CHILE

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

CHILE

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 Chile
Álvaro Fuentes Maldonado
Universidad Autónoma de Chile
Director corporativo de tecnologías

1.

Conclusiones

Un ecosistema en plena evolución

Los motores del cambio: Inversión y Talento como factores decisivos

Radiografía de la madurez

Conclusiones estratégicas

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

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

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

Aumento en la participación:
308 IES
9 países.

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

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

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

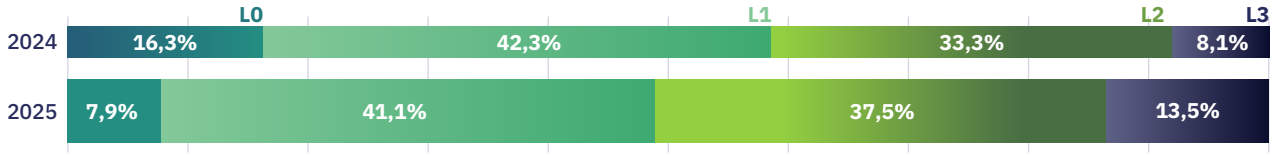
Un ecosistema en plena evolución

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

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

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

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



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

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

Iberoamérica avanza hacia un nuevo nivel de madurez.

Los motores del cambio: Inversión y Talento como factores decisivos

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

INVERTIR ES PROGRESAR: EL PRESUPUESTO COMO PALANCA DE MADUREZ

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

Los patrones de tendencia encontrados son los siguientes:

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

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

EL FACTOR HUMANO: EQUIPOS ESPECIALIZADOS COMO ACELERADORES DEL CAMBIO

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

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

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

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

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

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

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

FORTALEZAS CONSOLIDADAS

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

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

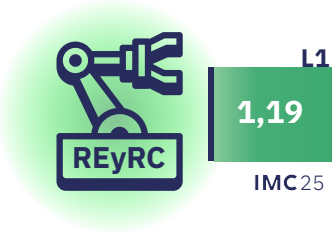
Esta evolución indica que las IES iberoamericanas están mejorando de forma decidida su capacidad para conocer sus activos, gestionar riesgos e implementar controles de monitoreo continuo, sentando las bases de una defensa más proactiva.

Avances en identificación, protección y detención

PRINCIPALES DEBILIDADES

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

La respuesta y la recuperación siguen siendo la tarea pendiente



RETOS

HETEROGENEIDAD

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

Múltiples realidades en la ciberseguridad universitaria.

UN AVANCE A MÚLTIPLES VELOCIDADES

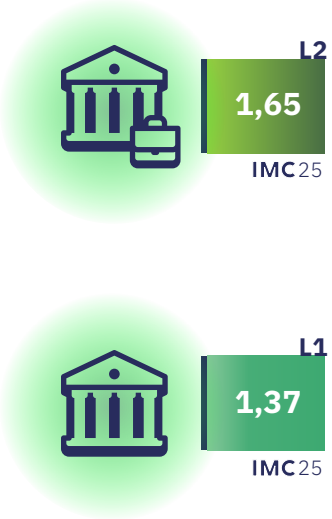
El progreso en ciberseguridad no es uniforme en toda la región, con países que lideran la adopción de prácticas avanzadas y otros que avanzan a un ritmo más moderado.

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

BRECHA PÚBLICO-PRIVADA

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

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



EL ROL DE LA INTELIGENCIA ARTIFICIAL

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

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

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

Despliegue incipiente y desigual

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

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

Conclusiones estratégicas

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

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

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

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

Hacia una ciberseguridad resiliente e integrada

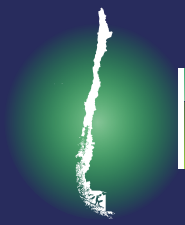
En síntesis, IMC funciona como un **predictor sólido del comportamiento real** frente a ciberamenazas. Invertir en madurez —tanto en estructura organizativa como en procesos y capacidades técnicas— se refleja directamente en una reducción del riesgo y del número de incidentes que afectan al funcionamiento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

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

2.

IMC Chile

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)

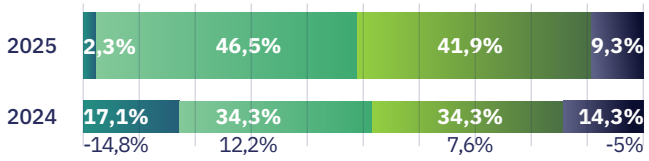
RESPONDER
1,16 (-0,03)

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.

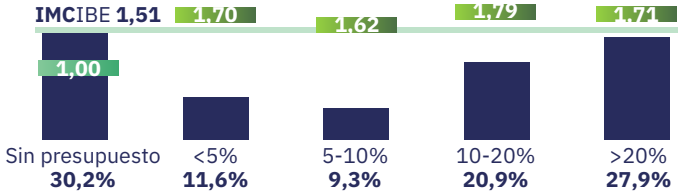
DISTRIBUCIÓN SEGÚN IMC



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).

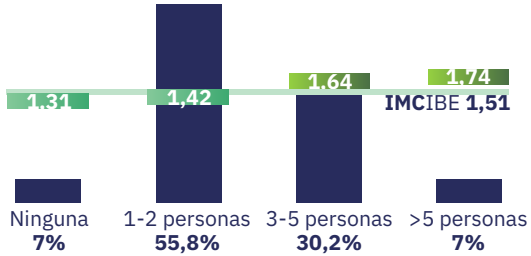
PRESUPUESTO



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.

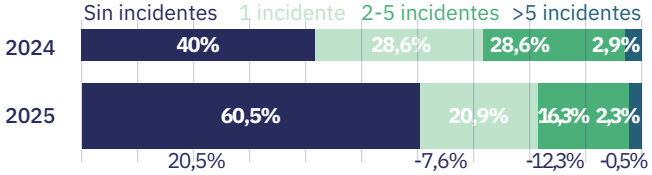
EQUIPOS DE CIBERSEGURIDAD



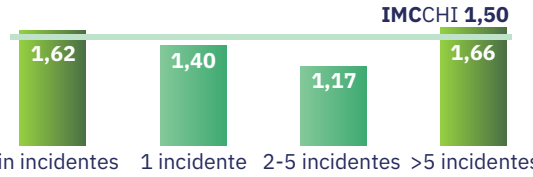
Más del 90% están compuestos por menos de 5 personas. Se observa una clara relación directa entre el tamaño de los equipos de seguridad y el nivel de madurez.

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.

3.

Resumen Ejecutivo

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.

CHILE

IMC 2025

Índice de Madurez en Ciberseguridad de las IES Iberoamericanas

metared by universia

Secretaría General Iberoamericana
Secretaria-Geral Ibero-Americana