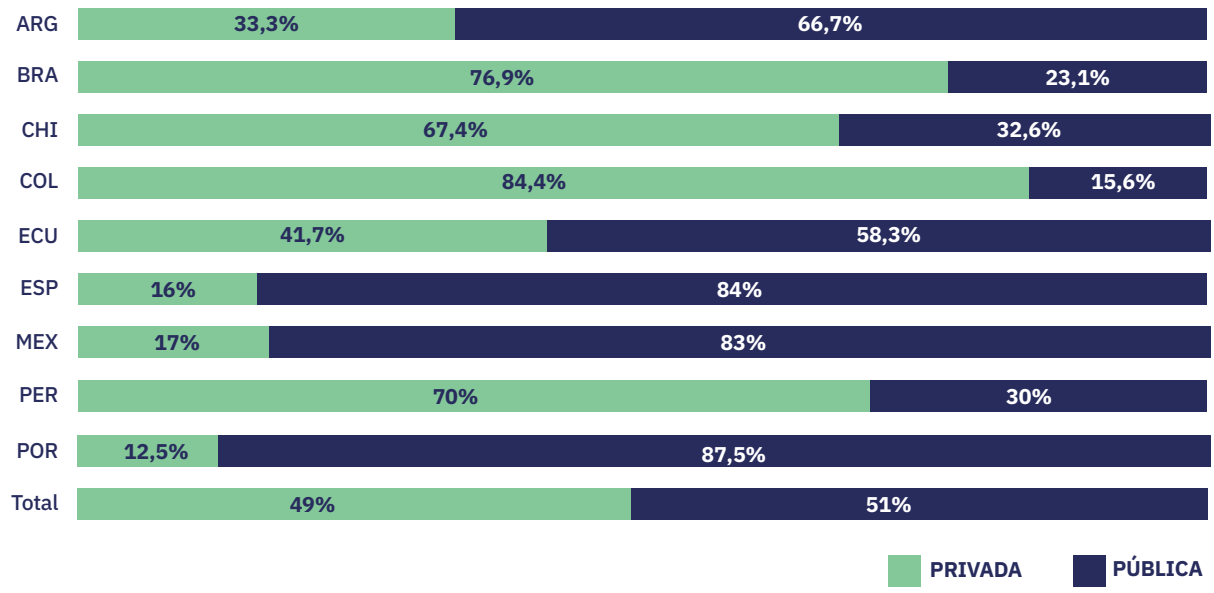
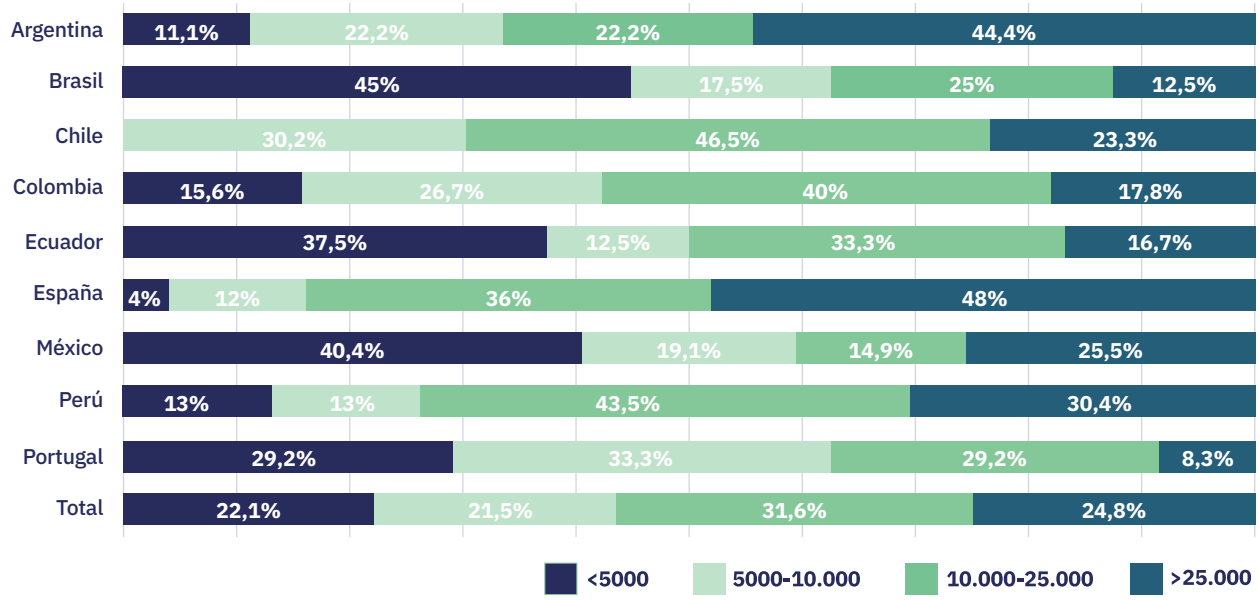


Gráfico 3: Distribución por tipo de IES (global y por país).



Algo similar ocurre con el tamaño de la IES de cada país. Como podemos apreciar en la siguiente gráfica, estamos ante una distribución heterogénea que muestra grandes diferencias en función del país de procedencia. Por ejemplo, España y Argentina cuentan con un porcentaje bajo de instituciones de menos de 5.000 estudiantes, frente a Brasil y México donde ese tipo de instituciones representa cerca de la mitad. Por lo tanto, a lo largo del desarrollo de este informe se tendrán en cuenta estos valores para la realización de un análisis específico que considere estas diferencias nacionales.

Gráfico 4: Distribución por número de estudiantes (global y por país).



Situación similar que ocurre en las IES públicas e IES privadas, donde cada país presenta una distribución diferente.

Gráfico 5: Distribución para las IES públicas por número de estudiantes (global y por país).

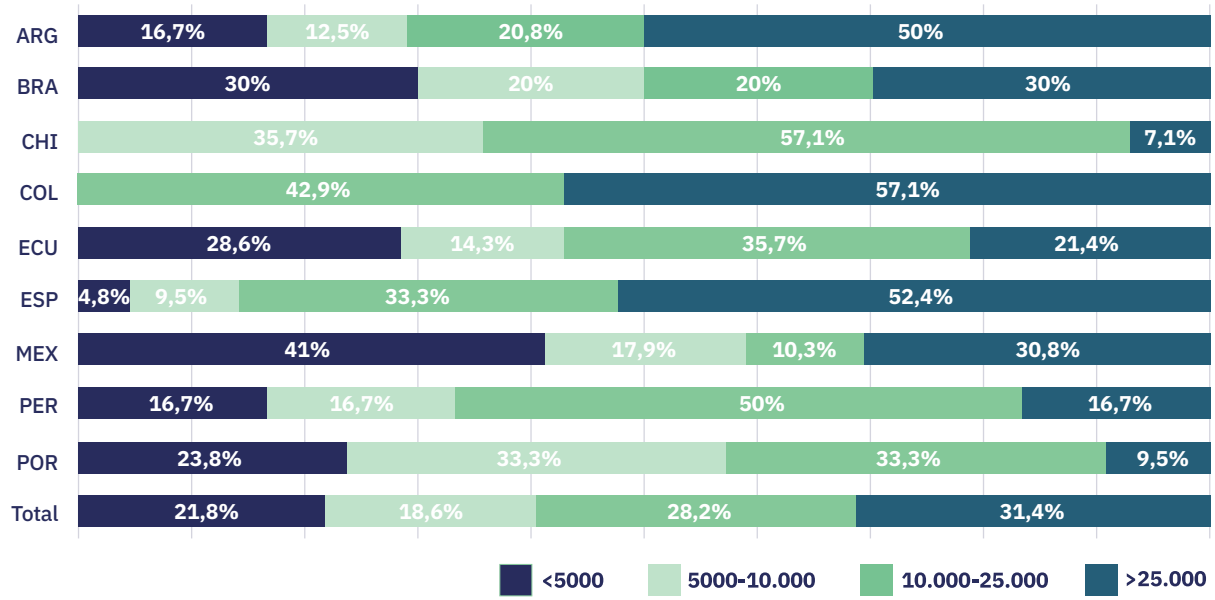
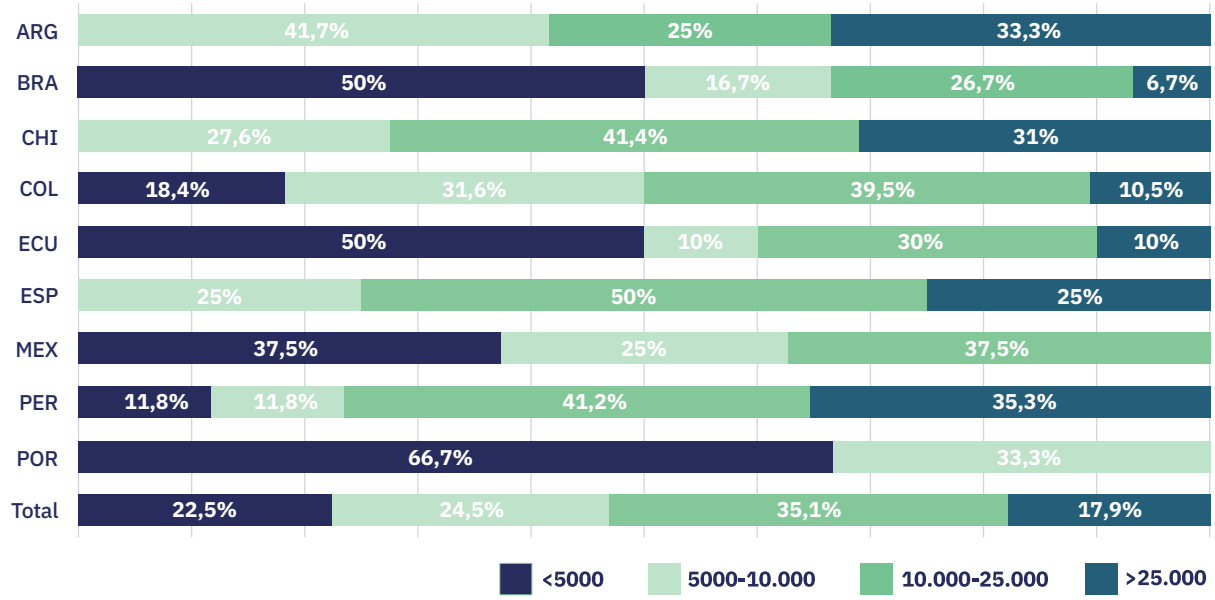


Gráfico 6: Distribución para las IES privadas por número de estudiantes (global y por país).



4.

IMC Iberoamericano

4.1 Evolución/tendencia

4.2 IMC por dominio de aplicación

4.3 Uso de la IA

4.4 Enfoque de las IES en torno a la ciberseguridad

4.5 IMC Iberoamericano por país

4.6 IMC Iberoamericano por tipo de institución

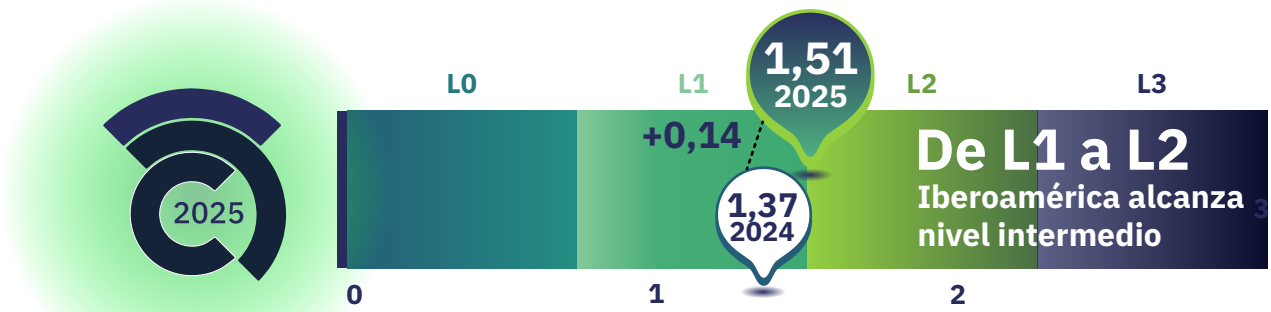
4.7 IMC Iberoamericano por tamaño

4.8 IMC según presupuesto asignado a ciberseguridad

4.9 Ciberincidentes en Iberoamérica

4.10 IMC Iberoamericano según la gestión interna de la ciberseguridad

4.1 Evolución/tendencia



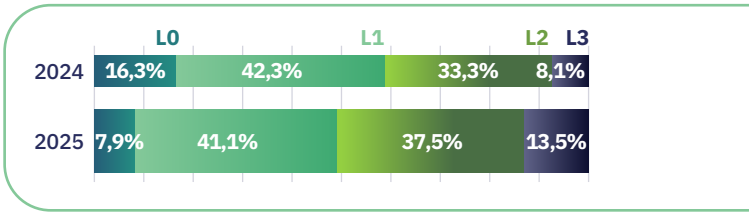
El IMC Iberoamericano sube de 1,37 a 1,51 y pasa del nivel básico (L1) al intermedio (L2).

El **IMC Iberoamericano global 2025**, calculado a partir del promedio de las **308 instituciones de educación superior (IES)** participantes de **9 países de la región,** alcanza un valor de **1,51.** Este resultado representa un **avance respecto al 1,37 obtenido en 2024,** lo que marca el paso **del nivel básico de madurez (L1) al nivel intermedio (L2)** dentro de la escala de cuatro niveles definidos (L0, L1, L2 y L3).

El progreso refleja un **esfuerzo colectivo de las IES iberoamericanas por fortalecer sus capacidades de ciberseguridad**, al tiempo que evidencia la importancia de continuar trabajando de manera coordinada para consolidar prácticas más maduras y avanzar hacia el nivel avanzado (L3).

Del total de instituciones participantes, **más de la mitad (51%)** se sitúan ya en el nivel **intermedio (L2) o avanzado (L3),** mientras que el **41,2%** permanece en el nivel **básico (L1)** y solo un **7,8%** —equivalente a **24 IES**— en el nivel **inicial (L0)**

Gráfico 7: Distribución de IES por nivel. IMC24 vs IMC25.



LAS CLAVES

La región en su conjunto ha pasado del nivel básico (L1) al intermedio (L2) en 2025, consolidando una tendencia de mejora en ciberseguridad.

Identificar (ID) y Detectar (DE) son los dominios que más crecen, lo que indica una atención creciente tanto a los controles técnicos como a la gestión de riesgos.

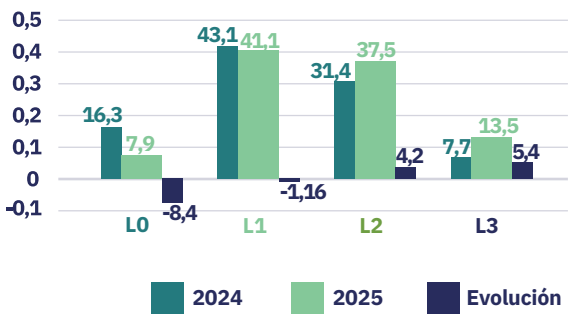
Gobernar (GB) y Proteger (PR) avanzan, aunque de forma más moderada, y aún requieren mayor impulso desde la alta dirección institucional.

Responder y Recuperar (REyRC) se mantiene como la principal tarea pendiente: sin mejorar la capacidad de respuesta, la resiliencia global de las IES seguirá limitada.

Si analizamos la gráfica de evolución de la distribución por niveles de madurez, vemos una clara **tendencia alcista.** En concreto, se reducen un 8,4% las IES en nivel inicial (L0), un 1,2% aquellas que estaban en nivel básico (L1) y, por contraparte, se incrementa un 4,2% las que están en nivel intermedio (L2) y un 5,4% las que consiguen situarse en nivel avanzado (L3).

En términos generales, el resultado de 2025 refleja el uso más extendido de prácticas avanzadas, la definición y documentación de políticas y procedimientos, y la asignación de recursos adecuados para respaldar los procesos. Asimismo, se observa que muchas de las tecnologías de seguridad aplicadas por las IES de la región se encuentran en un grado avanzado de implementación, que los equipos de ciberseguridad cuentan con personal especializado y dedicado, y que los procesos de gestión de riesgos están cada vez más formalizados. Todo ello, con la salvedad de la variabilidad natural entre instituciones, que aporta una visión matizada de la situación regional.

Gráfico 8: Evolución de la distribución por niveles de madurez (2024 vs. 2025, evolución).



4.2 IMC por dominio de aplicación

El análisis del **IMC Iberoamericano 2025 por dominios de aplicación confirma una evolución positiva** en comparación con la edición de 2024. En términos generales, la región ha pasado de un nivel básico (L1) en gran parte de sus dominios y subdominios a un **nivel intermedio (L2)** en gran parte de estos valores.

Gráfico 9: Radar IMC por dominio. IMC24 vs. IMC25.

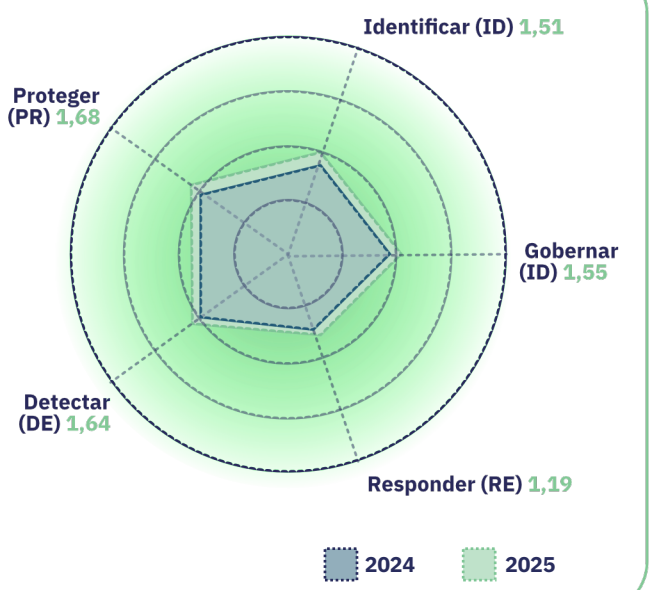


Gráfico 10: IMC por dominios y subdominios de aplicación.IMC24 vs. IMC25.

	IMC24	IMC25
IMC IBE 2025	L1	L2
GB0 Gobernar	L1	L2
GB1 Estrategia	L2	L2
GB2 Política	L2	L2
GB3 Normativa	L1	L2
GB4 Procedimientos	L1	L1
GB5 Responsabilidad	L1	L1
GB6 Presupuesto	L1	L1
ID0 Identificar	L1	L2
ID1 Inventario Activos	L1	L2
ID2 Análisis Riesgos	L1	L1
ID3 Análisis Impacto	L1	L2
PR0 Proteger	L2	L2
PR1 Accesos	L1	L1
PR2 Personal	L1	L1
PR3 Infraestructura	L3	L3
PR4 Equipos	L1	L1
PR5 Comunicaciones	L2	L2
PR6 Servicios	L2	L2
PR7 Información	L2	L2
PR8 Continuidad	L1	L1
PR9 Externos	L2	L2
DE0 Detectar	L1	L2
DE1 Intrusiones	L2	L2
DE2 Vigilancia	L1	L2
DE3 Actividad Usuarios	L2	L2
DE4 Anomalías	L1	L2
RE0 Responder	L1	L1
RE1 Gestión Incidentes	L1	L1
RE2 Mitigación	L1	L1
RE3 Recuperación	L1	L1

Identificar (ID) +0,19, Detectar (DE), +0,17 y Gobernar (GB), +0,12, lideran el fortalecimiento hacia el nivel intermedio (L2).

El dominio Gobernar avanza de 1,43 en 2024 a 1,55 en 2025 (+0,12), consolidando poco a poco su papel estratégico en las instituciones de educación superior de la región. Este crecimiento se apoya, sobre todo, en la mejora de los subdominios de Estrategia (1,64 → 1,79) y Política (1,72 → 1,83), lo que refleja un proceso de formalización más claro y coherente de las líneas de acción en materia de ciberseguridad. Asimismo, se observan incrementos en los ámbitos de Normativa y Procedimientos, lo que indica que las prácticas de seguridad empiezan a institucionalizarse con mayor firmeza y a integrarse en la cultura organizacional.

A pesar de estos avances, el dominio aún evidencia debilidades importantes en lo relativo a la Responsabilidad (1,28 → 1,43) y al Presupuesto (1,09 → 1,17), donde los progresos son apenas incipientes. Esto sugiere que, si bien la gobernanza de la ciberseguridad está mejor definida en términos estratégicos, todavía falta consolidar estructuras de responsabilidad claras y asignar recursos específicos que garanticen la sostenibilidad de las acciones emprendidas.

Por su parte, el dominio Identificar es el que muestra el salto más notable en esta edición, al pasar de 1,32 en 2024 a 1,51 en 2025 (+0,19), lo que implica una transición del nivel básico (L1) al nivel intermedio (L2). Este progreso responde principalmente a las mejoras en el Inventario de Activos (1,49 → 1,59) y en el Análisis de Impacto (1,10 → 1,51), dos aspectos clave para que las instituciones conozcan con mayor precisión sus recursos críticos y comprendan mejor las consecuencias que podrían derivarse de un incidente de seguridad.

Por otro lado, aunque el Análisis de Riesgos también progresa (1,36 → 1,44), aún se mantiene en un nivel moderado. Esto evidencia que la gestión preventiva de riesgos, si bien más extendida que en 2024, todavía no se realiza de manera plenamente sistemática en muchas instituciones, dejando un margen importante para reforzar la madurez de este dominio.

El dominio Proteger se mantiene como el más sólido en términos absolutos, con un avance de 1,54 a 1,68 (+0,14). Este resultado confirma que la protección técnica sigue siendo la principal prioridad para las IES iberoamericanas. Entre los subdominios, destacan los buenos resultados en Infraestructura (2,39 → 2,52) y Comunicaciones (2,10 → 2,11), que alcanzan niveles propios del nivel avanzado (L3) y demuestran un esfuerzo considerable en asegurar la capa tecnológica crítica de las instituciones.

Sin embargo, la situación es diferente en los subdominios de Personal (1,07 → 1,23) y Equipos (1,33 → 1,41), que se mantienen rezagados. Esto revela que, aunque las capacidades técnicas han crecido, los aspectos vinculados al factor humano y a la gestión de los recursos materiales continúan siendo puntos débiles que pueden comprometer la efectividad global de las estrategias de protección. En síntesis, la protección técnica progresa, pero aún es necesario reforzar el componente humano y operativo.

El dominio Detectar mejora de 1,47 en 2024 a 1,64 en 2025 (+0,17), lo que refleja un fortalecimiento en la capacidad de monitoreo y detección de anomalías dentro de las instituciones. Este avance se aprecia especialmente en los subdominios de Intrusiones (1,58 → 1,69) y Actividad de Usuarios (1,49 → 1,70), que evidencian una mayor atención a la vigilancia de sistemas y comportamientos anómalos que puedan anticipar un incidente de seguridad.

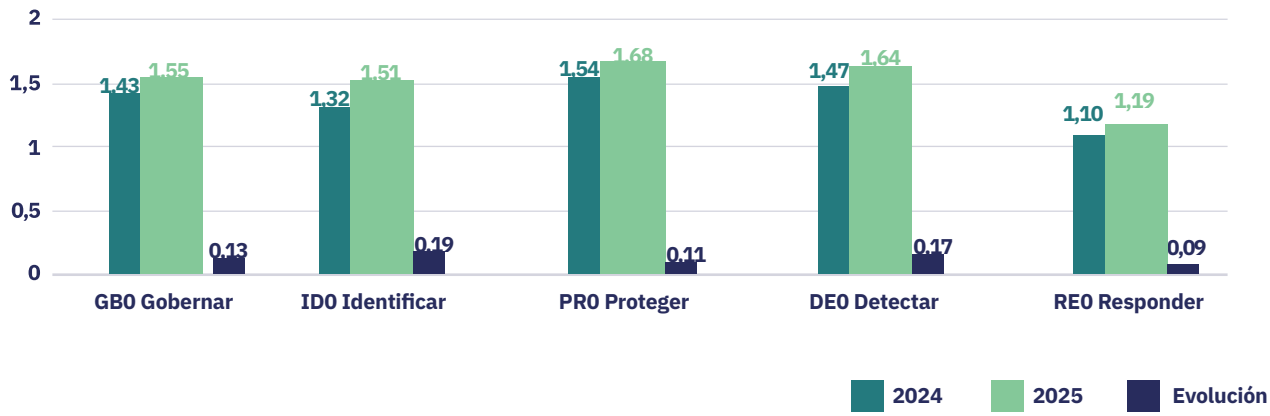
También el subdominio de Anomalías crece, aunque de manera más moderada (1,57 → 1,58), mostrando un desarrollo aún limitado en comparación con otros apartados. El principal desafío sigue siendo la Vigilancia (1,33 → 1,58), que, pese a mejorar, continúa en niveles bajos respecto a los demás. Esto indica que, aunque se avanza en la detección de incidentes, todavía no se alcanza un grado suficiente de madurez para considerar este dominio como plenamente robusto.

El dominio Responder y Recuperar muestra únicamente una mejora ligera, pasando de 1,10 en 2024 a 1,19 en 2025 (+0,09), lo que lo mantiene en el nivel básico (L1). Este resultado confirma que, si bien la región avanza en prevención y monitoreo, aún existe una marcada debilidad cuando se trata de enfrentar incidentes de seguridad y restablecer la normalidad operativa.

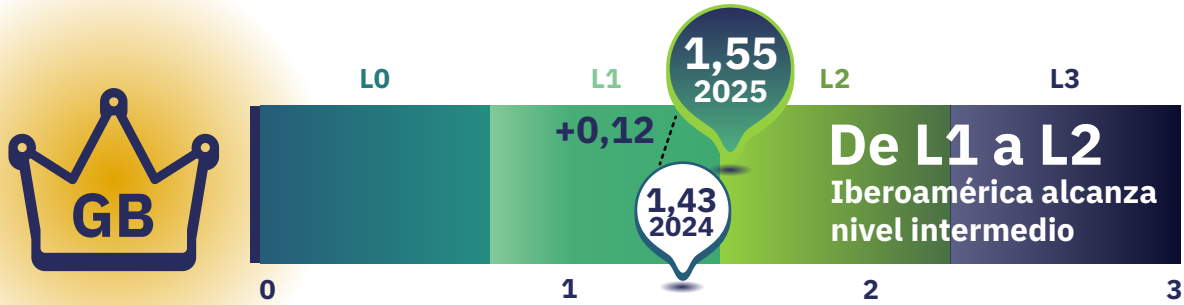
El subdominio más rezagado continúa siendo la Gestión de Incidentes (1,16 → 1,32), con un progreso casi imperceptible. Mitigación (1,10 → 1,13) y Recuperación (1,10 → 1,11) muestran mejoras algo más visibles, pero aún insuficientes para superar el umbral del nivel básico. En conjunto, los resultados de este dominio reafirman que la capacidad de respuesta es la principal tarea pendiente para las IES iberoamericanas: aunque se han reforzado los mecanismos de protección, identificación y monitoreo, las instituciones todavía no cuentan con procesos consolidados para reaccionar de forma eficaz y recuperarse rápidamente ante un ataque.

El siguiente gráfico resume la evolución de los valores entre 2024 y 2025, destacando las mejoras registradas en cada dominio:

Gráfico 11: IMC por dominio (2024, 2025, evolución).



4.2.1 GOBERNAR



El dominio **Gobernar (GB)** alcanza en el **IMC 2025** un nivel de madurez intermedio **(L2)** con un valor de **1,55,** ligeramente superior al registrado en 2024 **(1,43).** Este incremento, aunque moderado, refleja un fortalecimiento de las prácticas de gobernanza institucional en materia de ciberseguridad, con avances especialmente visibles en los subdominios estratégicos y normativos.

Los resultados confirman una evolución positiva en la definición de los marcos que orientan la ciberseguridad en las IES iberoamericanas. Tanto **Estrategia (1,79)** como **Política (1,83)** se consolidan en nivel intermedio **(L2),** evidenciando la existencia de planes institucionales más estructurados, alineados con los objetivos de transformación digital y las exigencias regulatorias.

Uno de los progresos más relevantes se observa en el subdominio **Normativa,** que pasa de **L1 (1,48)** en 2024 a **L2 (1,72)** en 2025. Este salto refleja una mayor formalización de marcos normativos específicos de ciberseguridad, así como una integración más clara de estos en las políticas generales de gestión de la información.

En los subdominios más operativos, como **Procedimientos (1,39), Roles (1,43) y Presupuesto (1,17),** se mantiene el nivel básico **(L1),** aunque todos presentan mejoras respecto al año anterior (1,34; 1,28 y 1,09,

Crece la madurez en gobernanza de la ciberseguridad en las IES iberoamericanas, destacando avances normativos y estratégicos pero con retos operativos y presupuestarios pendientes.

respectivamente). Esto indica que las universidades están avanzando gradualmente en la definición de responsabilidades y en la incorporación de procesos de gestión, pero aún enfrentan limitaciones en la asignación de recursos específicos y en la consolidación de estructuras estables de gobernanza.

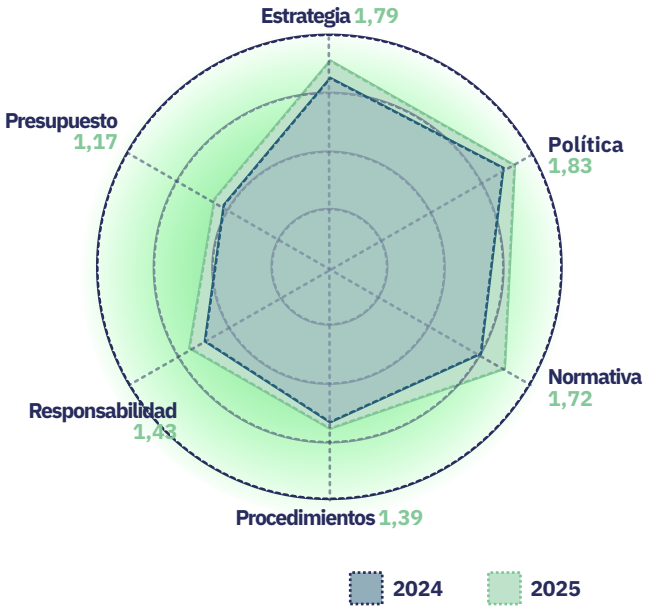
El valor de **1,55** posiciona a **Gobernar (GB)** por encima del **IMC global (1,51)** y lo sitúa como el **tercer dominio mejor valorado,** detrás de **Proteger (PR)** (1,68) y **Detectar (DE)** (1,64). Este comportamiento confirma que las IES iberoamericanas han fortalecido su capacidad de planificación y dirección en ciberseguridad, aunque todavía existe una brecha importante entre el desarrollo estratégico-normativo y la operatividad de los mecanismos de ejecución y control.

El gráfico 12 resume los resultados por subdominio, permitiendo visualizar la evolución experimentada entre 2024 y 2025, mientras que el gráfico 13 ilustra la distribución de los valores promedio y su nivel de consolidación dentro del dominio.

Gráfico 12 Niveles de madurez y valores promedio de los subdominios de Gobernar (GB). IMC24 vs. IMC25.

	IMC24	IMC25
GB1 Estrategia	L2 1,74	L2 1,79
GB2 Política	L2 1,72	L2 1,83
GB3 Normativa	L11,48	L2 1,72
GB4 Procedimientos	L1 1,34	L1 1,39
GB5 Roles	L1 1,28	L1 1,43
GB6 Presupuesto	L1 1,09	L1 1,17

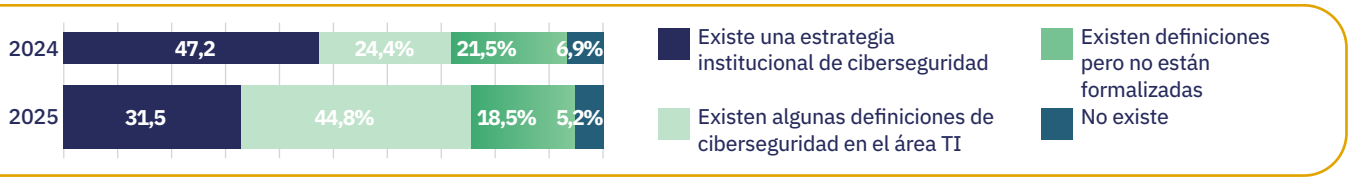
Gráfico 13: Radar subdominios Gobernar (GB). IMC24 vs. IMC25.



SUBDOMINIO: ESTRATEGIA

En cuanto a la **estrategia institucional de ciberseguridad,** el **31,5%** de las IES declara haber desarrollado una estrategia específica, mientras que un **44,8%** cuenta con **definiciones formalizadas dentro del área de TI.** Además, un **18,5%** dispone de **definiciones no formalizadas** y solo un **5,2%** no ha establecido lineamientos claros en esta materia.

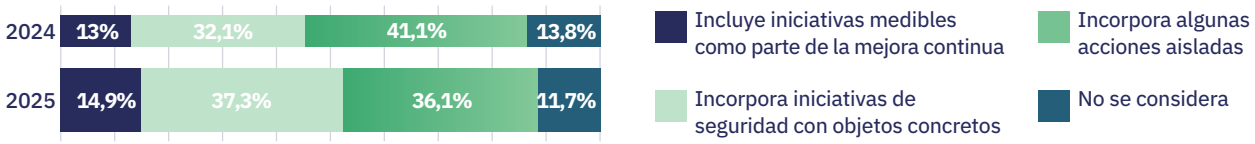
Gráfico 14: Existencia de estrategia de seguridad en las IES. IMC24 vs. IMC25.



Al comparar estos resultados con los del **IMC 2024**, se observa una **mejora sustancial.** El porcentaje de instituciones con algún tipo de estrategia formal —ya sea institucional o dependiente del área de TI— se ha incrementado **del 50% al 75%,** mientras que las IES con definiciones informales se reducen al **18%,** y las que carecen totalmente de ellas al **5%.** Estos avances evidencian un **progreso sostenido en la planificación estratégica** de la ciberseguridad dentro de las universidades e institutos iberoamericanos.

Tal como se señalaba en el informe anterior, el componente **Estrategia** es un indicador directo del **grado de compromiso de la dirección institucional** con la ciberseguridad, al reconocerla como una **dimensión transversal** y no exclusivamente tecnológica. En el **IMC 2025,** este compromiso se consolida, mostrando que un número creciente de instituciones incorpora la ciberseguridad dentro de sus **planes estratégicos institucionales** y le asigna un papel clave dentro de su modelo de gobernanza digital.

Gráfico 15: Consideración de la ciberseguridad en la estrategia institucional. IMC24 vs. IMC25.



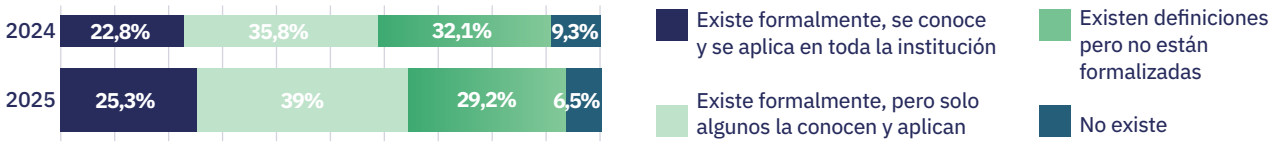
Los datos del estudio refuerzan esta tendencia: el **88,3%** de las IES incluye referencias a la ciberseguridad en sus **estrategias institucionales,** y dentro de este grupo, un **14,9%** contempla **iniciativas medibles** como parte de sus procesos de mejora continua, mientras que un **37,3%** incorpora **objetivos específicos** de ciberseguridad. En conjunto, estos porcentajes superan ampliamente los valores del año anterior (45%), lo que confirma que la ciberseguridad ha pasado de ser un elemento técnico a convertirse en un **eje estratégico y estructural** dentro de la gestión universitaria iberoamericana.

SUBDOMINIO: POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Este subdominio, considerado la **base de la gestión de la protección de la información** en cualquier organización, evalúa la existencia y el grado de desarrollo de políticas institucionales de seguridad. Las respuestas promediadas arrojan un valor de **1,83,** correspondiente a un **nivel de madurez intermedio (L2),** ligeramente superior al obtenido en 2024 **(1,72).** Aunque la diferencia es moderada, este incremento refleja una **mejora sostenida en la formalización y aplicación de políticas de seguridad de la información** dentro de las instituciones de educación superior.

Los datos de 2025 muestran que la **gran mayoría de las IES (93,5%)** cuenta con **iniciativas relacionadas con el desarrollo e implementación de políticas de seguridad.** De este grupo, un **25,3% ha completado el proceso de definición, difusión y aplicación institucional,** integrando la política en toda la organización. Un **39%** dispone de una **política formalmente definida, aunque su aplicación se limita a determinadas áreas** o grupos dentro de la institución.

Gráfico 16: Existencia de Políticas de Seguridad de la Información en las IES. IMC24 vs. IMC25.



Comparando con los resultados del **IMC 2024,** se observa un **incremento de aproximadamente tres puntos porcentuales** en las instituciones con políticas formales y aplicadas, acompañado de una **reducción equivalente en aquellas que sólo cuentan con definiciones informales (29,2%)** o que **aún carecen de un documento formal (6,5%),** frente al **9,3%** registrado el año anterior.

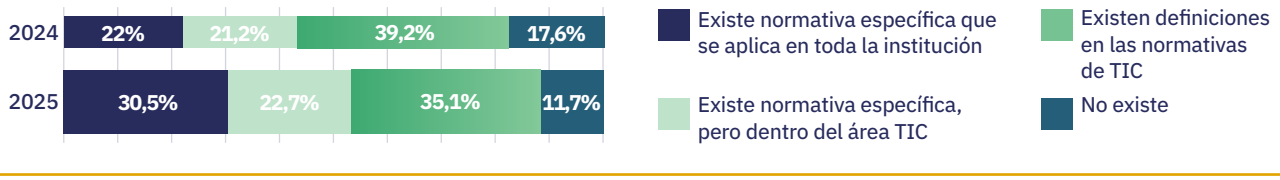
Estos resultados confirman una tendencia positiva hacia la **institucionalización de la seguridad de la información,** consolidando la existencia de políticas formales como **instrumento central de la gestión y el control de la ciberseguridad** en las universidades iberoamericanas.

SUBDOMINIO: NORMATIVA SOBRE CIBERSEGURIDAD

El subdominio **Normativa sobre Ciberseguridad** alcanza en el **IMC 2025** un valor promedio de **1,72,** correspondiente a un **nivel de madurez intermedio (L2).** Este resultado representa un avance respecto al estudio anterior **(1,48 en 2024)** y refleja un **mayor grado de formalización y documentación** de las normas que regulan la ciberseguridad en las instituciones de educación superior iberoamericanas.

En esta edición, un **30,5%** de las IES declara contar con una **norma específica de ciberseguridad aplicable a toda la institución,** lo que demuestra un esfuerzo creciente por establecer marcos normativos transversales. El grupo más numeroso, un **35,1%,** indica disponer de **definiciones normativas dentro del área de TIC,** mientras que un **22,7%** afirma contar con **normativas específicas aplicadas a dicha área.** Por su parte, un **11,7%** de las universidades **aún no dispone de ninguna normativa de ciberseguridad formalmente establecida,** reduciendo el porcentaje de ausencia normativa observado en 2024.

Gráfico 17: Existencia de Normativa de Seguridad de la Información en las IES. IMC24 vs. IMC25.



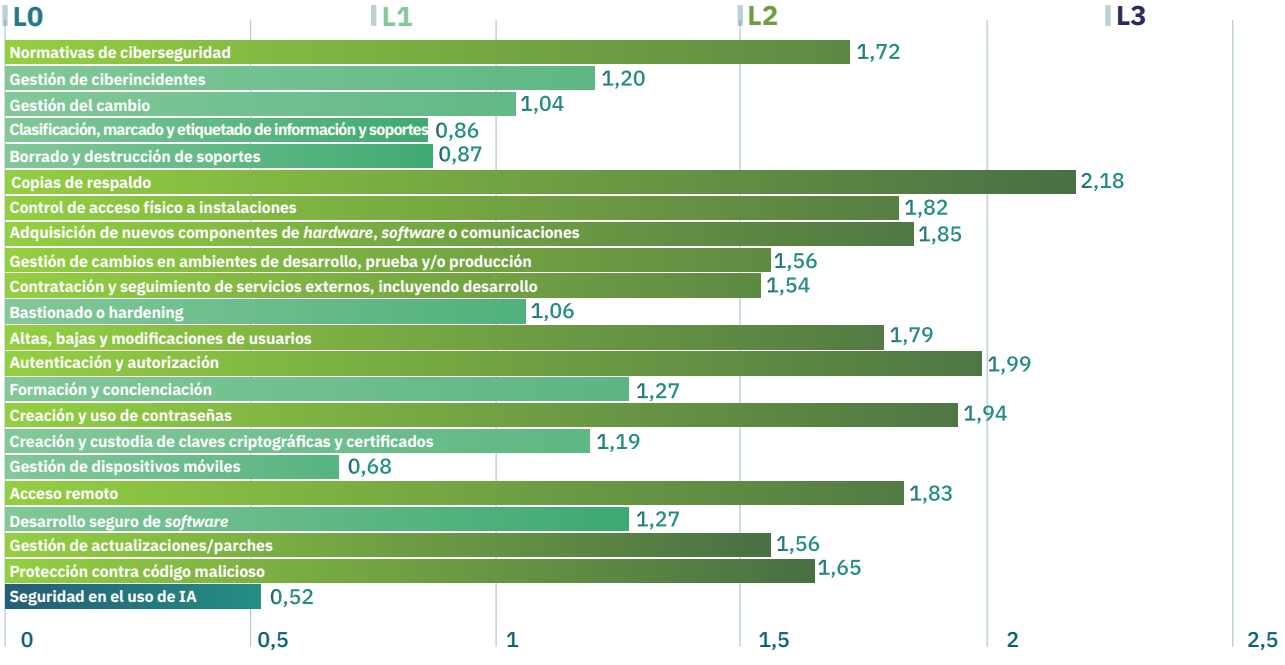
En conjunto, estos resultados confirman un **proceso de consolidación normativa** dentro del ámbito universitario iberoamericano, donde la ciberseguridad comienza a integrarse de manera explícita en los marcos regulatorios institucionales. Este avance contribuye a fortalecer la **coherencia y sostenibilidad de las políticas de seguridad** y a sentar las bases para una gestión más sistemática de los riesgos tecnológicos.

SUBDOMINIO: PROCEDIMIENTOS

Respecto a los procedimientos de seguridad elaborados por las IES que participaron este año, los datos obtenidos muestran que en promedio, la madurez obtenida es la correspondiente a un nivel básico L1 (1,39), con un valor que se encuentra en el mismo nivel de madurez pero solo 0,05 puntos por arriba del obtenido el año pasado (1,34).

Al observar cada procedimiento en particular, se concluye que todos mostraron algún crecimiento. Como el año pasado, los procedimientos que alcanzaron un nivel intermedio L2 son los relativos a copias de respaldo (2,18); control de acceso físico a instalaciones (1,82); adquisición de nuevos componentes de *hardware, software* o comunicaciones (1,85); alta, bajas y modificaciones de usuarios (1,79); autenticación y autorización (1,99); creación y uso de contraseñas (1,94); acceso remoto (1,83) y Gestión de actualizaciones/parches (1,56). Este año también alcanzan ese nivel los procedimientos de gestión de cambios en ambientes de desarrollo, prueba y/o producción (1,56) y contratación y seguimiento de servicios externos (1,54). El resto permanece en un nivel básico L1, con la excepción del procedimiento de gestión de dispositivos móviles que se mantiene en el nivel inicial L0 con un valor promedio de 0,68 .

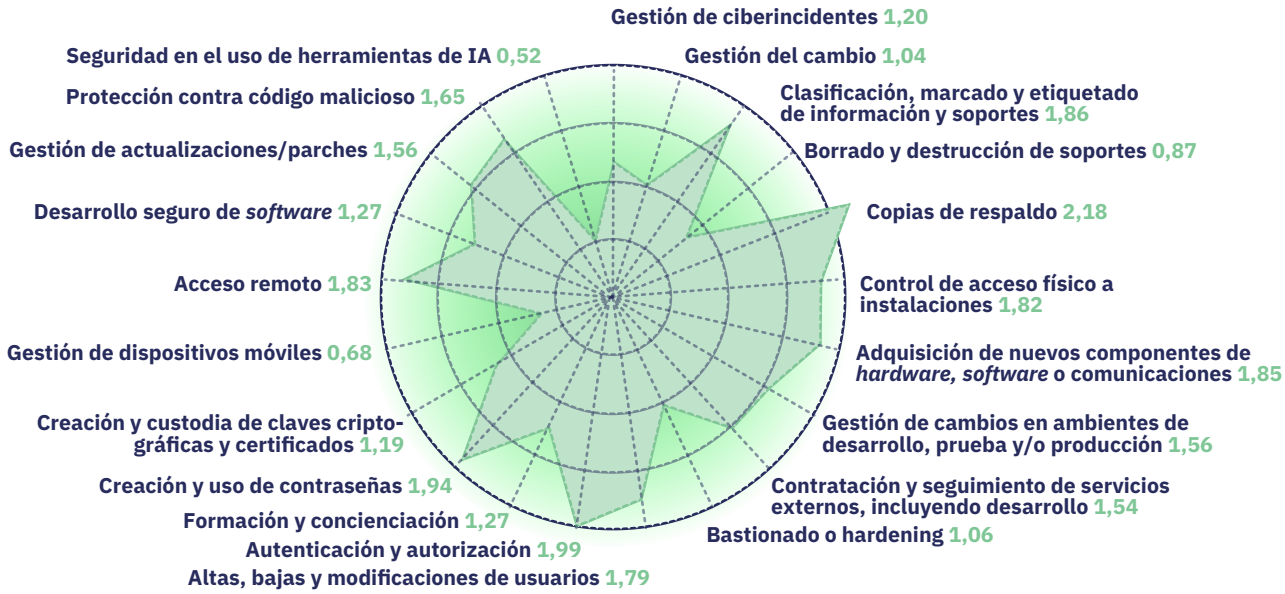
Gráfico 18: Valores alcanzados por los procedimientos en el IMC 2025.



Cabe acotar que el procedimiento de Seguridad en el uso de herramientas de Inteligencia Artificial, agregado para el estudio de este año, muestra un valor promedio de 0,52 correspondiente a un nivel de madurez inicial. El 67,5% de las IES manifestó no contar con un procedimiento definido lo que habilita una implementación *ad-hoc* y sólo algo menos del 5% (4,9%) indica haber formalizado un procedimiento que aplica y monitorea de forma regular.

El siguiente gráfico expone el nivel de madurez de cada uno de los procedimientos relevados este año:

Gráfico 19: Nivel de madurez de todos los componentes del dominio Gobernar IMC 2025.



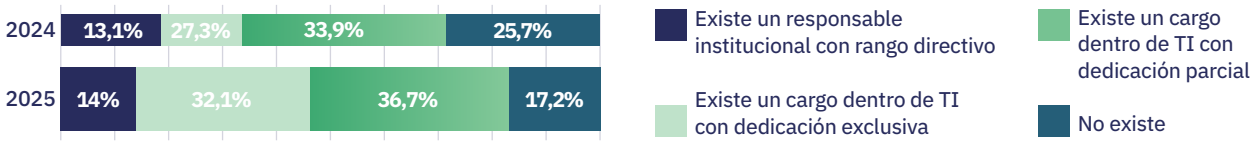
SUBDOMINIO: RESPONSABILIDAD

El subdominio **Responsabilidad** alcanza en el **IMC 2025** un **nivel básico (L1**) con un valor promedio de **1,43,** situándose **muy próximo al nivel intermedio (L2).** Este resultado representa una **mejora respecto al valor obtenido en 2024 (1,28),** manteniéndose dentro del mismo nivel de madurez pero con un progreso sostenido en la consolidación de estructuras de responsabilidad institucional.

Los datos muestran que el **82,8% de las IES cuenta con un responsable institucional de ciberseguridad,** lo que confirma una tendencia positiva frente al estudio anterior. Entre ellas, un **14%** indica que el **responsable tiene rango directivo,** lo que refleja un creciente involucramiento de los niveles ejecutivos en la gestión de la seguridad. Además, un **32,1%** cuenta con un **responsable de dedicación exclusiva dentro del área de TI,** mientras que el **36,7%** lo tiene con **dedicación parcial.**

Por otro lado, el **17,2% de las instituciones aún no dispone de una persona responsable de ciberseguridad,** una proporción que, aunque menor que en 2024, continúa representando un **riesgo crítico.** La ausencia de un referente institucional designado implica **carencias en la gobernanza, la toma de decisiones y la gestión de incidentes**, lo que puede comprometer la capacidad de respuesta ante amenazas y vulnerabilidades.

Gráfico 20: Existencia de un cargo responsable de la ciberseguridad. IMC24 vs. IMC25.



En conjunto, los resultados evidencian un **avance progresivo en la asignación formal de responsabilidades,** pero también subrayan la necesidad de fortalecer la **estructura de liderazgo y supervisión en ciberseguridad** dentro de las IES iberoamericanas.

SUBDOMINIO: PRESUPUESTO

El subdominio **Presupuesto** mantiene en el **IMC 2025** un **nivel básico (L1)** con un valor promedio de **1,17,** 8 puntos por encima del valor obtenido en 2024 (1,09). Continúa siendo el **aspecto con menor madurez dentro del dominio Gobernar (GB),** lo que evidencia que la **asignación de recursos financieros** sigue siendo uno de los principales retos para las IES iberoamericanas en materia de ciberseguridad.

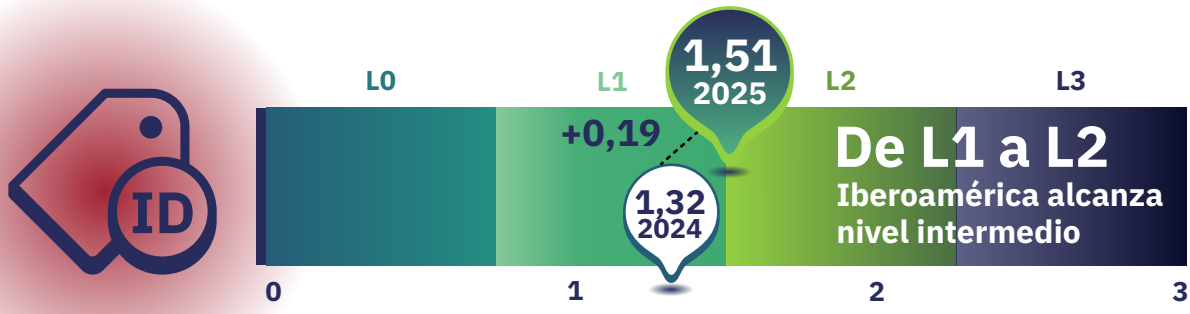
Los datos muestran que el **66,6%** de las universidades destina **fondos a iniciativas de ciberseguridad,** una proporción prácticamente idéntica a la registrada en el **IMC 2024 (65,5%).** Dentro de este grupo, un **5,5%** declara contar con un **presupuesto de ciberseguridad diferenciado del de TI** —ligeramente superior al **4,1%** del año anterior—, mientras que un **39,7%** dispone de **asignaciones específicas dentro del presupuesto de TI** y un **21,4%** las incluye **dentro de las partidas generales.**

Gráfico 21: Existencia de un presupuesto para ciberseguridad. IMC24 vs. IMC25.

Estos resultados indican un **avance en la madurez presupuestaria,** ya que crece la proporción de instituciones que incorporan **partidas específicas de TI** en detrimento de aquellas que dependen de **asignaciones generales,** aunque el **volumen total de inversión solo aumenta alrededor de un 1%.** Por otro lado, un **33,4%** de las IES manifiesta **no contar con ningún tipo de asignación presupuestaria para ciberseguridad,** un valor apenas inferior al **34,6%** observado en 2024.

En conjunto, el subdominio Presupuesto refleja una **mejora moderada pero aún insuficiente en la planificación y priorización financiera** de la ciberseguridad. La tendencia indica un **mayor reconocimiento institucional del tema,** aunque persiste la necesidad de **asegurar fondos estables y diferenciados** que garanticen la sostenibilidad de las políticas y medidas de protección implementadas.

4.2.2 IDENTIFICAR



El dominio **Identificar (ID)** alcanza en el **IMC 2025** un **nivel de madurez intermedio (L2)** con un valor promedio de **1,51,** lo que representa una **mejora significativa** respecto al **IMC 2024 (1,32, nivel básico L1).** Este **incremento de casi dos décimas** refleja que las instituciones de educación superior (IES) iberoamericanas están adoptando **prácticas de ciberseguridad más completas y estructuradas,** asignando **recursos adecuados y formalizando procesos** para una gestión más eficaz de los riesgos asociados a la información.

Los resultados de este año muestran que las IES avanzan en la **implementación de tecnologías de seguridad** —como sistemas de detección de intrusos y herramientas de cifrado—, al tiempo que consolidan **equipos especializados** en ciberseguridad y establecen **mecanismos formales de gestión de riesgos.** El valor promedio del dominio (1,51) **coincide con el IMC Global 2025,** a diferencia del año anterior, en el que el dominio **Identificar** (1,32) se situaba ligeramente por debajo del **IMC Global (1,37).**

En comparación con el resto de los dominios, **Identificar (ID)** mantiene, al igual que en 2024, el **anteúltimo lugar** en nivel de madurez, por detrás de **Proteger (PR), Detectar (DE) y Gobernar (GB),** y sólo por encima de **Responder y Recuperar (REyRC).** Pese a ello, el crecimiento observado

confirma una **tendencia sostenida hacia la madurez,** en línea con el fortalecimiento de los procesos de gobernanza y protección.

Al analizar los **tres subdominios** que conforman este ámbito, se observa que tanto **Inventario de Activos** como **Análisis de Impacto** han pasado **de un nivel básico (L1) a un nivel intermedio (L2).** Este avance refleja una **mayor capacidad de las IES para identificar, clasificar y gestionar sus activos críticos,** así como para **evaluar los efectos potenciales de incidentes o interrupciones** sobre sus servicios esenciales. En el caso del **subdominio Análisis de Riesgos,** aunque **permanece en nivel básico (L1),** muestra un **crecimiento moderado (de 1,36 a 1,44),** lo que sugiere un progreso incipiente en la aplicación de metodologías sistemáticas de evaluación de riesgos.

En conjunto, los resultados de este dominio indican que las universidades iberoamericanas avanzan en el **reconocimiento y gestión de sus activos de información,** pero aún deben reforzar la **identificación y priorización de riesgos** como parte integral de su estrategia de ciberseguridad institucional.

El gráfico 22 resume los valores promedio obtenidos por cada subdominio en el IMC 2025, comparados con el IMC 2024, mientras que el gráfico 23 muestra visualmente la distribución de estos valores y su nivel de consolidación dentro del domino.

Gráfico 22: Niveles de madurez y valores promedio de los subdominios de Identificar (ID). IMC24 vs. IMC25.

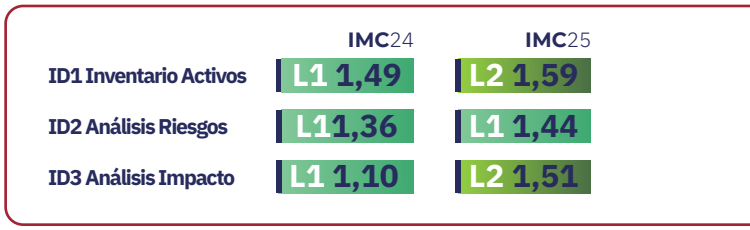
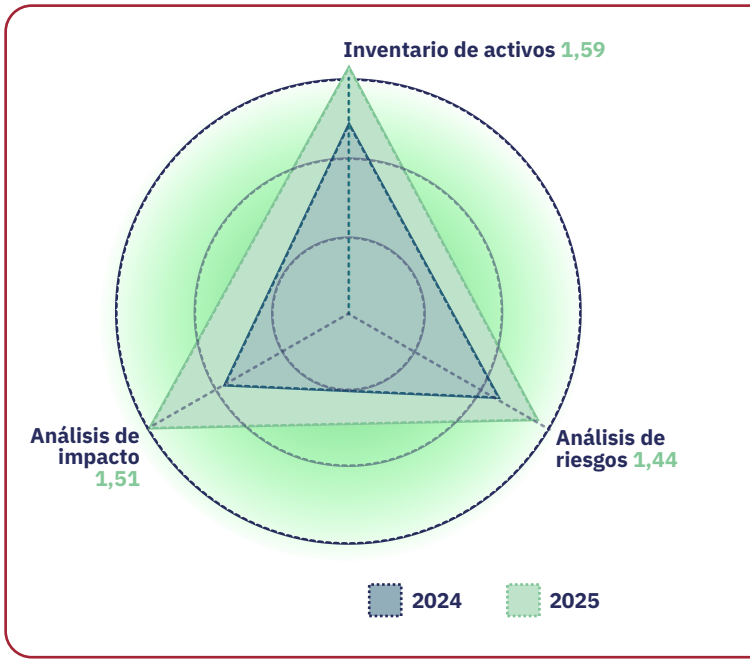


Gráfico 23: Radar subdominios Identificar (ID). IMC24 vs. IMC25.



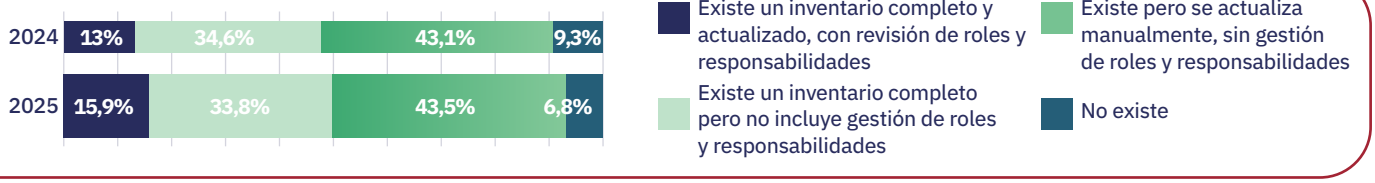
SUBDOMINIO: INVENTARIO DE ACTIVOS

El subdominio **Inventario de Activos** alcanza en el **IMC 2025** un **nivel de madurez intermedio (L2)** con un valor de **1,59,** avanzando un nivel respecto al **IMC 2024 (1,49).** Este resultado refleja una mejora en la **identificación y registro de los activos de información** críticos dentro de las instituciones de educación superior.

Los datos muestran que el **15,9% de las IES** dispone de un **inventario completo y actualizado,** que incluye la **revisión periódica de roles y responsabilidades,** porcentaje **casi 3 puntos por encima del de 2024 (13%).** Asimismo, un **33,8%** cuenta con un **inventario completo,** aunque **sin gestión asociada de roles o responsabilidades,** prácticamente en los mismo valores del **34,6% del año anterior.**

Por el contrario, un **43,5%** de las instituciones declara poseer un **inventario parcial, actualizado manualmente y de forma puntual,** y un **6,8%** indica **no disponer de ningún inventario.** Aunque estos valores mejoran respecto al **IMC 2024** —cuando el **9,3%** no contaba con inventario y el **43,1%** lo mantenía de forma parcial—, más de la **mitad de las IES** sigue sin una gestión integral de activos.

Gráfico 24: Existencia de un inventario de activos de información. IMC24 vs. IMC25.



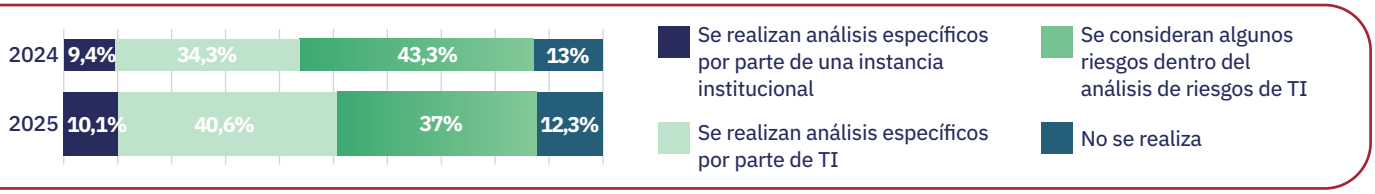
Esta situación evidencia que, si bien se observan **avances graduales,** la gestión sistemática de los activos de información **aún requiere mayor atención institucional.** Contar con un inventario completo y actualizado es un **elemento clave para identificar riesgos,** establecer **prioridades de protección** y orientar las **medidas de seguridad** hacia los recursos que aportan mayor valor a la organización.

SUBDOMINIO: ANÁLISIS DE RIESGO

Este subdominio, relacionado con los procesos de **identificación, evaluación y tratamiento de los riesgos** que pueden afectar a las IES, alcanza un **nivel de madurez básico (L1)** con un valor promedio de **1,44,** lo que supone una **mejora de 0,08 puntos respecto al IMC 2024 (1,36).** Aunque se mantiene dentro del mismo nivel, los resultados evidencian **avances leves en la gestión institucional del riesgo.**

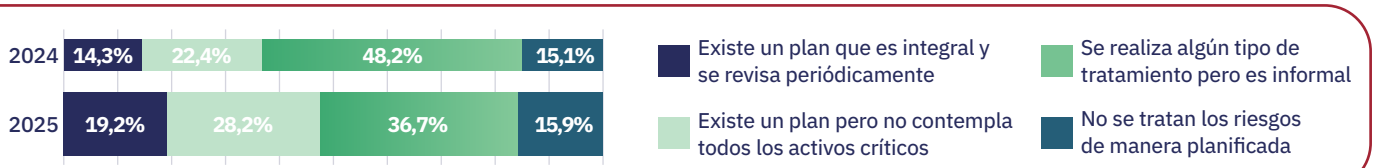
De acuerdo con los datos obtenidos en 2025, el **12,3%** de los consultados no realiza ningún análisis de riesgos. En contraste, el **37%** opta por un análisis parcial, mientras que el **40,6%** delega esta tarea específicamente al área de TI. Finalmente, un **10%** indica que el análisis es gestionado por una instancia institucional.

Gráfico 25: Realización de análisis de riesgos. IMC24 vs. IMC25.



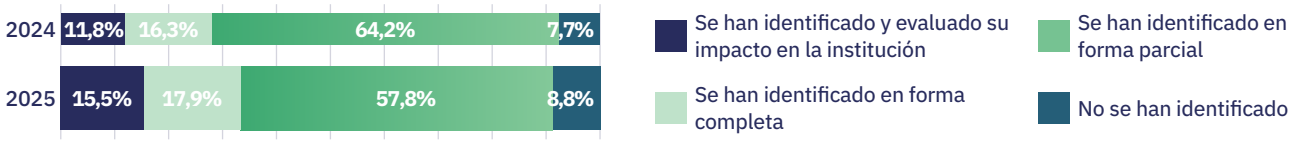
Si hablamos del tipo de tratamiento de riesgos que se realiza, se observa una evolución positiva en la formalización de los planes entre 2024 y 2025. El porcentaje de instituciones que cuentan con un **plan integral y revisión periódica aumentó del 14,3% al 19,2%.** Asimismo, los planes que contemplan activos críticos subieron del **22,4% al 28,2%.** Por el contrario, hubo una reducción significativa en el tratamiento informal de riesgos, que descendió del **48,2% al 36,7%,** mientras que la ausencia de planificación se mantuvo estable cerca del **15,9%.**

Gráfico 26: Tratamiento de riesgos. IMC24 vs. IMC25.



En cuanto a la **identificación y documentación de vulnerabilidades y amenazas** que podrían afectar a los activos vinculados a servicios esenciales, **más del 60% de las IES** declara hacerlo **solo de forma parcial o no hacerlo en absoluto.** Menos del **40%** realiza esta tarea de manera **completa,** y solo un **15,5%** evalúa además el **impacto potencial sobre la institución.**

Gráfico 27: Análisis de amenazas y vulnerabilidades. IMC24 vs. IMC25.



A pesar de la mejora observada, los datos ponen de manifiesto que la **evaluación sistemática de riesgos, amenazas y vulnerabilidades** sigue siendo un **aspecto poco desarrollado** dentro de las universidades iberoamericanas, limitando su capacidad para **anticipar incidentes y proteger eficazmente sus activos de información.**

SUBDOMINIO: ANÁLISIS DE IMPACTO EN LA INSTITUCIÓN

Este subdominio evalúa la **estimación del impacto sobre la continuidad de los activos** que sustentan los servicios críticos en las universidades participantes. En el **IMC 2025** alcanza un **nivel de madurez intermedio (L2)** con un valor promedio de **1,51,** registrando un **incremento de 0,41 puntos respecto al IMC 2024 (1,10).** Este avance refleja una **mayor atención institucional** hacia la continuidad operativa y la resiliencia ante incidentes que puedan afectar los procesos esenciales.

El **10,7% de las IES** realiza una **evaluación anual de impacto,** que incluye la **estimación de tiempos de recuperación,** los **recursos necesarios** y otros elementos propios de un proceso de **mejora continua.** Este porcentaje

supera al **6,9% de 2024,** lo que evidencia un **aumento de más de tres puntos** en la adopción de prácticas sistemáticas de análisis.

No obstante, una **cuarta parte de las IES** declara **no realizar ningún tipo de análisis de impacto,** y cerca del **40%** lo lleva a cabo de forma **básica,** limitada a algunos activos que dan soporte a servicios críticos y considerando únicamente el **tiempo de recuperación** como variable. En comparación con el **IMC 2024** —donde estos valores eran del **28,5%** y **40%,** respectivamente— se constata que **alrededor de un 3% adicional de instituciones** ha comenzado a trabajar en este ámbito.

Gráfico 28: Análisis de impacto sobre activos que soportan servicios críticos. IMC24 vs. IMC25.

Aun así, los resultados confirman que el **análisis de impacto** continúa siendo un **proceso en desarrollo,** con avances visibles pero desiguales entre las IES. Su consolidación será clave para **fortalecer los planes de continuidad de negocio** y garantizar una **respuesta más efectiva ante incidentes** que afecten los servicios críticos de las universidades iberoamericanas.

4.2.3 PROTEGER

El dominio **Proteger (PR)** vuelve a situarse a la cabeza de las categorías analizadas en el **IMC 2025,** con un **valor promedio de 1,68,** superior al **1,54 obtenido en el IMC 2024.** Este resultado confirma su **nivel de madurez intermedio (L2)** y lo posiciona **0,17 puntos por encima del IMC global (1,51).**

La continuidad de este dominio en el primer lugar del modelo refleja que las IES siguen priorizando la **protección de los activos de información,** mediante la **documentación de prácticas, la asignación de recursos específicos y la implementación sostenida de controles técnicos y organizativos**. Con ello, se consolida la idea de que la seguridad física y lógica constituye la base sobre la que las universidades iberoamericanas articulan su gestión de ciberseguridad.

Entre los **subdominios de Proteger,** destaca la **protección de las instalaciones e infraestructura física,** que asciende al **nivel avanzado (L3)** con un valor de **2,52.** Le siguen **Comunicaciones (2,11), Protección de la información (1,86), Externos (1,76) y Aplicaciones y servicios (1,75), todos ellos en nivel intermedio (L2).** En contraste, los subdominios de **Accesos (1,28), Personal (1,23), Equipos (1,41) y Continuidad del servicio (1,20) permanecen en nivel básico (L1).**

La comparación con 2024 muestra un **progreso sostenido en la mayoría de los subdominios,**

El dominio proteger consolida su liderazgo: las universidades avanzan en seguridad física y de red pero aún fallan en continuidad y gestión de accesos.

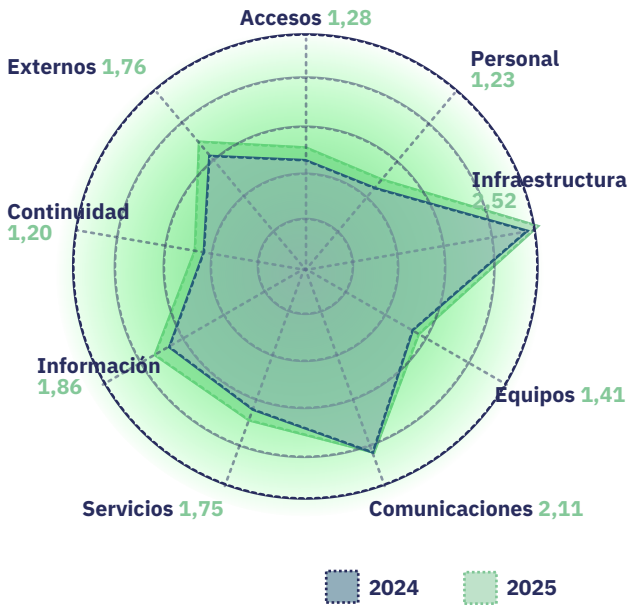
especialmente en infraestructura, que evoluciona de L2 a L3, y en la **formalización de medidas de seguridad en proveedores y servicios externos,** que mejoran su grado de cumplimiento.

Los gráficos 29 y 30 sintetizan los resultados comparativos entre ambos estudios.

Gráfico 29: Niveles de madurez y valores promedio de los subdominios de Proteger (PR). IMC24 vs. IMC25.

	IMC24	IMC25
PR1 Accesos	L1 1,15	L1 1,28
PR2 Personal	L1 1,13	L1 1,23
PR3 Infraestructura	L3 2,40	L3 2,52
PR4 Equipos	L1 1,33	L1 1,41
PR5 Comunicaciones	L2 2,10	L2 2,11
PR6 Servicios	L2 1,63	L2 1,75
PR7 Información	L2 1,69	L2 1,86
PR8 Continuidad	L1 1,11	L1 1,20
PR9 Externos	L2 1,69	L2 1,76

Gráfico 30: Radar subdominios Proteger (PR). IMC24 vs. IMC25.



SUBDOMINIO: CONTROL DE ACCESOS

La gestión de identidades mejora, pero la automatización y las soluciones IAM (Gestión de Identidades y Accesos) siguen siendo una deuda pendiente.

Solo un **6,5% de las IES** cuenta con una **gestión de identidades completamente integrada** mediante soluciones avanzadas de **IAM,** aunque se observa un aumento de dos puntos respecto a 2024. Un **40,3%** gestiona los accesos de forma **estandarizada** y conforme a políticas, aunque sin una integración total, y un **44,5%** mantiene **procesos básicos** apoyados en políticas generales. El **8,8%** restante carece de procedimientos formales, porcentaje que se redujo casi seis puntos respecto al año anterior. Estos resultados evidencian **una mejora leve pero sostenida** en la madurez de la gestión de identidades en las universidades.

La gestión de identidades mejora, pero la automatización y las soluciones IAM siguen siendo una deuda pendiente.

SUBDOMINIO: GESTIÓN DE PERSONAL

Este subdominio alcanza en el **IMC 2025** un valor promedio de madurez de **1,23,** correspondiente a un **nivel básico (L1).** Para el análisis, este dominio se evaluó nuevamente a través de tres aspectos clave:

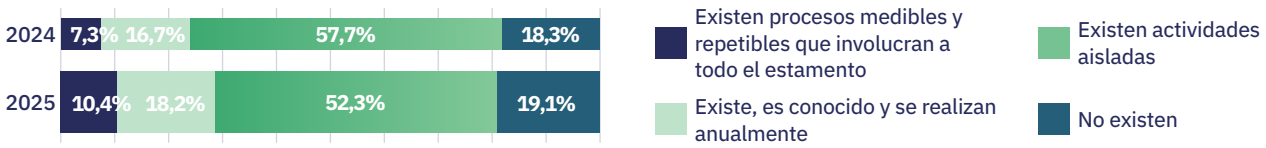
- la **existencia de una estructura de perfiles profesionales** con responsabilidades asociadas a la seguridad de la información y los servicios;
- las **acciones de concientización** dirigidas al cuerpo docente, personal no docente y estudiantado;
- y la **capacitación del personal de TI** en materia de ciberseguridad.

En relación con la **estructura de perfiles profesionales,** se obtuvo un valor promedio de **1,47 (L1).** Casi una quinta parte de las IES (18,8%) manifestó contar con una estructura que **define claramente perfiles y responsabilidades en ciberseguridad**, mientras que un **27%** indicó que las responsabilidades están **descritas de manera parcial o difusa.** El grupo más numeroso, **37%,** señaló que **su estructura de perfiles no incluye responsabilidades específicas en seguridad,** y un **17,2% afirmó no disponer** de una estructura formal de este tipo.

En cuanto a la **concientización del personal docente,** más de la mitad de las instituciones (52,3%) realizan **acciones aisladas,** sin aplicación sistemática a todo el colectivo. Casi un **30%** reporta **actividades anuales de sensibilización,** un **incremento de cinco puntos respecto al IMC 2024,** mientras que **cerca del 20% continúa sin implementar ningún proceso** formal en este ámbito.

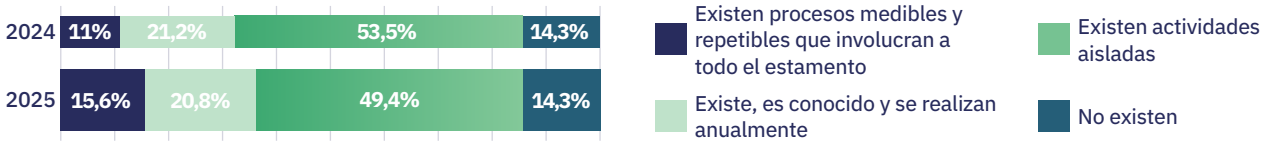
Docentes y personal mejoran su preparación, pero uno de cada tres estudiantes continúa sin recibir concientización en ciberseguridad.

Gráfico 31: Proceso de concientización de los docentes. IMC24 vs. IMC25.



Entre el **personal no docente,** la situación es similar, aunque se observa un **mayor grado de madurez**, con **procesos medibles y repetibles en el 15,6% de las IES,** frente al **10,4% observado en el caso del profesorado.**

Gráfico 32: Proceso de concientización del personal no docente. IMC24 vs. IMC25.



La **concientización en ciberseguridad dirigida a estudiantes** mantiene un panorama comparable al del año anterior, aunque con leves mejoras: un **28,9%** de las IES reconoce **no contar con programas de sensibilización** para este grupo (30,5% en 2024), y solo un **5,8% dispone de procesos formales y periódicos.** En consecuencia, prácticamente **uno de cada tres estudiantes** continúa sin recibir formación o mensajes regulares sobre ciberseguridad, lo que evidencia una brecha significativa en la formación de la comunidad universitaria.

Gráfico 33: Proceso de concientización de estudiantes. IMC24 vs. IMC25.

Por último, en lo relativo a la **capacitación del personal de TI,** el valor promedio alcanza 1,15 (L1). Más de la mitad de las IES (55,2%) dispone de planes básicos de formación en competencias de ciberseguridad para la totalidad o gran parte del personal técnico. Sin embargo, la mayoría de estos programas no se ajusta aún a las necesidades específicas de la institución ni a los diferentes niveles de responsabilidad del personal TIC, lo que limita su impacto real en la gestión integral de la seguridad.

SUBDOMINIO: PROTECCIÓN DE LAS INSTALACIONES E INFRAESTRUCTURA

Este subdominio alcanza en el **IMC 2025** un valor promedio de **2,52,** correspondiente a un **nivel de madurez avanzado (L3),** manteniendo el mismo nivel que en el relevamiento del año anterior. Este resultado refleja la **consolidación de políticas y directrices institucionales** orientadas a la protección física de los activos críticos, con **responsabilidades claramente asignadas y mecanismos formales de control y supervisión.**

El personal responsable **posee competencias adecuadas** y se observa un uso creciente de **tecnologías de seguridad de última generación,** con un **enfoque basado en la mejora continua.** En este sentido, la **gestión de riesgos físicos** se caracteriza por ser **altamente madura,** con acciones específicas para **identificar y mitigar amenazas** que puedan comprometer la disponibilidad y seguridad de los recursos.

Los datos muestran una **amplia cobertura de medidas preventivas** en las universidades iberoamericanas. Casi la totalidad de las instituciones relevadas **implementa mecanismos para proteger sus recursos físicos,** destacando:

- **Áreas protegidas, separadas y con control de acceso (91,5%).**
- **Identificación de personas que ingresan a áreas restringidas (88,1%).**
- **Acondicionamiento físico de los espacios (90,7%).**
- **Protección de las conexiones eléctricas (91,8%).**
- **Sistemas contra incendios (82%).**

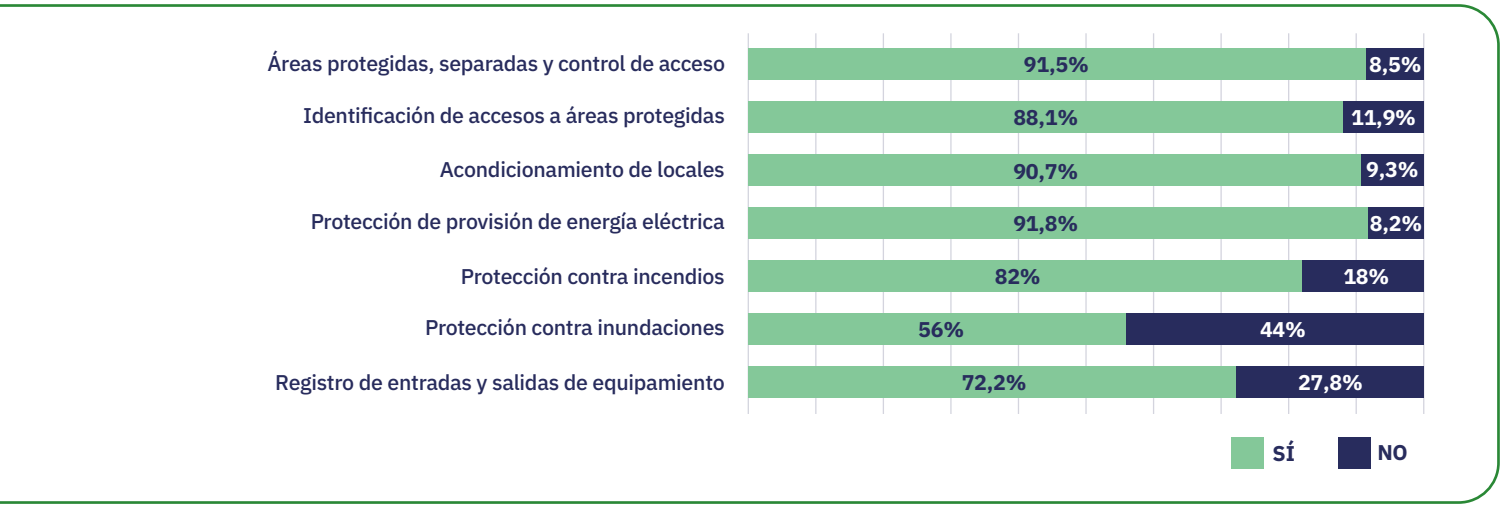
Sin embargo, se identifican **aspectos susceptibles de mejora.** Más de una cuarta parte de las IES **carece de un registro formal de entradas y salidas de equipamiento (27,8%),** lo que dificulta la trazabilidad y control de activos. Asimismo, **solo el 56% dispone de medidas de protección frente**

La seguridad física lidera la madurez en ciberseguridad universitaria, aunque persisten brechas en control logístico y registro de activos.

a inundaciones, posiblemente condicionado por **factores geográficos o estructurales** de las instalaciones.

En conjunto, los resultados confirman que la **seguridad física continúa siendo uno de los pilares más sólidos** de la ciberseguridad universitaria en la región, aunque aún es necesario avanzar hacia una **protección integral** que combine los controles físicos con **mecanismos de auditoría y registro más sistemáticos.**

Gráfico 34: Medidas de protección de las instalaciones e infraestructura implementadas por las IES.



SUBDOMINIO:
PROTECCIÓN DE APLICACIONES Y SERVICIOS

Este subdominio alcanza un **valor promedio de 1,75,** correspondiente a un **nivel de madurez intermedio (L2).** Se sitúa **0,07 puntos por encima del dominio Proteger (1,68) y 0,12 puntos por arriba del valor obtenido en el IMC 2024 (1,63),** confirmando una evolución leve pero sostenida en la aplicación de medidas de seguridad en sistemas y servicios informáticos.

Al igual que en el estudio anterior, este subdominio se evaluó a partir de cuatro aspectos principales: la **implementación de medidas de seguridad acordes al tipo de sistemas y datos gestionados, la protección de los recursos vinculados al correo electrónico, el**

El blindaje digital avanza lentamente: solo una de cada tres universidades protege de forma completa sus aplicaciones críticas.

aseguramiento de la navegación web y la adopción de prácticas de desarrollo seguro.

En relación con la **implementación de medidas de seguridad adecuadas,** los resultados muestran una situación muy similar a la observada en 2024. Un **35,7% de las IES aplica medidas parciales,** centradas únicamente en **aplicaciones y servicios críticos** (38,6% en el IMC 2024). Casi una **tercera parte (30,8%)** implementa **controles suficientes para mitigar riesgos,** pero solo en algunos servicios, lo que denota un enfoque limitado y sin cambios significativos respecto al año anterior (30,1%).

Por su parte, un **28,3%** de las instituciones declara **contar con medidas completas** en todas las aplicaciones y servicios críticos, aplicadas en base a un **plan de mitigación formalizado,** lo que representa una mejora moderada de cerca de **tres puntos porcentuales** respecto al estudio anterior. En el extremo opuesto, un **5,2% de las IES indica no aplicar ningún tipo de control,** valor levemente inferior al registrado en 2024 (5,7%).

En síntesis, los datos permiten concluir que, aunque las universidades iberoamericanas muestran una **mayor sistematización en la protección de sus aplicaciones y servicios, el ritmo de avance sigue siendo lento.** La adopción de medidas tiende a concentrarse en los sistemas más críticos, dejando **brechas de seguridad en entornos y servicios secundarios,** lo que subraya la necesidad de una **estrategia de protección más integral y homogénea** en el ámbito institucional.

SUBDOMINIO: PROTECCIÓN DE LA INFORMACIÓN

Este subdominio alcanza **1,86 (L2),** con un **incremento de 0,17 puntos** respecto a 2024. Más del **50% de las IES** dispone de una **política de protección de datos** integrada a la **política de seguridad institucional,** un aumento del 6% respecto al año anterior. Solo un **13,6%** aún no cuenta con dicho documento, lo que muestra una **tendencia positiva hacia la formalización de políticas de privacidad y seguridad de la información.**

SUBDOMINIO: PROTECCIÓN DE EQUIPOS

Con un **valor promedio de 1,41 (L1),** este subdominio mantiene un nivel básico. El **7,8% de las IES** no aplica controles en los puestos de trabajo, mientras que el **25,7% los realiza de forma informal.** Un **30,2% aplica controles parciales** y solo el **36,4% los implementa en todos los dispositivos** conectados.

En el caso de los **dispositivos BYOD (*Bring Your Own Device* o "trae tu propio dispositivo"),** casi la **mitad (45,8%)** carece de controles, y solo un **25%** aplica medidas formales, aunque algunas universidades lo hacen de forma limitada. Esto revela una **debilidad estructural** en la gestión de la seguridad del puesto de trabajo y los dispositivos personales.

SUBDOMINIO:
PROTECCIÓN DE LAS COMUNICACIONES

El subdominio **Protección de las Comunicaciones** mantiene un **nivel de madurez intermedio (L2),** mostrando una consolidación de las políticas de acceso y de los mecanismos técnicos para garantizar la seguridad en las redes institucionales.

Respecto a la implementación de **políticas de filtrado de tráfico,** los resultados evidencian un avance en la aplicación sistemática de controles. Un **8,8% de las IES** declara no contar con políticas de filtrado, mientras que un **15,2%** aplica estas medidas solo ante incidentes o situaciones de riesgo. Por su parte, un **34,1%** realiza el filtrado de manera permanente pero informal, sin estar plenamente alineado con las normativas vigentes, y el **41,9% restante** lo implementa de acuerdo con las políticas de acceso definidas en su normativa interna, lo que refleja una tendencia hacia la estandarización de estas prácticas.

Asimismo, el estudio analiza el uso de **redes privadas virtuales (VPN)** para las comunicaciones que se realizan fuera del dominio de seguridad institucional. En este aspecto, un **73,1% de las IES** afirma implementar siempre VPNs o evaluar su uso según la criticidad de los activos

involucrados, porcentaje que representa **un incremento de tres puntos** respecto al IMC 2024. Un **21,1%** indica que solo las aplica parcialmente, en determinadas redes o servicios, mientras que un **5,8%** no utiliza este tipo de protección.

Estos resultados evidencian una **mayor madurez en la protección del perímetro digital y las comunicaciones externas**, con una adopción más amplia de controles técnicos y una gestión más consciente de los riesgos asociados al tráfico de red y las conexiones remotas.

SUBDOMINIO: CONTINUIDAD DEL SERVICIO

Este subdominio, que evalúa la **existencia e implementación de planes de contingencia y continuidad operativa,** alcanza en el IMC 2025 un **nivel de madurez básico (L1),** con un valor promedio de **1,20, frente al 1,11** obtenido en el IMC 2024. Aunque el avance es moderado, evidencia una **tendencia positiva hacia la formalización de planes de continuidad** en las instituciones de educación superior.

Los resultados muestran que **casi un 30% de las IES** dispone de un **plan integral de contingencia y continuidad,** y que **solo un 12%** de ellas incluye **pruebas periódicas de restauración, recuperación y uso de medios alternativos** para las copias de seguridad. Por otro lado, un **49% de las instituciones** cuenta con un plan, pero su implementación es **incompleta o parcial,** mientras que el **21,4% restante aún no ha definido ningún plan formal.**

Las IES avanzan lentamente hacia la resiliencia operativa, pero la continuidad del servicio aún carece de madurez.

Gráfico 35: Plan de contingencia y continuidad.

Este subdominio se mantiene como **el punto más débil del dominio Proteger,** situándose **0,48 puntos por debajo** del valor promedio del dominio (1,68). Su nivel de madurez básico refleja que, aunque el reconocimiento de la importancia de la continuidad del servicio ha crecido, **la planificación y ejecución sistemática de medidas de contingencia sigue siendo limitada.** Esta situación, ya observada en el **IMC 2024,** pone de relieve la necesidad urgente de **fortalecer la resiliencia operativa** y garantizar la **disponibilidad continua de la información y los servicios críticos** en las IES iberoamericanas.

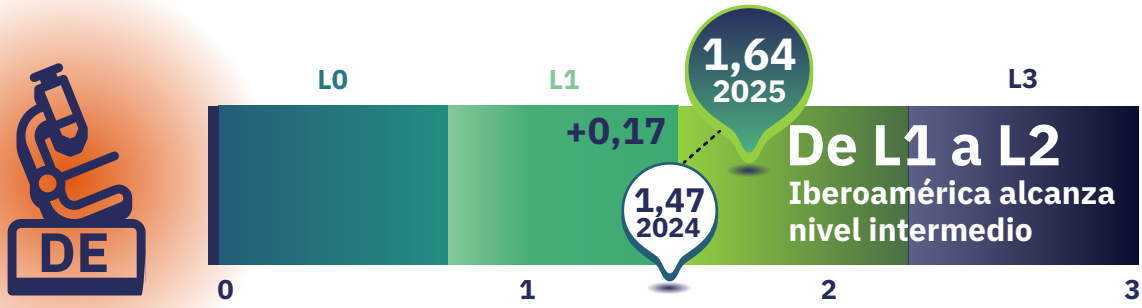
SUBDOMINIO:
PROTECCIÓN DE RECURSOS EXTERNOS

Con **1,76 (L2),** este subdominio mejora respecto al **IMC 2024 (1,69).** El **33,1% de las IES** incluye **requisitos de seguridad** en todas sus contrataciones **y acuerdos de nivel de servicio,** mientras que un **12,4%** no los contempla. El resto los aplica parcialmente, de manera **formal (22,4%) o informal (32,1%).** Estos resultados confirman una **progresiva incorporación de cláusulas de ciberseguridad** en las relaciones con terceros.

En conjunto, los resultados del **IMC 2025** consolidan a **Proteger (PR)** como el dominio más robusto del modelo, caracterizado por la **madurez técnica de sus controles físicos y de comunicaciones y por la tendencia a la formalización de políticas y procedimientos.**

No obstante, persisten **debilidades notables en la gestión de accesos, continuidad del servicio y seguridad del personal y los equipos,** que impiden alcanzar un nivel avanzado generalizado. Su fortalecimiento será determinante para lograr una **madurez integral y sostenible en ciberseguridad institucional.**

4.2.4 DETECTAR



El dominio **Detectar (DE)** alcanza en el **IMC 2025** un **nivel de madurez intermedio (L2),** con un valor promedio de **1,64,** lo que representa un avance respecto al **IMC 2024,** cuando se encontraba en un **nivel básico (L1, 1,47).** Esta mejora evidencia la adopción de **prácticas de ciberseguridad más completas y estructuradas,** así como una **mayor asignación de recursos técnicos y humanos** destinados a la detección y monitoreo de incidentes.

Los resultados de este año muestran que las IES iberoamericanas han **fortalecido la implementación de tecnologías de seguridad** orientadas a la **detección y análisis de eventos potenciales o reales,** tanto en casos de fallas como de ciberataques. Asimismo, se consolida la presencia de **personal especializado en ciberseguridad** y la **formalización de procedimientos de monitoreo y respuesta,** elementos que contribuyen a estabilizar este dominio en el nivel intermedio.

Al igual que en el estudio anterior, **Detectar (DE)** se mantiene en **segundo lugar** en el nivel de madurez, situándose únicamente por detrás de **Proteger (PR).** Su valor se ubica **0,13 puntos por encima del IMC Global (1,51),** lo que reafirma su papel como **pilar operativo clave en el fortalecimiento de la seguridad institucional.**

El dominio detectar se consolida como el segundo dominio más maduro y refuerza la capacidad preventiva de las IES.

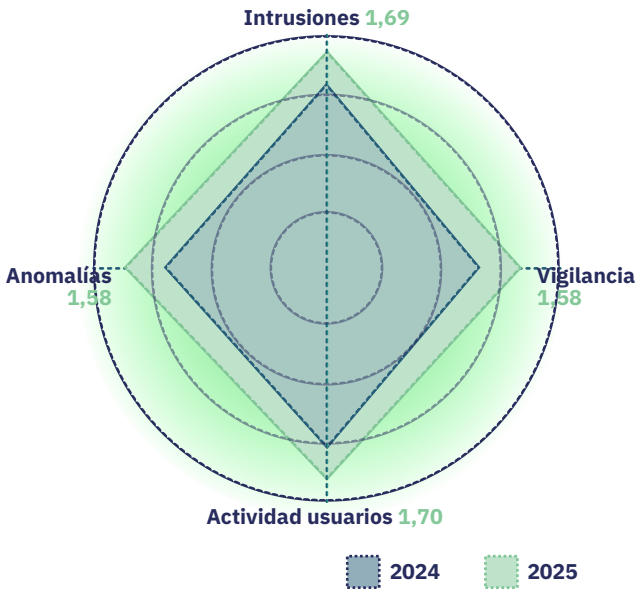
En conjunto, los resultados permiten concluir que las IES continúan **avanzando en la detección oportuna de incidentes y vulnerabilidades,** apoyándose en **mecanismos de monitoreo de red, fuentes de información internas y externas, y sistemas automáticos de análisis de eventos de ciberseguridad.**

En cuanto a los subdominios que integran este dominio, los cuatro alcanzan en 2025 un **nivel intermedio (L2).** En el IMC 2024 solo dos de ellos se encontraban en ese nivel **—Detección de intrusiones (1,58) y Detección de anomalías (1,57)—,** mientras que en la presente edición se suman **Monitoreo de infraestructura (1,58) y Análisis de eventos adversos (1,70),** que ascienden desde el nivel intermedio. Este progreso se asocia al **mayor despliegue de sistemas automatizados de recolección de eventos y a la ampliación de las capacidades de vigilancia** frente a comportamientos anómalos y vulnerabilidades detectadas.

Gráfico 36: Niveles de madurez y valores promedio de los subdominios de Detectar (DE). IMC24 vs. IMC25.

	IMC24	IMC25
DE1 Intrusiones	L2 1,58	L2 1,69
DE2 Vigilancia	L1 1,33	L2 1,58
DE3 Actividad Usuarios	L2 1,49	L2 1,70
DE4 Anomalías	L1 1,57	L2 1,58

Gráfico 37: Radar subdominios Detectar (DE). IMC24 vs. IMC25.



SUBDOMINIO: DETECCIÓN DE INTRUSIONES

Este subdominio alcanza un **nivel de madurez intermedio (L2),** con un **valor promedio de 1,69,** lo que supone un incremento de **0,11 puntos respecto al IMC 2024.** Esta evolución refleja una **mayor implementación de herramientas y procedimientos específicos** para la detección y prevención de intrusiones en las IES iberoamericanas.

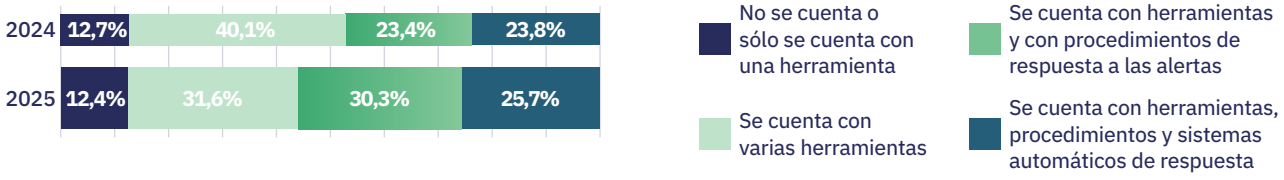
Al igual que en el estudio anterior, se consultó a las instituciones sobre la **disponibilidad de sistemas de detección o prevención de intrusiones (IDS/IPS).** Los resultados muestran que el **25,7%** de las IES dispone de herramientas, procedimientos y **sistemas automáticos de respuesta,** frente al **23,8%** registrado en 2024. Además, un **30,3%** cuenta con herramientas y procedimientos, aunque **sin automatización,** cifra que crece más de siete puntos en comparación con el año anterior (**23,4%).**

Las universidades refeurzan la detección de intrusiones con más herramientas y automatización.

Por su parte, el **31,6% manifiesta disponer de varias herramientas,** aunque sin especificar cuáles, porcentaje que **desciende significativamente respecto a 2024 (40,1%).** Esta reducción indica un **mayor grado de conocimiento y control sobre las soluciones implementadas,** lo que se traduce en una mejora cualitativa del subdominio.

Finalmente, el **12,4%** de las IES aún **no cuenta con componentes específicos** para la detección o prevención de intrusiones, o dispone únicamente de una herramienta aislada, porcentaje prácticamente **sin variaciones** respecto al año anterior **(12,7%).**

Gráfico 38: Sistemas de detección y prevención de intrusiones. IMC24 vs. IMC25.



En conjunto, los resultados evidencian un **fortalecimiento progresivo de las capacidades técnicas** de detección y respuesta temprana ante intrusiones, aunque todavía existe un **grupo minoritario de instituciones** con niveles muy bajos de implementación.

SUBDOMINIO:
MONITOREO CONTÍNUO/VIGILANCIA

Este subdominio, relativo a la **recolección de eventos de seguridad y al análisis de vulnerabilidades,** alcanza un **nivel de madurez intermedio (L2)** con un **valor promedio de 1,58**, lo que supone una mejora significativa respecto al **IMC 2024 (1,33),** cuando se encontraba en el nivel básico (L1). Este avance refleja una **mayor sistematización en los procesos de monitoreo y vigilancia** por parte de las IES iberoamericanas.

Aumenta la adopción de soluciones de vigilancia, pero el monitoreo aún no es plenamente integral.

Casi un **20% de las instituciones** dispone de **sistemas automáticos de recolección y correlación de eventos de seguridad** implementados en todos sus entornos, incluyendo herramientas como **SIEM, paneles de monitorización o repositorios centralizados de eventos.** Por su parte, un **16,6%** indica que **no cuenta con soluciones específicas,** o que utiliza sistemas de propósito general, frente al **27,9%** del año anterior, lo que muestra un desplazamiento positivo hacia la adopción de soluciones especializadas.

En cuanto a los **análisis de vulnerabilidades,** el porcentaje de **instituciones que realizan análisis específicos por una instancia institucional** ha subido 4 puntos, pasando **de un 22,5% en 2024 al 26,7% en 2025.** Así mismo, las IES que realizan **análisis por parte del área TI** sigue la misma tendencia: se **incrementa un 6,7% (18,4% en 2024, 25,1% en 2025).** Quedando un 48,2% de IES en 2025 que **no realizan** análisis de vulnerabilidades o lo hacen de forma muy básica, un **descenso del 10,8% frente al año anterior.**

La siguiente gráfica ilustra la **frecuencia y profundidad de los análisis de vulnerabilidades** realizados por las IES:

Gráfico 39: Análisis de vulnerabilidades en sistemas. IMC24 vs. IMC25.

SUBDOMINIO: MONITOREO DE LA ACTIVIDAD DE LOS USUARIOS

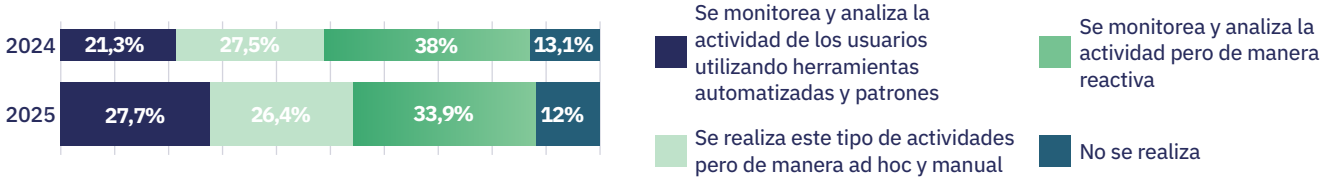
Este subdominio, centrado en el **monitoreo y análisis de la actividad de los usuarios en los sistemas y redes institucionales,** alcanza un **nivel de madurez intermedio (L2)** con un **valor promedio de 1,70,** manteniéndose en el mismo nivel que en 2024, pero con una **mejora de 0,21 puntos respecto al valor del año anterior (1,49).**

Un **27,7% de las IES** declara **monitorear la actividad de los usuarios mediante herramientas automatizadas basadas en patrones predefinidos,** lo que representa un incremento de casi siete puntos en relación con el IMC 2024 **(21,3%).** Este avance es especialmente significativo considerando que el número de instituciones participantes en la edición 2025 ha sido mayor.

En el otro extremo, un **12%** de las instituciones, con un **nivel de madurez inicial (L0), no realiza ningún tipo de monitoreo sobre sus usuarios.** Aunque este valor mejora ligeramente frente al **13,1% del año anterior,** sigue resultando preocupante que **más de una de cada diez IES carezca de mecanismos básicos de supervisión** sobre las actividades de quienes acceden a sus recursos tecnológicos.

El resto de las instituciones se distribuye entre aquellas que **realizan monitoreos reactivos** ante incidentes o sospechas **(33,9%, frente al 38% de 2024)** y las que lo hacen de manera **ad-hoc o no sistemática (26,4%,** apenas un punto por debajo del valor anterior, **27,5%).** Esta tendencia indica una **lenta transición desde prácticas reactivas hacia un monitoreo más preventivo y automatizado,** aunque todavía con importantes márgenes de mejora.

Gráfico 40: Monitoreo de la actividad de los usuarios. IMC24 vs. IMC25.



SUBDOMINIO: ANÁLISIS DE EVENTOS ADVERSOS

Este subdominio alcanza en el IMC 2025 un **nivel de madurez intermedio (L2)** con un **valor promedio de 1,58,** lo que supone un **crecimiento de 0,01 puntos respecto al año anterior (1,57) , manteniéndose en el mismo nivel L2** que en el IMC 2024.

En relación con el **análisis de alertas y eventos anómalos detectados por fuentes internas o externas, un 40,4% de las IES** declara realizar este proceso **de manera ad hoc o eventual,** tomando acciones reactivas según los incidentes ocurridos. Este porcentaje es **algo inferior al 45,9% registrado en 2024,** lo que sugiere un desplazamiento hacia prácticas más estructuradas.

Por su parte, un **11,1% de las instituciones** —aún en un **nivel inicial de madurez**— indica **no realizar ningún tipo de revisión o análisis de eventos adversos,** cifra que, aunque sigue siendo preocupante, **mejora frente al 13,4% del año anterior.**

En el extremo positivo, **casi la mitad de las IES (48,5%)** afirma realizar **análisis periódicos de anomalías y adoptar medidas correctivas en consecuencia.** Dentro de este grupo, **más del 20%** declara **evaluar y mejorar el proceso de forma continua,** porcentaje que crece de manera significativa respecto al **14,3% de 2024.** Este incremento refleja una **evolución hacia un enfoque más proactivo y de mejora continua,** aprovechando los datos obtenidos para fortalecer los mecanismos de detección temprana y respuesta ante incidentes.

4.2.5 RESPONDER Y RECUPERAR

El dominio **Responder y Recuperar (REyRC)** alcanza en el **IMC 2025 un nivel de madurez básico (L1), con un valor promedio de 1,19,** ligeramente superior al obtenido en el **IMC 2024 (1,10),** aunque sin lograr aún el salto al nivel intermedio.

Estos valores reflejan que los **procesos asociados a la gestión de incidentes, su mitigación y la posterior recuperación** se encuentran todavía en una etapa **incipiente y predominantemente ad-hoc, con procedimientos poco formalizados, personal no especializado y uso limitado de herramientas o tecnologías específicas** para la respuesta ante incidentes. La evolución positiva en el valor medio indica una **tendencia de mejora gradual,** pero el conjunto del dominio sigue mostrando una **madurez baja,** situándose como **el más rezagado del modelo IMC,** por debajo del valor global **(1,51),** y manteniendo así la posición observada en el estudio anterior.

El análisis de los **tres subdominios** que integran este componente **—Gestión de incidentes, Mitigación de incidentes y Recuperación—** confirma la misma situación. Todos ellos se encuentran en un **nivel básico (L1),** aunque con leves mejoras numéricas respecto al año anterior.

La mejora más notable se da en **Gestión de incidentes,** que pasa **de 1,16 a 1,32,** lo que evidencia un **mayor reconocimiento institucional**

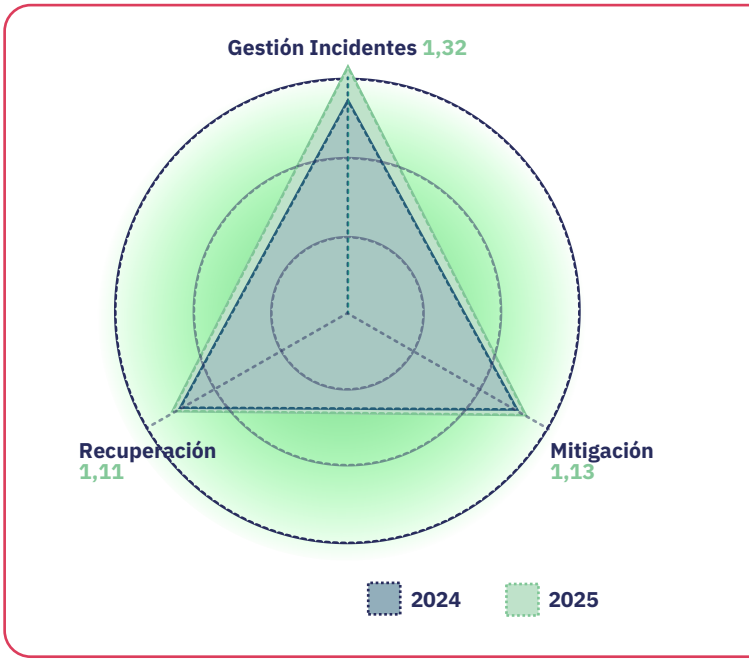
Las universidades avanzan tímidamente en respuesta y recuperación ante incidentes, aún en niveles básicos de madurez.

Gráfico 41: Niveles de madurez y valores promedio de los subdominios de Responder y Recuperar (REyRC). IMC24 vs. IMC25.

	IMC24	IMC25
RE1 Gestión Incidentes	L1 1,16	L1 1,32
RE2 Mitigación	L1 1,10	L1 1,13
RE3 Recuperación	L1 0,96	L1 1,11

de la necesidad de estructurar procedimientos de respuesta. Sin embargo, los valores asociados a **mitigación y recuperación** muestran progresos muy modestos, confirmando que la **capacidad de reacción ante incidentes y la restauración posterior de servicios críticos** continúan siendo **una de las principales debilidades** de las IES iberoamericanas en materia de ciberseguridad.

Gráfico 42: Radar subdominios Responder y Recuperar (REyRC). IMC24 vs. IMC25.



SUBDOMINIO: GESTIÓN DE INCIDENTES

En lo que respecta a la **gestión de incidentes,** resulta fundamental que las instituciones cuenten con **procedimientos claros y operativos** para su detección, análisis, respuesta y mitigación. En este sentido, el IMC 2025 muestra que **casi la mitad de las IES (47%)** dispone de este tipo de procedimientos, aunque en su mayoría **con características informales, sin estar plenamente documentados ni comunicados** a toda la comunidad institucional. Estas prácticas, de carácter **ad-hoc,** corresponden a un **nivel de madurez básico (L1).**

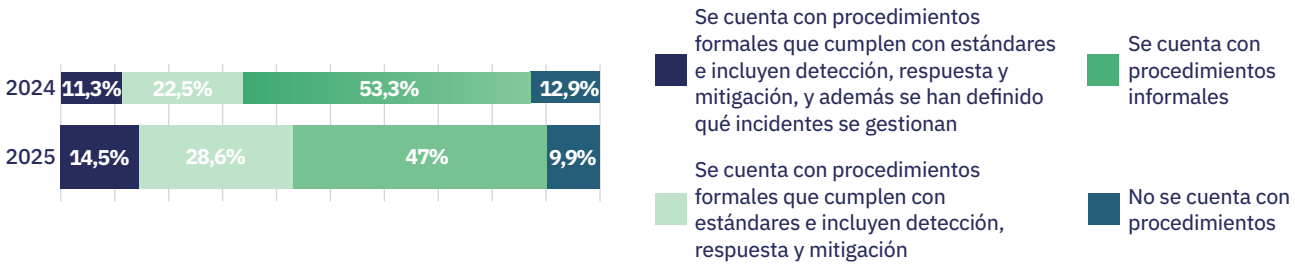
Por otro lado, un **43,1% de las instituciones** cuenta con **procedimientos integrales y documentados,** que describen las diferentes etapas del proceso de gestión de incidentes, alcanzando así un **nivel intermedio (L2).** Dentro de este grupo, una **tercera parte (14,5%)** ha definido además una **taxonomía formal de incidentes,** lo que permite **clasificar y priorizar los eventos** según su naturaleza y criticidad. Finalmente, **menos del 10%** de las IES —en **nivel inicial (L0**)— reconoce **no disponer de procedimientos** para la gestión de incidentes de seguridad.

Comparando estos valores con los del **IMC 2024,** se observa una **mejora de tres puntos porcentuales** en las instituciones que han desarrollado procedimientos formales y que además definen con claridad qué incidentes deben gestionarse. Asimismo, la **formalización de los procesos** muestra un progreso notable: si en 2024 las IES con procedimientos documentados

Casi la mitad de las universidades gestionan incidentes de forma informal, lo que limita su capacidad de respuesta.

representaban el **33,8%,** en 2025 este porcentaje se eleva al **43,1% (total de procedimientos formales),** lo que confirma una tendencia hacia una **mayor estructuración y profesionalización** de la gestión de incidentes.

Gráfico 43: Procedimientos de gestión de incidentes de seguridad. IMC24 vs. IMC25.



Aun así, el panorama general **sigue siendo motivo de atención.** La existencia de un número considerable de IES que gestiona incidentes de manera informal sugiere que, aunque hay conciencia del problema, **la madurez operativa aún es insuficiente.** En un contexto donde **cualquier punto vulnerable puede desencadenar un incidente mayor,** la **preparación institucional** resulta crítica para **reducir los tiempos de respuesta y contener los efectos** de los ciberataques.

Por tanto, el **reforzamiento urgente de las capacidades de respuesta y recuperación mediante procesos planificados, formalizados y difundidos** entre todos los actores institucionales se presenta como una **prioridad estratégica** para las IES iberoamericanas en su camino hacia una ciber resiliencia efectiva.

SUBDOMINIO: MITIGACIÓN

Los ataques de *ransomware* continúan afectando a organizaciones de todos los sectores, incluidas las instituciones de educación superior. Por ello, resulta especialmente relevante analizar si las **IES iberoamericanas** cuentan con **procedimientos formales para prevenir, mitigar y reaccionar** ante este tipo de incidentes.

Solo 1 de cada 10 universidades cuenta con un plan formal contra el *ransomware*.

Al igual que en 2024, el IMC 2025 muestra que la respuesta predominante (36,5%, prácticamente igual al 36,9% de 2024) corresponde a IES que realizan **acciones básicas frente a incidentes de *ransomware*, pero sin seguir un procedimiento aprobado ni con responsabilidades asignadas.** De manera similar, **un 30,3% de las IES declara no contar con un programa específico** para minimizar el impacto de estos ataques, un dato prácticamente invariable respecto al año anterior.

Solo un **9,5% de las universidades** dispone de un **procedimiento formal** que define las **tareas, recursos y responsabilidades** a aplicar en caso de *ransomware*, lo que representa un **incremento marginal (2%)** en comparación con 2024. Por su parte, un **23,7%** indica que realiza **acciones concretas, aunque basadas en procedimientos no formalizados,** manteniendo una situación muy similar a la del año pasado.

Estos resultados ponen de manifiesto que, pese a la creciente exposición al *ransomware* y a las graves **implicaciones operativas, éticas y legales** que conlleva, las IES iberoamericanas **no han incorporado aún de forma sistemática programas de mitigación debidamente estructurados y comunicados** a toda la comunidad institucional.

Resulta evidente, por tanto, la **necesidad urgente de avanzar hacia planes formales de mitigación y respuesta al *ransomware*,** que integren tanto **medidas preventivas** como **protocolos de recuperación rápida,** minimizando el impacto sobre la continuidad de los servicios académicos y administrativos.

SUBDOMINIO: RECUPERACIÓN

En este subdominio se analizó si las IES cuentan con **planes formales de recuperación** frente a incidentes de ciberseguridad. En 2025, apenas un **5,6% de las instituciones** declara disponer de un proceso **definido, aprobado y complementado con simulaciones periódicas y un programa de mejora continua,** lo que representa un **avance marginal de 0,6 puntos** porcentuales respecto al IMC 2024.

Solo 1 de cada 20 universidades cuenta con un plan de recuperación probado y en mejora continua.

Un **21,1%** de las IES indica que cuenta con **procedimientos definidos,** aunque las simulaciones son **esporádicas,** mostrando una mejora de más de tres puntos en relación con 2024. La mayoría **—51,6%—** dispone de **procedimientos aislados o no formalizados,** en línea con el comportamiento observado en la **gestión de incidentes** (47% con prácticas informales).

Finalmente, un **21,7%** manifiesta **no haber definido un plan formal de recuperación,** cifra prácticamente igual a la registrada en 2024 (22%). Este escenario confirma que la **madurez en recuperación ante incidentes sigue siendo incipiente,** con un nivel predominante **básico (L1) y avances limitados** en formalización y ejecución sistemática.

Pese a las mejoras moderadas —alrededor de un **3-4%** de IES pasaron de tener procedimientos aislados a definirlos y acompañarlos de simulaciones—, **la falta de una planificación estructurada continúa siendo una debilidad crítica** del ecosistema universitario iberoamericano.

Complementariamente, el estudio analizó la **frecuencia de incidentes de seguridad** que afectaron la operación institucional durante el último año. **La mitad de las IES indicó no haber sufrido incidentes significativos,** lo que supone un **incremento del 10% respecto a 2024.** Sin embargo, un **18,2%** reportó **entre uno y dos incidentes,** y un **19,8%** informó haber sufrido **de tres a cinco eventos** que impactaron en la **confidencialidad, integridad o disponibilidad** de sus activos. Por su parte, un **12,3%** reconoció **más de cinco incidentes,** un 5% menos que el año anterior.

Si bien el número de eventos reportados parece moderado, su impacto potencial sobre operaciones críticas —como la gestión académica, las inscripciones o la administración del personal— revela la **importancia estratégica de contar con planes de recuperación efectivos, que permitan minimizar tiempos de interrupción y garantizar la continuidad de los servicios esenciales.**

4.2.6 FORMACIÓN Y TALENTO

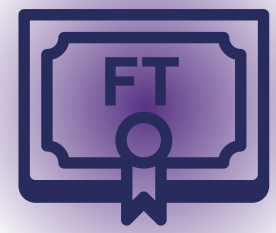
Al igual que en la edición anterior, el IMC 2025 incorpora el dominio de **Formación y Talento (FT),** atendiendo al papel central que desempeñan las IES tanto en la generación de conocimiento como en la formación de profesionales en un entorno intensivo en el uso de tecnologías.

En esta edición, el análisis se amplía mediante cinco preguntas orientadas a conocer, por un lado, la existencia de titulaciones o planes formativos específicos en ciberseguridad y, por otro, las estrategias de captación y retención de talento en este ámbito. El objetivo es obtener una visión actualizada del panorama formativo y de las dificultades a las que se enfrentan las universidades para disponer de personal especializado.

Los resultados muestran que **el 77% de las universidades participantes contribuye a la formación de profesionales en ciberseguridad.** Esta cifra supone un incremento del 14,9% respecto al IMC 2024 (62,1%). Aunque la evolución es positiva, sigue siendo insuficiente para compensar el déficit de profesionales especializados que señalan de forma recurrente distintos informes a escala regional y global.

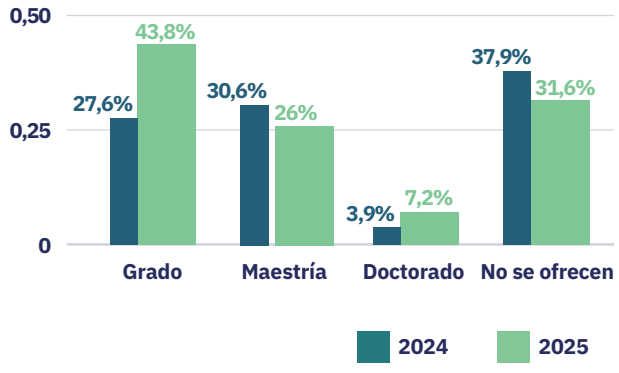
Las titulaciones de grado lideran la oferta situandose en el 43,8% de los casos e incrementado un 16,2% la oferta del año anterior.

En cuanto a la formación de posgrado, el **26% de las universidades ofrece programas de maestría y el 7,2% programas de doctorado.** En la edición anterior, estos porcentajes eran del 30,6% y del 3,9%, respectivamente. Las variaciones observadas se explican, en buena medida, por los cambios en la composición de la muestra entre ambos estudios. Por su parte, el **31,6% de las instituciones declara no contar con ninguna carrera vinculada a la ciberseguridad,** frente al 37,9% registrado en 2024, lo que apunta a una tendencia moderadamente favorable.



La tendencia es favorable: casi el **80% de las IES** ofrece **formación en ciberseguridad,** aunque sigue siendo insuficiente para compensar el **déficit de profesionales especializados.**

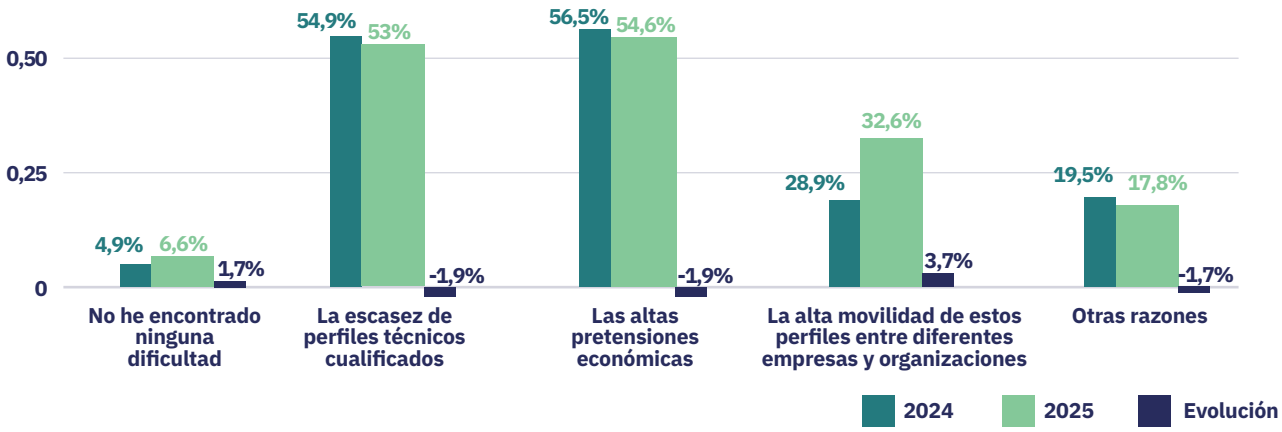
Gráfico 44: Oferta de carreras de grado y posgrados en ciberseguridad. IMC24 vs. IMC25.



En relación con la **captación de talento,** las universidades identifican nuevamente las **altas expectativas salariales** como la principal dificultad, señalada por el 54,6% de las participantes, un valor muy próximo al obtenido el año anterior (56,5%). A continuación, se sitúa la **escasez de perfiles técnicos cualificados,** mencionada por el 53% de las instituciones, también en línea con los resultados de 2024.

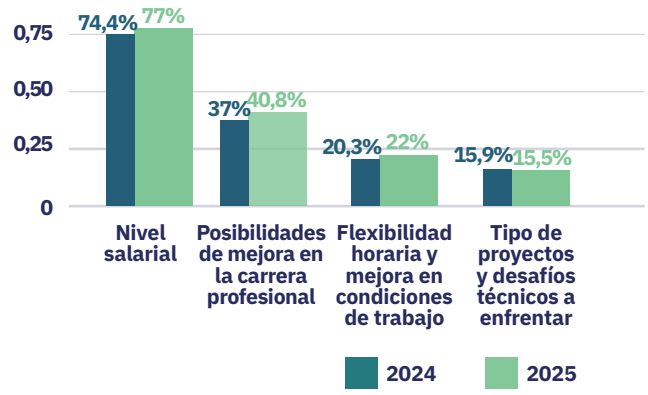
Otros factores relevantes son la **alta movilidad de estos perfiles entre organizaciones** (32,6%). Por su parte, un 17,8% alude a otras razones, mientras que solo un 6,6% afirma no haber encontrado dificultades significativas para la captación de talento especializado.

Gráfico 45: Dificultades principales para captar talento en perfiles de ciberseguridad. IMC24 vs. IMC25. y evolución.



Las **dificultades para la retención** de profesionales especializados reproducen un patrón similar. **El 77% de las universidades señala la imposibilidad de alcanzar el nivel salarial esperado por los especialistas** como el principal obstáculo, porcentaje ligeramente superior al registrado en el IMC 2024 (74,4%). Le siguen las **limitadas oportunidades de desarrollo de la carrera profesional (40,8%), la flexibilidad horaria y las condiciones de trabajo (22%) y el tipo de proyectos y desafíos técnicos disponibles (15,5%).** Estos valores se mantienen muy próximos a los observados en la edición anterior. Cabe recordar que las instituciones podían seleccionar múltiples opciones, reflejando así la concurrencia de varios factores.

Gráfico 46: Dificultades para retención de talento. IMC24 vs. IMC25.



El análisis pone de manifiesto, una vez más, las dificultades estructurales de las IES para posicionarse de forma competitiva en la retención de talento en ciberseguridad, especialmente en un contexto de recursos limitados en comparación con otros sectores, lo que impacta directamente en su capacidad salarial.

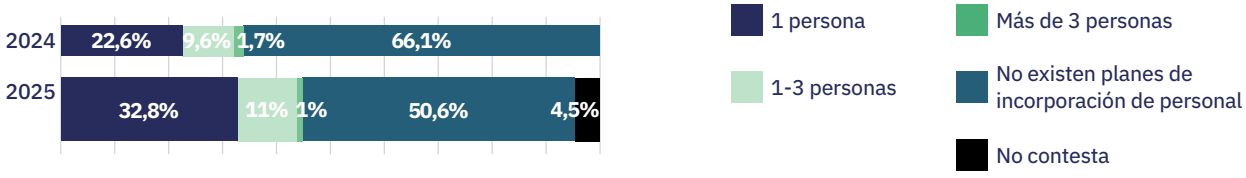
En cuanto a la **rotación de personal,** el 70,2% de las universidades indica no haber sufrido desvinculaciones de perfiles de ciberseguridad en los últimos 12 meses. Sin embargo, **el 29,8% ha tenido que reemplazar parte de su plantilla,** activando procesos de selección, incorporación y conformación de nuevos equipos.

Aunque el porcentaje de instituciones sin rotación sigue siendo elevado, es inferior al registrado en 2024 (72,8%), lo que confirma una ligera intensificación de la movilidad de estos perfiles.

Finalmente, respecto a las **previsiones de incorporación de personal,** el 50,6% de las universidades señala que no contempla nuevas contrataciones en el corto plazo. No obstante, **un 32,8% prevé incorporar una persona y un 11% entre una y tres,** mientras que solo un 1% contempla incorporar más de tres profesionales.

En comparación con el IMC 2024, cuando el 66,1% no tenía planes de incorporación, estos resultados reflejan una evolución moderada pero positiva en las expectativas de refuerzo de los equipos de ciberseguridad.

Gráfico 47: Personal de ciberseguridad a contratar en los próximos 12 meses. IMC24 vs. IMC25.



4.3 Uso de la Inteligencia Artificial

El IMC 2025 incorporó por primera vez una pregunta específica sobre el uso de herramientas de inteligencia artificial aplicadas a la ciberseguridad. El objetivo era conocer no solo si las universidades utilizan estas soluciones, sino también **en qué dominios** las integran y **cómo impactan en su nivel de madurez.**

Los datos muestran que el uso de IA es todavía incipiente, pero empieza a consolidarse en las áreas más operativas de la defensa digital. En promedio, las universidades afirman utilizar estas tecnologías principalmente en los dominios **Proteger (38,3%) y Detectar (32,5%),** seguidos por **Identificar (22,7%).** Su presencia es menor en **Responder y Recuperar (11%)** y claramente residual en **Gobernar (10,1%),** lo que confirma una orientación eminentemente técnica y todavía poco ligada a los procesos estratégicos o de gobierno de la ciberseguridad.

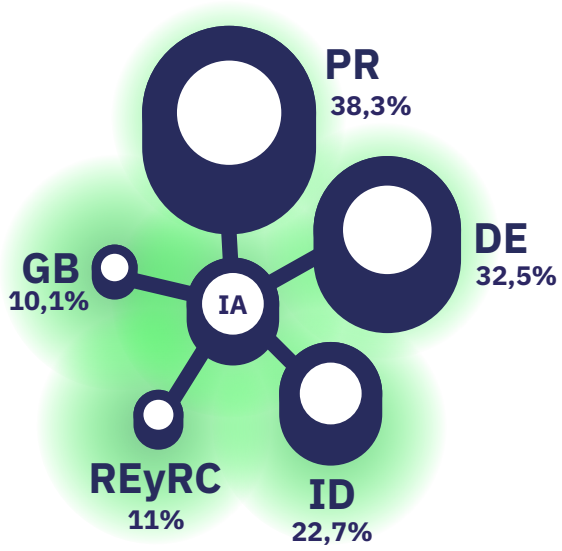
Este patrón se aprecia también en la madurez alcanzada dentro de los subdominios de las instituciones que sí utilizan IA. En el dominio **Proteger** destacan niveles avanzados (L3) en **Protección de la infraestructura (2,68) y Aseguramiento de las comunicaciones**, los únicos subdominios del marco que alcanzan ese grado. En contraste, los valores más bajos se observan en **Recuperación ante incidentes (1,30) y Continuidad del servicio (1,36),** ámbitos donde la automatización sigue siendo limitada y el peso de los procedimientos manuales continúa siendo decisivo.

PERSPECTIVA REGIONAL: UNA ADOPCIÓN DESIGUAL EN IBEROAMÉRICA

La integración de la inteligencia artificial no evoluciona al mismo ritmo en todos los países participantes. A partir de los datos del IMC 2025, se observa que:

Una capacidad con gran potencial, pero aún en fase de ajuste.

Gráfico 48: Dominios y uso de IA. IMC24



- **Colombia, Chile y Ecuador** encabezan la adopción de IA, especialmente en los dominios de PROTEGER y DETECTAR, donde alcanzan los porcentajes de uso más elevados de la región.
- **México y Perú** presentan una adopción intermedia, con una presencia relevante en tareas de detección e identificación, aunque menos extendida en gobernanza o recuperación.
- **Brasil, España, Argentina y Portugal** muestran un uso más prudente y contenido, con porcentajes muy bajos en el dominio GOBERNAR (entre el 0% y el 8%) y una aplicación de la IA principalmente orientada a automatizar funciones operativas.

Esta diversidad revela que, aunque la IA empieza a incorporarse en la gestión de ciberseguridad universitaria, **su despliegue continúa siendo fragmentado,** con marcadas diferencias entre países y un uso que se concentra en los procesos de defensa más inmediatos, sin extenderse aún a la gobernanza o la planificación estratégica.

En resumen, la IA se perfila como una herramienta con un gran potencial para reforzar la capacidad defensiva de las universidades, sobre todo en la protección de infraestructuras y la detección temprana de anomalías. Sin embargo, su implementación todavía es desigual, limitada y orientada casi exclusivamente a funciones operativas.

Para que su impacto sea plenamente significativo, será necesario avanzar hacia un uso más equilibrado y transversal, integrándola también en los procesos de **gobernanza, análisis de riesgos, continuidad, gestión de incidentes y recuperación,** ámbitos en los que la presencia de IA es hoy mínima.

4.4 Enfoque de las IES en torno a la ciberseguridad

El análisis multivariado de los resultados del **IMC 2025** confirma la existencia de tres componentes principales que explican cómo las instituciones de educación superior (IES) afrontan la ciberseguridad: **planificación y socialización, procedimental y defensivo.** Estos tres enfoques permiten identificar no sólo el nivel alcanzado por cada país, sino también las prioridades estratégicas y operativas de las instituciones de la región.

En términos globales, los resultados muestran una mejora moderada en los tres componentes respecto a 2024, con avances más notables en los planos **procedimental y de planificación y socialización,** mientras que el componente **defensivo** mantiene su posición de liderazgo.

- **Componente Defensivo (1,97):** se mantiene como el más sólido en la región, consolidado en el **nivel intermedio L2**, lo que refleja que la mayoría de las IES priorizan mecanismos técnicos de protección y defensa activa frente a amenazas. El crecimiento respecto a 2024 (1,94) es menor que en otros componentes, lo que sugiere que este enfoque se encuentra en una etapa de consolidación más que de expansión. Países como Colombia (2,30), España (2,20) y Perú (2,12) destacan con valores cercanos al nivel avanzado (L3).

- **Componente Procedimental (1,56):** presenta un avance significativo respecto al año anterior (1,47) pasando a un nivel de madurez **intermedio (L2).** Su mejora evidencia un mayor esfuerzo de las IES por institucionalizar procesos y políticas de seguridad. En particular, Colombia (1,92), España (1,67) y Chile (1,65) se ubican claramente por encima de la media iberoamericana, lo que refleja un mayor grado de formalización normativa y operativa.

- **Componente de Planificación y Socialización (1,26):** continúa siendo el menos desarrollado, aunque con un incremento respecto a 2024 (1,17). Esto indica que la formación, la concienciación y la integración de la comunidad universitaria en la cultura de la ciberseguridad avanzan, pero aún de forma lenta. Destacan España (1,49) y Colombia (1,48) con valores por encima de la media, mientras que Argentina (0,85) y Chile (1,16) permanecen rezagadas.

En conjunto, los resultados de 2025 consolidan la tendencia ya observada en 2024: **la ciberseguridad en las IES iberoamericanas se apoya fuertemente en medidas técnicas y defensivas,** mientras que los ámbitos de planificación estratégica y socialización avanzan con mayor lentitud. Esta brecha refleja que, aunque las universidades han fortalecido sus capacidades de respuesta tecnológica, aún deben trabajar en la integración institucional, la concienciación y la asignación de recursos a nivel organizacional.

LAS CLAVES

El componente defensivo mantiene su hegemonía y alcanza niveles cercanos a L3 en varios países.

El componente procedimental es el que más crece, indicando un esfuerzo creciente por normalizar políticas y procesos.

La planificación y socialización mejora ligeramente, pero sigue siendo el principal desafío para alcanzar una madurez integral.

4.5 IMC Iberoamericano por país

La edición 2025 del Índice de Madurez en Ciberseguridad (IMC) incorpora por primera vez la posibilidad de realizar estimaciones **nacionales** para **nueve países,** tras verificarse que contaban con una muestra suficiente y estable, y después de aplicar un proceso de validación en colaboración con las coordinaciones nacionales de MetaRed.

En el **IMC global** se incluyen todas las IES participantes de la región, sin importar su país de origen. Sin embargo, para el **IMC nacional** se procede de forma distinta: los resultados se agrupan por país.

Para cada país se calculó el **IMC Nacional** siguiendo exactamente la misma metodología que para el IMC iberoamericano:

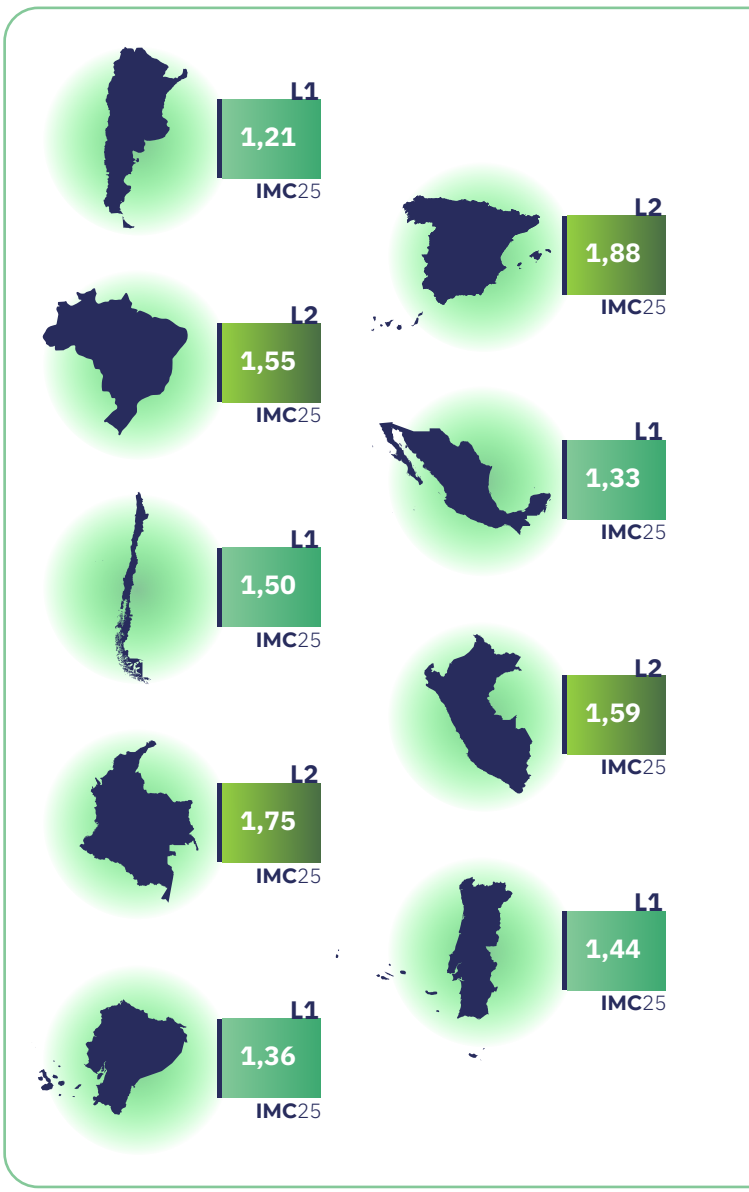
- **Promedio de las IES participantes,** sin aplicar ponderaciones externas.
- **Separación por sectores** (público y privado) únicamente cuando el tamaño muestral alcanzaba el mínimo exigido.
- **Análisis comparado frente al promedio regional,** para valorar el esfuerzo relativo de cada país.

Con esta ampliación, el IMC 2025 ofrece por primera vez una fotografía regional más completa y robusta, que permite identificar avances, brechas y patrones comunes en las capacidades de ciberseguridad de las instituciones de educación superior iberoamericanas.

El **IMC iberoamericano global** se sitúa este año en **1,51 (nivel L2, intermedio),** con cuatro países por encima de este valor: España, Colombia, Perú y Brasil. Si analizamos la diferencia de cada país respecto al promedio regional podemos obtener una estimación del esfuerzo relativo alcanzado:

La segunda edición de IMC amplía su alcance con la incorporación de Brasil y Perú.

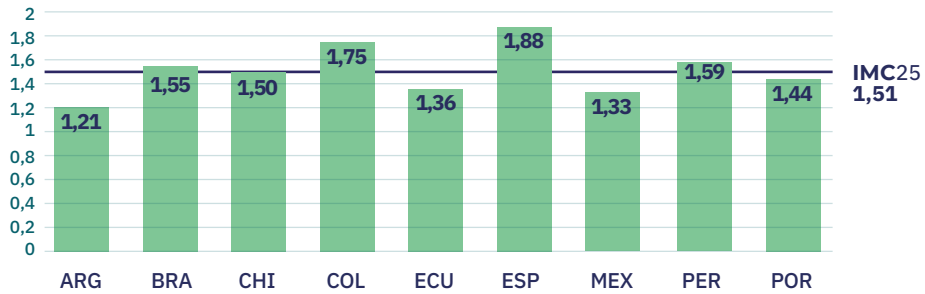
Gráfico 49: IMC25 por país.



- **España (+0,37) y Colombia (+0,23)** mantienen posiciones claramente por encima del promedio, al igual que en 2024.
- **Perú (+0,08) y Brasil (+0,04)** se sitúan ligeramente por encima, mostrando un punto de partida sólido y que sienta las bases para un análisis más profundo en futuras ediciones.
- **Ecuador** reduce significativamente su brecha: pasa de -0,38 en 2024 a -0,15 en 2025.
- **Chile,** que en 2024 estaba levemente por encima del promedio, desciende y se sitúa prácticamente en la media (-0,01).
- **México y Portugal** se alejan del promedio regional quedando a 18 centésimas y 7 centésimas, respectivamente.
- **Argentina (-0,30)** mantiene exactamente la misma diferencia negativa respecto a 2024.

España, Colombia, Perú y Brasil son los países con un nivel de madurez por encima de la media iberoamericana alcanzando el nivel intermedio (L2).

Gráfico 50: Comparativa IMC25 global y por países.

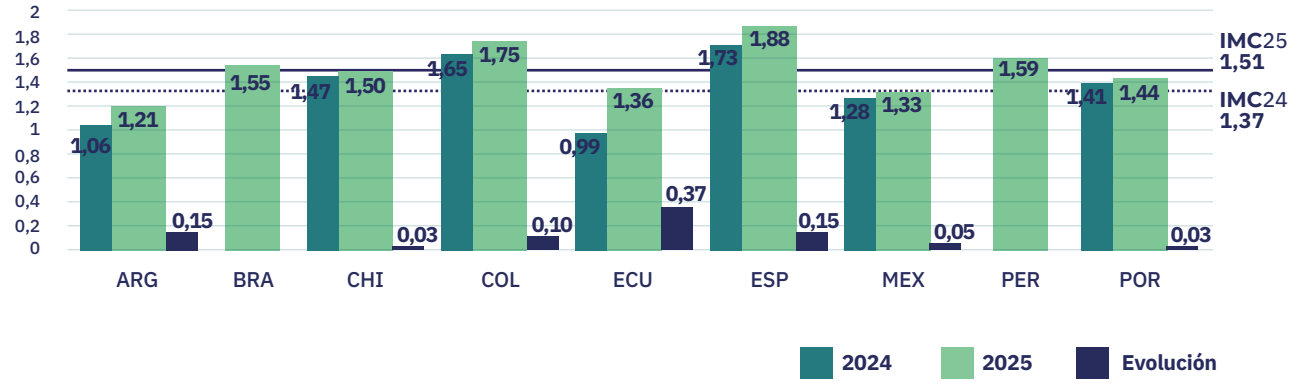


EVOLUCIÓN 2024–2025: MEJORA GENERAL, PERO CON RITMOS DIFERENTES

Si analizamos la evolución de los países desde el año pasado podemos observar como todos los países han incrementado en mayor o menor medida su nivel de madurez.

Iberoamérica, en tendencia alcista en su grado de madurez, crece 14 puntos sobre 2024.

Gráfico 51: Comparativa IMC25 global y por países.

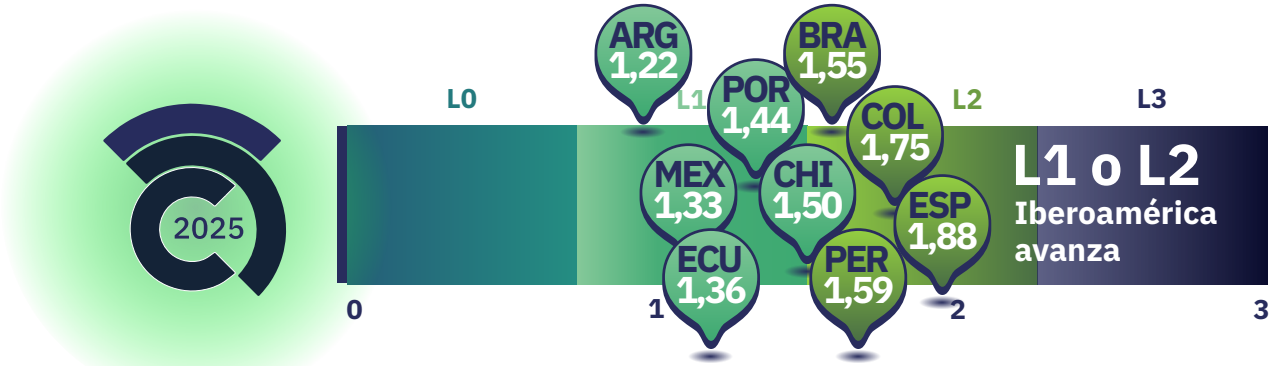


Los datos reflejan una evolución promedio de 14 centésimas, lideradas por el incremento de Ecuador (+0,37), Argentina (+0,15) y España (+0,15).

Por su parte, Colombia sube 10 centésimas, México 5, y Chile y Portugal 3 centésimas.

Brasil y Perú no disponen de datos comparables de 2024, al no haber alcanzado entonces la muestra suficiente; por tanto, no se incluyen en el análisis evolutivo.

DISTRIBUCIÓN POR NIVELES DE MADUREZ: CINCO PAÍSES EN NIVEL INTERMEDIO (L2)



Si hacemos una distribución por nivel de madurez, podemos apreciar cómo todos los países se encuentran en el nivel básico (L1) o intermedio (L2). En concreto, España, Colombia, Perú, Brasil y Chile se encuentran en el nivel intermedio, lo cual pone de manifiesto sus avances en cuanto a prácticas de ciberseguridad más completas, avanzadas y documentadas, con políticas y procedimientos bien definidos, uso de herramientas avanzadas, personal dedicado y procesos especializados de gestión de riesgos formalizados y regulados.

Por su parte, Portugal, Ecuador, México y Argentina se sitúan en nivel básico con prácticas menos maduras que los anteriores.

España, Colombia, Perú, Brasil y Chile se encuentran en nivel intermedio.

Portugal, Ecuador, México y Argentina se sitúan en nivel básico.

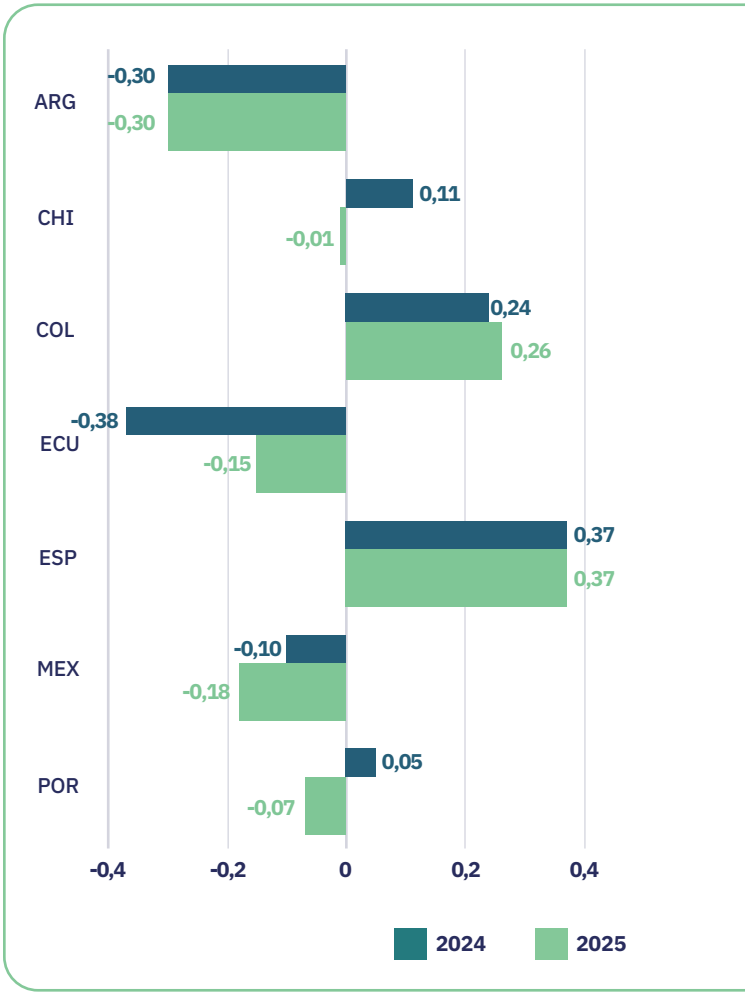
EVOLUCIÓN DE LA POSICIÓN RELATIVA FRENTE AL IMC IBEROAMERICANO

El análisis de la diferencia entre el IMC nacional de cada país y el **IMC promedio iberoamericano de cada año** permite observar no solo su evolución nominal, sino también **el esfuerzo relativo de cada sistema universitario respecto al conjunto de la región.** Esta medida aporta un contexto fundamental: un país puede mejorar su madurez, pero si la región avanza más rápido, su posición relativa puede mantenerse o incluso empeorar.

A partir de los resultados del IMC 2024 y 2025, se identifican las siguientes tendencias:

- **Argentina** mantiene una brecha constante de **-0,30,** situándose en ambos años **treinta centésimas por debajo del promedio iberoamericano.**
- **Chile** experimenta el cambio más notable en términos relativos: en 2024 estaba +0,11 por encima del IMC IBE, y en 2025 desciende hasta **-0,01,** ligeramente por debajo de la media regional.
- **Colombia** conserva una posición estable y claramente favorable, manteniéndose en torno a **+0,20** respecto al promedio en ambas mediciones.
- **Ecuador** muestra una mejora muy significativa: **pasa de -0,38 en 2024 a -0,15 en 2025,** reduciendo su brecha negativa en más de veinte centésimas y acercándose de forma notable al promedio iberoamericano.
- **España** reproduce exactamente la misma posición relativa en ambos años **(+0,37),** lo que refleja un desempeño sólido y sostenido.
- **México** presenta un retroceso: su diferencia **pasa de -0,10 a -0,18,** aumentando la distancia con respecto a la media regional en ocho centésimas.
- **Portugal** también muestra una **caída considerable: de +0,05 en 2024 a-0,07 en 2025,** lo que supone doce centésimas más de distancia negativa frente al promedio iberoamericano.

Gráfico 52: Evolución diferencia IMC país vs. IMC iberoamericano. IMC24 vs. IMC 25.

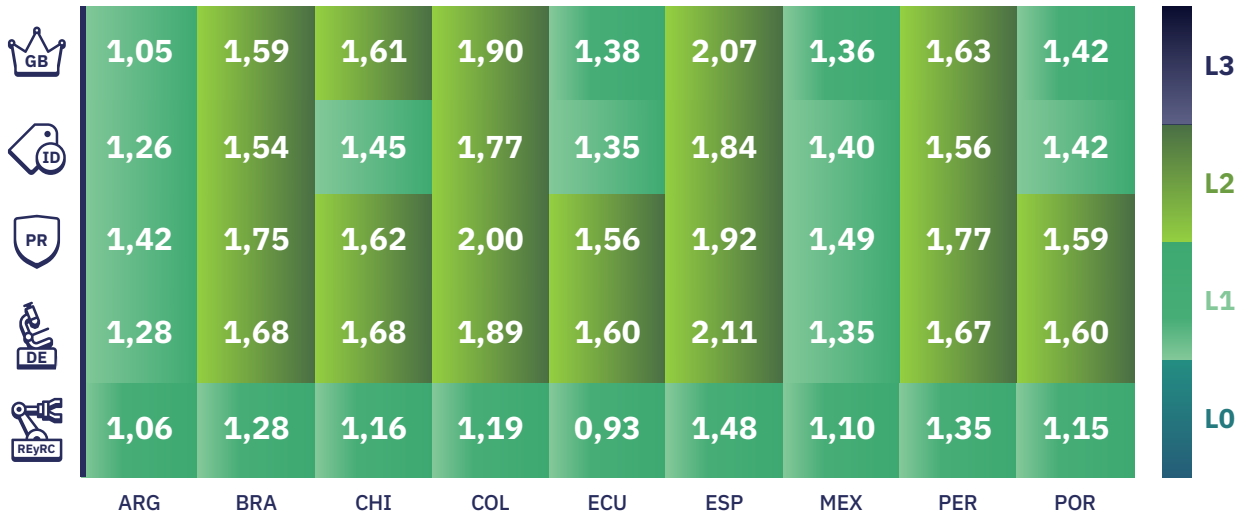


En conjunto, estas variaciones permiten identificar tendencias divergentes: mientras **Ecuador y Colombia reducen o sostienen brechas positivas respecto al promedio, México, Portugal y Chile pierden terreno relativo en la región, y España mantiene la tendencia** estable identificada en 2024.

MADUREZ NACIONAL POR DOMINIO

Si desglosamos los resultados del **IMC 2025 por países y dominios de aplicación,** se observa que en términos generales, la mayoría de los dominios superan la media iberoamericana. La única excepción es **Responder y Recuperar (REyRC),** que continúa rezagado y actúa como factor de penalización en el promedio global, confirmando que la gestión de incidentes sigue siendo la principal debilidad estructural en la región.

Gráfico 53: Comparativa IMC25 global y por países.



A nivel comparativo entre países, los datos muestran una clara segmentación: **Brasil, Colombia, España y Perú logran superar la media iberoamericana en prácticamente todos los dominios,** consolidándose como referentes regionales. En el extremo opuesto, **Argentina, Ecuador, México y Portugal se mantienen por debajo de la media en todos los apartados,** lo que refleja una brecha significativa respecto a los países más avanzados. **Chile,** por su parte, presenta un **desempeño intermedio:** con fortalezas en Gobernar y Detectar, pero con debilidades en Identificar y Proteger.

La gestión de incidentes sigue siendo la principal debilidad estructural en la región.

En cuanto a la distribución por dominios, la región mantiene una **tendencia común hacia la protección (PR, 1,68) y la detección (DE, 1,64)** como ejes más desarrollados, en línea con lo observado en la edición anterior. Los subdominios de protección de infraestructuras y comunicaciones, acciones tradicionales y más verticales dentro de los equipos de TI son las que mejor valor presentan, situándose cerca del nivel L3 o superándolo, como en el caso de la protección de infraestructuras.

La protección de la infraestructura es el único subdominio en nivel avanzado (L3) en la media iberoamericana.

Sin embargo, al analizar los matices nacionales surgen particularidades relevantes. En **España,** los dominios más sólidos son **Detectar (2,11) y Gobernar (2,07),** lo que supone un cambio respecto al estudio del año pasado: las acciones de prevención y monitoreo han logrado superar al tradicional énfasis en la gobernanza. En **México,** aunque la protección lidera, el segundo dominio más fuerte es **Identificar (1,40),** un comportamiento diferente al de la mayoría de los países, que suelen priorizar antes la detección.

En definitiva, los datos confirman que el progreso regional está siendo heterogéneo. Mientras algunos países consolidan avances importantes en todos los frentes, otros aún muestran grandes carencias en aspectos básicos. El caso de **Responder y Recuperar (1,19, con diferencias negativas en la mayoría de los países)** evidencia que la capacidad de resiliencia y recuperación frente a incidentes cibernéticos sigue siendo el gran desafío pendiente para las instituciones de educación superior iberoamericanas.

Gráfico 54: IMC25 por país.

IMC25 — L1 — 1,51

GB	**1,55**
ID	**1,51**
PR	**1,68**
DE	**0,64**
REyRC	**1,19**

IMC25ARG — L1 — 1,21

GB	**1,05** (-0,50)
ID	**1,26** (-0,25)
PR	**1,42** (-0,26)
DE	**1,28** (-0,36)
REyRC	**1,06** (-0,13)

IMC25BRA — L2 — 1,55

GB	**1,59** (+0,04)
ID	**1,54** (+0,03)
PR	**1,75** (+0,07)
DE	**1,68**(+0,04)
REyRC	**1,28** (+0,09)

IMC25CHI — L1 — 1,50

GB	**1,61** (+0,06)
ID	**1,45** (-0,06)
PR	**1,62** (-0,06)
DE	**1,68** (+0,04)
REyRC	**1,16** (-0,03)

IMC25COL — L2 — 1,75

GB	**1,90** (+0,35)
ID	**1,77** (+0,26)
PR	**2,00** (+0,32)
DE	**1,89** (+0,25)
REyRC	**1,19** (+0,00)

IMC25ECU — L1 — 1,36

GB	**1,38** (-0,17)
ID	**1,35** (-0,16)
PR	**1,56** (-0,12)
DE	**1,60** (-0,04)
REyRC	**0,93** (-0,26)

IMC25ESP — 21 — 1,88

GB	**2,07** (+0,52)
ID	**1,84** (+0,33)
PR	**1,92** (+0,24)
DE	**2,11**(+0,47)
REyRC	**1,48** (+0,29)

IMC25MEX — L1 — 1,33

GB	**1,36** (-0,19)
ID	**1,40** (-0,11)
PR	**1,49** (-0,19)
DE	**1,35** (-0,29)
REyRC	**1,10** (-0,09)

IMC25PER — 21 — 1,59

GB	**1,63** (+0,08)
ID	**1,56** (+0,05)
PR	**1,77** (+0,09)
DE	**1,67** (+0,03)
REyRC	**1,35** (+0,16)

IMC25POR — L1 — 1,44

GB	**1,42** (-0,13)
ID	**1,42** (-0,09)
PR	**1,59** (-0,09)
DE	**1,60** (-0,04)
REyRC	**1,15** (-0,04)

4.6 IMC Iberoamericano por tipo de institución

El sistema de educación superior en Iberoamérica presenta una realidad diversa: cada país cuenta con una proporción distinta de instituciones públicas y privadas, que a su vez pueden englobar diferentes tipos de estudios y modelos de gestión. Esta singularidad debe tenerse en cuenta al interpretar los resultados, pues la naturaleza jurídica y organizativa de cada institución influye de manera directa en sus capacidades y prioridades en materia de ciberseguridad.

En esta edición del IMC 2025 la muestra presenta un equilibrio mucho mayor que en el estudio anterior: **51% de universidades públicas y 49% privadas,** lo que aporta una visión más homogénea y representativa de la región. No obstante, esta distribución varía según el país: por ejemplo, en México predominan las instituciones públicas (39 frente a 8 privadas), mientras que en Colombia ocurre lo contrario (38 privadas frente a 7 públicas).

IMC POR TIPO

Los resultados globales muestran una diferencia clara entre ambos tipos de instituciones.

- **Instituciones públicas:** alcanzan un IMC global medio de **1,37 (L1),** lo que representa **14 centésimas por debajo del promedio iberoamericano (1,51).**
- **Instituciones privadas:** obtienen un IMC medio de **1,65 (L2),** situándose **14 centésimas por encima de la media regional.**

Gráfico 55: Participación IES públicas vs. privadas y nivel de madurez por tipo de IES.

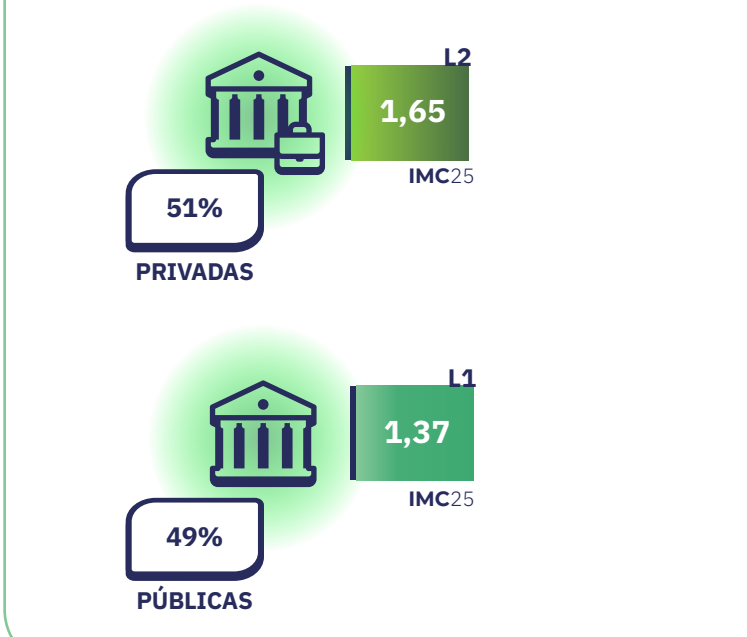
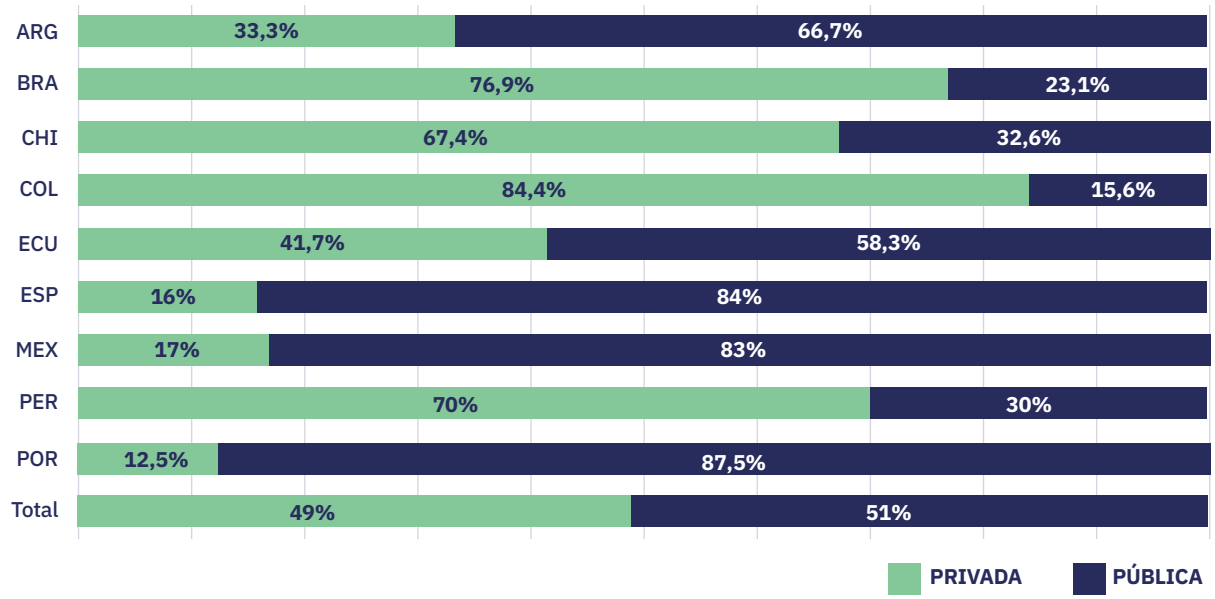


Gráfico 56: Distribución de la participación IES públicas vs. privadas por países.

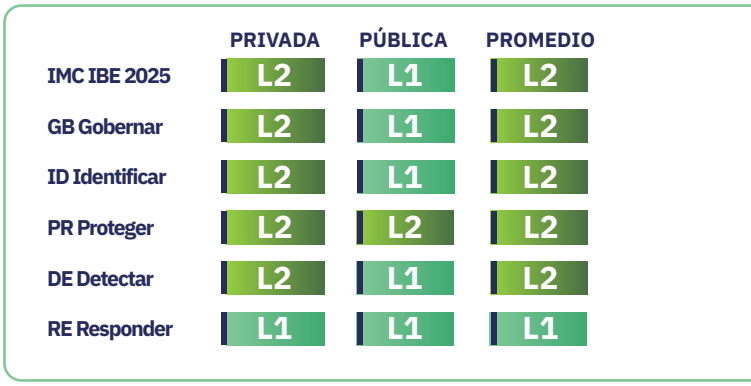


Esta brecha evidencia que, en general, las instituciones privadas han logrado avances más consistentes en sus políticas y prácticas de ciberseguridad, mientras que las públicas mantienen un ritmo de mejora más lento, condicionado probablemente por restricciones presupuestarias, procesos administrativos más complejos y menor flexibilidad organizativa.

El análisis por dominios confirma esta tendencia:

- En **Gobernar (GB),** las privadas muestran que los subdominios con mayores niveles de madurez son estrategia, políticas y normativa, mientras que las públicas todavía presentan carencias en aspectos como el desarrollo de procedimientos, la responsabilidad y la asignación presupuestaria.
- **En Identificar (ID),** las privadas destacan en inventario de activos y análisis de impacto, mientras que las públicas permanecen en niveles básicos en análisis de riesgos.
- En **Proteger (PR),** ambos tipos de institución obtienen sus valores más altos, aunque las privadas sobresalen en la gestión de infraestructuras y comunicaciones.
- En **Detectar (DE),** las privadas vuelven a situarse en un nivel superior, especialmente en vigilancia y análisis de anomalías.
- En **Responder y Recuperar (REyRC),** tanto públicas como privadas se mantienen en niveles básicos (L1), confirmando que la capacidad de gestión de incidentes sigue siendo la gran asignatura pendiente en todo el sistema.

Gráfico 57: IMC por dominio de aplicación.



Si analizamos los datos segmentados por país, podemos apreciar diferencias similares al año anterior entre los tipos de instituciones de cada país.

Gráfico 58: Nivel de madurez de las IES públicas vs. privadas por países.

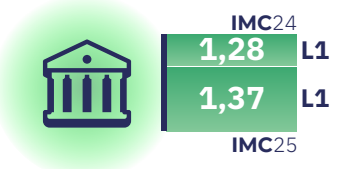
	ARG	BRA	CHI	COL	ECU	ESP	MEX	PER	POR
PRIVADAS	L2 **1,61**	L2 **1,64**	L2 **1,66**	L2 **1,72**	L1 **1,43**	L2 **1,88**	L2 **1,57**	L2 **1,70**	L1 **1,17**
PÚBLICAS	L1 **1,01**	L1 **1,31**	L1 **1,17**	L2 **1,86**	L1 **1,32**	L2 **1,88**	L1 **1,28**	L1 **1,30**	L1 **1,47**
DIF. PRIV-PÚBL.	0,60	0,33	0,49	-0,14	0,11	0,00	0,29	0,40	-0,30

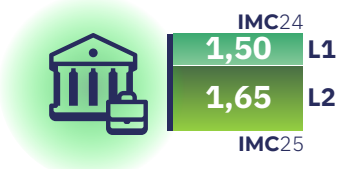
- **Argentina, Brasil, Chile, México y Perú:** la brecha es claramente favorable a las instituciones privadas (entre +0,29 y +0,60). Esto refleja que en estos países las privadas han invertido de manera más decidida en ciberseguridad, probablemente debido a su mayor flexibilidad en la gestión de recursos y a la presión competitiva del mercado.
- **Colombia:** se observa un comportamiento atípico. Aquí las públicas (1,86) superan a las privadas (1,72), invirtiendo la tendencia regional. Este resultado puede estar vinculado a políticas nacionales más activas en las universidades públicas, que han reforzado su estrategia de gobernanza y protección.
- **Ecuador y España:** las diferencias son mínimas (0,00–0,11), lo que indica una situación de equilibrio. En ambos casos, tanto públicas como privadas alcanzan valores muy similares, aunque en niveles distintos: mientras en España ambas tipologías se sitúan en valores altos (públicas 1,88 y privadas 1,88), en Ecuador los dos tipos de instituciones se encuentran en niveles más bajos (1,32 y 1,43, respectivamente).
- **Portugal:** es el único país, junto con Colombia, donde la diferencia es negativa (–0,30), es decir, las públicas (1,47) superan a las privadas (1,17).

EVOLUCIÓN RESPECTO A 2024

La comparación con el estudio del año pasado muestra que tanto públicas como privadas han avanzado, aunque en distinta magnitud:

- **Instituciones públicas:** evolucionan de **1,28 en 2024 a 1,37 en 2025,** con una mejora de **+0,09 puntos.**
- **Instituciones privadas:** progresan **de 1,50 a 1,65,** con un incremento de **+0,15** puntos, casi el doble que el de las públicas.





Por países, este patrón se repite de manera bastante homogénea: las privadas tienden a obtener mejor puntuación en todos los dominios, mientras que las públicas muestran resultados variables, dependiendo en gran medida del contexto nacional.

- **Colombia** mantiene su comportamiento diferencial: ya en 2024 las públicas estaban por encima, y en 2025 este patrón se repite, lo que parece consolidar una tendencia estructural en ese país.
- **España** presenta un caso interesante: en 2024 la diferencia era de +0,10 a favor de las privadas, mientras que en 2025 el valor se iguala. Esto sugiere que las universidades públicas españolas han acelerado su progreso y alcanzado a las privadas en ciberseguridad.
- En **Portugal,** la brecha se ha ampliado en contra de las privadas, confirmando un retroceso relativo frente a las públicas.

El análisis del **IMC 2025 por tipo de institución** confirma que la educación superior iberoamericana avanza de forma desigual en términos de ciberseguridad. Las IES privadas muestran, en general, un desarrollo más sólido y sostenido, mientras que las públicas enfrentan aún retos estructurales que ralentizan su madurez, especialmente en ámbitos como la gobernanza y la gestión de incidentes.

No obstante, ambas tipologías reflejan una mejora respecto a 2024, lo que evidencia una creciente toma de conciencia y un compromiso compartido con la protección de los activos de información en la región. Esta evolución no es uniforme: la ventaja de las universidades privadas es consistente en la mayoría de los países —particularmente en el Cono Sur—, mientras que las universidades públicas presentan una mayor variabilidad, con casos destacados de liderazgo como **Colombia y España.**

Este contraste refleja tanto la influencia del marco normativo y de los modelos de financiación nacionales como la capacidad de cada tipo de institución para priorizar y ejecutar inversiones estratégicas en ciberseguridad.

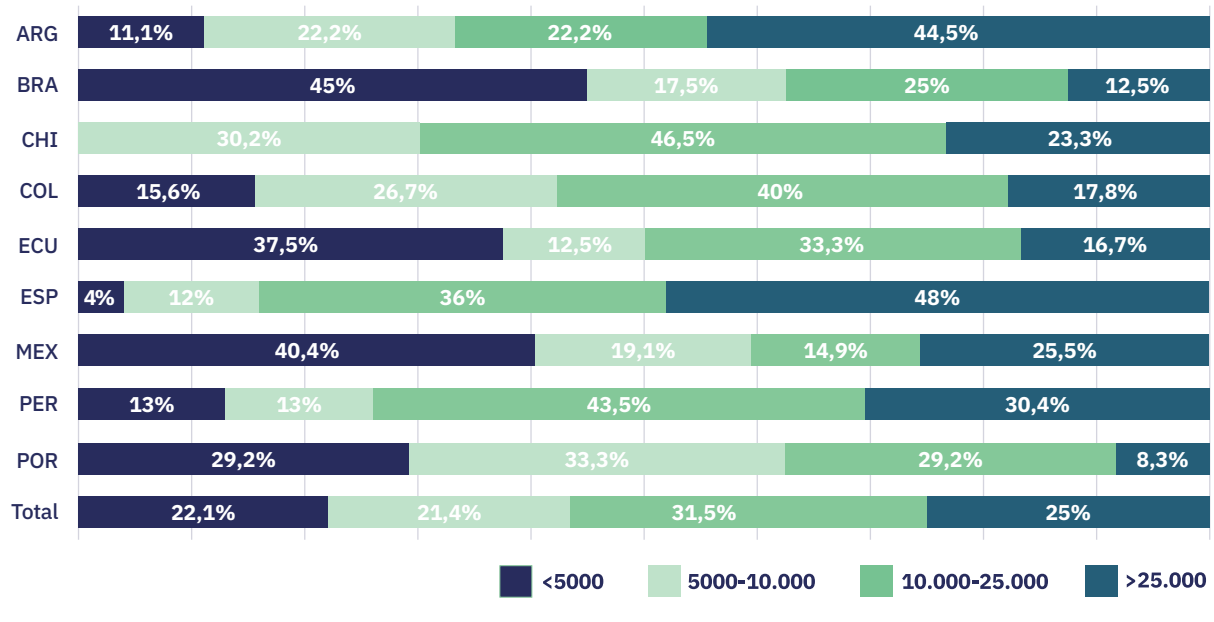
4.7 IMC Iberoamericano por tamaño

El tamaño de las instituciones de educación superior (IES) es un factor determinante en la gestión de la ciberseguridad. La magnitud de su comunidad estudiantil, del personal académico y de los equipos de apoyo influye directamente en el nivel de complejidad de los procesos, en la disponibilidad de recursos y en la capacidad para implementar políticas y controles de seguridad. Analizar la madurez en función del tamaño institucional permite identificar patrones diferenciales y orientar estrategias ajustadas a la realidad de cada grupo.

RELACIÓN CON EL NÚMERO DE ESTUDIANTES

Las IES iberoamericanas presentan una gran diversidad en términos de tamaño, desde instituciones con unos pocos cientos de estudiantes hasta universidades que superan los 25.000. Para este estudio se han establecido cuatro tramos de referencia: **menos de 5.000 estudiantes, entre 5.000 y 10.000, entre 10.000 y 25.000 y más de 25.000.**

Gráfico 59: Distribución del número de estudiantes por país.

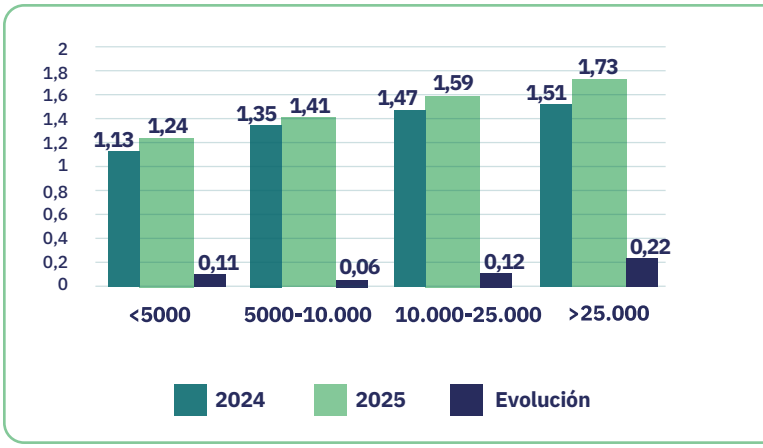


El análisis evidencia que existe una correlación positiva entre el tamaño y la madurez en ciberseguridad. En 2025, las instituciones más pequeñas **(<5.000 estudiantes) alcanzan un IMC medio de 1,24,** mientras que las de mayor tamaño **(>25.000 estudiantes) llegan a 1,73.** Entre ambos extremos se sitúan **las de 5.000–10.000 estudiantes (1,41) y las de 10.000–25.000 (1,59).** Por lo tanto, estamos ante un patrón claro: a mayor tamaño, mayor nivel de madurez.

Comparando con 2024, todas las categorías mejoran, pero el crecimiento es más acentuado en los tramos intermedios y superiores. En particular, las IES de más de 25.000 estudiantes pasan de **1,51 en 2024 a 1,73 en 2025** (+0,22), consolidándose como el grupo más maduro.

Este comportamiento puede explicarse por la mayor disponibilidad de recursos humanos y financieros de las instituciones grandes, así como por la necesidad de contar con políticas y procedimientos más formalizados para atender la complejidad de su gestión. Por el contrario, las instituciones más pequeñas muestran avances más modestos, limitadas por presupuestos más reducidos y una menor capacidad especialización en seguridad.

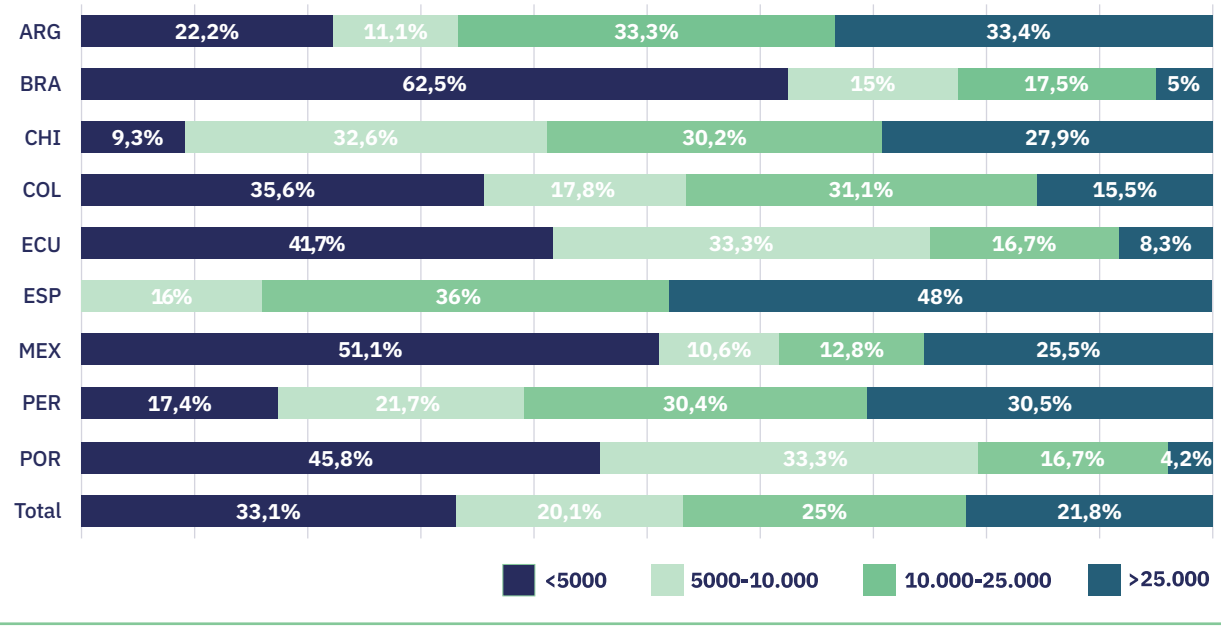
Gráfico 60: Evolución IMC según número de estudiantes. IMC24 vs. IMC 25.



RELACIÓN CON EL NÚMERO DE ACADÉMICOS

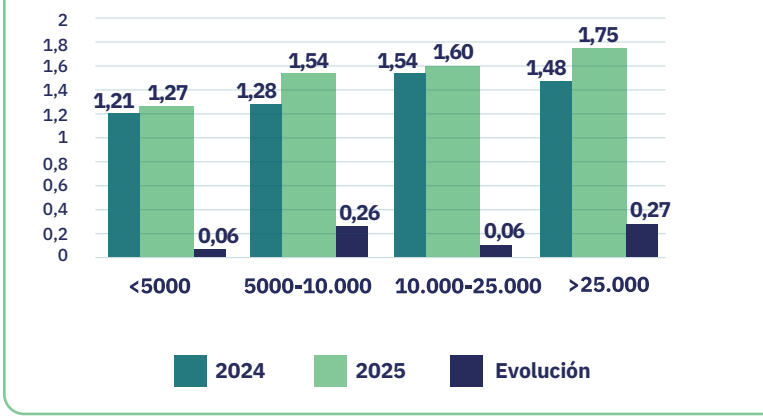
Cuando el análisis se realiza según el número de académicos se observa una tendencia similar. Las **IES con menos de 500 académicos presentan un IMC de 1,27,** mientras que aquellas **con más de 2.500 alcanzan 1,75.** Entre ambos extremos, **los valores intermedios (500–1.000 y 1.000–2.500) se sitúan en 1,54 y 1,60** respectivamente.

Gráfico 61: Distribución del número de académicos por país.



En comparación con 2024, todas las categorías muestran una mejora, destacando el incremento de las instituciones con mayor dotación académica, que pasan de **1,48 a 1,75 (+0,27).** Esto refleja que, a mayor número de personal docente, también se incrementa la capacidad de gestión, la conciencia institucional y el peso estratégico otorgado a la ciberseguridad.

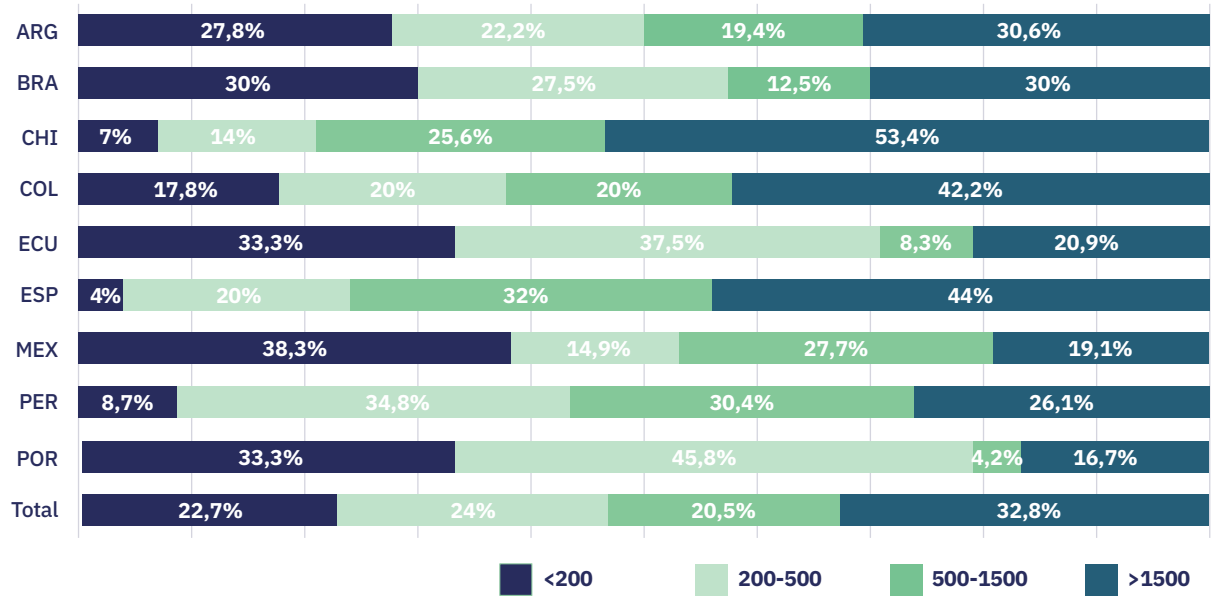
Gráfico 62: Evolución IMC según número de académicos. IMC24 vs. IMC 25.



RELACIÓN CON EL PERSONAL DE SERVICIOS (NO ACADÉMICOS)

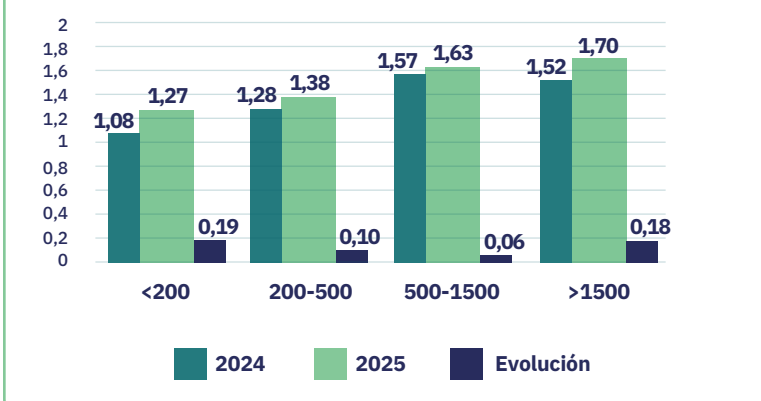
Por su parte, el análisis según el número de personal de servicios también confirma la correlación positiva entre tamaño y madurez. En 2025, las instituciones con menos de 200 trabajadores no académicos registran un IMC de **1,27, frente a un 1,70** en aquellas con más de 1.500.

Gráfico 63: Distribución del número de personal de servicios por país.



La evolución respecto a 2024 muestra un avance especialmente notable en las instituciones más grandes, que han pasado de **1,52 a 1,70 (+0,18).** En este caso, el incremento del personal de servicios está directamente relacionado con una mayor capacidad operativa para implementar controles técnicos, políticas de apoyo y planes de respuesta.

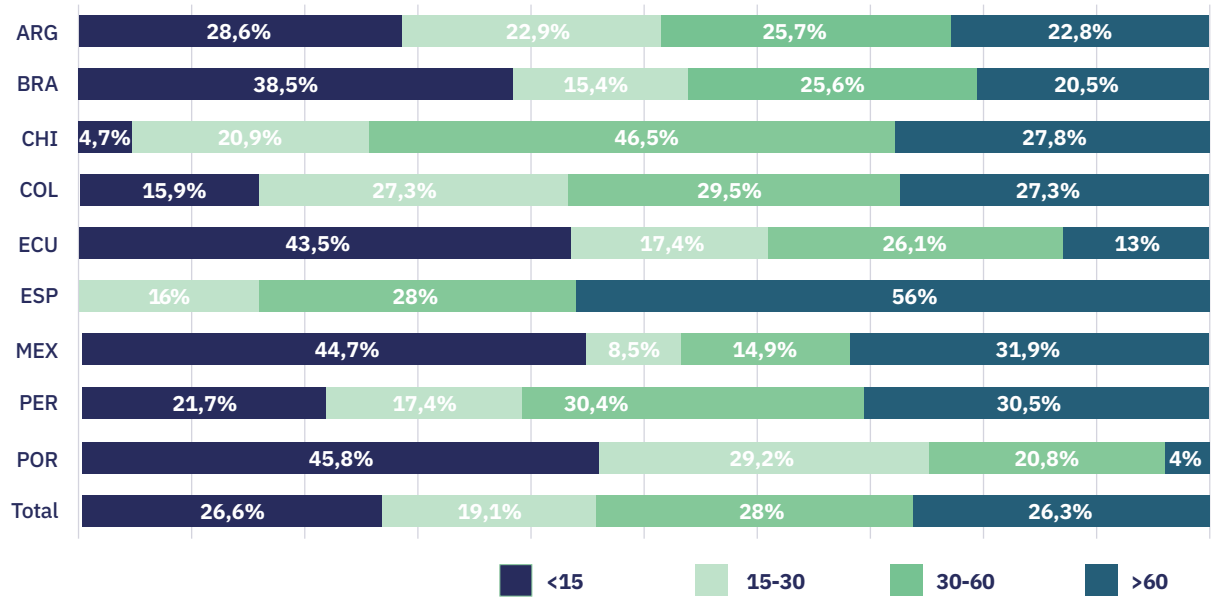
Gráfico 64: Evolución IMC según número de personal de servicios. IMC24 vs. IMC 25.



RELACIÓN CON PERSONAL TIC

El análisis del **IMC 2025 en función del personal TIC** confirma una relación directa entre la dotación de especialistas en tecnologías de la información y el nivel de madurez en ciberseguridad.

Gráfico 65: Distribución del número de personal TIC por país.



Las instituciones con **menos de 15 personas en sus equipos TIC** apenas alcanzan un valor de 1,19, situándose en el **nivel básico (L1),** aunque con una leve mejora respecto al 1,06 registrado en 2024. Este resultado refleja las limitaciones de los equipos reducidos para desplegar políticas y controles de seguridad de forma estructurada.

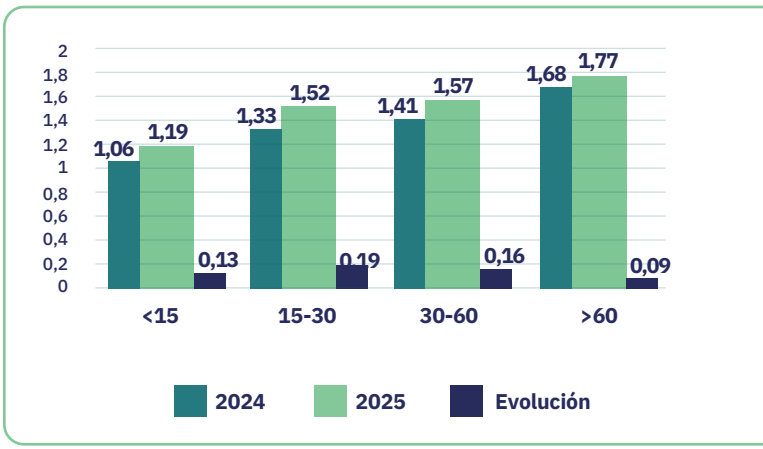
En el tramo de **15 a 30 profesionales TIC, el IMC se eleva a 1,52,** mostrando una ganancia significativa respecto al año anterior (1,33). Este grupo marca la transición hacia un nivel intermedio, señalando que, a partir de cierto volumen de personal especializado, las instituciones logran una mayor capacidad de gestión y control en sus procesos de ciberseguridad.

El grupo **de 30 a 60 integrantes alcanza un IMC de 1,57,** consolidándose en el nivel intermedio (L2). Aunque la mejora respecto a 2024 es más moderada (+0,16), se confirma que las instituciones con una masa crítica suficiente de profesionales TIC cuentan con estructuras y recursos más estables para afrontar amenazas.

Finalmente, **las instituciones con más de 60 profesionales TIC destacan con un valor de 1,77,** manteniendo la tendencia ascendente frente al 1,68 registrado en 2024. Este grupo se consolida como el más avanzado en términos de madurez, evidenciando que el tamaño de los equipos TIC constituye un factor determinante para alcanzar políticas más formales, mayor cobertura de controles y una mejor capacidad de respuesta.

Los resultados muestran la disponibilidad de personal TIC como **factor clave para el desarrollo de la ciberseguridad institucional.** Aunque todas las categorías experimentan mejoras respecto a 2024, las IES con equipos más pequeños mantienen una brecha importante respecto a las de mayor tamaño, lo que resalta la necesidad de apoyo a estos grupos con políticas de capacitación, cooperación interinstitucional y servicios compartidos.

Gráfico 66: Evolución IMC según número de personal TIC. IMC24 vs. IMC 25.



RELACIÓN CON EQUIPOS DE CIBERSEGURIDAD

El análisis del **IMC 2025 según el tamaño de los equipos de ciberseguridad** dentro de las IES revela la influencia directa de la disponibilidad de personal especializado sobre la madurez en ciberseguridad.

LAS CLAVES

Las universidades con equipos de más de 5 personas en ciberseguridad lideran el IMC 2025 con un valor de 1,93, muy por encima de la media iberoamericana (1,51).

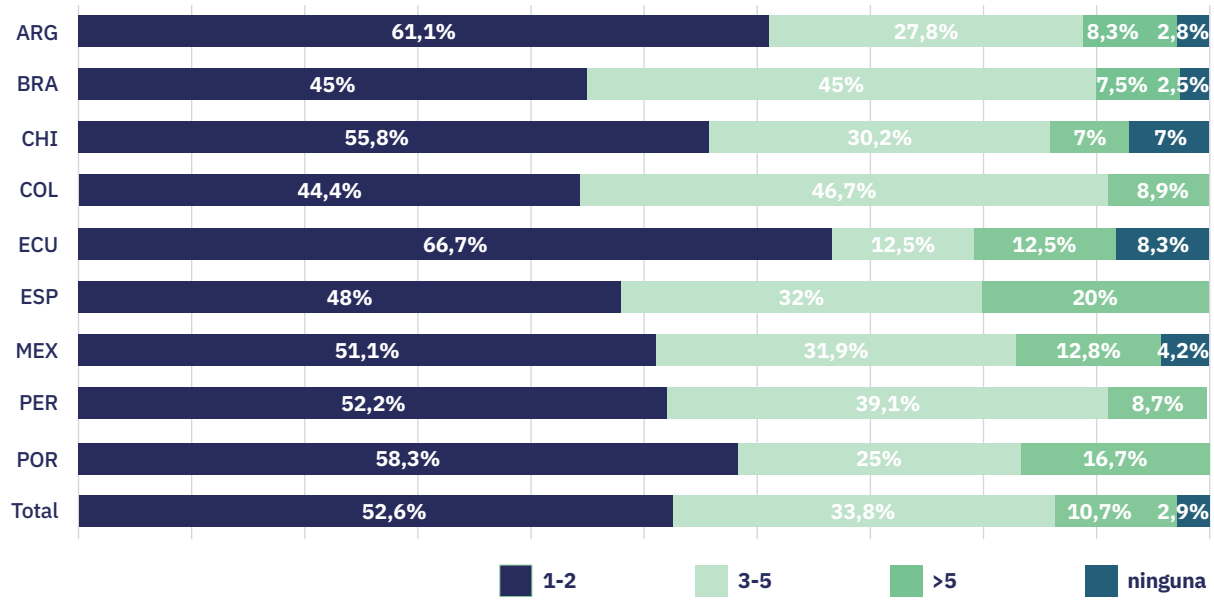
Sin personal especializado, el IMC apenas alcanza 1,03, situando a estas instituciones en un nivel de madurez básico e insuficiente.

El salto más significativo se da en universidades con equipos de 3 a 5 personas, que crecen de 1,61 en 2024 a 1,80 en 2025.

Las universidades con **equipos de más de 5 personas alcanzan el nivel más alto, con un IMC de 1,93,** lo que refleja prácticas más consolidadas, recursos suficientes para la gestión integral y una mayor capacidad para sostener procesos de prevención, detección y respuesta. Aunque se ve una leve reducción respecto a 2024 (1,95), estas IES mantienen su posición de liderazgo, situándose en la franja superior del nivel intermedio (L2), próximas al nivel avanzado (L3).

Las instituciones con **equipos de 3 a 5 personas** también muestran un desempeño sólido, alcanzando un **IMC de 1,80** frente al 1,61 del año anterior. Este avance de casi dos décimas indica que, a medida que los equipos se amplían, mejora la capacidad de gobernanza, identificación de activos críticos y formalización de procedimientos.

Gráfico 67: Distribución del tamaño de equipos de ciberseguridad por país.

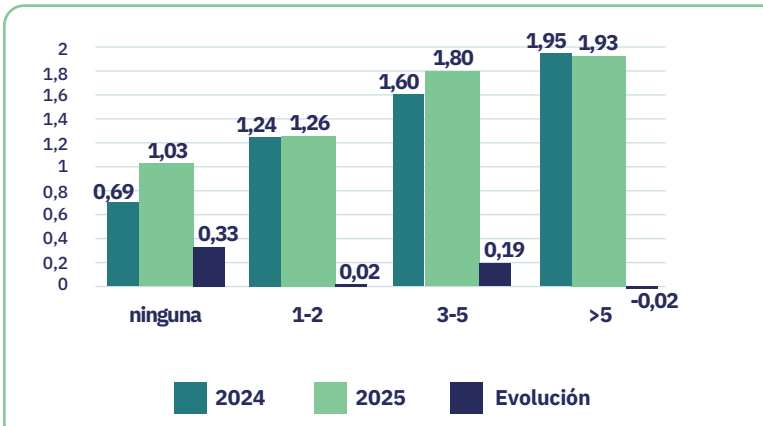


En contraste, las universidades con solo **1 o 2 personas** dedicadas a la ciberseguridad presentan un **IMC de 1,26**, lo que apenas supone una mejora marginal respecto al 1,24 de 2024. Este valor, claramente inferior a la media iberoamericana (1,51), confirma que contar con equipos mínimos limita las posibilidades de evolución hacia niveles superiores de madurez.

La situación más crítica corresponde a las instituciones que **no disponen de personal específico de ciberseguridad, cuyo IMC en 2025 es de apenas 1,03** (aunque mejora desde el 0,69 de 2024). Este dato revela que, sin recursos humanos dedicados, las prácticas en materia de seguridad son casi testimoniales, apoyándose en equipos TIC generales o en servicios externos, lo que las mantiene en un nivel inicial (L0-L1).

En conjunto, los resultados confirman que la **profesionalización y el dimensionamiento de los equipos de ciberseguridad son el factor más determinante** en la evolución del IMC. La diferencia entre universidades con equipos de más de 5 personas y aquellas con estructuras mínimas o inexistentes supera las **seis décimas de IMC,** lo que marca una brecha muy significativa dentro del ecosistema universitario iberoamericano.

Gráfico 68: IMC 25 según tamaño de equipos de ciberseguridad por país.



El análisis del IMC 2025 por tamaño confirma un patrón consistente: **las instituciones más grandes, ya sea por número de estudiantes, académicos o personal de servicios, presentan un mayor nivel de madurez en ciberseguridad.** Este resultado refleja que la escala institucional facilita la asignación de recursos, la formalización de estructuras de gobernanza y la implementación de prácticas más avanzadas.

Este patrón se refuerza al considerar la **dotación de personal TIC** y, de manera aún más determinante, la **composición de los equipos de ciberseguridad.** Las universidades con equipos TIC más amplios y con estructuras de ciberseguridad superiores a 5 personas logran valores de madurez significativamente más altos, alcanzando incluso posiciones cercanas al nivel avanzado. En el extremo opuesto, aquellas instituciones con equipos mínimos o sin personal dedicado a la ciberseguridad permanecen ancladas en niveles básicos, lo que limita gravemente su capacidad de respuesta y resiliencia.

No obstante, no debe pasarse por alto que **las instituciones más pequeñas y las que cuentan con recursos limitados muestran también una evolución positiva respecto a 2024.** Esto indica que, a pesar de sus restricciones, existe una creciente concienciación en este grupo que debería ser acompañada por políticas y programas específicos de apoyo, fomentando la cooperación interinstitucional y el acceso a servicios compartidos. De este modo, se contribuirá a reducir la brecha existente y a consolidar un ecosistema universitario iberoamericano más equilibrado y resiliente frente a las amenazas de ciberseguridad.

La dimensión de los equipos de ciberseguridad es el factor más determinante de la madurez: la brecha entre las universidades con grandes equipos y las que carecen de ellos supera las seis décimas de IMC.

4.8 IMC según presupuesto asignado a ciberseguridad

RELACIÓN ENTRE INVERSIÓN EN CIBERSEGURIDAD Y NIVEL DE MADUREZ INSTITUCIONAL

El análisis del presupuesto destinado a ciberseguridad dentro de las Instituciones de Educación Superior (IES) iberoamericanas revela un **vínculo directo entre la inversión específica en seguridad y el nivel de madurez alcanzado.** Aunque la evolución continúa siendo gradual, los resultados del **IMC 2025** confirman una **tendencia positiva hacia la consolidación de presupuestos diferenciados y la planificación estratégica de los recursos destinados a la protección de la información.**

En el estudio de este año, la **pregunta GB9** —referida a la existencia de un **presupuesto específico para ciberseguridad— muestra que dos tercios de las IES (66,6%) ya destinan fondos** a esta materia, cifra levemente superior al **65,4% registrado en el IMC 2024.** Este crecimiento, aunque moderado, demuestra un **proceso de institucionalización de la inversión en seguridad,** que avanza progresivamente hacia una estructura más formalizada dentro de los presupuestos tecnológicos.

Del total de instituciones que destinan fondos, un **39,6%** lo hace mediante **asignaciones específicas dentro del presupuesto de TI,** lo que supone un **incremento de 4 puntos porcentuales** respecto al año anterior (35,7%). Asimismo, un **5,5%** de las IES declara contar con un **presupuesto de ciberseguridad diferenciado,** separado del presupuesto general de TI, valor que **supera en 1,5 puntos al obtenido en 2024.** En el extremo opuesto, un **33,4%** de las IES **no cuenta con ningún tipo de asignación presupuestaria,** porcentaje apenas un punto menor que el año anterior, mientras que un **21,4%** utiliza **asignaciones generales** para cubrir gastos relacionados con la seguridad, sin una línea presupuestaria específica.

Las universidades que invierten más del 5% de su presupuesto TI en ciberseguridad alcanzan niveles de madurez significativamente superiores (IMC 1,79).

Estos datos reflejan una **maduración paulatina del enfoque financiero de la ciberseguridad:** las IES empiezan a reconocerla como un componente estructural de su gestión tecnológica, pero aún **predomina una dependencia del presupuesto de TI,** sin plena autonomía ni previsión multianual. La falta de una línea presupuestaria propia continúa limitando la posibilidad de desarrollar políticas sostenidas de formación, monitoreo, detección y respuesta ante incidentes.

RELACIÓN ENTRE PORCENTAJE DEL PRESUPUESTO TI DESTINADO A CIBERSEGURIDAD Y NIVEL DE MADUREZ

El análisis comparativo del **IMC según porcentaje del presupuesto TI asignado a ciberseguridad** evidencia una correlación directa entre nivel de inversión y madurez alcanzada. **Las IES que destinan más del 5% obtienen niveles de madurez claramente superiores,** acercándose o superando el **nivel intermedio (L2),** mientras que aquellas sin presupuesto específico permanecen en el **nivel básico (L1).**

Se observa que **el mayor salto de madurez (+0,23 puntos)** se da en las IES que destinan **entre el 5% y el 10%** del presupuesto TI a ciberseguridad, alcanzando una media de **1,79,** el más alto de todos los tramos analizados. Esto sugiere que **incrementos moderados y sostenidos de inversión tienen un impacto tangible en la capacidad institucional para gestionar la ciberseguridad,** al permitir fortalecer procesos clave, profesionalizar al personal y consolidar sistemas tecnológicos de protección y monitoreo.

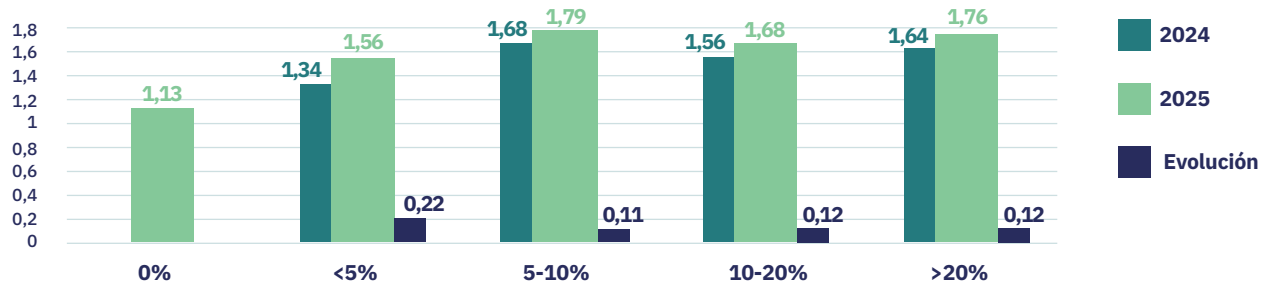
A partir de ese umbral del 5%, todas las categorías presentan **niveles de madurez superiores al promedio global (1,51),** lo que fortalece la idea de que **un esfuerzo presupuestario razonable, bien orientado, genera resultados medibles.** Por el contrario, las instituciones que **no asignan presupuesto** no solo no avanzan, sino que incluso **retroceden** respecto a 2024, cayendo **a un nivel medio de 1,13,** el más bajo de todo el espectro.

1 de cada 3 IES no dispone aún de presupuesto para ciberseguridad.

Crece el porcentade de IES con asignaciones específicas (+4 puntos) y líneas diferenciadas (+1,5 puntos).

En términos globales, **puede afirmarse que el punto de equilibrio entre inversión y madurez** se sitúa en el **tramo del 5–10%,** donde las IES logran un **nivel de madurez intermedio robusto (L2 alto)** sin necesidad de una estructura presupuestaria excesiva. Este dato constituye una referencia práctica para la planificación financiera de las instituciones que buscan consolidar su cultura de seguridad sin incrementar de manera desproporcinada sus gastos de TI.

Gráfico 69: Distribución según presupuesto destinado a ciberseguridad. IMC24 vs. IMC25. y evolución.



INTERPRETACIÓN Y TENDENCIAS

El avance hacia presupuestos específicos y diferenciados refleja un **cambio de paradigma:** la ciberseguridad deja de considerarse un gasto reactivo y comienza a tratarse como una **inversión estratégica en continuidad y confianza institucional.** No obstante, el hecho de que **uno de cada tres IES no cuente con presupuesto** sigue representando un riesgo crítico, al depender de asignaciones ad-hoc o decisiones coyunturales.

La evidencia muestra que los **incrementos moderados de inversión** —a partir del 5% del presupuesto TI— **no solo mejoran los indicadores técnicos, sino también los organizacionales,** al favorecer la planificación, la formación del personal y la adopción de tecnologías de detección y respuesta. Las instituciones que mantienen presupuestos diferenciados también

presentan **procesos más estables de gobernanza y auditoría,** reforzando el ciclo de mejora continua que caracteriza los niveles de madurez más altos del modelo IMC.

Los resultados del IMC 2025 permiten establecer las siguientes conclusiones:

- **El presupuesto es un factor decisivo en la madurez institucional:** sin una asignación presupuestaria, las IES tienden a permanecer en niveles básicos, incluso cuando cuentan con políticas formales.
- **A partir del 5% del presupuesto TI,** la ciberseguridad comienza a consolidarse como una práctica sistemática, sostenida por procesos y equipos especializados.
- Las IES con **líneas presupuestarias diferenciadas** presentan mejores capacidades de planificación y monitoreo, aunque aún son minoría.
- La **falta de previsión económica** continúa siendo uno de los principales obstáculos para alcanzar niveles avanzados de madurez.

El tramo de 5-10% se consolida como el punto de mayor eficiencia entre coste y madurez.

4.9 Ciberincidentes en Iberoamérica

El análisis de ciberincidentes reportados por las IES en Iberoamérica en 2025 ofrece una visión más precisa del nivel real de exposición de las universidades ante amenazas que afectan directa o indirectamente a servicios críticos.

La encuesta IMC 2025 preguntó por el número de incidentes significativos sufridos durante el último año, permitiendo evaluar no solo la frecuencia, sino también la evolución respecto a 2024 y las diferencias entre países.

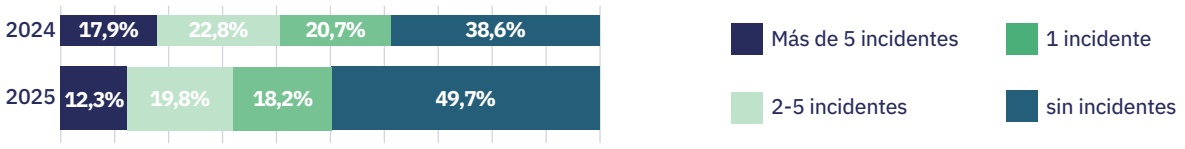
En 2025 se observa una **mejora significativa en la estabilidad operativa de las IES** de Iberoamérica. **Casi la mitad** de las universidades participantes **no reportaron incidentes que afectaran parcial o totalmente a sus sistemas críticos,** alcanzando un 49,7%, frente al 38,6% del año anterior. Este incremento de más de un 11% es uno de los cambios más notables del estudio. El resto de categorías también reflejan una evolución positiva:

- Las IES con **1 incidente** descienden ligeramente (18,2%, frente a 20,7% del IMC 2024).
- Las IES con de **2 a 5 incidentes** bajan al 19,8%, frente al 22,8% de 2024.
- Destaca la reducción de los casos más críticos, con **más de 5 incidentes,** de 17,9% en 2024 a **12,3%,** la cifra más baja registrada.

Este comportamiento sugiere que las universidades no solo podrían estar mejorando en prevención, sino también en la contención y gestión temprana de los ataques, reduciendo la probabilidad de recurrencia o propagación.

El número de IES afectadas en el último año se reduce un 11%.

Gráfico 70: Distribución número de incidentes de seguridad. IMC24 vs. IMC25.



EVOLUCIÓN/TENDENCIA

La comparación entre ambas ediciones confirma un **descenso global en la frecuencia de incidentes.** En 2025 hay **más IES sin incidentes y menos IES en todas las categorías,** lo que apunta a un ecosistema universitario más preparado y resiliente.

De forma agregada, el **promedio de incidentes por institución** aumenta ligeramente (de 9,62 a 10,96) debido a que ciertas IES concentran un número elevado de casos, pero este comportamiento no altera la tendencia general: **menos instituciones afectadas y menos recurrencia extendida.**

A nivel país, se observa una tendencia dual: por un lado, Argentina, Chile, Colombia, Ecuador y Portugal reportan un número de incidentes similar o ligeramente superior a 2024 y, por otro lado, España y México han reducido en estas incidencias.

Para entender mejor el impacto real de los ataques, es útil observar solo las IES que **reportaron al menos un incidente (50,3%).** Este enfoque permite identificar patrones internos y no diluir los datos con instituciones sin afectación:

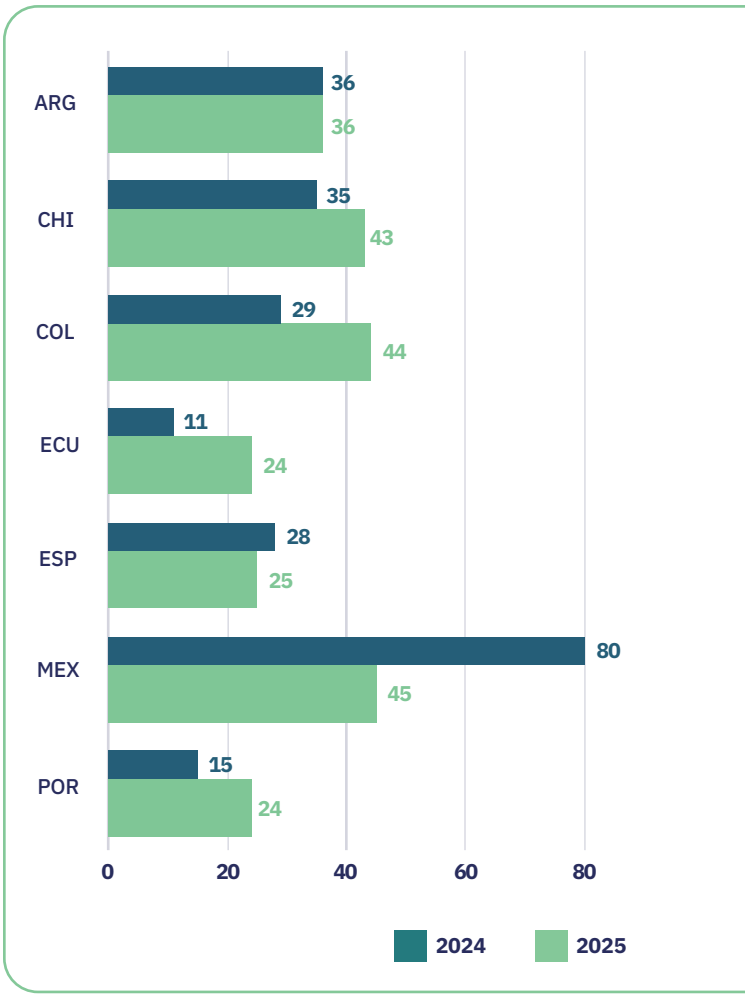
- El **promedio de incidentes por institución afectada** aumenta de 15,9 a 22,1, debido principalmente a unos pocos casos excepcionales con volúmenes muy altos de reportes.
- Sin embargo, la gran mayoría de universidades afectadas reportan **entre uno y cinco incidentes,** y este rango se reduce respecto a 2024.
- En casi todos los países se observa un **descenso en los incidentes severos** (más de 5), el indicador que mejor refleja la estabilidad de los sistemas.

Este patrón —menos IES afectadas, mayor concentración en unos pocos casos— señala que la región avanza en prevención, monitorización y detección, mientras que los desafíos se centran en un número reducido de IES con vulnerabilidades persistentes o mayor exposición a amenazas.

Menos instituciones afectadas pero más incidentes por institución.

El 50,3% de las IES reportan al menos un incidente.

Gráfico 71: Evolución número de incidentes. IMC24 vs. IMC 25.



RELACIÓN ENTRE EL IMC Y LA OCURRENCIA DE CIBERINCIDENTES

El análisis conjunto del nivel de madurez en ciberseguridad (IMC) y del número de incidentes reportados por las instituciones participantes revela una **relación directa entre la capacidad de gestión de la ciberseguridad y la estabilidad operativa de los sistemas universitarios.**

En general, las IES con **mayor puntuación en el IMC experimentan menos incidentes** que afectan a sus servicios críticos. Este patrón se observa de manera consistente en todos los dominios —Gobernar, Identificar, Proteger, Detectar y Responder/ Recuperar—, lo que demuestra que la madurez no depende de un único aspecto técnico, sino de un enfoque integral y equilibrado de la ciberseguridad.

Las instituciones con niveles más altos en **Gobernanza, Gestión de Riesgos y Protección** suelen mostrar una mayor capacidad para anticiparse a las amenazas, implementar controles preventivos y reducir la superficie de exposición. Estos elementos permiten a las IES **evitar incidentes o minimizar su impacto,** reduciendo la probabilidad de recurrencia o escalamiento.

Por su parte, los dominios **Detectar y Responder/ Recuperar** muestran un papel clave en la contención temprana. Las IES con mayor madurez en estas áreas suelen reportar **menos de incidentes severos,** lo que indica que la capacidad de monitorización y reacción temprana contribuye directamente a limitar la extensión del daño.

A nivel agregado, los datos muestran que:

- Las IES con **IMC más elevados reportan en proporción menos incidentes** en 2025.
- Las instituciones con **IMC más bajos** se concentran en los rangos de mayor recurrencia: 2 a 5 incidentes o más de 5.
- En 2025 se observa una **correlación clara:** los países con mayor madurez media también presentan una mayor proporción de IES libres de incidentes o con incidentes aislados.

Las IES con mayor puntuación en el IMC tienden a experimentar menos incidentes.

Este vínculo entre madurez y estabilidad confirma que el IMC no es únicamente una medida de cumplimiento o capacidad teórica, sino un indicador que se **traduce en resultados operativos cuantificables:** menos interrupciones, menor impacto en servicios críticos y mayor resiliencia institucional.

En síntesis, el 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.

4.10 IMC Iberoamericano según la gestión interna de la ciberseguridad

El análisis del IMC 2025 a partir del modelo de gestión interna de la ciberseguridad permite constatar diferencias relevantes en los niveles de madurez alcanzados por las IES. El promedio iberoamericano se sitúa en **1,51,** pero la forma en que las universidades organizan la función de seguridad marca diferencias sustantivas.

Las instituciones con una **gestión centralizada** alcanzan un IMC de **1,53,** ligeramente por encima de la media. Este modelo, caracterizado por concentrar la responsabilidad en un área o equipo específico, favorece la definición de políticas claras y la estandarización de procedimientos. Sus resultados son muy destacables en dominios como **Gobernar (1,58) y Detectar (1,67),** donde la centralización aporta coherencia y facilita el monitoreo.

El **modelo distribuido presenta un IMC de 1,48,** levemente por debajo de la media regional. Aunque este enfoque puede facilitar la integración de la ciberseguridad en diferentes áreas de la institución, los resultados muestran que dispersar responsabilidades sin mecanismos sólidos de coordinación tiende a diluir la efectividad. Aun así, destaca su rendimiento en **Gobernar (1,63) y Proteger (1,62),** lo que refleja que, con estructuras adecuadas, este modelo puede aportar valor en políticas de protección y gestión estratégica.

Por su parte, el modelo **híbrido,** que combina elementos de centralización y distribución, se posiciona con un IMC de **1,40,** claramente por debajo de la media. Aunque en teoría podría reunir las ventajas de los dos enfoques anteriores, los datos de 2025 indican que, en la práctica, la falta de claridad en roles y responsabilidades genera debilidades significativas. Si bien obtiene su mejor resultado en **Infraestructura (2,67),** probablemente ligado a esfuerzos técnicos concretos, en la mayoría de los dominios queda rezagado: **Gobernar (1,34), Proteger (1,65) e Identificar (1,43).**

La gestión centralizada se confirma como el modelo más eficaz en términos de madurez global.

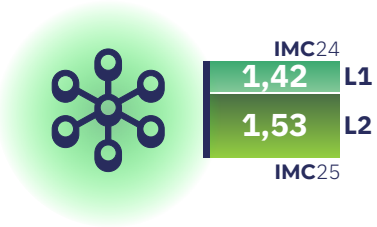
En conjunto, los resultados de este apartado permiten extraer varias conclusiones:

- La **gestión centralizada** se confirma como el modelo más eficaz en términos de madurez global.
- La **gestión distribuida** ofrece resultados intermedios, con avances en algunos dominios, pero dependiente de la coordinación interna.
- El **modelo híbrido,** pese a su potencial, refleja una mayor dificultad de implementación y termina situándose como la opción menos efectiva en 2025.

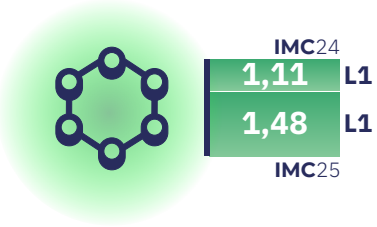
EVOLUCIÓN RESPECTO A 2024

El análisis comparado de los dos últimos años muestra que el **modelo de gestión de la ciberseguridad** tiene un impacto directo en el nivel de madurez alcanzado por las IES en Iberoamérica.

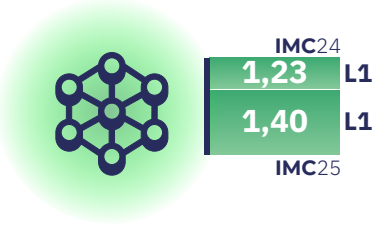
En 2024, el promedio iberoamericano se situaba en **1,37,** con diferencias notables entre los modelos: la gestión **centralizada (1,42)** era la que ofrecía mejores resultados, seguida de la **híbrida (1,23)** y, en último lugar, la **distribuida (1,11).** Estos datos ya apuntaban a la relevancia de contar con estructuras claras y coordinadas, frente a la dispersión de responsabilidades.



En 2025, el IMC global asciende a **1,51,** y con él se observa un crecimiento generalizado en los tres modelos, aunque con distinta intensidad:



- **Centralizada: pasa de 1,42 a 1,53 (+0,11),** manteniéndose como el modelo más sólido y confirmando que la concentración de responsabilidades favorece la coherencia estratégica.
- **Distribuida: evoluciona de 1,11 a 1,48 (+0,36),** registrando la mejora más significativa y reduciendo parte de la brecha con la centralizada. Este salto sugiere un mayor esfuerzo de



coordinación interna, aunque todavía presenta debilidades en dominios como Responder y Recuperar (1,12).

- **Híbrida: mejora de 1,23 a 1,40 (+0,17),** pero sigue siendo el modelo menos eficaz. A pesar de mostrar fortalezas puntuales, como en Infraestructura (2,67), la falta de claridad en roles y responsabilidades limita su madurez global.

El contraste entre 2024 y 2025 confirma que todas las modalidades de gestión avanzan, pero lo hacen a ritmos distintos. La gestión **centralizada** consolida su liderazgo, garantizando mayor consistencia en las políticas de seguridad. La gestión **distribuida,** aunque parte de niveles más bajos, logra un crecimiento notable, lo que demuestra que, con mecanismos adecuados de coordinación, puede convertirse en un modelo viable. En cambio, el enfoque **híbrido** sigue sin materializar su potencial y permanece rezagado, lo que sugiere que combinar centralización y distribución sin una estructura definida tiende a generar más fricciones que beneficios.

De cara al futuro, los resultados apuntan a la importancia de definir con precisión las responsabilidades y capacidades en cada modelo de gestión, más allá del tamaño o los recursos de la institución. La madurez en ciberseguridad no depende solo de invertir más, sino de organizar mejor la función de seguridad y asegurar su coherencia en toda la organización.

5.
IMC Argentina

meta red
by universia

Secretaría General Iberoamericana
Secretaria-Geral Ibero-Americana

IMC 2025
Índice de Madurez en Ciberseguridad de las IES Iberoamericanas

ARG

L0 L1 L2 L3

IMC24
1,06 L1
1,21 L1
IMC25

IMC ARGENTINA
1,21

2024-2025 EVOLUCIÓN
+0,15

IMC IBE DIFERENCIA
-0,30

TIPO DE IES
*evolución sobre IMC IES ARG.

PÚBLICAS
1,01 (+0,15)

PRIVADAS
1,61 (+0,33)

DOMINIOS
*evolución sobre IMC dominios IBE

PROTEGER
1,42 (-0,26)

DETECTAR
1,28 (-0,36)

IDENTIFICAR
1,26 (-0,25)

RESPONDER
1,06 (-0,13)

GOBERNAR
1,05 (-0,50)

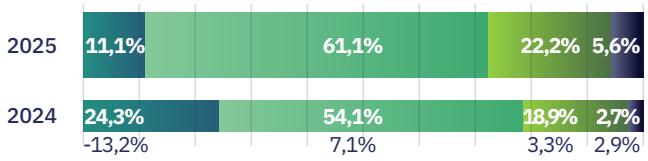
TOP 3
PROTEGER
DETECTAR
IDENTIFICAR

Ninguno supera el IMC25 (1,51).

Valores bajos y alejados de la media: **Gobernar Responder y Recuperar**

Gobernar presenta uno de los valores más bajos de Iberoamérica y se aleja en 0,50 puntos de la media.

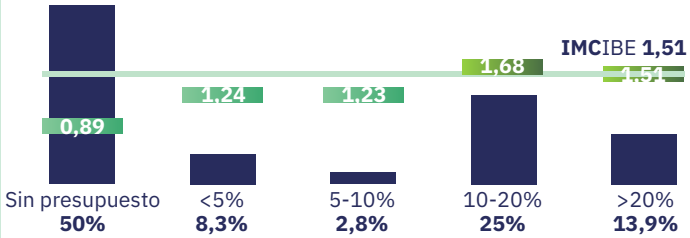
DISTRIBUCIÓN SEGÚN IMC



13,2% menos de IES en el nivel más bajo (inicial, L0)

8 de cada 10 IES argentinas por debajo del nivel intermedio (L2)

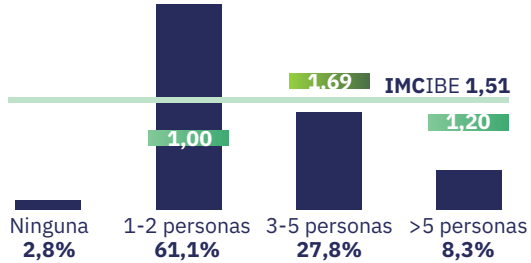
PRESUPUESTO



La mitad de las IES argentinas **no cuentan con presupuesto específico.**

El nivel de madurez de las IES con presupuesto del 10-20% duplica a las que no tienen importe asignado.

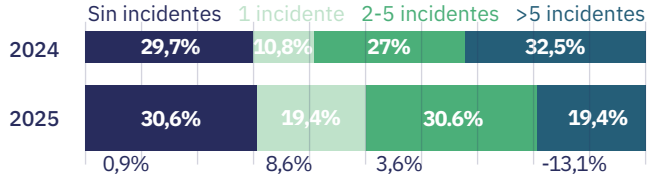
EQUIPOS DE CIBERSEGURIDAD



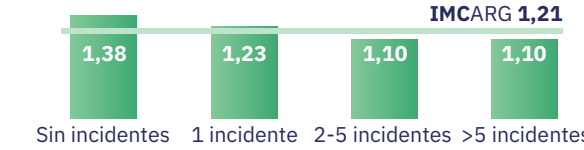
El 92% de equipos de ciberseguridad argentinos están compuestos por 5 o un número menor de personas.

CIBERINCIDENTES

DISTRIBUCIÓN DE LOS INCIDENTES



EVOLUCIÓN DEL IMC SEGÚN Nº DE INCIDENTES



7 de cada 10 IES argentinas han sufrido algún ciberincidente en el último año.

RESUMEN EJECUTIVO ARGENTINA

Argentina ha obtenido un **IMC 2025 de 1,21,** valor que corresponde al **nivel básico (L1)** dentro del modelo de madurez. Esto significa que en promedio, las instituciones de educación superior argentinas aún se encuentran en etapas iniciales de desarrollo de sus capacidades de ciberseguridad, con prácticas menos maduras que las de países más avanzados de la región. El resultado de Argentina quedó notablemente por debajo del promedio iberoamericano, que en 2025 alcanzó **1,51,** manteniéndose 0,30 puntos por debajo de la media regional, casi en la misma proporción que en 2024 (0,31). No obstante, el país mostró una **mejora significativa frente a 2024,** cuando su IMC había sido 1,06. Este aumento de +0,15 es uno de los más altos de la región, equiparable al progreso promedio iberoamericano, lo que podría reflejar un esfuerzo importante de las IES locales por elevar su madurez en ciberseguridad.

Sin embargo, aún con este avance, Argentina **permanece rezagada en el concierto regional** – países como España, Colombia o Brasil presentan niveles de madurez intermedios (L2) superiores, mientras este país sigue en nivel básico (L1).

En síntesis, Argentina logró mejorar su índice de madurez de ciberseguridad, pero **no consiguió cerrar la brecha** respecto al promedio regional.

BRECHA ENTRE UNIVERSIDADES PÚBLICAS Y PRIVADAS

Un análisis crítico revela **diferencias sustanciales de madurez** según el tipo de institución en Argentina. En 2025, las universidades **privadas** del país alcanzaron un IMC medio de **1,61,** superando incluso la media iberoamericana, mientras que las **públicas** apenas promediaron **1,01.** Esta brecha (≈0,60 puntos) **se ha ampliado** respecto a 2024, cuando las privadas marcaban 1,28 vs. 0,85 en las públicas (diferencia de 0,43).

Las cifras evidencian que las IES privadas han acelerado su madurez en el último año mucho más que las públicas. El resultado **invita a una reflexión crítica:** las instituciones públicas, mayoritarias en número y alcance, estarían encontrando obstáculos para desarrollar sus capacidades de ciberseguridad al mismo ritmo. Si bien ambos subsectores mejoraron su desempeño, las privadas muestran prácticas más formalizadas y recursos mejor aplicados, mientras que las universidades públicas **quedan rezagadas en aspectos clave.**

Esta disparidad, lejos de fomentar rivalidad, señala **un desafío para el país:** es necesario elevar el apoyo estructural y estratégico en el sector público para cerrar la brecha, atendiendo a que la ciberseguridad en la academia debe avanzar de manera homogénea. En particular, dominios como gobierno de la seguridad, procedimientos formales y asignación de presupuesto presentan diferencias marcadas a favor de las privadas, lo que sugiere que las universidades públicas requieren **mayor inversión y enfoque institucional** para no quedar vulnerables frente al creciente panorama de riesgos.

DISTRIBUCIÓN DE NIVELES DE MADUREZ EN LAS IES

La distribución del nivel de madurez entre las IES argentinas refleja un **predominio del nivel básico** con algunas mejoras en los extremos. En 2025, más de **60%** de las instituciones se ubican en **nivel L1 (básico),** mientras que alrededor de **22%** alcanzan el **nivel L2 (intermedio)** y **apenas 5,6% llegaron a L3 (avanzado).**

Aunque el grueso de las IES sigue operando con madurez limitada, esta distribución muestra un **avance respecto al año anterior:** en 2024 el nivel L0 (incipiente/inexistente) abarcaba un preocupante 24%. Sin embargo, esta proporción se redujo a **11% en 2025.** Es decir, varias universidades lograron salir del escalón más bajo de madurez. En consecuencia, aumentó tanto la proporción en L1 (de 54% a 61%) como en L2-L3 combinados (de 22% a 28%).

En términos generales, Argentina ha desplazado lentamente su base hacia mayor madurez, con menos instituciones completamente rezagadas y el doble de organizaciones en el nivel más alto (aunque L3 siga representando una minoría exigua del 5,6%).

Este panorama sugiere un **estado nacional todavía poco homogéneo:** la mayoría de las IES están en una etapa básica de madurez, con esfuerzos aislados que logran niveles intermedios o avanzados. El reto a futuro será **elevar el piso común de madurez** –reducir ese ~61% en nivel básico– para que más instituciones alcancen estándares intermedios, consolidando un estado general más robusto en ciberseguridad.

DESEMPEÑO POR DOMINIOS

El perfil de madurez de Argentina varía al examinar los dominios y subdominios específicos del modelo IMC, revelando **fortalezas técnicas y debilidades organizacionales.** Entre los cinco dominios principales, el país se desempeña mejor en **Proteger (PR),** con un valor promedio de **1,42,** seguido de cerca por **Detectar (DE)** con **1,28** e **Identificar (ID)** con **1,26.** Esto indica que las IES argentinas han avanzado en la implementación de controles de protección (ej.: medidas de seguridad en infraestructura, gestión de accesos, protección de datos) y en cierta medida en la identificación de activos y riesgos. En contraste, los dominios de **Gobernar (GB)** y **Responder y Recuperar (REyRC) presentan los puntajes más bajos (≈1,05–1,06),** reflejando rezagos en la gestión estratégica y la capacidad de **respuesta a incidentes.** De hecho, la respuesta a incidentes es el área más débil a nivel de dominio (1,06), lo cual sugiere que los procedimientos de detección, contención y recuperación ante ataques no están plenamente desarrollados.

Si analizamos subdominios destacables, sobresale **Infraestructura** (dentro del dominio Proteger) como **punto fuerte claro:** las universidades argentinas alcanzan en este subdominio un nivel cercano al intermedio-alto **(IMC ≈2,33 en 2025).** Esto implica que la protección de infraestructura tecnológica (redes, sistemas y centros de datos) está bastante madura, probablemente gracias a la adopción de herramientas y prácticas técnicas sólidas. También el subdominio **Comunicaciones** (seguridad en redes y comunicaciones) muestra un desempeño relativamente alto (cercano a 2,0), aunque se estancó en su mejora. En el lado opuesto, resaltan **deficiencias notables en subdominios de gobernanza:** por ejemplo, **Presupuesto** obtiene uno de los valores más bajos **(0,78),** evidenciando una **escasa asignación específica de recursos** para ciberseguridad y falta de planificación financiera en la materia. Asimismo, el subdominio **Normativa** (políticas y regulaciones internas) permanece débil con valor ~0,86, señal de que muchas IES carecen de políticas formales y marco normativo actualizado en seguridad. Otros aspectos de gobierno como **Responsabilidad** (roles y responsabilidades claras) también se mantienen por debajo de 1.0 en promedio. Estas brechas indican que, si bien Argentina ha avanzado en **medidas técnicas de protección,** aún adolece de **madurez en las dimensiones organizativas:** faltan estrategias integrales, políticas robustas, asignación presupuestaria adecuada y procesos documentados que sustenten la ciberseguridad de forma sistemática.

En resumen, **el desempeño por dominios es dispar** – fuerte en lo tecnológico-operativo, débil en gobierno y respuesta – lo que sugiere que el país deberá enfocarse en fortalecer los cimientos institucionales y procedimentales de la seguridad para equilibrar su perfil de madurez.

IMPACTO DEL TAMAÑO DEL EQUIPO DE CIBERSEGURIDAD

Los datos confirman la **correlación positiva entre el tamaño del equipo dedicado de seguridad y el nivel de madurez** de la institución, reforzando el vínculo observado en 2024.

Las IES argentinas que cuentan con **equipos más nutridos muestran una madurez muy superior** respecto de las que carecen de personal

especializado. En 2024, por ejemplo, las universidades con **3 a 5 profesionales** en ciberseguridad obtuvieron un IMC promedio de **1,52,** e incluso aquellas con **más de 5 personas** alcanzaron **1,51;** en cambio, las instituciones sin **ningún especialista dedicado** apenas lograron **0,62**; un nivel prácticamente incipiente.

De forma similar, en 2025 **se reafirma esta tendencia:** las IES con equipos de seguridad medianos (3-5 integrantes) lideraron con un IMC cercano a **1,69,** mientras que las que **no cuentan con un equipo** permanecieron alrededor de **1,0** (nivel básico). Incluso las organizaciones con solo **1 o 2 personas** dedicadas quedaron rezagadas, rondando IMC 1.0 en 2025.

Estas diferencias evidencian que **disponer de un equipo específico de ciberseguridad resulta crucial para elevar la madurez:** las instituciones con mayor personal pueden implementar más controles, especializar funciones (ej. análisis de riesgos, monitoreo, respuesta a incidentes) y sostener programas de mejora continua, alcanzando niveles de madurez notablemente más altos. Por el contrario, aquellas sin equipo dedicado –probablemente dependiendo de personal de TI generalista o externalizando en mínima medida– **no logran superar el nivel básico.** Este patrón, ya observado en el IMC 2024, se consolida en 2025 y envía un mensaje claro a las IES: **invertir en capital humano especializado en seguridad es un factor determinante** para avanzar en el modelo de madurez.

INFLUENCIA DEL PRESUPUESTO EN CIBERSEGURIDAD

De forma análoga al recurso humano, la **asignación de presupuesto específico en ciberseguridad** –y su peso relativo dentro del gasto de TI– tiene un impacto directo en el nivel de madurez alcanzado por las IES. Los datos de Argentina muestran una relación lógica: **mayor inversión, mayor madurez.** Aquellas instituciones que destinan una proporción elevada de su presupuesto de TI a seguridad obtienen **métricas de madurez muy superiores** a las que invierten poco.

En 2024, las universidades que asignaban **más del 10%** de su presupuesto de TI a ciberseguridad lograron IMC promedio en el rango **1,5–1,8,** con las de asignaciones **>20%** rozando el 1,77. En cambio, las IES con presupuesto **mínimo (<5%)** quedaron cerca de **0,8,** e incluso varias sin un presupuesto discernible para seguridad apenas promediaron ~0,9.

Esta brecha se mantuvo en 2025: las instituciones con **mayores partidas (>10%)** alcanzaron aproximadamente **1,68,** mientras que las de inversión marginal (por ejemplo las que declararon **0% del presupuesto** en seguridad) no superaron **0,9.** Cabe destacar que entre el rango bajo y medio (por ejemplo, entre destinar <5% vs. 5-10%) ya se aprecia un salto positivo de madurez (del orden de 0,9 a 1,2). En suma, **la proporción del presupuesto de TI dedicada a ciberseguridad guarda una relación proporcional con el IMC:** las IES que incorporan la seguridad como prioridad presupuestaria logran implementar mejores controles, herramientas y personal, reflejándose en niveles de madurez mayores.

Argentina, no obstante, evidencia que muchas instituciones aún **no asignan recursos suficientes** – el subdominio de Presupuesto fue uno de los más bajos del país, indicando que la inversión en ciberseguridad suele ser reducida. Este factor presupuestario, combinado con el tamaño del equipo, conforma un **eje crítico de mejora:** para transitar del nivel básico al intermedio, las IES argentinas necesitan respaldar sus políticas con **financiamiento adecuado y sostenido** en materia de seguridad digital.

INCIDENTES DE SEGURIDAD: EVOLUCIÓN Y RELACIÓN CON LA MADUREZ

La cantidad de **incidentes de seguridad registrados** en las IES argentinas proporciona otro indicador importante, tanto de la **exposición**

a amenazas como de la efectividad de las capacidades de seguridad desarrolladas.

En el último año analizado, Argentina reportó una ligera **disminución en el número de incidentes críticos:** el número promedio de incidentes anuales por institución bajó de **10,33 en 2024 a 9,94 en 2025.** Del mismo modo, entre aquellas universidades que sufrieron al menos un incidente, el promedio descendió levemente de **14,88 a 14,32 incidentes,** lo cual sugiere que, aunque los incidentes continúan siendo frecuentes, **su intensidad o recurrencia se habría moderado** ligeramente.

Esta tendencia es congruente con los esfuerzos de mejora en madurez: a mayor madurez, se esperarían mejores medidas preventivas y de detección, contribuyendo a contener el número de incidentes exitosos.

No obstante, el panorama de incidentes sigue siendo delicado. En 2024, **solo el 30% de las IES argentinas no reportó incidentes** de seguridad, mientras que el **70% restante sufrió uno o más.** De hecho, casi **un tercio (32%) enfrentó más de 5 incidentes** en el año – una cifra alta que evidencia la presión constante de ciberataques o fallas de seguridad en el sector. Esta realidad resalta la importancia de fortalecer capacidades de **detección y respuesta** (dominios donde Argentina está rezagada), ya que la mayoría de instituciones se ven efectivamente impactadas por incidentes de distinto grado.

Al explorar la **relación entre el nivel de madurez y la incidencia de incidentes,** emergen hallazgos interesantes y algo contraintuitivos. En la medición de 2024 se observó que, paradójicamente, **las instituciones con mayor número de incidentes reportados tendían a tener un IMC más alto.** Por ejemplo, las IES que sufrieron **más de 5 incidentes** alcanzaban en promedio un nivel de madurez **1,34,** superior al de aquellas **sin incidentes** (IMC 0,88). Esto puede interpretarse así: las universidades más grandes o avanzadas detectan y reportan más incidentes (por su exposición y capacidad de monitoreo), mientras las menos maduras quizá no registran incidentes ya sea por su pequeño tamaño o por falta de mecanismos de detección, generando una suerte de correlación positiva entre incidentes y madurez en 2024.

Sin embargo, en 2025 este patrón **parece haberse invertido.** Los datos muestran que las pocas instituciones que lograron **no tener incidentes** en el último año son ahora las de mayor madurez (IMC **1,38),** superando a aquellas con muchos incidentes (>5), que promedian alrededor de **1,10.** Es decir, conforme se eleva la madurez, las IES serían más eficaces en **prevenir y resistir incidentes,** rompiendo la tendencia previa. Posiblemente, las mejoras implementadas (p.ej. mejores controles preventivos o respuesta temprana) están evitando que los ataques deriven en incidentes significativos en las instituciones más avanzadas. Aun así, las organizaciones con 1 o pocos incidentes mantienen niveles de madurez intermedios (ej.: IMC 1,23 con un solo incidente), lo que sugiere que un **nivel básico de madurez conlleva seguir enfrentando varios incidentes.**

En conclusión, aunque el número de incidentes en Argentina sigue siendo alto, se observa una **leve reducción en frecuencia y un cambio en la dinámica** con la madurez: las IES más maduras están logrando contener mejor los incidentes, mientras que las menos maduras continúan expuestas. Esto realza la importancia de seguir elevando el nivel de madurez como vía para **reducir el impacto de los incidentes de seguridad** en el sistema universitario.

USO DE LA INTELIGENCIA ARTIFICIAL EN CIBERSEGURIDAD

El uso de inteligencia artificial (IA) en las tareas de ciberseguridad sigue siendo muy limitado en las instituciones de educación superior argentinas. Solo una fracción pequeña de IES declara emplearla en alguno de los dominios evaluados, con porcentajes de adopción que se sitúan, según el ámbito, entre el 2,8% y el 16,7%. Es decir, estamos ante una práctica todavía excepcional y en fase exploratoria.

En los datos del IMC se observa que, en varios dominios, **las instituciones que usan IA tienden a mostrar valores de madurez algo más altos que las que no la utilizan.** Ocurre, por ejemplo, en funciones como Identificar, Proteger, Detectar o Responder, donde las diferencias se sitúan, en general, en el rango de unas pocas décimas. Sin embargo, esta mejora no puede atribuirse de forma directa a la IA: es razonable pensar que las IES que se animan a experimentar con estas tecnologías son, en muchos casos, instituciones ya más estructuradas, con mayor capacidad técnica, organizativa y presupuestaria.

De hecho, el propio detalle de los resultados invita a la prudencia. Hay subdominios donde las IES sin IA presentan valores iguales o incluso superiores a las que sí la usan, especialmente en aspectos ligados a **infraestructura, procedimientos consolidados o ciertas actividades de detección,** dependiendo del dominio analizado. Además, el número de instituciones que declara utilizar IA es tan reducido que cualquier variación individual puede distorsionar las medias.

Más que una "prueba" de que la IA incrementa por sí sola la madurez, los datos parecen apuntar a otra lectura: **las IES que ya tienen un recorrido mayor en ciberseguridad son las que empiezan antes a explorar la IA** como un recurso complementario. Es decir, la IA aparece asociada a entornos que ya venían trabajando la gestión de riesgos, la continuidad, la monitorización o la respuesta a incidentes, y que ahora prueban nuevas herramientas para ganar eficiencia o visibilidad.

En este contexto, la IA se perfila como un posible factor de diferenciación a medio plazo, pero todavía **no hay evidencias suficientes para hablar de un impacto directo y generalizado en el IMC.** Lo que sí muestran los datos es una brecha incipiente entre un grupo muy reducido de pioneros y una mayoría de IES que aún no ha dado ese paso.

Adopción mínima de la IA en ciberseguridad y resultados condicionados por el contexto institucional.

En síntesis, el uso de IA en ciberseguridad en las IES argentinas es hoy **claramente minoritario y aún incipiente.** Las instituciones que la están probando tienden a obtener mejores resultados de madurez, pero es probable que ello refleje sobre todo un mayor grado de desarrollo previo en sus capacidades de ciberseguridad. El reto de los próximos años será comprobar si a medida que la IA se consolide y extienda, esas experiencias se traducen en mejoras tangibles y sostenidas para el conjunto del sistema.

6.
IMC Brasil

meta red
by universia

Secretaría General Iberoamericana
Secretaria-Geral Ibero-Americana

IMC 2025
Índice de Madurez en Ciberseguridad de las IES Iberoamericanas

BRA

L0 L1 L2 L3

1,55 L2

IMC25

IMC BRASIL

1,55

IMC IBE DIFERENCIA

+0,04

TIPO DE IES

PÚBLICAS 1,31

PRIVADAS 1,64

DOMINIOS

*evolución sobre IMC dominios IBE

PROTEGER 1,75 (+0,07)

DETECTAR 1,68 (+0,04)

GOBERNAR 1,59 (+0,04)

IDENTIFICAR 1,54 (+0,03)

RESPONDER 1,28 (+0,09)

TOP 3

PROTEGER

DETECTAR

GOBERNAR

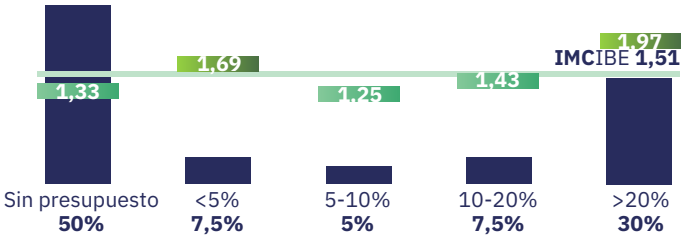
Proteger, Detectar Gobernar e Identificar superan la media de iberoamérica. En particular, destaca el 1,75 de Proteger.

Responder y Recuperar presenta el valor más bajo (1,28) para el país. Sin embargo, supera la media iberoamericana para dicho dominio (1,19).

DISTRIBUCIÓN SEGÚN IMC

7 de cada 10 IES brasileñas están en los niveles básico (L1) e intermedio (L2), repartidas en proporciones prácticamente similares.

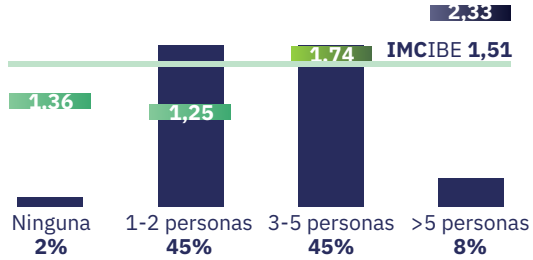
PRESUPUESTO



La mitad de las IES **no cuentan con presupuesto específico.**

El nivel de madurez más alto (1,97, casi L3) es de aquellas con un presupuesto asignado de más del 20%.

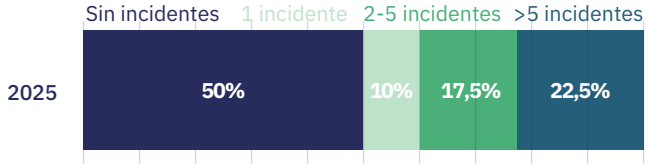
EQUIPOS DE CIBERSEGURIDAD



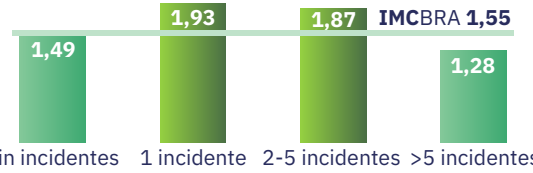
Más del 90% están compuestos por menos de 5 personas. El IMC alcanza el mayor valor para las IES con equipos de más de 5 personas (2,33, nivel L3).

CIBERINCIDENTES

DISTRIBUCIÓN DE LOS INCIDENTES



EVOLUCIÓN DEL IMC SEGÚN Nº DE INCIDENTES



8 de cada 10 IES brasileñas han sufrido algún ciberincidente en el último año.

RESUMEN EJECUTIVO BRASIL

Brasil se incorpora con uno de los niveles de madurez más elevados de toda Iberoamérica.

Brasil participa por primera vez en el Índice de Madurez en Ciberseguridad (IMC) en 2025. Al no existir datos correspondientes a 2024, no es posible realizar un análisis evolutivo comparable al del resto de países. Será en las próximas ediciones cuando se podrá observar la trayectoria del país y evaluar con mayor precisión la consolidación de sus capacidades. No obstante, la fotografía inicial que ofrece 2025 es ya muy relevante y sitúa a Brasil como uno de los ecosistemas universitarios más maduros del estudio.

En 2025, Brasil obtiene un **IMC promedio de 1,55,** superando el promedio regional (1,51) y situándose muy por encima de la mayoría de países evaluados. Aunque muy próximo al nivel 1. se encuentra dentro del nivel intermedio (L2), , lo que es particularmente significativo para un país que participa por primera vez. Este resultado sugiere la existencia de un ecosistema universitario con **capacidad técnica consolidada,** infraestructuras maduras y una aproximación general a la ciberseguridad más estructurada que la de otros países latinoamericanos que llevan varios años en el estudio.

DISTRIBUCIÓN DE NIVELES DE MADUREZ

La distribución de niveles confirma el buen punto de partida del país, pero debe interpretarse con cierta prudencia. Un poco más del **7%** de instituciones brasileñas aparece en el nivel incipiente (L0), algo poco habitual en el contexto iberoamericano. Cerca del **33%** de las instituciones se sitúan en nivel básico (L1), mientras que el **40%** opera ya en el nivel intermedio (L2). El resto representadas por un **20%** se sitúa en el nivel avanzado (L3). Este resultado sugiere un ecosistema sin capas especialmente rezagadas y con una base de capacidades relativamente extendida.

No obstante, esta lectura debe matizarse: Brasil cuenta con **un sistema universitario muy amplio y heterogéneo,** y el conjunto de instituciones participantes en 2025 representa solo una parte del total. Esto implica que, aunque los datos disponibles presentan una imagen sólida, no pueden extrapolarse automáticamente a todo el país sin considerar posibles sesgos de participación, como una mayor presencia de instituciones con más recursos o mejor organización interna.

Luego de España y ocupando el segundo lugar junto a Colombia cuenta con **20%** de IES en nivel avanzado (L3). Si esta tendencia se mantiene en futuras ediciones —y se amplía la diversidad de instituciones participantes— Brasil podría situarse entre los países con mayor probabilidad de alcanzar una masa crítica de instituciones en niveles superiores. Pero, de momento, esta posibilidad debe tomarse **con cautela,** ya que se requieren datos de continuidad y una participación más amplia para confirmar esta afirmación con un nivel adecuado de solidez

DESEMPEÑO POR DOMINIOS

Un perfil técnico muy robusto y una gobernanza que acompaña pero aún puede fortalecerse.

Brasil destaca especialmente en los dominios **Proteger y Detectar,** donde obtiene valores de **1,75 y 1,68,** respectivamente, situándose entre los más altos de todo el estudio. Estos resultados reflejan la existencia de una **infraestructura sólida,** buenas prácticas en comunicaciones, un entorno tecnológico cuidado y mecanismos de supervisión y vigilancia bien establecidos. El dominio **Identificar** también presenta un resultado notable **(1,54),** lo que indica que las instituciones gestionan de forma consistente sus activos, riesgos y dependencias.

Los dominios **Gobernar (1,59) y Responder y Recuperar (1,28)** presentan valores igualmente superiores al promedio regional, aunque con un margen mayor para mejorar. En ambos casos, los resultados sugieren que el país dispone de políticas, roles y procedimientos básicos, pero que aún no se encuentran plenamente desarrollados. En particular, la capacidad de **respuesta y recuperación** es buena, pero podría consolidarse con procesos más formales y mecanismos más homogéneos entre instituciones. En conjunto, Brasil ofrece un perfil técnico y una estructura organizativa bien encaminada, aunque todavía en fase de consolidación.

BRECHA ENTRE INSTITUCIONES PÚBLICAS Y PRIVADAS

El sector privado muestra una ventaja clara y sostenida en casi todos los dominios.

La comparación entre instituciones públicas y privadas revela una brecha marcada, mayor que en la mayoría de países participantes. Las instituciones privadas registran un IMC promedio de **1,64,** mientras que las públicas se sitúan en **1,31,** una diferencia amplia que aparece de forma consistente en todos los dominios del modelo. La distancia es especialmente significativa en **Gobernar, Identificar y Detectar,** donde las privadas alcanzan valores elevados —en algunos casos muy cercanos a 2,0— mientras que las públicas permanecen en niveles más moderados.

Este patrón sugiere que las instituciones privadas cuentan con **procesos más formalizados,** mejores esquemas de supervisión y planificación, mayor autonomía para invertir en tecnologías de seguridad y equipos más especializados. Por el contrario, las instituciones públicas muestran una madurez sólida pero menos homogénea, probablemente condicionada por limitaciones de gestión, disponibilidad presupuestaria o estructuras organizativas más rígidas. Aunque esto no implica que las públicas estén en una posición débil —sus resultados superan al promedio regional—, sí evidencia que **la brecha interna en Brasil es mayor que la de otros países,** y que la convergencia entre ambos sectores requerirá un esfuerzo adicional.

IMPACTO DEL TAMAÑO DE LOS EQUIPOS DE CIBERSEGURIDAD

Equipos estables y presencia mínima garantizada: una base sólida que sostiene la madurez del país.

A diferencia de otros países donde una parte significativa de instituciones carece de personal dedicado, en Brasil **todas excepto una de las participantes cuentan con al menos un equipo básico de seguridad,** lo cual ya supone un

indicador importante de madurez estructural. En 2025, las instituciones con **1–2 profesionales** presentan un IMC de **1,25,** mientras que aquellas con **3–5 personas alcanzan 1,74,** y las pocas que cuentan con **más de 5 integrantes llegan a 2,33.** La progresión es clara: a mayor tamaño del equipo, mayor madurez.

El hecho de que prácticamente no existan instituciones sin personal dedicado contribuye a explicar por qué Brasil parte de un nivel de madurez alto y homogéneo. En este contexto, el tamaño del equipo funciona más como un **acelerador gradual,** que permite mejorar especialmente los dominios técnicos, que como un factor de ruptura entre instituciones. Aun así, el patrón general coincide con el del resto de la región: el salto más relevante se produce cuando se pasa de grupos muy pequeños a equipos ya medianos, que permiten asumir más tareas, documentar procesos y sostener actividades de mejora continua.

INFLUENCIA DEL PRESUPUESTO EN CIBERSEGURIDAD

La relación entre inversión y madurez es especialmente fuerte en Brasil.

El presupuesto es un factor claramente diferenciador en Brasil. **Las instituciones que no destinan presupuesto TI a seguridad alcanzan un IMC de 1,33, mientras que las que invierten más del 20% llegan a 1,97.** Estos resultados muestran una correlación particularmente nítida entre inversión y madurez: cuanto mayor es la asignación presupuestaria, más sólido es el desempeño en los dominios técnicos y organizativos. El perfil de Brasil difiere así del de otros países donde la relación es más irregular o depende de otros factores, como la gobernanza o la disponibilidad de equipos. En Brasil, la inversión económica parece traducirse de forma más directa en capacidades tangibles y sostenibles.

Sin embargo, estos datos deben de tratarse con cautela dado el contexto particular del país, con un gran número de instituciones públicas y privadas. Por lo tanto, al igual que años anteriores con otros países, será importante realizar una monitorización de la evolución anual avalada o reforzada por un mayor número de instituciones participantes.

INCIDENTES DE SEGURIDAD

Perfil estable y homogéneo: los incidentes no diferencian el nivel de madurez.

Brasil presenta un comportamiento similar a otros países de la región en materia de incidentes. En 2025, las IES que no reportaron incidentes presentan un valor promedio de 1,49 (L1, Básico), frente al 1,55 (L2, Intermedio) del promedio nacional.

En las instituciones que sí han sufrido algún ciberincidente en este periodo, el valor de madurez obtenido es superior y asciende a valores de 1,93 y 1,87 para las IES que han reportado 1 ciberincidente y entre 2 y 5 ciberincidentes, respectivamente. Este dato sugiere, o podría interpretarse, como una mejora en el nivel de madurez reactiva a situaciones que han podido comprometer ciertos sistemas corporativos.

Uno de los países con mayor adopción:

la IA amplifica capacidades ya consolidadas.

Brasil adopta en forma moderada la IA según el estudio. En 2025, el uso de inteligencia artificial se concentra en los dominios técnicos: **Identificar (20%), Proteger (22,5%) y Detectar (17,5%),** mientras que su presencia en **Responder y Recuperar es más reducida (7,5%) y (15%) en Gobernar y Formación.**

Las instituciones que emplean IA obtienen valores sensiblemente superiores en madurez, especialmente en los dominios técnicos, lo que sugiere que esta tecnología actúa como un **refuerzo natural** de capacidades ya existentes. Sin embargo, como en otros países, es importante evitar conclusiones deterministas: el uso de IA puede ser tanto consecuencia como causa parcial de la madurez. Lo más probable es que las instituciones que ya contaban con prácticas sólidas y equipos especializados fueran precisamente las primeras en incorporar estas herramientas.

En conjunto, Brasil presenta un escenario donde la IA no es todavía un elemento transversal, pero sí un **complemento significativo** que potencia la fortaleza técnica del sistema y anticipa una posible expansión hacia dominios más organizativos en futuras ediciones.

7.

IMC Chile

metared
by universia

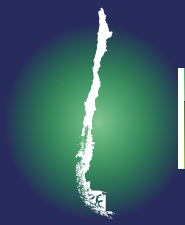
Secretaría General
Iberoamericana

Secretaria-Geral
Ibero-Americana

IMC 2025

Índice de Madurez en Ciberseguridad
de las IES Iberoamericanas

CHI



IMC24
1,47 L1
1,50 L2
IMC25

IMC CHILE
1,50

2024-2025 EVOLUCIÓN
+0,03

IMC IBE DIFERENCIA
-0,01

L0 L1 L2 L3

TIPO DE IES

*evolución sobre IMC IES CHI.

PÚBLICAS
1,17 (-0,01)

PRIVADAS
1,66 (+0,08)

DOMINIOS

*evolución sobre IMC dominios IBE

DETECTAR
1,68 (+0,04)

PROTEGER
1,62 (-0,06)

GOBERNAR
1,61 (+0,06)

IDENTIFICAR
1,45 (-0,06)

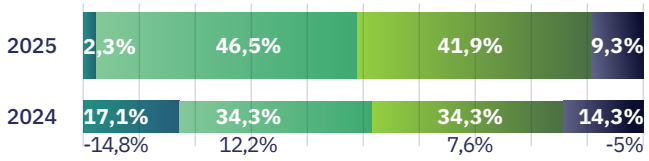
RESPONDER
1,16 (-0,03)

TOP 3
DETECTAR
PROTEGER
GOBERNAR

Detectar (1,68), Proteger (1,62) y Gobernar (1,61) obtienen la mejor puntuación y superan la media Iberoamérica (1,51).

Valores bajos: **Identificar (1,45) y Responder y Recuperar (1,16),** este último se aleja 0,35 de la media iberoamericana.

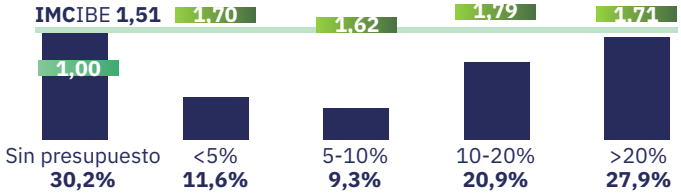
DISTRIBUCIÓN SEGÚN IMC



14,8% menos de IES en el nivel más bajo (inicial, L0), reduciéndose tan solo al 2,3%.

5 de cada 10 IES chilenas por debajo del nivel intermedio (L2).

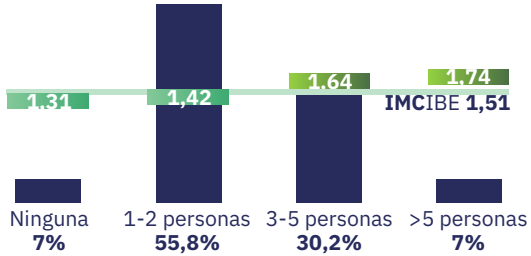
PRESUPUESTO



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

El nivel de madurez de las IES aumenta con la asignación de un presupuesto del 5% o mayor.

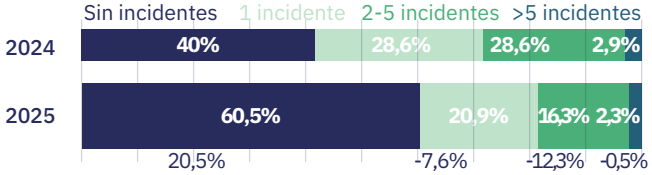
EQUIPOS DE CIBERSEGURIDAD



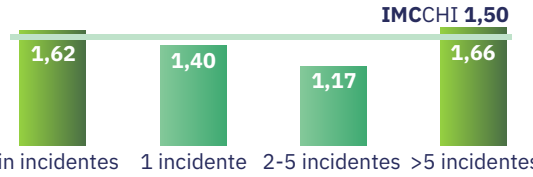
Más del 90% están compuestos por menos de 5 personas. Se observa una clara relación directa entre el tamaño de los equipos de seguridad y el nivel de madurez.

CIBERINCIDENTES

DISTRIBUCIÓN DE LOS INCIDENTES



EVOLUCIÓN DEL IMC SEGÚN Nº DE INCIDENTES



4 de cada 10 instituciones chilenas han sufrido algún ciberincidente en el último año.

RESUMEN EJECUTIVO CHILE

Chile ha obtenido un IMC 2025 de **1,50,** un valor que se sitúa en el límite inferior del nivel intermedio (L2) del modelo de madurez. Esto significa que en promedio, las instituciones de educación superior chilenas han alcanzado un grado de desarrollo de sus capacidades de ciberseguridad cercano a las etapas intermedias, aunque todavía no plenamente consolidado. El resultado de Chile prácticamente calca el promedio iberoamericano, situado en **1,51,** quedando 0,01 puntos por debajo de esa media. Mientras que en el año 2024, Chile se mantenía 0,10 puntos por encima de la media iberoamericana.

A nivel de evolución anual, Chile muestra **una mejora prácticamente nula** frente a 2024, cuando su IMC había sido de 1,47. El incremento de solo **+0,03** puntos evidencia un estancamiento en el último año, muy por debajo del progreso promedio iberoamericano (~+0,14). Mientras el conjunto de la región avanza de manera significativa, la madurez de ciberseguridad chilena se mantiene casi plana, haciendo que el país pierda la ligera ventaja relativa que ostentaba. Aun con un punto de partida relativamente alto, Chile no ha logrado impulsar su índice de forma notable y ha quedado rezagado en la dinámica de mejora respecto a sus pares. Países como España, Colombia o Brasil presentan niveles de madurez intermedios (L2) más altos, mientras Chile permanece apenas en el umbral entre el nivel básico e intermedio. En síntesis, el país ha mantenido su índice de madurez de ciberseguridad prácticamente sin avances, y **no ha conseguido capitalizar su posición previa** ligeramente superior al promedio regional.

BRECHA ENTRE UNIVERSIDADES PÚBLICAS Y PRIVADAS

Un análisis por tipo de institución revela **diferencias marcadas de madurez** en Chile según el sector. En 2025, las universidades **privadas** del país alcanzaron un IMC medio de **1,66,** superando incluso la media iberoamericana, mientras que las **públicas** apenas promediaron **1,17.** Esta brecha (≈0,49 puntos) se ha ampliado respecto a 2024, cuando las privadas marcaban 1,58 vs. 1,18 en las públicas (diferencia de 0,40). Las cifras evidencian que las IES privadas han acelerado su madurez en el último año mucho más que las públicas.

El resultado invita a una reflexión: las instituciones públicas estarían encontrando **obstáculos para desarrollar sus capacidades de ciberseguridad** al mismo ritmo. Si bien ambos subsectores han participado del incremento global de Chile (con un marcado avance en concentrado en niveles básicos e intermedios. Consecuentemente, aumentó la proporción conjunta en L1+L2 (de 69% en 2024 a ~88% en 2025), aunque disminuyó ligeramente en el caso privado y menos acusado en el público), las privadas muestran prácticas más formalizadas y recursos mejor aplicados, mientras que las universidades públicas quedan rezagadas en aspectos clave. Esta disparidad, podría señalar la necesidad de **elevar el apoyo estructural y estratégico en el sector público** para cerrar la brecha, atendiendo a que la ciberseguridad en la academia debe avanzar de manera homogénea. En particular, dominios como el gobierno de la seguridad, los **procedimientos formales y la asignación de presupuesto** presentan diferencias marcadas a favor de las privadas, lo que sugiere que las universidades públicas requieren mayor inversión y enfoque institucional para no quedar vulnerables frente al creciente panorama de riesgos.

DISTRIBUCIÓN DE NIVELES DE MADUREZ EN LAS IES

La distribución del nivel de madurez entre las IES chilenas refleja un **desplazamiento hacia niveles superiores,** con menos instituciones en el extremo más bajo. En 2025, casi **la mitad** de las IES se ubica en nivel L1 (básico, 46,5%) y una proporción muy cercana alcanza L2 (intermedio, 41,9%). Solo 9,3% logra el nivel L3 (avanzado), mientras que apenas un 2,3% permanece en nivel L0 (incipiente). En comparación, el año anterior

presentaba **más instituciones rezagadas:** en 2024 el nivel L0 abarcaba 17,1% de las IES y el avanzado L3 llegaba a 14,3%. Es decir, en el último año muchas universidades han salido del escalón incipiente (reduciendo L0 de 17% a 2%) y se han concentrado en niveles básicos e intermedios. Consecuentemente, aumentó la proporción conjunta en L1+L2 (de 69% en 2024 a ~88% en 2025), aunque **disminuyó ligeramente el porcentaje en L3** (de 14,3% a 9,3%).

Este panorama sugiere que Chile **ha fortalecido su base de madurez** al prácticamente eliminar los casos en nivel inexistente; ahora prácticamente todas las IES cuentan al menos con capacidades básicas. Sin embargo, la mayoría (casi 47%) continúa operando en un nivel básico de madurez, y solo una minoría (<10%) alcanza un estadio avanzado. La distribución **no es aún homogénea:** la mayor parte de instituciones se encuentra en etapas iniciales o medias, con unos pocos casos destacados en la cúspide. El **reto a futuro** radica en seguir empujando el piso hacia arriba –es decir, reducir ese 47% en nivel básico– de modo que más IES asciendan a niveles intermedios y avanzados. Si bien 2025 muestra progresos (menos "colas" en L0), Chile debe aspirar a **consolidar un estado general más robusto,** incrementando el porcentaje de instituciones al menos en nivel L2 para fortalecer la resiliencia colectiva en ciberseguridad.

DESEMPEÑO POR DOMINIOS

El perfil de madurez de Chile varía al examinar los dominios y subdominios del modelo IMC, revelando **fortalezas de corte técnico-operativo y debilidades en la respuesta e inversión.** Entre los cinco dominios principales, el país se desempeña mejor en **Detectar (DE)** con un valor promedio de **1,68,** seguido muy de cerca por **Proteger (PR, 1,62) y Gobernar (GB, 1,61).** Esto indica que las IES chilenas han implementado con relativo éxito controles de monitoreo, protección de infraestructura y ciertos aspectos de gestión de la seguridad.

En contraste, el dominio de **Responder y Recuperar (REyRC)** presenta el puntaje más bajo (IMC **1,16),** reflejando rezagos importantes en la **capacidad de respuesta a incidentes.** Igualmente, **Identificar (ID, 1,45)** se mantiene en un nivel apenas básico-intermedio. En síntesis, Chile exhibe un desempeño sólido en la **prevención y detección técnica** de amenazas, pero muestra debilidad en la **preparación y reacción ante incidentes.**

A nivel de subdominios específicos, destacan **puntos fuertes notables** en la dimensión tecnológica. En particular, **Infraestructura** –seguridad de redes, sistemas y centros de datos– alcanza un nivel cercano al avanzado (IMC **2,67** en 2025). Este valor sobresaliente sugiere que la protección de la infraestructura TI en muchas universidades chilenas es bastante madura, probablemente gracias a la adopción de buenas prácticas, herramientas robustas (firewalls, sistemas de prevención de intrusiones, etc.) y arquitecturas seguras. Otro subdominio bien posicionado es **Comunicaciones** (seguridad en redes y comunicaciones), con un desempeño aún alto (2,15 en 2025) aunque algo menor que el año previo. Estos logros evidencian que Chile ha **priorizado las medidas técnicas** de resguardo de sus activos digitales.

En el lado opuesto, sobresalen **brechas preocupantes** en subdominios de gobernanza y respuesta. Por ejemplo, **Presupuesto** obtiene en 2025 uno de los valores más bajos (IMC promedio **1,28,** e incluso apenas **0,64** en universidades públicas). Esto evidencia una **escasa asignación específica de recursos** para ciberseguridad en muchas IES, especialmente del sector público, y una falta de planificación financiera en la materia. Del mismo modo, dentro del dominio de Responder, el subdominio **Mitigación** (capacidades para contener y minimizar el impacto de incidentes) se encuentra en un nivel prácticamente incipiente (IMC **1,02** promedio; cerca de **0,3** en las instituciones públicas). Esto sugiere que la mayoría de universidades carece de procedimientos sólidos para mitigar y recuperar sistemas tras un ataque, quedando muy

vulnerables ante incidentes.

Si bien otros subdominios de gobierno han mejorado (e.g. Normativa alcanzó 1,84, indicando avance en políticas internas), aún existen déficits en aspectos organizativos: faltan **estrategias integrales, roles claros y financiamiento adecuado** que sustenten la seguridad de forma sistemática. En resumen, el **desempeño por dominios es dispar** –fuerte en lo técnico (infraestructura, comunicaciones) pero **débil en gobierno financiero y respuesta a incidentes**– lo que sugiere que el país deberá enfocar esfuerzos en **fortalecer los cimientos institucionales** (políticas, recursos, procesos) de la ciberseguridad para equilibrar su perfil de madurez.

IMPACTO DEL TAMAÑO DEL EQUIPO DE CIBERSEGURIDAD

Los datos confirman claramente la **correlación positiva** entre el tamaño del equipo de seguridad dedicado y el nivel de madurez de las IES, en línea con lo observado en el informe IMC 2024.

Las instituciones chilenas que cuentan con **más profesionales de ciberseguridad** exhiben una madurez muy superior a las que carecen de personal especializado. Por ejemplo, en 2024 las universidades con **más de 5 personas** dedicadas alcanzaron un IMC promedio de **2,0,** prácticamente nivel avanzado, mientras que aquellas **sin ningún** especialista apenas lograron **0,46** (nivel inicial). Incluso contar con un equipo **moderado (3 a 5 personas)** marcó una diferencia: estas IES promediaron 1,68 en 2024, frente a 1,39 en las que solo tenían 1-2 personas.

De forma similar, en 2025 se reafirma la tendencia: las instituciones con equipos medianos (3-5 integrantes) lideran con IMC **1,64,** y las pocas con equipos mayores mantienen un nivel de **1,74,** en tanto que las **organizaciones sin equipo** dedicado permanecen alrededor de **1,31** (nivel básico). Cabe notar que la brecha extrema se redujo ligeramente (en 2025 ninguna IES quedó por debajo de 1,0, a diferencia de 2024), lo cual podría indicar que algunas instituciones sin equipo han mejorado marginalmente su madurez. Sin embargo,aun así, siguen rezagadas frente a aquellas con personal.

Estas diferencias reiteran que **disponer de un equipo específico de ciberseguridad resulta crucial** para elevar la madurez: las IES con mayor personal pueden implementar más controles, especializar funciones (análisis de riesgos, monitoreo, respuesta, etc.) y sostener programas de mejora continua, alcanzando niveles de madurez notablemente más altos. Por el contrario, aquellas **sin equipo dedicado** –dependiendo quizá de personal TI generalista o de servicios externos mínimos– difícilmente superan el nivel básico. Este patrón, ya observado en 2024, se mantiene en 2025 y envía un mensaje claro: **invertir en capital humano especializado** en seguridad es un factor determinante para avanzar en el modelo de madurez.

INFLUENCIA DEL PRESUPUESTO EN CIBERSEGURIDAD

De forma análoga al recurso humano, la **asignación de presupuesto específico** en ciberseguridad –y su peso relativo dentro del gasto de TI– tiene un impacto directo en el nivel de madurez alcanzado por las IES.

Los datos de Chile muestran una relación lógica: **mayor inversión, mayor madurez.** Aquellas instituciones que destinan una proporción elevada de su presupuesto de TI a seguridad obtienen métricas de madurez muy superiores a las que invierten poco.

En 2024, las universidades que asignaban **menos del 5% del presupuesto** del Área TI registraron un IMC promedio bajísimo (0,44), mientras que las que dedicaban **más del 20%** alcanzaron niveles cercanos al avanzado (IMC 2,05). Incluso inversiones intermedias reflejaron mejoras graduales: por ejemplo, destinar entre 5% y 10% del presupuesto a seguridad se asoció a IMC 1,22, frente a 1,59 en el rango de 10-20%.

En 2025 esta brecha se mantiene: las instituciones con las mayores partidas (>20%) rondan IMC ~1,7–1,8, mientras que las de inversión marginal (e.g. algunas declarando 0% específico) no superan 1,0. Es destacable que entre rangos bajos y medios ya se aprecia un **salto de madurez:** por ejemplo, pasar de no asignar nada a destinar aunque sea <5% puede elevar el IMC de 1,0 a 1,7. En suma, la **proporción del presupuesto de TI dedicada a ciberseguridad** guarda una relación proporcional con el IMC: las IES que incorporan la seguridad como prioridad presupuestaria logran implementar **mejores controles, herramientas y personal,** reflejándose en niveles de madurez mayores.

No obstante, en Chile muchas instituciones **aún no asignan recursos suficientes.** Como ya se indicó, el subdominio Presupuesto fue de los más bajos del país, evidencia de que la inversión en ciberseguridad suele ser limitada o inexistente en numerosas IES. Este factor presupuestario, combinado con el tamaño del equipo, conforma un **eje crítico de mejora:** para transitar del nivel básico al intermedio, las universidades necesitan respaldar sus políticas con financiamiento adecuado y sostenido en seguridad digital.

INCIDENTES DE SEGURIDAD: EVOLUCIÓN Y RELACIÓN CON LA MADUREZ

El número de **ciberincidentes** registrados en las IES chilenas ofrece otro indicador importante, tanto de la exposición a amenazas como de la efectividad de las capacidades de seguridad. En el último periodo analizado, Chile reporta una **disminución notable en la cantidad de incidentes.** El número promedio de incidentes críticos anuales por institución bajó de **1,46** en 2024 a **0,91** en 2025. De modo similar, entre las universidades que sufrieron al menos un incidente, el promedio descendió ligeramente de 2,43 a 2,29 incidentes en el año. Estas cifras sugieren que, aunque los incidentes siguen ocurriendo, su **frecuencia e intensidad se han moderado.** Es probable que una mayor madurez esté permitiendo prevenir o contener mejor muchos ataques, reduciendo la cantidad de incidentes exitosos.

Cabe destacar que la proporción de IES **sin ningún incidente** aumentó sustancialmente: en 2024, solo el 40% de las instituciones no reportó incidentes (es decir, 60% sufrió al menos uno), mientras que en 2025 se estima que **cerca del 60%** logró no tener incidentes en el año. Esto refleja un avance en protección y resiliencia, ya que **más de la mitad** del sistema universitario evitó brechas reportables en 2025.

Al explorar la relación entre el nivel de madurez y la incidencia de incidentes, emergen hallazgos reveladores. En 2024 se observaba un patrón **paradójico:** las instituciones con **mayor número de incidentes** tendían a presentar un IMC más alto. Por ejemplo, las IES que sufrieron **más de 5** incidentes alcanzaron en promedio un nivel de madurez **2,30,** muy superior al de aquellas **sin incidentes (IMC 1,48).** Esto podría interpretarse así: las universidades más grandes o más avanzadas detectan y reportan más incidentes (por su mayor exposición y mejores mecanismos de monitoreo), mientras que las menos maduras quizá **no registran incidentes** –sea por su pequeño tamaño o por falta de capacidad de detección– generando una correlación positiva entre incidentes reportados y madurez.

Sin embargo, en 2025 esta dinámica **cambia significativamente.** Los datos muestran que las instituciones que **no tuvieron ningún incidente** en el último año ahora exhiben una madurez igual o superior a las más atacadas. En efecto, las IES **sin incidentes** promedian un IMC **1,62,** prácticamente al nivel de aquellas con **más de 5 incidentes (IMC 1,66).** Es decir, conforme se eleva la madurez, las universidades parecen más eficaces en **prevenir y resistir incidentes,** rompiendo la tendencia previa. Además, las organizaciones con **2 a 5 incidentes** en 2025 muestran uno de los IMC más bajos (1,17), lo que sugiere que un nivel de madurez básico conlleva seguir enfrentando varios incidentes, mientras que los niveles intermedios-altos permiten reducirlos. Posiblemente, las mejoras implementadas (mejores controles preventivos, detección temprana, respuesta eficaz) están evitando que los ataques se

materialicen en incidentes significativos en las instituciones más avanzadas.

En conclusión, aunque el panorama de incidentes en Chile **sigue siendo delicado,** se observa una disminución en su frecuencia y un **cambio en la relación con la madurez:** las IES más maduras están logrando 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. Las tendencias positivas en 2025 –menos incidentes y una correlación más sana con la madurez– son alentadoras, pero consolidar estos logros requerirá persistir en el fortalecimiento de las capacidades de ciberseguridad en todas las instituciones del país.

USO DE LA INTELIGENCIA ARTIFICIAL EN CIBERSEGURIDAD

Adopción desigual y efectos aún difíciles de aislar en las IES chilenas.

El uso de inteligencia artificial (IA) aplicada a la ciberseguridad en las instituciones de educación superior chilenas presenta un escenario heterogéneo. Aunque la adopción global sigue siendo reducida, ciertos dominios muestran porcentajes notablemente superiores a los observados en la región. Destacan **Proteger y Detectar,** donde alrededor del 40% de las IES declara emplear IA, frente a cifras mucho menores en ámbitos como **Gobernar, Responder y Recuperar o Formación,** que apenas alcanzan entre el 7% y el 9%. Es decir, el uso existe, pero está concentrado en funciones muy específicas.

En los resultados de madurez, se observa que en varias áreas las instituciones que afirman utilizar IA tienden a mostrar **puntuaciones ligeramente superiores,** especialmente en dominios operativos como **Proteger o Detectar.** Sin embargo, también aparecen casos donde las diferencias son mínimas o incluso inversas. Por ejemplo, en **Responder y Recuperar** el IMC medio de las IES con IA es levemente inferior al de aquellas que no la usan, lo que sugiere que el impacto no es uniforme ni necesariamente atribuible a la tecnología por sí sola.

Este patrón invita a una lectura cautelosa. Es probable que las universidades que han empezado a experimentar con IA cuenten ya con **equipos más desarrollados, procesos maduros o mayor capacidad organizativa,** factores que por sí mismos influyen en su nivel de madurez. La heterogeneidad de las puntuaciones refuerza esta idea: en algunos subdominios críticos —como infraestructura, vigilancia o comunicaciones— los valores de ambos grupos son muy similares, y en otros la diferencia favorece a las IES sin IA, mientras que en algunos ocurre lo contrario. Con un número relativamente reducido de instituciones declarando uso de IA, es difícil atribuir las variaciones directamente a su implementación.

Más que evidencias de un efecto inmediato, los datos parecen reflejar un **interés creciente por explorar nuevas capacidades,** especialmente en ámbitos donde la automatización tiene más sentido operativo. La concentración del uso de IA en dominios relacionados con monitoreo, servicios y comunicaciones apunta precisamente a esta búsqueda de eficiencia y visibilidad, más que a una estrategia plenamente desplegada en toda la organización.

En conjunto, Chile presenta un escenario particular: **no existe un patrón** único que vincule uso de IA y mayor madurez, pero sí señales de que las instituciones más avanzadas comienzan a integrar estas tecnologías en áreas específicas. A medida que aumente la adopción y se consoliden buenas prácticas, será posible observar si estas iniciativas exploratorias se traducen en mejoras sostenidas y más amplias dentro del ecosistema universitario.

8.

IMC Colombia

metared
by universia

Secretaría General Iberoamericana
Secretaria-Geral Ibero-Americana

IMC 2025

Índice de Madurez en Ciberseguridad de las IES Iberoamericanas

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)

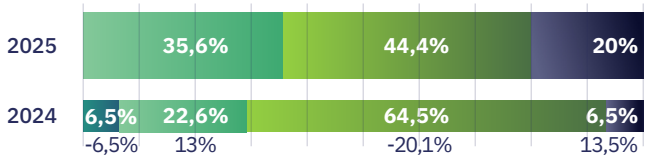
RESPONDER
1,19 (0,00)

TOP 3
PROTEGER
GOBERNAR
DETECTAR

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

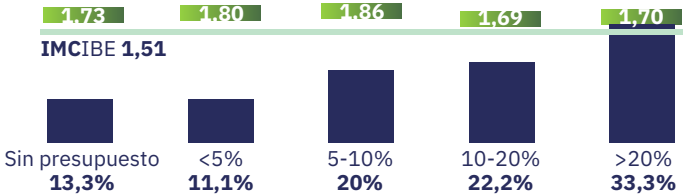
Responder y Recuperar (1,19), presenta el mismo valor que la media iberoamericana para este dominio.

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).

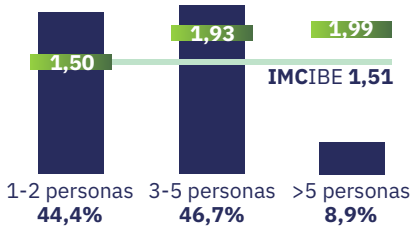
PRESUPUESTO



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.

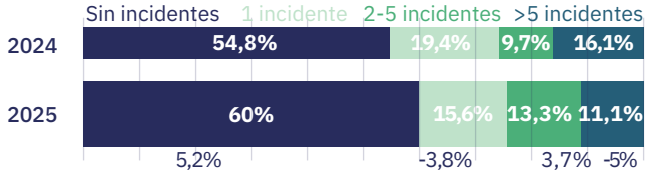
EQUIPOS DE CIBERSEGURIDAD



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.

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.

9.
IMC Ecuador

metared
by universia

Secretaría General
Iberoamericana
Secretaria-Geral
Ibero-Americana

IMC 2025
Índice de Madurez en Ciberseguridad
de las IES Iberoamericanas

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)

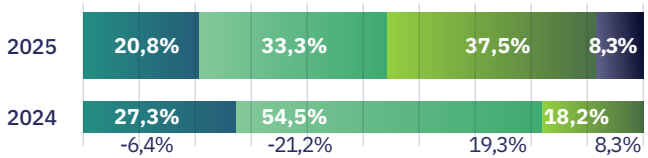
RESPONDER 0,93 (-0,26)

TOP 3
DETECTAR
PROTEGER
GOBERNAR

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

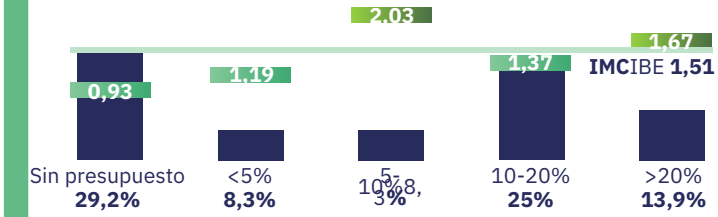
Gobernar e Identificar tienen valores más bajos y alejados de la media, pero Responder y Recuperar es el que más se aleja (0,58 puntos).

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)

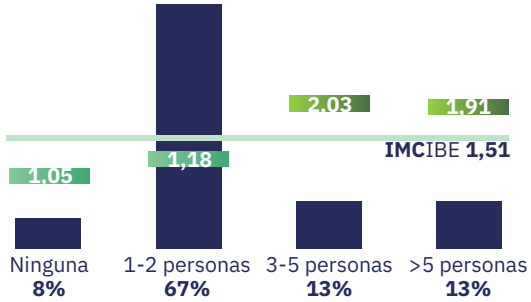
PRESUPUESTO



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.

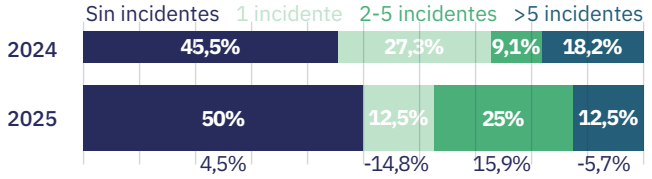
EQUIPOS DE CIBERSEGURIDAD



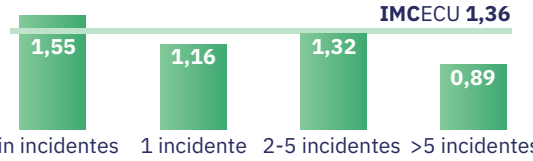
La gran mayoría de IES ecuatorianas (66%) cuentan con equipos de ciberseguridad pequeños, compuestos por 1-2 personas.

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.

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.

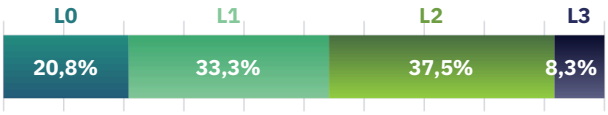
BRECHA ENTRE UNIVERSIDADES PÚBLICAS Y PRIVADAS

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.

10.
IMC España

metared
by universia

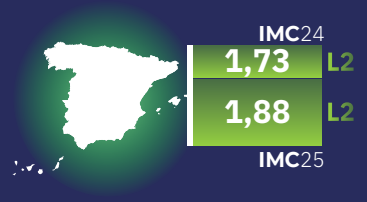
Secretaría General
Iberoamericana
Secretaria-Geral
Ibero-Americana

IMC 2025

Índice de Madurez en Ciberseguridad
de las IES Iberoamericanas

ESP

L0 L1 L2 L3



IMC ESPAÑA
1,88

2024-2025 EVOLUCIÓN
+0,15

IMC IBE DIFERENCIA
+0,37

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)

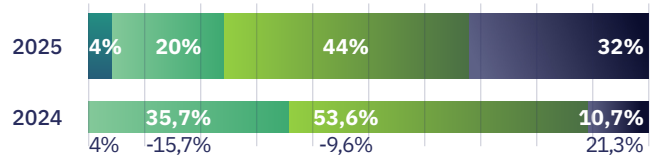
RESPONDER 1,48 (+0,39)

TOP 3
DETECTAR
GOBERNAR
PROTEGER

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

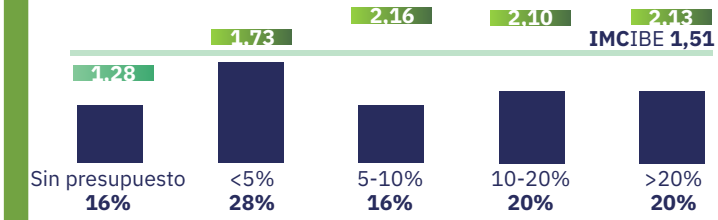
Responder y Recuperar (1,48), se encuentra a tan solo 3 décimas de superarla.

DISTRIBUCIÓN SEGÚN IMC



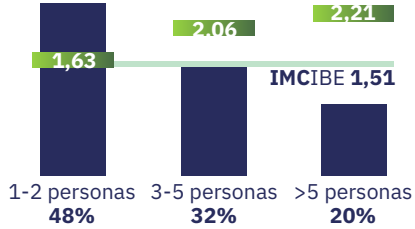
Crecen un 21% las IES del nivel más alto (avanzado, L3).
7 de cada 10 IES españolas se encuentran en niveles intermedio (L2) o avanzado (L3).

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.

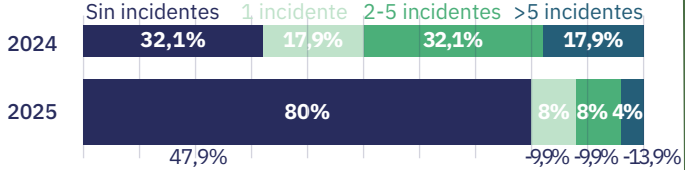
EQUIPOS DE CIBERSEGURIDAD



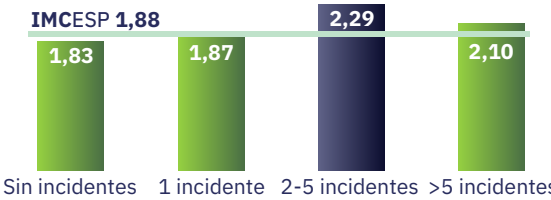
Cerca del 50% están compuestos por 1 o 2 personas.
Clara tendencia alcista en el nivel de madurez de aquellas IES con equipos de mayor tamaño.

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).

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.

11.
IMC México

meta red
by universia

Secretaría General
Iberoamericana

Secretaria-Geral
Ibero-Americana

IMC 2025

Índice de Madurez en Ciberseguridad
de las IES Iberoamericanas

MÉX

L0 L1 L2 L3

TIPO DE IES

*evolución sobre IMC IES MÉX.

PÚBLICAS 1,57 (+0,16)

PRIVADAS 1,28 (+0,04)

DOMINIOS

*evolución sobre IMC dominios IBE

PROTEGER 1,49 (-0,19)

IDENTIFICAR 1,40 (-0,11)

GOBERNAR 1,36 (-0,19)

DETECTAR 1,35 (-0,29)

RESPONDER 1,10 (-0,09)

TOP 3

PROTEGER

IDENTIFICAR

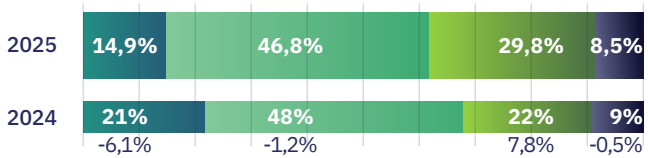
GOBERNAR

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

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

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

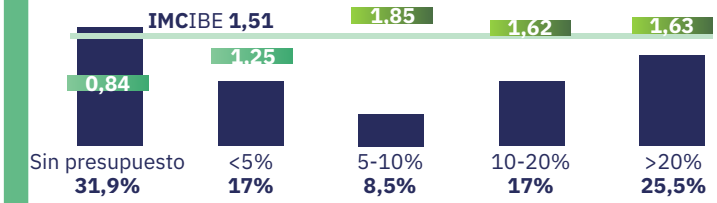
DISTRIBUCIÓN SEGÚN IMC



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

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

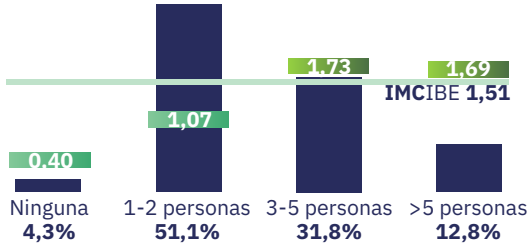
PRESUPUESTO



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

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

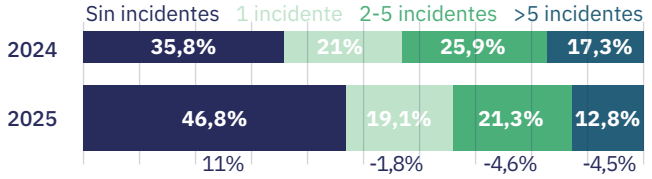
EQUIPOS DE CIBERSEGURIDAD



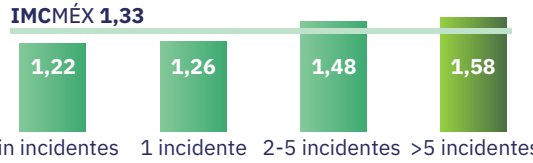
8 de cada 10 equipos están compuestos por menos de 5 personas. Se observa una relación directa entre el tamaño de los equipos de seguridad y el nivel de madurez, excepto en los equipos de más de 5 personas, en los que el IMC parece descender, aunque no significativamente.

CIBERINCIDENTES

DISTRIBUCIÓN DE LOS INCIDENTES



EVOLUCIÓN DEL IMC SEGÚN Nº DE INCIDENTES



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

RESUMEN EJECUTIVO MÉXICO

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

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

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

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

BRECHA ENTRE INSTITUCIONES PÚBLICAS Y PRIVADAS

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

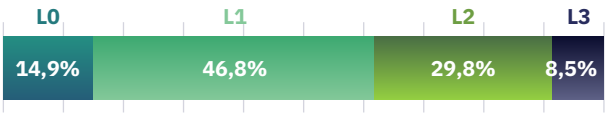
Las IES privadas muestran mejores resultados en prácticamente todos los subdominios de Gobernar: estrategia, normativa, procedimientos y asignación de presupuesto. Por el contrario, las IES públicas presentan déficits más marcados en presupuesto, documentación técnica y definición de roles, tres elementos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

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

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

DISTRIBUCIÓN DE NIVELES DE MADUREZ

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



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

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

DESEMPEÑO POR DOMINIOS

Fortalezas en Infraestructura y Comunicaciones,

debilidades en Gobernanza y Respuesta.

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

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

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

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

IMPACTO DEL TAMAÑO DEL EQUIPO DE CIBERSEGURIDAD

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

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

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

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

INFLUENCIA DEL PRESUPUESTO EN LA MADUREZ

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

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

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

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

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

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

INCIDENTES DE SEGURIDAD: EVOLUCIÓN Y RELACIÓN CON LA MADUREZ

Un factor crítico que evidencia diferencias profundas en resiliencia

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

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

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

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

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

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

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

USO DE LA INTELIGENCIA ARTIFICIAL EN CIBERSEGURIDAD

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

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

Incorporación limitada y efectos aún en evaluación dentro del ecosistema universitario.

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

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

12.
IMC Perú

metared
by universia

Secretaría General
Iberoamericana
Secretaria-Geral
Ibero-Americana

IMC 2025

Índice de Madurez en Ciberseguridad
de las IES Iberoamericanas

PER

1,59 L2

IMC25

IMC PERÚ

1,59

IMC IBE DIFERENCIA

+0,08

L0 L1 L2 L3

TIPO DE IES

PÚBLICAS 1,30

PRIVADAS 1,70

DOMINIOS

*evolución sobre IMC dominios IBE

PROTEGER 1,77 (+0,09)

DETECTAR 1,67 (+0,03)

GOBERNAR 1,63 (+0,08)

IDENTIFICAR 1,56 (+0,05)

RESPONDER 1,35 (+0,16)

TOP 3

PROTEGER

DETECTAR

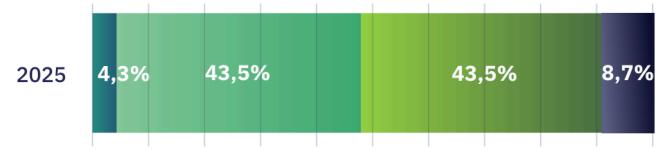
GOBERNAR

Todos los dominios, salvo Responder y Recuperar (1,35) superan el IMC 2025 (1,51).

Supera en todos los casos el promedio iberoamericano de cada dominio.

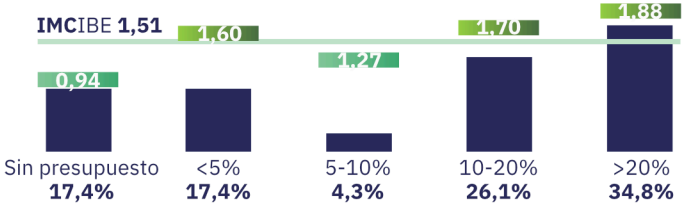
Proteger (1,77) presenta el valor más alto, solo superado por Colombia (2,00) y España (1,92).

DISTRIBUCIÓN SEGÚN IMC



El 87% de las IES peruanas se sitúa en nivel básico (L1) y nivel intermedio (L2).

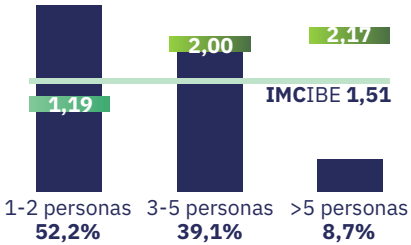
PRESUPUESTO



Cerca del 20% de las IES **no cuentan con presupuesto específico.**

Contar con un presupuesto asignado presenta una relación directa con el nivel de madurez en todos los rangos de presupuesto asignado.

EQUIPOS DE CIBERSEGURIDAD

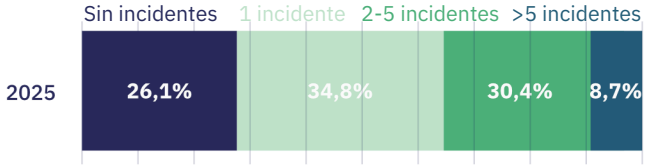


La mayoría de equipos de ciberseguridad están compuestos por 1-2 personas (52%).

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

Algo más de 7 de cada 10 instituciones peruanas han sufrido algún ciberincidente en el último año.

RESUMEN EJECUTIVO PERÚ

Perú se incorpora al estudio con una base de madurez sólida, superando el promedio regional.

En su primera participación en el Índice de Madurez en Ciberseguridad (IMC) 2025, Perú alcanza un IMC promedio de **1,59,** por encima del promedio regional (1,51). Este resultado inicial sugiere que el ecosistema universitario peruano dispone de capacidades técnicas ya consolidadas y de infraestructuras de seguridad razonablemente maduras.

En comparación internacional, solo unos pocos países muestran valores superiores (por ejemplo, España y Colombia), por lo que el desempeño peruano es de los más altos en Iberoamérica. Este nivel indica que las universidades peruanas gestionan relativamente bien sus activos críticos, riesgos y dependencias, y cuentan con buenas prácticas técnicas en la mayoría de los dominios.

No obstante, al carecer de datos históricos, aún no se puede afirmar con certeza si Perú avanzará rápidamente: el potencial es interesante, pero habrá que ver su evolución en ediciones posteriores. Lo que se observa es que el punto de partida 2025 es positivo,y abre la posibilidad de que Perú consolide una madurez superior, aunque es necesario interpretarla con cautela. Al ser una muestra limitada (23 instituciones evaluadas), es posible que haya sesgos de participación (por ejemplo, mayor presencia de IES con más recursos o mejor organización interna). En todo caso, este primer diagnóstico es alentador: Perú queda situado entre los países con mejor desempeño técnico en la región.

DISTRIBUCIÓN DE NIVELES DE MADUREZ

La distribución de instituciones peruanas por nivel muestra que solo una minoría está en lo inicial, mientras que la mayoría opera en el nivel intermedio o avanzado. En detalle, el **4,3%** de las IES evaluadas se ubica en el primer nivel (L0), mientras que el **43,5%** alcanza el nivel básico (L1) y otro **43,5%** el nivel intermedio (L2). Finalmente, un **8,7%** (dos IES) llega al nivel avanzado (L3). Esto significa que casi la mitad de las instituciones muestra capacidades intermedias o superiores, y solo muy pocas se encuentran rezagadas. Esta distribución sugiere un ecosistema con una base de madurez bastante extendida, sin capas masivas de IES en el nivel más bajo.

Sin embargo, es importante matizar esta lectura: la muestra puede no representar a todas las universidades. Es posible que hayan participado en mayor medida aquellas más preparadas, por lo que la proporción de IES en niveles altos podría estar sobreestimada respecto al sistema completo. Asimismo, el hecho de que exista un 8,7% en L3 es positivo, pero este grupo aún es pequeño, por lo que es recomendable analizar si se incrementa en futuras ediciones.

En resumen, la distribución actual es un buen indicio de un punto de partida sólido, pero requiere confirmación con más datos y una muestra más amplia para garantizar su representatividad.

BRECHA ENTRE INSTITUCIONES PÚBLICAS Y PRIVADAS

El sector privado lidera la madurez con ventaja notable sobre el público.

En Perú se observa una brecha interna marcada donde las universidades privadas logran una madurez promedio significativamente mayor que las públicas. El IMC promedio de las instituciones **privadas es de 1,70,** frente a **1,30 en las públicas.** Esta diferencia (0,40 puntos) es mayor que la registrada en la mayoría de países de la región. Además, las instituciones privadas dominan en todos los dominios evaluados; por ejemplo, en **Proteger** alcanzan 1,92 contra 1,34 de las públicas, y en **Gobernar** 1,76 vs. 1,27. Solo en **Normativa** la brecha es menor (1,59 vs. 1,50).

Este patrón sugiere que las universidades privadas cuentan con procesos más formalizados y recursos dedicados: disponen de mayor autonomía presupuestaria, personal especializado y tecnologías avanzadas. En cambio, las públicas, aunque en promedio sólidas, muestran resultados más dispersos, probablemente limitadas por presupuestos ajustados o rígidas estructuras organizativas. No obstante, es destacable que ambas superan el nivel básico y están por encima del promedio regional en la mayoría de dominios. La brecha indica que para alcanzar una convergencia será necesario que las instituciones públicas fortalezcan sus estructuras de gestión y acceso a recursos.

DESEMPEÑO POR DOMINIOS

Perú muestra fortalezas claras en los dominios técnicos, con oportunidades de mejora en los organizativos. En 2025, los dominios más desarrollados son **Proteger** (IMC 1,77) y **Detectar** (1,67), seguidos por Gobernar (1,63) e Identificar (1,56). El dominio más bajo es **Responder y Recuperar** (1,35), aunque aun así está por encima del promedio regional en esta dimensión (1,19). En conjunto, la mayoría de los dominios técnicos supera cómodamente la media regional, lo que refleja que las instituciones peruanas tienen infraestructuras y prácticas de seguridad sólidas (comunicación segura, monitoreo y seguimiento establecidos, gestión consistente de activos y riesgos).

Por el contrario, los dominios más organizativos (obernanza y respuesta) tienen valores modestos. Esto indica que, si bien existen políticas y roles básicos, faltan procesos más formales y un enfoque sistemático. En particular, la capacidad de respuesta a incidentes podría beneficiarse de protocolos más homogéneos entre instituciones.

En líneas generales, Perú ofrece **un perfil técnico robusto con gobernanza alineada, pero aún con margen de consolidación.** En el futuro, sería deseable reforzar los dominios organizativos (planes, procedimientos y recursos humanos) para equilibrar el desempeño general.

IMPACTO DEL TAMAÑO DE LOS EQUIPOS DE CIBERSEGURIDAD

El tamaño del equipo dedicado impacta de forma determinante en la madurez.

En Perú existe una relación muy clara entre la cantidad de profesionales de seguridad y el nivel de madurez. Las instituciones con un equipo **pequeño (1–2 personas)** presentan un IMC promedio muy bajo (1,19). En cambio, aquellas con equipos medianos **(3–5 personas) alcanzan un IMC de 2,00,** y las que cuentan con **más de 5 profesionales llegan a 2,17.**

La progresión es muy pronunciada con un salto más relevante al pasar de equipos muy pequeños a medianos, llevando a las instituciones al nivel intermedio (L2). Este comportamiento reafirma que contar con personal dedicado es clave para avanzar: los equipos más grandes permiten documentar procesos, asumir tareas de mejora continua y sostener la vigilancia permanente.

En Perú prácticamente todas las IES evaluadas disponen de al menos un profesional de seguridad, por lo que la ausencia total de personal no es un factor explicativo (a diferencia de otros países). En cambio, la amplitud del equipo funciona como un **acelerador** ampliando las capacidades técnicas y organizativas de forma clara. Este patrón coincide con la tendencia regional, aunque en Perú la diferencia es especialmente fuerte.

INFLUENCIA DEL PRESUPUESTO EN CIBERSEGURIDAD

La inversión creciente en seguridad impulsa la madurez, sobre todo cuando supera el 10% del presupuesto.

El análisis por presupuesto confirma que, en Perú, dedicar una mayor proporción del presupuesto de TI a seguridad se correlaciona con niveles más altos de madurez. Las instituciones que asignan más del 10% de su presupuesto a ciberseguridad obtienen un IMC muy superior al resto. En detalle, las IES que destinan entre **10–20% alcanzan un IMC promedio de 1,70,** y aquellas que superan el **20% llegan a 1,88,** los valores más altos del país. En contraste, **las que no cuentan con presupuesto asignado se quedan en valores de madurez de 0,94.**

Estos datos muestran que el salto más significativo ocurre al rebasar el umbral del 10%. Por debajo de ese nivel, la relación no es tan nítida (tal vez por muestras pequeñas). Pero una vez que la inversión se vuelve considerable (>10%), la madurez se dispara. Esto refleja que las instituciones peruanas traducen el presupuesto en recursos técnicos y humanos concretos: con más fondos, mejoran sus infraestructuras, herramientas de protección y procesos internos. En conjunto, se confirma que aumentar la asignación presupuestaria es un impulsor clave de la madurez en Perú, similar a lo observado en otros países donde la inversión es un diferenciador claro.

INCIDENTES DE SEGURIDAD

Patrón inrregular: los incidentes no muestran relación directa con la madurez.

En 2025, la mayoría de instituciones peruanas reporta al menos un incidente. La distribución es: **26,1% sin incidentes, 34,8% con un incidente, 30,4% con 2–5 incidentes, y 8,7% con más de cinco.** El promedio general de incidentes reportados es de 2,83 por institución (entre las que reportaron alguno, el promedio asciende a 3,82).

Sin embargo, al comparar niveles de madurez según la experiencia de incidentes no se observa un patrón lineal. Las IES que no registraron incidentes tienen un IMC promedio de **1,66,** mientras que las que tuvieron **uno sólo** presentan un IMC mucho menor (1,35). Por su parte, aquellas con **2–5 incidentes** alcanzan el IMC más alto (1,78), y las con **más de 5** un 1,73.

En resumen, no hay una correlación directa: ni las más maduras detectan sistemáticamente más incidentes, ni las menos maduras los evitan por completo. Este escenario sugiere que otros factores (como el tamaño del equipo o el perfil de los ataques) pueden influir más que la madurez en el número de incidentes observados. En cualquier

caso, el dato clave es que el reporte de incidentes no discrimina en bloque a las IES más maduras; los valores son heterogéneos entre todos los niveles.

USO DE LA INTELIGENCIA ARTIFICIAL EN CIBERSEGURIDAD

Adopción incipiente, concentrada en dominios técnicos.

En Perú la adopción de herramientas de IA en ciberseguridad todavía es limitada. Solo un **8,7%** de las IES emplea IA en el dominio **Gobernar;** en cambio, los dominios más técnicos registran un uso relativamente mayor: **39,1% en Detectar y 34,8% en Proteger,** mientras que **Identificar y Formación tienen 26,1% y 21,7%** respectivamente. En **Responder y Recuperar es muy bajo (13,0%).**

Curiosamente, el uso de IA en Perú no está asociado con mayor madurez promedio. Las instituciones que utilizan IA en el dominio Gobernar registran un IMC inferior (1,21) al de las que no la usan (1,63), por ejemplo. Esto sugiere que, por ahora, la IA es incorporada principalmente por instituciones aún en proceso de consolidación, o que la adopción es demasiado incipiente como para elevar el desempeño general. En muchos casos, las universidades que aplican IA podrían ser las pioneras que aún no han terminado de fortalecer otros aspectos de seguridad.

En definitiva, aunque en Perú un número creciente de IES comienza a experimentar con IA en funciones técnicas, aún es un complemento minoritario y no aparece como factor determinante de la madurez.

13.
IMC Portugal

meta red
by universia

Secretaría General
Iberoamericana

Secretaria-Geral
Ibero-Americana

IMC 2025

Índice de Madurez en Ciberseguridad
de las IES Iberoamericanas

POR

IMC PORTUGAL
1,44

2024-2025 EVOLUCIÓN
+0,03

IMC IBE DIFERENCIA
-0,07

L0 L1 L2 L3

TIPO DE IES

PÚBLICAS
1,47 (+0,08)

PRIVADAS
1,17 (-0,36)

DOMINIOS

*evolución sobre IMC dominios IBE

DETECTAR
1,60 (-0,04)

PROTEGER
1,59 (-0,09)

IDENTIFICAR
1,42 (-0,09)

GOBERNAR
1,42 (-0,13)

RESPONDER
1,15 (-0,04)

TOP 3

DETECTAR

PROTEGER

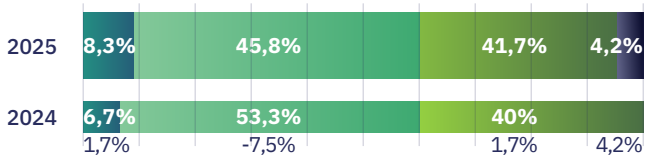
GOBERNAR/ IDENTIFICAR

Detectar y Proteger superan el IMC 2025 (1,51) en 8 y 9 centésimas respectivamente.

Gobernar e Identificar obtienen una puntuación de 1,42 un poco por debajo de la media iberoamericana .

Responder y Recuperar presenta el valor más bajo y alejado de la media.

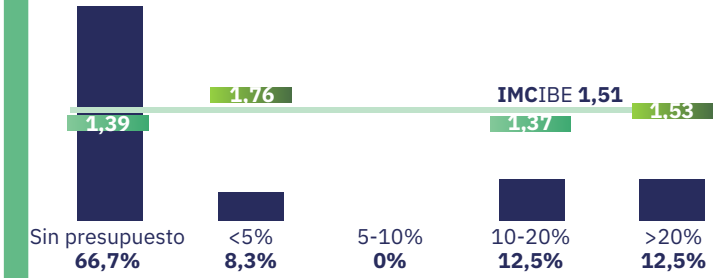
DISTRIBUCIÓN SEGÚN IMC



La mayoría de IES portuguesas (87,5%) se sitúan entre el nivel L1 (básico) y L2 (intermedio).

Ligera tendencia a mayor nivel madurez: bajan un 7,5% las IES en L1, y aumentan un 1,7% y un 4,2% las de L2 y L3.

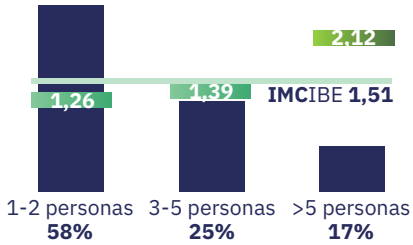
PRESUPUESTO



Casi el 70% de las IES **no cuentan con presupuesto específico.**

El nivel de madurez de las IES con presupuesto de menos del 5% es el más alto (1,76), 0,25 que la media iberoamericana.

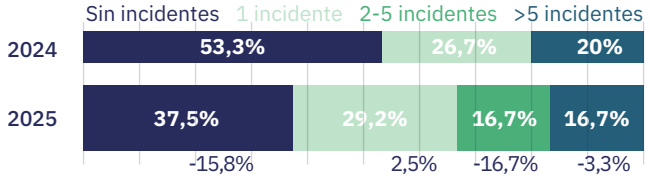
EQUIPOS DE CIBERSEGURIDAD



Casi un 20% de equipos de ciberseguridad portugueses están compuestos de más de 5 personas. El valor del IMC se incrementa notablemente en función del tamaño del equipo. En el caso de Portugal, las IES con más de 5 personas en su equipo alcanzan 2,12 (intermedio, L2).

CIBERINCIDENTES

DISTRIBUCIÓN DE LOS INCIDENTES



EVOLUCIÓN DEL IMC SEGÚN Nº DE INCIDENTES

6 de cada 10 instituciones portuguesas han sufrido algún ciberincidente en el último año.

RESUMEN EJECUTIVO PORTUGAL

Portugal muestra uno de los perfiles más equilibrados y homogéneos de la región aunque no alcanza el nivel intermedio (L2)

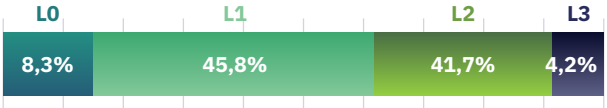
Portugal obtiene en 2025 un **IMC de 1,44,** una mejora respecto a 2024 (1,41), que indica una evolución moderada pero consistente. El país se mantiene en el nivel básico (L1), aunque cerca del umbral intermedio y por encima de países como México (1,33) o Ecuador (1,36).

La mejora, aunque no tan pronunciada como en otros países, se caracteriza por su **estabilidad:** Portugal presenta valores relativamente altos y equilibrados en la mayoría de los dominios, sin grandes oscilaciones y sin brechas profundas entre áreas técnicas y organizativas. Este rasgo distingue al país dentro de la región, donde es habitual observar sistemas más heterogéneos.

No obstante, el país se mantiene aún por debajo del promedio iberoamericano de 2025 (1,51), lo que indica un margen de avance especialmente en aspectos organizativos y de respuesta.

DISTRIBUCIÓN DE NIVELES DE MADUREZ

Los valores de 2025 muestran la siguiente distribución en Portugal:



El país presenta un porcentaje alto de IES en **nivel intermedio (L2)**, por debajo de Colombia, España, Perú y Chile. Esto indica un sistema universitario con bases relativamente sólidas y una consolidación técnica más avanzada que en países que siguen anclados en L1.

El porcentaje de instituciones en L0 (8,3%) es bajo comparado con otros países, lo que sugiere que la mayor parte del sistema ha superado los niveles más incipientes. La presencia de instituciones en L3 (4,2%) es modesta, pero consistente con el perfil de estabilidad del país.

BRECHA ENTRE INSTITUCIONES PÚBLICAS Y PRIVADAS

Giro llamativo en 2025: las públicas pasan a liderar el IMC medio.

En 2024, las instituciones privadas de Portugal presentaban un IMC medio de **1,53, frente a 1,39** en las públicas, con una diferencia de unas **0,14 décimas a favor del sector privado.** En 2025 la foto cambia de forma llamativa: las privadas descienden a un IMC de **1,17,** mientras que las públicas ascienden a **1,47,** situándose **0,30 puntos por encima** y dejando el promedio nacional en **1,44.**

Este cambio sugiere un reequilibrio significativo entre ambos sectores, aunque es probable que en parte esté influido por variaciones en el conjunto de instituciones participantes y no solo por la evolución interna de cada una.

Si se observa el detalle por dominios, el patrón se repite. En 2024 las privadas lideraban en **Identificar** (1,48 frente a 1,41) y **Proteger** (1,68 frente a 1,59). En 2025, sin embargo, las públicas pasan a obtener **1,48 en Identificar frente a 0,94 en las privadas, y 1,61 en Proteger frente a 1,46**

en el sector privado. Algo similar ocurre en **Gobernar,** donde las públicas alcanzan **1,47 frente a 1,04** en las privadas, y en varios subdominios —como **Estrategia, Normativa o Análisis de riesgos**— donde las universidades públicas muestran una mejora muy clara respecto al año anterior.

Esta evolución no significa necesariamente que las privadas hayan "dejado de hacer cosas" en ciberseguridad, sino que **la mejora del sector público ha sido más intensa** y, posiblemente, concentrada en un subconjunto de instituciones que han dado saltos importantes en gobernanza, identificación de activos y gestión técnica. Llama la atención que, pese a que el subdominio **Presupuesto** sigue siendo bajo en ambos casos (en torno a **0,43–0,67 puntos),** las públicas consigan mejores resultados en dominios como **Gobernar o Identificar,** lo que sugiere un esfuerzo organizativo relevante más allá del nivel de inversión estrictamente declarado.

En conjunto, Portugal presenta una brecha entre públicas y privadas que no es extrema, pero sí **dinámica:** de una ventaja clara del sector privado en 2024 se pasa a un liderazgo del sector público en 2025, especialmente en dominios organizativos. Las privadas mantienen buenos niveles técnicos —sobre todo en infraestructuras y comunicaciones—, mientras que las públicas parecen haber acelerado la formalización de políticas, roles y estrategia. Será importante observar en los próximos ejercicios si esta tendencia se consolida o si obedece, en parte, a cambios en la muestra y a proyectos concretos de un grupo reducido de IES.

DESEMPEÑO POR DOMINIOS

Los valores por dominio en 2025 son: **Gobernar (GB): 1,42, Identificar (ID): 1,42, Proteger (PR): 1,59, Detectar (DE): 1,60, Responder (RE): 1,15.**

Portugal exhibe fortalezas muy claras en los dominios **Proteger y Detectar,** cuyos valores se sitúan cerca del nivel intermedio. Esto se refleja en subdominios con puntuaciones elevadas como en Infraestructura (2,20), Comunicaciones (2,15), Información (2,16) y Actividad de Usuarios (1,83). Esta fortaleza técnica sitúa a Portugal entre los países con mayor control técnico de la región, junto a España, Colombia y Brasil.

Portugal destaca en infraestructura y detección, pero mantiene brechas en respuesta y formalización organizativa.

Los dominios **Gobernar e Identificar** muestran valores promedio sólidos (1,42), superiores al de varios países vecinos, pero aún insuficientes para alcanzar un nivel intermedio pleno. La debilidad más marcada continúa siendo el dominio **Responder y Recuperar,** con un valor de 1,15 y 0,96, lo que evidencia carencias en mitigación, recuperación y gestión formal de incidentes.

IMPACTO DEL TAMAÑO DE LOS EQUIPOS DE CIBERSEGURIDAD

La presencia de un equipo dedicado es uno de los factores más determinantes para avanzar en el modelo de madurez.

Los datos de Portugal confirman la relación positiva entre el tamaño del equipo especializado y el nivel de madurez de las instituciones, aunque el patrón es menos lineal que en otros países como España o México. En 2024, las IES sin personal dedicado presentaban un IMC de **1,37,** mientras que aquellas con **1–2 personas** alcanzaban **1,38,** mostrando un salto relevante simplemente por contar con un mínimo de personal especializado. Las instituciones con **3–5 integrantes lograban 1,54,** y no se registraban IES con **más de 5 personas.**

En 2025 estas tendencias se mantienen, pero con matices. Del relevamiento realizado surge que no existen IES sin personal mientras que el grupo con **1–2 personas registra un IMC de 1,26,** valor inferior al registrado el año anterior, lo que indicaría una desmejora en las capacidades. Esta misma situación se plantea para **las instituciones con equipos de 3–5 personas, que alcanzan un IMC de 1,39,** ubicándose ya en el nivel básico y con valores menores que los registrados en el IMC 2024. **El grupo con más de 5 profesionales obtiene un IMC de 2,12,** valor que muestra una tendencia ascendente notoria, sumando a que en el año anterior no se habían relevado IES portuguesas con dicha dimensión de personal.

Sin embargo, los valores alcanzados deben interpretarse con cautela. Es posible que la muestra de 2025 incluya centros con equipos grandes pero con desafíos importantes en gobernanza o gestión operativa, o que las instituciones más sólidas del año anterior no hayan participado en 2025. Con todo, el patrón general sí se mantiene: **tener más personal especializado aumenta la probabilidad de alcanzar mejores niveles de madurez,** especialmente en Portugal, donde incluso superar los 5 profesionales supone un salto inmediato de casi un punto en el IMC.

En términos prácticos, el análisis de 2024 y 2025 envía un mensaje claro y consistente con el resto de la región: **la presencia de un equipo dedicado es uno de los factores más determinantes para avanzar en el modelo de madurez.** Las instituciones con personal mínimo tienden a estancarse en niveles básicos, mientras que aquellas con equipos de tamaño medio (3–5 personas) son las que muestran una trayectoria de progreso más estable. El aumento del valor para IES con grupos de más de 5 profesionales en 2025 refuerza esta tendencia general; aún cuando es necesario considerar el contexto particular de cada institución y la importancia de combinar capital humano con gobernanza, procesos y recursos adecuados.

INFLUENCIA DEL PRESUPUESTO EN CIBERSEGURIDAD

El análisis de Portugal muestra que el presupuesto sigue siendo un factor importante para explicar la madurez, aunque con un comportamiento menos lineal que en otros países de la región. En 2025, las instituciones que asignan **0–5%** de su presupuesto de TI a ciberseguridad registran un IMC medio de **1,76,** alcanzando un nivel intermedio (L2), mientras que aquellas que destinan entre **5–10%** alcanzan **1,44,** o sea un nivel básico (L1). En el tramo **10–20%,** el IMC obtiene un valor de **1,37,** correspondiente a un nivel básico. Las IES que invierten **más del 20%,** por su parte, tienen un IMC de **1,53,** lo que muestra una progresión positiva aunque requiere interpretar estos datos con prudencia, debido a su comportamiento errático.

Comparado con 2024, el país mostraba aumentos modestos en los tramos bajos y un salto más visible a partir del 10%, pero este patrón no se mantiene o lo hace solo para presupuestos superiores al 20%.

Este fenómeno puede deberse a varios factores. En primer lugar, las instituciones con porcentajes elevados de presupuesto podrían estar respondiendo a incidentes recientes o necesidades urgentes, destinando recursos a medidas reactivas que aún no se reflejan plenamente en su madurez global. En segundo lugar, las cifras sugieren que el gasto solo genera mejoras sostenidas cuando va acompañado de **gobernanza, procesos estables y equipos**

capacitados. De hecho, el subdominio **Presupuesto** sigue mostrando valores alarmantemente bajos en el país, en torno a 0,46, lo que indica que la cultura de planificación financiera en ciberseguridad todavía está en una fase muy incipiente.

Con todo, el mensaje que dejan los datos es claro: **las instituciones que asignan un presupuesto específico para seguridad avanzan más rápidamente,** y aquellas que invierten al menos un 20% alcanzan niveles significativamente superiores al promedio nacional. El reto para Portugal no es únicamente aumentar la inversión, sino **garantizar que esa inversión esté alineada con una estrategia, con roles definidos y con la capacidad operativa necesaria para ejecutar las acciones previstas.** Solo así el presupuesto podrá convertirse en un verdadero motor de madurez y no en un indicador aislado.

INCIDENTES DE SEGURIDAD: EVOLUCIÓN Y RELACIÓN CON LA MADUREZ

Aumento notable de la criticidad y una relación compleja con la madurez.

El comportamiento de los ciberincidentes en las IES portuguesas muestra una evolución particular entre 2024 y 2025. A diferencia de otros países donde los incidentes se estabilizan o disminuyen, Portugal registra un **incremento muy marcado en la criticidad:** el número medio de incidentes críticos reportados por las instituciones pasa de **13,60 en 2024 a 39,50 en 2025,** casi triplicando la cantidad.

Este aumento no implica necesariamente una mayor vulnerabilidad general, pero sí revela una combinación de **mejor capacidad de detección** en algunas IES y **persistentes debilidades de resiliencia** en otras.

En términos de distribución, los datos muestran que **las instituciones se reparten de forma equilibrada entre aquellas sin incidentes,** las que sufren un único caso y las que registran varios. El patrón observado es el siguiente:

- **Sin incidentes: IMC 1,55**
- **1 incidente: IMC 1,39**
- **2 a 5 incidentes: IMC 1,43**
- **Más de 5 incidentes: IMC 1,25**

Este comportamiento sugiere un fenómeno ya visto en otros países en etapas previas: **las instituciones más maduras detectan y reportan más incidentes,** mientras que las menos desarrolladas pueden registrar pocos casos, pero no necesariamente porque estén mejor protegidas, sino porque cuentan con una capacidad limitada para identificarlos o documentarlos.

No obstante, el salto en criticidad de 2025 invita a una lectura más matizada. Algunos subdominios clave ayudan a entender esta situación:

- **Mitigación (0,96) y Recuperación (0,96)** siguen siendo áreas débiles.
- **Continuidad (0,83)** muestra fragilidad, especialmente en IES con múltiples incidentes.
- **Responsabilidad y procedimientos** presentan valores dispares entre instituciones, dificultando respuestas coordinadas.

En conjunto, estos indicadores reflejan que, aunque Portugal tiene **una madurez técnica sólida** (buenos resultados en infraestructura, y comunicaciones), la capacidad de **responder, contener y recuperarse** sigue siendo un desafío significativo.

Un aspecto relevante de la evolución 2024–2025 es que **la correlación entre número de incidentes y mayor madurez no se invierte,** pero sí se diluye. En 2024, las instituciones con más incidentes tendían a situarse claramente por encima de la media. En 2025, las diferencias entre grupos son menores y las IES con cero incidentes no aparecen rezagadas, lo que apunta a una mejora relativa en prevención o, al menos, a que un número creciente de instituciones consigue pasar el año sin incidentes críticos detectados.

En resumen:

- **Aumenta la criticidad,** aunque no necesariamente la vulnerabilidad general.
- **Se amplía la brecha interna:** algunas IES mejoran la detección, otras continúan sin procesos robustos de respuesta.
- **La relación entre incidentes y madurez se suaviza,** un paso previo a lo que ya se observa en países más avanzados.
- **Responder sigue siendo el dominio más débil,** lo que amplifica el impacto de los incidentes que sí ocurren.

En síntesis, Portugal presenta un escenario de incidentes complejo: detecta más, pero aún **responde y se recupera con dificultad.** Mejorar los procesos de gestión de incidentes —especialmente mitigación, recuperación y continuidad— será clave para que el país pueda consolidar un ecosistema universitario más resiliente en los próximos años.

USO DE LA INTELIGENCIA ARTIFICIAL EN CIBERSEGURIDAD

El uso de inteligencia artificial (IA) en las IES portuguesas sigue siendo limitado, aunque algo más extendido que en otros países de la región. Los datos muestran que la adopción se concentra en dominios claramente técnicos: **Proteger (37,5%), Detectar (29,2%) e Identificar (20,8%).** En cambio, la IA está totalmente ausente en **Gobernar** y **Responder,** y prácticamente residual en **Formación (4,2%).** Este patrón revela que la tecnología se está aplicando principalmente en tareas operativas orientadas al análisis, la vigilancia o la automatización de detecciones, y no en ámbitos estratégicos o organizativos.

Adopción selectiva y beneficios aún incipientes,

condicionados por la madurez previa de cada institución.

Al comparar el nivel de madurez entre instituciones que usan IA y las que no, se aprecian diferencias relevantes en varios dominios. Las IES que han incorporado IA muestran valores superiores en **Identificar (IMC 1,86 frente a 1,33), Proteger (1,74 frente a 1,26) y Detectar (1,62 frente a 1,36).** Sin embargo, esta ventaja desaparece en dominios como **Gobernar** y **Responder y Recuperar,** donde directamente no existe adopción de IA. Esto sugiere que la tecnología se está incorporando en áreas donde Portugal ya presenta fortalezas técnicas, pero no está aún integrada como parte de una estrategia global de seguridad.

Aun así, estas diferencias deben interpretarse con cautela. Como ocurre en otros países, es probable que las instituciones que utilizan IA sean también aquellas con **equipos más especializados, procesos más maduros o mayor disponibilidad presupuestaria,** factores que influyen tanto en su nivel de madurez como en su capacidad para adoptar nuevas tecnologías. La IA, en este sentido, parece reflejar más un **síntoma de madurez previa** que un impulsor directo y homogéneo del avance.

Otro aspecto destacable es la ausencia total de IA en **Responder y Recuperar,** un dominio que ya es débil en Portugal y que podría beneficiarse en el futuro de capacidades de automatización, priorización y análisis acelerado. La falta de adopción en este ámbito sugiere que la IA aún no está integrada en la gestión de incidentes ni en la recuperación, dos áreas clave para mejorar la resiliencia del país.

En conjunto, Portugal muestra un escenario donde la IA se utiliza, pero de manera muy focalizada, con beneficios visibles en dominios técnicos pero sin efectos globales en la estructura del IMC. El país cuenta con una base tecnológica sólida que podría facilitar la expansión futura de estas herramientas, pero su impacto dependerá de que la adopción vaya acompañada de mejoras en gobernanza, roles, procedimientos y capacidad de respuesta.

Anexo 1

Ficha técnica

Descripción de la muestra

Con el fin de garantizar una representación adecuada de la diversidad existente entre las IES incluidas en esta medición, se optó por un **diseño muestral estratificado con asignación proporcional.** Para la definición de los estratos se consideraron dos variables: el **país de origen** de la institución y su **naturaleza jurídica,** diferenciando entre IES púbilcas y privadas según su forma de propiedad o administración.

El proceso de conformación de la muestra se desarrolló en dos etapas. En primer lugar, se estimó el tamaño de cada estrato dentro del universo de estudio a partir de **estadísticas oficiales de educación superior correspondientes a cada país,** información que fue posteriormente contrastada y validada por los coordinadores del **Grupo de Trabajo Internacional en Ciberseguridad de MetaRed.**

En una segunda etapa, se estableció un tamaño muestral esperado por estrato que permitiera trabajar con un **error muestral máximo del 8%,** lo que dio lugar a una muestra teórica de **387 casos.**

De cara al análisis desagregado de los resultados, se aplicó un tratamiento específico a aquellos estratos que no alcanzaron un volumen de respuestas cercano al previsto inicialmente.

Concluida la fase de levantamiento de información se registraron **308 respuestas válidas, un 80% del total esperado.** Tal como se detalla en el cuerpo del informe, y para preservar la solidez y calidad de los análisis, se elaboraron informes desagregados para los **nueve países** que alcanzaron un número de respuestas consistente con los criterios muestrales definidos, quedando la zona Centroamerica y Caribe por debajo del tamaño mínimo muestral y sin posibilidad de informe específico.

Conviene señalar que, cuando el análisis se realiza a nivel agregado para toda **Iberoamérica,** se incorporan **todas las respuestas recibidas,** independientemente del país de origen.

Por su parte, en los **reportes individuales de las instituciones** pertenecientes a los **cuatro países que no alcanzaron el umbral mínimo de respuestas,** la información se presenta únicamente en comparación con los valores agregados de Iberoamérica.

En la siguiente tabla se detallan, para cada estrato, los valores correspondientes al **universo poblacional,** la **muestra esperada** y las **respuestas recibidas,** agrupando los países o zonas en función del grado de cumplimiento de las respuestas previstas.

Gráfico 72: Ficha técnica del IMC 2025.

	Tamaño de los estratos en la población			Tamaño de los estratos de la muestra			Respuestas recibidas por estrato		
	PÚBLICAS	PRIVADAS	TOTAL	PÚBLICAS	PRIVADAS	TOTAL	PÚBLICAS	PRIVADAS	TOTAL
ARGENTINA	71	66	137	18	18	36	24	12	36
BRASIL	312	2.283	2.595	23	24	47	10	30	40
CHILE	25	30	55	13	13	26	14	29	43
COLOMBIA	121	265	386	21	22	43	7	38	45
ECUADOR	33	27	60	14	13	27	14	10	24
ESPAÑA	50	34	84	17	14	31	21	4	25
MÉXICO	822	2.526	3.348	24	24	48	39	8	47
PERÚ	52	46	98	17	16	33	6	17	23
PORTUGAL	42	60	102	16	18	34	21	3	24
CENTROAM./ CARIBE	9	12	21	7	8	15		1	1
TOTAL GENERAL	1.537	5.349	6.886	170	170	340	156	152	308

IMC 2025

Índice de Madurez en Ciberseguridad de las IES Iberoamericanas

metared by universia

Secretaría General Iberoamericana
Secretaria-Geral Ibero-Americana