IMC 2024

Índice de Madurez en Ciberseguridad de las IES Iberoamericanas

metared
by universia

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

Edición
MetaRed by Universia - Fundación Universia

Diseño
María Moraleja Vicente

IMC 2024

Índice de Madurez en Ciberseguridad de las IES Iberoamericanas

metared by universia

Contenidos IMC 2024.

Prólogo.

Conseguir universidades más seguras desde la colaboración internacional. Con este objetivo en mente, se abre una nueva puerta hacia un horizonte donde el sector de la Educación Superior se convierta en un ecosistema fuerte y seguro.

Iberoamérica nos une, la ciberseguridad nos necesita y como creadores de comunidades, Fundación Universia apuesta y apostará por crear redes que faciliten y mejoren a todas y cada una de las Instituciones de Educación Superior que conforman este proyecto colaborativo, MetaRed.

Con este informe sentamos las bases para un futuro en el que todos estemos más protegidos en el mundo digital. El valor de este primer IMC no reside sólo en los datos, que nos harán crear estrategias y acciones más fiables y directas, sino en el poder que hemos obtenido al crearlo entre todos. Un trabajo de las universidades, con las universidades y para las universidades. Un trabajo de cada uno/a de vosotros/as, en el que habéis puesto vuestro máximo interés para llegar a 247 instituciones, 10 países y más de 6.5 millones de estudiantes representados.

Es hora de crecer. Es hora de mejorar. Es hora de colaborar.

Rafael Hernández

Vicepresidente de Fundación Universia

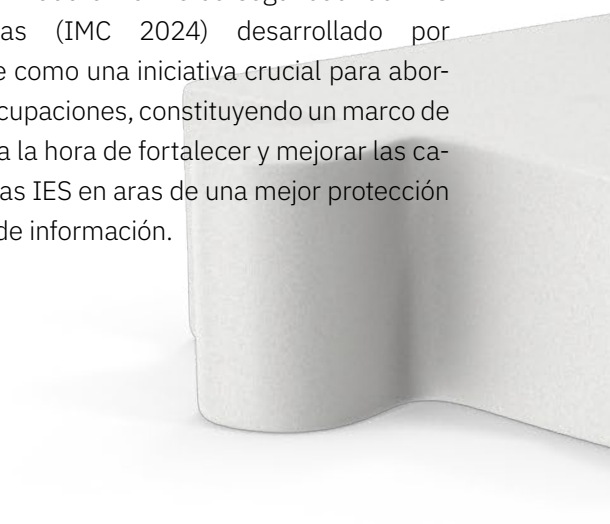
Presentación.

En un mundo cada vez más interconectado y dependiente de la tecnología digital, la ciberseguridad se ha convertido en una preocupación central para todo tipo de instituciones. En este universo también se incluyen las universidades, que vienen experimentando un proceso inexorable de transformación digital.

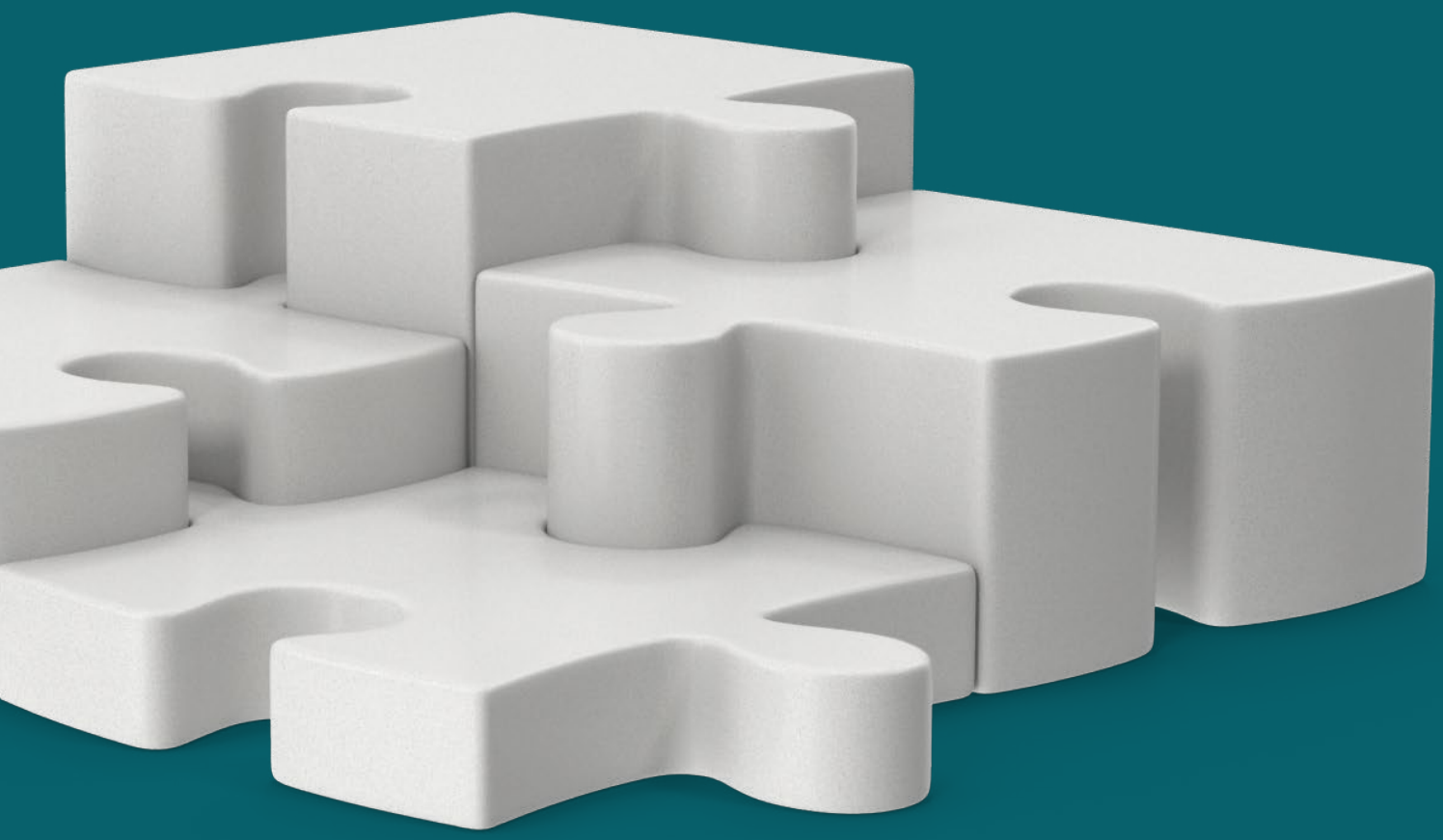
Una visión integral de la protección de los activos de información requiere considerar no sólo los aspectos tecnológicos sino también, los procesos y los recursos humanos, partiendo de un conocimiento profundo de las amenazas, vulnerabilidades y riesgos a los que se encuentran expuestos. Conocer el estado actual en el que se encuentra la entidad en materia de ciberseguridad y determinar si se encuentran implementadas las medidas necesarias para mitigar los riesgos a los que se expone, constituye una paso fundamental para gestionar adecuadamente los activos de información y avanzar hacia una mayor resiliencia.

Además de identificar las fortalezas y debilidades en materia de protección de activos de información, resulta relevante contar con un modelo uniforme que habilite la comparación con otras entidades de la región y del propio país, con las que se comparte un contexto común y funciones similares.

En base a lo previamente expresado, el proyecto del Índice de Madurez en Ciberseguridad de IES iberoamericanas (IMC 2024) desarrollado por Metared, surge como una iniciativa crucial para abordar estas preocupaciones, constituyendo un marco de referencia útil a la hora de fortalecer y mejorar las capacidades de las IES en aras de una mejor protección de los activos de información.



Una visión integral de la protección de los activos de información.



1.
MetaRed: La importancia de la colaboración en ciberseguridad.

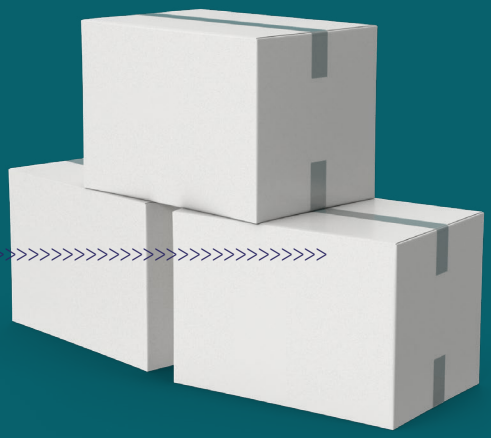
MetaRed es la mayor red de redes de colaboración de Instituciones de Educación Superior (IES) iberoamericanas, tanto públicas como privadas. Su objetivo es apoyar a las instituciones de los países participantes en retos claves como la transformación digital, el emprendimiento, la sostenibilidad y la responsabilidad social universitaria.

En el ámbito de la transformación digital, la red MetaRed TIC conforma una estructura de colaboración con más de 1200 instituciones de 15 países diferentes, representadas por sus responsables de Tecnologías de la Información y la Comunicación (TIC), junto a un comité Internacional de Presidentes/as Rectores/as y diversos Grupos de Trabajo, tanto nacionales como internacionales, enfocados en la compartición de buenas prácticas, casos de éxito y desarrollo de proyectos. Los Grupos de Trabajo Internacionales, están formados por los coordinadores y coordinadoras de los grupos de trabajo de cada país, y están divididos en ciberseguridad, tecnologías educativas, madurez digital, relación con proveedores y la red de mujeres TIC.

La constante y rápida evolución de la tecnología es un reto de nuestra sociedad y nuestras instituciones. Todas las IES están siendo afectadas por estos movimientos que requieren un arduo esfuerzo de los dirigentes, técnicos y usuarios de las instituciones. Áreas como la ciberseguridad han incrementado notablemente las necesidades de recursos humanos especializados, herramientas, procesos y buenas prácticas, situación que se repite por igual en las IES de cualquier país, independientemente de su tamaño o tipología. Esto deriva en la necesidad de crear alianzas y establecer una estrecha colaboración entre instituciones afines, que permita el fortalecimiento conjunto del sector de la educación superior iberoamericana.

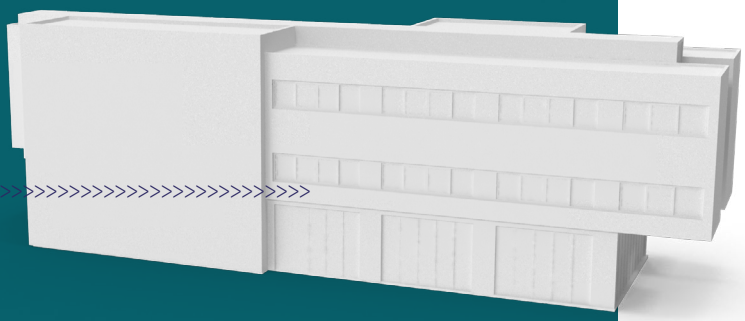
meta red
by universia

3 redes temáticas
TIC, X y S

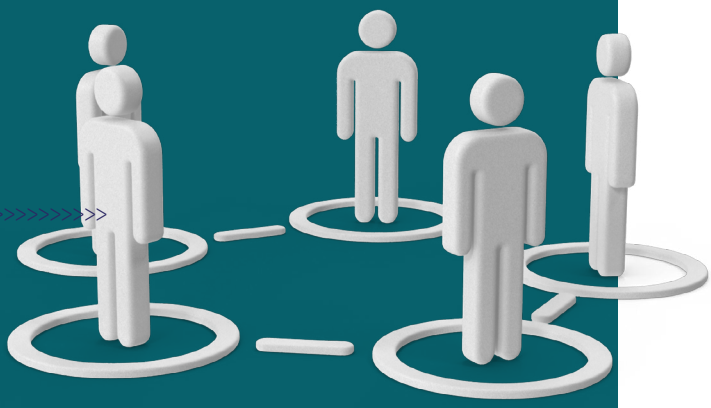


15 países

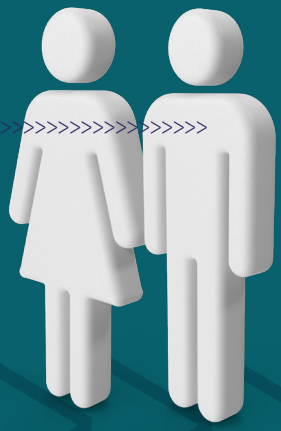
+1.800 IES



+130
grupos de trabajo



+28.000 Personas



Grupo de Trabajo Internacional en Ciberseguridad.

En este sentido, el Grupo de Trabajo Internacional (GTI) de Ciberseguridad juega un importante papel. La compartición de experiencias constituye uno de los pilares para la creación de instituciones más ciberseguras. La identificación, documentación y publicación de buenas prácticas, casos de éxito, estudios del sector y de tecnologías vinculadas al sector son una ventaja a nivel de costes y de operación, para afrontar el incremento en los ciberataques hacia nuestras instituciones.

El trabajo de todos los componentes del GTI de ciberseguridad puede servir como una herramienta para protegernos, pero su verdadero valor es ser una fuente de conocimiento global para afrontar el cambio cultural necesario para crear IES más seguras.

Coordinadores y coordinadoras.

MetaRed TIC Argentina

Javier Diaz

Universidad Nacional de la Plata
Secretario de Vinculación e Innovación Tecnológica

MetaRed TIC Brasil

Domingos Sávio Alcântara Machado

Universidade Tiradentes
Vice-Presidência de Estratégia, Internacionalização e Inovação

MetaRed TIC Centroamérica y el Caribe

José Luis Regalado Menchaca

Universidad Tecnológica Centroamericana
UNITEC Honduras
CIO

MetaRed TIC Chile

Álvaro Fuentes Maldonado

Universidad Autónoma de Chile
Director corporativo de tecnologías

MetaRed TIC México

Héctor Bonola

Universidad Veracruzana
Dirección de Servicios de Red
e Infraestructura Tecnológica

MetaRed TIC Colombia

Maritza Giraldo Agudelo

Universidad Pontificia Bolivariana
Directora de Infraestructura
Tecnológica Multicampus

MetaRed TIC Perú

Silvana Balarezo

Universidad Peruana
de Ciencias Aplicadas
Gerente de Experiencia
de Aprendizaje Digital

MetaRed TIC Ecuador

Carlos Gabriel Córdova Erreis

Universidad Técnica Particular
de Loja
Gerente TI

MetaRed TIC Perú

Gumercindo Bartra Gardini

Pontificia Universidad Católica
del Perú
Director de la Maestría de Ingeniería
de las Telecomunicaciones

MetaRed TIC Ecuador

Julia Alexandra Pineda Arévalo

Universidad Técnica Particular
de Loja
Coordinadora de Seguridad y Riesgos

MetaRed TIC Portugal

Carla Alexandra Santos

Politécnico de Coimbra
Departamento de Tecnologias de
Informação e Comunicação

Crue Digitalización, España

Francisco José Sampalo Lainz

Universidad Politécnica
de Cartagena
Responsable de Seguridad

MetaRed TIC Portugal

Tiago Pedrosa

Instituto Politécnico de Bragança
Profesor, CISO y Coordinador CSIRT

2. Conclusiones

"Si no puedes medirlo, no puedes mejorarlo"

Peter Drucker

Esta frase de Peter Drucker encapsula la esencia de la medición en la gestión y mejora de cualquier proceso. En el contexto de la ciberseguridad, la capacidad de medir el estado y la madurez de las prácticas de seguridad es fundamental para identificar áreas de mejora y desarrollar estrategias efectivas. Este informe presenta el Índice de Madurez en Ciberseguridad de las Instituciones de Educación Superior (IES) Iberoamericanas, basado en un modelo integral que abarca los dominios de Gobernar, Detectar, Proteger, Identificar, Responder/Recuperar, y Formación y Talento.

A través de un análisis detallado y sistemático de estos dominios, hemos evaluado el grado de preparación y resiliencia de las instituciones educativas frente a las amenazas cibernéticas. Los hallazgos de este informe no solo proporcionan una visión del estado actual de la ciberseguridad en el sector educativo iberoamericano, sino que también ofrecen una base sólida para la implementación de mejoras continuas y el fortalecimiento de las estrategias de seguridad.

En las siguientes secciones, se presentan las principales conclusiones obtenidas del estudio, destacando las fortalezas y debilidades identificadas en cada dominio, así como recomendaciones específicas para avanzar hacia un mayor nivel de madurez en ciberseguridad. Este enfoque estructurado y basado en datos permite a las universidades no solo comprender su posición actual, sino también trazar un camino claro hacia una mayor protección y resiliencia en el entorno digital.

Retos actuales.

» Las IES que cuentan con una estrategia institucional formalizada de ciberseguridad adquieren un nivel de madurez avanzado, muy superior al nivel de madurez inicial que presentan las instituciones que no han recibido ese apoyo.

6 de cada 10
IES de Iberoamérica han sufrido algún tipo de ciberincidente en el último año.

El número de ciberataques se ha incrementado un 46% en los últimos dos años y sigue al alza en los últimos meses, según informes de grandes consultoras y empresas de ciberinteligencia y ciberseguridad como Crowdstrike y Checkpoint.

El sector de la educación superior es uno de los sectores más afectados a nivel global. En 2023, las instituciones educativas y de investigación estuvieron entre los principales objetivos de los ciberataques, ocupando una posición destacada junto con los sectores de salud y gobierno. Este sector enfrenta desafíos significativos debido a la gran cantidad de datos sensibles que manejan y a las limitaciones en recursos para ciberseguridad.

15,9
ciberincidentes anuales abiertos por institución.

En este contexto, los datos recogidos muestran que 6 de cada 10 IES de Iberoamérica han sufrido algún tipo de ciberincidente en el último año, que ha derivado en afectación total o parcial de los principales servicios y aplicaciones corporativas.

Este indicador, junto con el promedio de 15,9 ciberincidentes abiertos por institución al año, según datos recabados en el IMC 2024, nos enfrenta a un reto que puede marcar el futuro de muchas instituciones y que requerirá un fuerte apoyo institucional para afrontar, con garantías y seguridad, un cambio cultural dentro de las organizaciones. Estamos en un momento en el que la ciberseguridad debe considerarse una materia transversal a toda la entidad. No es una responsabilidad exclusiva del área de TI, sino de toda la comunidad universitaria, que juega un papel fundamental para garantizar la seguridad de la información y la continuidad del servicio, así como de los equipos rectorales, que tienen la importante labor de garantizar el gobierno y la gestión de la seguridad de la información.

Ciberseguridad en las IES Iberoamericanas. Situación actual.

» Las IES que presentan un IMC más elevado disponen de un presupuesto de ciberseguridad equivalente a más del 5% del total asignado para el área TI

» La creación de equipos específicos de ciberseguridad se consolida como uno de los factores con mayor peso en el nivel de madurez de las instituciones.

El Índice de Madurez en Ciberseguridad de las IES Iberoamericanas se sitúa en un nivel básico (L1) con un valor 1,37. Este valor, cercano al umbral mínimo del nivel de madurez intermedio (L2, 1,50), refleja una situación en la cual, las instituciones son conscientes de la necesidad de realizar prácticas de ciberseguridad apoyadas en recursos y herramientas adecuadas. Sin embargo, no llegan a estar formalizadas y no cuentan con recursos suficientes para materializar las iniciativas apropiadas en el corto plazo.

El IMC por país es encabezado por España (IMC 1,73), Colombia (IMC 1,62), Chile (IMC 1,47) y Portugal (IMC 1,41). El resto de países presentan niveles de madurez por debajo de la media de Iberoamérica. En concreto, México (IMC 1,27), Argentina (IMC 1,06) y Ecuador (IMC 0,99). Estos valores hacen que España y Colombia cuenten con un nivel de madurez intermedio (L2), frente al resto de países que quedan en un nivel básico (L1).

Por dominios de aplicación, los datos reflejan una tendencia global hacia la realización de acciones de protección, donde las IES iberoamericanas muestran su máximo nivel promedio con un nivel de madurez de 1,54 puntos (L2, Intermedio). Efectivamente, el dominio Protección (PR) recoge todas las acciones de aseguramiento de la información, del acceso, de la infraestructura, de los equipos, de las comunicaciones y de otros elementos claves para la institución. La capacidad de detección (Detectar - DE) y el gobierno de la ciberseguridad (Gobernar - GB) muestran niveles de madurez muy cercanos al nivel intermedio. Sin embargo, quedan en un grado básico (L1), lo que vislumbra instituciones con prácticas de

El Índice de Madurez en Ciberseguridad de las IES Iberoamericanas se sitúa en un **nivel básico** con un valor de **1,37**

detección más completas a nivel de recursos y documentación. Sin duda, son acciones cruciales en materia de seguridad de nuestras instituciones, pero que necesitan ser complementadas con el resto de dominios analizados para alcanzar una protección homogénea.

Las acciones de ciberseguridad requieren recursos adecuados para afrontar los retos analizados. La inversión económica juega un papel fundamental. IMC 2024 refleja cómo las IES que presentan un valor más elevado disponen de un presupuesto de ciberseguridad equivalente a más del 5% del total asignado para el área TI, pasando de un nivel inicial (L0) y básico (L1), a un nivel intermedio (L2) de madurez.

La otra pieza clave es el factor humano. La composición de equipos de ciberseguridad calificados y comprometidos con la institución, puede ser un elemento diferenciador. IMC 2024 muestra una clara y fuerte evolución ascendente en el grado de madurez de las IES en función del tamaño de los equipos de ciberseguridad.

01.

Las IES que no cuentan con equipos de ciberseguridad han obtenido un IMC de 0,69, situando su madurez en un nivel inicial (L0). **Partiendo de este valor, aquellas que cuentan con equipos de ciberseguridad dedicados comienzan a incrementar su nivel de madurez hasta rozar el nivel avanzado (L3).**

02.

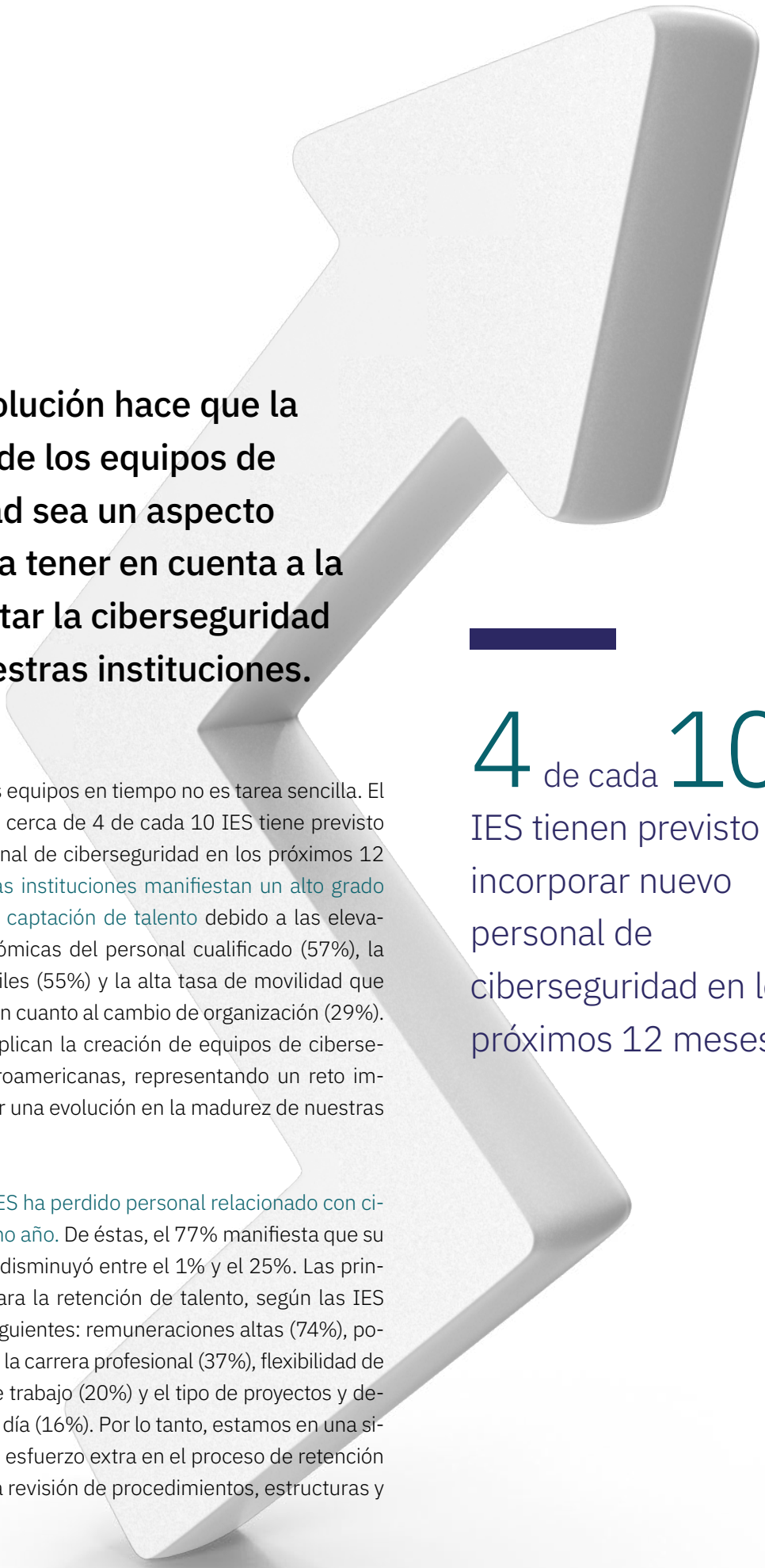
Las instituciones que crearon equipos pequeños (1 o 2 personas), consiguen un nivel de madurez básico (L1, 1,24).

03.

Las que ya cuentan o han evolucionado a equipos medianos (entre 3 y 5 personas) suben otro grado y alcanzan el nivel intermedio (L2, 1,60).

04.

Como último escalón analizado, aquellas que cuentan con más de 5 personas, se sitúan también en dicho nivel (L2, 1.95), pero con un valor más cercano al máximo estadío (L3).



Esta clara evolución hace que la composición de los equipos de ciberseguridad sea un aspecto fundamental a tener en cuenta a la hora de afrontar la ciberseguridad dentro de nuestras instituciones.

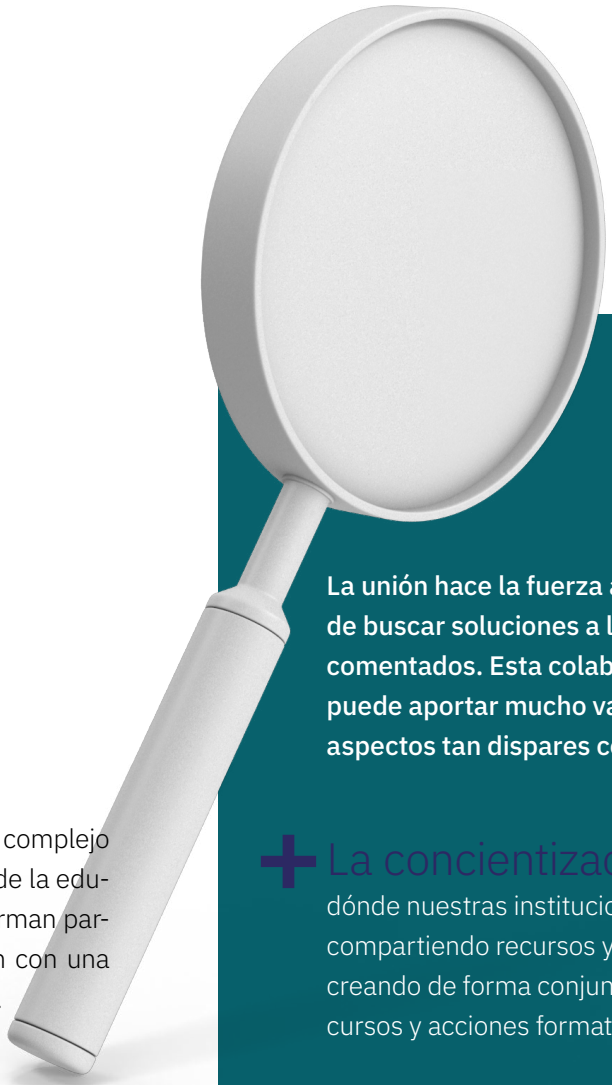
Crear y consolidar estos equipos en tiempo no es tarea sencilla. El IMC 2024 muestra que cerca de 4 de cada 10 IES tiene previsto incorporar nuevo personal de ciberseguridad en los próximos 12 meses. Sin embargo, las instituciones manifiestan un alto grado de complejidad para la captación de talento debido a las elevadas pretensiones económicas del personal cualificado (57%), la escasez de dichos perfiles (55%) y la alta tasa de movilidad que los mismos presentan en cuanto al cambio de organización (29%). Son aspectos que complican la creación de equipos de ciberseguridad en las IES iberoamericanas, representando un reto importante para garantizar una evolución en la madurez de nuestras instituciones.

Así mismo, el 37% de IES ha perdido personal relacionado con ciberseguridad en el último año. De éstas, el 77% manifiesta que su personal especializado disminuyó entre el 1% y el 25%. Las principales motivaciones para la retención de talento, según las IES participantes, son las siguientes: remuneraciones altas (74%), posibilidades de mejora en la carrera profesional (37%), flexibilidad de horario y condiciones de trabajo (20%) y el tipo de proyectos y desafíos técnicos del día a día (16%). Por lo tanto, estamos en una situación que requiere un esfuerzo extra en el proceso de retención de talento y por ende, la revisión de procedimientos, estructuras y condiciones laborales.

4 de cada 10

IES tienen previsto incorporar nuevo personal de ciberseguridad en los próximos 12 meses.

Oportunidades.



Aunque el panorama global es hoy incierto y complejo en el campo de la ciberseguridad, el sector de la educación superior y en concreto las IES que forman parte de la red colaborativa MetaRed, cuentan con una poderosa arma, respaldada en la propia red.

El poder de la colaboración internacional puede consignarse como un factor diferenciador, capaz de brindar un alto valor para nuestro sector.

El aprovechamiento de las buenas prácticas en países referentes por su nivel de madurez, el estudio de normativa desarrollada, la experiencia en la gestión operativa de tantas instituciones, la optimización de recursos técnicos, etc., es una base de conocimiento y especialización tan grande que, bien compartida, puede ayudar a incrementar el nivel de madurez de nuestras organizaciones.

La unión hace la fuerza a la hora de buscar soluciones a los retos comentados. Esta colaboración puede aportar mucho valor en aspectos tan dispares como:

+ La concientización, dónde nuestras instituciones ya están compartiendo recursos y materiales, creando de forma conjunta nuevos cursos y acciones formativas, etc.

+ La captación de talento, dónde proyectos como el Capture The Flag (CTF) Iberoamericano, fomentan la creación y descubrimiento de talento en ciberseguridad.

+ La medición, comprensión y conocimiento de la situación real de nuestras instituciones es un paso previo para la creación y ejecución de estrategias que deriven en acciones de mejora y fortalecimiento de la seguridad de la información en nuestras instituciones. Es el caso de este informe IMC 2024.

El 62%
de las IES ofrecen programas formativos relacionados con la ciberseguridad.

El papel de las IES en la ciberseguridad.

El presente Informe del Sector de la Educación Superior en Iberoamérica, además de medir el nivel de madurez de la ciberseguridad interna de cada institución, país o global, cuenta con un componente adicional centrado en el compromiso y responsabilidad que las IES tienen como organizaciones creadoras de talento, fuentes de educación, investigación y transferencia de conocimiento a la sociedad. En este sentido, estas instituciones tienen la responsabilidad de trabajar para reducir al máximo varios de los retos a los que nos enfrentamos en este campo. En concreto, nos referimos a todo lo relativo a la creación de talento y puestos cualificados que puedan atender la alta demanda de estos profesionales a nivel global.

Según los datos obtenidos, el 62% de las IES participantes ofrecen programas formativos relacionados con la ciberseguridad, siendo el 27,6% programas de grado y el 35,5%, formación de postgrado. Estas cifras serán objeto de estudio en siguientes informes del IMC, con el objetivo de analizar su evolución y apoyar la toma de decisiones que permitan un reajuste entre la oferta y la demanda de este colectivo profesional.

Resultados obtenidos.

	ARGENTINA	CHILE	COLOMBIA	ECUADOR	ESPAÑA	MÉXICO	PORTUGAL	IBEROAM.
IMC GLOBAL	L1	L1	L2	L1	L2	L1	L1	L1
GB	L1	L2	L2	L1	L2	L1	L1	L1
Estrategia	L1	L2	L2	L1	L2	L2	L2	L2
Política	L1	L2	L2	L1	L3	L2	L2	L2
Normativa	L1	L2	L2	L0	L2	L1	L1	L1
Procedimientos	L1	L1	L2	L1	L2	L1	L1	L1
Responsabilidad	L0	L2	L2	L0	L2	L1	L2	L1
Presupuesto	L1	L1	L2	L1	L1	L1	L0	L1
ID	L1	L1	L2	L1	L1	L1	L1	L1
Inventarios activos	L1	L1	L2	L1	L2	L1	L2	L1
Análisis riesgos	L1	L1	L2	L0	L2	L1	L1	L1
Análisis impacto	L1	L1	L2	L1	L1	L1	L1	L1
PR	L1	L2	L2	L1	L2	L1	L2	L2
Accesos	L1	L1	L1	L1	L2	L1	L1	L1
Personal	L1	L1	L2	L1	L1	L1	L1	L1
Infraestructura	L2	L2	L3	L2	L3	L2	L2	L3
Equipos	L1	L1	L2	L1	L2	L1	L2	L1
Comunicaciones	L2	L3	L3	L2	L2	L2	L2	L2
Servicios	L1	L2	L2	L1	L2	L2	L1	L2
Continuidad	L1	L1	L1	L1	L1	L1	L1	L1
Externos	L1	L2	L2	L1	L2	L2	L2	L2
DE	L1	L2	L2	L1	L2	L1	L2	L1
Intrusiones	L1	L2	L2	L1	L2	L1	L1	L2
Vigilancia	L1	L1	L2	L1	L2	L1	L1	L1
Actividad usuarios	L1	L2	L2	L1	L2	L1	L2	L2
Anomalías	L1	L2	L2	L1	L2	L1	L2	L1
REyRC	L1	L1	L1	L0	L2	L1	L1	L1
Gestión incidentes	L1	L1	L1	L1	L2	L1	L1	L1
Mitigación	L1	L1	L1	L0	L2	L1	L1	L1
Recuperación	L1	L1	L1	L0	L1	L1	L1	L1

Tabla 1: IMC por dominio y subdominio

3.
IMC: Índice de Madurez en Ciberseguridad.

3.
IMC: Índice de Madurez en Ciberseguridad.

El IMC 2024 es un marco general que permite evaluar el estado actual de la ciberseguridad en las universidades e IES de Iberoamérica. Ofrece una visión detallada y específica del nivel de madurez de estas instituciones y habilita la comparación con entidades de similar naturaleza del propio país y de otros participantes en el estudio. La misión de este informe es convertirse en una herramienta valiosa para la toma de decisiones estratégicas y operativas y para una mejor asignación de recursos al momento de desarrollar iniciativas específicas de protección de los activos de información.

Las universidades e IES son depositarias de una gran cantidad de información sensible, desde datos personales de estudiantes y profesores hasta investigaciones de vanguardia y propiedad intelectual. Proteger esta información no es solo una cuestión de seguridad, sino también de responsabilidad social y cumplimiento normativo. Implica que la institución es capaz de gobernar y gestionar sus activos de información, preservando el valor que se genera a partir de ellos.

Además, estas instituciones vienen poniendo de manifiesto un proceso paulatino e inexorable de transformación digital, acelerado por la pandemia mundial de COVID-19, que ha demostrado no tener vuelta atrás.

Si bien existen y se aplican diversos marcos de evaluación de la madurez en ciberseguridad en entidades de distintos tipos y en diferentes latitudes, este estudio viene a llenar un vacío a nivel de la región Iberoamericana para el ámbito de la enseñanza superior, con el objetivo de contribuir a una mejora en la ciberseguridad en este tipo de instituciones.

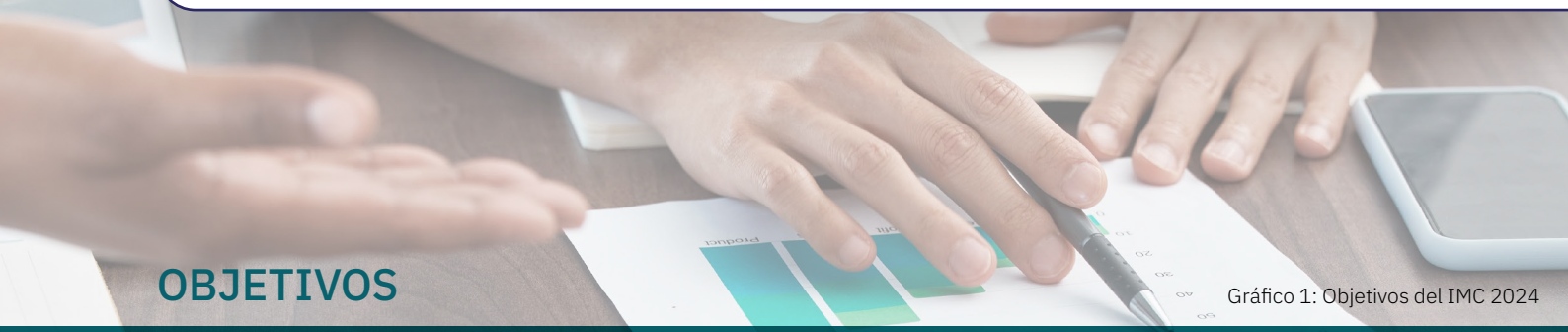
Por este motivo, el IMC 2024 está dirigido a autoridades nacionales vinculadas a las IES, directivos de estas instituciones, responsables de áreas de TIC y Seguridad de la Información (o similar), equipos técnicos y académicos vinculados a iniciativas de ciberseguridad en el ámbito académico.

Se espera que, como resultado del presente estudio, las instituciones participantes puedan:

Conocer el estado de situación de la ciberseguridad en las IES de la región iberoamericana que integran MetaRed.

Obtener un panorama general que les permita comparar su nivel de madurez con otras instituciones de su propio país y con el promedio en Iberoamérica.

Adoptar medidas fundadas para mejorar el estado de la ciberseguridad en sus respectivos ámbitos.



OBJETIVOS

Gráfico 1: Objetivos del IMC 2024

Proporcionar un análisis detallado de la situación actual de las IES en términos de ciberseguridad, identificando fortalezas, áreas de mejora y habilitando la comparación con otras IES de la región.

Ofrecer un marco que permita a las instituciones desarrollar e implementar estrategias de mejora contínua en sus prácticas de ciberseguridad.

Apoyar los proyectos de MetaRed para crear un plan de acciones colaborativas global más preciso, de alto valor añadido.

Elevar la conciencia y comprensión de la ciberseguridad dentro de las comunidades universitarias, promoviendo una cultura de prevención y respuesta efectiva ante incidentes cibernéticos.

3.1 Modelo IMC.

El modelo del IMC 2024 se basa en los principios y dominios del Framework de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos, ampliamente reconocido internacionalmente. La elección de este framework se debe a su enfoque integral y flexible, que permite una adaptación efectiva a las necesidades y realidades de cualquier tipo de entidad, incluyendo las IES iberoamericanas.

Además, se integraron controles y prácticas de otros estándares y normas internacionales, como **ISO/IEC 27001:2022 y 27002:2022 y el Esquema Nacional de Seguridad de España,** para asegurar una cobertura completa de los aspectos relevantes en materia de seguridad de la información.

Este enfoque híbrido y personalizado justifica la elección del modelo, ya que combina aspectos relevantes de estándares globales de reconocimiento internacional, adaptándose a un contexto específico de la región. En suma, proporciona un marco robusto y efectivo para la evaluación y mejora de la madurez en ciberseguridad para IES de la región.

3.2 Dominios.

A continuación se muestran los 6 dominios considerados en este estudio, y se explica brevemente su alcance.

Gobernar (GB)

Involucra el establecimiento, compromiso y monitoreo de la ciberseguridad por parte de la dirección de la organización. Esto resulta fundamental para incorporar la ciberseguridad en su funcionamiento. Con este objetivo se relacionan la definición de la estrategia de ciberseguridad, la elaboración, mantenimiento y comunicación de políticas, el establecimiento de procesos y procedimientos, la identificación de roles y responsabilidades en materia de ciberseguridad y de las tareas que hacen a la gestión de la ciberseguridad. Se vincula a comprender el contexto, establecer la estrategia, gestionar el riesgo sobre la cadena de suministro, definir los roles, responsabilidades y autoridades, elaborar políticas, implementar procesos y procedimientos y supervisar las actividades que se llevan a cabo para cumplir los objetivos fijados.

Detectar (DE)

Involucra acciones orientadas a buscar y analizar posibles ataques y compromisos a la ciberseguridad. Permite el descubrimiento y análisis oportunos de anomalías, indicadores de compromiso y otros eventos de ciberseguridad potencialmente adversos, que pueden indicar la ocurrencia de ataques o incidentes de ciberseguridad. En esta etapa se encuentra el monitoreo de red a través de fuentes de información internas o externas, la configuración de herramientas para tal fin y el análisis de eventos.

Identificar (ID)

Implica determinar el riesgo actual de ciberseguridad para la organización. Para ello es necesario conocer sus activos (por ejemplo, datos, hardware, software, sistemas, instalaciones, servicios y personas) y los riesgos de ciberseguridad relacionados a ellos. Todo esto a fin de dedicar esfuerzos para la identificación de mejoras necesarias respecto a las políticas, procesos, procedimientos y prácticas de la organización que respaldan la gestión de la ciberseguridad. La identificación de estas políticas, procesos, procedimientos y prácticas también se incluye en esta etapa.

Responder y recuperar (REyRC)

El primero de estos términos refiere a cómo actuar ante un incidente de ciberseguridad detectado. Cubre la gestión, análisis, mitigación y comunicación de incidentes de ciberseguridad y procesos vinculados. Recuperar, por su parte, implica restaurar activos y operaciones que se vieron afectados por un incidente de ciberseguridad. Incluye acciones en pos de la restablecimiento oportuno de las operaciones normales para reducir y contener el impacto. Entre ellos se encuentra contar con planes de contingencia y de recuperación, y con los procedimientos asociados.

Proteger (PR)

Se refiere a las tareas de implementación de controles para mitigar los riesgos de ciberseguridad existentes, con el objetivo de proteger los activos para reducir la probabilidad y el impacto de eventos adversos de ciberseguridad. En esta etapa se encuentran la concientización y el entrenamiento, la seguridad de datos, la gestión de identidades, la seguridad de la plataforma y la resiliencia de la infraestructura tecnológica.

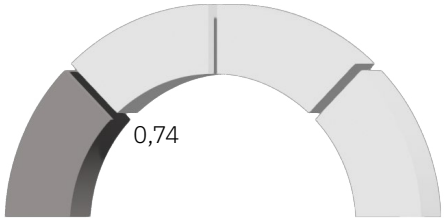
Formación y talento (FT)

Adicionalmente a los dominios contemplados en el marco de Ciberseguridad del NIST, se considera como parte del relevamiento un dominio complementario referido a la formación en ciberseguridad y a la captación y retención de talentos en el área respectiva de la institución. Este dominio se incluye en razón de tratarse de organizaciones dedicadas a la educación universitaria. Sin embargo, se aclara que los aspectos comprendidos en este nuevo dominio no son contemplados en la determinación del nivel de madurez de la institución.

3.3
Niveles de madurez.

Se definen niveles de madurez de acuerdo al estado de implementación de los controles en cada dominio. Cada control, definido en los diferentes dominios, será correlacionado dentro de los 4 niveles de madurez concretados: L0, L1, L2, L3. A continuación se muestran las características incluidas en cada uno de los 4 niveles.

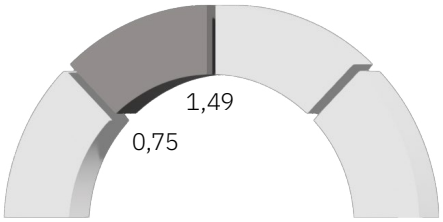
L0 INICIAL



No se realizan prácticas de ciberseguridad.

- Conciencia mínima sobre la importancia de la ciberseguridad.
- Ausencia de políticas y procedimientos formales.
- Uso limitado y no sistemático de tecnologías de seguridad.
- Sin personal dedicado específicamente a la ciberseguridad.
- Falta de procesos formales de gestión de riesgos.

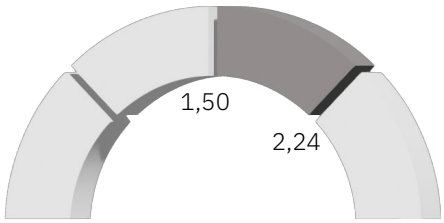
L1 BÁSICO



Se realizan prácticas iniciales, pero pueden ser ad hoc o informales.

- Establecimiento de políticas y procedimientos básicos.
- Implementación inicial de tecnologías de seguridad.
- Personal responsable de la ciberseguridad, aunque no especializado.
- Inicio de procesos formales de identificación y evaluación de riesgos.

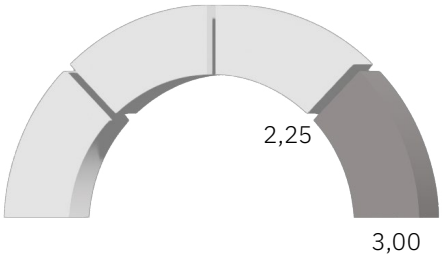
L2 INTERMEDIO



Las prácticas de ciberseguridad son más completas y avanzadas que en L1. Están documentadas y se proporcionan recursos adecuados para apoyar el proceso.

- Políticas y procedimientos bien definidos y documentados.
- Implementación avanzada de tecnologías de seguridad, incluyendo sistemas de detección de intrusos y herramientas de cifrado.
- Personal de ciberseguridad dedicado y especializado.
- Procesos de gestión de riesgos formalizados y regularizados.

L3 AVANZADO



Las prácticas de ciberseguridad son más avanzadas que en L2. Las actividades están guiadas por políticas u otras directivas organizacionales. Se asignan responsabilidades e instancias de rendición de cuentas y de autoridad para realizar las prácticas. El personal que realiza las prácticas tiene habilidades y conocimientos adecuados. Se evalúa y realiza un seguimiento de la eficiencia de las actividades.

- Políticas y procedimientos integrados en todas las operaciones de la institución.
- Uso de tecnologías de seguridad de última generación y enfoque proactivo en la mejora continua.
- Equipo de ciberseguridad altamente especializado y capacitado.
- Gestión de riesgos altamente madura con un enfoque proactivo en identificación y mitigación de amenazas.

3.4
Tipología de la muestra.

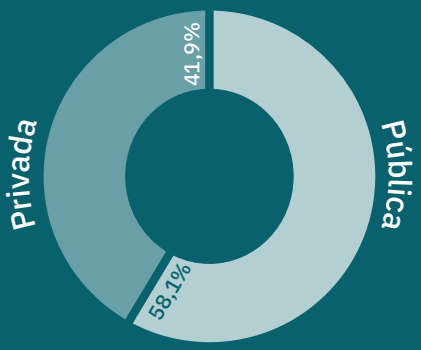
En esta primera edición contamos con la participación de **247 IES de 10 países de Iberoamérica, que representan a más de 6.5 millones estudiantes de educación superior,** según los datos provistos en la encuesta por las instituciones.

La participación ha provenido de los siguientes países/regiones:

- Argentina (ARG)
- Brasil (BRA)
- Chile (CHI)
- Colombia (COL)
- Centroamérica y el Caribe (CyC)
- Ecuador (ECU)
- España (ESP)
- México (MEX)
- Perú (PER)
- Portugal (POR)

Tipología de las IES.

A nivel de tipología de las IES, hemos contado con una mayor cantidad de respuestas provenientes de IES públicas, con un 58,1%, frente al 41,9% de IES privadas. Cabe acotar, sin embargo, que esta tipología tiene una fuerte dependencia de la distribución en el país de origen.



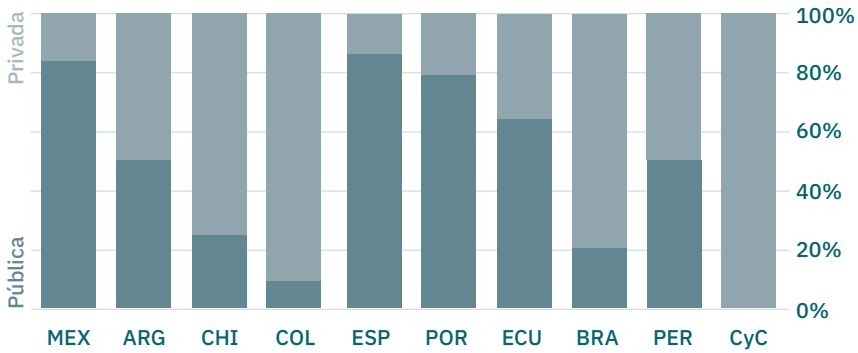


Gráfico 2: Distribución por tipo de IES (Global y por país)

Algo similar ocurre con el tamaño teniendo en cuenta la cantidad de estudiantes promedio de cada IES, donde encontramos importantes diferencias según el país.

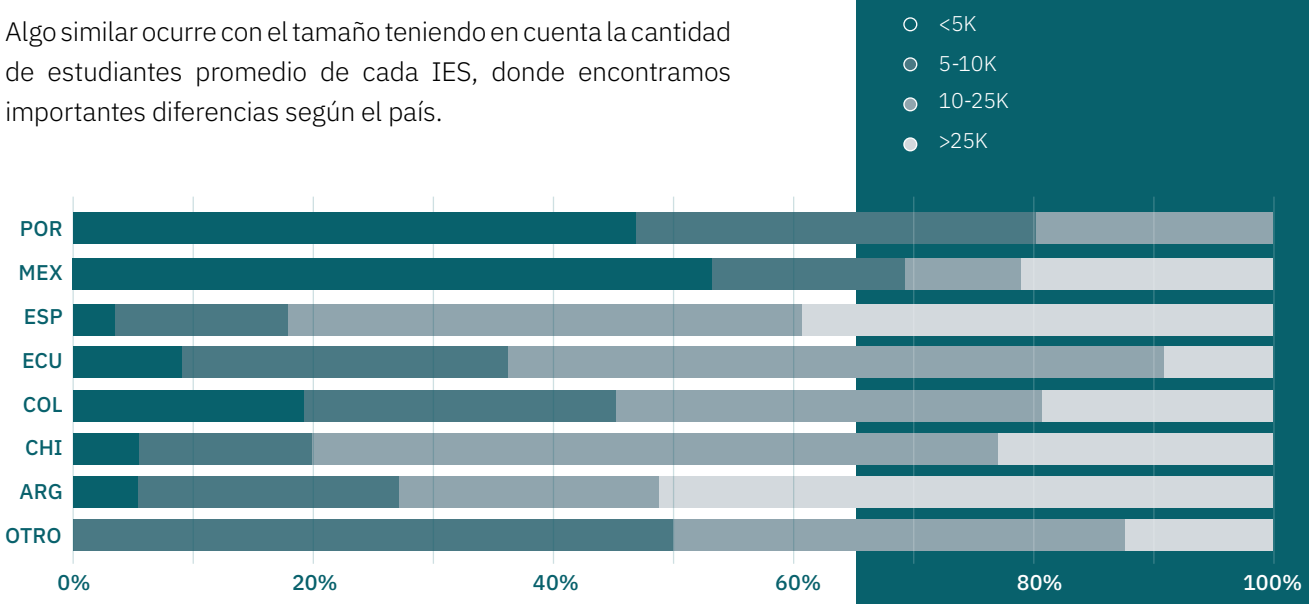


Gráfico 3: Distribución por tamaño de IES (nº de estudiantes), por país

Este mismo análisis puede realizarse según se trate de IES públicas o privadas en cada país.

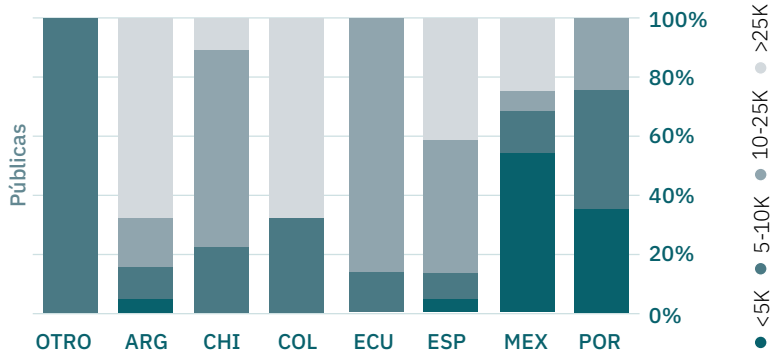


Gráfico 4: Distribución por tamaño de IES públicas (nº de estudiantes), por país

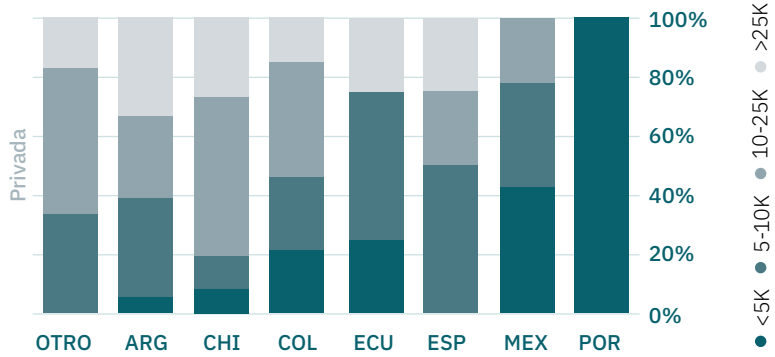
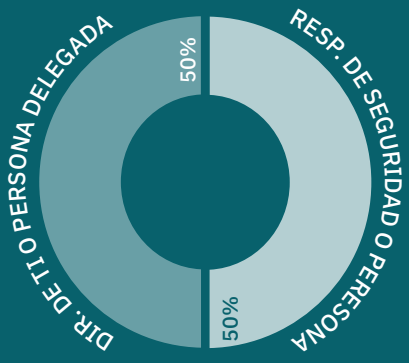


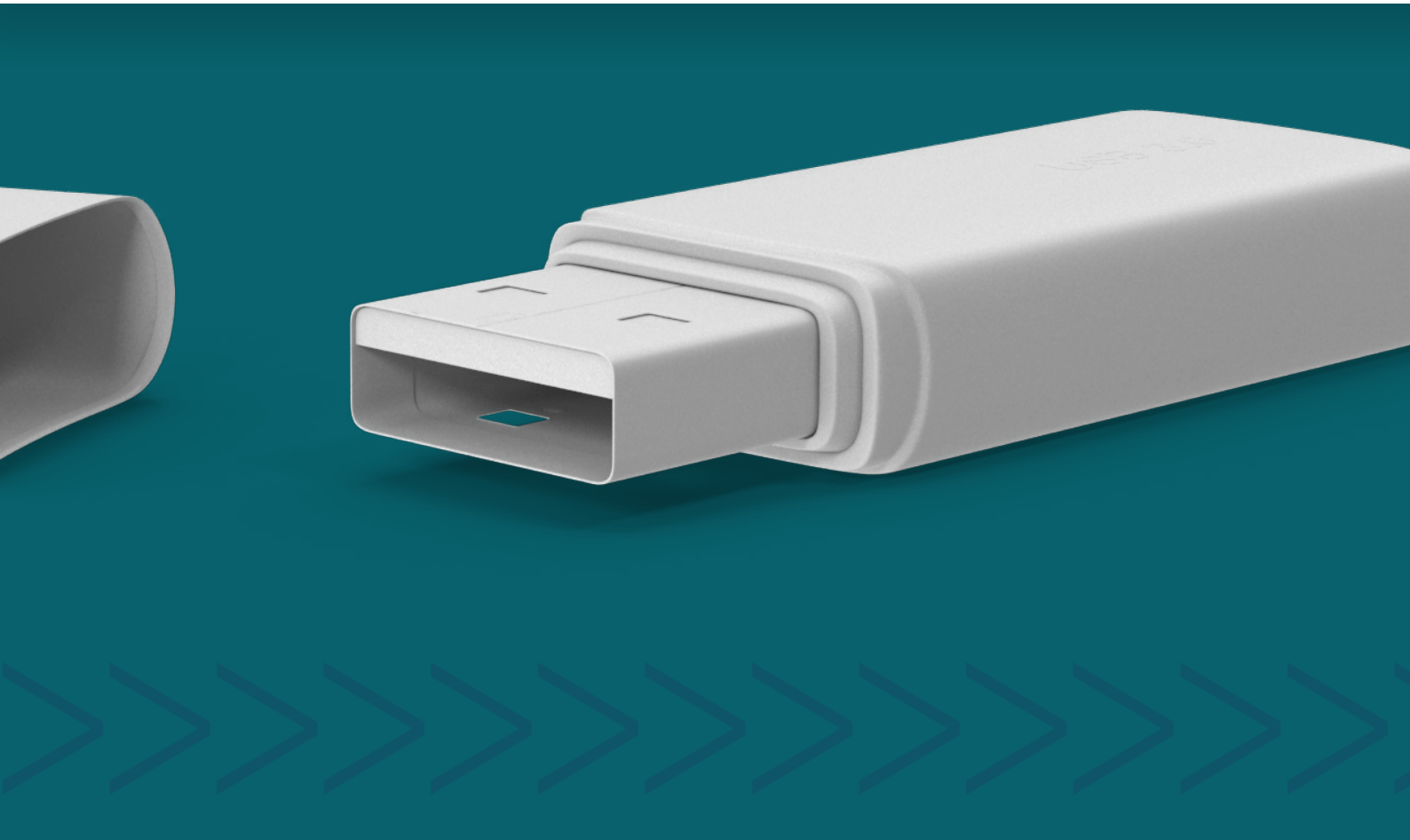
Gráfico 5: Distribución por tamaño de IES públicas (nº de estudiantes), por país

Perfil del encuestado.

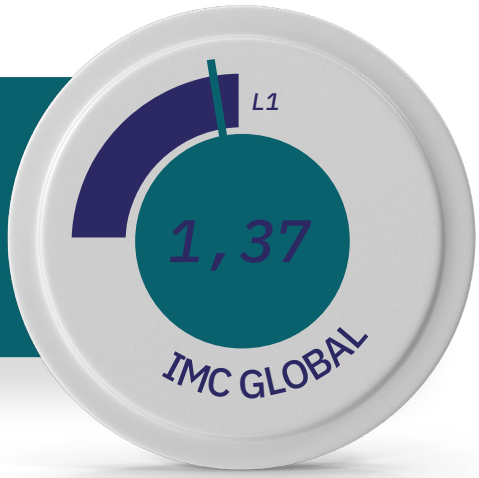
En cuanto al perfil de las personas que respondieron las preguntas de la encuesta, el 48,6% de los encuestados ocupa puestos de responsable de seguridad o CISO y el 51,4%, son Directores/as del área IT.



4.
Resultados IMC. Nivel de Madurez.



4.1
IMC Iberoamericano.



El IMC Iberoamericano global, calculado según el promedio de todas las IES participantes de los diferentes países, es 1.37, lo que sitúa al sector de la educación superior iberoamericana en un nivel de madurez básico (L1), de los cuatro niveles de madurez disponibles (L0, L1, L2 y L3).

Este valor se encuentra muy cerca de la frontera con el nivel de madurez intermedio L2 (1,50) y refleja cómo, observando los promedios, las prácticas realizadas son iniciales. Sin embargo, también es importante señalar que una parte de estas instituciones ha comenzado a establecer prácticas más completas o avanzadas (documentadas y apoyadas parcialmente en recursos y herramientas adecuadas). Sin embargo, el hecho de encontrarse dentro del nivel L1 lleva a pensar en la necesidad de reforzar todos los procesos, tal como veremos más adelante al estudiar de manera más profunda los distintos dominios.

Si analizamos las IES según su nivel de madurez, obtenemos que **el 16,3% presentan el nivel de madurez inicial (L0),** lo que es indicador de acciones de ciberseguridad muy limitadas o casi nulas, sin gobierno ni gestión.

Por su parte, algo más de **4 de cada 10 instituciones (43,1%) presenta un nivel básico (L1),** caracterizado por la realización de prácticas iniciales ad hoc o informales.

Un 31,4% de las IES muestra un nivel de madurez intermedio (L2), con prácticas de ciberseguridad más completas y avanzadas que en L1, especialmente en cuanto a la documentación y asignación de recursos.

Por último, **las IES con un nivel de madurez avanzado (L3) representan tan solo el 7,7% del total**.

Gráfico 6: Distribución de las IES por nivel de madurez

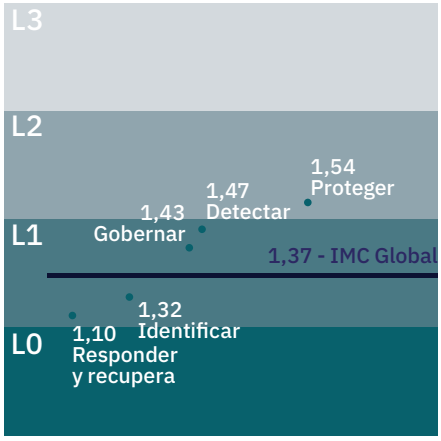
Una vez analizado el IMC iberoamericano a nivel global, podemos enfocarnos en los diferentes dominios de estudio incluidos en este modelo. Según esto, los datos reflejan una tendencia global hacia la realización de acciones de protección, para lo cual las IES iberoamericanas muestran su máximo nivel promedio, con un nivel de madurez de 1,54 puntos (L2). Este dominio Proteger (PR) recoge todas las acciones de preservación de la información, el acceso, la seguridad de la infraestructura, de los equipos, de las comunicaciones y de otros elementos clave para la institución. Sin duda, se trata de acciones clave en la seguridad de nuestras instituciones pero que deben ser complementadas con el resto de dominios analizados para contribuir a un nivel de seguridad homogéneo.

En segundo lugar, la capacidad de detección, es decir el dominio Detectar (DE), muestra un nivel de madurez básico de 1,47 (L1), muy cercano al umbral inferior del nivel de madurez intermedio L2, lo que puede interpretarse como la existencia de IES con prácticas de detección más completas a nivel de recursos y documentación.

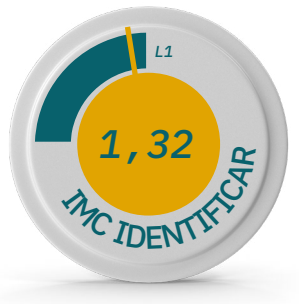
Por su parte, el Gobierno (GB) de la ciberseguridad ocupa el tercer puesto, con un valor de 1,43, lo que lo sitúa en un nivel básico L1, tan solo a 7 puntos de un nivel intermedio L2. Se trata de una situación promisoria, a partir de la cual, es posible avizorar que siga incrementando su valor en los próximos años, reflejando una tendencia positiva de las IES hacia una cultura de seguridad general.

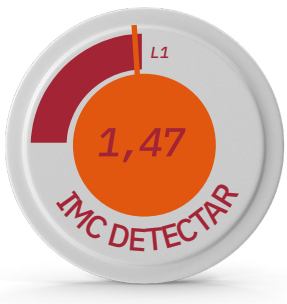
A continuación, el dominio Identificar (ID) presenta un promedio de 1,32 puntos (básico L1), y el dominio Responder y Recuperar (REyRC), un valor de 1,10 puntos (inicial, L1). Ambos valores se encuentran por debajo del IMC global iberoamericano (1,37).

Esta priorización de la protección y detección frente a otros dominios como el gobierno, la identificación, o la respuesta y recuperación, nos ofrece una visión global del estado general de madurez en ciberseguridad de nuestras IES. Refleja la preocupación subyacente de nuestras instituciones por su capacidad de atender los diferentes frentes de trabajo en los que nos encontramos inmersos.



Priorización de la protección y detección frente a otros dominios.

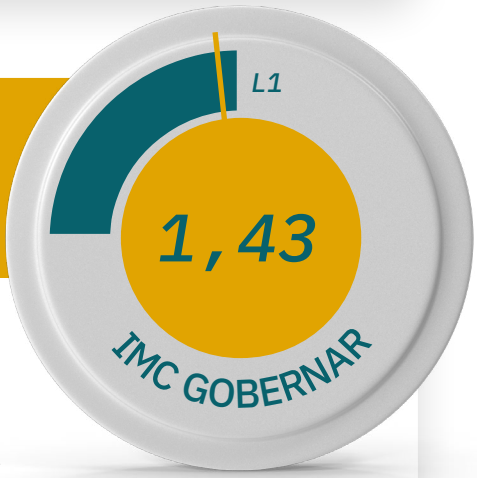




Infografía 1: Niveles de madurez por dominio

4.2
IMC por dominio de aplicación.

Gobernar.



Para el dominio Gobernar (GB), las IES iberoamericanas muestran un nivel de madurez básico L1 (1,43), lo que refleja un estado en el que algunas prácticas ya podrían encontrarse documentadas y se contaría con iniciativas de ciberseguridad que estarían recibiendo recursos pero de manera parcial.
El valor para este dominio se sitúa levemente por encima del valor IMC Global (1,37) y hace que este dominio ocupe el tercer puesto, tras Proteger (PR) y Detectar (DE).

Los subdominios con mayor nivel de madurez son los relativos a la existencia de una política de seguridad, y a la consideración de la ciberseguridad como un aspecto estratégico en las IES .

En el otro extremo, pero siempre dentro del nivel básico L1, se observa que el subdominio Presupuesto (1,09), muestra que no se considera a la hora de asignar fondos específicos para ciberseguridad. Esto podría interpretarse como una **falta de visibilidad de la relevancia del área o bien, como una escasa inversión en las iniciativas de ciberseguridad institucional.**

Subdominios de Gobernar y su correspondiente nivel

SUBDOMINIO	IMC
Estrategia	*L2 (1,64)*
Política	*L2 (1,72)*
Normativa	*L1 (1,48)*
Procedimientos	*L1 (1,34)*
Roles y responsabilidades	*L1 (1,28)*
Presupuesto	*L1 (1,09)*

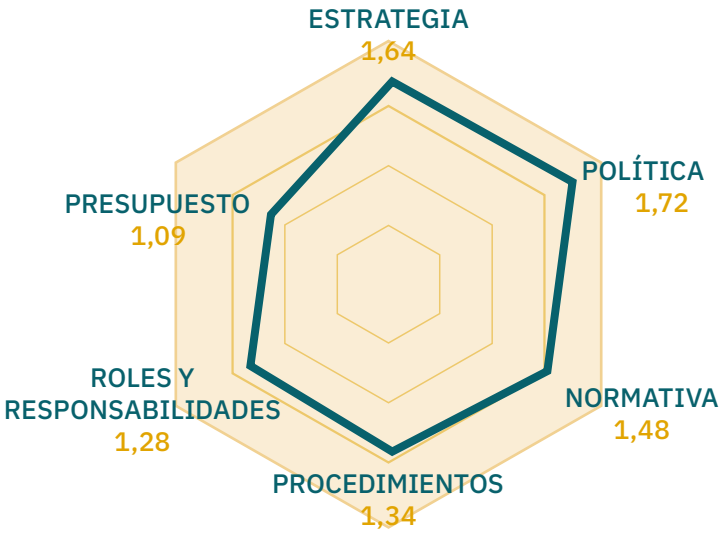


Gráfico 7: Subdominios de Gobernar y su correspondiente nivel

Subdominio

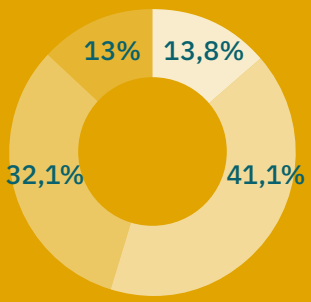
ESTRATEGIA

Profundizando el análisis, a nivel del elemento estratégico, el 47,2% de las IES participantes manifiestan haber desarrollado una estrategia institucional de ciberseguridad, mientras que el 24,4% cuenta con algunas definiciones formalizadas pero dentro del ámbito del área de TI, el 21,5% dispone de algunas definiciones no formalizadas y el 6,9% no ha establecido definiciones claras en este sentido.

Así pues, si comparamos el grado de madurez de las instituciones según sus avances en la determinación de una estrategia de ciberseguridad, podemos concluir que **casi el 50% ya cuenta con un documento de este tipo, mientras que prácticamente el 25% manifiesta haber desarrollado lineamientos sobre ciberseguridad pero desde el área de TI, y un porcentaje similar posee definiciones informales o directamente no cuenta con ellas.** Esto muestra que a nivel estratégico, este tema es tomado en cuenta por las IES, si bien es un proceso aún en desarrollo.

Gráfico 8: Existencia de una estrategia de ciberseguridad en las IES

Gráfico 9: Consideración de la ciberseguridad en la estrategia institucional



- No se considera
- Incorpora algunas acciones aisladas
- Incorpora iniciativas de ciberseguridad con objetos concretos
- Incluye iniciativas medibles como parte de la mejora continua

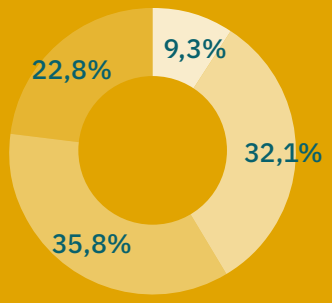
Asimismo, el componente estrategia se basa también el apoyo de la dirección de la institución, abordando la ciberseguridad no solo como un aspecto del área de TI, sino como una problemática transversal a toda la organización. Por lo tanto, el valor que el compromiso de los equipos rectorales o directivos puedan otorgar a la seguridad de la información se puede medir, en cierta manera, por el grado de desarrollo de una estrategia institucional.

Los datos obtenidos muestran que una **gran parte de las IES tienen referencias a la ciberseguridad en sus estrategias institucionales (86,2%).** De estos, un 13% incluye iniciativas de ciberseguridad medibles como parte del proceso de mejora continua y un 32,1% incorpora objetivos concretos. Estos datos reafirman el concepto de proceso en desarrollo expresado más arriba, en cuanto a la relevancia que va ocupando la ciberseguridad entre los aspectos estratégicos de las IES.

Subdominio

POLÍTICA

Gráfico 10: Existencia de una política de seguridad de la información



- No existe
- Existen definiciones pero no están formalizadas
- Existe formalmente, pero sólo algunos la conocen y aplican
- Existe formalmente, se conoce y se aplica en toda la institución

Por su parte, a nivel de política de seguridad de la información, los datos relevados muestran que **la mayor parte de las IES cuenta con iniciativas en relación a su política de seguridad (90%).** Sin embargo, sólo el 22,8% la ha definido formalmente, dado a conocer a todo el personal y aplicado en toda la institución. Por su parte, el 35,8% la ha definido formalmente pero sólo es conocida y aplicada por parte de la comunidad objetivo, y el 32,1% restante indica contar con definiciones en un estadío informal. Esto pone de relieve la existencia de acciones a nivel global en pos de contar con una política de seguridad, al tiempo que muestra que esta no ha sido incorporada aún en el marco normativo ni comunicada ni aplicada de manera integral. Por último, casi un 10% manifiesta no contar con este tipo de instrumentos normativos, que constituyen, sin duda, un pilar de la protección de la información.

La gráfica muestra las respuestas obtenidas a la pregunta correspondiente a políticas, en totales y en porcentajes.

Subdominio

PRESUPUESTO

El ítem correspondiente al presupuesto se halla en un nivel básico L1 (1,09) a nivel global, ocupando el nivel más bajo de las distintas preguntas dentro del dominio Gobernar (GB). Los datos muestran que el 65,5% destina fondos a las iniciativas de ciberseguridad, pero sólo el 4,1% de las IES cuenta con un presupuesto de ciberseguridad diferenciado de TI. Por otro lado, el 35,8% tiene asignaciones específicas dentro del presupuesto de TI y el 25,6%, dentro de las asignaciones generales. Por último, el 34,6% de las instituciones manifiesta no contar con asignación de presupuesto para ciberseguridad de ninguna naturaleza.

Gráfico 11: Presupuesto para ciberseguridad

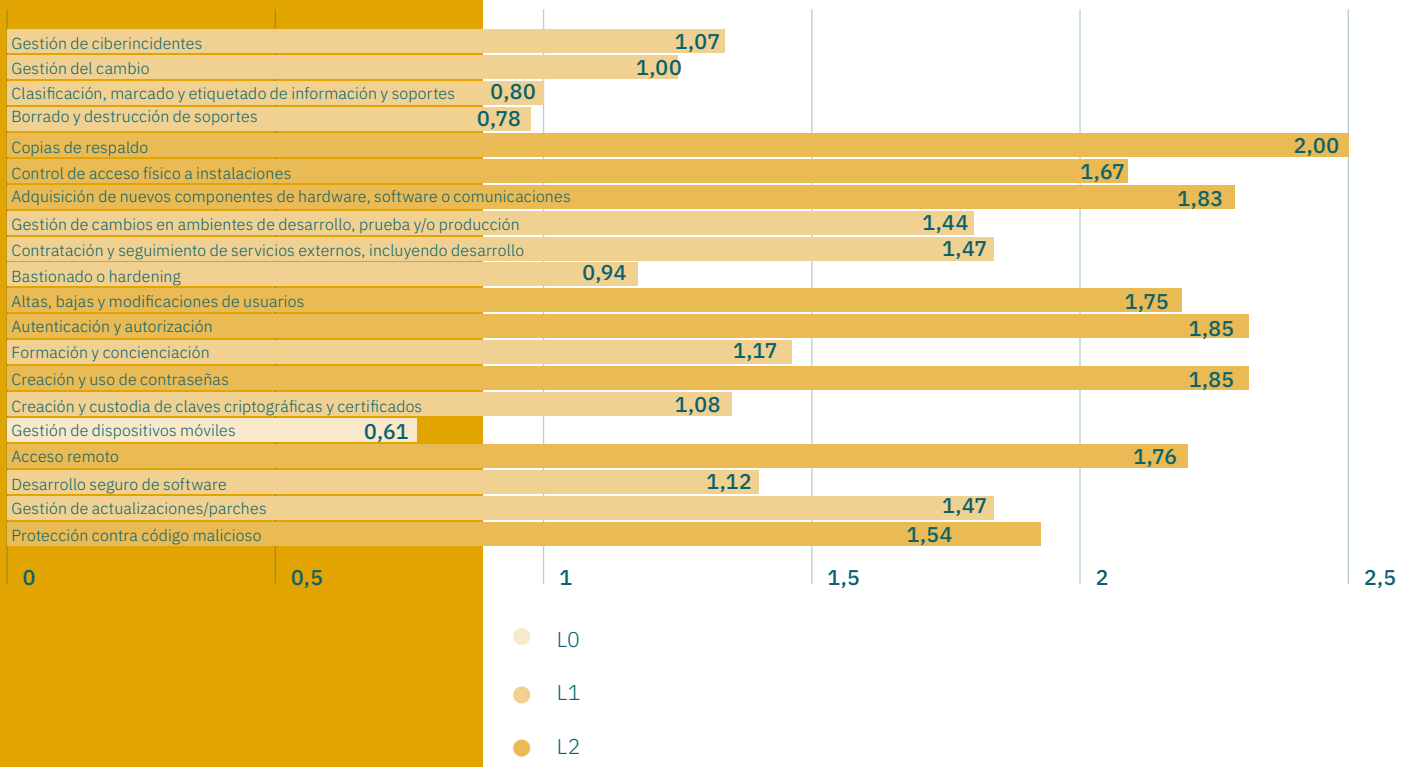
Subdominio

PROCEDIMIENTOS

En cuanto a los procedimientos de seguridad, los datos obtenidos señalan que en promedio, el nivel de madurez es básico L1 (1,34). Aquellos que alcanzaron un nivel intermedio L2 son los relativos a acceso remoto; creación y uso de contraseñas; autenticación y autorización; altas, bajas y modificación de usuarios; adquisición de nuevos componentes de TI; control de acceso físico a las instalaciones y copias de respaldo. El resto se mantuvo en el nivel básico L1 con la excepción de los de gestión de dispositivos móviles (0,61), que mostró un nivel de madurez inicial L0 correspondiente a la ausencia total de prácticas.

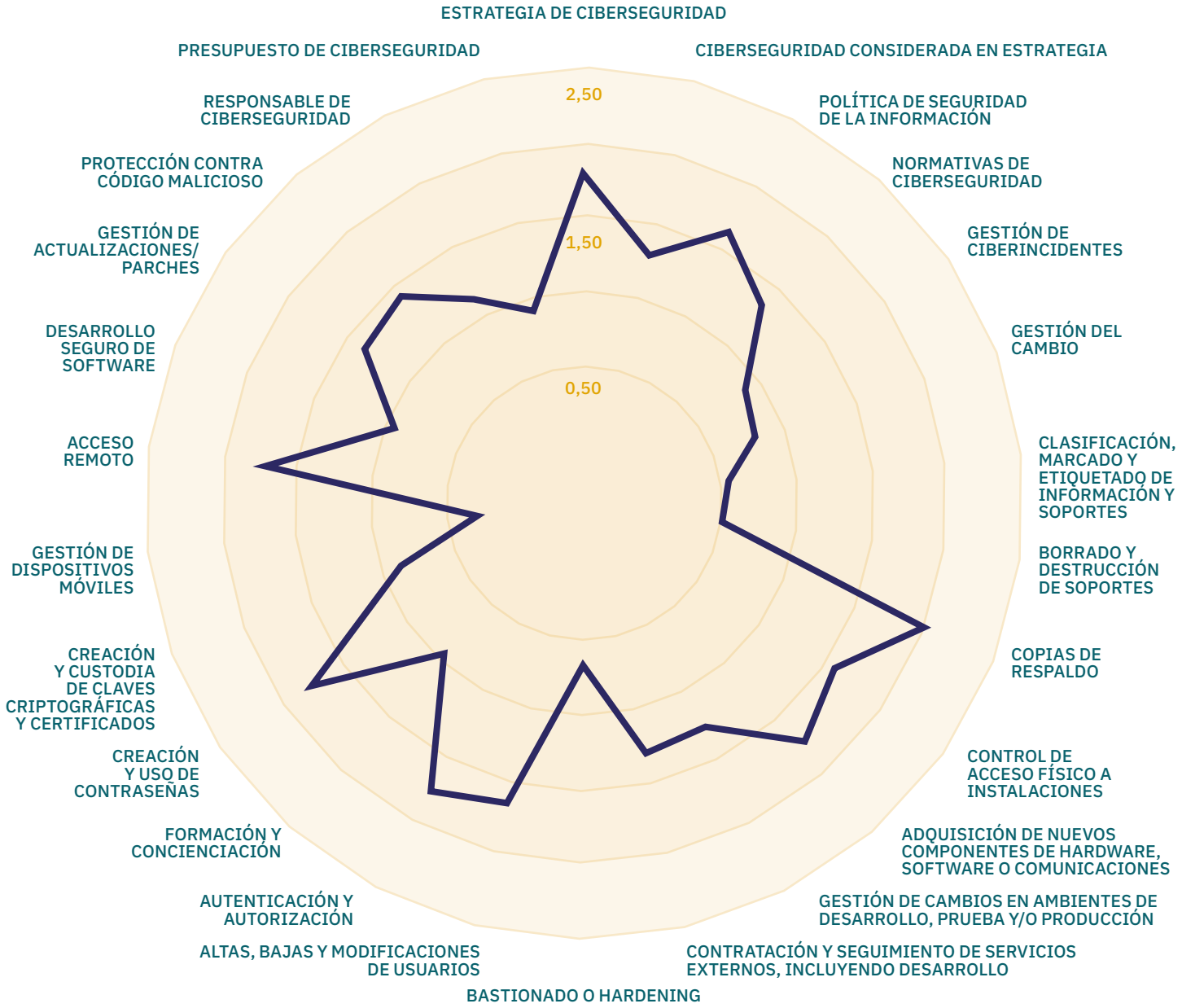
A continuación, el gráfico muestra el nivel de madurez de cada uno de los procedimientos relevados.

Gráfico 12: Existencia de procedimientos de ciberseguridad

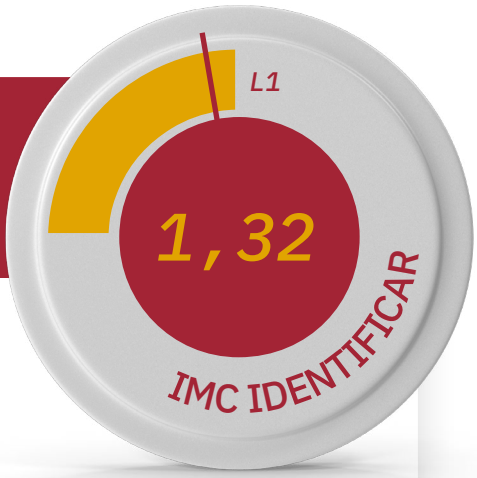


Por último, a nivel general del dominio Gobernar (GB), de los 27 aspectos que se cubren, el que presenta un mayor grado de madurez es el que indaga sobre la existencia de un procedimiento para el proceso de realización de copias respaldo (backups), con un valor promedio de 2,0 (L2). En el otro extremo, el desarrollo de procedimientos de gestión de dispositivos móviles (0,61) muestra un nivel de madurez inicial L0, denotando que no se realizan prácticas vinculadas a dicho proceso.

Gráfico 13: Nivel de madurez de todos los componentes del dominio Gobernar



Identificar.



Para el dominio IDENTIFICAR (ID), las IES iberoamericanas muestran un nivel de madurez promedio básico L1 (1,32), lo que pone de manifiesto una **baja capacidad para gestionar los riesgos** que pueden afectarlas.

En este caso, el valor promedio se sitúa levemente por debajo del valor del IMC Global (1,37), poniendo a este dominio en el anteúltimo puesto, luego de Proteger (PR), Detectar (DR) y Gobernar (GB) y antes que Responder y Recuperar (REyRC).

Todos los subdominios se encuentran en el nivel básico L1, siendo el más alto (cercano a L2) el correspondiente a la realización de un inventario de activos, y el más bajo el análisis de impacto de cualquier escenario de riesgo en la institución.

Estos valores estarían evidenciando que no se avanza en una gestión de riesgos integral y efectiva, siendo que se logra identificar los activos y se analizan en forma parcial los riesgos, pero no se llega a determinar el verdadero impacto que esos riesgos podrían tener sobre los servicios críticos de las IES.

Subdominios de Identificar y su correspondiente nivel

SUBDOMINIO	IMC
Inventario activos	*L1 (1,49)*
Análisis riesgo	*L1 (1,36)*
Análisis impacto	*L1 (1,10)*

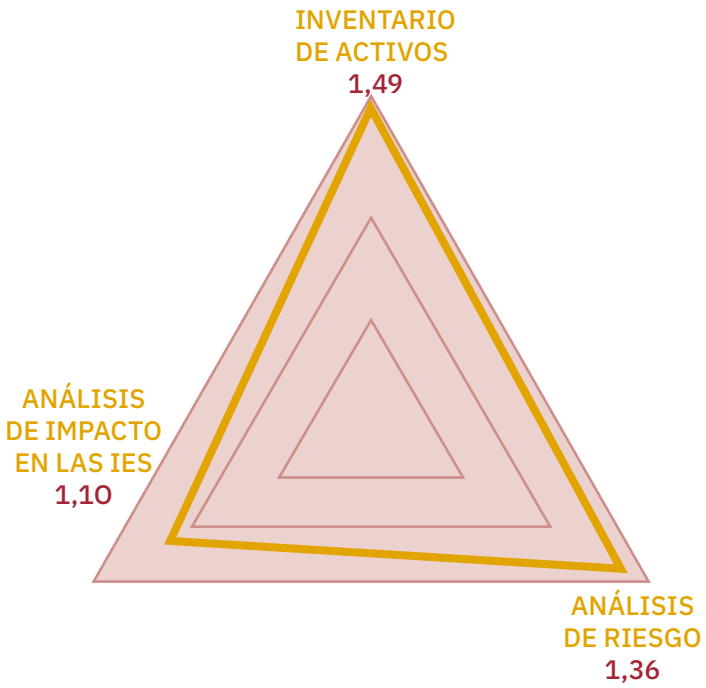


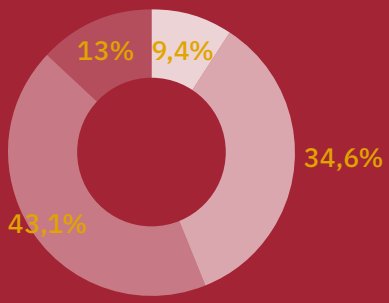
Gráfico 14: Subdominios de Identificar y su correspondiente nivel

Subdominio

ANÁLISIS DE RIESGO

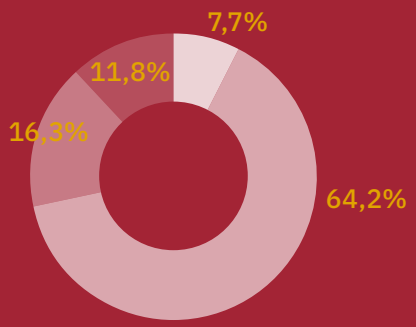
Ahondando en el segundo de los subdominios, vinculado a la realización de un proceso de análisis de riesgo en las IES, puede observarse que, **el 43% de las IES informó que el área de TI considera en forma específica los riesgos de ciberseguridad, y el 13%, que dichos riesgos se consideran a nivel institucional.** Cabe mencionar que específicamente para estas dos respuestas, se alcanza un nivel de madurez intermedio correspondiente a L2, lo que lleva a suponer que las prácticas están documentadas y se asignan recursos de manera adecuada. Sin embargo, **casi un 45% de las IES no realiza análisis de riesgos de ninguna naturaleza o sólo considera algunos riesgos de ciberseguridad dentro del análisis de riesgos de TI.** Cabe preguntarse entonces cuáles son las bases sobre las cuales estas IES determinan las medidas de seguridad a establecer.

Gráfico 15: Análisis de riesgo



- No se realiza
- Se consideran algunos riesgos dentro del análisis de riesgos de TI
- Se realizan análisis específicos por parte de TI
- Se realizan análisis específicos por parte de una instancia institucional

Gráfico 16: Análisis de amenazas y vulnerabilidades en las IES



- No se han identificado
- Identificados en forma parcial
- Identificados en forma completa
- Se han identificado y evaluado su impacto en la institución

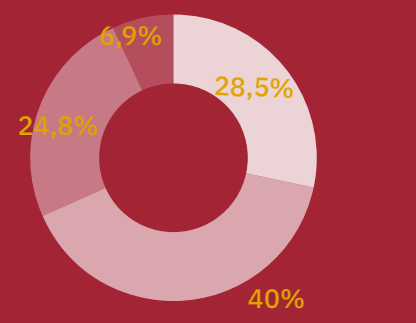
Al momento de indagar **sobre la identificación y documentación de vulnerabilidades y amenazas** que podrían afectar a los activos asociados a servicios esenciales o críticos, puede determinarse que **más de la mitad (64,2%) identifica solo de manera parcial estos aspectos tan determinantes a la hora de evaluar los riesgos, y un 7,7%, no realiza ningún tipo de análisis** en este sentido. En este último caso, el nivel de madurez es inicial L0, registrando uno de los valores más bajos de todos los aspectos analizados para este dominio.

En el otro extremo y con un nivel de madurez intermedio de L2, algo más que una cuarta parte de las IES encuestadas indica haber identificado los riesgos en forma completa y más de un 10%, haber realizado además, una evaluación de esos riesgos.

Subdominio

ANÁLISIS DE IMPACTO EN LA INSTITUCIÓN

Gráfico 17: Análisis de impacto sobre activos que soportan servicios críticos



- No se realiza
- Análisis básico sobre algunos activos que soportan servicios críticos, estimando tiempo de recuperación
- Análisis esporádico sobre activos que soportan servicios críticos, estimando tiempo de recuperación, recursos y otros aspectos
- Análisis integral, anual y ad-hoc, sobre activos que soportan servicios críticos, bajo un enfoque de mejora continua

Por último, se analiza con mayor detalle la pregunta relativa a la determinación del impacto sobre la continuidad de los activos que soportan los servicios críticos en la IES. Aquí encontramos que **una cantidad muy baja (6,9%) realiza un análisis de impacto sobre la institución,** de manera anual o siempre que las circunstancias lo requieran, con una estimación integral de ventanas de recuperación, recursos requeridos y otros aspectos que hacen a un proceso de mejora contínua.

En el caso antes mencionado y para aquellas IES que realizan este tipo de análisis pero en forma esporádica (24,8%), las entidades muestran un nivel de madurez intermedio de L2, es decir, prácticas documentadas y una adecuada asignación de recursos. Sin embargo, más del 50% realiza algún tipo de análisis de impacto pero de manera parcial o directamente, no avanza para nada en este sentido. Esta situación es realmente preocupante, considerando el efecto que un evento de relevancia (por ejemplo, una falla masiva o un ataque de ransomware) podría ocasionar para la actividad de la IES.

En último término, analizando en forma global las respuestas a las 5 preguntas que integran este Dominio, todas se encuentran en en nivel básico L1, destacándose que en la primera de las preguntas relativa a la realización de un inventario de activos, el mayor valor alcanzado (1,49) se encuentra justo en el límite con L2. En sentido inverso, la pregunta referida al análisis de impacto obtiene un valor de 1,10, siendo el más bajo de las preguntas que componen este dominio.

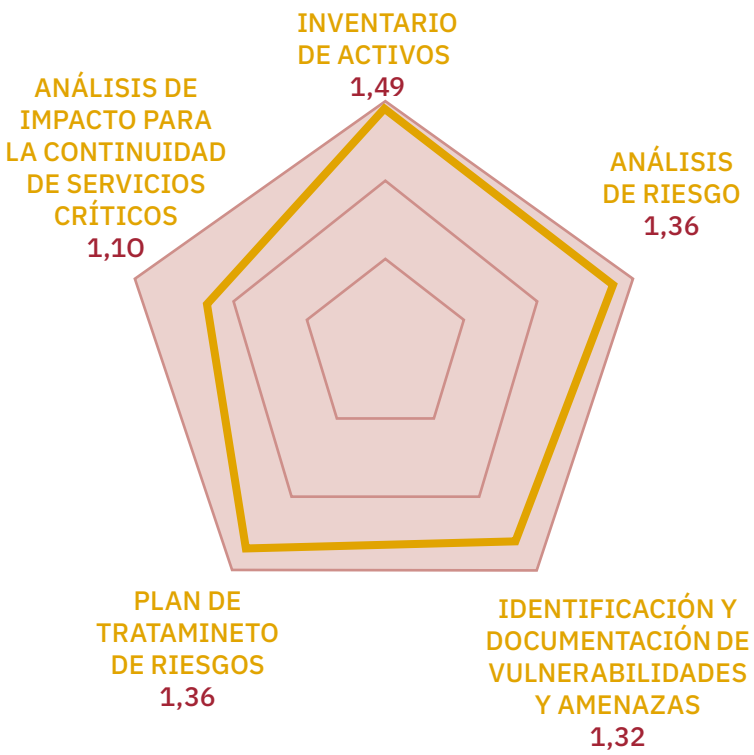
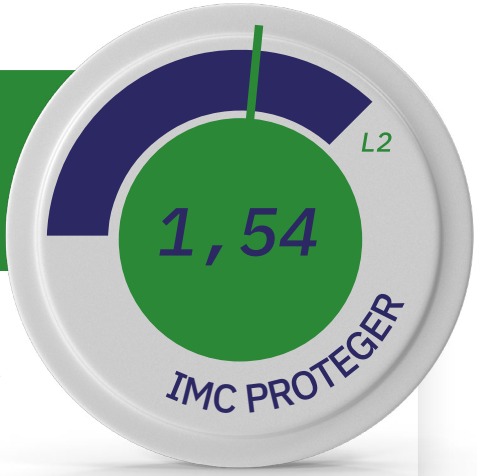


Gráfico 18: Componentes del dominio Identificar

Proteger.



Como ya se mencionó más arriba, el dominio PROTEGER (PR) es, de los 5 dominios que componen este estudio, el que cuenta con el mayor nivel de madurez, con un valor de 1,54. Se encuentra ubicado por encima del IMC Global (1,37). Esto lo coloca en el nivel de madurez intermedio L2, siendo el único que se ubica en este nivel, evidenciando que las prácticas se encuentran documentadas y se asignan los recursos necesarios para la protección de los activos de información en las IES.

Se observa, en consiguiente, que **la implementación de controles para asegurar los activos de información se encuentra en un lugar prioritario en este tipo de instituciones,** especialmente frente a otras facetas de la ciberseguridad consideradas en el modelo IMC.

La protección de las instalaciones y la infraestructura alcanza un nivel avanzado L3, con prácticas guiadas por políticas específicas, asignación de responsabilidades y de autoridad, instancias de rendición de cuentas y de generación de habilidades para quienes realizan las tareas, y evaluación y seguimiento de las actividades.

Por otro lado, varios subdominios alcanzan el nivel intermedio L2, con prácticas documentadas y una adecuada asignación de recursos para el objetivo definido. Son los relativos a la protección de las comunicaciones (2,10), la protección de aplicaciones y servicios informáticos (1,63), la protección de la información (1,69) y la correspondiente a los recursos externos (1,69). El resto de los subdominios se mantiene en un nivel básico L1, es decir con prácticas ad-hoc o informales.

Subdominios de Proteger y su correspondiente nivel

SUBDOMINIO	IMC
Accesos	*L1 (1,49)*
Personal	*L1 (1,36)*
Infraestructura	*L2 (1,10)*
Equipos	*L1 (1,49)*
Comunicaciones	*L2 (1,36)*
Aplicaciones y servicios	*L2 (1,10)*
Información	*L2 (1,69)*
Continuidad	*L1 (1,49)*
Externos	*L2 (1,36)*

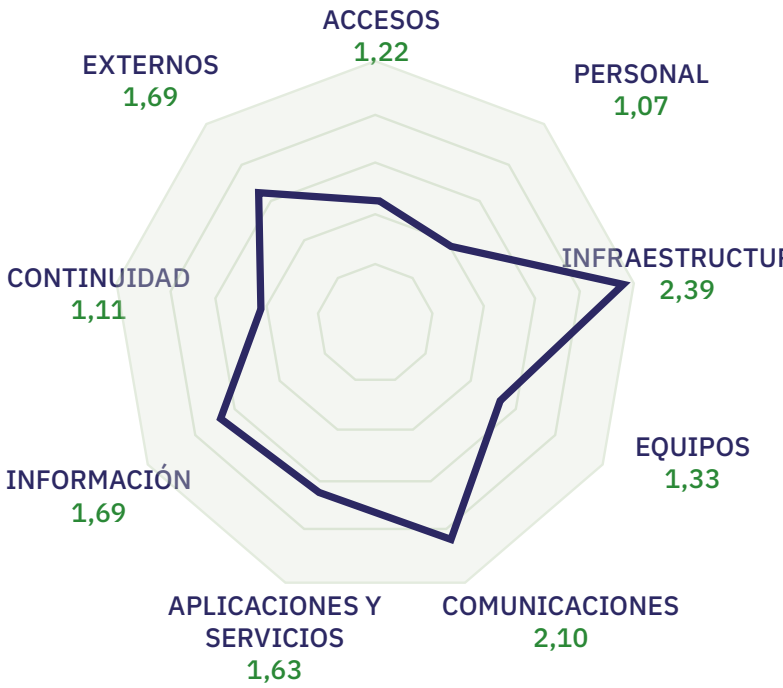


Gráfico 19: Subdominios de Proteger y su correspondiente nivel

Subdominio

GESTIÓN DEL PERSONAL

Profundizando en uno de los aspectos relevados en este dominio relativo al rol central para la ciberseguridad del recurso humano, se plantean en el modelo tres preguntas relativas a la concientización del cuerpo docente, personal no docente y plantel estudiantil.

En el caso de los docentes, más del 50% de las IES manifiestan realizar solo actividades aisladas y casi un 25 % indica que existe algún tipo de concientización anual. En el menor nivel de compromiso con esta temática, cerca de un 20% indica no tener implementado ningún tipo de proceso de concientización. Solo en el segundo caso (procesos anuales de formación) se alcanzó un nivel de madurez intermedio L2, con documentación de prácticas y asignación de recursos.

Tabla 2: Proceso de Concientización de los Docentes

	%	IMC
Existen procesos medibles y repetibles que involucran a todo el estamento	*7 ,3*	*L2 (1,89)*
Existe, es conocido y se realiza anualmente	*16,7*	*L2 (1,70)*
Existen actividades aisladas	*57,7*	*L1 (1,37)*
No existen	*18,2*	*L1 (0,84)*

Tabla 3: Proceso de Concientización del personal No Docente

	%	IMC
Existen procesos medibles y repetibles que involucran a todo el estamento	21,1	L2(1,93)
Existe, es conocido y se realiza anualmente	7,3	L2 (1,71)
Existen actividades aisladas	53,3	L1 (1,28)
No existen	14,3	L1 (0,73)

Tabla 4: Proceso de Concientización de los Estudiantes

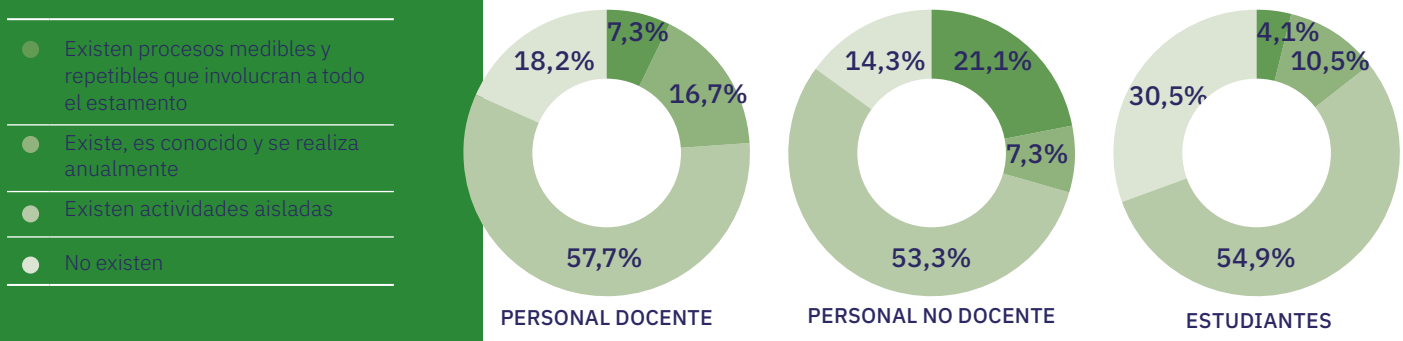
	%	IMC
Existen procesos medibles y repetibles que involucran a todo el estamento	4,1	L2(1,94)
Existe, es conocido y se realiza anualmente	10,5	L2 (1,82)
Existen actividades aisladas	54,9	L1 (1,39)
No existen	30,5	L1 (1,08)

En cuanto a la concientización del personal no docente, se observa un comportamiento similar al del cuerpo de profesores, pero con un mayor porcentaje de procesos medibles y repetibles (21,1%) frente a sólo un 7% en el caso de docentes.

Finalmente, la concientización en ciberseguridad dirigida a estudiantes muestra también un comportamiento similar a los anteriores, aunque con un porcentaje superior en el grupo de IES que indica que directamente no cuenta con procesos de concientización para este grupo (30,5%).

Comparando los tres grupos a quienes se dirige la concientización en ciberseguridad, encontramos que **los procesos medibles y repetibles tienen mayor presencia entre el personal no docente,** es decir el personal que lleva adelante las tareas administrativas y corporativas de las IES, mientras que en el caso de los estudiantes, la incidencia de este grupo es la menor. Entre estos últimos, se manifiesta con fuerza la inexistencia de procesos de concientización (30,5%), o sea que **1 de cada 3 alumnos no recibe ningún tipo de capacitación** en ciberseguridad, tomando las IES en su conjunto.

Gráfico 20: Proceso de Concientización de los Docentes, No Docentes y Estudiantes



Subdominio

CONTROL DE ACCESOS

Otra de las preguntas indaga sobre la gestión de identidades y accesos, y la utilización de soluciones de IAM. En este caso, **sólo un 4,9% de las IES cuenta con una gestión de identidades completamente integrada a las operaciones de la institución implementada con soluciones avanzadas de IAM,** mientras que un 35,4% si bien lo hace en forma estandarizada y de acuerdo a las políticas, aún tienen que mejorar su integración en los sistemas y su automatización; un 45% solo cuenta con políticas básicas para la gestión de identidades mostrando un estadío inicial en este aspecto; y el 4,6% no cuenta con un proceso formal para la gestión de identidades.

Solo en el primer caso (gestión de identidades completamente integrada) se alcanzó un nivel de madurez intermedio L2, con documentación de prácticas y asignación de recursos.

Tabla 5: Gestión de identidades

	%	IMC
La gestión de identidades se encuentra completamente integrada con las operaciones de la institución, utilizando soluciones avanzadas de IAM para una gestión eficiente y segura de identidades y accesos. Se realizan revisiones periódicas y mejoras continuas del proceso basadas en la evaluación del riesgo, auditorías, etc.	*4,9*	*L2 (2,04)*
La gestión de identidades se realiza de acuerdo con políticas bien definidas y estandarizadas en toda la institución. Se utilizan soluciones de gestión de identidades y accesos (IAM) para automatizar el proceso, aunque aún hay margen de mejora en la integración de sistemas y la automatización	*35,4*	*L1 (1,71)*
Existen políticas básicas para la gestión de identidades y se ha comenzado a estandarizar la creación y gestión de cuentas y accesos, pero la implementación es inconsistente y no abarca a toda la organización	*45,1*	*L1 (1,23)*
No existe un proceso formal de gestión de identidades. Las cuentas y los accesos se crean y gestionan de manera individual sin políticas o procedimientos estandarizados	*14,6*	*L1 (0,75)*

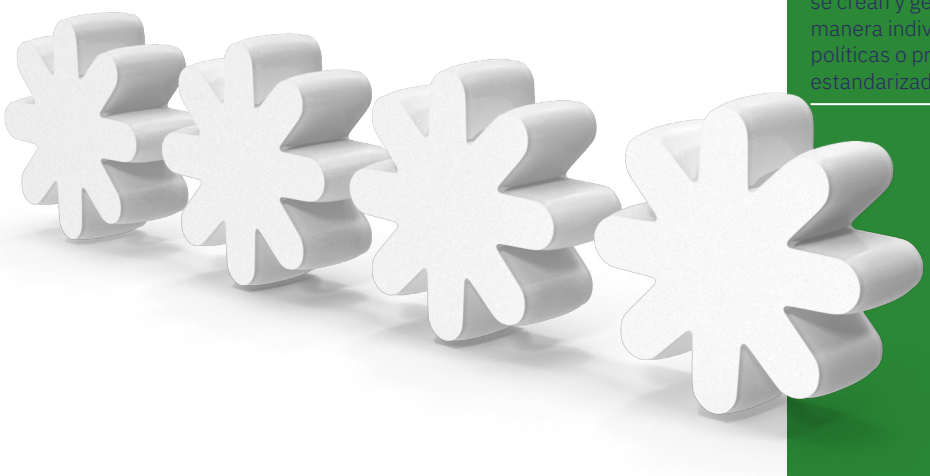


Tabla 6: Aplicación de medidas de seguridad en aplicaciones y servicios críticos

	%	IMC
Se implementan medidas suficientes en todas las aplicaciones y servicios críticos, en base al plan de mitigación de riesgos	25,6	L2 (1,82)
Solo en algunas aplicaciones y servicios críticos se aplican medidas suficientes, en base al plan de mitigación de riesgos	30,1	L2 (1,57)
Se aplican medidas parciales sólo para algunas aplicaciones y/o servicios críticos	38,6	L1 (1,02)
No se aplican	5,7	L0 (0,60)

Subdominio

PROTECCIÓN DE APLICACIONES Y SERVICIOS INFORMÁTICOS

En cuanto a la implementación de medidas de seguridad adecuadas y acordes al tipo de datos objeto de tratamiento y al entorno en el que se ejecutan en las aplicaciones, se observa que casi un 40% de las IES aplica medidas parciales y sólo para algunas aplicaciones y servicios críticos. Le sigue casi una tercera parte que aplica medidas suficientes para mitigar riesgos, pero solo en algunas aplicaciones y servicios críticos.

Por otro lado, solo un 25% de las IES, con un nivel de madurez de L2, indica que se implementan medidas suficientes en todas las aplicaciones y servicios críticos en base a un plan de mitigación de riesgos. En el otro extremo, un 5,7% menciona que no implementa ningún tipo de control. En este último caso, el nivel alcanzado inicial es de L0 (0,60), poniendo de manifiesto la inexistencia de prácticas relativas a la implementación de medidas de seguridad en aplicaciones y servicios críticos. Es uno de los valores más bajos obtenidos para una respuesta a las preguntas que incluye este estudio.

Tabla 7: Protección de datos personales

	%	IMC
Existe una política de protección de datos y la política de seguridad hace referencia a ella	52,4	L2 (1,60)
No existe una política de protección de datos, pero la política de seguridad menciona los aspectos más relevantes relativos a la protección de datos personales	18,7	L2 (1,66)
No existe una política de protección de datos, pero la política de seguridad hace cierta referencia a ella	15	L1 (0,99)
No existe una política de protección de datos ni se la referencia en la política de seguridad de la información	13,8	L1 (0,81)

Subdominio

PROTECCIÓN DE LA INFORMACIÓN

Una de las preguntas de este Dominio se orienta a determinar si se realizan análisis de vulnerabilidades en los sistemas de la institución. Al respecto, las IES participantes indican que un 40% dispone de soluciones de vigilancia para determinar la superficie de exposición en relación a las vulnerabilidades y deficiencias en la configuración, alcanzando las que respondieron en este sentido un nivel de madurez intermedio L2. Sin embargo, más de la mitad manifiesta contar con soluciones de esta naturaleza y realizar solo algunos análisis (un 44,7%) o directamente ningún tipo de acciones en este sentido (14,2%). Cabe mencionar que en este último caso, el nivel de madurez, como era esperable, fue inicial L0, indicando lo que surge de la opción de respuesta, es decir, que no se cuenta con prácticas al respecto.

Subdominio

PROTECCIÓN DE COMUNICACIONES

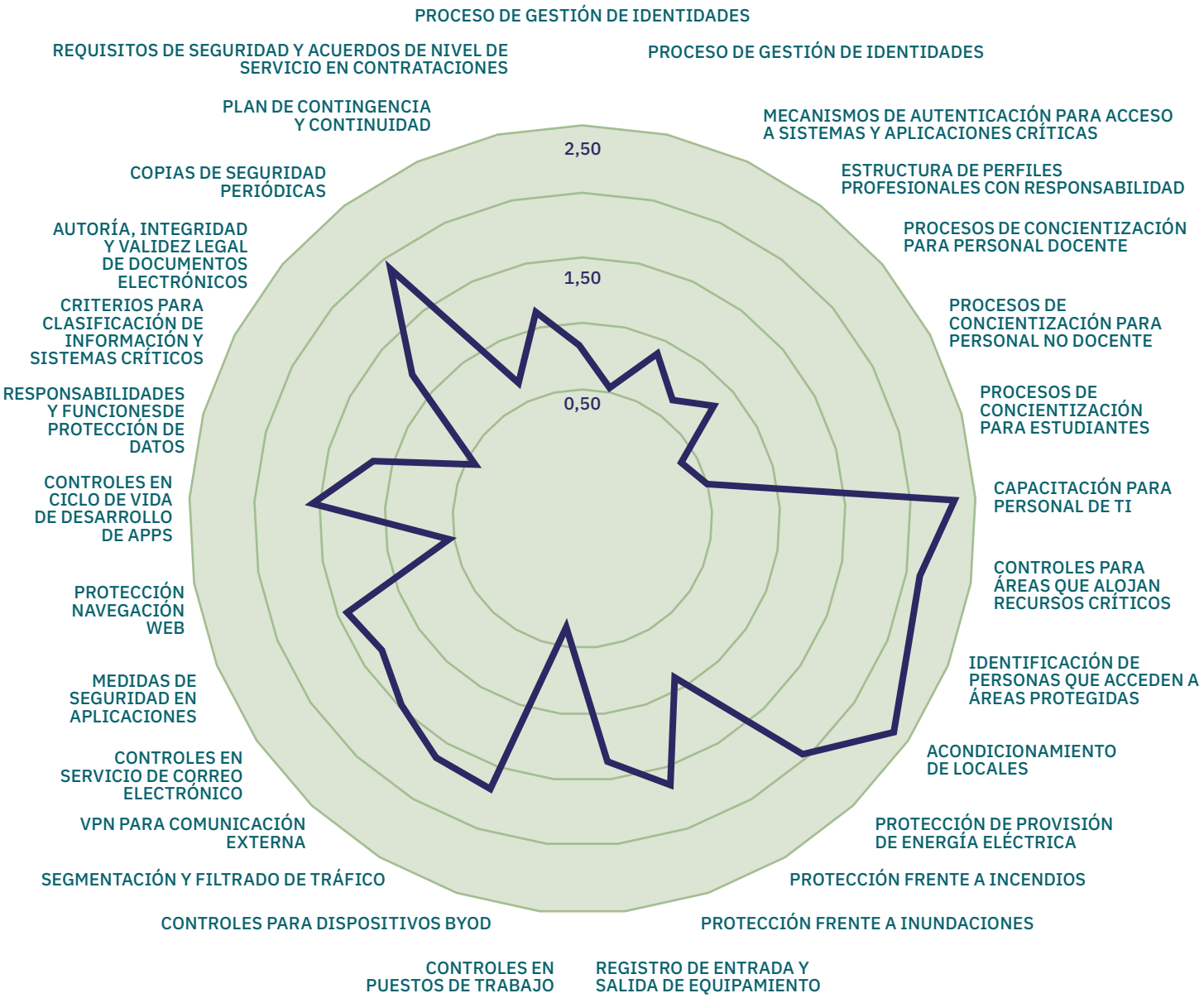
Además, como parte del IMC 2024, se incluye una pregunta en la que se invita a las IES a indicar si se implementan redes privadas virtuales (VPN) cuando la comunicación tiene lugar a través de redes que se encuentran fuera del propio dominio de seguridad. En este sentido, casi un 70% indica que siempre se implementan VPNs cuando se accede desde fuera del dominio o bien, que se realiza en función de cada caso en particular. Esto último lleva a suponer que se revisa la criticidad de los activos de información involucrados. Un 25% informa que se implementan VPNs solo para algunas redes o servicios y un 7%, con un nivel de madurez básico que apenas alcanza a L1, no implementa VPNs. El tránsito por la pandemia global de COVID-19, con la expansión del trabajo remoto que aparentemente llegó para quedarse, puede haber servido como disparador de la atención de este tipo de problemáticas. Sin embargo, por lo que se observa, ello no ha ocurrido en todos los casos.

Tabla 8: Implementación de VPNs

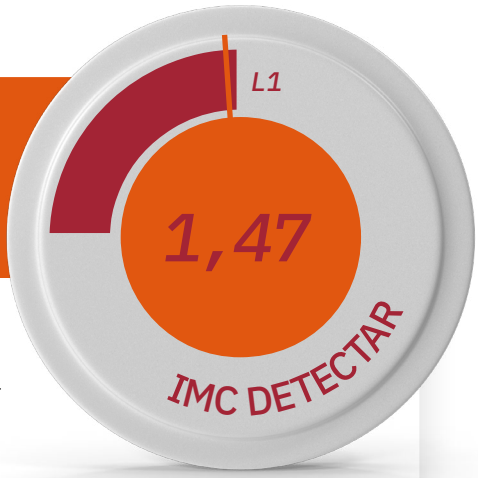
	%	IMC
Se implementan VPN para todo acceso desde fuera del dominio de seguridad de la universidad	45,9	L2 (1,58)
Se implementan VPNs como resultado de analizar cada caso en particular	22	L1 (1,41)
Se implementan VPNs sólo para el acceso a algunas redes y/o servicios	25,2	L1 (1,09)
No se implementan VPNs	6,9	L1 (0,80)

Finalmente, considerando los 29 ítems que componen este dominio, encontramos que varios alcanzan un nivel de madurez avanzado L3, siendo estos los relativos a copias de respaldo y los relacionados con la protección física de las instalaciones. Las cuestiones vinculadas a la protección de los puestos de trabajo, incluyendo notebooks y celulares, transmisión segura de información a través de VPNs y otras medidas de seguridad física, alcanzan un nivel de madurez intermedio L2, correspondiendo a prácticas debidamente documentadas y una adecuada asignación de recursos. Quedan con un nivel de madurez básico L1, denotando prácticas ad-hoc los procesos de concientización, la protección de dispositivos del tipo BYOD y la gestión de identidades. Podría afirmarse que estos últimos son mecanismos de protección cuya relevancia surgió en forma más reciente por ser problemáticas más actuales, mientras que los que ya alcanzan un mayor nivel de madurez, son los que vienen siendo implementados hace tiempo.

Gráfico 21: Nivel de madurez de todos los componentes del dominio Proteger



Detectar.



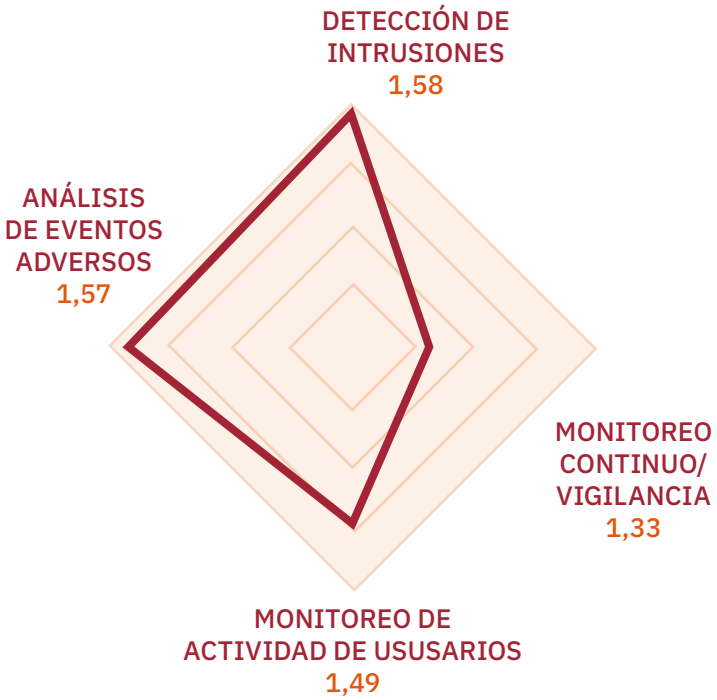
El Dominio DETECTAR (DE) muestra un valor promedio de madurez de 1,47, correspondiente a un nivel básico L1, ubicándose casi en la frontera con la cota inferior de L2 (nivel intermedio). Esto pone de manifiesto prácticas iniciales, mayormente informales y ad-hoc, con un grado de evolución que con algunas mejoras, podría evolucionar a un segundo nivel de madurez, caracterizado a los fines del presente estudio, por el uso de prácticas documentadas y una asignación apropiada de recursos.

De los 5 dominios contemplados, es el segundo en nivel de madurez, detrás del Dominio Proteger, y se encuentra algunas décimas por encima de IMC global (1,37).

Es posible inferir entonces, que las IES establecen acciones para identificar y analizar de manera oportuna, posibles ataques y compromisos a su ciberseguridad, aunque como se mencionó, estas prácticas son consideradas iniciales o incipientes aún, de acuerdo al nivel de madurez alcanzado. Entre otras cosas, se considera en este dominio el monitoreo de red a través de fuentes de información internas o externas, la configuración de herramientas para dicho objetivo y el análisis de eventos de ciberseguridad.

Se dedican esfuerzos a la identificación de eventos adversos e intrusiones pero las tareas de monitoreo que podrían insumir más tiempo y recursos, aún no reciben suficiente atención.

Profundizando en los aspectos que componen este dominio, encontramos que la detección de intrusiones (1,58) y el análisis de eventos adversos (1,57) alcanzan un nivel de madurez intermedio L2; mientras que las labores de monitoreo sobre la infraestructura (1,33) y de los usuarios (1,49), por su parte, solo alcanzan un nivel de madurez básico L1, aunque con valores elevados dentro del rango numérico comprendido en este nivel.



Subdominios de Detectar y su correspondiente nivel

SUBDOMINIO	IMC
Intrusiones	*L2 (1,58)*
Vigilancia	*L1 (1,33)*
Actividad usuarios	*L1 (1,49)*
Anomalías	*L2 (1,57)*

Gráfico 22: Subdominios de Detectar y su correspondiente nivel

Tabla 9: Soluciones de vigilancia

	%	IMC
Se realizan análisis periódicos mediante soluciones de vigilancia para determinar la superficie de exposición en relación a vulnerabilidades y deficiencias de configuración y se realiza un seguimiento de la corrección de dichas vulnerabilidades	*22,4*	*L2 (1,86)*
Se realizan análisis periódicos mediante soluciones de vigilancia para determinar la superficie de exposición en relación a vulnerabilidades y deficiencias de configuración	*18,3*	*L2 (1,63)*
Se realizan algunos análisis pero no se cuenta con soluciones de vigilancia para determinar la superficie de exposición en relación a vulnerabilidades y deficiencias de configuración	*44,7*	*L1 (1,21)*
No se realiza ningún análisis	*14,2*	*L0 (0,74)*

Subdominio

DETECCIÓN DE INTRUSIONES

Una de las preguntas de este Dominio se orienta a determinar si se realizan análisis de vulnerabilidades en los sistemas de la institución. Al respecto, las IES participantes indican que un 40% dispone de soluciones de vigilancia para determinar la superficie de exposición en relación a las vulnerabilidades y deficiencias en la configuración, alcanzando las que respondieron en este sentido un nivel de madurez intermedio L2. Sin embargo, más de la mitad manifiesta contar con soluciones de esta naturaleza y realizar solo algunos análisis (un 44,7%) o directamente ningún tipo de acciones en este sentido (14,2%). Cabe mencionar que en este último caso, el nivel de madurez, como era esperable, fue inicial L0, indicando lo que surge de la opción de respuesta, es decir, que no se cuenta con prácticas al respecto.

Subdominio

MONITOREO DE ACTIVIDAD DE LOS USUARIOS

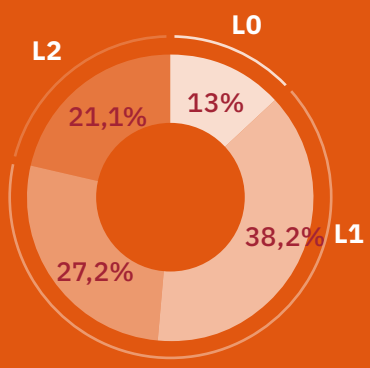
Relacionado con la pregunta anterior, al preguntar sobre el monitoreo y análisis de la actividad de los usuarios en los sistemas y redes para identificar eventos de ciberseguridad, se encontró que algo más del 20 % monitorea y analiza el proceder de los usuarios mediante herramientas automatizadas y en base a patrones predefinidos, alcanzando un nivel de madurez intermedio de L2.

El resto se reparte entre aquellas que lo hacen en forma reactiva (38,2%) o ad-hoc (27,2%) o directamente, no realizan ningún tipo de actividad de esta naturaleza (13%). Cabe acotar que en este último caso, el nivel de madurez es inicial L0, denotando la ausencia total de prácticas.

Tabla 10: Monitoreo de actividades de los usuarios

	%	IMC
Se realiza utilizando herrameintas automatizadas según patrones predefinidos	21,1	L2 (2,02)
Se realiza de manera ad hoc y manualmente	27,2	L1 (1,53)
Se realiza de manera reactiva	38,2	L1 (1,13)
No se realiza	13	L2 (0,67)

Gráfico 23: Monitoreo y análilsis de la actividad de los usuarios



Subdominio

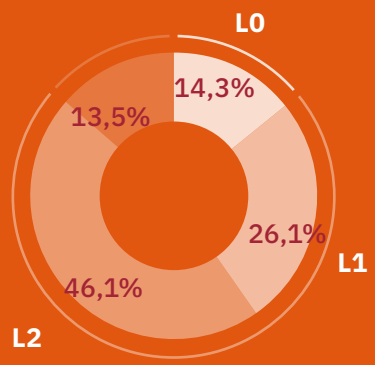
ANÁLISIS DE EVENTOS ADVERSOS

En cuanto a la pregunta sobre análisis de alertas y eventos anómalos detectados por fuentes de información interna o externa, un 45,93% indica que se realiza únicamente en forma ad-hoc y que en función de la anomalía, se establecen las acciones a seguir. Del resto, un 40% realiza algún tipo de análisis periódico, procediendo luego en consecuencia, y de estas, una fracción equivalente al 14.2% también realiza a partir de estas acciones, un proceso de mejora contínua.Cabe acotar que en este último caso, el nivel de madurez alcanzado por las IES que respondieron la pregunta con esta opción de respuesta, es de L2 (intermedio), o sea mostrando prácticas documentadas y suficientes recursos asignados. Para terminar, el 13,4% de las IES no lleva a cabo ningún tipo de análisis sobre las alertas y eventos anómalos detectados, tanto de fuente de información interna como externa.

Tabla 11:
Análisis de alertas y eventos anómalos

	%	IMC
Se hacen análisis periódicamente, se toman acciones en consecuencia y se evalúa y mejora el proceso en forma contínua	*14,3*	*L2 (2,13)*
Se hacen análisis periódicamente y se toman acciones en consecuencia	*26,1*	*L1 (1,67)*
Solo se hacen ad hoc o eventualmente y se toman acciones en consecuencia	*46,1*	*L1 (1,15)*
No se llevan a cabo	*13,5*	*L2 (0,73)*

Gráfico 24:
Análisis de alertas y eventos anómalos



- No se llevan a cabo
- Solo se hacen ad hoc o eventualmente y se toman acciones en consecuencia
- Se hacen análisis periódicamente y se toman acciones en consecuencia
- Se hacen análisis periódicamente, se toman acciones en consecuencia y se evalúa y mejora el proceso en forma contínua

Por último, se presentan a continuación, las 5 preguntas incluídas en este dominio. Cabe acotar que llamativamente, la pregunta que mostró un menor nivel de madurez en el promedio de las respuestas, con un valor cercano a 1, fue la relativa a la disponibilidad de sistemas automáticos de recolección de eventos de seguridad, conocidos como SIEM (Sistema gestión de eventos e información de seguridad). Este tipo de sistemas requieren en general una importante inversión y un alto grado de preparación para su configuración y explotación.

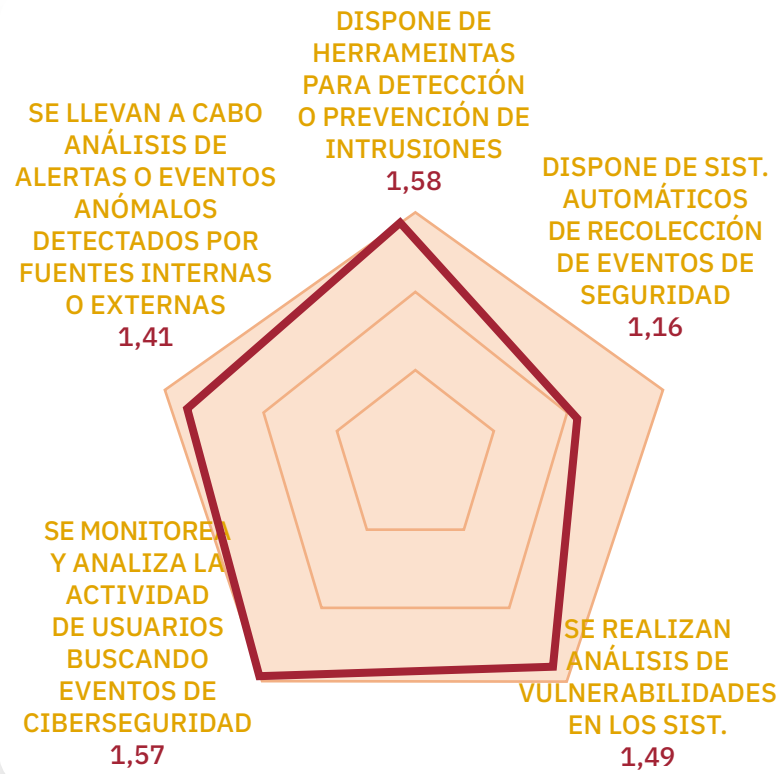


Gráfico 25: Componentes del dominio Detectar

Responder y recuperar.

Para el Dominio RESPONDER Y RECUPERAR (REyRC), el nivel promedio obtenido es de 1,10, correspondiente al nivel básico L1 en la escala de madurez. Esto sugiere que en el caso de las prácticas comprendidas en este dominio, su desarrollo es ad-hoc o informal, reflejado en políticas y procedimientos básicos, en un estadío inicial para la implementación de tecnologías de seguridad, personal no especializado al que se le han asignado funciones de ciberseguridad, y un incipiente desarrollo de los procesos de identificación y evaluación de riesgos.

Por su valor, ocupa el lugar más bajo de los dominios incluídos en el estudio, lógicamente por debajo del valor de IMC global (1,37).

Analizando cada uno de los 3 subdominios que conforman este dominio, que comprende la gestión de incidentes, su mitigación y recuperación posterior, se observa que todos ellos caen en un nivel de madurez básico L1.

Subdominios de Proteger y su correspondiente nivel

SUBDOMINIO	IMC
Gestión de incidentes	*L1 (1,16)*
Mitigación de incidentes	*L1 (1,10)*
Recuperación	*L1 (0,96)*

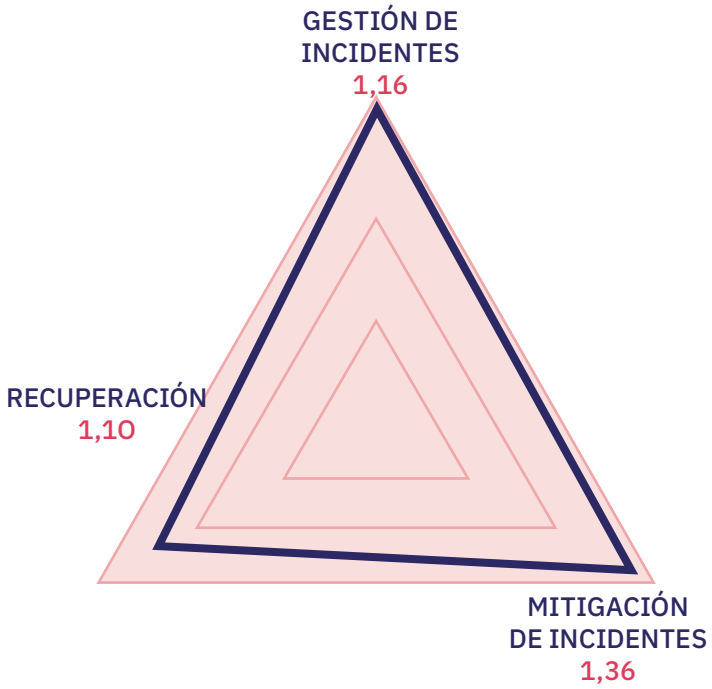


Gráfico 26: Subdominios de Detectar y su correspondiente nivel

Subdominio

GESTIÓN DE INCIDENTES

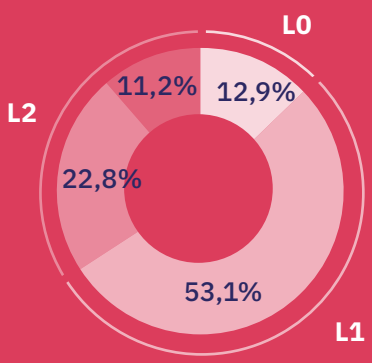
En lo que refiere a la gestión de incidentes, es relevante saber si la institución cuenta con procedimientos para llevarla a cabo. Se observa que más de la mitad de las IES los ha desarrollado (53,1%), pero con características informales, posiblemente no documentados ni comunicados apropiadamente a la comunidad alcanzada. En estos casos, el nivel de madurez alcanzado es básico L1, lo que implica que las prácticas son básicas, de características ad-hoc.

Por otro lado, aproximadamente un tercio de los encuestados cuenta con procedimientos integrales, que describen las etapas de detección, respuesta y mitigación. Para estas respuestas, el nivel de madurez alcanzado fue intermedio de L2, evidenciando procedimientos documentados y una adecuada asignación de recursos. De estos, una tercera parte a su vez, dispone también de una taxonomía (11,2% de todos los participantes en el estudio) y en base a ella, determina qué incidentes se van a tratar. Finalmente, y con un nivel inicial L0, un 12,9% indicó no contar con procedimientos para la gestión de incidentes de seguridad.

Tabla 12: Procedimientos de Gestión de incidentes de ciberseguridad

	%	*IMC*
Se cuenta con procedimientos formales que cumplen con los estándares e incluyen las etapas de detección, respuesta y mitigación, y además se han definido qué incidentes se gestionan (taxonomía)	*11,2*	*L2 (2,03)*
Se cuenta con procedimientos formales que cumplen con los estándares e incluyen las etapas de detección, respuesta y mitigación	*22,8*	*L2 (1,83)*
Se cuenta con procedimientos informales	*53,1*	*L1 (1,29)*
La institución no cuenta con procedimientos	*12,9*	*L0 (0,62)*

Gráfico 27: Procedimientos de Gestión de incidentes de ciberseguridad



- La institución no cuenta con procedimientos
- Se cuenta con procedimientos informales
- Se cuenta con procedimientos formales que cumplen con los estándares e incluyen las etapas de detección, respuesta y mitigación
- Se cuenta con procedimientos formales que cumplen con los estándares e incluyen las etapas de detección, respuesta y mitigación, y además se han definido qué incidentes se gestionan (taxonomía)

El panorama que se recrea a partir de las respuestas a esta pregunta parece no ser en primera instancia preocupante, debido a la existencia de un grupo bastante numeroso de IES que cuenta con procedimientos para gestionar informalmente incidentes de seguridad. Sin embargo, hoy en día, este nivel de informalidad puede no resultar suficiente ya que cualquier puesto de trabajo desatendido puede ser el origen de un incidente mayor y la preparación de la organización para afrontar un incidente resulta crucial para su rápida contención y remediación. Efectivamente, un usuario que no conoce cómo proceder frente a la detección de un evento anómalo y dañino para la organización o un equipo de ciberseguridad o TI que debe atender el incidente y no se encuentra preparado para ello, puede dilatar involuntariamente los tiempos de respuesta y contribuir sin proponérselo, con la expansión de la superficie atacada. Por lo tanto, resulta necesario mejorar de manera urgente, las capacidades de respuesta y recuperación frente a incidentes en las IES iberoamericanas, a través de procesos planificados, formalmente definidos y comunicados a todos los involucrados.

Tabla 13: Plan o procedimiento anti ransomware

	%	IMC
Existe un procedimiento aprobado formalmente que define tareas, recursos y responsabilidades asignadas	7,5	L2 (2,22)
Se realizan acciones concretas y se asignan responsabilidades en base a un procedimiento no aprobado formalmente	24,1	L2 (1,87)
Se realizan tareas básicas pero no responden a un procedimiento aprobado ni se asignan responsabilidades	36,9	L1 (1,24)
No se cuenta con procedimientos	31,5	L1 (0,94)

Subdominio

MITIGACIÓN DE INCIDENTES

Los incidentes de ransomware, especialmente a partir de la pandemia de COVID 19, se encuentran a la orden del día, afectando a organizaciones de todo tipo. Dentro de este grupo, también se encuentran las IES, por lo que resulta de interés saber si estas instituciones cuentan con un plan o con procedimiento anti ransomware.

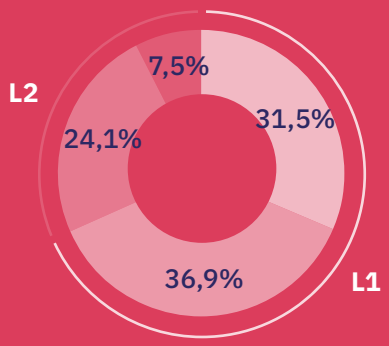
En este caso, se observó que la opción que recibió un número mayor de respuestas(36,9%) es aquella correspondiente a la realización de algunas tareas básicas en relación a los incidentes de ransomware, que no responden a un procedimiento aprobado ni a una asignación prevista de responsabilidades. En

este grupo, se alcanza un nivel de madurez básico equivalente a L1. Con un valor similar, aunque un poco menor (31,5%), las IES encuestadas indican que no cuentan con un programa para minimizar el impacto del ransomware.

Desafortunadamente, solo una fracción muy menor (7,5%) indica que existe un procedimiento formal que define las tareas, recursos y responsabilidades asignadas y un 24,1% señala que se realizan acciones concretas pero en base a un procedimiento no aprobado formalmente. En estos dos últimos casos, el nivel de madurez fue de L2, o sea intermedio, correspondiente a prácticas documentadas y una adecuada asignación de recursos.

Frente a los efectos devastadores del ransomware sobre la operación de las entidades afectadas y los problemas éticos y legales implicados en cualquier pago de rescate, las IES iberoamericanas deberían trabajar hacia la definición de un programa anti malware, debidamente formalizado y comunicado a todo el personal. que incorpore todas las medidas que aseguren una rápida recuperación.

Gráfico 28: Plan o procedimiento anti ransomware



Subdominio

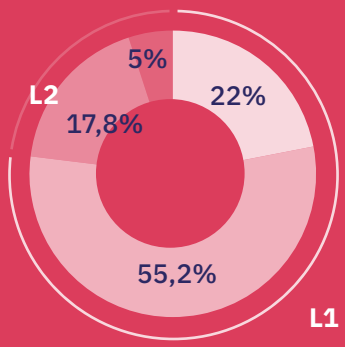
RECUPERACIÓN

Finalmente, se indagó si respecto a la recuperación frente a incidentes, las IES cuentan con un plan. Al respecto, solo un 5% señala que dispone de un proceso definido y aprobado, de un plan de simulaciones y de un programa de mejora contínua en este aspecto. Un 17,8% indica que cuenta con procedimientos definidos pero que solo realiza simulaciones esporádicas. En estos dos grupos de respondentes, el nivel de madurez alcanzado es intermedio de L2, es decir, instituciones que han documentado sus prácticas y asignado recursos de manera oportuna. Una mayoría, representada por un 55,2% indica que existen procedimientos aislados, coincidiendo con un valor muy similar (53,1%) obtenido en la opción de respuesta a la pregunta sobre

Tabla 14: Plan de recuperación ante incidentes

	%	IMC
Existen procedimientos definidos y aprobados, plan de simulaciones y un programa de mejora continua	5	L2 (2,21)
Existen procedimeintos definidos y se realizan simulaciones esporádicas	17,8	L2 (1,84)
Existen algunos procedimientos aislados	55,2	L1 (1,38)
No se ha definido formalmente un plan	22	L1 (0,78)

Gráfico 29: Plan de recuperación ante incidentes



- No se ha definido un plan
- Existen procedimientos aislados
- Existen procedimeintos definidos y se realizan simulaciones esporádicas
- Existen procedimientos definidos y aprobados, plan de simulaciones y un programa de mejora continua

los incidentes de seguridad, que indica que son informales, como se mencionó más arriba. Por último, un 22%, señala que no se ha definido formalmente un plan, con un nivel de madurez también de L1 (básico), como en la opción de respuesta anterior.

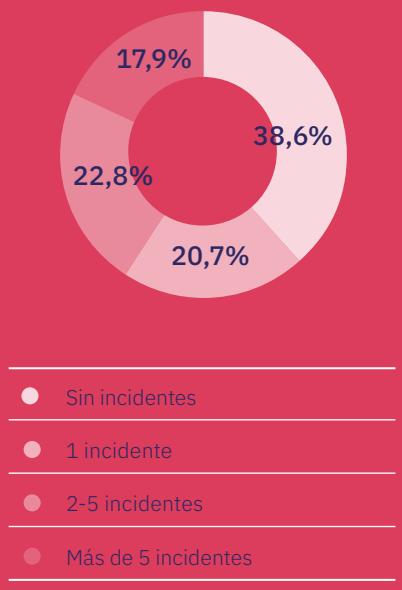
Lo anterior pone de manifiesto un estadío muy incipiente de implementación de medidas de seguridad y programas muy limitados de gestión de incidentes de seguridad.

Además, se preguntó sobre el número de incidentes de seguridad que habían afectado a la operación parcial o totalmente en el último año (aclarando que estos valores no inciden en el nivel de madurez), para determinar si existen consecuencias concretas derivadas del nivel de preparación de las IES, mostrado en otras preguntas de la encuesta.

Puede observarse que casi un 40% indica no haber sufrido n incidente de seguridad durante el último año, mientras un 20,7% y un 22,8% señala haber sido afectadas por 1 o 2 a 5 incidentes. Un 17,9% en cambio, señala que tuvo más de 5 incidentes que afectaron la confidencialidad, integridad o disponibilidad de sus activos de información.

Es importante mencionar que la cantidad de incidentes puede parecer baja, pero si se piensa en que 3 veces por ejemplo, en un período de 12 meses, una IES pudo ver su operación (elaboración de actas de notas, inscripción de alumnos, alta y baja de personal docente y no docente, etc.) interrumpida parcial o totalmente, estos valores cobran relevancia. Observar que casi un 18% de los encuestados responde que sufrió más de 5 incidentes y que el 22,8% se vió afectado entre 2 y 5 veces, motiva un grado importante de preocupación.

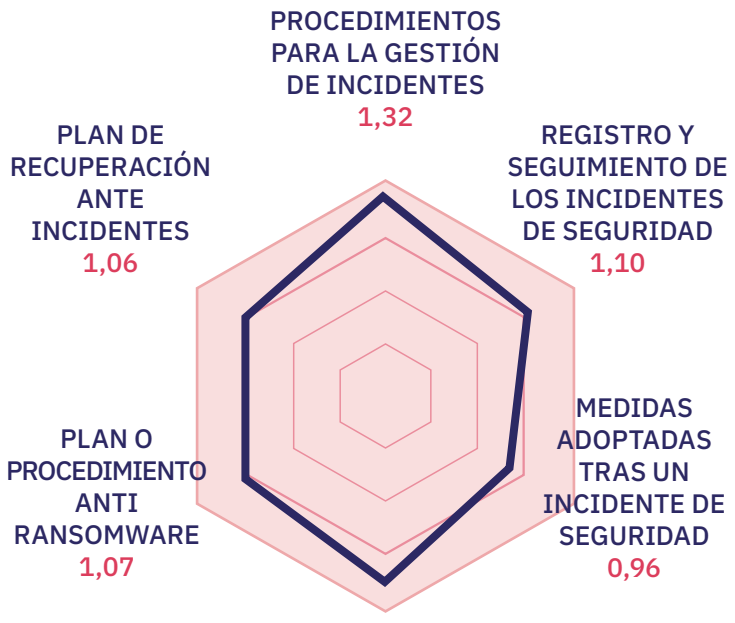
Gráfico 30: Plan o procedimiento anti ransomware



Como resumen para el dominio Responder y Recuperar, (REyRC) cuyo IMC global fue 1,10 (básico L1), puede verse que el valor de todos los ítems es cercano a 1 y se ubica en dicho nivel de madurez (L1).

El valor promedio más bajo fue de 0,96 en la pregunta sobre las medidas de seguridad tomadas sobre los activos afectados por un incidente de seguridad. Por otro lado, las que buscaban determinar si las IES contaban con procedimientos de gestión de incidentes y su comunicación a entidades externas, son las presentan mayor nivel de madurez en del dominio. Por último, los niveles globales menores se dieron en las preguntas relacionadas con acciones concretas ante un incidente como por ejemplo, el registro, la contención y la recuperación.

Gráfico 31: Componentes del dominio Detectar



Formación y talento.

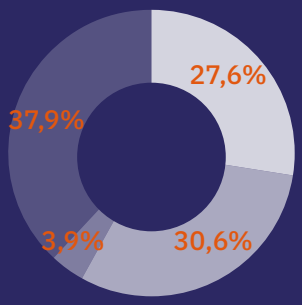
Como se explicó previamente, el dominio Formación y Talento (FT) no fue incorporado en forma directa al cálculo del nivel de madurez IMC 2024. Sin embargo, se incluyeron en el modelo 5 preguntas sobre esta temática, dada la función principal que desarrollan las IES y por su calidad de usuarias intensivas de las tecnologías. Esto último se basa en que estas entidades necesitan contar con un plantel de especialistas en Tecnología y Seguridad.

Con este fin, en este dominio se agregaron preguntas relacionadas con la existencia de carreras y/o planes de formación en ciberseguridad (1 pregunta) y con las estrategias de captación (2 preguntas) y retención (2 preguntas) de talento en ciberseguridad, apuntando a conocer el panorama actual y las dificultades que este tipo de instituciones atraviesa.

Más de la mitad de las universidades participantes (62,1%) aporta a la comunidad profesionales con formación en ciberseguridad. Cabe destacar que se registra, tanto a nivel global como en cada región, falta de profesionales formados en esta disciplina, tanto en la industria, como en el sector público y la academia.

Respecto a la existencia de programas de formación que imparten contenidos relacionados con la ciberseguridad, el 27,6% indica que cuenta con formación a nivel de grado y el 34,5%, formación de postgrado (correspondiendo el 30,6% a Programas de Maestría y el 3,9% a Programas de Doctorado). El 37,9% restante indica que no cuenta con carreras de ninguna naturaleza en este campo.

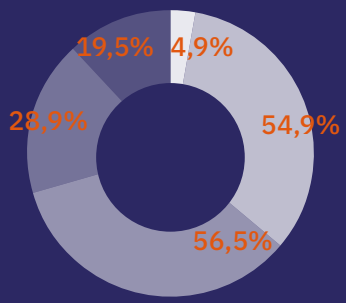
Gráfico 32: Oferta de carreras en ciberseguridad



- Carreras de grado
- Maestrías
- Doctorados
- No posee

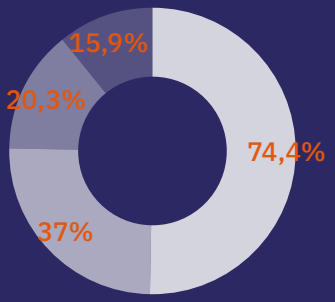
Al momento de determinar las principales razones por las cuales existen dificultades para captar talentos para cubrir perfiles de ciberseguridad, se encontró que el principal motivo son las altas pretensiones económicas (56,5%) de los postulantes, seguido con un valor similar por la escasez de perfiles técnicos especializados (54,9%). Otras razones que se mencionaron fueron la fuerte movilidad de estos perfiles entre organizaciones, es decir, una fuerte rotación. Solo algo menos del 5% señaló no encontrar ninguna dificultad.

Gráfico 33: Dificultades para contratar personal para ciberseguridad



- No he encontrado ninguna dificultad
- Escasez de perfiles técnicos cualificados
- Altas pretensiones económicas
- Alta movilidad de estos perfiles entre diferentes organizaciones
- Otras razones

Gráfico 34: Dificultades para retener talentos

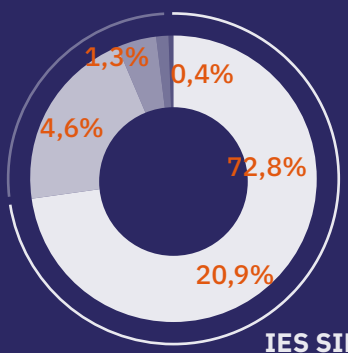


- El nivel salarial
- Las posibilidades de mejora en la carrera profesional
- La flexibilidad horaria y condiciones de trabajo
- El tipo de proyectos y desafíos técnicos

Considerando las dificultades para retener talentos en ciberseguridad, como era de esperarse, unas 2 terceras partes de las IES es el nivel salarial (74,4%), seguido de las posibilidades de crecimiento y mejora salarial (37%), la flexibilidad horario y las condiciones de trabajo (20,3%) y el tipo de proyectos y desafíos técnicos (15,9%).

Las respuestas a estas preguntas ponen de manifiesto las dificultades que tiene la mayoría de las IES para adoptar una postura competitiva a la hora de retener personal, dado los bajos recursos que generalmente se le asignan en comparación con la industria.

Gráfico 35: pporcentaje de perfiles de ciberseguridad desvinculados en el último año



- 0%
- 1-25%
- 26-50%
- 51-75%
- 76-100%

Cabe acotar que en este dominio se incluyó también una pregunta orientada a determinar el porcentaje de perfiles relacionados con la ciberseguridad se han desvinculado de su institución en los últimos 12 meses.

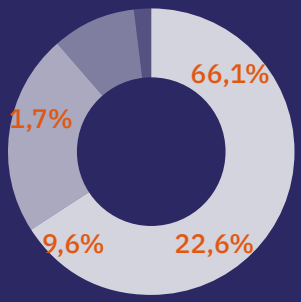
De ello puede observarse que en el 72,8% de las IES no se han desvinculado perfiles relacionados con ciberseguridad en los últimos 12 meses, mientras que el 27,2% restante han experimentado desvinculaciones en el personal responsable de ciberseguridad, aunque no todas ellas en la misma proporción.

Si bien el porcentaje que ha mantenido los recursos humanos que trabajan en ciberseguridad en las IES es relativamente alto, no se debe descuidar que más de una cuarta parte de las IES ha tenido que lidiar con el costo que implica dicha desvinculación (búsqueda de RRHH capacitados, inducción del los nuevos RRHH, conformación de nuevos equipos y roles, entre otros).

Finalmente, una pregunta buscó indagar si se tenía previsto incorporar personal de ciberseguridad en los próximos 12 meses. Las opciones de respuesta eran 4 y se buscaba determinar si no tenían planes de ampliación de la planta de profesionales abocados a la ciberseguridad, si se planeaba incorporar a una persona, entre 1 y 3 personas o más de 3 personas.

Según las respuestas recibidas, se observó que el 66,1% de las IES no planea incorporar personal para ciberseguridad, porcentaje cercano a aquél de las IES que no han experimentado desvinculaciones. El 33,9% de las IES por su parte, planea incorporar al menos 1 persona al equipo de ciberseguridad, porcentaje similar e incluso un poco superior al de aquellas IES donde ha habido desvinculaciones de personas que trabajaban en ciberseguridad. Esto da a pensar que quienes han tenido bajas están pensando en reemplazarlas e incluso en ampliar el equipo de ciberseguridad.

Gráfico 36: Previsión de incorporar personal de ciberseguridad en los próximos 12 meses



- No existen planes de incorporación de personal
- Se incorporará una persona
- Se incorporarán 1-3 personas
- Se incorporarán más de 3 personas

4.3
Enfoques de las IES en torno a la ciberseguridad.

Un análisis multivariado de los datos refleja correlaciones de diversos indicadores del modelo, haciendo que su peso en el IMC calculado tenga una fuerte relación. Los componentes identificados muestran la forma en la que las instituciones abordan la ciberseguridad y se podrían catalogar de la siguiente forma:

Esta información podría indicar una priorización de las IES a la hora de afrontar la ciberseguridad. En concreto, RC1 refleja al grupo de IES donde hay un fuerte comportamiento hacia la planificación de las acciones y la formación y concientización de la comunidad universitaria. RC2 representa el grupo de IES donde la normalización y creación de procedimientos de seguridad juega un papel fundamental para su personal. Por último, se identifica un tercer grupo, RC3, con una componente más técnica y centrado la operación de ciberseguridad en el ámbito de prevención proactiva y la defensa activa.

Estos componentes nos permiten identificar los enfoques de ciberseguridad predominantes en las IES de cada país. En concreto, podemos ver como en todos los países prima la ciberseguridad operativa (RC3), que presenta los valores más altos, con varios países como Chile, Colombia y España dentro del nivel intermedio L2 de madurez y un promedio iberoamericano muy cercano a ese valor (1,94).

A nivel procedimental (RC2), la media iberoamericana se sitúa en un nivel básico L1, con un valor de 1,47, y con todos los países por encima de 1,27, siendo Chile (1,74), Colombia (1,60) y México (1,48) los que tienen una madurez por encima de la media (1,47).

Por último, a nivel de planificación y socialización el promedio se sitúa en 1,17 puntos, con Colombia (1,64), España (1,42) y México (1,23) con valores superiores a ese umbral.

	ARGENTINA	CHILE	COLOMBIA	ECUADOR	ESPAÑA	MÉXICO	PORTUGAL	IBEROAM.
RC1	*L0 (0,71)*	*L1 (1,06)*	*L2 (1,64)*	*L1 (0,98)*	*L1 (1,42)*	*L1 (1,23)*	*L1 (1,10)*	*L1 (1,17)*
RC2	*L1 (1,27)*	*L2 (1,74)*	*L2 (1,60)*	*L1 (1,41)*	*L1 (1,38)*	*L1 (1,48)*	*L1 (1,28)*	*L1 (1,47)*
RC3	*L2 (1,70)*	*L2 (2,21)*	*L2 (2,23)*	*L2 (1,67)*	*L2 (2,17)*	*L2 (1,76)*	*L2 (1,93)*	*L2 (1,94)*

Tabla 15: Componentes global y por país

4.4
IMC Iberoamericano por país.

La primera edición de IMC ha contado con la participación de 10 países/regiones de Iberoamérica

En el cálculo del IMC global se tienen en cuenta todas las IES participantes, independientemente de su país. Sin embargo, para el IMC nacional se realiza una agrupación por país. Para asegurar que el cálculo del IMC nacional sea lo más preciso posible, se requiere que el tamaño muestral obtenido en cada país cumpla con un mínimo y que los datos obtenidos hayan pasado un proceso de revisión general por el/la coordinador/a de MetaRed en el país. Este proceso adicional refuerza el valor de los resultados entregados en este informe, asegurando la reducción de sesgos y la existencia de posibles datos erróneos. Por lo tanto, tras este proceso se ha obtenido el IMC nacional para los siguientes 7 países.

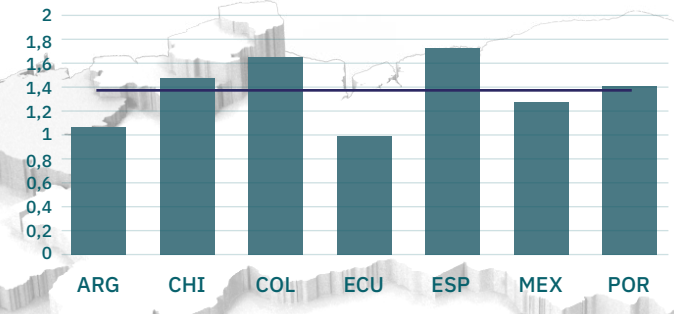


Gráfico 37: Comparativa IMC global y por países

Gráfico 38: IMC por país

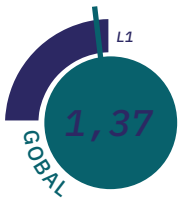
A nivel global, España (1.73), Colombia (1.65), Chile (1.47) y Portugal (1,41) presentan un IMC global mayor, con 36, 28, 10 y 4 puntos, respectivamente, por encima del IMC global. En un segundo grupo encontramos a México (1,28), Argentina (1,06) y Ecuador (0,99) por debajo del umbral del IMC promedio.

Tabla 16: Diferencia entre el IMC global y por países

	ARGENTINA	CHILE	COLOMBIA	ECUADOR	ESPAÑA	MÉXICO	PORTUGAL
IMC NACIONAL	*1,06*	*1,47*	*1,65*	*0,99*	*1,73*	*1,28*	*1,41*
IMC GLOBAL	*1,37*	*1,37*	*1,37*	*1,37*	*1,37*	*1,37*	*1,37*
DIFERENCIA	-0,31	**0,10**	**0,28**	-0,38	**0,36**	-0,09	**0,04**

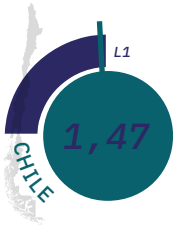
Si desglosamos estos valores por dominio de aplicación y país, Colombia y España superan la media iberoamericana para los cinco dominios principales. Por contraparte, Argentina y Ecuador se sitúan por debajo del promedio en todos los dominios.

Gráfico 39: Diferencia entre el IMC global y por países

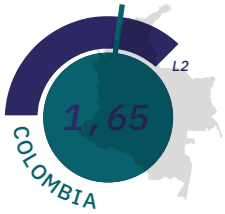


GB	1,43
ID	1,32
PR	1,54
DE	1,47
REyRC	1,10

GB	1,06
ID	1,01
PR	1,32
DE	1,14
REyRC	0,80

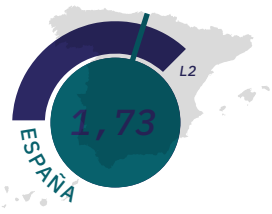


GB	**1,60**
ID	1,28
PR	**1,58**
DE	**1,66**
REyRC	**1,25**

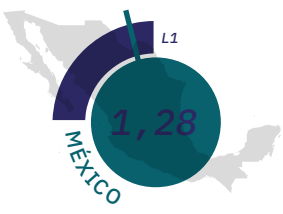


GB	**1,76**
ID	**1,62**
PR	**1,90**
DE	**1,77**
REyRC	**1,19**

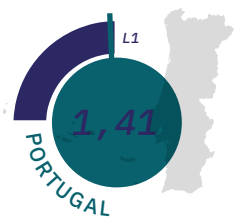
GB	0,93
ID	0,97
PR	1,36
DE	0,94
REyRC	0,74



GB	**1,95**
ID	**1,46**
PR	**1,80**
DE	**1,94**
REyRC	**1,51**



GB	1,29
ID	**1,35**
PR	1,43
DE	1,30
REyRC	1,03



GB	1,30
ID	1,42
PR	**1,59**
DE	**1,70**
REyRC	1,06

El valor del IMC global no es el promedio del IMC por país, sino el valor promedio de todas las IES participantes a nivel global

En cuanto a los dominios, los datos muestran una tendencia común hacia la realización de acciones de protección (1,54) y detección (1,47) como aspectos con mayor nivel de madurez medio. Como excepción, España antepone a esto las acciones de Gobierno, Riesgo y Cumplimiento (GRC) englobadas dentro del dominio Gobernar (GB), donde muestra un nivel de madurez muy cercano a L2 (1,95) y que queda justificado debido a la normativa española de ciberseguridad, definida en el Esquema Nacional de Seguridad regulado por el Real Decreto 311/2022, de obligado cumplimiento para las Administraciones Públicas de este país.

Estos datos sitúan a **Colombia** y **España** a la cabeza de Iberoamérica, con un nivel de madurez intermedio (L2) frente al nivel básico (L1) del resto de países.

Tabla 17: Diferencia entre el IMC global y por país, según cada Dominio

	ARGENTINA	CHILE	COLOMBIA	ECUADOR	ESPAÑA	MÉXICO	PORTUGAL	DIFERENCIA
GB (1,43)	1,06 (-0,37)	**1,60 (+0,17)**	**1,76 (+0,33)**	0,93 (-0,50)	**1,95 (+0,52)**	1,29 (-0,14)	1,30 (-0,13)	-0,12
ID (1,32)	1,01 (-0,31)	1,28 (-0,04)	**1,62 (+0,30)**	0,97 (-0,35)	**1,46 (+0,14)**	**1,35 (+0,03)**	**1,42 (+0,10)**	-0,13
PR (1,54)	1,32 (-0,22)	**1,58 (+0,04)**	**1,90 (+0,36)**	1,36 (-0,18)	**1,80 (+0,26)**	1,43 (-0,11)	**1,59 (+0,05)**	**+0,20**
DE (1,47)	1,14 (-0,33)	**1,66 (+0,19)**	**1,77 (+0,30)**	0,94 (-0,53)	**1,94 (+0,47)**	1,30 (-0,17)	**1,70 (+0,23)**	**+0,16**
REyRC (1,10)	0,80 (-0,30)	**1,25 (+0,15)**	**1,19 (+0,09)**	0,74 (-0,36)	**1,51 (+0,41)**	0,03 (-0,07)	1,06 (-0,04)	**-0,12**

Si analizamos la desviación por dominios a nivel global, observamos que es positiva en el dominio Proteger (PR) (+0,20) y en el dominio Detectar (DE) (+0,16), mientras que los dominios Identificar (ID), Gobernar (GR) y Responder y Recuperar (REyRC) quedan con una desviación negativa situada entre 12 y 13 centésimas negativas con respecto al valor promedio global.

4.5
IMC Iberoamericano por tipo de institución.

Las IES públicas analizadas se sitúan ligeramente por debajo del IMC global (1,37), con un valor de 1,28, mientras que las IES de ámbito privado superan este valor en 23 puntos hasta situarse en el valor de 1,50.

La educación superior en Iberoamérica es un sector que se enfrenta a grandes retos y desafíos en el marco de la ciberseguridad. Gran parte de estos retos son comunes a todos los países participantes. Sin embargo, la singularidad de cada país hace que presenten matices e interpretaciones diferentes de los datos obtenidos en el presente estudio.

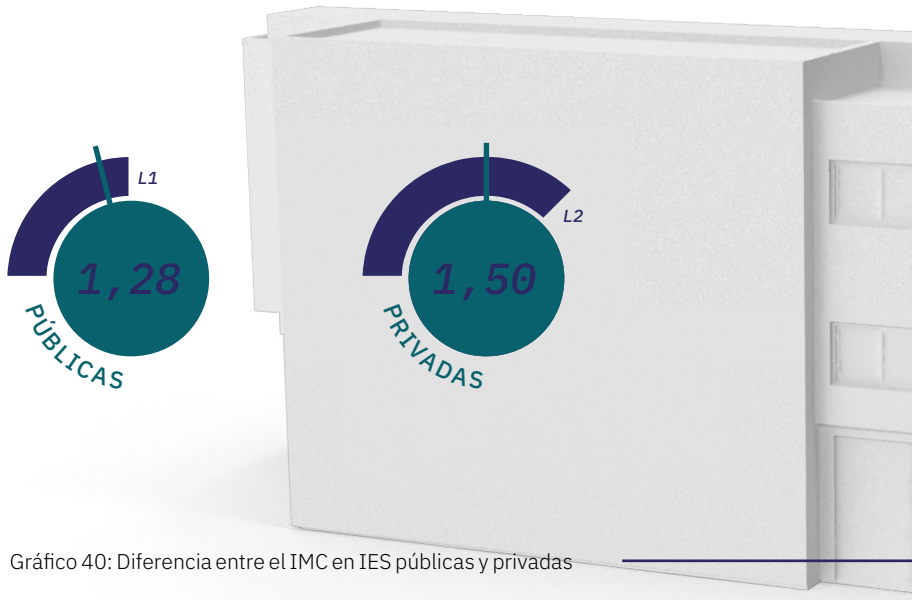


Gráfico 40: Diferencia entre el IMC en IES públicas y privadas

Una de estas singularidades es la tipología y estructura de las IES, tal como presentamos en el apartado 4 sobre “Tipología de la muestra”. Tras analizar los datos obtenidos, se puede apreciar como el grado de madurez difiere en función del tipo de institución.

Esta diferencia se traslada a nivel regional, afectando especialmente a países como Argentina y Ecuador, donde se presentan importantes diferencias de madurez entre sus instituciones públicas y privadas. En concreto, Argentina presenta un IMC de 0,85 en sus IES públicas, frente al 1,28 de sus IES privadas. Misma situación que ocurre en Ecuador, donde las diferencias de IMC entre IES públicas y privadas son mayores, cercanas a 50 puntos de madurez.

Por otro lado, destaca el caso de Colombia, dónde las IES públicas han obtenido un IMC promedio más alto que las IES privadas. Situación que no ocurre en ningún otro país analizado, donde la tendencia natural es que las instituciones de origen privado superen en nivel de madurez en ciberseguridad a las de origen público. Este dato puede atender al número de respuestas recibidas por las IES colombianas, dónde las instituciones públicas representan sólo en 10% de la muestra del país. Por lo tanto, será un punto de estudio en siguientes ediciones del IMC con el objetivo de confirmar la tendencia o corregir esta desviación.

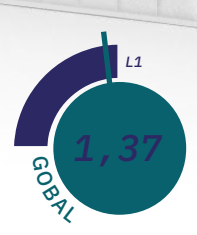
La siguiente tabla muestra una comparativa del IMC obtenido en cada uno de los países para sus IES públicas y privadas. La columna de la derecha muestra la diferencia entre ambos tipos.

Tabla 18: IMC por tipo de institución por país

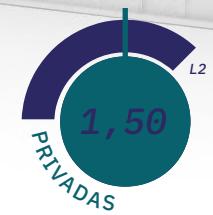
	ARGENTINA	CHILE	COLOMBIA	ECUADOR	ESPAÑA	MÉXICO	PORTUGAL
PRIVADAS	L1 (1,28)	L2 (1,58)	**L2 (1,63)**	L1 (1,30)	**L2 (1,82)**	L1 (1,41)	**L2 (1,28)**
PÚBLICAS	L1 (0,85)	L1 (1,15)	**L2 (1,79)**	L1 (0,81)	**L2 (1,72)**	L1 (1,25)	L1 (1,,39)
DIF. PRIV.-PÚBL.	0,43	0,40	**-0,16**	0,49	**0,10**	0,16	0,14

En cuanto a Dominios, observamos que las instituciones privadas presentan grados de madurez más elevados en todos los dominios, situándose entre 16 y 29 puntos por encima de las instituciones públicas.

Gráfico 19: Diferencia entre el IMC global y por países



GB	**1,43**
ID	1,32
PR	**1,54**
DE	**1,47**
REyRC	**1,10**



GB	**1,60**
ID	**1,41**
PR	**1,67**
DE	**1,64**
REyRC	1,20

GB	1,31
ID	1,25
PR	**1,45**
DE	**1,37**
REyRC	1,02

0,22

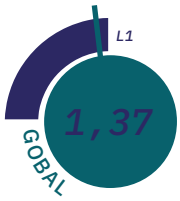
Diferencia PRIV.-PÚBL.

0.29
0.16
0.22
0.27
0.18

Las diferencias son más significativas en el dominio **gobernar** y **detectar,** con valores superiores a 25 puntos.

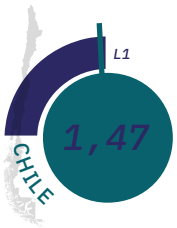
Esta tendencia global se mantiene en los diferentes países, con la única excepción de Colombia, tal y como se ha comentado. Como mención especial, destaca la situación de España y Portugal en el dominio Gobernar (GB), donde las IES públicas de estos países muestran valores superiores a los de las IES privadas. Se trata de una condición natural debido a la normativa de obligado cumplimiento para Administraciones Públicas que deriva de las políticas y directivas de la Unión Europea en materia de ciberseguridad.

Gráfico 42: Diferencia entre el IMC global y por países

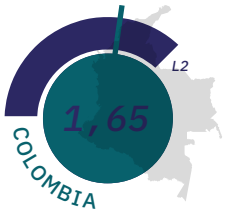


IES	1.37
GB	1.43
ID	1.32
PR	1.54
DE	1.48
REyRC	1.10
RC1	1.17
RC2	1.47
RC3	1.94

IES	1.28	0.85
GB	1.31	0.82
ID	1.28	0.75
PR	1.56	1.10
DE	1.30	0.98
REyRC	1.02	0.60
RC1	0.82	1.10
RC2	0.61	0.98
RC3	1.75	0.60
	PRIV.	**PÚBL.**

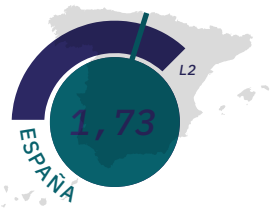


IES	1.58	1.18
GB	1.72	1.27
ID	1.40	0.95
PR	1.67	1.32
DE	1.74	1.44
REyRC	1.37	0.91
RC1	1.13	0.83
RC2	1.85	1.44
RC3	2.32	1.89
	PRIV.	**PÚBL.**

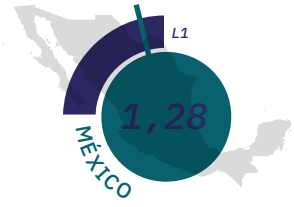


IES	1.63	1.79
GB	1.77	1.68
ID	1.56	2.19
PR	1.87	2.15
DE	1.78	1.67
REyRC	1.19	1.25
RC1	1.52	2.67
RC2	1.65	1.17
RC3	2.26	2.00
	PRIV.	**PÚBL.**

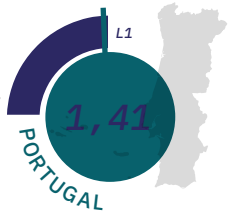
IES	1.30	0.81
GB	1.39	0.67
ID	1.08	0.90
PR	1.50	1.27
DE	1.47	0.64
REyRC	1.04	0.57
RC1	1.00	0.96
RC2	1.44	1.39
RC3	2.08	1.43
	PRIV.	**PÚBL.**



IES	1.82	1.72
GB	1.79	1.98
ID	1.53	1.45
PR	1.83	1.79
DE	2.34	1.87
REyRC	1.58	1.50
RC1	1.50	1.41
RC2	1.19	1.42
RC3	2.08	2.18
	PRIV.	**PÚBL.**



IES	1.41	1.25
GB	1.57	1.24
ID	1.49	1.32
PR	1.52	1.42
DE	1.43	1.28
REyRC	1.05	1.02
RC1	1.25	1.23
RC2	1.34	1.50
RC3	2.17	1.67
	PRIV.	**PÚBL.**



IES	1.53	1.39
GB	1.22	1.33
ID	1.48	1.41
PR	1.66	1.57
DE	1.88	1.66
REyRC	1.42	0.97
RC1	1.25	1.06
RC2	1.58	1.21
RC3	2.11	1.89
	PRIV.	**PÚBL.**

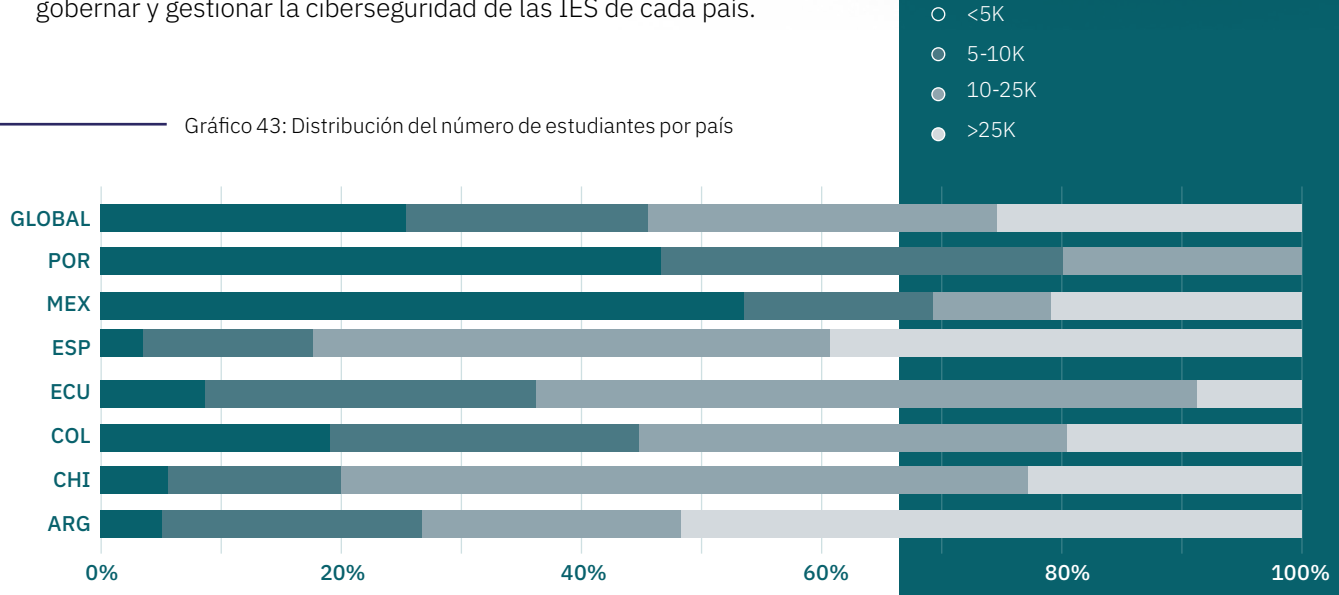
4.6
IMC Iberoamericano por tamaño.

En este apartado se realiza un análisis sobre el tamaño de las instituciones de educación superior de Iberoamérica según la cantidad de estudiantes y la relación de empleados dedicados a ciberseguridad y se revisa la relación entre el IMC y la cantidad de incidentes de seguridad.

Relación con el número de estudiantes

En Iberoamérica se encuentra una gran diversidad de IES que, en términos de tamaño de estudiantes, varían desde algunos cientos a miles de estudiantes. Tras analizar los percentiles con mayor número de estudiantes, se han establecido 4 tramos de clasificación: menos de 5.000 estudiantes, entre 5.000 y 10.000 estudiantes, entre 10.000 y 25.000 estudiantes y más de 25.000 estudiantes. En base a esta clasificación, la siguiente gráfica muestra la distribución porcentual por país. Gráfica que refleja una dispersión diferente en cada país que puede tener implicaciones a la hora de gobernar y gestionar la ciberseguridad de las IES de cada país.

Gráfico 43: Distribución del número de estudiantes por país



Por ejemplo, en Argentina el mayor porcentaje de IES está en el rango de más de 25.000 estudiantes. En Chile y Ecuador priman las IES dentro del rango de 10.000 a 25.000 estudiantes. Colombia muestra un ecosistema más repartido. En España hay igualdad entre el rango de 10.000-25.000 y más de 25.000. Y, por su parte, México y Portugal tienen un alto porcentaje de IES con menos de 5.000 estudiantes.

Estas cifras, junto al número de personal docente y no docente, conforman la comunidad universitaria de cada institución y son el elemento clave a la hora de mejorar la protección personal de estos usuarios y la seguridad corporativa de la institución.

Gráfico 44: Diferencia entre el IMC global y por países

Según IMC 2024, el tamaño de la comunidad universitaria tiene una relación directa con el grado de madurez. A mayor tamaño, mayor nivel de madurez. Las IES de menos de 5.000 estudiantes presentan un nivel de madurez básico (L1, 1,12 puntos). Aquellas cuyo número de estudiantes se encuentra dentro del rango de 5.000 a 10.000 suben a 1,34 puntos y las que están dentro del rango 10.000 a 25.000 rozan el nivel intermedio (L1, 1,46). Valor que es superado por las IES de más de 25.000 estudiantes y que en promedio se encuentran dentro del nivel de madurez intermedio (L2) con 1,51 puntos.

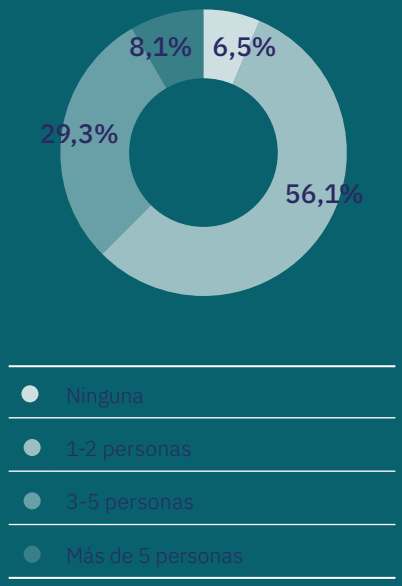
Las personas son el recurso más valioso en el ámbito de la ciberseguridad.

Equipos de ciberseguridad

La formación de equipos cualificados y capacitados para satisfacer las elevadas demandas de la sociedad digital actual obliga a las IES a fortalecer sus equipos de ciberseguridad e invertir en medidas de prevención. De este modo, se puede evitar el alto costo asociado a un ciberataque o a una fuga de información, tanto para el funcionamiento como para la reputación de estas instituciones.

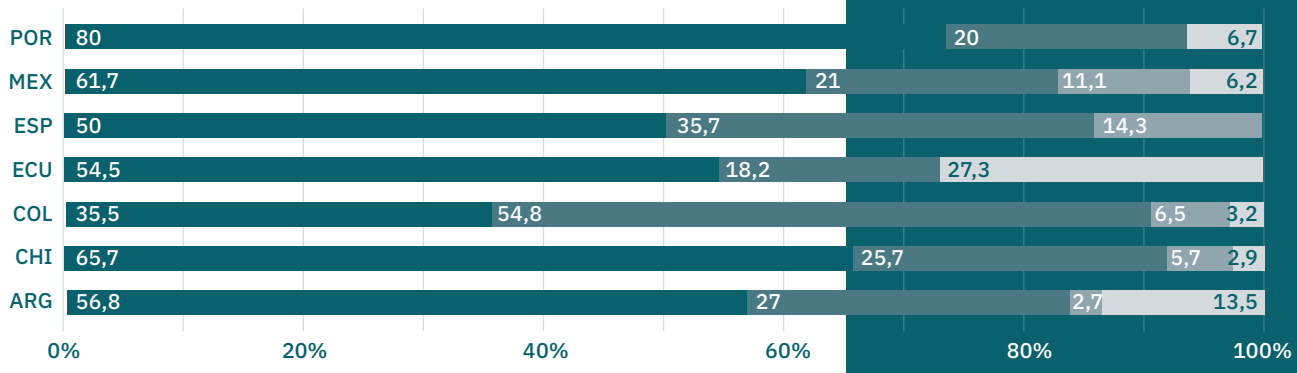
En este sentido, los datos obtenidos de IMC 2024 muestran cómo la tendencia más común de las IES en Iberoamérica es contar con equipos de ciberseguridad de 1 o 2 personas, con un 56,1% de las IES analizadas. Frente al 29,3% que cuentan con equipos medianos de 3 a 5 personas y el 8,1% cuyos equipos están conformados por más de 5 personas. Esto hace que el 93,5% de las IES tengan equipos de ciberseguridad y el 6,5% no cuenten con ninguna persona en ciberseguridad.

Gráfico 45: Configuración de los equipos de ciberseguridad en Iberoamérica



A nivel nacional, España destaca al ser el único país que cuenta con presencia de personal dedicado en todas sus Instituciones. Por su parte, la situación de Ecuador muestra un alto grado de IES sin equipos de ciberseguridad, con un 27,30%, valor muy superior al resto de países analizados.

Gráfico 46: Distribución en porcentaje y por país, de la conformación de equipos de seguridad de las IES, según su cantidad de integrantes

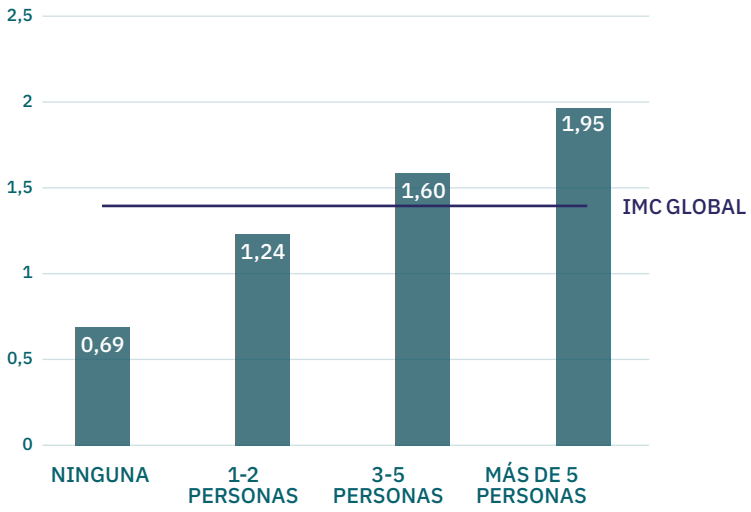


El tamaño de los equipos de ciberseguridad es uno de los indicadores que mayor repercusión tienen en el nivel de madurez de las IES.

Los datos obtenidos reflejan una fuerte relación entre el número de personas que componen los equipos de ciberseguridad y el valor del IMC. A mayor tamaño del equipo de ciberseguridad, mayor valor de madurez. Situación que ocurre en el promedio iberoamericano y en cada uno de los países analizados.

A nivel global, el IMC de las IES que no tienen equipos de seguridad se encuentra en el nivel más bajo de la escala, nivel inicial (L0), con 0,69 puntos. Las IES con equipos pequeños de 1 o 2 personas ascienden a nivel básico (L1, 1.24). Las IES con equipos medianos de 3 a 5 personas pasan a nivel intermedio (L2, 1.60) y aquellas que cuentan con más de 5 personas se sitúan nivel intermedio (L2, 1.95). Valores que hacen que el tamaño de los equipos de ciberseguridad sea un elemento a tener muy en cuenta a la hora de afrontar con garantías los retos y desafíos de la ciberseguridad dentro de nuestra institución.

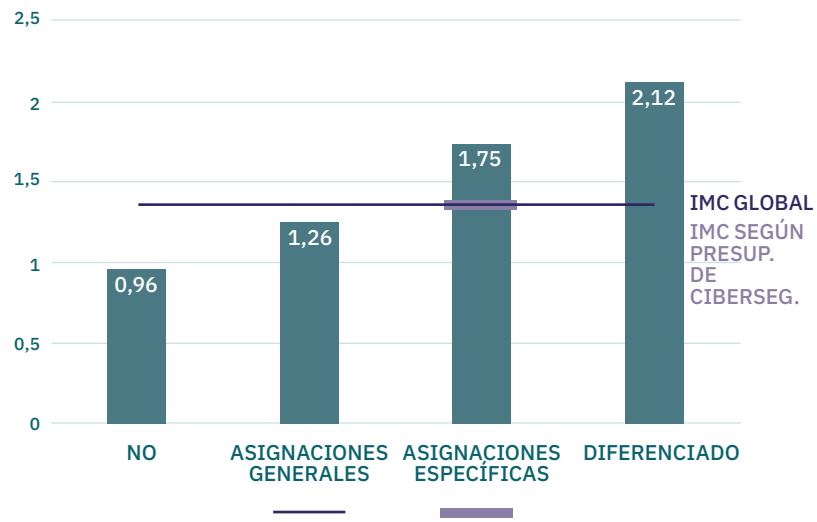
Gráfico 47: Comparativa IMC global y por tamaño de equipos



4.7
IMC Iberoamericano por presupuesto.

La asignación específica de presupuesto a las iniciativas de ciberseguridad es fundamental para cualquier entidad, incluyendo a las IES. Por otro lado, la realidad indica que solo en los últimos años se ha tomado conciencia de esta situación. Así, en muchas organizaciones, no se otorga finaciación específica para esta área o, en el mejor de los casos, esta se encuentra englobada en los fondos asignados al área de TI. Este último caso obliga a los proyectos de ciberseguridad a competir con otras iniciativas no necesariamente vinculadas a la protección de los activos de información.

Gráfico 48: Presupuesto para ciberseguridad



En cuanto al presupuesto, el 65,4% de las IES indicó que cuenta con partidas para la realización de inversiones y gastos en ciberseguridad. Sin embargo, sólo el 10% tiene un presupuesto de ciberseguridad diferenciado del presupuesto del área TI, mientras que el resto cuenta con asignaciones presupuestarias para ciberseguridad (35,7%) o tienen asignaciones generales para utilizar en este tipo de actividades (25,6%). El 34,6% restante respondió que no cuenta con un presupuesto para iniciativas de ciberseguridad.

Presupuesto específico.

Para conocer la realidad de las universidades iberoamericanas, se incluyeron en el dominio Gobernar (GB) dos preguntas, con el objetivo de determinar si existe un presupuesto específico para ciberseguridad en la IES y, en caso que se incluyera en el presupuesto de TI y fuera conocido, se requería indicar el porcentaje.

Tabla 19: Existencia de presupuesto específico para ciberseguridad

	%	IMC
Existe un presupuesto de ciberseguridad diferenciado de TI	*10%*	*L2 (2,12)*
Existe asignaciones específicas dentro del presupuesto de TI	*35,7%*	*L2 (1,75)*
Existen asignaciones generales que se usan en ciberseguridad	*25,6%*	*L1 (1,26)*
No existe	*34,6%*	*L0 (0,96)*

Tras analizar los datos obtenidos, se puede apreciar como el grado de madurez difiere en función de la manera en que se asigna un presupuesto para ciberseguridad. Las IES que cuentan con un presupuesto diferenciado, así como aquéllas que tienen asignaciones específicas se encuentran en un nivel intermedio L2 (con valores de 2,12 y 1,75 respectivamente) por encima del IMC global (1,43) que se corresponde con un nivel básico L1. Las IES que cuentan con partidas generales del presupuesto, por su parte, y aquéllas que no tienen presupuesto asignado, se sitúan por debajo del IMC Global, en un nivel básico L1 con valores de 1,26 y 0,96, respectivamente.

Este comportamiento se observa para todos los países, aunque con variaciones en sus valores de nivel de madurez. Sólo en España (1,81) y Colombia (1,50), las IES que han informado usar asignaciones generales del presupuesto para ciberseguridad, han obtenido un IMC promedio L2, correspondiente a un nivel intermedio. Esta situación no se repite en ningún otro país analizado.

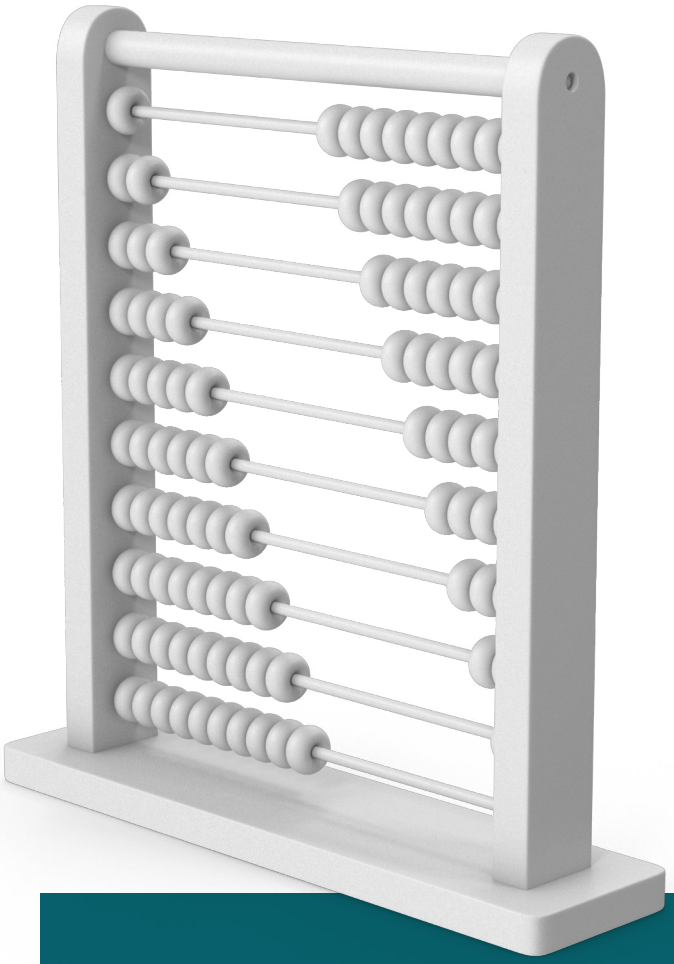


Tabla 20: ¿Existe un presupuesto específico para ciberseguridad?

	ARGENTINA	CHILE	COLOMBIA	ECUADOR	ESPAÑA	MÉXICO	PORTUGAL	OTROS
NO EXISTE	L0 (0,71)	L1 (0,77)	L1 (1,23)	L0 (0,67)	L1 (1,19)	L1 (0,96)	L1 (1,32)	L0 (0,65)
ASIGNACIONES GENERALES	L1 (0,98)	L1 (1,18)	**L2 (1,50)**	L1 (0,95)	**L2 (1,81)**	L1 (1,18)	**L1 (1,44)**	L1 (1,22)
ASIGNACIONES ESPECÍFICAS	**L2 (1,76)**	**L2 (1,76)**	**L2 (1,73)**	**L1 (1,40)**	L1 (1,18)	**L2 (1,73)**	**L2 (2,24)**	**L2 (1,68)**
PRESUPUESTO DIFERENCIADO		**L3 (2,31)**	**L2 (1,75)**		**L1 (1,44)**	**L3 (2,41)**		
TOTAL	L1 (1,06)	**L1 (1,47)**	**L2 (1,62)**	L1 (0,99)	L1 (1,26)	L1 (1,27)	**L1 (1,41)**	**L1 (1,43)**

Observando el orden de magnitud de los presupuestos de ciberseguridad, encontramos que más de la mitad de las IES no han respondido la pregunta en la cual se solicitaba indicar el presupuesto de ciberseguridad de su institución.

Entre las IES que han reportado esta información, se observa que el 11,8% cuenta con fondos asignados a ciberseguridad, en montos equivalentes a menos del 5% del presupuesto del área TI. Un 20%, por su parte, afirma encontrarse en el rango entre el 5 y el 10%, un 30% consume entre el 10 y el 20% del presupuesto de informática y el 38,2%, una cantidad mayor a dicho porcentaje. Estas respuestas permiten afirmar que aproximadamente **7 de cada 10 IES utilizan más del 10% del presupuesto TI en acciones de ciberseguridad.**

Gráfico 49: Cantidad de IES según porcentaje de presupuesto

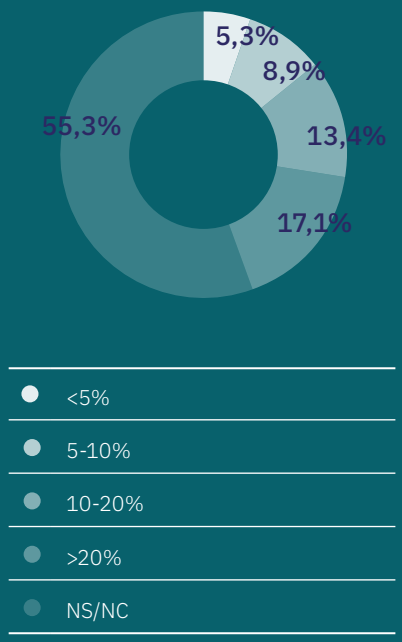


Tabla 21: Nivel de madurez por país según porcentaje de presupuesto

	ARGENTINA	CHILE	COLOMBIA	ECUADOR	ESPAÑA	MÉXICO	PORTUGAL	OTROS	TOTAL
<5%	1	1	2		4	4	1		13
5-10%	4	3	5	1	3	4	1	1	22
10-20%	1	9	7	3	1	7	3	2	33
>20%	3	7	5	2	6	18	1		42
NC	28	15	12	5	14	48	9	5	136

Como podemos apreciar en la siguiente gráfica, el presupuesto asignado a ciberseguridad tiene una repercusión directa en el grado de madurez de las universidades en este campo. Según los datos obtenidos, aquellas instituciones que cuentan con un presupuesto de ciberseguridad inferior al 5% del presupuesto total del área TI, presentan un IMC de 1,33 (L1, nivel de madurez básico) por debajo del IMC Globa l (1,37). Mientras que en un nivel intermedio L2, con valores que superan al IMC Global (1,37), se encuentran aquellas que cuentan con un presupuesto de ciberseguridad en el rango del 5% al 10%, con un nivel de madurez de 1,67; con un nivel de madurez de 1,55, las IES con presupuesto de entre 10 y 20%; y con un nivel de madurez de 1,64, las universidades que destinan más del 20% del presupuesto a ciberseguridad.

Gráfico 50: Porcentaje del presupuesto de TI asignado a ciberseguridad

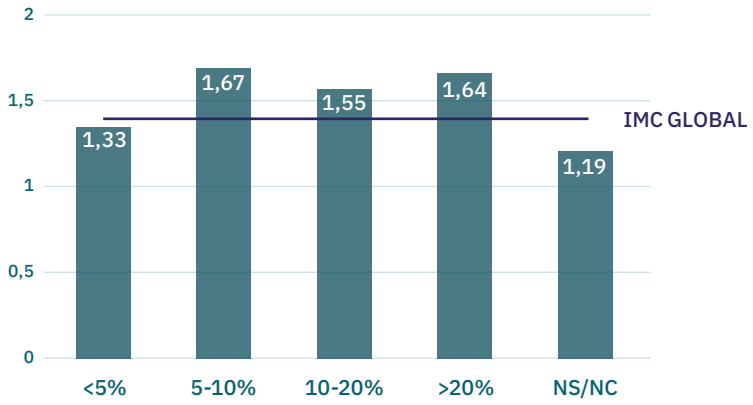


Tabla 22: ¿Existe un presupuesto específico para ciberseguridad?

	ARGENTINA	CHILE	COLOMBIA	ECUADOR	ESPAÑA	MÉXICO	PORTUGAL	OTROS
<5%	0,81	0,43	**1,83**		**1,41**	**1,38**	1,26	
5-10%	**1,76**	1,21	**2,10**	**1,69**	**1,87**	**1,58**	1,29	0,67
10-20%	0,85	**1,59**	**1,59**	1,17	**2,22**	**1,59**	1,33	**2,07**
>20%	**1,57**	**2,05**	**1,71**	0,92	**1,99**	**1,41**	**2,06**	
NS/NC	0,92	1,26	**1,38**	0,77	**1,65**	1,13	**1,40**	1,33
TOTAL	1,06	**1,47**	**1,62**	0,99	**1,73**	1,27	1,19	**1,43**

El presupuesto asignado tiene repercusión directa en el grado de madurez en ciberseguridad de las universidades.

4.8
IMC Iberoamericano según la gestión interna de la ciberseguridad.

En el caso de las IES de Iberoamérica, otra particularidad que se presenta es la manera en que se lleva a cabo la gestión interna de la ciberseguridad. En algunas instituciones, ésta se encuentra centralizada. Es decir, hay un responsable o un área que lleva a cabo la gestión de la ciberseguridad para toda la organización. En otras, las acciones relacionadas a esta gestión son realizadas por personas o equipos de distintos departamentos, institutos y/o facultades. Un tercer grupo, la realiza de manera híbrida, estando algunas acciones centralizadas y otras distribuidas.

La tendencia muestra que las IES, tanto las de gestión centralizada como las que la realizan de manera distribuida o híbrida, aparecen con un nivel de madurez básico de L1. En el caso de las primeras, el valor del IMC promedio es de 1,42, levemente superior al IMC global (1,37). En los otros dos casos, el valor promedio aparece por debajo del IMC global (1,37), siendo de 1,11 para la de gestión distribuída y de 1,23 para las de gestión híbrida.

Esta misma tendencia se da en todos los dominios. Ello puede deberse a que cuando la gestión de la ciberseguridad está distribuida es necesario coordinar acciones, lo que demandaría otra dinámica de trabajo y muchas veces, dificultará las tareas. Por ejemplo, se requiere considerar esta naturaleza cuando se definen, se implementan y se comunican acciones relacionadas a la ciberseguridad.

Una gestión centralizada ofrece beneficios en cuanto a la madurez.

la mayor diferencia entre la gestión centralizada respecto a la gestión distribuida e híbrida se da en el dominio Gobernar.

Tabla 23: Nivel de madurez por tipo de gestión interna de las IES de acuerdo a cada dominio

	CENTRALIZADA	DISTRIBUIDA	HÍBRIDA	GLOBAL
IMC	**1.42**	1.11	1.23	**1.37**
GB	**1.50**	1.09	1.24	**1.43**
ID	**1.37**	1.00	1.26	1.32
PR	**1.58**	1.30	**1.44**	**1.54**
DE	**1.53**	1.26	1.28	**1.47**
REyRC	1.14	0.95	0.91	1.10

4.9
Análisis detallado por país.

Una herramienta para la creación o actualización de estrategias y acciones de mejora de la ciberseguridad de la IES de MetaRed.

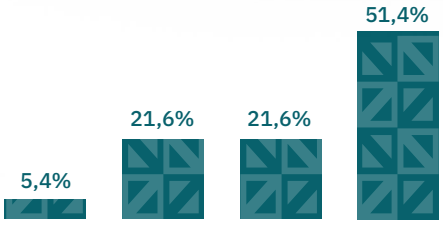
El objetivo de este apartado es mostrar un análisis detallado de la situación nacional de cada país, comparada con la media iberoamericana, como herramienta para la creación o actualización de estrategias y acciones de mejora de la ciberseguridad de las IES en los diferentes países que forman parte de MetaRed.

Esta información se completa con un cuadro de mandos que muestra un análisis individualizado de cada IES participante en este estudio. La información específica de cada institución será comunicada a la persona responsable en ciberseguridad de cada organización y sólo estará disponible para esa institución, asegurando la privacidad de los datos obtenidos. Una vez recibida, el responsable podrá acceder a un cuadro de mandos con toda la información de su institución comparada con las medias de su país e iberoamericana.

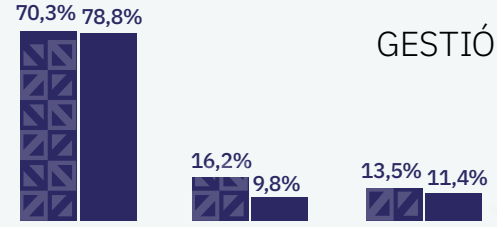
Argentina.

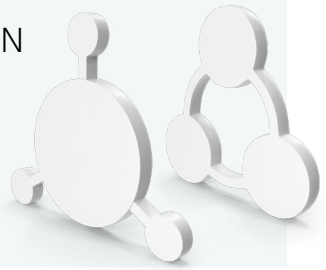
IMC 1,06 · L1 BÁSICO

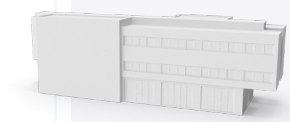
TAMAÑO DE IES



GESTIÓN

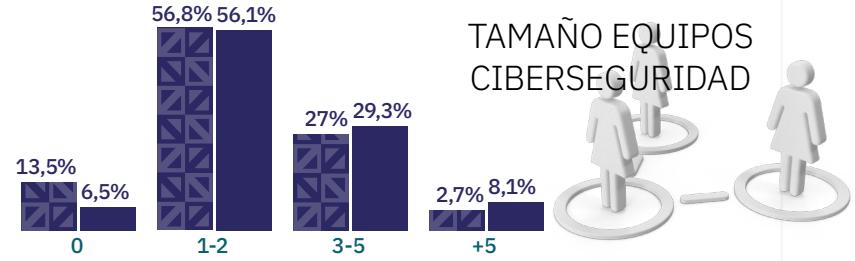






TIPO DE IES

TAMAÑO EQUIPOS CIBERSEGURIDAD



PRESUPUESTO

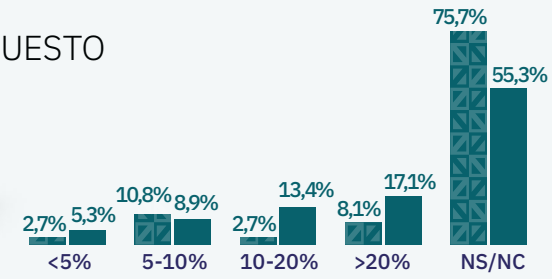
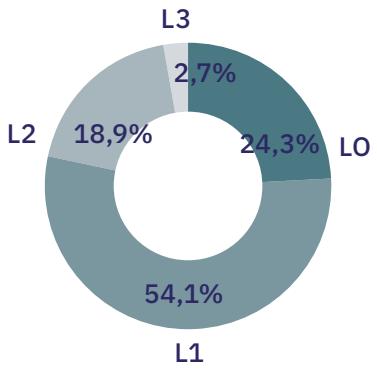


Gráfico 51: Nivel de madurez de IES en Argentina



Argentina se sitúa en un nivel de madurez básico L1, con un IMC de 1,06 puntos, 31 puntos por debajo del IMC (1,37). Este valor ubica a Argentina en uno de los niveles de madurez más bajos de los países participantes en esta edición.

De las universidades encuestadas, el 24,3% presentan un nivel de madurez inicial (L0), un 54,1% un nivel de madurez básico (L1), un 18,9% un nivel intermedio (L2) y tan solo el 2,7%, un nivel avanzado (L3). Estos valores sitúan a cerca de 8 de cada 10 IES argentinas dentro de un nivel de madurez básico (L1) o inicial (L0), estando la media iberoamericana en 4 de cada 10 IES.

Tipos de Institución

Al igual que en la mayoría de los países analizados, estos valores muestran ligeras diferencias en función del tipo de institución. En concreto, las IES públicas argentinas presentan un IMC de 0,85, frente a 1,28 de las instituciones privadas. Ambas muestran un nivel de madurez básico (L1), lo que refleja la realización de prácticas ad-hoc o informales, políticas o procedimientos limitados, implementaciones incipientes de tecnologías de seguridad, escaso personal de ciberseguridad y/o con baja especialización y procesos de identificación y evaluación de riesgos en fase inicial.

Una mención especial requieren las IES públicas argentinas, en las que el IMC se sitúa en un nivel básico (L1) pero con un valor muy bajo, cercano al nivel de madurez inicial (L0), que tiene su umbral superior en 0,75 puntos. Si profundizamos en los dominios de aplicación, Argentina queda por debajo de la media iberoamericana en los cinco dominios del modelo de madurez, siendo los valores con mayor diferencia los correspondientes al dominio Gobernar (GB), Detectar (DE) e Identificar (ID) con 37, 33 y 31 puntos negativos de diferencia, respectivamente.

Argentina requerirá un análisis detallado de la situación de sus IES con el fin de crear acciones de corrección que permitan un incremento del IMC a corto plazo.

Dominios de aplicación

Si profundizamos en los dominios de aplicación, Argentina queda por debajo de la media iberoamericana en los cinco dominios del modelo de madurez, siendo los valores con mayor diferencia los correspondientes al dominio Gobernar (GB), Detectar (DE) e Identificar (ID) con 37, 33 y 31 puntos negativos de diferencia, respectivamente.

Gráfico 52: Nivel de madurez de IES en Argentina según el dominio

En líneas generales, las IES argentinas priorizan las acciones operativas (RC3) de prevención y defensa, frente a las acciones procedimentales de definición de normativa interna y procedimientos de seguridad (RC2) y las acciones de planificación y socialización de las personas que componen la comunidad universitaria (RC1).

Si focalizamos sobre el IMC de cada dominio en función del tipo de institución (pública o privada), obtenemos valores similares al IMC global (1,37) salvo en el dominio Proteger (PR) de las IES privadas argentinas, donde superan mínimamente dicho valor. El resto de dominios siempre quedan por debajo, independientemente de si son IES públicas o privadas, aunque en el caso de las públicas, tal y como hemos mencionado, las diferencias son considerablemente mayores (entre 32 y 53 puntos).

Gráfico 53: Nivel de madurez de IES en Argentina según el commponente

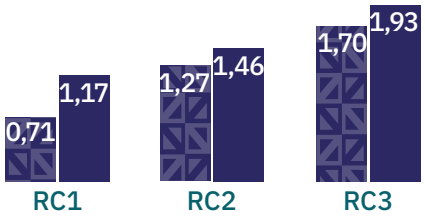
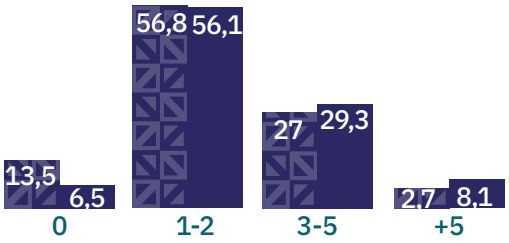


Tabla 24: Nivel de madurez de cada dominio en función del tipo de IES

	GLOBAL	GB	ID	PR	DE	REyRC
PRIVADA	1,28	1,31	1,28	1,56	1,30	1,02
PÚBLICA	0,85	0,82	0,75	1,10	0,98	0,60
DIFERENCIA	0,43	0,49	0,53	0,46	0,32	0,42

Equipos de ciberseguridad

Gráfico 54: Composición del equipo de ciberseguridad en función del porcentaje de IES argentinas



En lo que respecta a la creación y consolidación de equipos de ciberseguridad dentro de las IES, Argentina muestra que un 13,5% de instituciones no cuenta con ninguna persona asignada a labores de ciberseguridad. Este dato, relacionado con la parte presupuestaría anterior y la situación nacional específica del país, nos hace pensar en la necesidad de acciones nacionales que visualicen la importancia de la ciberseguridad y su componente económica, pasando de invertir en situaciones post-incidentes a acciones preventivas.

El resto de IES (86,5%) cuenta con personal asignado, siendo la tendencia más común contar con equipos de 1 o 2 personas (56,8%) o equipos entre 3 y 5 personas (27%) y en muy pocas ocasiones (2,7% de los casos), se dispone de más de 5 personas. Esta situación es muy similar a la media iberoamericana en los rangos intermedios. Sin embargo, Argentina muestra un 6% menos de IES con equipos de más de 5 personas y un 6% más de instituciones sin equipos específicos de ciberseguridad.

Gráfico 55: Nivel de madurez de las IES argentinas según la composición de sus equipos de ciberseguridad

Al comparar estos datos con el IMC, se observa una clara curva creciente, pasando del nivel más bajo (L0, con 0,62 puntos) de las IES que no cuentan con personal, hasta el nivel intermedio (L2, con 1,51 puntos) y ampliamente superior a la media nacional (1,06) de las IES que han apostado por equipos cualificados en ciberseguridad de más de 3 personas.

Tabla 25: Comparación entre IES argentinas, iberoamericanas e IMC según integración del equipo de ciberseguridad

	0 MIEMBROS	1-2 MIEMBROS	3-5 MIEMBROS	+5 MIEMBROS
ARGENTINA	13,5	56,8	27	2,7
IBEROAMÉRICA	6,5	56,1	29,3	8,10
IMC	0,62 L0	0,93 L1	1,51 L2	1,50 L2

Presupuestos de ciberseguridad

En cuanto al presupuesto, cerca de 6 de cada 10 IES argentinas cuentan con partidas presupuestarias para la realización de inversiones y gastos en ciberseguridad. Sin embargo, ninguna de estas instituciones tiene un presupuesto de ciberseguridad diferenciado del presupuesto del área TI. La tendencia es usar parcialmente partidas presupuestarias generales para ciberseguridad (35,1%) o contar con partidas específicas dentro del presupuesto del área TI (24,3%).

Gráfico 56: Porcentaje de IES argentinas según presupuesto

Si comparamos el IMC promedio de las IES según la existencia o no de presupuesto de ciberseguridad, podemos ver que aquellas que no cuentan con presupuesto de ningún tipo asignado a ciberseguridad muestran un nivel de madurez inicial L0, por debajo del IMC medio del país, dato que afecta a 4 de cada 10 IES argentinas.

Por su parte, aquellas instituciones que cuentan con presupuesto para ciberseguridad dentro de las partidas generales del área TI suben 27 puntos y se posicionan en un nivel básico L1, aunque siguen por debajo del IMC medio.

Por último, podemos ver como aquellas IES que ya cuentan con asignaciones específicas tienen una importante mejoría en su nivel de madurez, situándose en niveles intermedios y superando ampliamente la media nacional en 70 puntos. Estos datos ponen de manifiesto la importancia del presupuesto de ciberseguridad dentro de las IES argentinas y el papel relevante que tiene esta inversión en el nivel de madurez nacional, como muestra el gráfico.

Gráfico 57: Nivel de madurez de IES en Argentina según presupuesto

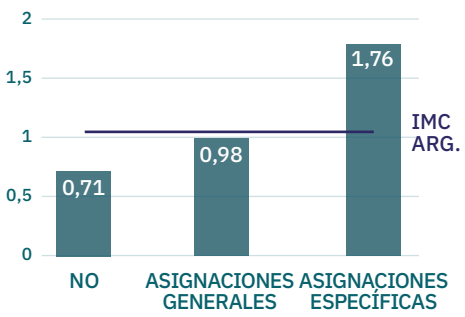
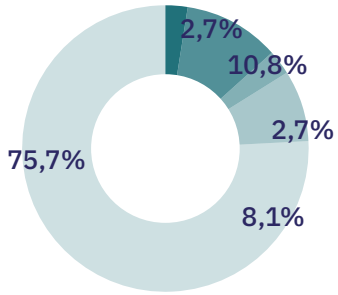


Gráfico 58: Porcentaje del presupuesto de ciberseguridad en comparación con presupuesto de TI



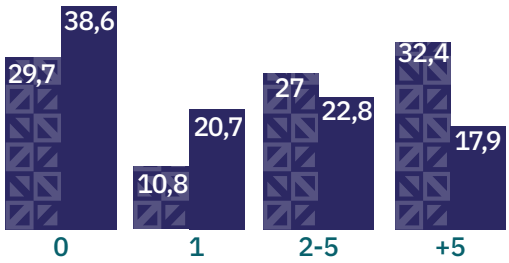
- <5%
- 5-10%
- 10-20%
- >20%
- NS/NC

En cuanto al orden de magnitud del presupuesto asignado a ciberseguridad, el 75,7% de las IES argentinas no han indicado la asignación presupuestaria para ciberseguridad, frente al 24,3% que han especificado el porcentaje de presupuesto de ciberseguridad sobre el presupuesto total del área IT. De estas últimas, el 11,1% cuenta con menos del 5%, el 44,4% en el rango del 5-10% y el total restante del 44,5%, por encima del 10%.

Comparando el IMC en función del porcentaje de presupuesto asignado, se obtiene una tendencia creciente. Sin embargo, la baja tasa de respuesta en esta pregunta hace que los datos obtenidos para este indicador deban tratarse con cautela, al contar con una muestra menor en este apartado.

Ciberincidentes

Gráfico 59: Comparativa ciberincidentes sufridos por IES en el último año en Argentina y en Iberoamérica



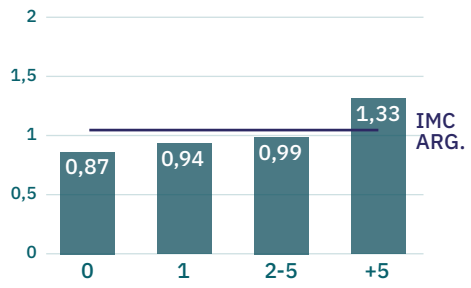
En cuanto al porcentaje de IES de Argentina que han sufrido algún incidente de seguridad con afectación a la operación de la institución de forma parcial o total, el porcentaje asciende al 70,27%. Es decir, 7 de cada 10 IES argentinas ha sufrido algún tipo de incidente en el último año. Si analizamos el detalle, podemos ver que el 32,4% ha sufrido más de 5 incidentes y el 27% entre dos y cinco de estas situaciones. Estos valores son superiores a la media iberoamericana, donde el promedio de IES que han reportado algún incidente es de 61,4%, un 8,9% inferior que en Argentina.

Si bien los ciberincidentes suelen generar un refuerzo en las acciones de ciberseguridad de la institución afectada, lo que repercute en un incremento de su IMC, en el caso de Argentina, esto ocurre de forma más gradual. Es decir, el IMC de las instituciones afectadas muestra un ligero incremento en los tramos de uno a cinco ciberincidentes, y no es hasta el tramo de más de cinco ciberincidentes cuando su IMC supera el valor de la media nacional.

En concreto, se observa un incremento importante en las universidades que han tenido alguna incidencia en el último año. En especial, en aquellas que reciben su primer ciberincidente, donde el refuerzo de la ciberseguridad de la institución, consecuencia de esta situación hace que el IMC suba en promedio 40 puntos.

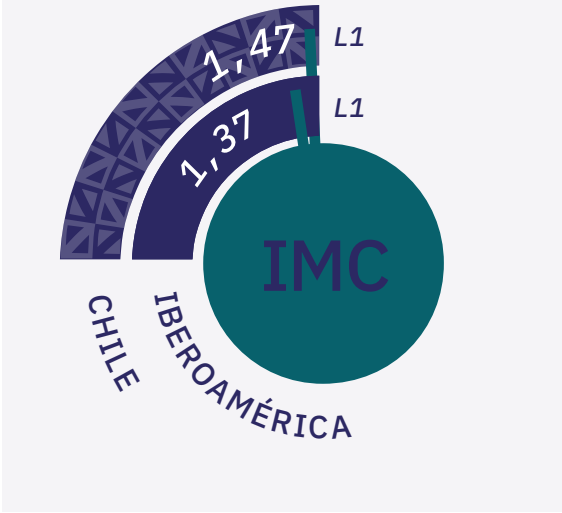
Como podemos apreciar en la siguiente gráfica, el presupuesto tiene una repercusión directa en el grado de madurez de las instituciones. Según los datos obtenidos, aquellas IES que cuentan con un presupuesto de ciberseguridad inferior al 5% del presupuesto total del área de TI presentan un IMC de 0,43 (L0, nivel de madurez inicial), frente al nivel al 1,21 (L1, nivel básico) de las IES que cuentan con un presupuesto de ciberseguridad en el rango del 5%-10%, o los valores superiores a 1,5 puntos (L2, nivel intermedio) de las instituciones con presupuesto superior al 10%.

Gráfico 60: Nivel de madurez de IES que sufrieron incidentes en el último año en Argentina

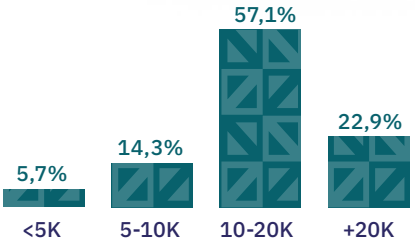


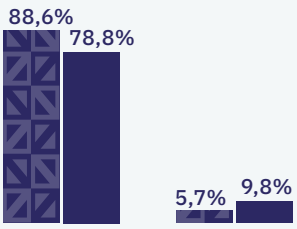
Chile.

IMC 1,47 · L1 BÁSICO

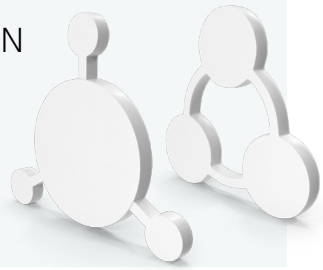


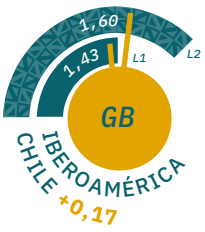
TAMAÑO DE IES

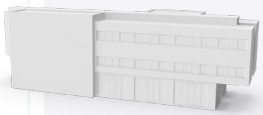




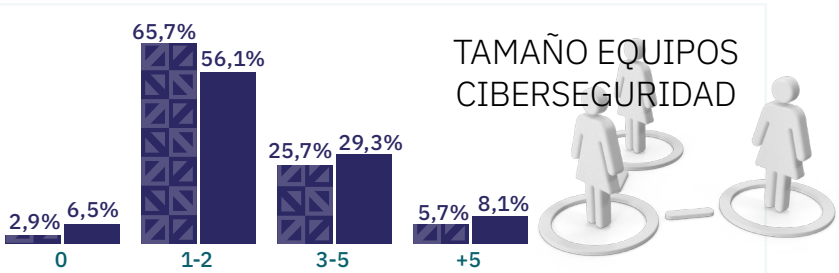
GESTIÓN



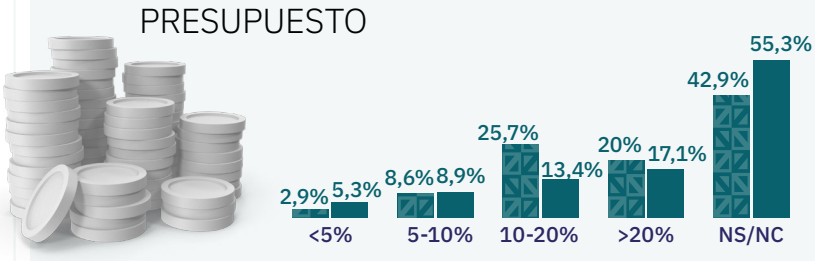




TIPO DE IES



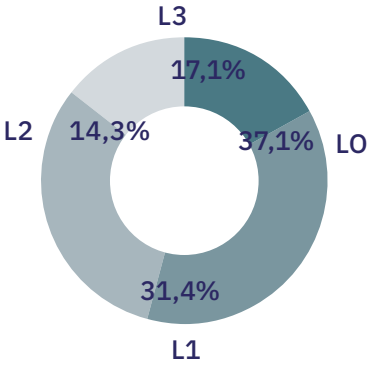
TAMAÑO EQUIPOS CIBERSEGURIDAD



PRESUPUESTO

Chile se sitúa en un nivel de madurez básico L1, con un IMC de 1,47 puntos y a tan solo 3 puntos del nivel de madurez intermedio L2. Esta valoración ubica a las IES del país 10 puntos por encima del IMC iberoamericano y como tercer país en nivel de madurez de los participantes en esta edición del IMC Iberoamericano.

Gráfico 61: Nivel de madurez de IES en Chile



De las IES encuestadas en Chile, el 17,1% se sitúa en un nivel inicial L0, un 37,1% en un nivel básico, L1, un 31,4% en un nivel intermedio, L2, y el 14,3% restante en un nivel avanzado, L3. Se observa entonces que esos valores ubican al 45,70% de las IES chilenas dentro de un nivel de madurez intermedio o avanzado, siendo la media iberoamericana del 40,8%.

Tipos de Institución

Al igual que en la mayoría de los países analizados, estos valores muestran diferencias en función del tipo de institución. En concreto, las IES públicas chilenas presentan un IMC de 1,18 (L1), frente a 1,58 (L2) de las IES privadas.

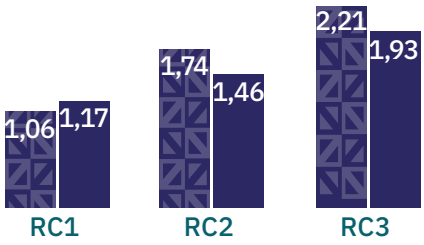
Esto posiciona a las IES públicas de Chile en un nivel de madurez básico (L1), con acciones poco definidas o poco maduras. Por su parte, las IES privadas de Chile muestran un nivel de madurez intermedio (L2), lo que refleja la existencia de políticas y procedimientos bien definidos y documentados, la implementación de tecnologías de seguridad como sistemas de detección de intrusos o herramientas de cifrado, personal de seguridad dedicado y con algún grado de especialización y procesos de gestión de riesgos formalizados, entre otras características.

Dominios de aplicación

Si profundizamos en los dominios de aplicación, Chile supera la media iberoamericana en cuatro de los cinco dominios del modelo de madurez. El único dominio donde no se supera ese umbral es el dominio Identificar (ID) con un valor muy similar a la media iberoamericana. Los valores con mayor diferencia son los correspondientes al dominio Detectar (DE), Gobernar (GB) y Responder y Recuperar (REyRC) con 19, 17 y 15 puntos de diferencia, respectivamente. Proteger (PR) por su parte, presenta un valor por encima (1,58) pero muy cercano a la media iberoamericana (1,54) para ese dominio.

Gráfico 62: Nivel de madurez de IES en Chile según el dominio

Gráfico 63: Nivel de madurez de IES en Chile según el commponente



Comparando las IES públicas y privadas a nivel de dominios, las diferencias se mantienen similares al IMC global (1,37), con valores más altos en las instituciones privadas y diferencias situadas en torno a los 40 puntos en todos los dominios.

En términos generales, las IES chilenas afrontan la ciberseguridad desde una perspectiva operativa (RC3), donde priman las acciones de prevención y defensa, al igual que la mayoría de los países analizados. Así mismo, los datos muestran una fuerte correlación entre los indicadores que analizan la normativa y procedimientos de seguridad, componentes RC2 y RC1, referidos a la parte de planificación y concienciación en ciberseguridad de los diferentes actores de la comunidad universitaria.

Tabla 26: Nivel de madurez de cada dominio en función del tipo de IES

	GLOBAL	GB	ID	PR	DE	REyRC
PRIVADA	1,58	1,71	1,40	1,67	1,74	1,37
PÚBLICA	1,18	0,27	0,95	1,32	1,44	0,91
DIFERENCIA	0,40	0,44	0,45	0,35	0,30	0,46

Equipos de ciberseguridad

Por otra parte, la creación y consolidación de equipos de ciberseguridad dentro de las universidades es un reto importante y que puede marcar el transcurrir de la evolución del grado de madurez en ciberseguridad dentro de nuestras IES. Según los datos recogidos, el 97,9% de las instituciones chilenas cuenta con equipos de ciberseguridad específicos. De ellas, el 65,7% está conformado por 1 o 2 personas; el 25,7% por 3 a 5 y tan solo el 5,7%, por equipos de más de 5 personas.

En comparación con la media iberoamericana, el número de IES de Chile que cuentan con equipos de ciberseguridad es superior a la media iberoamericana. Sin embargo, se han detectado ligeras diferencias en el número de personas que componen estos equipos. Los datos reflejan que los equipos de ciberseguridad de Chile cuentan con menos personas que la media global.

Si comparamos el IMC de las IES chilenas en función del número de personas que componen el equipo de ciberseguridad, podemos observar una clara relación entre ambos indicadores. En concreto, aquellas instituciones que no cuentan con equipos de ciberseguridad presentan un nivel de madurez inicial (L0), lo que refleja que las prácticas de ciberseguridad no son una prioridad en esas instituciones. Por su parte, las instituciones que cuentan con pequeños equipos de 1 o 2 personas incrementan su nivel de madurez a un nivel básico (L1), implementando prácticas básicas y no formalizadas, frente a las instituciones con equipos de 3 más de 3 personas que suben a un nivel intermedio (L2) y presentan una gestión y gobierno de la ciberseguridad más maduro.

Gráfico 64: Composición del equipo de ciberseguridad en función del porcentaje de IES chilenas

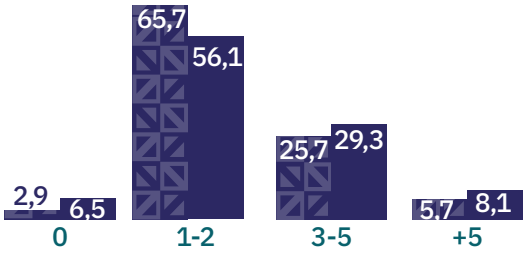


Gráfico 65: Nivel de madurez de las IES chilenas según la composición de sus equipos de ciberseguridad

Tabla 27: Comparación entre IES chilenas, iberoamericanas e IMC según integración del equipo de ciberseguridad

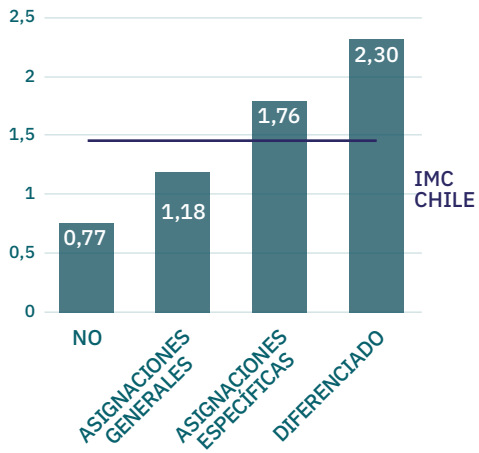
	0 MIEMBROS	1-2 MIEMBROS	3-5 MIEMBROS	+5 MIEMBROS
CHILE	2,9	65,7	25,7	5,7
IBEROAMÉRICA	6,5	56,1	29,3	8,10
IMC	0,46 L0	1,39 L1	1,68 L2	2 L2

Presupuestos de ciberseguridad

Gráfico 66: Porcentaje de IES chilenas según presupuesto

En cuanto al presupuesto, 8 de cada 10 IES chilenas cuentan con partidas presupuestarias para la realización de inversiones y gastos en ciberseguridad y cerca de 4 de cada 10 disponen de un presupuesto diferenciado del asignado al área TI. Esta circunstancia no es habitual en el resto de países iberoamericanos y sitúa a Chile a la cabeza, en este sentido.

Gráfico 67: Nivel de madurez de IES en Chile según presupuesto



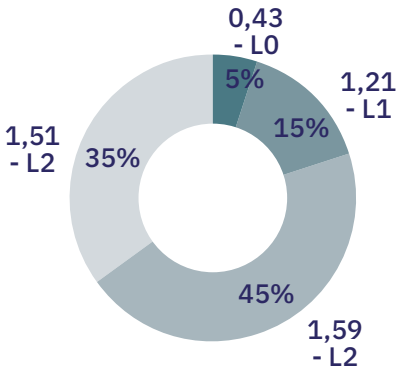
Si comparamos el IMC promedio de las instituciones chilenas según la existencia o no de presupuesto de ciberseguridad, se observa una tendencia ascendente muy clara y definida. Podemos ver cómo se escala desde un nivel inicial (L0) hasta un nivel avanzado (L3) en función de si no se dispone de presupuesto, se dispone de partidas generales o específicas, hasta llegar a contar con un presupuesto diferenciado del área IT. Se trata sin dudas, de una situación que pone en valor la importancia de apostar por una inversión en ciberseguridad dentro de la estrategia institucional, no solo del área técnica.

Analizando el orden de magnitud de los presupuestos de ciberseguridad, encontramos que 4 de cada 10 IES chilenas no han indicado el presupuesto de ciberseguridad de su institución.

Por su parte, de las IES que han reportado esta información, el 5% cuenta con fondos para ciberseguridad equivalentes a menos del 5% del presupuesto del área IT. Un 15% afirman encontrarse en el rango entre el 5 y el 10%. Un 45% consume entre el 10 y el 20% del presupuesto de informática, y el 35% más de ese porcentaje. Esto hace que 8 de cada 10 IES de Chile utilicen más del 10% del presupuesto de TI en acciones de ciberseguridad.

Como vemos, el presupuesto tiene una repercusión directa en el grado de madurez de las IES. Según los datos, aquellas que cuentan con un presupuesto de ciberseguridad inferior al 5% del presupuesto total del TI presentan un IMC de 0,43 (L0, nivel de madurez inicial), frente al nivel al 1,21 (L1, nivel básico) de las IES que cuentan con un presupuesto de ciberseguridad en el rango del 5%-10%, o los valores superiores a 1,5 puntos (L2, nivel intermedio) de las instituciones con presupuesto superior al 10%.

Gráfico 68: Porcentaje del presupuesto de ciberseguridad en comparación con presupuesto de TI, y nivel de madurez según este porcentaje



<5%
5-10%
10-20%
>20%

Ciberincidentes

Si hablamos del número de IES que han sufrido ciberincidentes en el último año, con afectación de la operación de la institución de forma parcial o total, el porcentaje asciende al 60%. Es decir, 6 de cada 10 IES en Chile ha sufrido algún tipo de incidente en el último año. Al analizar en profundidad, podemos ver que el 28,6% ha sido objeto de al menos un ciberincidente, el 28,6%, entre 2 y 5 incidentes anuales y el 2,9%, más de 5. Son valores muy similares a la media iberoamericana, donde el promedio de IES que han reportado algún incidente es de 61,4%, un 1,4% superior que en Chile.

La tendencia normal en la gran mayoría de países analizados muestra una relación directa entre el número de ciberincidentes y un mayor grado de madurez, especialmente a raíz de sufrir un primer caso. En Chile, la tendencia no sigue esta lógica y muestra un valor superior en aquellas instituciones que no han sufrido ningún ciberincidente, frente a las que han sufrido menos de 5 en el año, aunque los valores obtenidos en el IMC según el número de incidentes son similares. Se aprecia un salto de IMC importante en aquellas IES que han manifestado sufrir más de 5 ciberincidentes. En este caso, su IMC ha pasado a valores que muestran un grado de madurez avanzado L3, con un valor de IMC promedio de 2,3.

Gráfico 69: Comparativa ciberincidentes sufridos por IES en el último año en Chile y en Iberoamérica

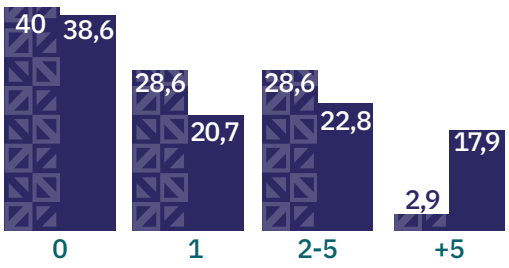
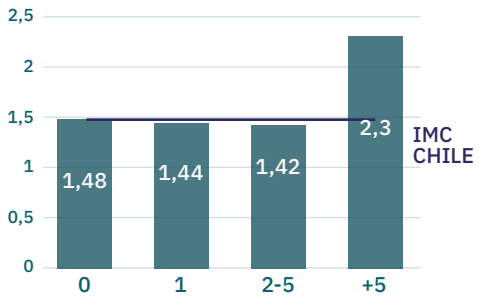
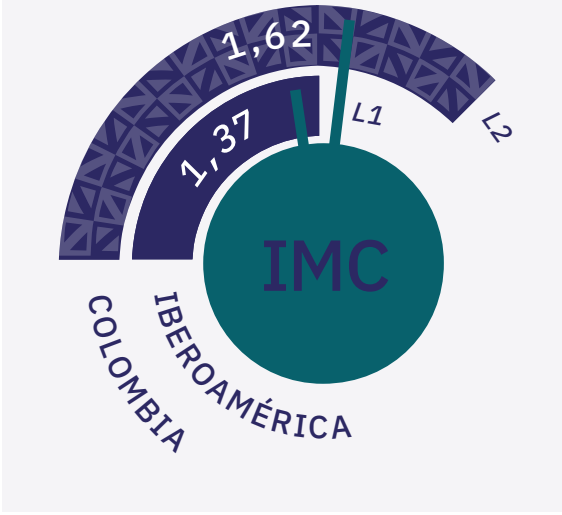


Gráfico 70: Nivel de madurez de IES que sufrieron incidentes en el último año en Argentina

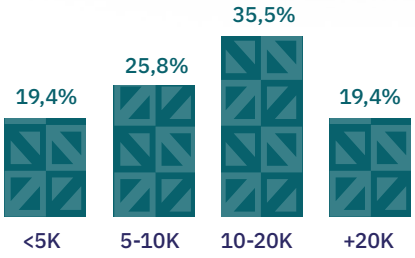


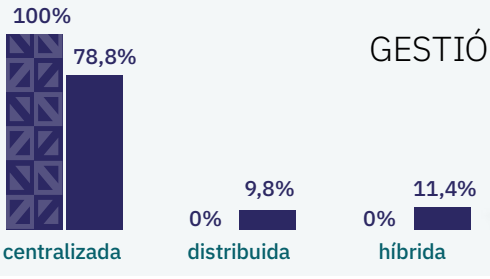
Colombia.

IMC 1,62 · L2 INTERMEDIO

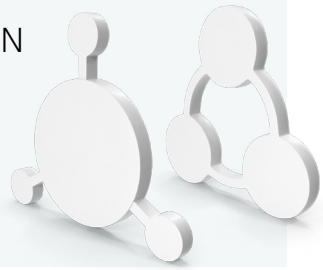


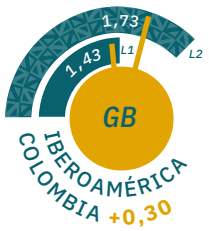
TAMAÑO DE IES

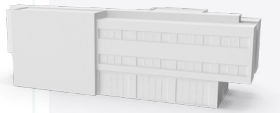




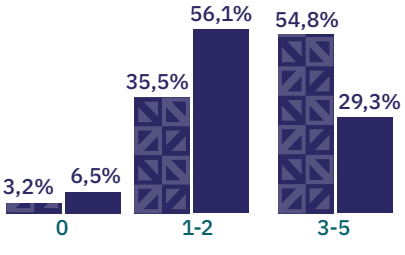
GESTIÓN





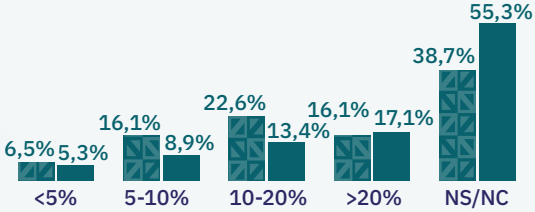


TIPO DE IES



TAMAÑO EQUIPOS CIBERSEGURIDAD

PRESUPUESTO

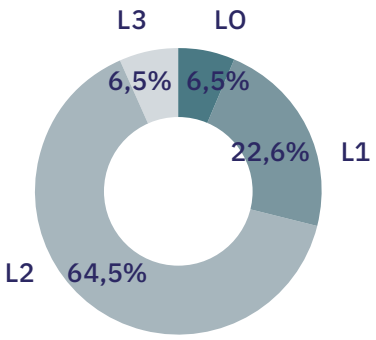


Colombia se ubica en un nivel de madurez intermedio (L2), con un IMC de 1,62 puntos. Esta valoración sitúa a las IES del país 25 puntos por encima del IMC iberoamericano (1,37).

Colombia se sitúa como el segundo país con mayor nivel de madurez.

De las IES encuestadas en este país, tan solo el 6,5% se sitúa en un nivel inicial L0, un 22,6% en un nivel básico L1, el 64,5% en un nivel intermedio L2, y el 6,5% restante en un nivel avanzado L3. Se trata de valores que ubican al 71% de las IES colombianas dentro de un nivel de madurez intermedio o avanzado, siendo la media iberoamericana del 40,8%.

Gráfico 71: Nivel de madurez de IES en Colombia



Tipos de Institución

Al igual que en la mayoría de los países analizados, estos valores muestran diferencias en función del tipo de institución. En concreto, las IES públicas colombianas presentan un IMC de 1,79 (L2), frente a 1,61 (L2) de las IES privadas. Esta situación, en la que el IMC de las IES públicas es superior al IMC de las privadas, no es la tendencia normal de Iberoamérica, siendo Colombia el único país analizado dónde se presenta este caso. Si nos fijamos en la muestra analizada en este país, detectamos que el número de IES públicas es bajo (3), en comparación con las IES privadas (28). Por lo tanto, no se pueden formular conclusiones firmes en cuanto a estos datos, que serán objeto de estudio en siguientes ediciones del IMC Iberoamericano.

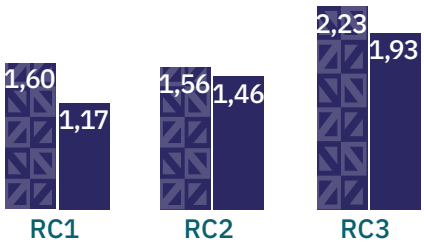
En su conjunto, es posible afirmar que estos valores sitúan a las IES de Colombia en nivel de madurez intermedio (L2), lo que refleja la existencia de políticas y procedimientos bien definidos y documentados, implementación de tecnologías de seguridad como sistemas de detección de intrusos o herramientas de cifrado, personal de seguridad dedicado y con cierta especialización y procesos de gestión de riesgos formalizados, entre otros.

Dominios de aplicación

Si profundizamos en los dominios de aplicación, Colombia supera la media iberoamericana en todos dominios del modelo de madurez. Los valores con mayor diferencia son los correspondientes al dominio Proteger (PR), Identificar (ID) y Gobernar (GB) con 36, 32 y 30 puntos de diferencia, respectivamente.

Gráfico 72: Nivel de madurez de IES en Colombia según el dominio

Gráfico 73: Nivel de madurez de IES en Colombia según el commponente



Comparando las IES públicas y privadas a nivel de dominios, las diferencias se mantienen similares al IMC global (1,37), con valores más altos en las instituciones privadas y diferencias situadas en torno a los 40 puntos en todos los dominios.

En términos generales, las IES chilenas afrontan la ciberseguridad desde una perspectiva operativa (RC3), donde priman las acciones de prevención y defensa, al igual que la mayoría de los países analizados. Así mismo, los datos muestran una fuerte correlación entre los indicadores que analizan la normativa y procedimientos de seguridad, componentes RC2 y RC1, referidos a la parte de planificación y concienciación en ciberseguridad de los diferentes actores de la comunidad universitaria.

Tabla 28: Nivel de madurez de cada dominio en función del tipo de IES.

	GLOBAL	GB	ID	PR	DE	REyRC
PRIVADA	1,61	1,73	1,58	1,87	1,75	1,19
PÚBLICA	1,79	1,68	2,19	2,15	1,67	1,25
DIFERENCIA	-0,18	0,05	-0,61	-0,28	0,08	-0,06

Equipos de ciberseguridad

Por otra parte, la creación y consolidación de equipos de ciberseguridad dentro de las IES es un reto importante y que puede marcar el transcurrir de la evolución del grado de madurez en ciberseguridad dentro de nuestras universidades. Según los datos recogidos, el 96,8% de las instituciones colombianas cuenta con equipos de ciberseguridad específicos. De ellas, el 35,5% son equipos de ciberseguridad de 1 o 2 personas, el 54,8% de 3 a 5 personas y, tan solo, el 6,5%, de más de 5 personas.

En comparación con la media iberoamericana, el número de IES de Colombia que cuentan con equipos de ciberseguridad es superior a la media iberoamericana en un 3,3%. Además, los equipos de ciberseguridad colombianos cuentan con más personas que la media Iberoamericana. En concreto, la situación habitual es disponer de equipos de 3 a 5 personas (54,8%), un valor un 25,5% superior al de Iberoamérica (29,3%).

Si comparamos el IMC de las IES colombianas en función del número de personas que integran el equipo de ciberseguridad, podemos observar una clara relación entre ambos indicadores. En concreto, aquellas instituciones que no cuentan con equipos de ciberseguridad presentan un nivel de madurez básico (L1), implementando prácticas básicas y no formalizadas. Por su parte, las instituciones que cuentan con pequeños equipos de ciberseguridad ven incrementado su nivel de madurez a grado intermedio (L2). Este valor va aumentando conforme los equipos de ciberseguridad cuentan con más personas, pasando de un IMC de 1,54 de las IES con equipos de 1 o 2 personas hasta un IMC de 2,03 en las IES con equipos de más de 5 personas.

Gráfico 74: Composición del equipo de ciberseguridad en función del porcentaje de IES colombianas

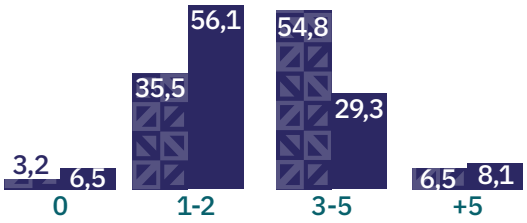


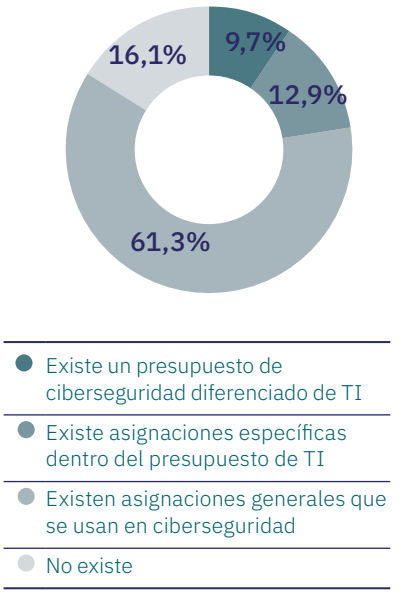
Gráfico 75: Nivel de madurez de las IES colombianas según la composición de sus equipos de ciberseguridad

Tabla 29: Comparación entre IES colombianas, iberoamericanas e IMC según integración del equipo de ciberseguridad

	0 MIEMBROS	1-2 MIEMBROS	3-5 MIEMBROS	+5 MIEMBROS
COLOMBIA	3,2	35,5	54,8	6,5
IBEROAMÉRICA	6,5	56,1	29,3	8,10
IMC	1,03 L1	1,54 L2	1,66 L2	2,03 L2

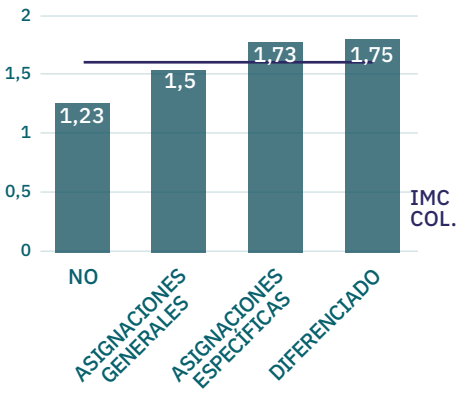
Presupuestos de ciberseguridad

Gráfico 76: Porcentaje de IES colombianas según presupuesto



En cuanto al presupuesto, el 84% de las IES colombianas cuenta con partidas presupuestarias para la realización de inversiones y gastos en ciberseguridad. La existencia de asignaciones generales para TI que son usadas parcialmente en acciones de ciberseguridad, representa el 61,3% de la IES, frente al 12,9% que tienen asignadas partidas específicas del presupuesto TI y el 9,7%, que tienen presupuestos diferenciados del área de TI. En función de lo indicado, se puede afirmar que se trata de datos con tendencias similares a los registrados en otros países de Iberoamérica.

Gráfico 77: Nivel de madurez de IES en Colombia según presupuesto

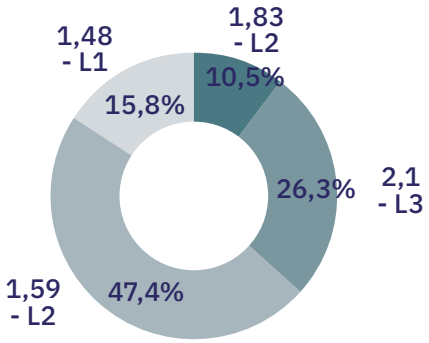


Si comparamos el IMC promedio de las instituciones colombianas según la existencia o no de presupuesto de ciberseguridad, se observa una tendencia ascendente muy clara y definida. Podemos ver como el valor del IMC es más elevado pasando de un valor 1,23 (L1, básico) hasta 1,75 (L2, intermedio) en función de si no se dispone de presupuesto, se dispone de partidas generales o específicas hasta llegar a presupuesto diferenciado del área TI. Se trata de una situación que pone en valor la importancia de apostar por una inversión en ciberseguridad dentro de la estrategia institucional, no solo del área técnica.

Analizando el orden de magnitud de los presupuestos de ciberseguridad encontramos que el 38,7% de las IES colombianas no han indicado el presupuesto de ciberseguridad de su institución.

Por su parte, un 10,5% de las IES que han reportado esta información cuenta con fondos para ciberseguridad equivalente a menos del 5% del presupuesto del área de TI. Un 26,3% afirma encontrarse en el rango entre el 5 y el 10%. Un 47,4% consume entre el 10 y el 20% del presupuesto de informática y el 15,8%, más de ese porcentaje. Esto hace que 6 de cada 10 IES colombianas utilicen más del 10% del presupuesto TI en acciones de ciberseguridad.
La situación media en las IES Iberoamericanas es que el presupuesto tienen una repercusión directa en el IMC de la institución. Es decir, un mayor presupuesto deriva en un mayor valor del IMC. En el caso de Colombia, se observa una situación diferente en los rangos de mayor presupuesto. En concreto, los datos reflejan una reducción del IMC para los presupuestos altos. Esta condición deberá ser analizada en profundidad y realizar un seguimiento de su evolución en futuros años con el objetivo de detectar posibles anomalías o situaciones excepcionales que limiten o bloqueen el crecimiento del nivel de madurez de estas IES.

Gráfico 78: Porcentaje del presupuesto de ciberseguridad en comparación con presupuesto de TI, y nivel de madurez según este porcentaje



<5%
5-10%
10-20%
>20%

Ciberincidentes

Si hablamos del número de IES que han sufrido ciberincidentes en el último año, con afectación de la operación de la institución de forma parcial o total, el porcentaje asciende al 45,2%. Es decir, el 54,8% de las IES en Colombia no ha sufrido ningún tipo de ciberincidente en el último año. Al analizar en mayor detalle, podemos ver que el 19,4% ha sido blanco de al menos un ciberincidente, el 9,7% de entre 2 y 5 ataques anuales y el 16,1%, de más de 5 incidentes. Estos datos presentan diferencias con el promedio iberoamericano, especialmente en el porcentaje de instituciones sin ciberincidentes (Colombia 54,8%, Iberoamérica 38,6%) e instituciones que han sufrido entre 2 y 5 ciberincidentes (Colombia 9,7%, Iberoamérica 22,8%). El resto de grupos, comparten valores con el resto de países analizados.

Gráfico 79: Comparativa ciberincidentes sufridos por IES en el último año en Colombia y en Iberoamérica

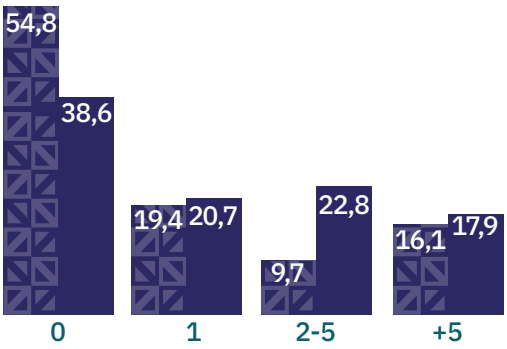
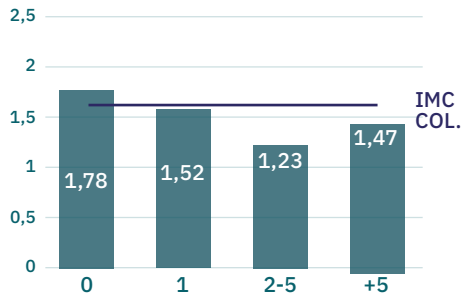


Gráfico 80: Nivel de madurez de IES que sufrieron incidentes en el último año en Colombia



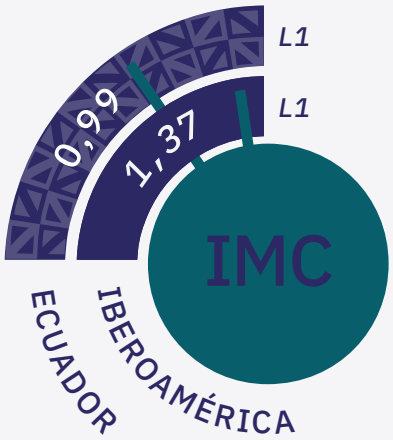
La tendencia normal detectada en la gran mayoría de países analizados muestra una relación directa entre el número de ciberincidentes y un mayor grado de madurez, especialmente a raíz de sufrir un primer ciberincidente. En el caso de Colombia, al igual que ocurre con Chile, la tendencia no sigue esta lógica y muestra un IMC superior en aquellas instituciones que no han sufrido ningún ciberincidente, frente a las que han sufrido menos de cinco ciberincidentes en el año, tal y como muestra la gráfica.

Estas fluctuaciones podrían deberse a la rigurosidad y esfuerzo de crítica interna de las IES que han sufrido más de 2 ciberincidentes al año, haciendo que las respuestas al modelo hayan sido exigentes y por ende, el valor de IMC en esos casos haya sido menor.

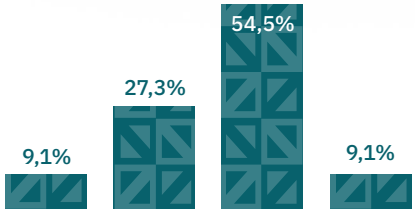
Al igual que con otras situaciones e indicadores ya descritos, esta información tiene por objetivo sentar las bases para un estudio evolutivo de los datos en los siguientes años que permita tener el mayor conocimiento posible de la situación real de Colombia en materia de ciberseguridad en el sector de la educación superior, contribuyendo a crear estrategias y acciones de mayor valor global.

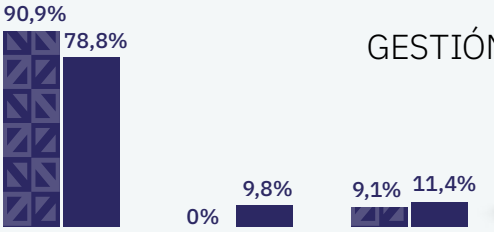
Ecuador.

IMC 0,99 · L1 BÁSICO

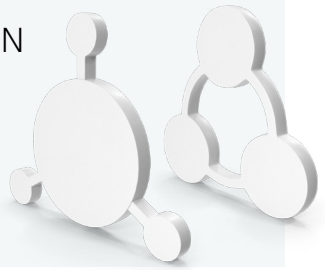


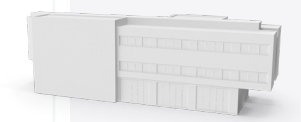
TAMAÑO DE IES



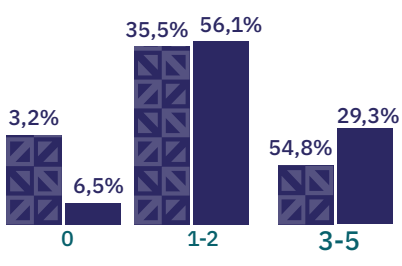


GESTIÓN





TIPO DE IES



TAMAÑO EQUIPOS CIBERSEGURIDAD

PRESUPUESTO

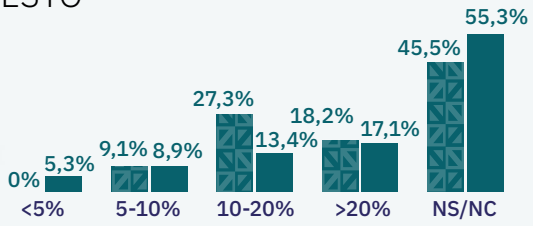
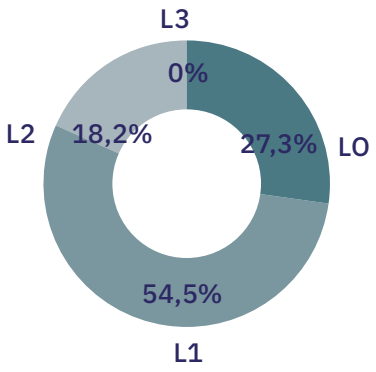


Gráfico 81: Nivel de madurez de IES en Ecuador



Ecuador se sitúa en un nivel de madurez básico (L1), con un IMC de 0,99 puntos. Valoración que ubica a las IES del país 38 puntos por debajo del IMC iberoamericano con el valor de IMC más bajo de los países participantes en esta edición del IMC Iberoamericano.

De las IES encuestadas, el 27% se sitúan en un nivel inicial (L0). El 55% en un nivel básico (L1) y el 18% en un nivel intermedio (L2). Por lo tanto, ninguna de las IES ecuatorianas supera el umbral del nivel de madurez avanzado (L3), siendo el único país, junto a Portugal, donde se da esta situación.

Tipos de Institución

Solo el 18% de las IES está en un nivel intermedio, lo que hace que 8 de cada 10 instituciones de Ecuador presenten un grado de madurez inicial o básico.

Al igual que en la mayoría de los países analizados, estos valores muestran diferencias en función del tipo de institución. En concreto, las IES públicas de Ecuador presentan un IMC de 0,81 (L1), frente a 1,30 (L1) de las IES privadas, dejando a las instituciones privadas 49 puntos por encima de las públicas.

Esto sitúa a las IES públicas de Ecuador en un nivel de madurez básico (L1) muy cercano al umbral del nivel inicial (L0), con acciones poco definidas o poco maduras. Por su parte, las IES privadas de Ecuador se encuentran en el mismo nivel de madurez básico (L1), con un IMC de 1,30. Se sitúen por lo tanto, en un estado de madurez más avanzado y cercano al umbral mínimo del nivel intermedio (L2, 1,50), lo que refleja una evolución hacia la existencia de políticas y procedimientos bien definidos y documentados, implementación de tecnologías de seguridad como sistemas de detección de intrusos o herramientas de cifrado, personal de seguridad dedicado y con cierta especialización y procesos de gestión de riesgos formalizados, entre otros.

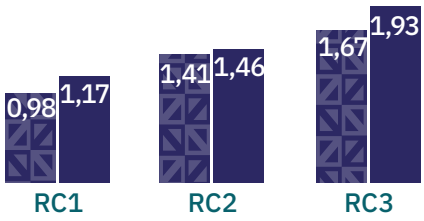
Dominios de aplicación

Si profundizamos en los dominios de aplicación, Ecuador se sitúa por debajo de la media iberoamericana en todos los dominios del modelo de madurez. Los valores con mayor diferencia corresponden al dominio Detectar , Gobernar y Responder y Recuperar, con 53, 50 y 36 puntos de diferencia, respectivamente.

Gráfico 82: Nivel de madurez de IES en Ecuador según el dominio

Comparando las IES públicas y privadas a nivel de dominios, las diferencias se mantienen similares al IMC global, con valores más altos en las instituciones privadas y diferencias situadas en torno a los 50 puntos en todos los dominios. Mención especial requieren las acciones de detección (dominio Detectar), donde las diferencias entre IES públicas y privadas adquieren superan los 80 puntos, dejando a las públicas en clara desventaja en este sentido.

Gráfico 83: Nivel de madurez de IES en Ecuador según el commponente



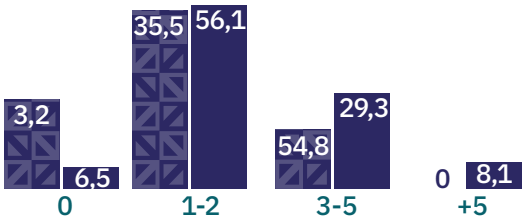
Al igual que sucede en la gran mayoría de países analizados, en términos generales, las IES ecuatorianas afrontan la ciberseguridad desde una perspectiva operativa (RC3), donde priman las acciones de prevención y defensa, al igual que la mayoría de los países analizados. Así mismo, los datos muestran una fuerte correlación entre los indicadores que analizan la normativa y procedimientos de seguridad, componente RC2 y el componente RC1, referido a la parte de planificación y concienciación en ciberseguridad de los diferentes actores de la comunidad universitaria.

Tabla 30: Nivel de madurez de cada dominio en función del tipo de IES

	GLOBAL	GB	ID	PR	DE	REyRC
PRIVADA	1,30	1,39	1,08	1,50	1,47	1,04
PÚBLICA	0,81	0,67	0,90	1,27	0,64	0,57
DIFERENCIA	0,49	0,63	0,18	0,23	0,83	0,47

Equipos de ciberseguridad

Gráfico 84: Composición del equipo de ciberseguridad en función del porcentaje de IES ecuatorianas



Igualmente, crear y consolidar equipos de ciberseguridad en las IES es un reto considerable, capaz de influir en el avance del nivel de madurez en ciberseguridad dentro de las instituciones académicas en Ecuador. Según los datos recogidos, el 72,7% de las IES en Ecuador cuentan con equipos de ciberseguridad específicos, frente al 27,3% que no dispone de equipos específicos de ciberseguridad (valor muy superior a la media iberoamericana situada en el 6,5%).

La mayoría de IES ecuatorianas (54,5%) dispone de equipos de 1 o 2 personas. El 18,2% tiene equipos de 3 a 5 personas y ninguna de las instituciones participantes dispone de equipos de más de 5 personas. En comparación con la media iberoamericana, Ecuador presenta un 21% más de instituciones que no disponen de equipos de ciberseguridad.

Gráfico 85: Nivel de madurez de las IES ecuatorianas según la composición de sus equipos de ciberseguridad

Si comparamos el IMC de las IES ecuatorianas en función del número de personas que componen el equipo de ciberseguridad, podemos observar una clara relación entre ambos indicadores. En concreto, aquellas instituciones que no cuentan con equipos de ciberseguridad presentan un nivel de madurez inicial (L0), lo que refleja que las prácticas de ciberseguridad no son una prioridad en esas instituciones. Por su parte, las IES que cuentan con pequeños equipos de 1 o 2 personas incrementan su nivel de madurez a un nivel básico (L1), implementando prácticas básicas y no formalizadas, frente a las instituciones con equipos de más de 3 personas que suben a un nivel intermedio (L2) y presentan una gestión y gobierno de la ciberseguridad más maduro.

Tabla 31: Comparación entre IES ecuatorianas, iberoamericanas e IMC según integración del equipo de ciberseguridad

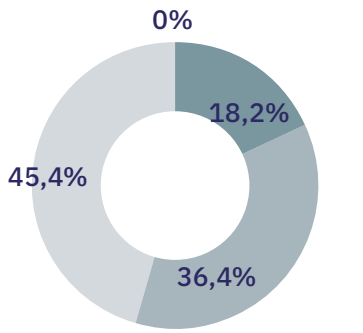
	0 MIEMBROS	1-2 MIEMBROS	3-5 MIEMBROS	+5 MIEMBROS
ECUADOR	27,3	54,5	18	0
IBEROAMÉRICA	6,5	56,1	29,3	8,10
IMC	0,50 L0	1,03 L1	1,61 L2	

Presupuestos de ciberseguridad

En cuanto al presupuesto, el 54,6% de las IES en Ecuador cuenta con partidas presupuestarias para la realización de inversiones y gastos en ciberseguridad, frente al 45,4% que no disponen de presupuesto de ningún tipo para ciberseguridad.

Según las respuestas obtenidas, el 18,2% manifiesta disponer de ciertas asignaciones específicas para ciberseguridad disponibles dentro del presupuesto del área IT. Por su parte, el 36,4% suele usar partidas presupuestarias generales de Ti y ninguna institución participante cuenta con presupuesto diferenciado.

Gráfico 86: Porcentaje de IES ecuatorianas según presupuesto



Si comparamos el IMC promedio de las instituciones ecuatorianas según la existencia o no de presupuesto de ciberseguridad, se observa una tendencia ascendente muy clara y definida. Podemos ver cómo se escala desde un nivel inicial (L0) hasta situarse cerca del nivel intermedio (L2), en función de si no se dispone de presupuesto o se dispone de partidas generales o específicas.

Gráfico 87: Nivel de madurez de IES en Ecuador según presupuesto

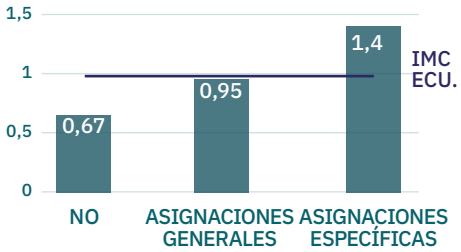
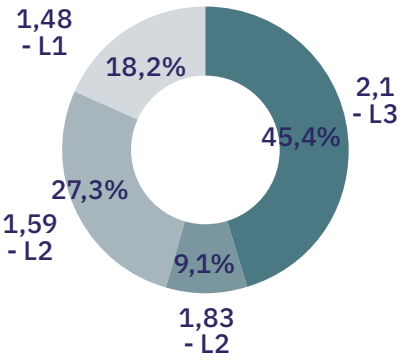


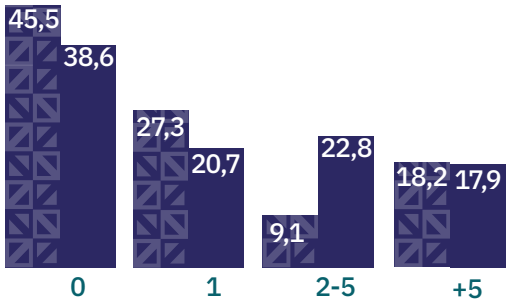
Gráfico 88: Porcentaje del presupuesto de ciberseguridad en comparación con presupuesto de TI, y nivel de madurez según este porcentaje



Analizando el orden de magnitud de los presupuestos de ciberseguridad encontramos que el 45,4% de las instituciones invierte un importe inferior al 5% del presupuesto de IT. Siendo el 9,1% de las IES las que invierten entre el 5 y el 10% del presupuesto del área IT, el 27,3% en el rango del 10-20% y el 18,2% las que realizan un gasto equivalente a más del 20% de presupuesto que la institución asigna al área IT.

Ciberincidentes

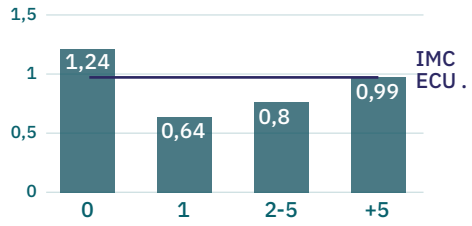
Gráfico 89: Comparativa ciberincidentes sufridos por IES en el último año en Ecuador y en Iberoamérica



Si hablamos del número de IES que han sufrido ciberincidentes en el último año, con afectación de la operación de la institución de forma parcial o total, el porcentaje asciende al 54,6%. Es decir, cerca de 6 de cada 10 IES en Ecuador ha sufrido algún tipo de incidente en el último año. Al analizar en mayor detalle, podemos ver que el 27,3% ha sido blanco de al menos un ciberincidente, el 9,1% también ha sufrido entre 2 y 5 incidentes anuales y el 18,2%, más de 5. Son valores muy similares a la media iberoamericana, donde el promedio de IES que han reportado algún incidente es de 61,4%, un 6,8% superior que en Ecuador.

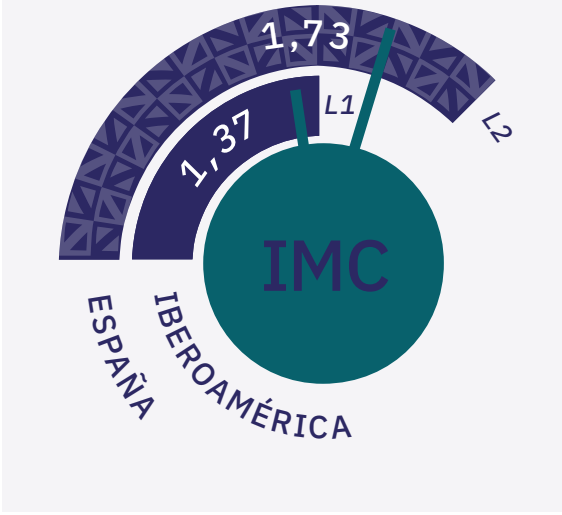
La tendencia normal detectada en la gran mayoría de países analizados, muestra una relación directa entre el número de ciberincidentes y un mayor grado de madurez, especialmente a raíz de sufrir un primer caso. En Ecuador, la tendencia no sigue esta lógica y muestra un valor superior en aquellas instituciones que no han sufrido ningún ciberincidente frente a las que han sufrido algún evento de esta naturaleza en el año. Entre las instituciones que han sufrido ciberincidentes, su nivel de madurez se incrementa desde 0,64 a 0,99, en función del número de casos ocurridos.

Gráfico 90: Nivel de madurez de IES que sufrieron incidentes en el último año en Ecuador

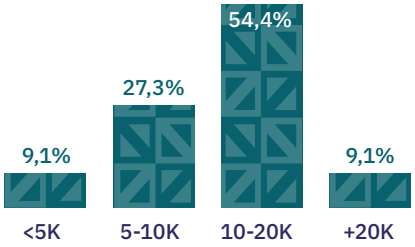


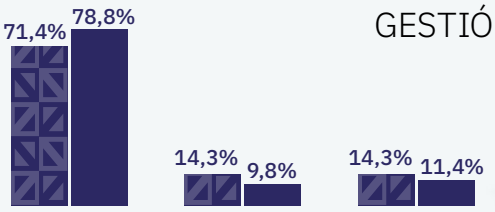
España.

IMC 1,73 · L2 INTERMEDIO

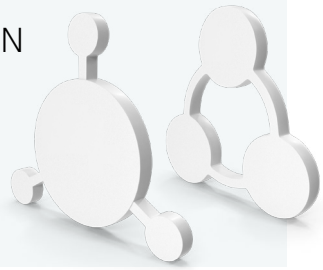


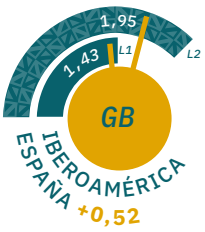
TAMAÑO DE IES



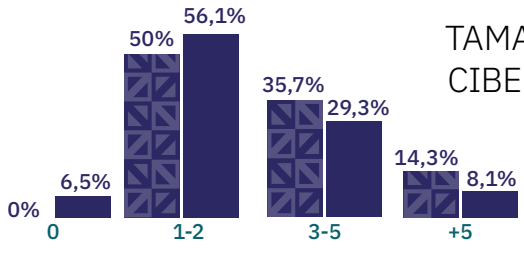


GESTIÓN

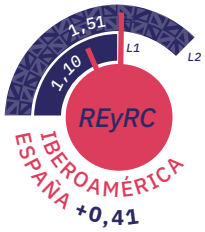




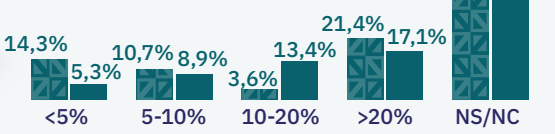
TIPO DE IES



TAMAÑO EQUIPOS CIBERSEGURIDAD



PRESUPUESTO

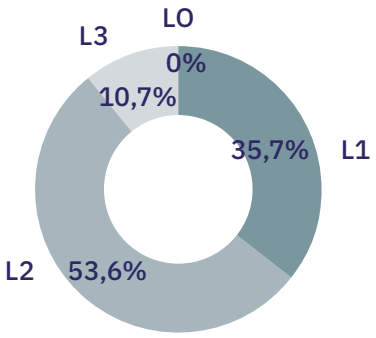


España obtiene un nivel de madurez L2, con un IMC de 1,73 puntos, 36 puntos por encima del IMC iberoamericano.

España se sitúa como el país con mayor nivel de madurez.

De las IES encuestadas en España, todas presentan un nivel de madurez superior a L0, situando al 35,7% dentro del nivel de madurez básico (L1), un 53,6% con un nivel intermedio (L2) y un 10,7% en nivel avanzado (L3). Se trata de valores que sitúan a 6 de cada 10 instituciones españolas dentro de un nivel de madurez intermedio o avanzado, siendo la media iberoamericana del 40,8%.

Gráfico 91: Nivel de madurez de IES en España



Tipos de Institución

Al igual que en la mayoría de los países analizados, estos valores muestran ligeras diferencias en función del tipo de institución. En concreto, las IES públicas españolas presentan un IMC de 1,72, frente a 1,82 de las universidades privadas. En ambos casos, el nivel de madurez es intermedio (L2), lo que refleja la existencia de políticas y procedimientos bien definidos y documentados, la implementación de tecnologías de seguridad como sistemas de detección de intrusos o herramientas de cifrado, personal de seguridad dedicado y con cierta especialización y procesos de gestión de riesgos formalizados, entre otros. Sin embargo, se encuentra todavía a medio camino para la consecución de un nivel de madurez avanzado y delimitado por el umbral de 2,25.

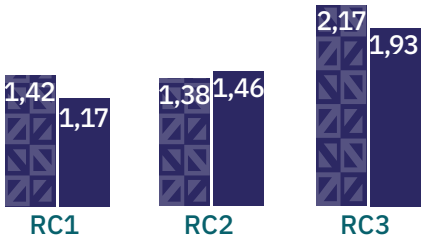
Dominios de aplicación

Si profundizamos en los dominios de aplicación, España supera la media iberoamericana en los 5 dominios del modelo de madurez. Los valores con mayor diferencia son los correspondientes al dominio Gobernar (GB), Detectar (DE) y Responder y Recuperar (REyRC) con 52, 47 y 41 puntos de diferencia, respectivamente.

Gráfico 92: Nivel de madurez de IES en España según el dominio

Las diferencias entre instituciones públicas y privadas se mantienen similares al IMC global a excepción del dominio Gobernar (GB), donde las públicas superan en 19 puntos a las privadas. Esta condición viene derivada del marco de cumplimiento normativo de España. El Esquema Nacional de Seguridad, de aplicación a todo el Sector Público, ofrece un marco común de principios básicos, requisitos y medidas de seguridad para una protección adecuada de la información tratada y los servicios prestados. En este marco, las acciones incluidas dentro del dominio Gobernar (GB) están ampliamente desarrolladas, lo que justifica el grado de madurez de las universidades públicas españolas en esta materia.

Gráfico 93: Nivel de madurez de IES en España según el commponente



El ENS se consolida como un elemento vertebrador de la ciberseguridad de las universidades españolas.

En términos generales, las IES españolas afrontan la ciberseguridad desde una perspectiva operativa (RC3), donde priman las acciones de prevención y defensa, al igual que la mayoría de los países analizados. Así mismo, los datos muestran una fuerte correlación entre los indicadores que analizan la normativa y procedimientos de seguridad, componente RC2 y el componente RC1, referido a la parte de planificación y concienciación en ciberseguridad de los diferentes actores de la comunidad universitaria.

Tabla 32: Nivel de madurez de cada dominio en función del tipo de IES

	GLOBAL	GB	ID	PR	DE	REyRC
PRIVADA	1,82	1,79	1,53	1,83	1,75	1,58
PÚBLICA	1,72	1,98	1,45	1,79	1,87	1,50
DIFERENCIA	-0,10	-0,19	-0,08	-0,04	-0,12	0,08

Equipos de ciberseguridad

Por otra parte, la creación y consolidación de equipos de ciberseguridad dentro de las IES es un reto importante y que puede marcar el transcurrir de la evolución del grado de madurez en ciberseguridad dentro de las IES españolas. Según los datos recogidos, en el 50% de las IES, el equipo de ciberseguridad se compone de 1 o 2 personas, el 35,7% cuenta con entre 3 y 5 personas dedicadas y tan solo el 14,3% tiene equipos de más de 5 miembros. Estos valores sitúan a España como el único país del estudio donde todas las IES participantes han indicado que disponen de equipo de ciberseguridad. Además, se puede observar cómo los equipos compuestos por una o dos personas son un 6% inferiores a la media iberoamericana, frente a los equipos de más personas que se ubican un 6% por encima de la media.

Si comparamos el IMC de las IES españolas en función del número de personas que componen el equipo de ciberseguridad, podemos observar una clara relación entre ambos indicadores. En concreto, aquellas instituciones que cuentan con equipos de 1 o 2 personas tienen un nivel de madurez intermedio (L2) pero con valores muy cercanos a la frontera con L1. Por su parte, las que tienen equipos de entre 3 y 5 personas, consolidan el nivel intermedio (L2). Por último, aquellas que han creado equipos de más de 5 personas consiguen un nivel de madurez avanzado (L3).

Gráfico 94: Composición del equipo de ciberseguridad en función del porcentaje de IES españolas

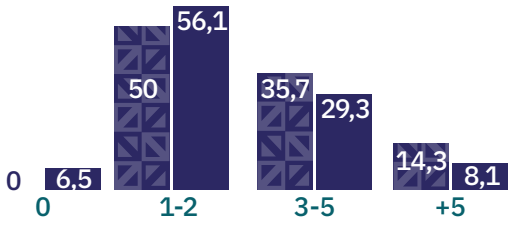


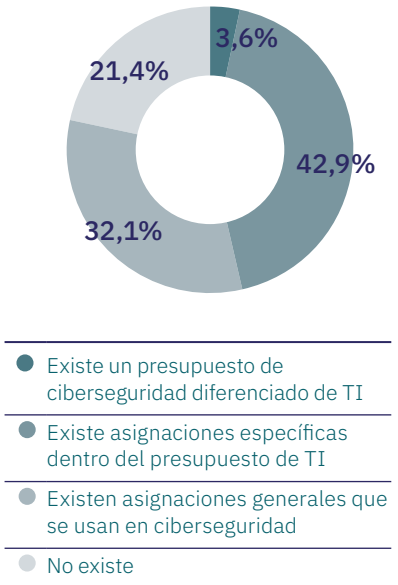
Gráfico 95: Nivel de madurez de las IES españolas según la composición de sus equipos de ciberseguridad

Tabla 32: Comparación entre IES españolas, iberoamericanas e IMC según integración del equipo de ciberseguridad

	0 MIEMBROS	1-2 MIEMBROS	3-5 MIEMBROS	+5 MIEMBROS
COLOMBIA	3,2	35,5	54,8	6,5
IBEROAMÉRICA	6,5	56,1	29,3	8,10
IMC	1,03 L1	1,54 L2	1,66 L2	2,03 L2

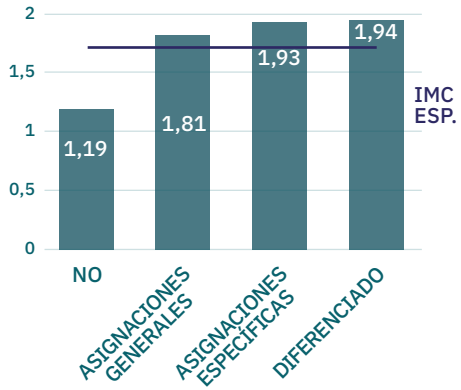
Presupuestos de ciberseguridad

Gráfico 96: Porcentaje de IES españolas según presupuesto



En cuanto al presupuesto, 8 de cada 10 universidades españolas cuenta con partidas presupuestarias para la realización de inversiones y gastos en ciberseguridad. Sin embargo, tan solo el 3,6% de estas universidades tiene un presupuesto de ciberseguridad diferenciado del presupuesto del área de TI. Sin embargo, la tendencia es contar con partidas específicas dentro del presupuesto del dicha área (42,9%) o usar parcialmente partidas presupuestarias generales para ciberseguridad (32,1%).

Gráfico 97: Nivel de madurez de IES en España según presupuesto



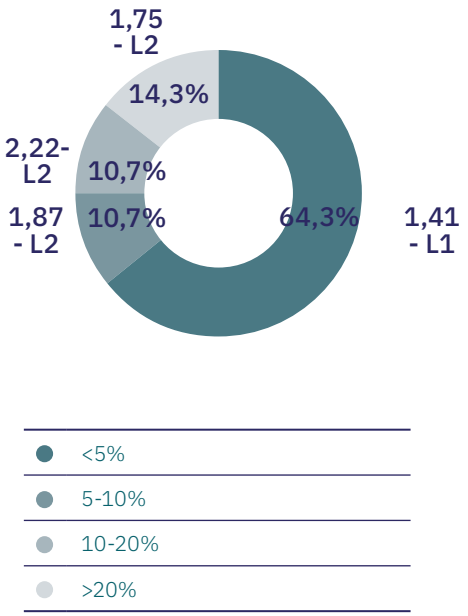
Si comparamos el IMC promedio de las IES según la existencia de presupuesto de ciberseguridad, podemos ver como aquellas instituciones que no cuentan con presupuesto de ningún tipo asignado a ciberseguridad muestran importantes diferencias en el nivel de madurez (62 puntos), quedando en un nivel de madurez básico (L1), frente a valores intermedios (L2) del resto.

Así mismo, el contar con asignaciones específicas para ciberseguridad dentro del presupuesto del área TI o contar con un presupuesto independiente para ciberseguridad hace que estas IES suban su nivel de madurez de forma moderada, tal como podemos apreciar en la gráfica.

En cuanto al orden de magnitud del presupuesto asignado a ciberseguridad, el 64,3% de las universidades españolas afirman contar con una asignación presupuestaria para ciberseguridad en un orden de magnitud menor del 5% del presupuesto total del área de TI. Un 10,71% estiman este valor en un rango entre el 5-10%, un 10,7% en el rango 10-20% y un 14,3% supera el umbral del 20% del presupuesto del área TI.

Como podemos apreciar en la siguiente gráfica, el presupuesto tiene una repercusión directa en el grado de madurez de las universidades. Según los datos obtenidos, aquellas IES que cuentan con un presupuesto de ciberseguridad inferior al 5% del presupuesto total del área TI presentan un IMC de 1,41 (L1, nivel de madurez básico), frente al nivel al 1,87 (L2, nivel intermedio) de las instituciones que cuentan con un presupuesto de ciberseguridad en el rango del 5% al 10%, o el 2,22 (L2, nivel intermedio) de las IES con presupuesto entre el 10% y el 20%.

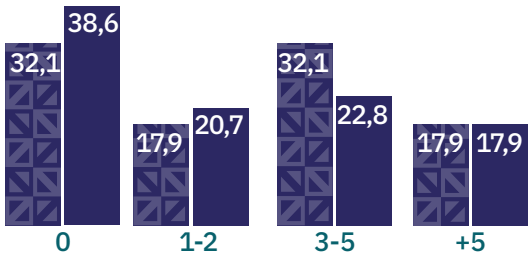
Gráfico 98: Porcentaje del presupuesto de ciberseguridad en comparación con presupuesto de TI, y nivel de madurez según este porcentaje



Ciberincidentes

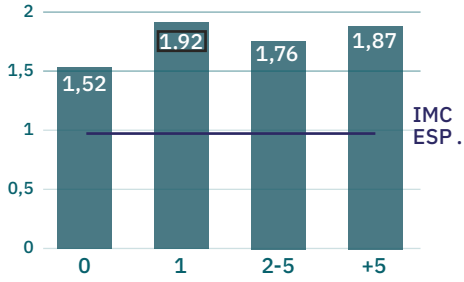
En cuanto al número de IES españolas que han sufrido ciberincidentes en el último año, con afectación de la operación de la institución de forma parcial o total, el porcentaje asciende al 67,86%. Es decir, cerca de 7 de cada 10 instituciones ha sufrido algún tipo de incidente en el último año. Al analizar en mayor detalle, podemos ver que el 32,1% ha sufrido entre 2 y 5 ataques anuales y el 17,9% más de 5 incidentes. Son valores ligeramente superiores a la media iberoamericana, donde el promedio de IES que han reportado algún incidente es de 61,38%, un 6,5% inferior que en España.

Gráfico 99: Comparativa ciberincidentes sufridos por IES en el último año en España y en Iberoamérica



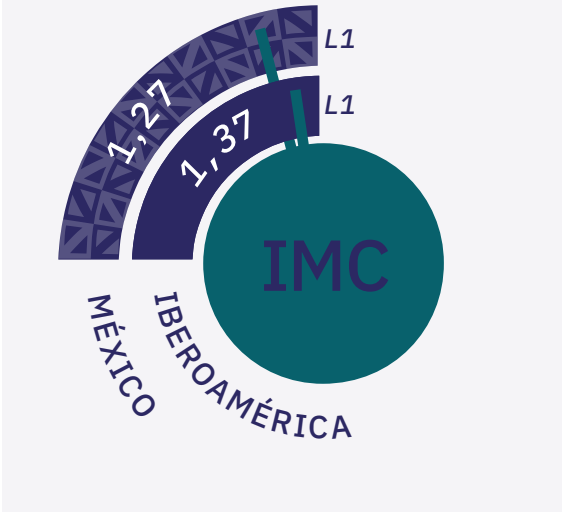
Los ciberincidentes de las IES tienen un impacto directo en el IMC. En concreto, se observa un incremento importante en las instituciones que han tenido alguna incidencia en el último año, en especial en aquellas que reciben su primer ciberincidente, donde se plantea un refuerzo de la ciberseguridad de la institución. Como consecuencia de esta situación, el IMC sube en promedio 40 puntos.

Gráfico 100: Nivel de madurez de IES que sufrieron incidentes en el último año en España

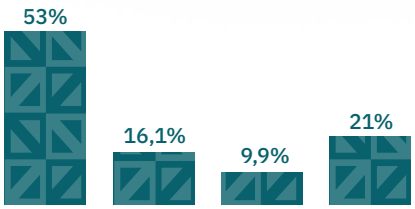


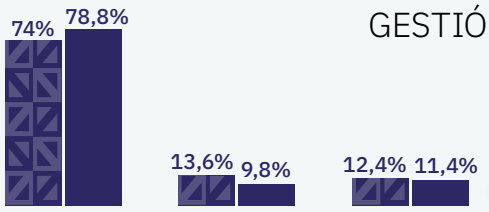
México.

IMC 1,27 · L1 BÁSICO

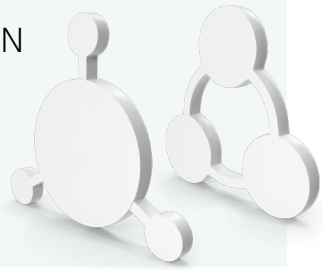


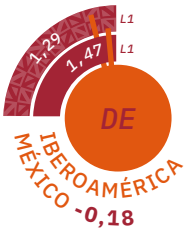
TAMAÑO DE IES

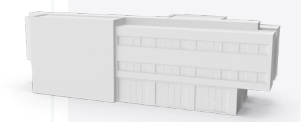




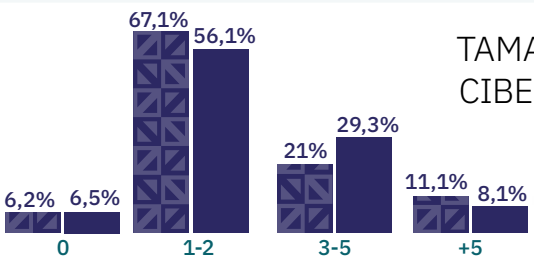
GESTIÓN





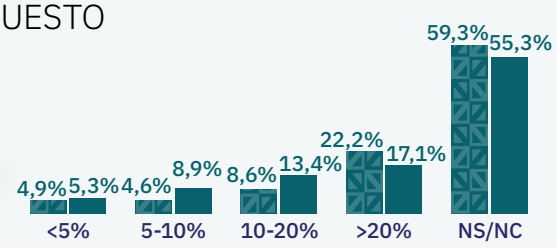


TIPO DE IES



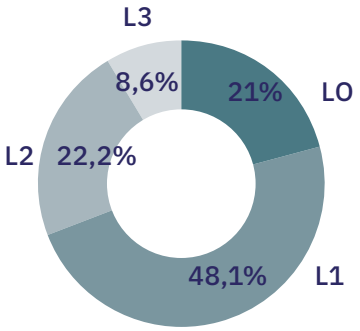
TAMAÑO EQUIPOS CIBERSEGURIDAD

PRESUPUESTO



México se sitúa en un nivel de madurez básico (L1) con un IMC de 1,27 puntos, a 23 puntos del nivel de madurez intermedio (L2). Esta valoración ubica a las IES del país diez puntos por debajo del IMC iberoamericano.

Gráfico 101: Nivel de madurez de IES en México



De las IES encuestadas en México, el 21% se sitúa en un nivel inicial (L0), un 48% en un nivel básico (L1), el 22%, en un nivel intermedio (L2) y el 9% restante en un nivel avanzado (L3). Son valores que sitúan al 30,80% de las IES mexicanas dentro de un nivel de madurez intermedio o avanzado, siendo la media iberoamericana del 40,8%.

Tipos de Institución

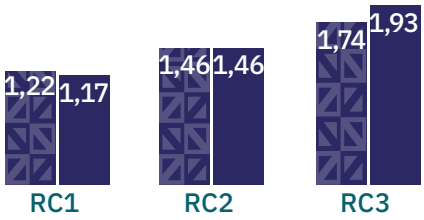
Al igual que en la mayoría de los países analizados, el valor del IMC obtenido muestra diferencias en función del tipo de institución. En concreto, las IES públicas presentan un IMC de 1,24 (L1), frente a 1,41 (L1) de las IES privadas. Esto sitúa a las IES de México en un nivel de madurez básico (L1), con acciones poco definidas o poco maduras, con instituciones privadas cerca del umbral mínimo para el nivel intermedio (1,49), lo que refleja una mayor madurez de estas frente a homólogas públicas.

Dominios de aplicación

Si profundizamos en los dominios de aplicación, México queda por debajo de la media iberoamericana en cuatro de los 5 dominios del modelo de madurez. El dominio Identificar (ID) es el único dominio del IMC dónde México ha obtenido un valor superior al promedio de Iberoamérica. Los valores con mayor diferencia son los correspondientes al dominio Detectar (DE), Gobernar (GB) y Responder y Recuperar (REyRC) con 18, 15 y 12 puntos de diferencia, respectivamente.

Gráfico 102: Nivel de madurez de IES en México según el dominio

Gráfico 103: Nivel de madurez de IES en México según el commponente



Comparando las IES públicas y privadas a nivel de dominios, las diferencias se mantienen similares al IMC global, con valores más altos en las instituciones privadas y diferencias situadas en torno a los 15 puntos en todos los dominios.

En términos generales y de forma similar a la mayoría de países analizados, las IES mexicanas afrontan la ciberseguridad desde una perspectiva operativa (RC3), donde priman las acciones de prevención y defensa, al igual que la mayoría de los países analizados. Así mismo, los datos muestran una fuerte correlación entre los indicadores que analizan la normativa y procedimientos de seguridad, componente RC2 y el componente RC1, referido a la parte de planificación y concienciación en ciberseguridad de los diferentes actores de la comunidad universitaria.

Tabla X: Nivel de madurez de cada dominio en función del tipo de IES

	GLOBAL	GB	ID	PR	DE	REyRC
PRIVADA	1,41	1,57	1,49	1,52	1,43	1,05
PÚBLICA	1,24	1,22	1,31	1,40	1,26	1,00
DIFERENCIA	0,17	0,35	0,18	0,12	0,17	0,05

Equipos de ciberseguridad

Como hemos podido ver en otros países de estudio, la creación y consolidación de equipos de ciberseguridad dentro de las universidades es un reto importante y que puede marcar el transcurrir de la evolución del grado de madurez en ciberseguridad dentro de nuestras instituciones. Según los datos recogidos, el 93,8% de las IES mexicanas cuenta con equipos de ciberseguridad específicos. De ellas, el 61,7% son equipos de ciberseguridad de 1 o 2 personas, el 21% de 3 a 5 personas y el 11,1%, de más de 5 personas.

En comparación con la media iberoamericana, México sigue una distribución prácticamente idéntica. Se aprecian ligeras desviaciones en el alza del número de equipos de 1 o 2 personas (5%) y en equipos de más de 5 personas (3%), y en contrapartida, un menor porcentaje de los equipos de 3 a 5 personas (8%).

Si comparamos el IMC de las IES mexicanas en función del número de personas que componen el equipo de ciberseguridad, podemos observar una clara relación entre ambos indicadores. En concreto, aquellas instituciones que no cuentan con equipos de ciberseguridad presentan un nivel de madurez inicial (L0), lo que refleja que las prácticas de ciberseguridad no son una prioridad en esas instituciones. Por su parte, las instituciones que cuentan con pequeños equipos de 1 o 2 personas incrementan su nivel de madurez a un nivel básico (L1), implementando prácticas básicas y no formalizadas, frente a las instituciones con equipos de 3 más de 5 personas que suben a un nivel intermedio (L2), y presentan una gestión y gobierno de la ciberseguridad más maduro.

Gráfico 104: Composición del equipo de ciberseguridad en función del porcentaje de IES mexicanas

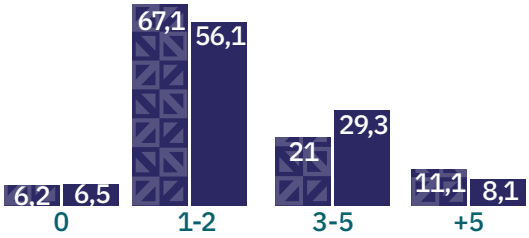


Gráfico 105: Nivel de madurez de las IES españolas según la composición de sus equipos de ciberseguridad

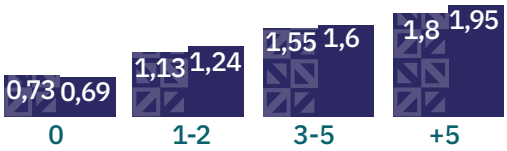
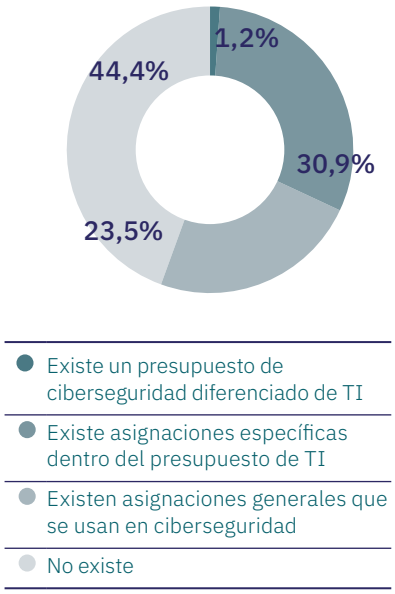


Tabla 33: Comparación entre IES mexicanas, iberoamericanas e IMC según integración del equipo de ciberseguridad

	0 MIEMBROS	1-2 MIEMBROS	3-5 MIEMBROS	+5 MIEMBROS
MÉXICO	6,2	61,7	21	11,1
IBEROAMÉRICA	6,5	56,1	29,3	8,10
IMC	0,73 L0	1,13 L1	1,55 L2	1,80 L2

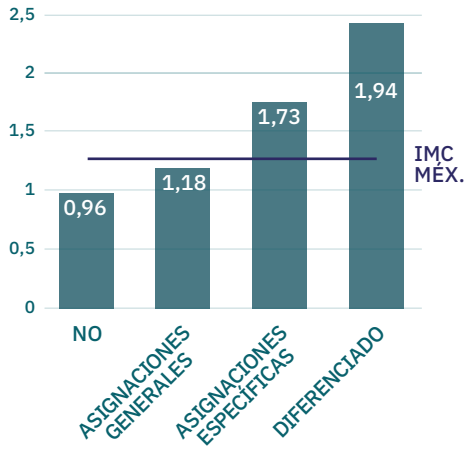
Presupuestos de ciberseguridad

Gráfico 106: Porcentaje de IES mexicanas según presupuesto



En cuanto al presupuesto, 6 de cada 10 IES mexicanas cuentan con partidas presupuestarias para la realización de inversiones y gastos en ciberseguridad y en su gran mayoría, se utilizan partidas del presupuesto del área IT. En concreto, el 23,5% usan asignaciones generales del área TI para cuestiones de ciberseguridad, el 30,9% ha reservado recursos dentro del presupuesto de TI y solo el 1,2% tiene un presupuesto diferenciado. Como dato importante y que requerirá un seguimiento en años sucesivos, es el alto porcentaje de IES que no disponen de ningún tipo de presupuesto para ciberseguridad y que en esta edición asciende al 44,4% de las instituciones en México.

Gráfico 107: Nivel de madurez de IES en México según presupuesto



Si comparamos el IMC promedio según la existencia o no de presupuesto de ciberseguridad, se observa una tendencia ascendente clara y definida. Vemos cómo se escala desde un nivel básico (L1) hasta un nivel avanzado (L3) en función de si no se dispone de presupuesto, se dispone de partidas generales o específicas hasta llegar a presupuesto diferenciado del área TI. La situación que pone en valor la importancia de apostar por una inversión en ciberseguridad dentro de la estrategia institucional, no solo del área técnica.

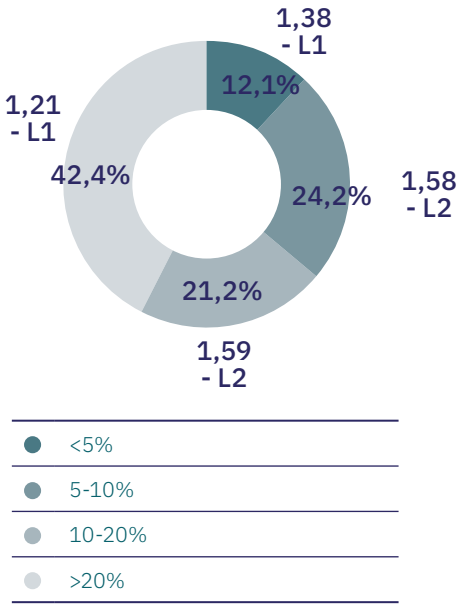
Analizando el orden de magnitud de los presupuestos de ciberseguridad, cerca del 60% de las IES mexicanas encuestadas no han indicado el presupuesto de ciberseguridad de su institución.

Por su parte, las IES que han reportado esta información, se observa que el 12,1% cuenta con fondos para ciberseguridad equivalentes a menos del 5% del presupuesto del área TI. Un 24,2% afirma encontrarse en el rango entre el 5 y el 10%, un 21,2% consume entre el 10 y el 20% del presupuesto de informática y el

42,4%, una cantidad mayor a ese porcentaje. Esto hace que 6 de cada 10 IES de México utilicen más del 10% del presupuesto de TI en acciones de ciberseguridad.

Como podemos apreciar en la siguiente gráfica, el presupuesto tiene una repercusión directa en el grado de madurez de las universidades. Según los datos obtenidos, aquellas instituciones que cuentan con un presupuesto de ciberseguridad inferior al 5% del presupuesto total del área de TI presentan un IMC de 1,38 (L1, nivel de madurez básico), frente al nivel 1,58 y 1,59 (L2, nivel intermedio) de las IES que cuentan con un presupuesto de ciberseguridad en el rango del 5% al 10% y del 10% al 20% respectivamente. Como características adicionales y comunes a gran parte de los países de estudio, los presupuestos superiores al 20% vienen acompañados de valores de IMC más bajos. Este dato será objeto de estudio en futuras ediciones y podría estar derivado de un mayor pensamiento autocrítico de estas instituciones.

Gráfico 108: Porcentaje del presupuesto de ciberseguridad en comparación con presupuesto de TI, y nivel de madurez según este porcentaje



Ciberincidentes

Si hablamos del número de IES que han sufrido ciberincidentes en el último año, con afectación de la operación de la institución de forma parcial o total, el porcentaje asciende al 64,2%. Es decir, 6 de cada 10 IES en México ha sufrido algún tipo de incidente en el último año. Al revisar en mayor detalle, podemos ver que el 21% ha sido blanco de al menos un ciberincidente, el 25,9%, entre 2 y 5 ataques anuales y el 17,3%, más de 5 incidentes. Son valores muy similares a la media iberoamericana, donde el promedio de IES que han reportado algún incidente es de 61,4%, haciendo que México esté por encima del valor medio un 2,8%.

La tendencia normal detectada en la gran mayoría de países analizados muestra una relación directa entre el número de ciberincidentes y un mayor grado de madurez, especialmente a raíz de sufrir un primer caso. En México, se mantiene esta tendencia hacia un mayor nivel de madurez a mayor número de ciberincidentes sufridos, con la excepción del primero, ya que las IES que han sufrido un ciberincidente este año muestran un IMC más bajo. Esta situación puede ser anecdótica pero deberá ser evaluada en posteriores ediciones del IMC.

Gráfico 109: Comparativa ciberincidentes sufridos por IES en el último año en México y en Iberoamérica

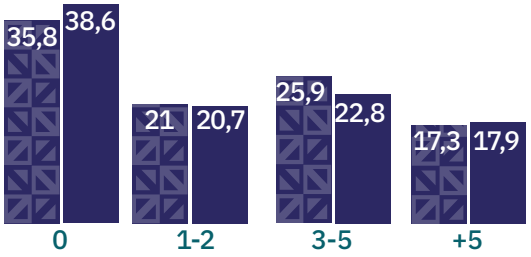
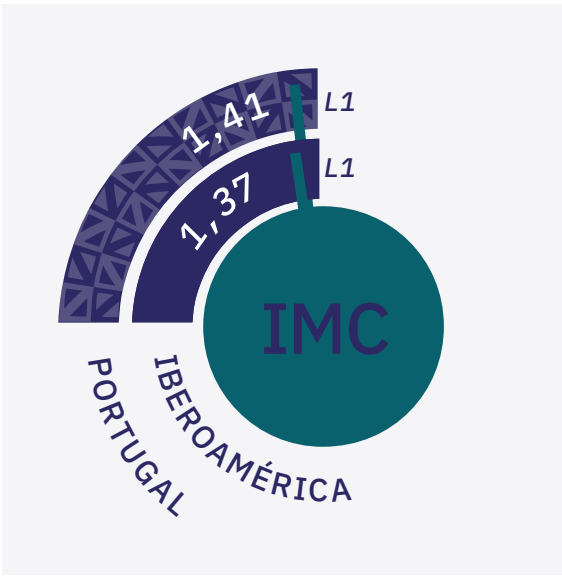


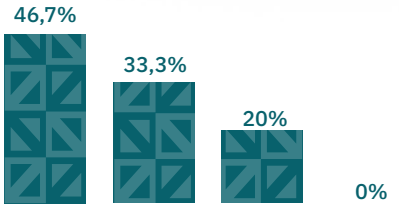
Gráfico 110: Nivel de madurez de IES que sufrieron incidentes en el último año en México

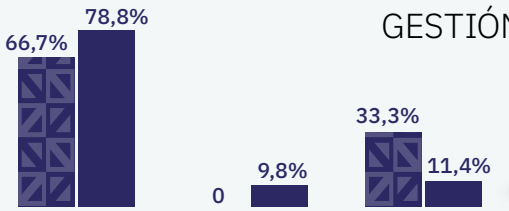
Portugal.

IMC 1,41 · L1 BÁSICO

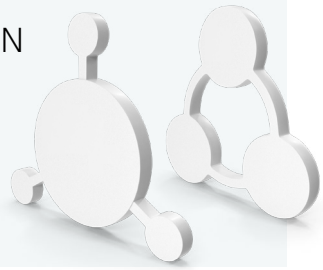


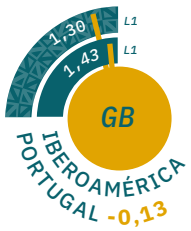
TAMAÑO DE IES

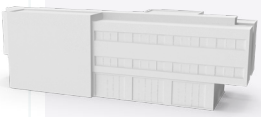


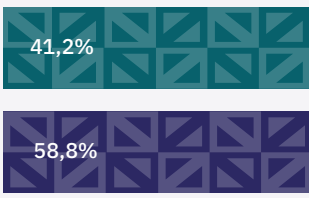


GESTIÓN

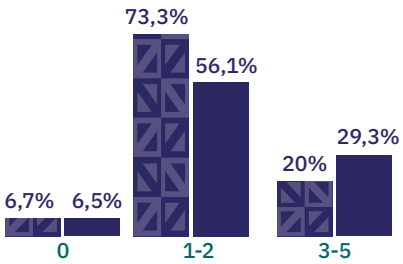




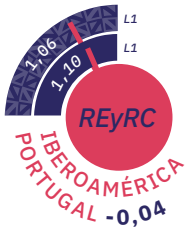




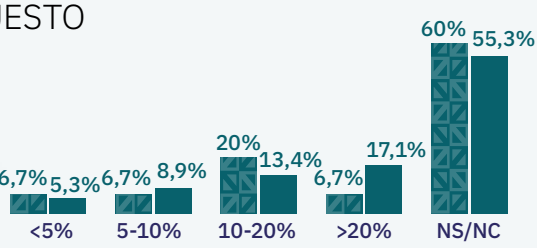
TIPO DE IES



TAMAÑO EQUIPOS CIBERSEGURIDAD

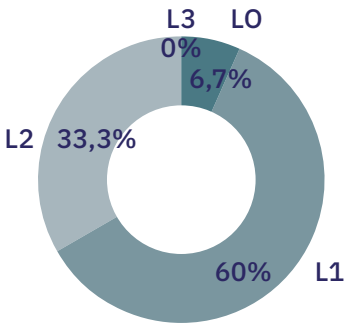


PRESUPUESTO



Portugal se sitúa en un nivel de madurez básico (L1) con un IMC de 1,41 puntos, a tan solo 9 puntos del nivel de madurez intermedio (L2). Esta valoración ubica a las IES del país 4 puntos por encima del IMC iberoamericano (1,37).

Gráfico 111: Nivel de madurez de IES en Portugal



De las IES encuestadas en Portugal, el 7% se sitúan en un nivel inicial (L0), un 60% en un nivel básico (L1), y el 33% en un nivel intermedio (L2). Por lo tanto, el nivel de madurez avanzado (L3) queda desierto y ninguna de las IES relevadas ha obtenido puntuación suficiente para alcanzar este nivel de madurez. Esto hace que Portugal cuente con un 33% de IES en nivel de madurez intermedio o avanzado, siendo la media iberoamericana del 40,8%, una diferencia que sitúa a Portugal un 7,8% por debajo de este valor.

Tipos de Institución

Al igual que en la mayoría de los países analizados, el valor del IMC obtenido muestra diferencias en función del tipo de institución. En concreto, las IES públicas presentan un IMC de 1,39 (L1) frente a 1,53 (L2) de las IES privadas.

Esto sitúa a las IES públicas de Portugal en un nivel de madurez básico (L1) muy cercano a un nivel L2 (a 10 puntos), lo que refleja acciones poco definidas o poco maduras con clara tendencia hacia una mejora hacia un nivel superior de madurez.

Por su parte, las IES privadas de Portugal muestran un nivel de madurez intermedio (L2) lo que refleja la existencia de políticas y procedimientos bien definidos y documentados, implementación de tecnologías de seguridad como sistemas de detección de intrusos o herramientas de cifrado, personal de seguridad dedicado y con cierta especialización y procesos de gestión de riesgos formalizados, entre otros.

Dominios de aplicación

Si profundizamos en los dominios de aplicación, Portugal queda por encima de la media iberoamericana en tres de los cinco dominios del modelo de madurez. Es decir, Portugal se sitúa por encima del promedio en acciones de Identificar (ID), Prevenir (PR) y Detectar (DE) con valores ligeramente superiores a la media de cada dominio. Por otro lado, el dominio Gobernar (GB) y Responder y Recuperar (REyRC) quedan por debajo de la media a 13 y 4 puntos de diferencia, respectivamente.

Por lo tanto, Portugal presenta un IMC por dominio muy próximo al promedio de Iberoamérica y con una clara proyección hacia las acciones de Detección (DE), donde las diferencias con la media son más abultadas y llegan a los 23 puntos de diferencia.

Gráfico 112: Nivel de madurez de IES en Portugal según el dominio

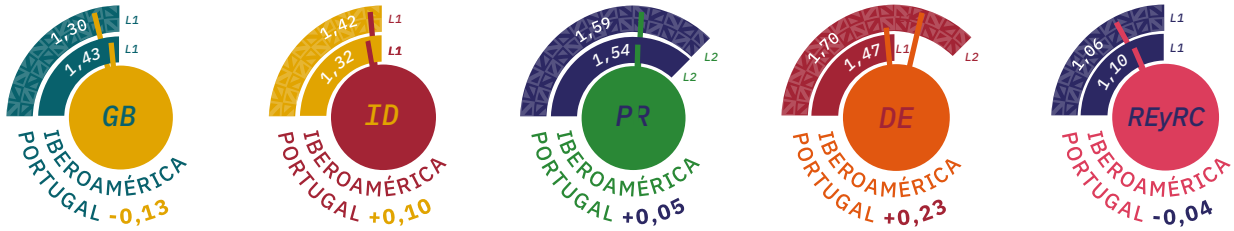
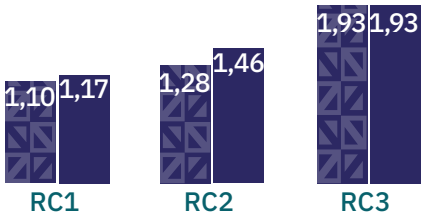


Gráfico 113: Nivel de madurez de IES en Portugal según el commponente



Comparando las IES públicas y privadas a nivel de dominios, las diferencias se mantienen similares al IMC global, con valores más altos en las instituciones privadas y diferencias situadas entre los 10 y los 14 puntos, con la excepción del dominio Responder y Recuperar (REyRC) dónde las diferencias ascienden a los 45 puntos a favor de las IES privadas. Este dominio queda como uno de los más débiles para las IES públicas portuguesas, con un IMC para Responder y Recuperar (REyRC) de 0,97, siendo el valor más bajo en Portugal.

En términos generales y de forma similar a la mayoría de países analizados, las instituciones portuguesas afrontan la ciberseguridad desde una perspectiva operativa (RC3), donde priman las acciones de prevención y defensa, al igual que la mayoría de los países analizados. Así mismo, los datos muestran una fuerte correlación entre los indicadores que analizan la normativa y procedimientos de seguridad, componente RC2 y el componente RC1, referido a la parte de planificación y concienciación en ciberseguridad de los diferentes actores de la comunidad universitaria.

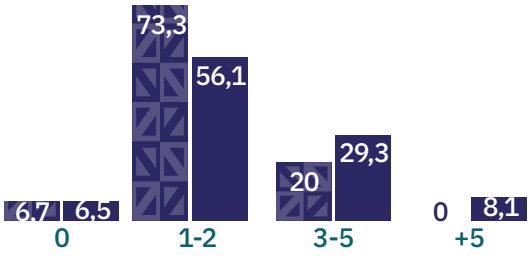
Tabla 34: Nivel de madurez de cada dominio en función del tipo de IES

	GLOBAL	GB	ID	PR	DE	REyRC
PRIVADA	1,53	1,22	1,48	1,66	1,88	1,42
PÚBLICA	1,39	1,33	1,41	1,57	1,66	0,97
DIFERENCIA	0,14	-0,11	0,07	0,09	0,22	0,45

Equipos de ciberseguridad

Además, establecer y fortalecer equipos de ciberseguridad en las IES constituye un desafío significativo que puede influir en el desarrollo del nivel de madurez en ciberseguridad dentro de las instituciones portuguesas. Según los datos recogidos, el 93,3% de las IES portuguesas cuenta con equipos de ciberseguridad específicos. De ellas, el 73,3% son equipos de ciberseguridad de 1 o 2 personas, el 20% de 3 a 5 personas y ninguna de las instituciones participantes ha indicado contar con equipos de más de 5 personas.

Gráfico 114: Composición del equipo de ciberseguridad en función del porcentaje de IES portuguesas



En comparación con la media iberoamericana, Portugal sigue la misma tendencia y la gran mayoría de IES cuentan con equipos pequeños de 1 o 2 personas. Sin embargo, en Portugal el porcentaje de estos equipos asciende al 73,3% del total, 17 puntos porcentuales por encima de la media iberoamericana. Todo esto en detrimento de equipos más grandes, dónde su cifra está por debajo de la media.

Gráfico 115: Nivel de madurez de las IES portuguesas según la composición de sus equipos de ciberseguridad

Las IES con equipos de de 1 o 2 personas superan a la media iberoamericana en un 17%. Esto hace que los equipos medianos (3 a 5 personas) sean un 9% menos y los equipos grandes (más de 5 personas) no sean una opción en Portugal en las IES analizadas.

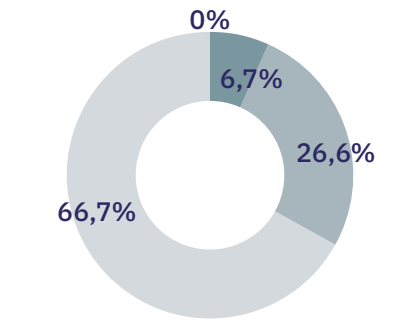
Si comparamos el IMC de las IES portuguesas según el número de personas que componen el equipo de ciberseguridad, podemos observar una clara relación entre ambos indicadores. En concreto, aquellas instituciones que no cuentan con equipos de ciberseguridad presentan un nivel de madurez básico (L1), con un valor de 1,37 puntos. Este valor asciende a 1,38 (L1) para las que cuentan con equipos pequeños de 1 o 2 personas y a 1,54 (L2), para las instituciones con equipos medianos compuestos de 3 a 5 personas.

Tabla 35: Comparación entre IES portuguesas, iberoamericanas e IMC según integración del equipo de ciberseguridad

	0 MIEMBROS	1-2 MIEMBROS	3-5 MIEMBROS	+5 MIEMBROS
PORTUGAL	6,7	73,3	20	0
IBEROAMÉRICA	6,5	56,1	29,3	8,10
IMC	1,37 L1	1,38 L1	1,54 L2	

Presupuestos de ciberseguridad

Gráfico 116: Porcentaje de IES portuguesas según presupuesto



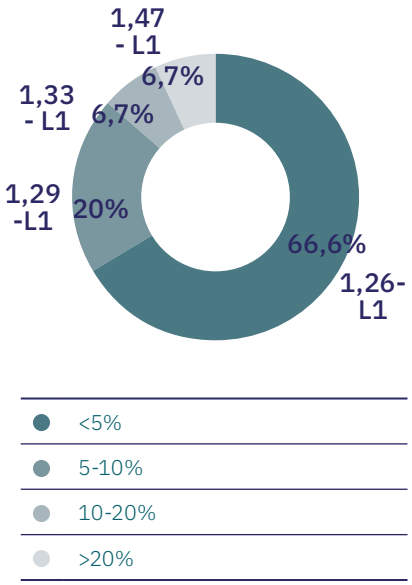
En cuanto al presupuesto, solo 4 de cada 10 IES portuguesas cuentan con partidas presupuestarias para la realización de inversiones y gastos en ciberseguridad y ninguna cuenta con presupuesto diferenciado para ciberseguridad.

De las IES que usan presupuesto del área de TI, el 6,7% usan asignaciones específicas o partidas reservadas para ciberseguridad y el 26,6% no cuentan con ninguna reserva y usan las partidas presupuestarias generales del área mencionada.

Si comparamos el IMC promedio según la existencia o no de presupuesto de ciberseguridad, se observa una tendencia ascendente muy clara y definida. Podemos ver cómo se escala desde un nivel básico (L1) hasta casi alcanzar el nivel avanzado (L3), en función de si no se dispone de presupuesto, se dispone de partidas generales o partidas específicas. Se trata de una situación que pone en valor la importancia de apostar por una inversión en ciberseguridad dentro de la estrategia institucional, no solo del área técnica.

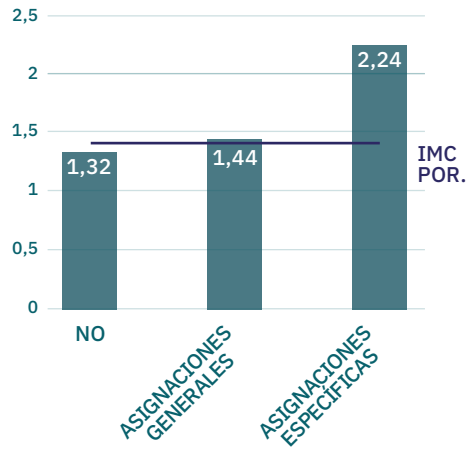
Analizando el orden de magnitud de los presupuestos de ciberseguridad, encontramos que el 66,6% cuenta con un importe para ciberseguridad equivalente a menos del 5% del presupuesto del área TI. Un 20% afirma encontrarse en el rango entre el 5 y el 10%, un 6,7% consume entre el 10 y el 20% del presupuesto de informática y el 6,7%, más de ese porcentaje.

Gráfico 117: Porcentaje del presupuesto de ciberseguridad en comparación con presupuesto de TI, y nivel de madurez según este porcentaje



Como podemos apreciar en la siguiente gráfica, el presupuesto tiene una repercusión directa en el grado de madurez de las IES. Según los datos obtenidos, el valor del IMC tiene una tendencia al alza en función del porcentaje de presupuesto asignado. Los valores pasan de 1,26 de las IES con presupuesto menor al 5% del presupuesto del área de TI hasta el 1,47 de las que tienen un presupuesto equivalente superior al 20% del área de TI. Esto hace que las IES portuguesas pasen de nivel de madurez básico hasta rozar el nivel intermedio (L2, umbral en 1,50).

Gráfico 118: Nivel de madurez de IES en Portugal según presupuesto



Ciberincidentes

Gráfico 119: Comparativa ciberincidentes sufridos por IES en el último año en México y en Iberoamérica

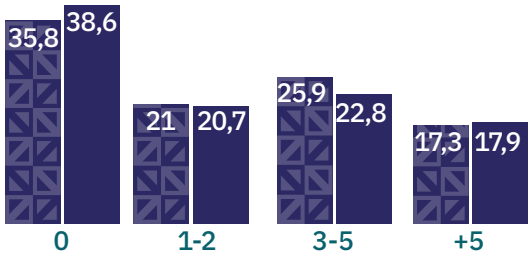
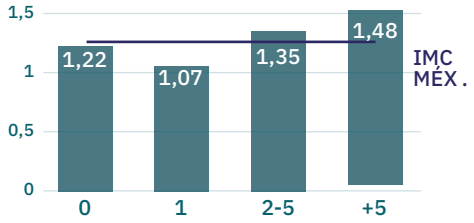


Gráfico 120: Nivel de madurez de IES que sufrieron incidentes en el último año en México

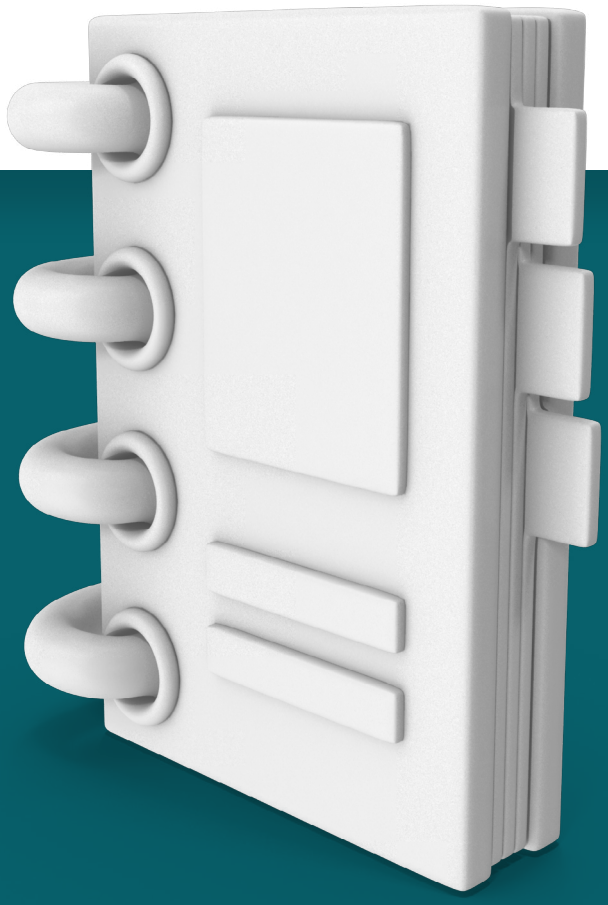


Si hablamos del número de IES que han sufrido ciberincidentes en el último año, con afectación de la operación de la institución de forma parcial o total, el porcentaje asciende al 46,7%. Es decir, cerca de la mitad de las IES en Portugal ha sufrido algún tipo de incidente en el último año. Al analizar en mayor detalle la situación, podemos ver que el 26,7% al menos un ciberincidente, y el 20%, más de 5 incidentes.

Estos valores presentan diferencias con respecto a la media en Iberoamérica en el número de IES que no han sufrido ningún ciberincidente en el último año, con Portugal un 15% por encima, y en las instituciones que han recibido de 2 a 5 ciberincidentes, rango donde las instituciones portuguesas no han reportado ningún caso.

La tendencia normal detectada en la gran mayoría de países analizados muestra una relación directa entre el número de ciberincidentes y un mayor grado de madurez, especialmente a raíz de sufrir un primer evento de este tipo. En el caso de Portugal, se mantiene esta tendencia hacia un mayor nivel de madurez a mayor número de ciberincidentes recibidos, pasando de un IMC de 1,3 puntos para las IES que no han sufrido ninguno, a un 1,67 en las que han recibido más de 5 en el último año.

Anexo I. Ficha técnica. Descripción de la muestra.



Con el objetivo de asegurar una representación adecuada de la realidad diversa de las IES que abarca esta medición, se aplicó un muestreo estratificado con asignación proporcional, utilizando dos variables para generar los estratos: país de origen y tipo de institución, es decir, si se trata instituciones de naturaleza pública o privada en cuanto a su propiedad o administración.

Para la conformación de la muestra, en primer lugar, se determinó el tamaño de cada estrato en el universo o población a estudiar, recurriendo a estadísticas oficiales de educación superior de cada país, información que posteriormente fue validada por los coordinadores del Grupo de Trabajo Internacional en Ciberseguridad de Metared.

En segundo lugar, se definió un tamaño esperado para cada estrato que asegurara un error muestral máximo de 5%, conformándose así una muestra con un total de 340 casos.

Para efectos del análisis desagregado de los datos, se realizó un tratamiento diferenciado de los estratos que no alcanzaron una cantidad de respuestas cercana a lo esperado.

Una vez finalizado el plazo de la medición, se contabilizó un total de 247 respuestas, lo que representa un 73% de lo esperado. Tal como se indicó en el cuerpo del informe, para garantizar la calidad de los análisis y dado que los estratos de cuatro países no lograron alcanzar un número adecuado de respuestas, se resolvió sólo generar informes desagregados respecto de aquellos siete países que sí alcanzaron una cantidad de respuestas representativa de acuerdo con el criterio muestral original. En esa misma línea, si se contabilizan únicamente los siete países con respuestas suficientes, la muestra teórica queda conformada por 245 casos y la cantidad de respuestas recibidas alcanza a 238, lo que implica un 97% de cumplimiento respecto de lo esperado.

Cabe consignar que, cuando hablamos del comportamiento general de la población estudiada, es decir, Iberoamérica como un todo, se incluyen en el análisis todas las respuestas recibidas.

En el caso de los reportes individuales de las instituciones que pertenecen a los cuatro países con respuestas insuficientes, sólo se incluye la comparación con los datos de Iberoamérica.

En la siguiente tabla, se muestran para cada uno de los estratos, los valores de la población, de la muestra esperada y de las respuestas recibidas, agrupando la información de los países o zonas según el logro de las respuestas esperadas.

Tabla 36: Comparación entre IES portuguesas, iberoamericanas e IMC según integración del equipo de ciberseguridad

	Tamaño de los estratos en la población			Tamaño de los estratos de la muestra			Respuestas recibidas por estrato		
	PÚBLICAS	PRIVADAS	TOTAL	PÚBLICAS	PRIVADAS	TOTAL	PÚBLICAS	PRIVADAS	TOTAL
Países con respuestas según lo requerido por el diseño muestral									
ARGENTINA	71	66	137	18	18	36	19	18	37
CHILE	25	30	55	13	14	27	9	26	35
COLOMBIA	121	265	386	20	22	42	3	28	31
ECUADOR	33	27	60	14	13	27	7	4	11
ESPAÑA	50	34	84	17	14	31	24	4	28
MÉXICO	822	2.526	3.348	24	24	48	67	14	81
PORTUGAL	42	60	102	16	18	34	12	3	15
Subtotal	1.164	3.008	4.172	122	123	245	141	97	238
Países con respuestas inferiores a lo requerido por el diseño muestral									
BRASIL	312	2.283	2.595	23	24	47	1	4	5
PERÚ	52	46	98	17	16	33	1	1	2
CENTROAMÉRICA Y EL CARIBE	9	12	21	7	8	15	1	1	2
Subtotal	373	2.341	2.714	47	48	95	3	6	9
TOTAL GENERAL	1.537	5.349	6.886	169	171	340	144	103	247

metared
by universia

IMC 2024

Índice de Madurez en Ciberseguridad de las IES Iberoamericanas