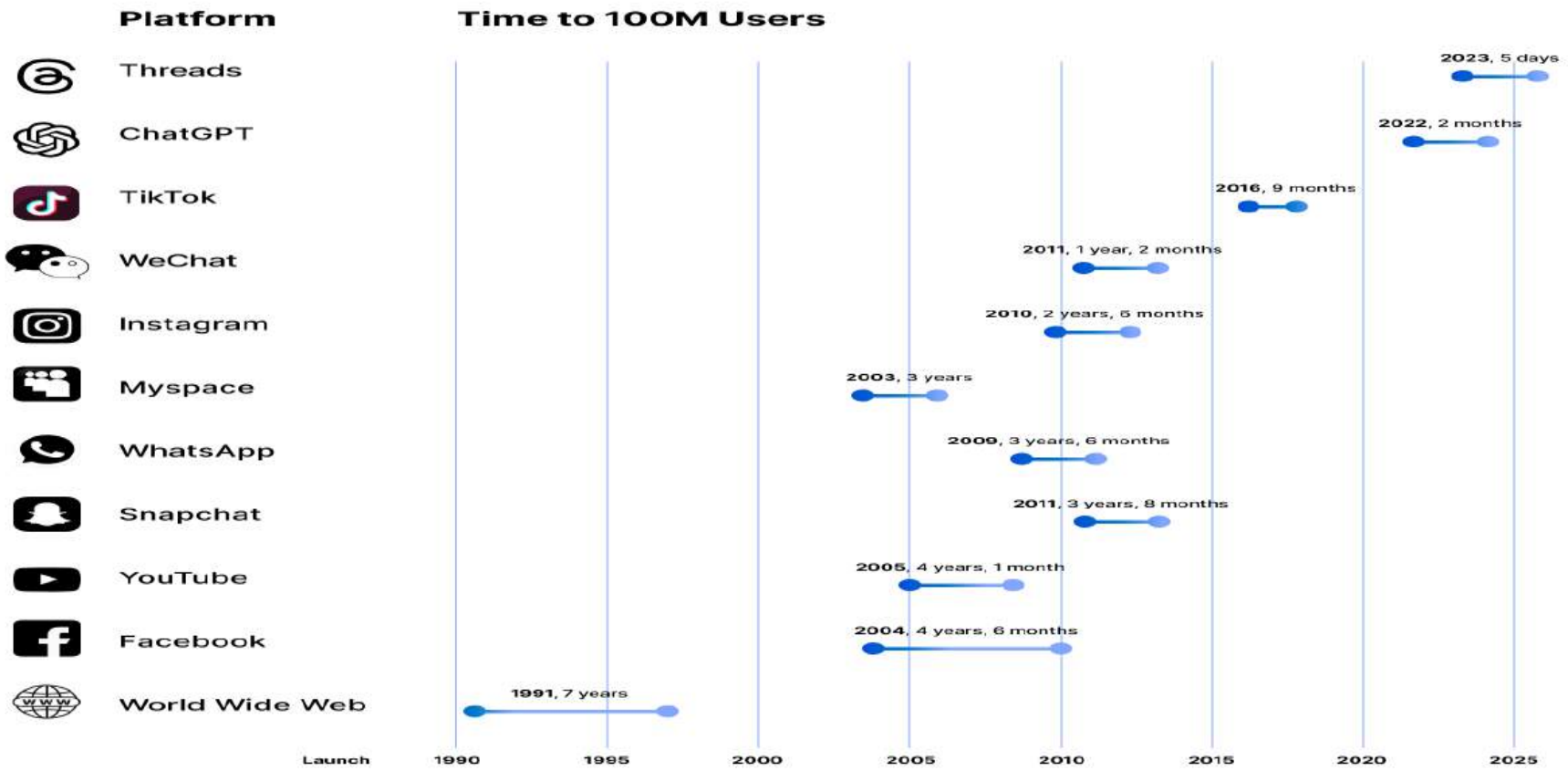
Ciberseguridad en la Era Exponencial + IMC 2024

Javier Díaz
jdiaz@unlp.edu.ar

Estamos en la Era Exponencial

- “Exponencial” caracteriza a la aceleración de los avances tecnológicos actual.
- El libro: la Era Exponencial (Azeem Azar, 2021) Los cambios radicales ya no se llevan adelante en siglos o décadas, sino en años y hasta en meses.
- Ejemplo: ChatGPT alcanzó los cien millones de usuarios en tres meses, más rápido que TikTok, logrando dicho hito en nueve meses, mientras que Instagram lo hizo en dos años y medio.
- Mientras el cambio tecnológico se acelera rápidamente, la sociedad evoluciona a un ritmo más gradual e incremental. Se está produciendo una brecha entre la tecnología y la sociedad; ***“brecha exponencial”***

Top Apps and Websites: The Journey to 100 Million Users



Techopedia

Crece el uso de la IA

- Muchas personas utilizan la IA en el trabajo en Europa. En Dinamarca (enero 2024) el 65 % de los profesionales del marketing, el 64 % de los periodistas y el 30 % de los abogados, usan IA en el trabajo. https://bfi.uchicago.edu/insights/the-adoption-of-chatgpt/
- Un tercio de los trabajadores estadounidenses usaron IA generativa en el trabajo durante la última semana de agosto 2024

https://static1.squarespace.com/static/60832ecef615231cedd30911/t/66f0c3fbabdc0a173e1e697e/1727054844024/BBD_GenAI_NBER_Sept2024.pdf

Crece el uso de la IA

- El estudio de Dinamarca descubrió que los usuarios pensaban que la IA reducía a la mitad su tiempo de trabajo para el 41% de las tareas que realizan en el trabajo.
- En EEUU tres experimentos , 4.867 desarrolladores de software, se revela un aumento del 26,08 % en la cantidad de tareas completadas entre los desarrolladores que utilizan la herramienta de IA.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4945566

Ejemplos de la Era Exponencial

Navegando por la frontera tecnológica irregular: evidencia experimental de campo de los efectos de la IA en la productividad y la calidad de los trabajadores del conocimiento

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4573321

Estudio de productividad de usar ChatGPT 4 en 18 tareas

- Los consultores que utilizaron IA terminaron un 12,2% más de tareas en promedio, completaron tareas un 25,1% más rápido y produjeron resultados de calidad un 40% más altos que aquellos que no la utilizaron.

4 áreas de estudio de las 18 tareas

- creatividad (por ejemplo, “Proponer al menos 10 ideas para un zapato nuevo dirigido a una población desatendida como mercado o deporte”),
- pensamiento analítico (por ejemplo, “Segmentar el mercado de la industria del calzado basado en los usuarios”),
- competencia en redacción (por ejemplo, “Redactar una copia de marketing de un comunicado de prensa para su producto”),
- capacidad de persuasión (por ejemplo, “Escriba un memorando inspirador para los empleados detallando por qué su producto eclipsaría a sus competidores”)

Vectores de ataque con IA

- Operaciones de Influencia
  - Engaños con imágenes generadas por IA y deepfakes
- Ingeniería Social
  - Phishing
  - Vishing: Voice Cloning-as-a-Service (VCaaS)
- Servicios y colaboración en la Deep Web con IA-como-Servicio
  - Herramientas maliciosas de IA para identificando vulnerabilidades para explotarlas
  - Participantes en estos foros han anunciado chatbots personalizados con IA, diseñados para crear programas maliciosos.

Vectores de ataque con IA

- Engaños con imágenes generadas por IA y deepfakes
  - Caso de uso 1: Actores de amenazas patrocinados por el estado usan imágenes generadas por IA para difundir propaganda en redes sociales.
  - Caso de uso 2: Actores de amenazas utilizan videos deepfake en vivo haciéndose pasar por un ejecutivo para engañar a un empleado de finanzas y hacer que transfiera millones a una cuenta maliciosa.
  - Caso de uso 3: Imágenes generadas por IA aumentan la interacción de los empleados en campañas de phishing.

IA y deepfakes

- Finance worker pays out $25 million after video call with deepfake CFO ‘chief financial officer’, 2/feb/24

https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

- Deepfake fraud directed at banks on the rise (june 2024)

https://www.thebanker.com/Deepfake-fraud-directed-at-banks-on-the-rise-1718178559

- How I used deepfakes to bypass security verifications in a bank.

"Deepfake Offensive Toolkit"

https://github.com/sensity-ai/dot

Principales amenazas ENISA

- DOS / DDOS / RDOS (Ransom Denial of Service)
- Ramsonware
- Datos Personales / sensibles
- Social Engineering
- Malware
- Ataques a Cadena de Suministro
- Amenazas Web
- File Integrity Monitoring and Incident Detection (FIMI)
- Ataques Zero Day

Principales amenazas CISO (Feb 2024)

- Ataques Ramsonware
- Malware
- Fraude x correo electrónico (correo corporativo comprometido)
- Compromiso de cuentas en la nube
- Amenaza interior (negligencia, accidente o intencional)
- Ataques DDOS
- Ataques a Cadena de Suministro
- Smishing (SMS phishing)/Vishing (Voice phishing)

Ciberataque a Costa Rica

- Primer ataque 17/4/22 a los servidores del Ministerio de Hacienda de Costa Rica, inutilizo la Administración Tributaria Virtual (ATV) y el Sistema de Información Aduanera (TICA). Dos días después, el sitio web del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones fue hackeado. Horas más tarde, Conti atacó un servidor de correo electrónico del Instituto Meteorológico Nacional robando la información contenida en el mismo. Pidieron 20Musd
- El Grupo Hive 31/5/22 ataco la Caja Costarricense de Seguro Social y obligo a cerrar todos sus sistemas críticos, Historia Única Digital de Salud y el Sistema Centralizado de Recaudación. Pidieron 5Musd.efectos hasta junio inclusive

https://cyberlaw.ccdcoe.org/wiki/Costa_Rica_ransomware_attack_(2022)#:~:text=The%20Conti%20Group%2C%20which%20claimed,companies%20operating%20in%20Costa%20Rica

Incremento Ciberataques

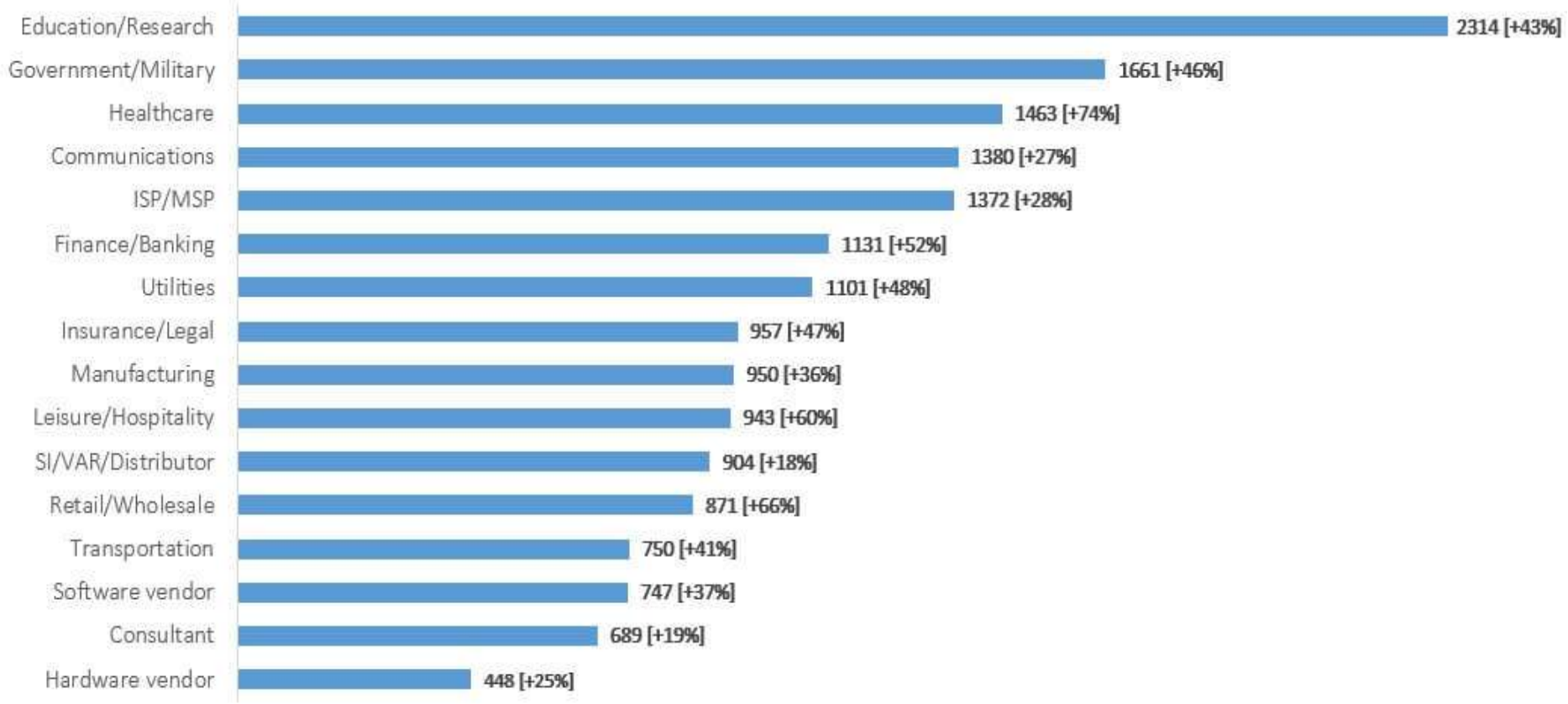
- **38%** es el porcentaje de incremento de los ciberataques en el año 2022 respecto del año anterior .
  https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/
- **30 %** aumento interanual de los ciberataques en el segundo trimestre de 2024, alcanzando 1636 ataques por organización por semana.
- Sectores más atacadas: Educación/Investigación (3.341 ataques por semana), Gobierno/Militar (2.084) y Salud (1.999).
- América Latina (+53%), África (+37%) y Europa (+35%) mostraron los mayores aumentos en ataques cibernéticos en el segundo trimestre de 2024, en comparación interanual.

Instituciones educativas europeas son el sector con más ciberataques: superan a Instituciones militares

- Estudio de Check Point realizado por su división de Inteligencia de Amenazas, ha analizado los ciberataques y amenazas recibidas en distintos sectores, desde enero a julio de 2023.
- En concreto, según los datos recabados, cada organización enmarcada en el sector de la educación o de la investigación ha recibido **una media de 2.256 ciberataques semanales** durante la primera mitad de 2023, mientras que el sector militar desciende la cifra a una media semanal de 1.759 ataques por organización. (11% de incremento)

- *https://tekiosmag.com/2023/09/08/instituciones-educativas-europeas-son-el-sector-con-mas-ciberataques-superan-al-militar/*

Avg. Weekly Cyber Attacks per Organinzation by Sector in 2022 showing all sectors suffer double-digit increase comapred to 2021



Mas de la mitad de las IES víctimas de ataques de *Ransomware* pagaron para recuperar datos

- Encuesta a más de 200 IES en 14 países.
- **63%,** utilizaron backups para restaurar sus datos, mientras que **56%** pagó el rescate.
- Las IES que utilizaron sus sistemas de respaldo de datos tuvieron menores costos de recuperacion **$980,000 libras esterlinas,** respecto de los que pagaron rescate **$1.3 million de libras esterlinas**.

- *https://www.highereddive.com/news/higher-education-ransomware-paid-ransom-college/689929/*

Noticias de Ciberataques Argentina

- Hackearon el INTA y piden un rescate de u$s 2 millones: hay 7000 afectados

https://www.cronista.com/infotechnology/actualidad/hackearon-al-inta-y-piden-un-rescate-de-us-2-millones-hay-7000-afectados/

- Por un hackeo, el INTA no puede utilizar sus radares meteorológicos en pleno temporal

https://www.infobae.com/economia/campo/2023/05/24/por-un-hackeo-el-inta-no-puede-utilizar-sus-radares-meteorologicos-en-pleno-temporal/

- Hackeo al INTA: Argentina lidera el ranking de ciberataques en la región. Un **promedio de 2.052 ataques semanales.**

https://news.agrofy.com.ar/noticia/204770/hackeo-inta-argentina-lidera-ranking-ciberataques-region

Incremento Ciberataques

- Ataque de ransomware a CONICET 20 abril del 2022, efectos mas de un mes

https://www.perfil.com/noticias/modo-fontevecchia/un-hackeo-anonimo-sigue-afectando-al-conicet-modof.phtml

- Ataque a la UBA desde 15/12/2023 con impacto hasta febrero

https://www.unvime.edu.ar/la-uba-sufrio-un-ciberataque-de-ransomware-docentes-y-alumnos-no-pueden-acceder-a-los-sistemas/

- La Argentina registró más de 262 millones de intentos de ciberataques durante el primer trimestre del 2024

*h*ttps://www.forbesargentina.com/innovacion/ciberataques-argentina-registraron-262-millones-intentos-intrusion-primer-trimestre-n53913

Es noticia! Les pasa a las Universidades ...

https://www.ull.es/portal/noticias/2022/universidades-exponen-casos-de-ciber-ataques/

Un ciberataque dejará a la UAB sin servicios informáticos durante toda la semana

V+

• Todos los portales están desconectados y sólo se pueden hacer las clases presenciales que no requieran el uso de un ordenador

Campus de la Universidad Autónoma de Barcelona (UAB) / UAB

Los 'piratas' de la UAB amenazan con filtrar los datos robados en 24 horas

Los ciberdelincuentes de PYSA publican un ultimátum en la 'deep web' un mes después de secuestrar los servidores de la institución

Hackeo a Universidad Autonoma de Barcelona

En los rankings la UAB figura entre las 200 mejores del mundo.
https://www.uab.cat/web/conoce-la-uab/la-uab/la-uab-en-los-rankings-1345670592413.html

El ataque ransomware a la UAB habría afectado hasta 650.000 archivos Datos personales. Pidieron 3.5 Millones de Euros. https://blog.elhacker.net/2021/10/el-ataque-ransomware-la-uab-universidad-barcelona-pysa.html

El ataque afecto todos los servicios informáticos (hasta la red de WIFI) y estuvo sin servicio por mas de 5 meses. Tuvo que buscar empleados jubilados que conocieran como eran los circuitos en papel para funcionar durante la emergencia. Según palabras del rector volvieron retrocedieron tres décadas.

Ejercitar respuestas a Incidentes Ciberseguridad

- 287 días: Promedio de tiempo para detectar y contener un incidente de seguridad

https://venturebeat.com/security/report-average-time-to-detect-and-contain-a-breach-is-287-days

- Ejercicios para personal Directivo
  - Decisiones al máximo nivel
  - Perspectiva Legal
  - Perspectiva Económica Financiera
  - Perspectiva Comunicaciones

Impactos de un Ciberataque

- Impacto Económico Financiero
  - Directo
  - Indirecto
- Impacto en Imagen y Prestigio
  - Servicios directos
  - Redes sociales
- Otros Impactos
  - salud

Política Seguridad de la Información

- Modelo de Política de Seguridad de la Información para Organismos Públicos.

https://www.argentina.gob.ar/noticias/elaboran-modelo-de-politica-de-seguridad-de-la-informacion-para-organismos-publicos

- Requisitos mínimos de Seguridad de la Información para Organismos. Decisión Administrativa 641/2021 Jefatura de Gabinete de Ministros.
- Política de seguridad de la información de las Instituciones Universitarias Públicas.
    - Resolución C.E. CIN: 1669/22

Aspectos a incluir en Politica de Ciberseguridad

Protección de datos: El RGPD establece los requisitos específicos para empresas y organizaciones sobre recogida, almacenamiento y gestión de los datos personales. Se aplican tanto a las organizaciones europeas como a las organizaciones que tienen su sede fuera de la UE.

Responsable de Privacidad de la Información de la Organización, CPO

Datos personales

Privacidad

Derecho al olvido

Https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm

Privacidad: ejemplo de cookies

- Almacenar o acceder a información en un dispositivo
- Desarrollar y mejorar productos
- Utilizar estudios de mercado a fin de generar información sobre el público
- Medir el rendimiento de los anuncios
- Seleccionar contenido personalizado
- Crear un perfil para la personalización de contenidos
- Seleccionar anuncios básicos
- Seleccionar anuncios personalizados
- Crear un perfil publicitario personalizado
- Utilizar datos de localización geográfica precisa
- Medir el rendimiento del contenido
- Analizar activamente las características del dispositivo para su identificación

Preparándose en Ciberseguridad

- Organización: Política Seguridad de la Información
  - CISO
  - Comité de Ciberseguridad
- Tecnología
  - SOC
  - CSIRT
- Ejercitar respuestas a incidentes
  - Gestión, económico financiero, abogados, comunicación, tecnología

Estructuras Ciberseguridad

- CISO Responsable Seguridad de la Información (Chief Información Security Officer)

- SOC Centro de Operación de Seguridad similar al Centro de Operación de Redes

- CSIRT: Prevenir, detectar, gestionar, mitigar e investigar problemas e incidentes de seguridad, coordinando acciones para la protección de los usuarios y los servicios de las Universidades.

Perspectiva de Género en Ciberseguridad

- El enfoque de género en la Política Nacional de Ciberseguridad de Chile *https://rchdt.uchile.cl/index.php/RCHDT/article/view/51577*
- Ciberseguridad & Género

https://www.gob.mx/gncertmx/articulos/ciberseguridad-genero-264162

- Enfoque de género en la ciberseguridad

https://www.observatorioigualdadyempleo.es/enfoque-de-genero-en-la-ciberseguridad/

- Marco para el desarrollo de una política de ciberseguridad que responda a las cuestiones de género

https://www.apc.org/es/pubs/marco-para-el-desarrollo-de-una-politica-de-ciberseguridad-que-responda-las-cuestiones-de-1

Acciones promovidas por MetaRED:

- Formación en Ciberseguridad
  - Cursos CISO (quinta edición)
  - Liga de CTF MetaRED (4 etapas en 2024)
- Concientización en Ciberseguridad
  - Kit INCIBE MetaRED
  - CONSEG
  - Angeles y Atenea (CCN SEG)
- Creación Sello 3C: Cultura, Conciencia y Comunicación en Ciberseguridad
- Estudio de Estado de Madurez en Ciberseguridad de las Universidades de Iberoamérica. Role Play CCN CERT
- Estrategias con proveedores

IMC 2024 IES MetaRed

“si no puedes medirlo, no puedes mejorarlo”

Peter Drucker

meta red
by universia


Patricia Pandrini


Paula Venosa


Gastón Zamorano


Daniel Genta


6,5M
estudiantes
247
IES
12
Países

Center for Internet Security (CIS) + Formación Talento

6 dominios

28 subdominios

48 indicadores del modelo

7 indicadores de caracterización

11 indicadores complementarios

Gobernar (GB)

Identificar (ID)

Proteger (PR)

Detectar (DE)

Responder y Recuperar (REyRC)

Formación y **Talento (FT**)

DOMINIOS DE APLICACIÓN

6 dominios

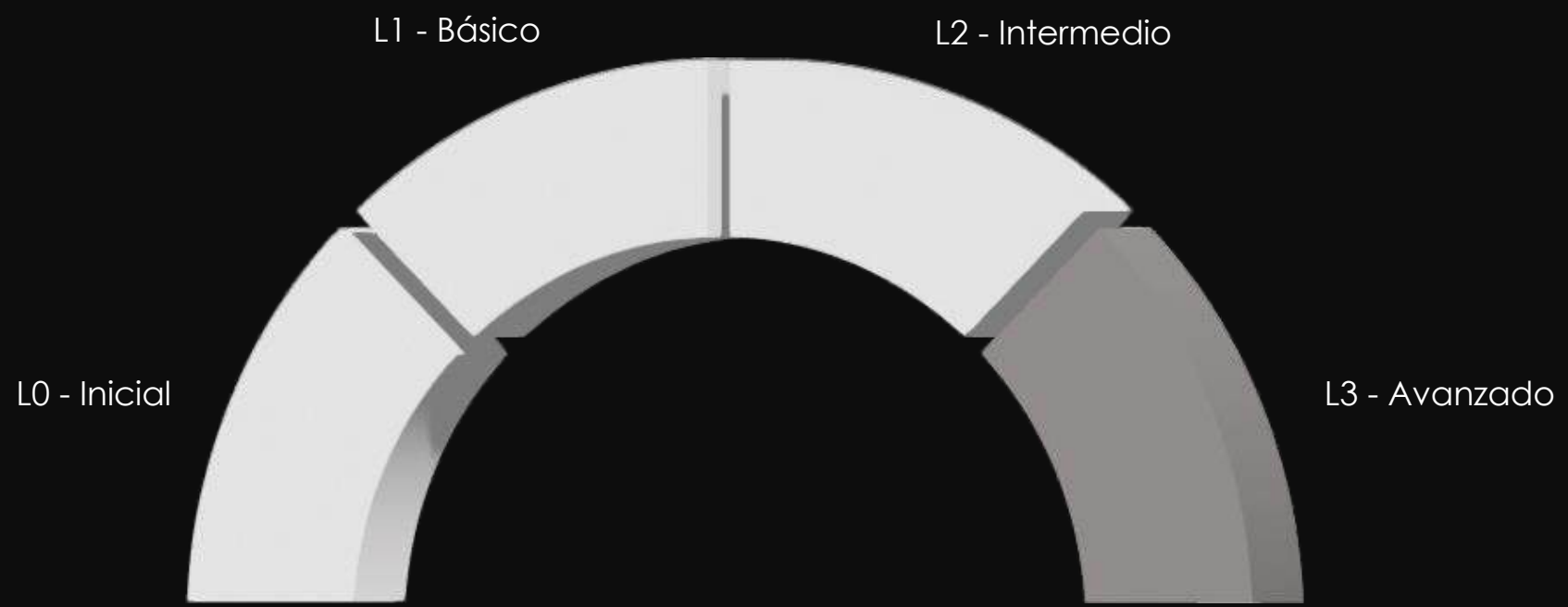
Gobernar (GB): establecer y supervisar políticas de ciberseguridad a nivel directivo

Identificar (ID): reconocer los activos críticos y evaluar los riesgos,

Proteger (PR): implementar controles que reduzcan los riesgos cibernéticos,

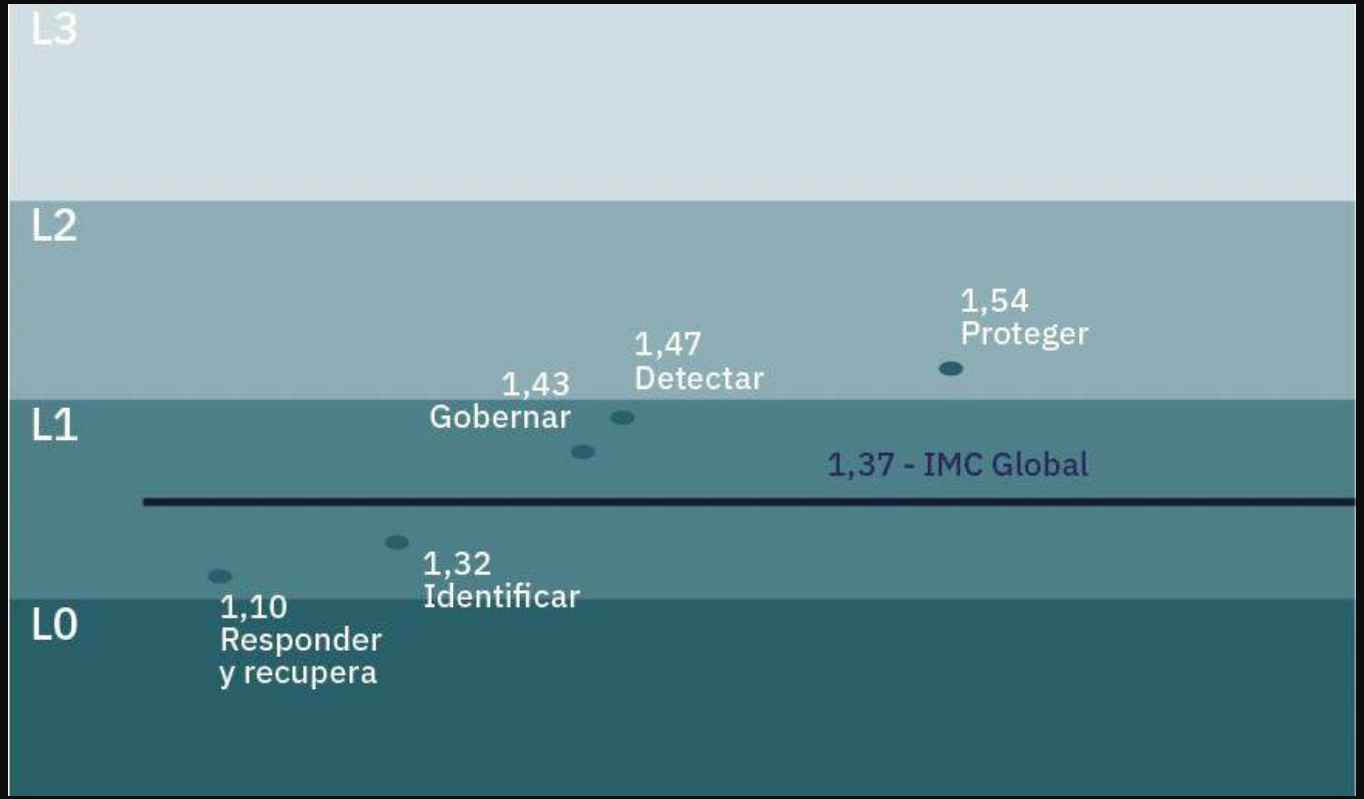
Detectar (DE): Monitoreo para identificar ataques o anomalías en sistemas

Responder y Recuperar (REyRC): Respuesta y mitigación, así como restauración


L1 - Básico
L2 - Intermedio
L0 - Inicial
L3 - Avanzado


L1
1,43
IMC GOBERNAR
L1
1,32
IMC IDENTIFICAR
L2
1,54
IMC PROTEGER
L1
1,47
IMC DETECTAR
L1
1,10
IMC RESPONDER Y RECUPERAR

IMC / Dominio


L3
L2
L1
L0
1,54
Proteger
1,47
Detectar
1,43
Gobernar
1,37 - IMC Global
1,32
Identificar
1,10
Responder
y recupera

IMC / Dominio

1,06

L1 /Básico

1,47

L1 /Básico

1,65

L2 /Intermedio

0,99

L1 /Básico

1,73

L2 /Intermedio

1,28

L1 /Básico

1,41

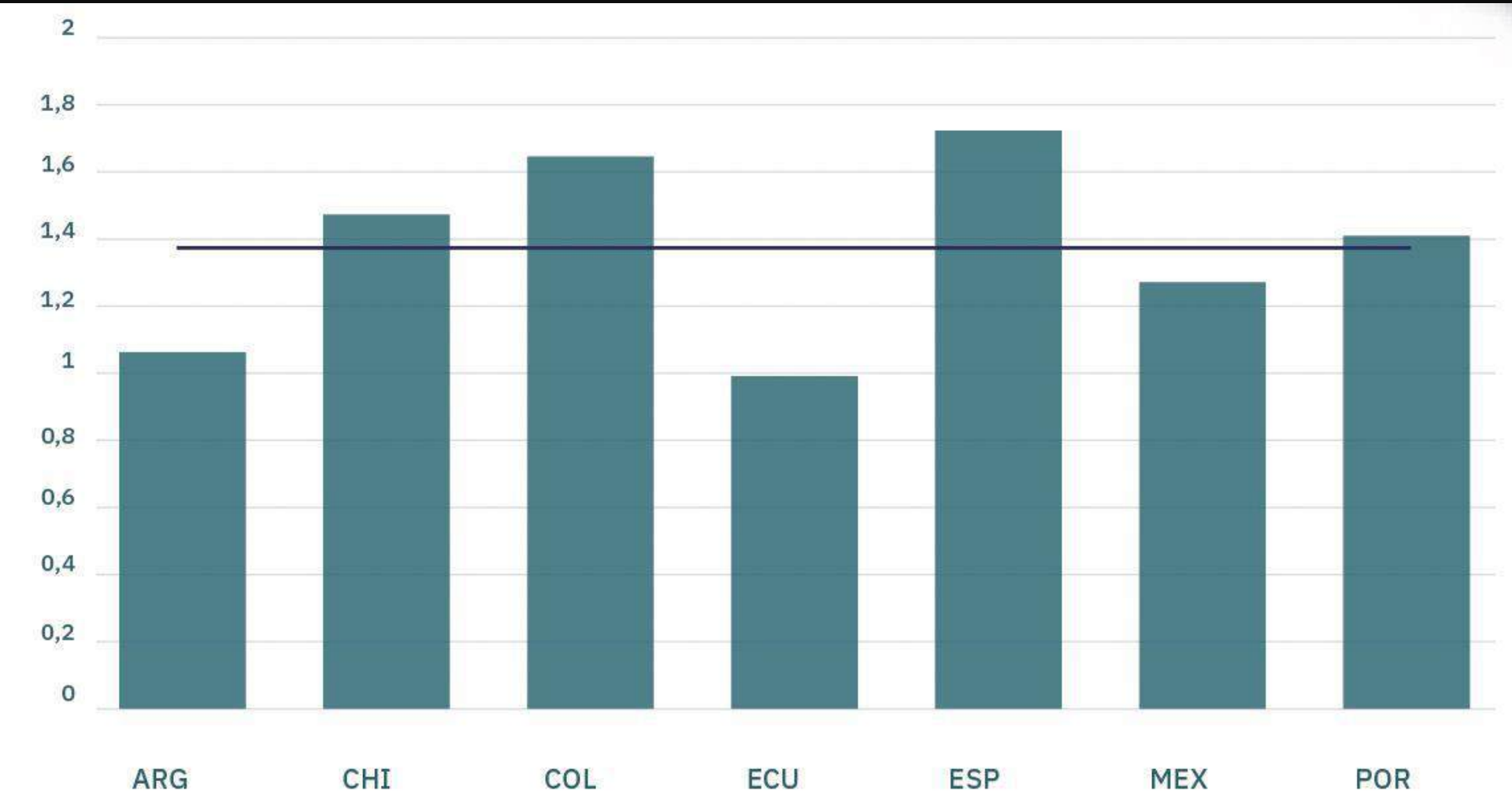
L1 /Básico

IMC / País

Resultados obtenidos.

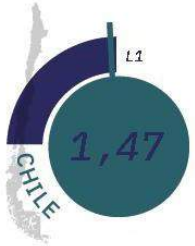
	ARGENTINA	CHILE	COLOMBIA	ECUADOR	ESPAÑA	MÉXICO	PORTUGAL	IBEROAM
IMC GLOBAL	L1	L1	L2	L1	L2	L1	L1	L1
GB	L1	L2	L2	L1	L2	L1	L1	L1
Estrategia	L1	L2	L2	L1	L2	L2	L2	L2
Política	L1	L2	L2	L1	L3	L2	L2	L2
Normativa	L1	L2	L2	L0	L2	L1	L1	L1
Procedimientos	L1	L1	L2	L1	L2	L1	L1	L1
Responsabilidad	L0	L2	L2	L0	L2	L1	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


2
1,8
1,6
1,4
1,2
1
0,8
0,6
0,4
0,2
0
ARG
CHI
COL
ECU
ESP
MEX
POR

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**

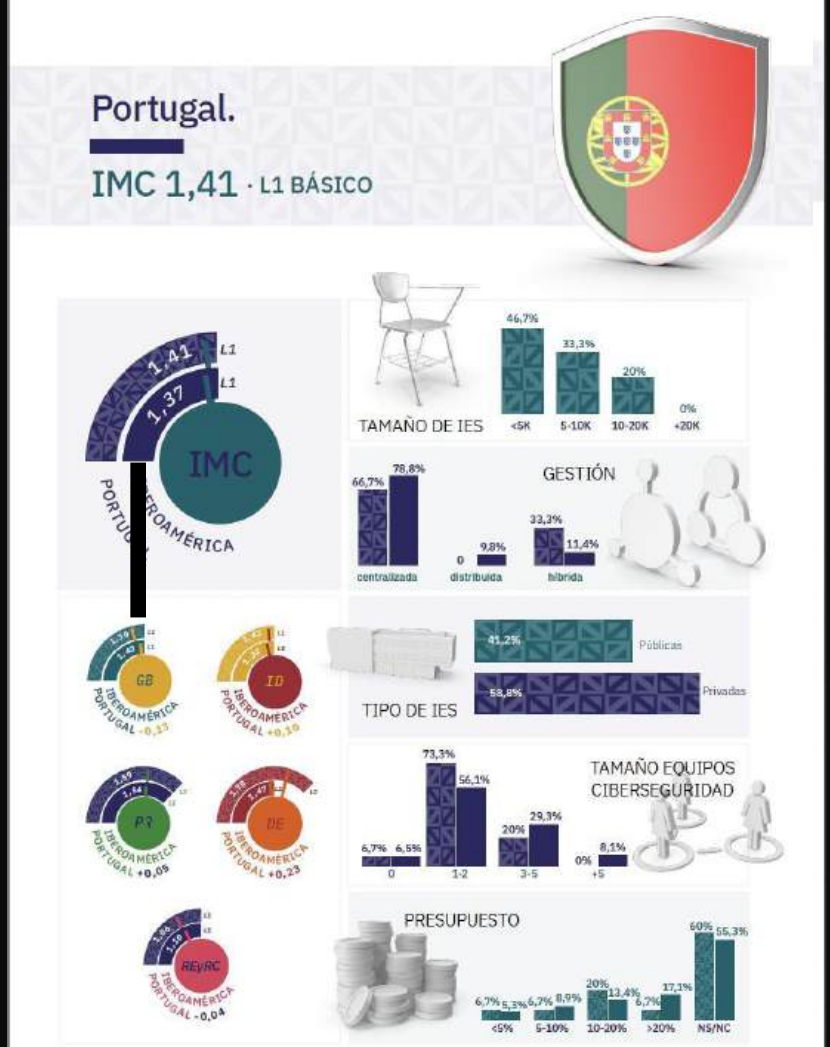
GB	0,93
ID	0,97
PR	1,36
DE	0,94
REyRC	0,74

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

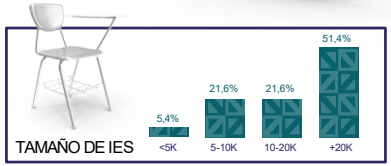
GB	1,30
ID	1,42
PR	**1,59**
DE	**1,70**
REyRC	1,06

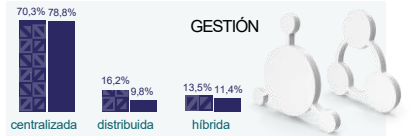
IMC / Perfil del país

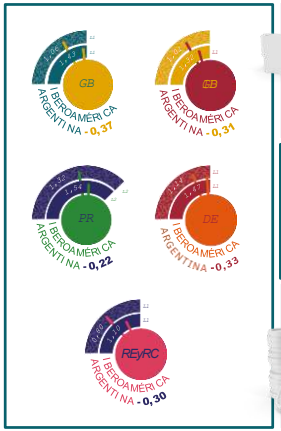


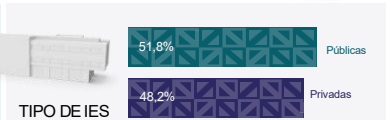
Argentina.

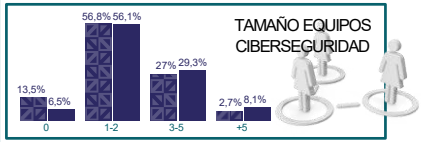
IMC 1,06 · L1 BÁSICO

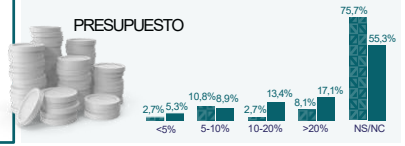












Hallazgos IMC 2024 para Argentina

1. Niveles de madurez en ciberseguridad:

Las instituciones de educación superior (IES) en Argentina se encuentran predominantemente en niveles de madurez básicos (54.1%) o iniciales (24.3%). Solo el 2.7% ha alcanzado niveles avanzados.

2. Presupuestos para ciberseguridad:

Una gran mayoría (75.7%) de las IES argentinas no informaron presupuestos específicos para ciberseguridad, y de las que sí lo hicieron, la mayoría asignó entre el 5% y el 10% de su presupuesto de TI a ciberseguridad

Hallazgos IMC 2024 para Argentina (cont.)

3. **Incidentes de ciberseguridad**:

Alrededor del 70.27% de las IES argentinas han experimentado incidentes de ciberseguridad en el último año, y el 32.4% reportó más de cinco incidentes. Esto es superior al promedio iberoamericano del 61.4%.

4. **Personal dedicado a ciberseguridad:**

El 13.5% de las IES argentinas no tiene personal dedicado a la ciberseguridad, mientras que el 56.8% tiene equipos de 1-2 personas. Solo el 2.7% cuenta con más de cinco empleados dedicados a ciberseguridad, en comparación con el promedio iberoamericano del 6%.

Hallazgos IMC 2024 ppara Argentina (cont.2)

5. Dominios de ciberseguridad:

Argentina se encuentra por debajo del promedio iberoamericano en los cinco dominios de madurez: Gobernar, Detectar, Identificar, Proteger y Recuperar. Las brechas más significativas se encuentran en Gobernanza y Detección

6. Próximos pasos

Estos hallazgos destacan la necesidad de que las IES argentinas se enfoquen en mejorar su infraestructura de ciberseguridad, particularmente a través de la asignación de presupuestos, la especialización del personal y la formalización de políticas de ciberseguridad.

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.

IMC 2024 IES MetaRed

https://www.metared.org/global/imc-2024.html

para descargar el informe global; y las universidades

que contestaron el relevamiento, pueden acceder a un dashboard de su

Universidad (comprobandola con su país o con datos globales)

meta red
by universia

¡¡Muchas gracias!!