PERÚ

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

PERÚ

IMC 2025

Índice de Madurez en Ciberseguridad de las IES Iberoamericanas

metaRed by universia

Secretaría General Iberoamericana
Secretaria-Geral Ibero-Americana

Contenidos IMC 2025.

Prólogo 5
Presentación 6
1. Conclusiones 7
2. IMC Perú 16
3. Resumen Ejecutivo 18
3.1 Brecha entre universidades públicas y privadas 19
3.2 Distribución de niveles de madurez 19
3.3 Desempeño por dominios 20
3.4 Impacto del tamaño del equipo de ciberseguridad 20
3.5 Influencia del presupuesto en ciberseguridad 21
3.6 Incidentes de seguridad: evolución y relación con la madurez 21
3.7 Uso de la Inteligencia Artificial en ciberseguridad 22

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 Perú
Silvana Balarezo

Universidad Peruana
de Ciencias Aplicadas
Gerente de Experiencia
de Aprendizaje Digital

1.

Conclusiones

- Un ecosistema en plena evolución
- Los motores del cambio: Inversión y Talento como factores decisivos
- Radiografía de la madurez
- Conclusiones estratégicas

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

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

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

Aumento en la participación:
308 IES
9 países.

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

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

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

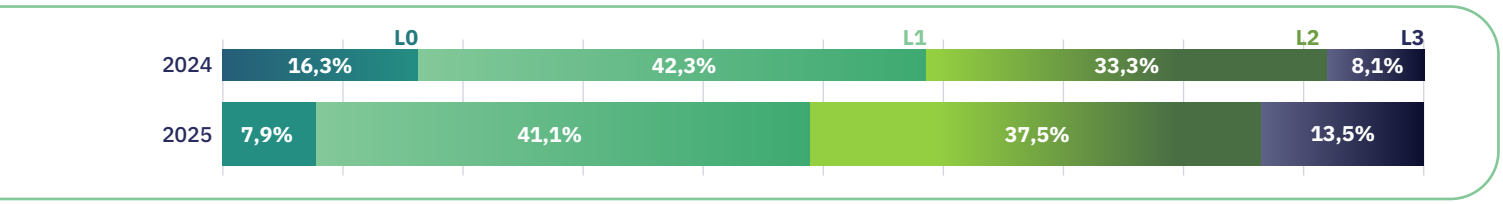
Un ecosistema en plena evolución

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

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

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

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



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

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

Iberoamérica avanza hacia un nuevo nivel de madurez.

Los motores del cambio: Inversión y Talento como factores decisivos

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

INVERTIR ES PROGRESAR: EL PRESUPUESTO COMO PALANCA DE MADUREZ

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

Los patrones de tendencia encontrados son los siguientes:

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

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

EL FACTOR HUMANO: EQUIPOS ESPECIALIZADOS COMO ACELERADORES DEL CAMBIO

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

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

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

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

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

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

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

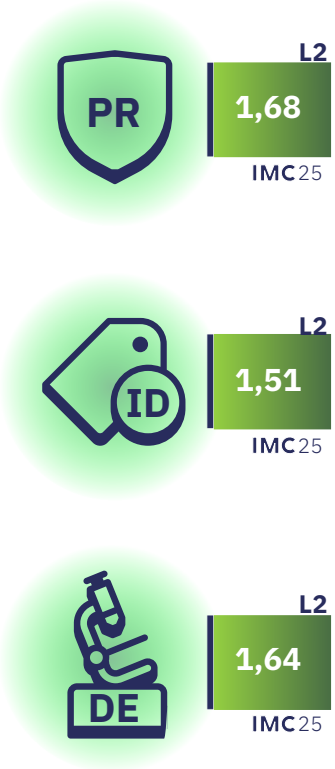
FORTALEZAS CONSOLIDADAS

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

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

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

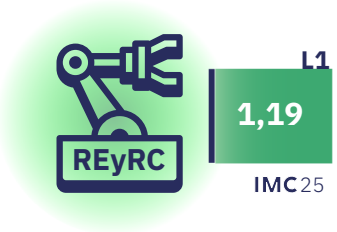
Avances en identificación, protección y detención



PRINCIPALES DEBILIDADES

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

La respuesta y la recuperación siguen siendo la tarea pendiente



RETOS

HETEROGENEIDAD

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

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.

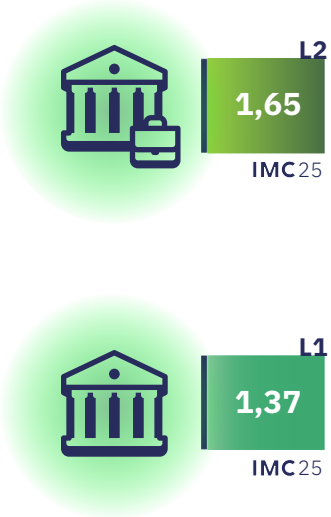
Múltiples realidades en la ciberseguridad universitaria.

- **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 Perú

PER

L0 L1 L2 L3

1,59 L2

IMC25

IMC PERÚ

1,59

IMC IBE DIFERENCIA

+0,08

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

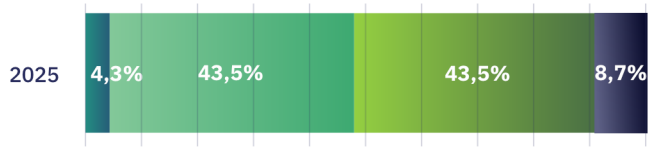
GOBERNAR

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.

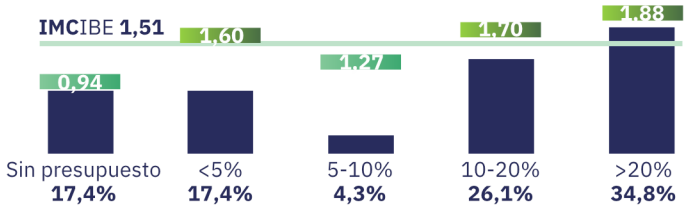
Proteger (1,77) presenta el valor más alto, solo superado por Colombia (2,00) y España (1,92).

DISTRIBUCIÓN SEGÚN IMC



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

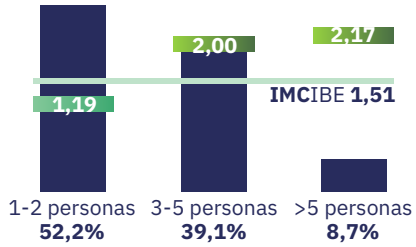
PRESUPUESTO



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

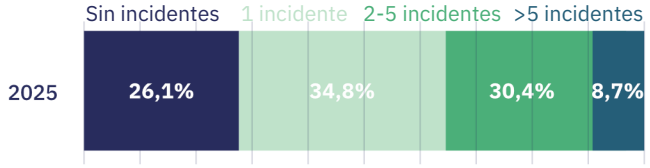


La mayoría de equipos de ciberseguridad están compuestos por 1-2 personas (52%).

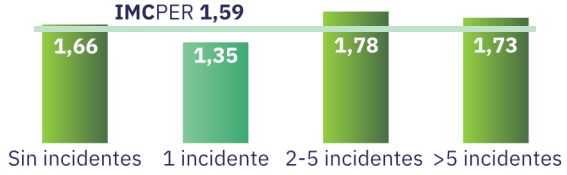
Clara tendencia alcista en el nivel de madurez de aquellas IES con equipos de mayor tamaño.

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.

3.

Resumen Ejecutivo

3.1 Brecha entre universidades públicas y privadas

3.2 Distribución de niveles de madurez

3.3 Desempeño por dominios

3.4 Impacto del tamaño del equipo de ciberseguridad

3.5 Influencia del presupuesto en ciberseguridad

3.6 Incidentes de seguridad: evolución y relación con la madurez

3.7 Uso de la Inteligencia Artificial en ciberseguridad

RESUMEN EJECUTIVO 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.

PERÚ

IMC 2025

Índice de Madurez en Ciberseguridad de las IES Iberoamericanas

metared by universia

Secretaría General Iberoamericana
Secretaria-Geral Ibero-Americana