Ciberseguridad en la Era Exponencial: Estrategia Metared

Javier Díaz

IV Jornada de Transformación Digital

STxD, UNCuyo - 2025

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.

Aceleración en la Era Exponencial

🥇 **Threads (2023)** alcanzó los **100 millones de usuarios en solo 5 días**, convirtiéndose en la aplicación con el crecimiento más rápido registrado.

⚡ **ChatGPT (2022)** llegó a los **100 millones en apenas 2 meses**, superando ampliamente a todas las plataformas anteriores de su tipo.

📱 **TikTok (2016)** logró esa cifra en **9 meses**, consolidando el nuevo ritmo de adopción de aplicaciones sociales.

📷 **Instagram (2010)** necesitó **2 años y 6 meses**, mostrando la aceleración tecnológica en la década siguiente.

🌐 **World Wide Web (1991)** tardó **7 años** en alcanzar 100 millones de usuarios, reflejando la enorme brecha temporal respecto de las apps modernas.

Uso de IA en Universidades

- Inglaterra: Encuesta 1,047 estudiantes de 166 IES, flash survey sobre IA generative en Educación Superior, realizada en Julio 2025

- La mayoría de los estudiantes **, 85 por ciento**, dijeron que usarían IA generativa el ultimo año. Los tres usos principales de una larga lista de opciones son :
  - brainstorming (55 %),
  - Usándolo y preguntándole como un tutor (50 %)
  - Estudiando para exámenes o quizzes (46 %).
  - Usándolo como un motor de búsqueda Avanzado, es un uso destacado

Crece el uso de la IA agosto 2025

- ***OpenAI (ChatGPT)***
  - **Semanal**: aproximadamente **700 millones**
  - **Mensual estimado**: entre **900 millones y 1,4 mil millones**,
- ***Google Gemini***
  - **Marzo 2025**: cerca de **350 millones**
  - **Mayo 2025**: ya superaba los **400 millones de usuarios**
  - **Julio 2025**: alcanzó los **450 millones de MAU**
- **Perplexity AI:** Según varias fuentes, se estima que tiene entre **15 y 22 millones** de usuarios activos mensuales
- **DeepSeek: enero 2025** aproximadamente **33,7 millones** de usuarios activos mensuales

Principios básicos (CIA Triad)

- **Confidencialidad:** Garantiza que la información sólo sea accesible por las personas autorizadas. En otras palabras: proteger la información contra accesos no autorizados.
- **Integridad:** Garantiza que la información sólo pueda ser modificada por quien está autorizado a hacerlo. En otras palabras: proteger la información contra accesos no autorizados.
- **Disponibilidad:** Garantiza que los usuarios autorizados tienen acceso a la información y recursos relacionados cuando lo necesiten.

Ejemplo: banca online → datos cifrados (C), registros contables no alterados (I), plataforma siempre operativa (A).

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.

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 to check security verifications in a bankt against deepfakes.

"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

WEF Global Cybersecurity Outlook 2025

- **El panorama de amenazas**
  - Ransomware riesgo Nº1 (phishing/ BEC (Business Email Compromise)/vishing)
  - GenAI abarata y masifica campañas: más phishing/deepfakes creíbles, multilingües y a escala; la CaaS/RaaS baja barreras y profesionaliza al adversario.
  - Convergencia con crimen organizado: bandas “tradicionales” entran al ciber fraudes → mayor impacto social y apetito por blancos críticos.

- **Seguridad en la “Intelligent Age”**
  - Paradoja IA: solo 37% tiene procesos para evaluar seguridad de herramientas IA
  - IA para la defensa: prioriza detección temprana, triage, priorización, análisis de anomalías…

WEF Global Cybersecurity Outlook 2025…

- **Interdependencias del ecosistema y riesgos**
  - **Cadena de suministro:** principal preocupación a escala ecosistema;
  - **Concentración de proveedores críticos** = puntos sistémicos de falla (efectos dominó)
  - **Tensiones geopolíticas:** ~60% ajusta estrategia; cambios de vendedores, pólizas
  - **Regulación:** eleva piso de ciberseguridad resiliente, aumenta fragmentación y complejidad

  Estado de la ciberresiliencia

  - **Complejidad y evolución de amenazas;** la respuesta a incidentes exige cultura de apertura y reporte temprano (formación, soportes dedicados, canales anónimos).
  - **Enfoque de ecosistema y cooperación público-privada (intercambio de inteligencia)**
  - **Realismo operativo:** 100% seguro es imposible; elevar lo básico (gestión de vulnerabilidades, hardening) y resiliencia de negocio más allá del “checklist regulatorio”.

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.boletinoficial.gob.ar/detalleAviso/primera/301511/20240102

- 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

Hackeo a Universidad Autónoma 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: afecto 650.000 archivos. 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 retrocedieron tres décadas.

Impactos de un Ciberataque

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

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.

Acciones promovidas por MetaRED:

- **Formación en Ciberseguridad**
  - Cursos CISO (24 argentinos, próximo feb 2025)
- **Concientización en Ciberseguridad**
  - Kit INCIBE MetaRED
  - Angeles y Atenea (CCN SEG)
- **Sello 3C**: Cultura, Conciencia y Comunicación en Ciberseguridad (31/oct)
  https://www.metared.org/global/sello-c3-cyber.html
- **Liga CTFs** en CTFtime (MX 24/oct, CL 14/nov, AR 4/dic)
- **IMC 2024** y 2025

IMC2024 x MetaRED:

- **Se relevaron** 247 IES, 12 países, 6.5M estudiantes
  - España,
  - Colombia,
  - Chile,
  - Portugal,
  - Mexico,
  - Ecuador,
  - Argentina
- Modelo: 6 dominios, 66 indicadores

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

Dominios de aplicación

- **Gobernar (GB):** establecer/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
- **Formación Talento (FT)**


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

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**

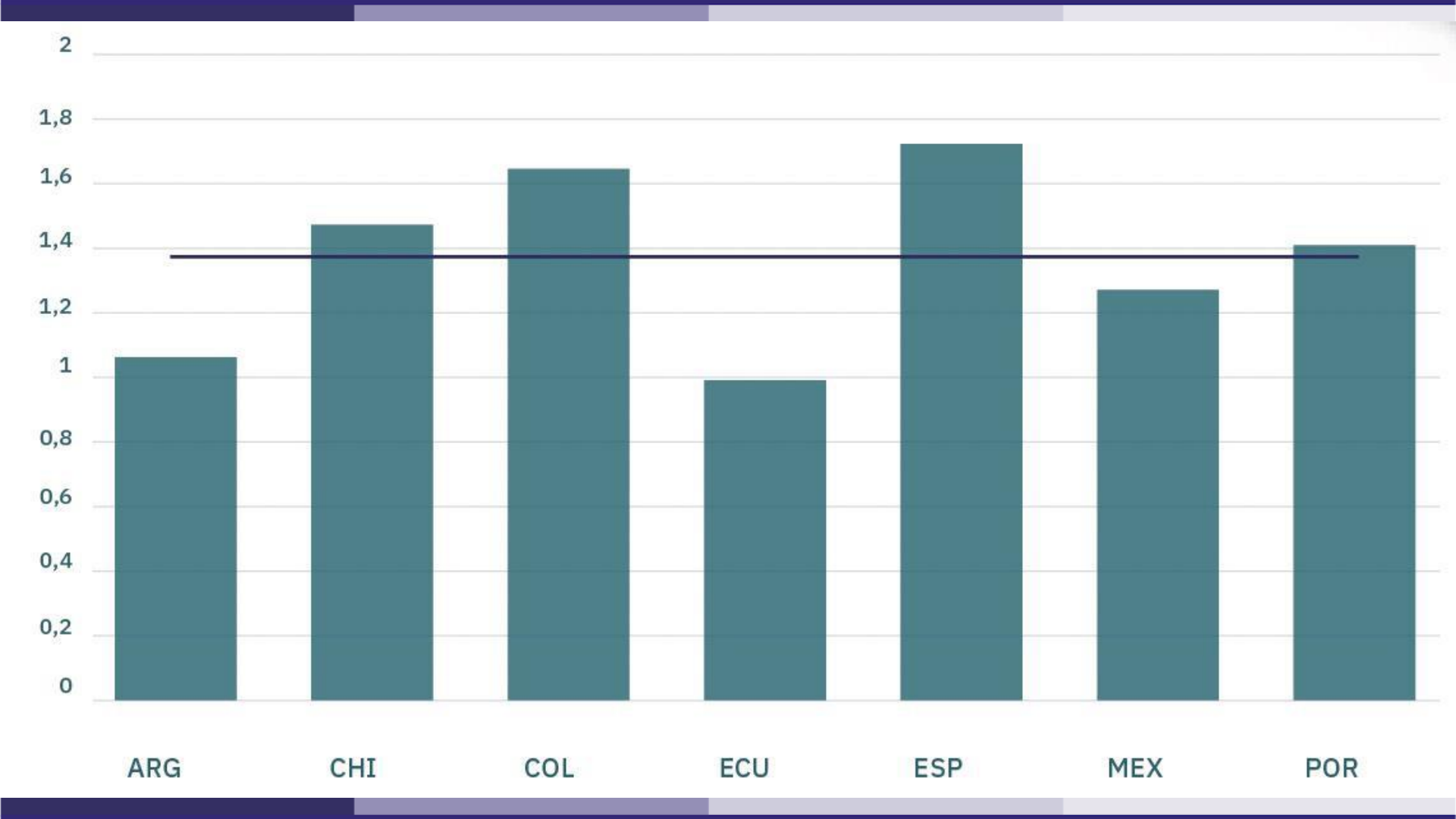
GB	**1,76**
ID	**1,62**
PR	**1,90**
DE	**1,77**
REyRC	**1,19**

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


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

Hallazgos IMC 2024 para Argentina

1. **Niveles de madurez en ciberseguridad:**

Básicos (54.1%)
Iniciales (24.3%).
Avanzados (2.7%)

2. **Presupuestos para ciberseguridad:**

75.7% no informaron presupuestos específicos para ciberseguridad, 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**:

70.27% han experimentado incidentes de ciberseguridad en el último año
32.4% reportó más de cinco incidentes.
(Esto es superior al promedio iberoamericano del 61.4%.)

4. **Personal dedicado a ciberseguridad**

13.5% no tiene personal dedicado a la ciberseguridad,
56.8% tiene equipos de 1-2 personas.
2.7% cuenta con más de cinco empleados dedicados a ciberseguridad
(En comparación con el promedio iberoamericano del 6%)

Hallazgos IMC 2024 para 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.

Comparar IMC 2024 y 2025

- **Establecer línea de base**
  - Permite identificar cuáles son las áreas críticas
- **Medir avances y retrocesos**
  - Cada edición anual permite comparar los resultados propios respecto del año anterior.
- **Priorizar inversiones y acciones**
  - La evolución año a año permite identificar qué medidas fueron efectivas y cuáles no.
- **Facilitar la colaboración interinstitucional**
  - Comparar resultados ayuda a generar alianzas y aprendizajes compartidos.
- **Vincular con marcos de mejora continua**
  - IMC anual como “checklist” de resiliencia dentro de planes estratégicos

Ventajas IMC IES de MetaRed

- **Monitoreo de tendencias**
  - Detectar si las amenazas evolucionan más rápido que las capacidades de respuesta.
- **Transparencia y rendición de cuentas**
  - Mostrar el compromiso con la mejora de la ciberseguridad.
- **Ajuste de políticas públicas**
  - Para diseñar estrategias nacionales/regionales de apoyo a las IES.
- **Generación de evidencia para talento y formación**
  - Permite identificar la necesidad de nuevos programas académicos o de capacitación.
- **Construcción de cultura institucional**
  - Asumir la ciberseguridad como parte del día a día.
- **Benchmarking sostenido**
  - Medirse frente a sí misma y frente a sus pares

Ciberseguridad en la Era Exponencial: Estrategia Metared

https://www.metared.org/ar/ciberseguridad.html