ARGENTINA

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

ARGENTINA IMC 2025

Índice de Madurez en Ciberseguridad de las IES Iberoamericanas

metared by universia

Secretaría General Iberoamericana
Secretaria-Geral Ibero-Americana

Contenidos IMC 2025.

Prólogo

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

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

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

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

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

Vamos en la dirección correcta.

Sigamos empujando.

Rafael Hernández

Vicepresidente de Fundación Universia

Presentación

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

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

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

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

MetaRed TIC 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

1.

Conclusiones

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

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

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

Aumento en la participación:
308 IES
9 países.

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

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

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

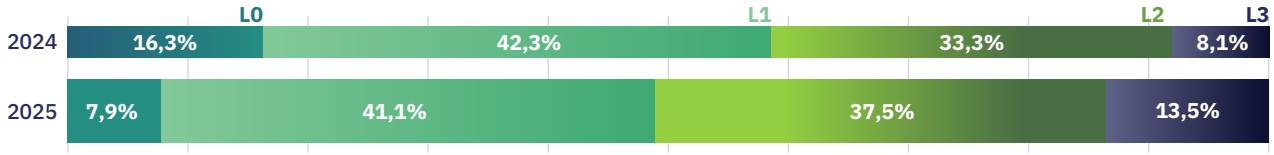
Un ecosistema en plena evolución

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

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

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

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



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

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

Iberoamérica avanza hacia un nuevo nivel de madurez.

Los motores del cambio: Inversión y Talento como factores decisivos

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

INVERTIR ES PROGRESAR: EL PRESUPUESTO COMO PALANCA DE MADUREZ

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

Los patrones de tendencia encontrados son los siguientes:

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

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

EL FACTOR HUMANO: EQUIPOS ESPECIALIZADOS COMO ACELERADORES DEL CAMBIO

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

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

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

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

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

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

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

FORTALEZAS CONSOLIDADAS

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

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

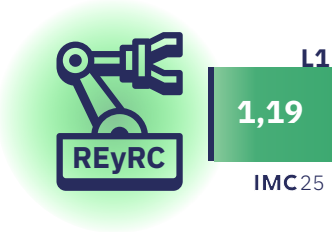
Esta evolución indica que las IES iberoamericanas están mejorando de forma decidida su capacidad para conocer sus activos, gestionar riesgos e implementar controles de monitoreo continuo, sentando las bases de una defensa más proactiva.

Avances en identificación, protección y detención

PRINCIPALES DEBILIDADES

- El informe identifica de manera inequívoca al dominio **Responder y Recuperar (REyRC)** como la principal debilidad estructural de la región. Con un IMC de solo **1,19** y un avance mínimo de +0,09 puntos, este dominio permanece anclado en un nivel básico.
- Las implicaciones de esta debilidad son estratégicas: sin una capacidad de respuesta y recuperación eficaz, la resiliencia global de las instituciones permanece limitada, sin importar cuánto mejoren en prevención y detección. Esta sigue siendo la "principal tarea pendiente para las IES iberoamericanas".

La respuesta y la recuperación siguen siendo la tarea pendiente



RETOS

HETEROGENEIDAD

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

Múltiples realidades en la ciberseguridad universitaria.

UN AVANCE A MÚLTIPLES VELOCIDADES

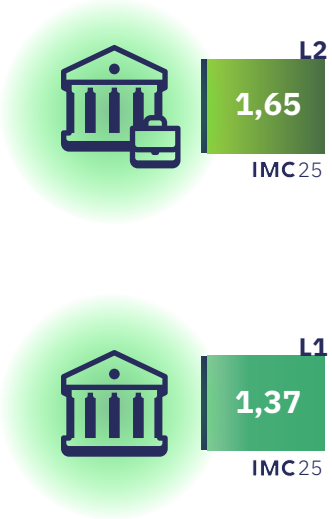
El progreso en ciberseguridad no es uniforme en toda la región, con países que lideran la adopción de prácticas avanzadas y otros que avanzan a un ritmo más moderado.

- **Líderes por encima de la media: España (1,88), Colombia (1,75), Perú (1,59) y Brasil (1,55**) se consolidan como los países con mayor nivel de madurez, superando el promedio regional (1,51).
- **El mayor crecimiento: Ecuador** destaca como el país con el mayor incremento anual, mejorando su IMC en **+0,37** puntos y reduciendo significativamente su brecha con la media.
- **Progreso Sostenido: Argentina y España** también muestran un avance notable, con un incremento de +0,15 puntos cada uno.
- **Ritmo Moderado: México, Chile y Portugal** presentan un crecimiento más lento en el último año.

BRECHA PÚBLICO-PRIVADA

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

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



EL ROL DE LA INTELIGENCIA ARTIFICIAL

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

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

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

Despliegue incipiente y desigual

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

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

Conclusiones estratégicas

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

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

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

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

Hacia una ciberseguridad resiliente e integrada

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

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

2.

IMC Argentina

ARG

IMC24
1,06 L1
1,21 L1
IMC25

IMC ARGENTINA
1,21

2024-2025 EVOLUCIÓN
+0,15

IMC IBE DIFERENCIA
-0,30

L0 L1 L2 L3

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)

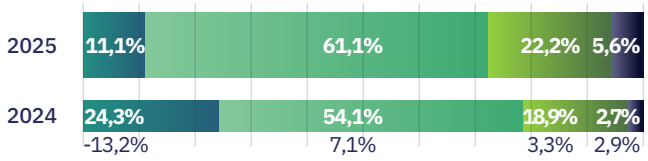
TOP 3
PROTEGER
DETECTAR
IDENTIFICAR

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.

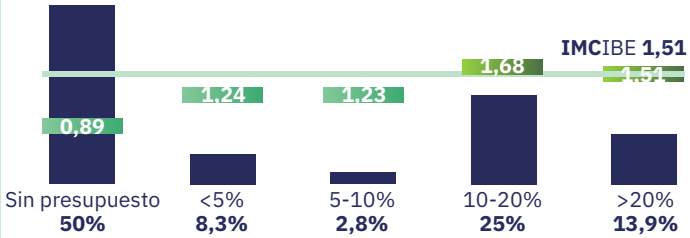
DISTRIBUCIÓN SEGÚN IMC



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

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

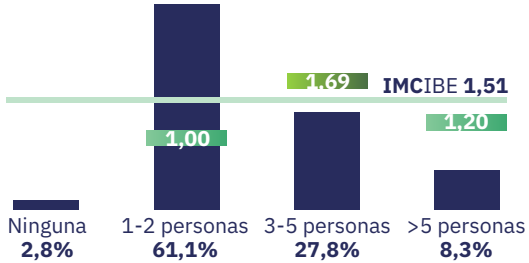
PRESUPUESTO



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.

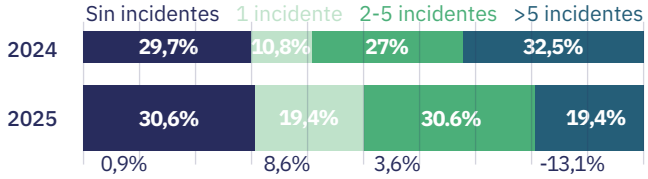
EQUIPOS DE CIBERSEGURIDAD



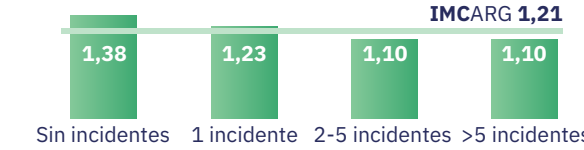
El 92% de equipos de ciberseguridad argentinos están compuestos por 5 o un número menor de personas.

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.

3.

Resumen Ejecutivo

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.

ARGENTINA

IMC 2025

Índice de Madurez en Ciberseguridad de las IES Iberoamericanas

metared by universia

Secretaría General Iberoamericana
Secretaria-Geral Ibero-Americana