PORTUGAL

IMC 2025

Índice de Maturidade em Cibersegurança
das IES Ibero-Americanas

metared 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

PORTUGAL 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 Portugal

Carla Alexandra Santos

Politécnico de Coimbra

Departamento de Tecnologias de Informação e Comunicação

MetaRed TIC Portugal

Tiago Pedrosa

Instituto Politécnico de Bragança

Profesor, CISO y Coordinador CSIRT

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.

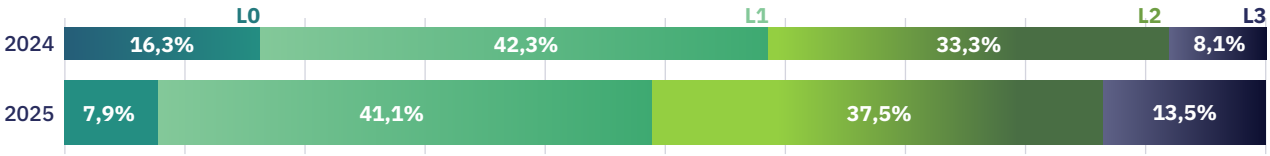
Um ecossistema em plena evolução

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.

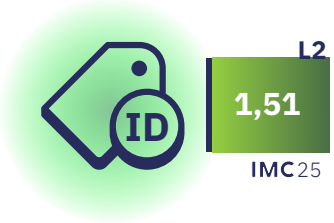
FORÇAS CONSOLIDADAS

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

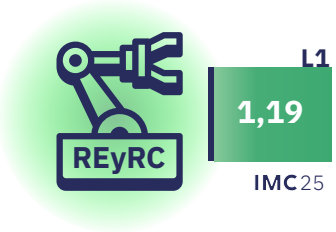
Avanços em Identificar, Proteger e Detetar



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

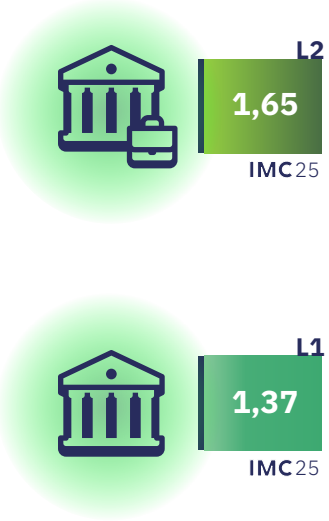
O progresso em cibersegurança não é uniforme em toda a região, com países que lideram a adoção de práticas avançadas e outros que avançam em um ritmo mais moderado.

- **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 Portugal

POR

L0 L1 L2 L3

IMC24 1,41 L1

1,44 L1 IMC25

IMC PORTUGAL
1,44

2024-2025 EVOLUÇÃO
+0,03

DIFERENÇA IMC IBE
-0,07

TIPOS DE IES
*evolução no IMC IES POR.

PÚBLICAS 1,47 (+0,08)

PRIVADAS 1,17 (-0,36)

DOMÍNIOS
*evolução nos domínios IBE do IMC

DETETAR 1,60 (-0,04)

PROTEGER 1,59 (-0,09)

IDENTIFICAR 1,42 (-0,09)

GOVERNAR 1,42 (-0,13)

RESPONDER 1,15 (-0,04)

TOP 3

DETETAR

PROTEGER

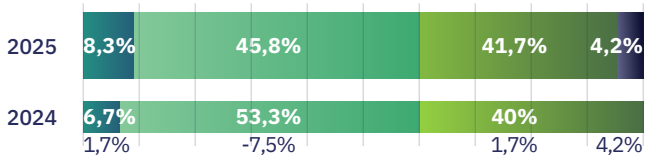
GOVERNAR/ IDENTIFICAR

Detetar e Proteger superam o IMC de 2025 (1,51) em 8 e 9 centésimos, respectivamente.

Governar e Identificar obtêm uma pontuação de 1,42, ligeiramente abaixo da média ibero-americana. .

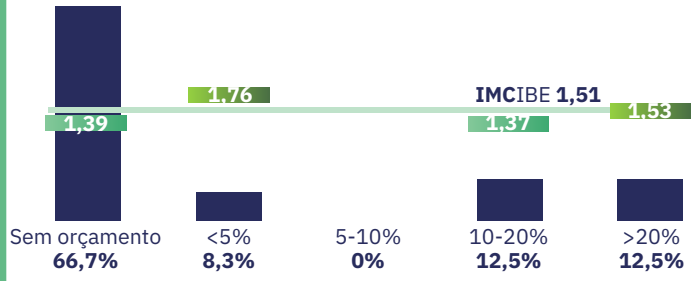
Responder e Recuperar apresenta o valor mais baixo eé o mais distante da média.

DISTRIBUIÇÃO SEGUNDO IMC



A maioria das IES portuguesas (87,5%) situa-se nos níveis L1 (básico) e L2 (intermediário). Observa-se uma ligeira tendência para um nível de maturidade mais elevado: o número de IES em L1 diminuiu 7,5%, enquanto o número em L2 e L3 aumentou 1,7% e 4,2%, respetivamente.

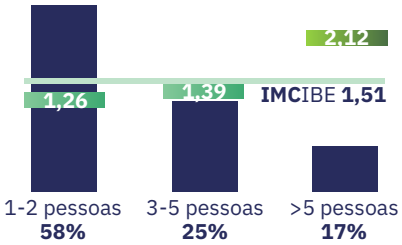
ORÇAMENTO



Quase 70% das IES **não possuem um orçamento específico.**

O nível de maturidade das IES com orçamentos inferiores a 5% é o mais elevado (1,76), 0,25 acima da média ibero-americana.

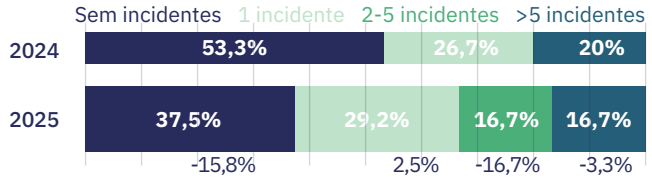
EQUIPES DE CIBERSEGURANÇA



Quase 20% das equipes de cibersegurança portuguesas são compostas por mais de 5 pessoas. A pontuação do IMC aumenta significativamente com o tamanho da equipe. Em Portugal, as IES com equipes de mais de 5 pessoas atingem uma pontuação de 2,12 (nível intermediário, L2).

CIBERINCIDENTES

DISTRIBUIÇÃO DE INCIDENTES



EVOLUÇÃO DO IMC SEGUNDO O NÚMERO DE INCIDENTES

Seis em cada dez instituições portuguesas sofreram algum tipo de incidente cibernético no último ano.

3.

Resumo Executivo

RESUMO EXECUTIVO PORTUGAL

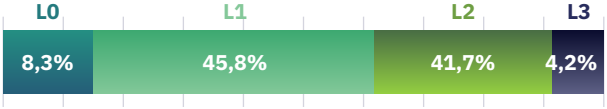
Portugal apresenta um dos perfis mais equilibrados e homogéneos da região, embora não atinja o nível intermédio (L2).

Portugal obtém em 2025 um **IMC de 1,44,** uma melhoria face a 2024 (1,41), que indica uma evolução moderada, mas consistente. O país mantém-se no nível básico (L1), embora próximo do limiar intermédio e acima de países como o México (1,33) ou o Equador (1,36).

A melhoria, embora não tão acentuada como noutros países, caracteriza-se pela sua **estabilidade:** Portugal apresenta valores relativamente elevados e equilibrados na maioria dos domínios, sem grandes oscilações e sem brechas profundas entre áreas técnicas e organizativas. Este traço distingue o país dentro da região, onde é habitual observar sistemas mais heterogéneos.

Não obstante, o país continua abaixo da média ibero-americana de 2025 (1,51), o que indica uma margem de progressão, especialmente em aspetos organizativos e de resposta.

DISTRIBUCIÓN DE NIVELES DE MADUREZ



O país apresenta uma percentagem elevada de instituições em **nível intermédio (L2),** abaixo da Colômbia, Espanha, Peru e Chile. Isto indica um sistema universitário com bases relativamente sólidas e uma consolidação técnica mais avançada do que em países que continuam ancorados no L1.

A percentagem de instituições em L0 (8,3%) é baixa em comparação com outros países, o que sugere que a maior parte do sistema superou os níveis mais incipientes. A presença de instituições em L3 (4,2%) é modesta, mas consistente com o perfil de estabilidade do país.

LACUNA ENTRE INSTITUIÇÕES PÚBLICAS E PRIVADAS

Mudança marcante em 2025: as públicas passam a liderar o IMC médio.

Em 2024, as instituições privadas de Portugal apresentavam um **IMC médio de 1,53, face a 1,39** nas públicas, com uma diferença de cerca de **0,14 décimas a favor do setor privado.** Em 2025, o panorama muda de forma marcante: as privadas descem para um IMC de **1,17,** enquanto as públicas sobem para **1,47,** situando-se **0,30 pontos acima** e deixando a média nacional em **1,44.**

Esta mudança sugere um reequilíbrio significativo entre ambos os setores, embora seja provável que esteja em parte influenciada por variações no conjunto de instituições participantes e não apenas pela evolução interna de cada uma.

Se observarmos o detalhe por domínios, o padrão repete-se. Em 2024, as privadas lideravam em **Identificar** (1,48 face a 1,41) e **Proteger** (1,68 face a 1,59). Em 2025, porém, as públicas passam a obter **1,48 em Identificar face a 0,94 nas privadas, e 1,61 em Proteger face a 1,46 no**

setor privado. Algo semelhante acontece em **Governar,** onde as públicas atingem **1,47 face a 1,04** nas privadas, e em vários subdomínios — como **Estratégia, Normativa ou Análise de riscos**— onde as universidades públicas mostram uma melhoria muito clara face ao ano anterior.

Esta evolução não significa necessariamente que as privadas tenham "deixado de fazer coisas" em cibersegurança, mas sim que **a melhoria do setor público foi mais intensa** e, possivelmente, concentrada num subconjunto de instituições que deram saltos importantes em governação, identificação de ativos e gestão técnica. Chama a atenção que, apesar de o subdomínio **Orçamento** continuar baixo em ambos os casos (em torno de **0,43–0,67 pontos),** as públicas consigam melhores resultados em domínios como **Governar ou Identificar,** o que sugere um esforço organizativo relevante para além do nível de investimento estritamente declarado.

No conjunto, Portugal apresenta uma brecha entre públicas e privadas que não é extrema, mas é **dinâmica:** de uma vantagem clara do setor privado em 2024 passa-se para uma liderança do setor público em 2025, especialmente em domínios organizativos. As privadas mantêm bons níveis técnicos —especialmente em infraestruturas e comunicações—, enquanto as públicas parecem ter acelerado a formalização de políticas, papéis e estratégia. Será importante observar nos próximos exercícios se esta tendência se consolida ou se resulta, em parte, de alterações na amostra e de projetos concretos de um grupo reduzido de IES.

DESEMPENHO POR DOMÍNIOS

Os valores por domínio em 2025 são: **Governar (GB): 1,42, Identificar (ID): 1,42, Proteger (PR): 1,59, Detetar (DE): 1,60, Responder (RE): 1,15.**

Portugal apresenta pontos fortes muito claros nos domínios **Proteger e Detetar,** cujos valores se situam próximos do nível intermédio. Isto reflete-se em subdomínios com pontuações elevadas, como Infraestruturas (2,20), Comunicações (2,15), Informação (2,16) e Atividade dos utilizadores (1,83). Esta robustez técnica coloca Portugal entre os países com maior controlo técnico da região, juntamente com Espanha, Colômbia e Brasil.

Os domínios **Governar e Identificar** mostram valores médios sólidos (1,42), superiores aos de vários países vizinhos, mas ainda insuficientes para alcançar um nível intermédio pleno. A fragilidade mais marcada continua a ser o domínio **Responder e Recuperar,** com um valor de 1,15 e 0,96, o que evidencia carências em mitigação, recuperação e gestão formal de incidentes.

Portugal destaca-se em infraestruturas e deteção, mas mantém brechas na resposta e na formalização organizativa.

IMPACTO DA DIMENSÃO DAS EQUIPAS DE CIBERSEGURANÇA

A presença de uma equipa dedicada é um dos fatores mais determinantes para avançar no modelo de maturidade.

Os dados de Portugal confirmam a relação positiva entre a dimensão da equipa especializada e o nível de maturidade das instituições, embora o padrão seja menos linear do que noutros países, como Espanha ou México. Em 2024, as IES sem pessoal dedicado apresentavam um IMC de **1,37,** enquanto aquelas com **1–2 pessoas** atingiam **1,38,** mostrando um salto relevante pelo simples facto de contarem com um mínimo de pessoal especializado. As instituições com **3–5 elementos atingiam 1,54,** e não se registavam IES com **mais de 5 pessoas.**

Em 2025, estas tendências mantêm-se, mas com nuances. Do levantamento realizado resulta que não existem IES sem pessoal, enquanto o grupo com **1–2 pessoas regista um IMC de 1,26,** valor inferior ao registado no ano anterior, o que indicaria uma deterioração das capacidades. Esta mesma situação verifica-se **nas instituições com equipas de 3–5 pessoas, que atingem um IMC de 1,39,** situando-se já no nível básico e com valores inferiores aos registados no IMC 2024. **O grupo com mais de 5 profissionais obtém um IMC de 2,12,** valor que mostra uma tendência ascendente notória, a que acresce o facto de no ano anterior não terem sido identificadas IES portuguesas com essa dimensão de pessoal.

No entanto, os valores atingidos devem ser interpretados com cautela. É possível que a amostra de 2025 inclua centros com equipas grandes, mas com desafios importantes em governação ou gestão operacional, ou que as instituições mais sólidas do ano anterior não tenham participado em 2025. Ainda assim, o padrão geral mantém-se: **ter mais pessoal especializado aumenta a probabilidade de alcançar melhores níveis de maturidade,** especialmente em Portugal, onde mesmo ultrapassar os 5 profissionais representa um salto imediato de quase um ponto no IMC.

Em termos práticos, a análise de 2024 e 2025 transmite uma mensagem clara e coerente com o resto da região: **a presença de uma equipa dedicada é um dos fatores mais determinantes para avançar no modelo de maturidade.** As instituições com pessoal mínimo tendem a estagnar em níveis básicos, enquanto aquelas com equipas de dimensão média (3–5 pessoas) são as que mostram uma trajetória de progresso mais estável. O aumento do valor para as IES com grupos de mais de 5 profissionais em 2025 reforça esta tendência geral, ainda que seja necessário considerar o contexto particular de cada instituição e a importância de combinar capital humano com governação, processos e recursos adequados.

INFLUÊNCIA DO ORÇAMENTO EM CIBERSEGURANÇA

A análise de Portugal mostra que o orçamento continua a ser um fator importante para explicar a maturidade, embora com um comportamento menos linear do que noutros países da região. Em 2025, as instituições que afetam **0–5%** do seu orçamento de TI à cibersegurança registam um IMC médio de **1,76,** atingindo um nível intermédio (L2), enquanto aquelas que destinam entre **5–10%** atingem **1,44,** ou seja, um nível básico (L1). No escalão **10–20%,** o IMC obtém um valor de **1,37,** correspondente a um nível básico. As IES que investem **mais de 20%,** por sua vez, têm um IMC de **1,53,** o que mostra uma progressão positiva, embora estes dados devam ser interpretados com prudência, devido ao seu comportamento errático.

Comparado com 2024, o país mostrava aumentos modestos nos escalões baixos e um salto mais visível a partir dos 10%, mas este padrão não se mantém, ou só o faz para orçamentos superiores a 20%.

Este fenómeno pode dever-se a vários fatores. Em primeiro lugar, as instituições com percentagens elevadas de orçamento poderão estar a responder a incidentes recentes ou a necessidades urgentes, destinando recursos a medidas reativas que ainda não se refletem plenamente na sua maturidade global. Em segundo lugar, os números sugerem que a despesa só gera melhorias sustentadas quando é acompanhada de **governação, processos estáveis e equipas capacitadas.** De

facto, o subdomínio **Orçamento** continua a apresentar valores alarmantemente baixos no país, em torno de 0,46, o que indica que a cultura de planeamento financeiro em cibersegurança ainda se encontra numa fase muito incipiente.

Ainda assim, a mensagem deixada pelos dados é clara: **as instituições que afetam um orçamento específico para a segurança avançam mais rapidamente,** e aquelas que investem pelo menos 20% atingem níveis significativamente superiores à média nacional. O desafio para Portugal não é apenas aumentar o investimento, mas **garantir que esse investimento esteja alinhado com uma estratégia, com papéis definidos e com a capacidade operacional necessária para executar as ações previstas.** Só assim o orçamento poderá transformar-se num verdadeiro motor de maturidade e não num indicador isolado.

INCIDENTES DE SEGURANÇA: EVOLUÇÃO E RELAÇÃO COM A MATURIDADE

Aumento notável da criticidade e uma relação complexa com a maturidade.

O comportamento dos ciberincidentes nas IES portuguesas mostra uma evolução particular entre 2024 e 2025. Ao contrário de outros países onde os incidentes estabilizam ou diminuem, Portugal regista um **aumento muito acentuado da criticidade:** o número médio de incidentes críticos reportados pelas instituições passa de **13,60 em 2024 para 39,50 em 2025,** quase triplicando a quantidade.

Este aumento não implica necessariamente uma maior vulnerabilidade geral, mas revela uma combinação de **melhor capacidade de deteção** em algumas IES e **persistentes fragilidades de resiliência** noutras.

Em termos de distribuição, os dados mostram que **as instituições se repartem de forma equilibrada entre aquelas sem incidentes,** as que sofrem um único caso e as que registam vários. O padrão observado é o seguinte:

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

Este comportamento sugere um fenómeno já observado noutros países em fases anteriores: **as instituições mais maduras detetam e reportam mais incidentes,** enquanto as menos desenvolvidas podem registar poucos casos, mas não necessariamente por estarem mais bem protegidas, e sim porque dispõem de uma capacidade limitada para os identificar ou documentar.

No entanto, o salto de criticidade em 2025 convida a uma leitura mais matizada. Alguns subdomínios-chave ajudam a compreender esta situação:

- **Mitigação (0,96) e Recuperação (0,96)** continuam a ser áreas frágeis.
- **Continuidade (0,83)** mostra fragilidade, especialmente em IES com múltiplos incidentes.
- **Responsabilidade e procedimentos** apresentam valores díspares entre instituições, dificultando respostas coordenadas.

No conjunto, estes indicadores refletem que, embora Portugal tenha **uma maturidade técnica sólida** (bons resultados em infraestruturas e comunicações), a capacidade de **responder, conter e recuperar** continua a ser um desafio significativo.

Um aspeto relevante da evolução 2024–2025 é que **a correlação entre número de incidentes e maior maturidade não se inverte,** mas dilui-se. Em 2024, as instituições com mais incidentes tendiam a situar-se claramente acima da média. Em 2025, as diferenças entre grupos são menores e as IES com zero incidentes não aparecem em atraso, o que aponta para uma melhoria relativa na prevenção ou, pelo menos, para o facto de um número crescente de instituições conseguir passar o ano sem incidentes críticos detetados.

Em resumo:

- **Aumenta a criticidade,** embora não necessariamente a vulnerabilidade geral.
- **Alarga-se a brecha interna:** algumas IES melhoram a deteção, outras continuam sem processos robustos de resposta.
- **A relação entre incidentes e maturidade suaviza-se,** um passo prévio ao que já se observa em países mais avançados.
- **Responder continua a ser o domínio mais frágil,** o que amplifica o impacto dos incidentes que efetivamente ocorrem.

Em síntese, Portugal apresenta um cenário de incidentes complexo: deteta mais, mas continua a **responder e a recuperar com dificuldade.** Melhorar os processos de gestão de incidentes — especialmente mitigação, recuperação e continuidade — será fundamental para que o país possa consolidar, nos próximos anos, um ecossistema universitário mais resiliente

UTILIZAÇÃO DA INTELIGÊNCIA ARTIFICIAL EM CIBERSEGURANÇA

A utilização de inteligência artificial (IA) nas IES portuguesas continua a ser limitada, embora algo mais difundida do que noutros países da região. Os dados mostram que a adoção se concentra em domínios claramente técnicos: **Proteger (37,5%), Detetar (29,2%) e Identificar (20,8%).** Em contrapartida, a IA está totalmente ausente em **Governar e Responder,** e é praticamente residual em **Formação (4,2%).** Este padrão revela que a tecnologia está a ser aplicada principalmente em tarefas operacionais orientadas para a análise, a vigilância ou a automatização de deteções, e não em âmbitos estratégicos ou organizativos.

Adoção seletiva e benefícios ainda incipientes,

condicionados pela maturidade prévia de cada instituição.

Ao comparar o nível de maturidade entre instituições que utilizam IA e as que não utilizam, observam-se diferenças relevantes em vários domínios. As IES que incorporaram IA apresentam valores superiores em **Identificar (IMC 1,86 face a 1,33), Proteger (1,74 face a 1,26) e Detetar (1,62 face a 1,36).** No entanto, esta vantagem desaparece em domínios como **Governar e Responder,** onde simplesmente não existe adoção de IA. Isto sugere que a tecnologia está a ser incorporada em áreas onde Portugal já apresenta pontos fortes técnicos, mas ainda não foi integrada como parte de uma estratégia global de segurança.

Ainda assim, estas diferenças devem ser interpretadas com cautela. Como acontece noutros países, é provável que as instituições que utilizam IA sejam também aquelas com **equipas mais especializadas, processos mais maduros ou maior disponibilidade orçamental,** fatores que influenciam tanto o seu nível de maturidade como a sua capacidade para adotar novas tecnologias. A IA, neste sentido, parece refletir mais um **sintoma de maturidade prévia** do que um impulsionador direto e homogéneo do avanço.

Outro aspeto digno de destaque é a ausência total de IA em **Responder,** um domínio que já é frágil em Portugal e que poderia beneficiar no futuro de capacidades de automatização, priorização e análise acelerada. A falta de adoção neste domínio sugere que a IA ainda não está integrada na gestão de incidentes nem na recuperação, duas áreas fundamentais para melhorar a resiliência do país.

No conjunto, Portugal apresenta um cenário em que a IA é utilizada, mas de forma muito focalizada, com benefícios visíveis em domínios técnicos, mas sem efeitos globais na estrutura do IMC. O país dispõe de uma base tecnológica sólida que poderá facilitar a expansão futura destas ferramentas, mas o seu impacto dependerá de que a adoção seja acompanhada por melhorias em governação, papéis, procedimentos e capacidade de resposta.

PORTUGAL

IMC 2025

Índice de Maturidade em Cibersegurança
das IES Ibero-Americanas

meta red
by universia

Secretaría General
Iberoamericana
Secretaria-Geral
Ibero-Americana