BRASIL

IMC 2025

Índice de Maturidade em Cibersegurança das IES Ibero-Americanas

meta red by universia

Secretaría General Iberoamericana
Secretaria-Geral Ibero-Americana

Realizado por
MetaRed by Universia - Fundación Universia

Direção
Jesús Martínez Martínez

Equipa técnica
Jesús Martínez Martínez
Patricia Pandrini
Paula Venosa
Gastón Zamorano Seguel
Daniel Felipe Genta García
Ricardo Estévez Serrano

Edição
MetaRed by Universia - Fundación Universia

Design
María Moraleja Vicente

BRASIL IMC 2025

Índice de Maturidade em Cibersegurança das IES Ibero-Americanas

metared by universia

Secretaría General Iberoamericana
Secretaria-Geral Ibero-Americana

Conteúdo IMC 2025.

Prólogo

Em um momento em que a transformação digital está redefinindo a universidade, na MetaRed temos uma convicção firme: la cibersegurança deixou de ser um assunto técnico para se tornar um pilar estratégico sem o qual não há futuro digital possível. Proteger o que somos e o que construímos é hoje indispensável para manter a confiança e garantir que nossas instituições possam avançar sem medo.

Essa realidade é o que nos impulsiona a fortalecer a colaboração e o apoio mútuo. Nenhuma universidade pode percorrer esse caminho sozinha, e é aí que a MetaRed ganha sentido: **conectar talentos, compartilhar experiências e construir soluções comuns para desafios que também são comuns.**

Com essa ambição nasceu, em 2024, o Índice de Maturidade em Cibersegurança (IMC). O que começou como uma iniciativa modesta tornou-se, em um ano, uma ferramenta-chave para a região. A edição de 2025 demonstra isso: 308 instituições e um projeto que passa de 7 para 9 países com a incorporação do Brasil e do Peru. Mais do que números, são sinais de confiança e de um projeto que já não é piloto, mas sim um instrumento real para orientar a melhoria institucional.

Mas o valor do IMC não reside apenas nos dados, e sim no que possibilita como comunidade: **aprender, nos comparar, melhorar e decidir com maior clareza.** Cada indicador e cada análise deste relatório são um convite para avançar de forma conjunta e fortalecer nossas capacidades.

Na MetaRed, mantemos um compromisso claro: **continuar construindo um ecossistema universitário ibero-americano mais forte, mais seguro e melhor preparado.** A cibersegurança não é um desafio que se supera em um ano; é um caminho, e percorrê-lo acompanhados faz toda a diferença.

Estamos na direção certa.

Vamos continuar avançando.

Rafael Hernández

Vice-presidente da Fundación Universia

Apresentação

A digitalização avança em um ritmo vertiginoso e, com ela, cresce também a exposição das instituições a novas ameaças. Nesse cenário, a cibersegurança já não é apenas uma questão tecnológica: é um eixo estratégico para garantir a confiança, a continuidade e a resiliência de nossas universidade.

O **Índice de Maturidade em Cibersegurança das IES ibero-americanas (IMC)** nasceu em 2024 com um propósito claro: oferecer às instituições um marco de referência que lhes permita conhecer sua situação, comparar-se com seus pares e orientar seus esforços de melhoria. No entanto, seu verdadeiro valor se revela ao repetir o exercício ano após ano, pois somente assim é possível medir a evolução, identificar tendências e aprender coletivamente.

A edição de 2025 marca um passo decisivo nesse caminho: **308 Instituições de Ensino Superior participaram, ampliando a base de 7 para 9 países com a incorporação do Brasil e do Peru.** Esse crescimento reforça a representatividade do relatório e consolida o IMC como a principal ferramenta de diagnóstico e acompanhamento da maturidade em cibersegurança universitária na Ibero-América.

Medir não é suficiente se não se transforma em aprendizado. Por isso, o **IMC 2025** não apenas apresenta resultados, mas também **mostra como cada instituição evolui diante dos desafios da segurança digital,** como as capacidades compartilhadas são fortalecidas e como se constrói, passo a passo, um ecossistema universitário ibero-americano mais seguro, conectado e resiliente.

MetaRed TIC Brasil

Domingos Sávio Alcântara Machado

Universidade Tiradentes

Vice-Presidência de Estratégia, Internacionalização e Inovação

1.

Conclusões

Um ecossistema em plena

Os motores da mudança: Investimento e Talento como fatores decisivos

Radiografia da maturidade

Conclusões estratégicas

O Índice de Maturidade em Cibersegurança (IMC) 2025 marca um marco na avaliação da segurança digital no setor de educação superior ibero-americano.

O Índice de Maturidade em Cibersegurança (IMC) 2025 marca um marco na avaliação da segurança digital no setor de educação superior ibero-americano. Esta segunda edição não apenas oferece um retrato atualizado do estado da cibersegurança, mas também, pela primeira vez, permite uma análise evolutiva rigorosa para medir o progresso e as tendências na região. O notável crescimento na participação, que alcança **308 Instituições de Ensino Superior (IES) de 9 países,** consolida o IMC como a principal ferramenta de diagnóstico e acompanhamento estratégico em nível regional. Este relatório revela um achado fundamental: o ecossistema universitário ibero-americano deu um salto qualitativo, avançando de forma coletiva para um novo e mais robusto nível de maturidade.

O modelo mantém a coerência com o estudo anterior e se baseia na versão 2.0 do **Cybersecurity Framework** *do National Institute of Standards and Technology (NIST)* dos Estados Unidos. Além disso, integra práticas e controles de padrões internacionais como **ISO/IEC 27001:2022, ISO/IEC 27002:2022 e o Esquema Nacional de Segurança (ENS) da Espanha,** garantindo uma cobertura completa e atualizada dos aspectos-chave da segurança da informação.

Aumento da participação:
308 IES
9 países.

Uma novidade em 2025 é a incorporação de questões relacionadas ao **uso de ferramentas de inteligência artificial (IA)** e suas implicações na cibersegurança. Esse enfoque híbrido, que combina marcos internacionais consolidados com novas dimensões tecnológicas, oferece um modelo robusto, contextualizado e alinhado com os desafios atuais da região.

Em síntese, o IMC 2025 dá continuidade ao caminho iniciado em 2024, consolidando um marco de referência sólido e eficaz para a avaliação e a melhoria da maturidade em cibersegurança nas IES da Ibero-América.

O IMC foi atualizado:
incorporação questões sobre o uso de ferramentas de IA.

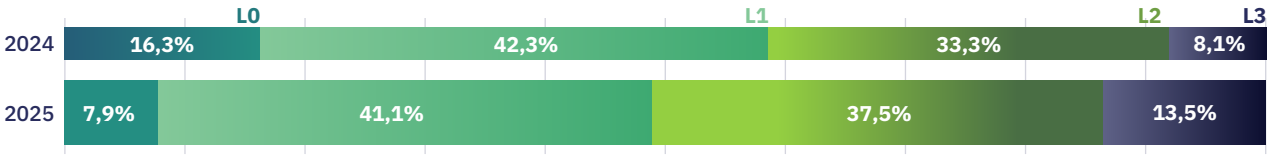
Um ecossistema em plena evolução

O IMC ibero-americano global avançou de 1,37 (Nível Básico - L1) em 2024 para 1,51 (Nível Intermediário - L2) em 2025. Este avanço representa um marco estratégico. Em termos práticos, evidencia uma mudança fundamental em direção a um "uso mais amplo de práticas avançadas, a definição e documentação de políticas e procedimentos e a alocação de recursos adequados para apoiar os processos".

Essa evolução se manifesta claramente na distribuição das instituições por níveis de maturidade, onde se observa um deslocamento significativo em direção aos estágios mais avançados:

De Básico a Intermediário: um salto qualitativo para a Região.

Gráfico 1: Comparação dos níveis de maturidade. Evolução 2024-2025.



A análise dessa transição revela duas tendências-chave: uma **redução drástica das instituições no nível inicial (L0), que cai 8,4 pontos percentuais,** e um **crescimento notável nos níveis intermediário e avançado (L2 e L3), que, em conjunto, aumentam sua representatividade em mais de 9,5 pontos percentuais.**

Esse avanço geral se sustenta em fatores determinantes como a alocação de orçamentos específicos e a crescente especialização das equipes, que atuam como verdadeiros motores da mudança.

Ibero-América avança para um novo nível de maturidade.

Os motores da mudança: Investimento e Talento como fatores decisivos

Uma leitura transversal do relatório revela dois fatores que explicam de forma contundente as diferenças de maturidade entre instituições: a existência de um orçamento formal de cibersegurança e a disponibilidade de equipes especializadas.

INVESTIR É PROGREDIR: O ORÇAMENTO COMO ALAVANCA DE MATURIDADE

Os dados mostram uma correlação inequívoca entre investimento e maturidade. **As universidades que investem 5% ou mais do seu orçamento de TI em cibersegurança alcançam níveis de maturidade significativamente superiores.**

Os padrões de tendência identificados são os seguintes:

- **Intervalo de investimento: faixa de 5-10% do orçamento de TI** não apenas alcança o IMC mais alto (1,79), como também apresenta o maior salto de maturidade (+0,23 pontos) em relação ao ano anterior. Esse dado sugere que 5-10% representa o limiar de investimento mais eficiente, no qual os recursos são suficientes para viabilizar um ecossistema de segurança integral (pessoas, processos e tecnologia).
- **O risco da inação:** O dado mais preocupante é que **uma em cada três instituições (33,4%) ainda não possui orçamento.** Esse grupo não apenas não evolui, como retrocede em sua maturidade, passando de um IMC de 1,34 para 1,13. Esse retrocesso é o principal fator que freia um avanço regional mais rápido e alimenta diretamente o grupo de IES atrasadas no Nível Básico (L1), ampliando a lacuna de maturidade em vez de reduzi-la.
- **Tendência à formalização:** Observa-se uma evolução positiva em direção à institucionalização dos gastos. Aumentam as **partidas específicas dentro de TI (+4,0 pontos) e os orçamentos diferenciados (+1,5 pontos),** enquanto diminuem as alocações gerais não específicas.

O ajuste do investimento e a formalização do orçamento são condições indispensáveis para planejar, medir e sustentar as capacidades de cibersegurança. Esse recurso financeiro é o que permite viabilizar o outro pilar fundamental: o capital humano.

O FATOR HUMANO: EQUIPES ESPECIALIZADAS COMO ACELERADORES DA MUDANÇA

Assim como no IMC 2024, a análise dos dados de 2025 demonstra que **a dimensão das equipes de cibersegurança é o fator mais determinante da maturidade.**

A disponibilidade de pessoal dedicado e especializado tem um impacto direto e massivo no IMC de uma instituição.

- **Liderança consolidada:** As IES com equipes de **mais de 5 pessoas** lideram com um IMC de 1,93, muito acima da média regional (1,51).
- **Alto risco:** No extremo oposto, aquelas **sem pessoal especializado** alcançam apenas um IMC de 1,03, um nível de maturidade básico e insuficiente para enfrentar o atual cenário de ameaças.
- **Ponto de inflexão:** O salto qualitativo mais significativo ocorre ao consolidar equipes de **3 a 5 pessoas,** que melhoram seu IMC de 1,60 para 1,80 em um único ano, demonstrando ser o limiar que acelera a institucionalização das práticas de segurança.

A diferença entre as universidades com equipes grandes e aquelas que não possuem equipes supera seis décimos de IMC, marcando uma diferença estrutural. Essa evidência reforça que investir em talento não é um custo, mas sim o principal acelerador da mudança.

A dimensão das equipes de cibersegurança é o fator mais determinante da maturidade.

Radiografia da maturidade: Forças, fraquezas e o grande desafio pendente

Embora a região apresente uma melhoria generalizada, a análise detalhada por domínios revela um padrão de desenvolvimento claro e consistente. As instituições ibero-americanas conseguiram consolidar fortemente suas capacidades de prevenção e monitoramento, mas enfrentam uma fraqueza persistente em sua capacidade de resposta a incidentes. Esse padrão de desenvolvimento assimétrico revela uma estratégia regional centrada na prevenção, mas com uma perigosa falta de preparação para o "dia seguinte". Ainda que muros mais altos estejam sendo construídos, não existem planos eficazes de resposta e recuperação, o que pode deixar as instituições em um estado de falsa segurança.

FORÇAS CONSOLIDADAS

O progresso regional concentra-se em três domínios-chave que constituem o núcleo das capacidades preventivas:

- O domínio **Proteger (PR)** mantém-se como o mais sólido em termos absolutos, alcançando um IMC de 1,68. Isso confirma que a implementação de controles técnicos continua sendo a principal prioridade das IES.
- Os domínios **Identificar (ID) e Detetar (DE),** com 1,51 e 1,64 respectivamente, são os que apresentam maior crescimento, com aumentos de +0,19 e +0,17 pontos.

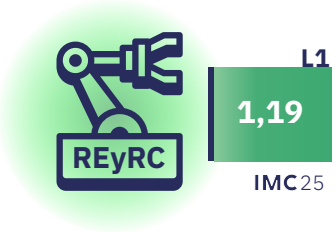
Essa evolução indica que as IES ibero-americanas estão aprimorando de forma consistente sua capacidade de conhecer seus ativos, gerenciar riscos e implementar controles de monitoramento contínuo, estabelecendo as bases para uma defesa mais proativa

Avanços em Identificar, Proteger e Detetar.

PRINCIPAIS FRAQUEZAS

- O relatório identifica de forma inequívoca o domínio **Responder e Recuperar (REyRC)** como a principal fraqueza estrutural da região. Com um IMC de apenas 1,19 e um avanço mínimo de +0,09 pontos, esse domínio permanece em um nível básico.
- As implicações dessa fraqueza são estratégicas: sem uma capacidade eficaz de resposta e recuperação, a resiliência global das instituições permanece limitada, independentemente de quanto avancem em prevenção e detecção. Essa continua sendo a principal tarefa pendente para as IES ibero-americanas.

Resposta e Recuperação continuam sendo a tarefa pendente



DESAFIOS

HETEROGENEIDADE

A média ibero-americana de 1,51 oculta um mosaico de realidades muito diversas. A análise das diferenças por país e por tipo de instituição é fundamental para compreender as lacunas existentes e desenhar estratégias de melhoria eficazes e contextualizadas, reconhecendo que não existe um único caminho para a maturidade.

múltiplas realidades na cibersegurança universitária.

UM AVANÇO EM MÚLTIPLAS VELOCIDADES

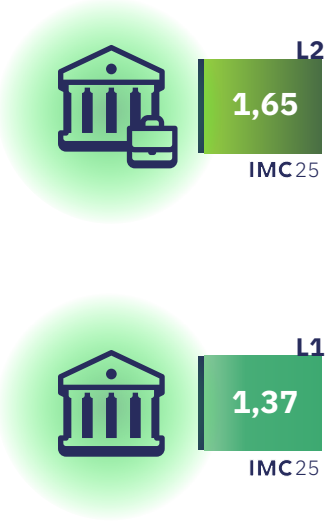
O progresso em cibersegurança não é uniforme em toda a região, com países que lideram a adoção de práticas avançadas e outros que avançam em um ritmo mais moderado.

- **Líderes acima da média: España (1,88), Colombia (1,75), Perú (1,59) y Brasil (1,55**) consolidam-se como os países com maior nível de maturidade, superando a média regional (1,51).
- **Maior crescimento: O Ecuador** destaca-se como o país com o maior incremento anual, melhorando seu IMC em **+0,37** pontos e reduzindo significativamente sua lacuna em relação à média.
- **Progresso sustentado: Argentina y España** também apresentam avanços relevantes, com incremento de +0,15 pontos cada.
- **Ritmo moderado: México, Chile e Portugal** apresentam um crescimento mais lento no último ano.

LACUNA PÚBLICO-PRIVADA

A tipologia da instituição é outro fator diferenciador chave. Os dados de 2025 confirmam e ampliam uma tendência já observada:

- As **IES privadas (IMC 1,65)** apresentam, em média, um nível de maturidade superior às **IES públicas (IMC 1,37).**
- A lacuna entre ambos os tipos de instituição aumentou no último ano. As privadas avançaram em um ritmo quase duas vezes maior (+0,15 pontos) do que as públicas (+0,09 pontos), o que sugere maior agilidade na alocação de recursos e na tomada de decisões.
- Essa tendência não é universal. Existem exceções relevantes: **na Colômbia e em Portugal, as universidades públicas superam as privadas, enquanto na Espanha ambos os setores alcançaram paridade,** demonstrando um desenvolvimento equilibrado.



O PAPEL DA INTELIGÊNCIA ARTIFICIAL

Pela primeira vez, o IMC 2025 analisa o uso da Inteligência Artificial (IA) como uma capacidade emergente na cibersegurança universitária. Os resultados revelam uma implantação ainda incipiente e desigual, mas com padrões claros de adoção que apontam para seu potencial como ferramenta de defesa.

O uso da IA em cibersegurança caracteriza-se atualmente pelos seguintes aspectos:

- **Concentração operacional:** O uso da IA concentra-se nos domínios mais técnicos. **38,3%** das IES a utilizam em tarefas de **Proteger** e **32,5%** em **Detetar,** principalmente para automatizar o monitoramento e a análise de ameaças.
- **Ausencia Estratégica:** Sua presença é mínima em áreas de governança e resposta, como **Governar (10,1%) e Responder e Recuperar (11,0%),** indicando que ainda não foi integrada à tomada de decisões estratégicas.

Implantação incipiente e desigual.

- **Adoção heterogênea:** A implantação é desigual entre países. **Brasil, Chile e Equador** posicionam-se na liderança da adoção, enquanto outros países apresentam um uso mais prudente e limitado.

A IA, tal como é utilizada atualmente, reforça a capacidade defensiva, mas não resolve a fraqueza estrutural da região: identificar antes não implica responder melhor. Se não for acompanhada por estruturas maduras de resposta, a lacuna entre alerta e ação pode inclusive se ampliar

Conclusões estratégicas

O IMC 2025 confirma que o ecossistema universitário ibero-americano deu um passo firme rumo à maturidade, refletindo um esforço coletivo e um compromisso crescente com a cibersegurança. No entanto, esse progresso generalizado evidencia três imperativos estratégicos que serão determinantes para alcançar um estado de resiliência sustentável.

- **Institucionalizar o investimento:** É imperativo superar a dependência de alocações gerais e formalizar orçamentos específicos para cibersegurança. A evidência é clara: sem investimento planejado, não há avanço sustentado.
- **Investir em talento:** A dimensão e a especialização das equipes de cibersegurança são o fator crítico de sucesso. As instituições devem priorizar a atração e retenção de talento como o principal acelerador da maturidade.
- **Superar a tarefa pendente:** A região deve concentrar seus esforços em fortalecer as capacidades de resposta e recuperação. Uma defesa robusta é incompleta sem planos eficazes para gerenciar e recuperar-se de incidentes.

Rumo a uma cibersegurança resiliente e integrada.

Em síntese, o IMC funciona como um **preditor sólido do comportamento real** diante de ciberameaças. Investir em maturidade — tanto na estrutura organizacional quanto em processos e capacidades técnicas — reflete-se diretamente na redução do risco e no número de incidentes que afetam o funcionamento das instituições de ensino superior.

O futuro de uma universidade digitalmente robusta e resiliente não depende apenas da aquisição de tecnologia, mas da decisão de seus líderes de institucionalizar o investimento, profissionalizar o talento e dominar a capacidade de resposta.

2.

IMC Brasil

BRA

1,55 L2

IMC25

IMC BRASIL

1,55

DIFERENÇA IMC IBE

+0,04

L0 L1 L2 L3

TIPOS DE IES

PÚBLICAS 1,31

PRIVADAS 1,64

DOMÍNIOS

*evolução nos domínios IBE do IMC

PROTEGER 1,75 (+0,07)

DETETAR 1,68 (+0,04)

GOVERNAR 1,59 (+0,04)

IDENTIFICAR 1,54 (+0,03)

RESPONDER 1,28 (+0,09)

TOP 3

PROTEGER

DETETAR

GOVERNAR

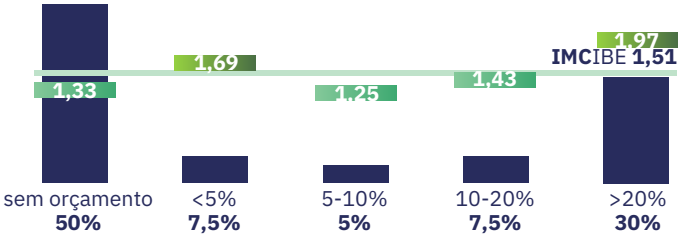
As pontuações em Proteger, Detetar, Governar e Identificar superam a média ibero-americana. Proteger se destaca com uma pontuação de 1,75.

Responder e Recuperar apresentam a pontuação mais baixa (1,28) para o país. No entanto, supera a média ibero-americana para esse domínio (1,19).

DISTRIBUIÇÃO SEGUNDO IMC

7 de cada 10 IES brasileiras estão nos níveis básico (L1) e intermediário (L2), distribuídas em proporções praticamente semelhantes.

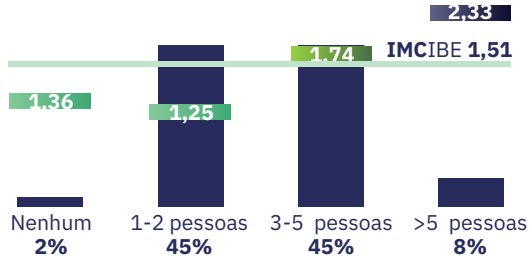
ORÇAMENTO



Metade das IES brasileiras não conta com orçamento de cibersegurança.

O nível de maturidade mais alto (1,97, quase o nível L3) corresponde às IES com orçamento alocado superior a 20%

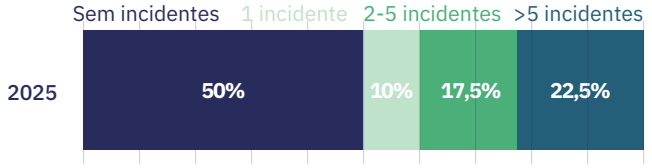
EQUIPES DE CIBERSEGURANÇA



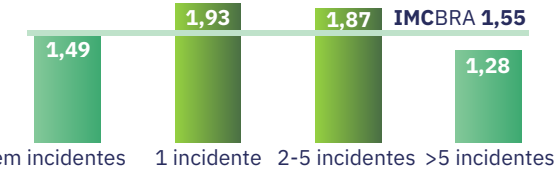
Mais de 90% são compostas por menos de 5 pessoas. O IMC atinge seu valor mais alto para instituições de ensino superior com equipes de mais de 5 pessoas (2,33, nível L3).

CIBERINCIDENTES

DISTRIBUIÇÃO DE INCIDENTES



EVOLUÇÃO DO IMC SEGUNDO O NÚMERO DE INCIDENTES



8 de cada 10 instituições brasileiras sofreram algum ciberincidente no último ano

3.

Resumo Executivo

RESUMO EXECUTIVO BRASIL

Brasil se incorpora com um dos níveis de maturidade mais elevados de toda a Ibero-América.

O Brasil participa pela primeira vez no Índice de Maturidade em Cibersegurança (IMC) em 2025. Como não existem dados correspondentes a 2024, não é possível realizar uma análise evolutiva comparável à dos demais países. Será nas próximas edições que será possível observar a trajetória do país e avaliar com maior precisão a consolidação de suas capacidades. No entanto, a fotografia inicial apresentada em 2025 já é muito relevante e posiciona o Brasil como um dos ecossistemas universitários mais maduros do estudo.

Em 2025, o Brasil obtém um **IMC médio de 1,55,** superando a média regional (1,51) e situando-se bem acima da maioria dos países avaliados. Embora muito próximo do nível 1, encontra-se dentro do nível intermediário (L2), o que é particularmente significativo para um país que participa pela primeira vez. Esse resultado sugere a existência de um ecossistema universitário com **capacidade técnica consolidada,** infraestruturas maduras e uma abordagem geral à cibersegurança mais estruturada do que a de outros países latino-americanos que participam do estudo há vários anos.

DISTRIBUIÇÃO DOS NÍVEIS DE MATURIDADE

A distribuição dos níveis confirma o bom ponto de partida do país, mas deve ser interpretada com certa cautela. Pouco mais de **7%** das instituições brasileiras aparece no nível incipiente (L0), algo pouco habitual no contexto ibero-americano. Cerca de **33%** das instituições situam-se no nível básico (L1), enquanto **40%** já operam no nível intermediário (L2). O restante, representado por **20%,** encontra-se no nível avançado (L3). Esse resultado sugere um ecossistema sem camadas particularmente atrasadas e com uma base de capacidades relativamente disseminada.

No entanto, essa leitura deve ser relativizada: o Brasil possui **um sistema universitário muito amplo e heterogêneo,** e o conjunto de instituições participantes em 2025 representa apenas uma parte do total. Isso implica que, embora os dados disponíveis apresentem uma imagem sólida, não podem ser automaticamente extrapolados para todo o país sem considerar possíveis vieses de participação, como uma maior presença de instituições com mais recursos ou melhor organização interna.

Depois da Espanha e ocupando a segunda posição junto com a Colômbia, o país conta com **20%** das IES no nível avançado (L3). Se essa tendência se mantiver nas próximas edições —e se ampliar a diversidade de instituições participantes— o Brasil poderá posicionar-se entre os países com maior probabilidade de alcançar uma massa crítica de instituições em níveis superiores. Por enquanto, essa possibilidade deve ser considerada **com cautela,** pois são necessários dados de continuidade e uma participação mais ampla para confirmar essa afirmação com um nível adequado de solidez.

DESEMPENHO POR DOMÍNIOS

Um perfil técnico muito robusto e uma governança que acompanha, mas ainda pode ser fortalecida.

O Brasil se destaca especialmente nos domínios **Proteger e Detetar,** onde obtém valores de **1,75 e 1,68, respectivamente,** situando-se entre os mais altos de todo o estudo. Esses resultados refletem a existência de uma infraestrutura sólida, boas práticas em comunicações, um ambiente tecnológico bem estruturado e mecanismos de supervisão e monitoramento bem estabelecidos. O domínio **Identificar** também apresenta um resultado relevante **(1,54),** indicando que as instituições gerenciam de forma consistente seus ativos, riscos e dependências.

Os domínios **Governar (1,59) e Responder e Recuperar (1,28)** apresentam valores igualmente superiores à média regional, embora com maior margem de melhoria. Em ambos os casos, os resultados sugerem que o país dispõe de políticas, papéis e procedimentos básicos, mas que ainda não estão plenamente desenvolvidos. Em particular, a capacidade de resposta e recuperação é adequada, mas poderia ser consolidada com processos mais formais e mecanismos mais homogêneos entre instituições. No conjunto, o Brasil apresenta um perfil técnico e uma estrutura organizacional bem encaminhados, ainda que em fase de consolidação.

LACUNA ENTRE INSTITUIÇÕES PÚBLICAS E PRIVADAS

O setor privado mostra uma vantagem clara e sustentada em quase todos os domínios.

A comparação entre instituições públicas e privadas revela uma lacuna significativa, maior do que na maioria dos países participantes. As instituições privadas registram um IMC médio de **1,64,** enquanto as públicas situam-se em **1,31,** uma diferença relevante que se manifesta de forma consistente em todos os domínios do modelo. A distância é especialmente significativa em **Governar, Identificar e Detetar,** onde as privadas alcançam valores elevados —em alguns casos muito próximos de 2,0— enquanto as públicas permanecem em níveis mais moderados.

Esse padrão sugere que as IES privadas contam com **processos mais formalizados,** melhores esquemas de supervisão e planejamento, maior autonomia para investir em tecnologias de segurança e equipes mais especializadas. Por outro lado, as instituições públicas apresentam uma maturidade sólida, porém menos homogênea, provavelmente condicionada por limitações de gestão, disponibilidade orçamentária ou estruturas organizacionais mais rígidas. Embora isso não implique que as públicas estejam em posição fraca —seus resultados superam a média regional—, evidencia que a **lacuna interna no Brasil é maior do que em outros países,** e que a convergência entre ambos os setores exigirá um esforço adicional.

IMPACTO DO TAMANHO DAS EQUIPES DE CIBERSEGURANÇA

Equipes estáveis e presença mínima garantida: uma base sólida que sustenta a maturidade do país.

Diferentemente de outros países onde uma parte significativa das instituições carece de pessoal dedicado, no Brasil **todas as IES participantes contam com pelo menos uma equipe básica de segurança,** o que já representa um indicador

relevante de maturidade estrutural. Em 2025, as instituições com **1–2 profissionais** apresentam um IMC de **1,25,** enquanto aquelas com **3–5 pessoas alcançam 1,74,** e as poucas que contam com **mais de 5 integrantes chegam a 2,33.** A progressão é clara: quanto maior o tamanho da equipe, maior a maturidade.

O fato de praticamente não existirem instituições sem pessoal dedicado contribui para explicar por que o Brasil parte de um nível de maturidade elevado e homogêneo. Nesse contexto, o tamanho da equipe funciona mais como um **acelerador gradual,** permitindo melhorias especialmente nos domínios técnicos, do que como um fator de ruptura entre instituições. Ainda assim, o padrão geral coincide com o do restante da região: o salto mais relevante ocorre na transição de equipes muito pequenas para equipes de porte médio, que permitem assumir mais funções, documentar processos e sustentar atividades de melhoria contínua.

INFLUÊNCIA DO ORÇAMENTO EM CIBERSEGURANÇA

A relação entre investimento e maturidade é especialmente forte no Brasil.

O orçamento é um fator claramente diferenciador no Brasil. **As instituições que não destinam orçamento de TI à segurança alcançam um IMC de 1,33, enquanto aquelas que investem mais de 20% chegam a 1,97.** Esses resultados mostram uma correlação particularmente clara entre investimento e maturidade: quanto maior a alocação orçamentária, mais sólido é o desempenho nos domínios técnicos e organizacionais. O perfil do Brasil difere, assim, do de outros países onde a relação é mais irregular ou depende de outros fatores, como a governança ou a disponibilidade de equipes. No Brasil, o investimento econômico parece traduzir-se de forma mais direta em capacidades tangíveis e sustentáveis.

No entanto, esses dados devem ser tratados com cautela, dado o contexto particular do país, com um grande número de instituições públicas e privadas. Portanto, assim como em anos anteriores com outros países, será importante realizar um monitoramento da evolução anual, respaldado ou reforçado por um maior número de instituições participantes.

INCIDENTES DE SEGURANÇA

Perfil estável e homogêneo: os incidentes não diferenciam o nível de maturidade.

O Brasil apresenta um comportamento semelhante ao de outros países da região em relação a incidentes. Em 2025, as IES que não reportaram incidentes apresentam um valor médio de 1,49 (L1, Básico), frente a 1,55 (L2, Intermediário) da média nacional.

Nas instituições que sofreram algum ciberincidente nesse período, o nível de maturidade é superior, alcançando valores de 1,93 e 1,87 para aquelas que reportaram um ciberincidente e entre 2 e 5 ciberincidentes, respectivamente. Esse dado sugere — ou pode ser interpretado como — uma melhoria no nível de maturidade reativa diante de situações que possam ter comprometido determinados sistemas corporativos.

USO DA INTELIGÊNCIA ARTIFICIAL EM CIBERSEGURANÇA

Um dos países com maior adoção: la IA amplia capacidades já consolidadas.

O Brasil é um dos países com maior adoção de IA no estudo. Em 2025, o uso de inteligência artificial concentra-se nos domínios técnicos: **Identificar (20%), Proteger (22,5%) y Detetar (17,5%),** enquanto sua presença em **Responder e Recuperar é mais reduzida (7,5%) e (15%) en Governar e Formação.**

As instituições que utilizam IA apresentam níveis de maturidade significativamente superiores, especialmente nos domínios técnicos, o que sugere que essa tecnologia atua como um **reforço natural** de capacidades já existentes. No entanto, como em outros países, é importante evitar conclusões deterministas: o uso de IA pode ser tanto consequência quanto causa parcial da maturidade. O mais provável é que as instituições que já possuíam práticas sólidas e equipes especializadas tenham sido precisamente as primeiras a incorporar essas ferramentas.

De forma geral, o Brasil apresenta um cenário em que a IA ainda não é um elemento transversal, mas sim um **complemento relevante** que potencializa a robustez técnica do sistema e antecipa uma possível expansão para domínios mais organizacionais nas próximas edições.

BRASIL

IMC 2025

Índice de Maturidade em Cibersegurança das IES Ibero-Americanas

metared by universia

Secretaría General Iberoamericana
Secretaria-Geral Ibero-Americana