CEDIA-CUDI

SOC-CSIRT · VOC · Red Nacional de Investigación y Educación

CUDI
Corporación Universitaria para el Desarrollo de Internet

El Fin del Parcheo Ciego

Jorge Merchán

Gerente de Seguridad de la Información · CEDIA

Organiza: CUDI México · Día Virtual de Ciberseguridad · 16 Junio 2026

TLP:CLEAR

Ponente

Jorge Merchán

Líder de Seguridad de la Información · CEDIA

Apasionado de la ciberseguridad, Ingeniero en Electrónica y Telecomunicaciones, Máster en Sistemas Informáticos y Ciberseguridad, con más de 10 años de experiencia en Seguridad de la Información y Ciberseguridad, ha trabajado en sectores clave como el financiero, telecomunicaciones, multinacionales y academia, tanto a nivel nacional como internacional. Es miembro activo de iniciativas regionales e internacionales como RedCLARA, LACNIC, LAC4, ITU, FIRST y GEANT, contribuyendo en formación y cooperación en gestión de incidentes y cumplimiento normativo.

ECOSISTEMA REGIONAL E INTERNACIONAL

- RedCLARA
- LACNIC
- LAC4
- UIT / ITU
- FIRST
- GÉANT
- CSIRTAméricas
- Program Committee FIRST '23 / '25

PRIMERO, UN CONTEXTO

¿Qué es una **NREN?**

National Research and Education Network. Una red dedicada exclusivamente a la academia, la ciencia y la investigación.

Ecuador **CEDIA**	México **CUDI**	Brasil **RNP**	Chile **REUNA**	Colombia **RENATA**
Argentina **INNOVA-RED**	EE.UU. **Internet2**	Europa **GÉANT**	Reino Unido **JISC**	Japón **SINET**

Más de 60 NRENs en el mundo. Una en cada país que entendió que la academia es estratégica.

C E D I A - C U D I

SOC-CSIRT · VOC · Red Nacional de Investigación y Educación

Cómo un VOC convierte listas interminables de parches en decisiones de riesgo: ver, priorizar y proteger lo que el atacante realmente explota.

Organiza: CUDI México · Día Virtual de Ciberseguridad · 16 Junio 2026

TLP:CLEAR

LUNES POR LA MAÑANA

Abres el escáner de vulnerabilidades.

11.432

hallazgos abiertos en tu institución.

Tu equipo es de tres personas. Tienes esta semana.

¿Por cuál empiezas?

UNA VERDAD INCÓMODA

Nadie puede parchearlo todo.

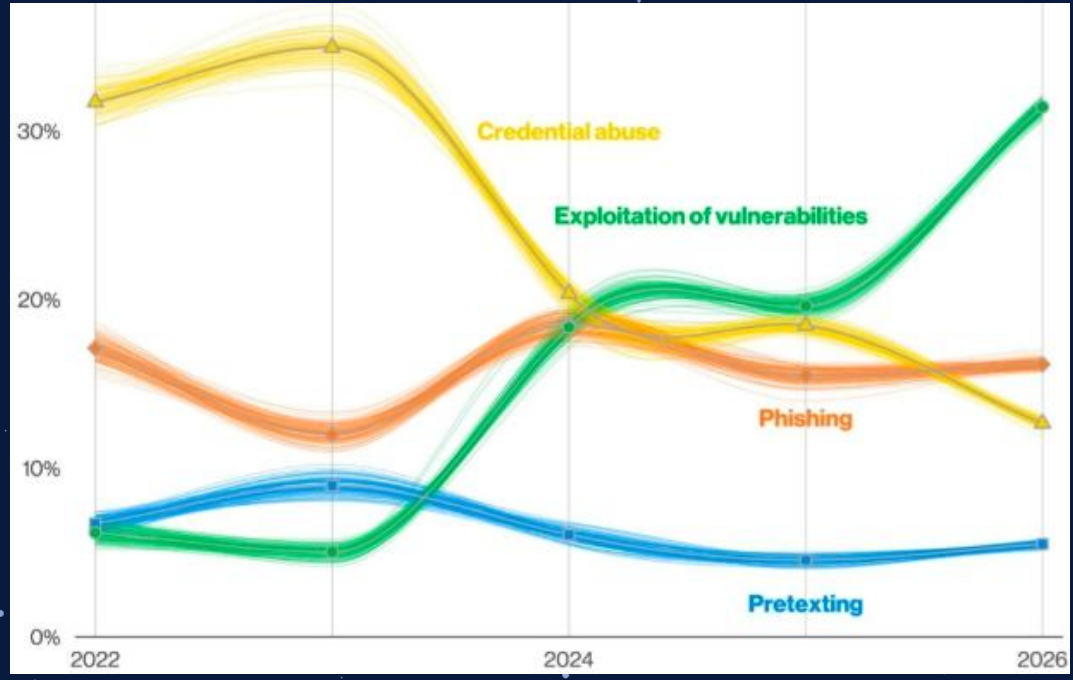
Y el atacante lo sabe. No necesita todas tus puertas abiertas. Le basta con una que tú no estabas mirando.

TLP:CLEAR

LA AVALANCHA · 2026

48.000

vulnerabilidades (CVE) publicadas en un solo año.



133

nuevas CVE cada día

9°

año consecutivo de récord

+10 %

vs. 2025 (40.009 CVE)

Fuente: NVD / CVE.org · análisis FIRST.org · 2025–2026.

PERO AQUÍ ESTÁ EL GIRO

Solo el

1,4 %

de las vulnerabilidades publicadas se explota de verdad en ataques del mundo real.

El otro 98,6 % consume el tiempo de tu equipo sin reducir el riesgo real.

Fuente: Root Evidence, “Stop Counting CVEs”, Q1 2026 · FIRST·EPSS · CISA KEV.

EL PROBLEMA TIENE NOMBRE

Parcheo ciego

Tratar 11.432 hallazgos como si todos importaran lo mismo. Ordenar por severidad teórica (CVSS) y trabajar la lista de arriba hacia abajo, sin saber qué mira ni qué usa el atacante.

Severidad ≠ riesgo	Un CVSS 9.8 que nadie explota es ruido; un 7.5 activamente explotado es una emergencia.
Esfuerzo mal asignado	El equipo agota su tiempo en miles de parches que el atacante ignora.
Lo crítico sigue abierto	Mientras corres la lista, la exposición que sí se explota permanece sin tocar.

EL SECTOR EDUCATIVO EN LA MIRA

4.300

ataques semanales por institución educativa.

El sector más atacado del mundo. Y, con frecuencia, el menos preparado.

3.065

ataques semanales por organización en América Latina · +108 % interanual

Superficie expuesta

Portales, campus distribuidos, investigación, miles de cuentas y dispositivos BYOD. Una universidad expone como una empresa grande.

Fuente: Check Point Research, Education Sector Threat Report 2025.

65 %

de los activos en universidades es Shadow IT: nadie sabe que existe.

No puedes proteger —ni parchear—
lo que no sabes que existe.

DONDE SE ESCONDE

- Servidores de laboratorio olvidados
- Portales departamentales sin inventario
- Servicios de un docente que ya no está
- Nubes contratadas sin pasar por TI

Fuente: Shadow IT in Higher Education, Forrester · ENISA Threat Landscape./ Education.

¿QUIÉNES LO EXPLOTAN?

No improvisan. Reutilizan.

Los grupos criminales no buscan la CVE más nueva: buscan la vulnerabilidad conocida que sigue abierta. Por eso la antigüedad de un parche no lo hace menos urgente.

DATA BROKER

ShinyHunters

Robo masivo y exfiltración de credenciales académicas.

RANSOMWARE

LockBit

Ransomware como servicio. Foco en infraestructura crítica.

LATAM

GordonFreeman

Clúster L4TAMFUCKERS. Objetivos en Ecuador y la región.

APT-LIKE

SHADOW-AETHER

Actor persistente emergente. Técnicas evasivas.

No son hackers de película. Son organizaciones con KPIs, y la academia es un objetivo rentable.

LA PREGUNTA CORRECTA

Deja de preguntar:

“¿Cuál de los 11.432 parcho primero?”

Empieza a preguntar:

“¿Qué ve el atacante de mí, y cuál de mis exposiciones está usando hoy?”

LA RESPUESTA

VOC

Vulnerability Operations Center

Centro de Operaciones de Vulnerabilidades

El vigía que todo lo ve. Así llamamos al VOC dentro de nuestro modelo de ciberresiliencia.

Un VOC no produce listas de parches. Produce decisiones: descubre tu superficie real (incluido el Shadow IT), correlaciona cada exposición con inteligencia de amenazas y entrega a TI exactamente lo que debe cerrar hoy para evitar el desastre de mañana.

TLP:CLEAR

CÓMO FUNCIONA UN VOC

Tres motores, una decisión.

01

Descubrir

Mapea la superficie de exposición externa, incluido el Shadow IT. Ilumina los activos que el escáner interno nunca vio.

02

Correlacionar

Cruza cada exposición con inteligencia de amenazas, EPSS y el catálogo KEV. ¿Esto se está explotando ahora?

03

Priorizar

Entrega a TI una lista corta y accionable: qué cerrar hoy, con contexto, dueño y plazo. No mil tareas; las que importan.

Descubrir · correlacionar · priorizar → cerrar la brecha antes de la explotación.

EL CAMBIO DE MODELO

PARCHEO CIEGO

- Ordena por severidad CVSS
- Trabaja una lista interminable
- Solo ve activos conocidos
- Severidad teórica, sin contexto
- Reactivo: parchea por inercia
- El equipo se agota sin reducir riesgo

VOC · DECISIÓN POR RIESGO

- Prioriza por exposición + explotación real
- Entrega una lista corta y accionable
- Descubre el Shadow IT (65 % oculto)
- Contexto: EPSS, KEV, inteligencia
- Anticipa: cierra antes del incidente
- El equipo enfoca su esfuerzo donde importa

Mismo equipo. Mismo presupuesto. Resultado distinto.

PRIORIZACIÓN BASADA EN RIESGO

De 11.432 a lo que de verdad importa hoy.

Hallazgos del escáner
Todo lo detectado en activos conocidos

+ Shadow IT descubierto
El VOC suma la exposición que no veías

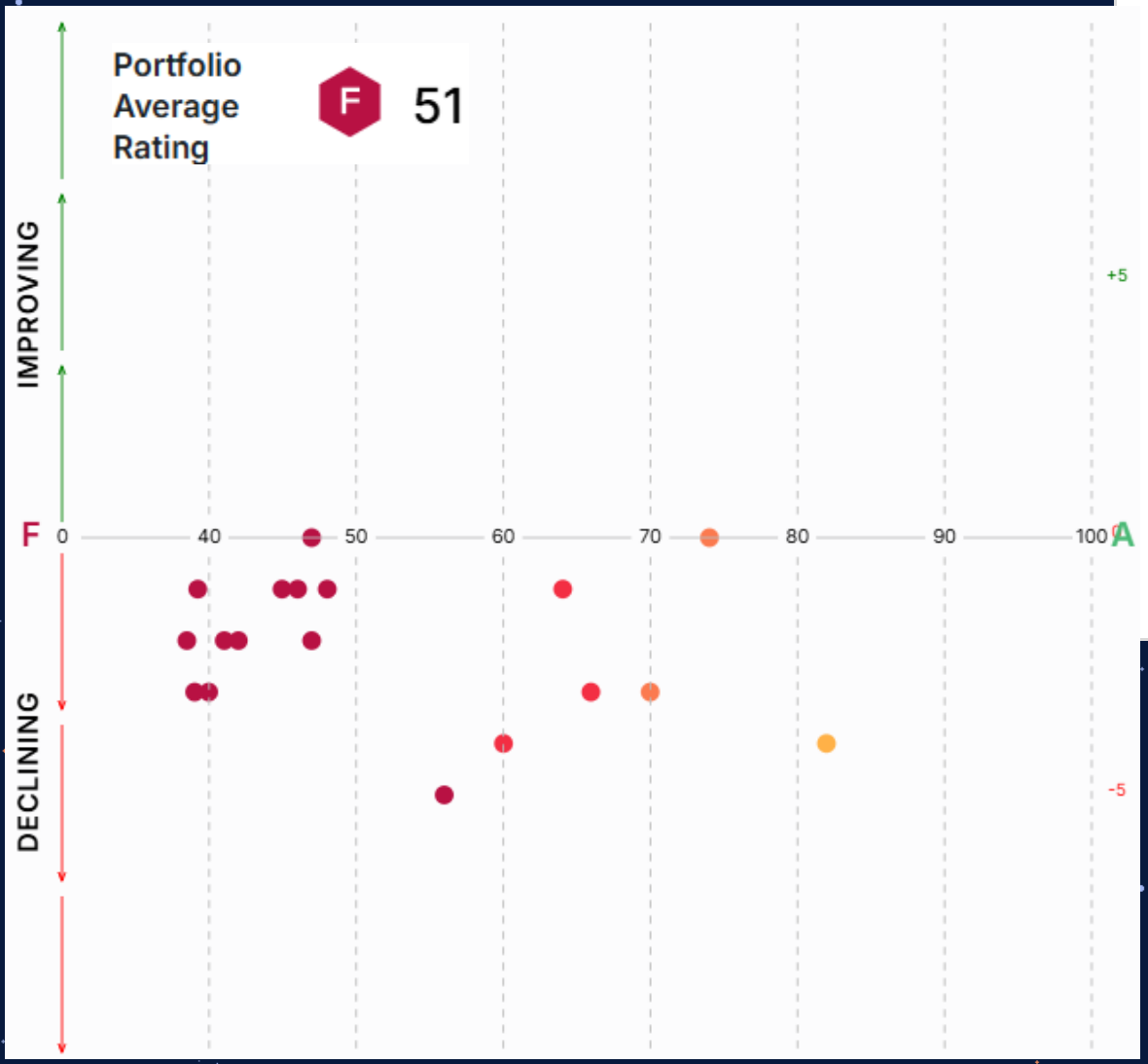
Filtro CVSS alto / crítico
Severidad teórica relevante

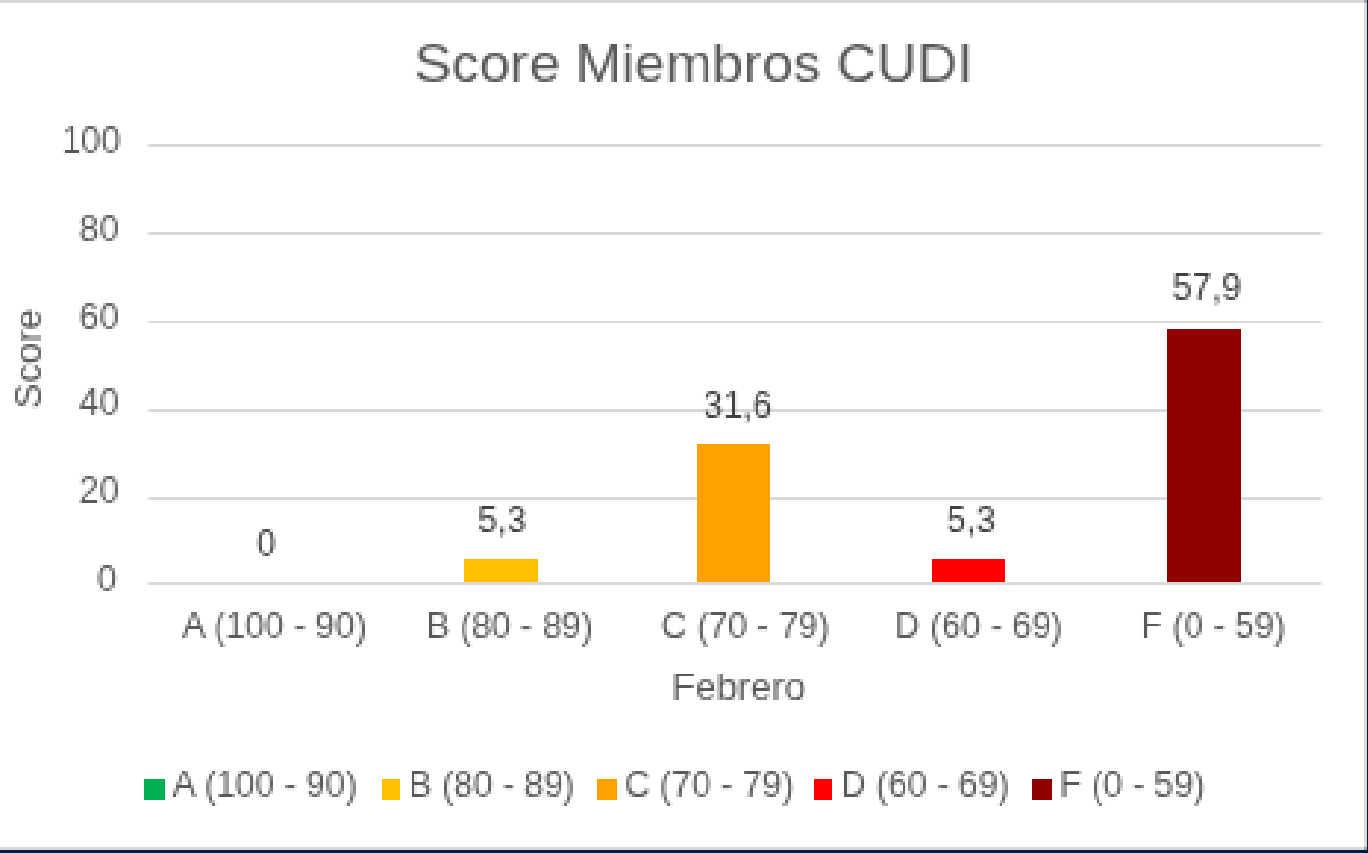
Explotación conocida (KEV) / EPSS alto
Lo que los atacantes usan hoy

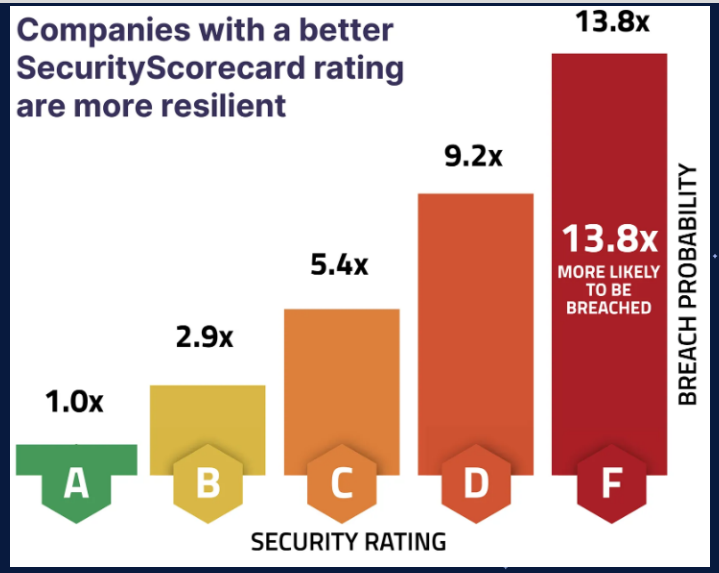
Expuesto + explotable + tuyo
Cerrar HOY

CVSS dice cuán grave podría ser. EPSS y KEV dicen si está pasando. El VOC suma tu exposición real. · Cifras ilustrativas del método.

Realidad del Sector académico Mexico







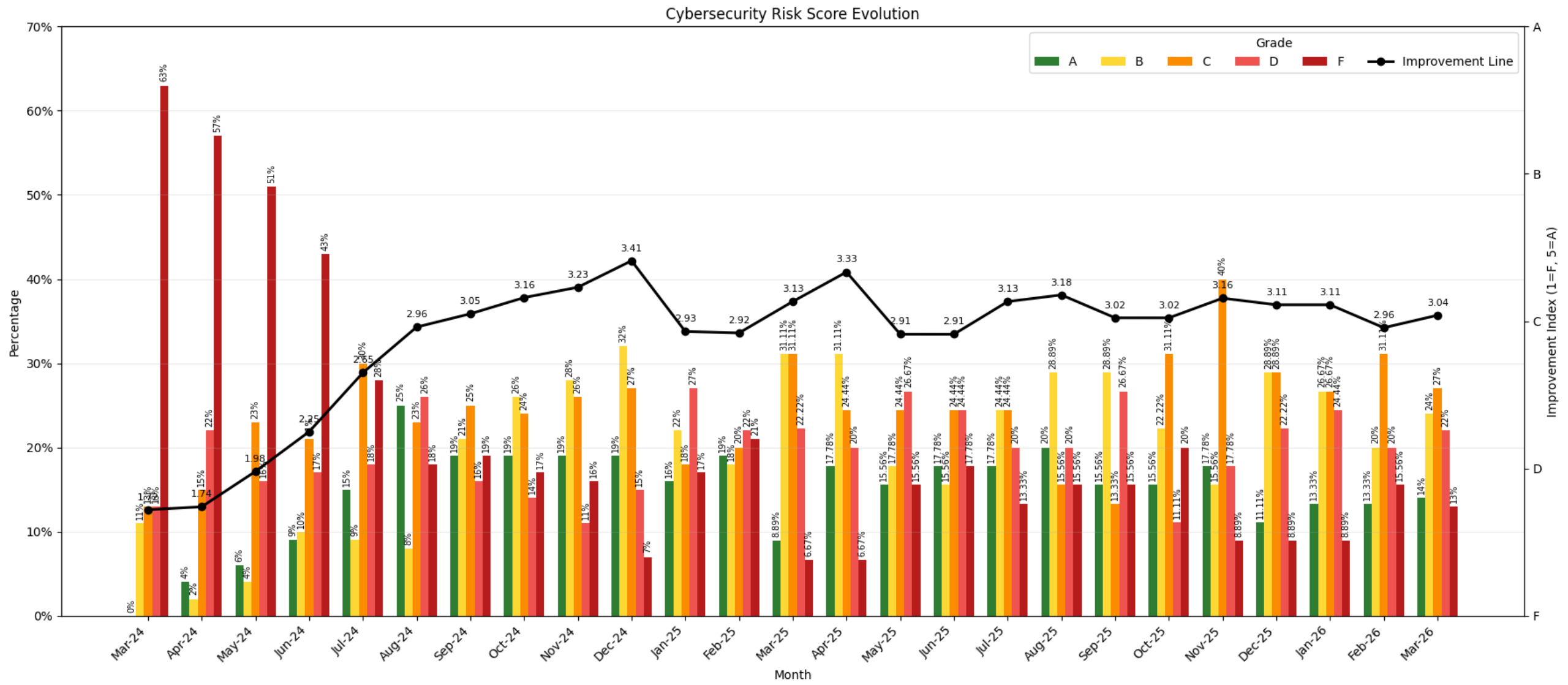
TLP:CLEAR

Realidad del Sector académico Mexico

F 34

Factor	Score	Impact	Issues			Findings
Network Security	F 25	↘ 40.7	133	434	758	1.8K
Patching Cadence	F 39	↘ 12.5	0	3.0K	33.5K	61.8K
Endpoint Security	F 45	↘ 2.0	0	26	0	26
IP Reputation	F 53	↘ 1.3	0	0	21	21
Information Leak	F 59	↘ 0.1	0	0	1.0K	5.3K
Application Security	D 60	↘ 7.4	11	0	62	2.2K
Cubit Score	A 90	↘ 1.4	1	0	0	2
DNS Health	A 99	— 0.0	0	0	2	5
Hacker Chatter	A 100	— 0.0	no issues			0
Social Engineering	A 100	— 0.0	no issues			16

58 → 78



Fuente: Proyecto DALIA, CEDIA · mediciones de exposición externa integradas al VOC · Mayo 2024 – Nov 2025.

BENEFICIOS PARA LAS IES

Lo que gana tu institución.

Visibilidad total

Inventario real de tu superficie externa, incluido el Shadow IT que hoy no ves.

Foco, no ruido

Una lista corta y priorizada por riesgo real, no miles de tareas sin contexto.

Tiempo ganado

Cierras la brecha antes de que el atacante la explote.

Métrica de avance

Un puntaje de exposición medible que mejora mes a mes y se reporta a la rectoría.

Menos incidentes

Reducción concreta de la probabilidad de ransomware y fuga de datos.

Defensa en red

Inteligencia compartida entre instituciones: lo que ataca a una, alerta a todas.

LA IDEA QUE NOS LLEVAMOS

El fin del parcheo ciego no empieza con más recursos.

Empieza con visibilidad.

Ver primero. Priorizar por riesgo. Cerrar lo que el atacante realmente usa.

EMPEZAR HOY

Agenda un diagnóstico de exposición.

Descubre qué ve el atacante de tu institución hoy. El primer paso para dejar de parchear a ciegas es, simplemente, ver. CEDIA y la comunidad CUDI pueden hacerlo juntas.

socsirt.cedia.edu.ec

SOC-CSIRT · VOC · CEDIA

Yupaychani. Gracias. Thank you.

Jorge Merchán – jorge.merchan@cedia.org.ec

Gerente de Seguridad de la Información · CEDIA SOC-CSIRT