8vo SEMINARIO LATINOAMERICANO GROp 2026 · ALGERisk

Ciberresiliencia financiera

Anticipación, respuesta y recuperación frente a ataques

Aplicando el modelo DALIA

Jorge Merchán Lima · CISM, CISSP

Gerente de Seguridad de la Información · CEDIA (Ecuador)

247

días

Tiempo medio para identificar y contener una brecha en 2026.

Seis días MÁS que en 2025.

IBM / Ponemon, Cost of a Data Breach Report 2026

LA ASIMETRÍA

Ellos operan en minutos.
Nosotros respondemos en meses.

! EL ATACANTE

- Acceso inicial vendido el mismo día
- Cifrado completo en horas
- Deepfake convincente en una llamada
- Automatiza con IA generativa

? LA ENTIDAD

- 165 días para identificar la brecha
- 55 días adicionales para contenerla
- Comités que sesionan una vez al mes
- Planes que se prueban una vez al año

IBM Cost of a Data Breach 2026 — cifras de servicios financieros (165 + 55 días)

LA FACTURA

El tiempo es la variable de costo

$6.29M

Costo medio de una brecha en servicios financieros

+26%

Por encima del promedio global de todas las industrias

+12%

De incremento interanual: sube más rápido que el mercado

2º

Sector más caro del mundo para ser vulnerado

Brechas que superan los 200 días: $5.65M

Brechas contenidas antes de 200 días: $4.32M

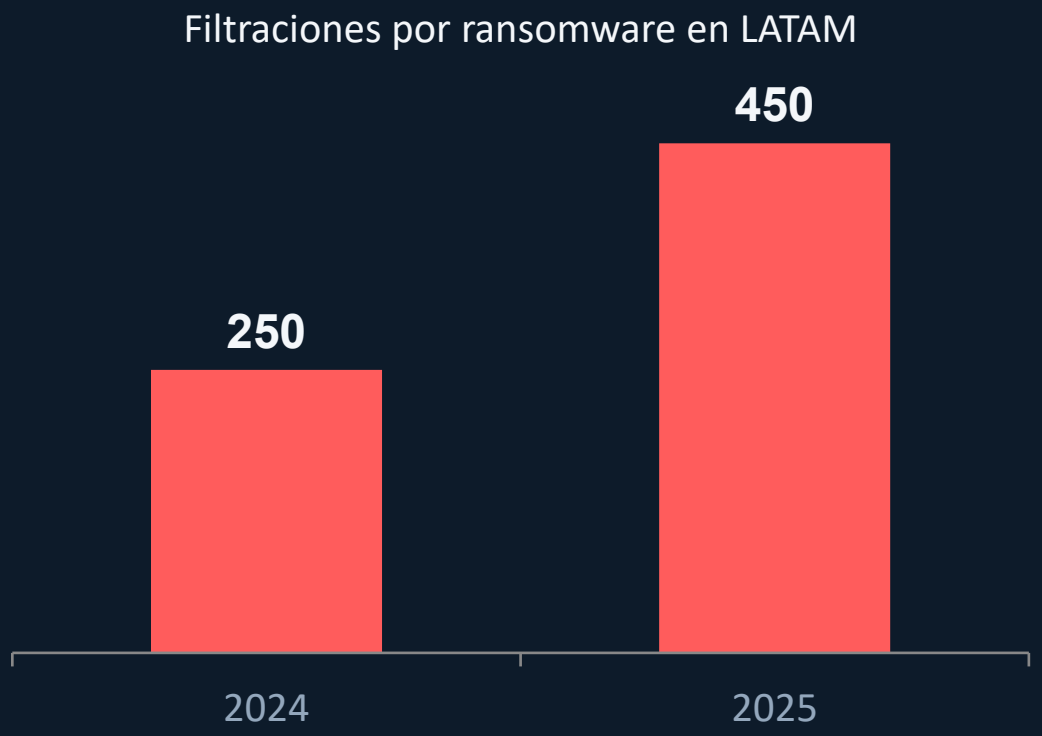
$1.33M

es lo que cuesta la lentitud

IBM / Ponemon, Cost of a Data Breach Report 2026

AMÉRICA LATINA

No somos el promedio. Somos peor.



+78% de aumento interanual en filtraciones por ransomware

48 → 79 variantes de ransomware activas en la región

79% de los incidentes financieros en LATAM son ransomware (global: 53%)

Intel 471, Latin America Cyber Threat Landscape 2026 · Duke University & Digi Americas, Panorama de amenazas LATAM 2025

CASO REAL · BRASIL 2025

Ocho entidades. Un solo proveedor.

US$ 148M

desviados desde ocho instituciones financieras mediante el compromiso de un proveedor fintech conectado al sistema de pagos instantáneos Pix del Banco Central de Brasil, aprovechando credenciales de acceso interno.

1 El perímetro ya no es suyo

Su superficie de ataque incluye la de cada tercero crítico conectado a su core.

2 El fraude entró como operación válida

Credenciales legítimas: ningún control de firma o malware lo habría marcado.

3 El impacto fue sistémico

Un solo punto de falla propagó pérdida simultánea a ocho balances distintos.

Intel 471, Latin America Cyber Threat Landscape 2026

EL ACELERADOR

La IA no cambió las amenazas. Cambió su economía.

+56% crecimiento interanual de ataques impulsados por IA

62% de los ataques con IA apuntan a financiero y energía

~45% de los ataques con IA usan suplantación por deepfake

+US$1M de costo adicional promedio por brecha con IA

«La ciberseguridad debe tratarse como una prioridad de estabilidad financiera, no como un asunto meramente técnico u operativo.» — FMI, Informe de Estabilidad Financiera Mundial

IBM Cost of a Data Breach 2026 · FMI, Global Financial Stability Report (2026)

LA DISTINCIÓN QUE IMPORTA

Ciberseguridad ≠ Ciberresiliencia

CIBERSEGURIDAD

«¿Cómo evito que entren?»

- Controles, prevención, perímetro
- Métrica: vulnerabilidades cerradas
- Dueño: TICS+SI
- **Éxito = que no pase nada**

CIBERRESILIENCIA

«¿Cuánto tardo en volver a operar?»

- Anticipar, absorber, recuperar, aprender
- Métrica: MTTD, MTTR, RTO cumplido
- Dueño: el directorio y el negocio
- **Éxito = seguir operando cuando pasa**

EL PROBLEMA DE DISEÑO

Tenemos las normas correctas. Implementadas como tres islas.

ISO/IEC 27001:2022

El sistema de gestión

Gobierno, riesgos, controles, evidencia. Vive con el CISO.

ISO/IEC 27032

La ciberseguridad

Amenazas del ciberespacio y colaboración entre partes interesadas.

ISO 22301:2019

La continuidad

BIA, RTO/RPO, estrategias de recuperación. Vive con riesgo operacional.

Tres dueños. Tres comités. Tres auditorías. Y a las 2 de la mañana del incidente, se conocen por WhatsApp.

EL CUELLO DE BOTELLA REAL

Las alertas crecen exponencialmente. Las horas del analista, no.

VOLUMEN DE ALERTAS

Crecimiento exponencial

Más servicios digitales. Más terceros conectados. Más telemetría. Más superficie. Más ruido.

CAPACIDAD HUMANA

Crecimiento lineal (o cero)

El mismo equipo. El mismo presupuesto. Ocho horas al día. Y rotación por agotamiento.

La brecha entre ambas se llama «alerta no investigada»

¿Y si el escudo no es de uno, sino de todos?

Noventa defensas aisladas → una sola defensa con noventa sensores.

ARQUITECTURA DALIA

Cuatro capacidades, un solo organismo

HEIMDALL

VOC

Gestión de vulnerabilidades y exposición. Ve venir el ataque antes de que ocurra.

JARVIS

SOC

Monitoreo continuo, correlación y triage asistido por IA. 24/7.

AVENGERS

CSIRT

Respuesta, contención y análisis forense. Miembro pleno de FIRST.

PROFESSOR X

GRC

Gobierno, riesgo y cumplimiento. Traduce la operación a decisión y evidencia.

Orquestadas por IA sobre un único flujo de datos y un único ciclo de mejora: IA + Seguridad de la Información.

DALIA IMPACTA

Siete movimientos para operacionalizar DALIA en una entidad financiera.

Anticipación · Respuesta · Recuperación

EL MODELO COMPLETO

Siete movimientos, tres tiempos

ANTICIPACIÓN

- **I** — Inteligencia
- **M** — Monitoreo
- **P** — Preparación

RESPUESTA

- **A** — Automatización
- **C** — Colaboración

RECUPERACIÓN

- **T** — Trazabilidad
- **A** — Aprendizaje

Cada letra necesita las tres cosas: un dueño, una métrica y una evidencia. Sin las tres, es una diapositiva, no un control.

PARA EL AUDITOR Y EL COMITÉ

IMPACTA sobre las tres normas

Movimiento	ISO/IEC 27001:2022	ISO/IEC 27032	ISO 22301:2019	NIST CSF 2.0
I · Inteligencia	Cl. 6.1 riesgos · A.5.7 threat intel · A.5.19-22 proveedores	Inteligencia y contexto del ciberespacio	Cl. 8.2 análisis de contexto	IDENTIFY
M · Monitoreo	A.8.15-16 registro y monitoreo · A.5.7	Vigilancia compartida de amenazas	Cl. 8.4 alerta temprana	DETECT
P · Preparación	A.5.24 planificación de incidentes · Cl. 9.1	Ejercicios entre partes interesadas	Cl. 8.2 BIA · 8.3 estrategias · 8.5 pruebas	PROTECT
A · Automatización	A.5.25-26 evaluación y respuesta · A.8.16	Mecanismos técnicos coordinados	Cl. 8.4 respuesta a incidentes	RESPOND
C · Colaboración	A.5.5-6 contacto con autoridades y grupos	Núcleo: responsabilidad compartida	Cl. 8.4.3 comunicación con partes	RESPOND
T · Trazabilidad	Cl. 7.5 información documentada · A.5.28 evidencia	Reporte y notificación coordinada	Cl. 8.6 documentación de recuperación	RECOVER
A · Aprendizaje	A.5.27 aprender de incidentes · Cl. 10	Mejora del ecosistema	Cl. 9.1 evaluación · 10.2 mejora	GOVERN

Mapeo de elaboración propia. Verificar numeración de cláusulas contra la edición vigente de cada norma.


UNIFIED SECURITY INTELLIGENCE ECOSYSTEM
VOC (Vulnerability Operations Center) Agent
Attack Surface Management
Brond Protection
Vulnerability Analysis
SOC (Security Operations Center) Agent
SIEM
SOAR
GRC (Governance, Risk and Compliance) Agent
ECS1 Regulations (ISO 27001)
ECS1 Regulations (Government Cybersecurity Schemo)
LPDCP Compliance (Personal Data Protection Law)
CSIRT (Computar Security Incident Response Team) Agent
Orchestration with other CSIRTs
Comprehensive Data & Threat Intelligence
Risk & Compliance Data Flows
DALIA
From Analysis to Action
DALIA
ACTIONABLE MITIGATION
INCIDENT MANAGEMENT
(Advanced Ticketing Platform)
AUTOMATED DEFENSE & CONTAINMENT
Higher Education Institutions (IES) Ecosystem
Higher Education Institutions
IES 'A", 'B', 'N"
Higher Education Institutions (IES)
Higher Education Institutions (IES) Ecosystem
Higher Education Institutions
IES 'A", 'B', 'N"
Higher Education Institutions (IES)
BENEFITS ACHIEVED FOR UNIVERSITIES
Collaborative Cyber Resilience Model
1. ENHANCED CYBER RESILIENCE
1. ENHANCED RESILIENCE
(Reduced Attack Surface & Exposure)
2. COLLECTIVE DEFENSE
(Shared Security Posture & Benefits)
3. 360-DEGREE VISIBILITY
(Real-time Risk & Performance Dashboard)
4. GUARANTEED COMPLIANCE
4. GUARANTEED COMPLIANCE
(Alignment with LOPDP, EGSI, SGSI)
5. OPTIMIZED OPERATIONAL EFFICIENCY
5. OPTIMIZED EFFICIENCY
(AI-Driven Advanced Management)

RESULTADOS

RESULTADOS OPERACIONALES | Phase 1 (Mar 2024 – Mar 2026)

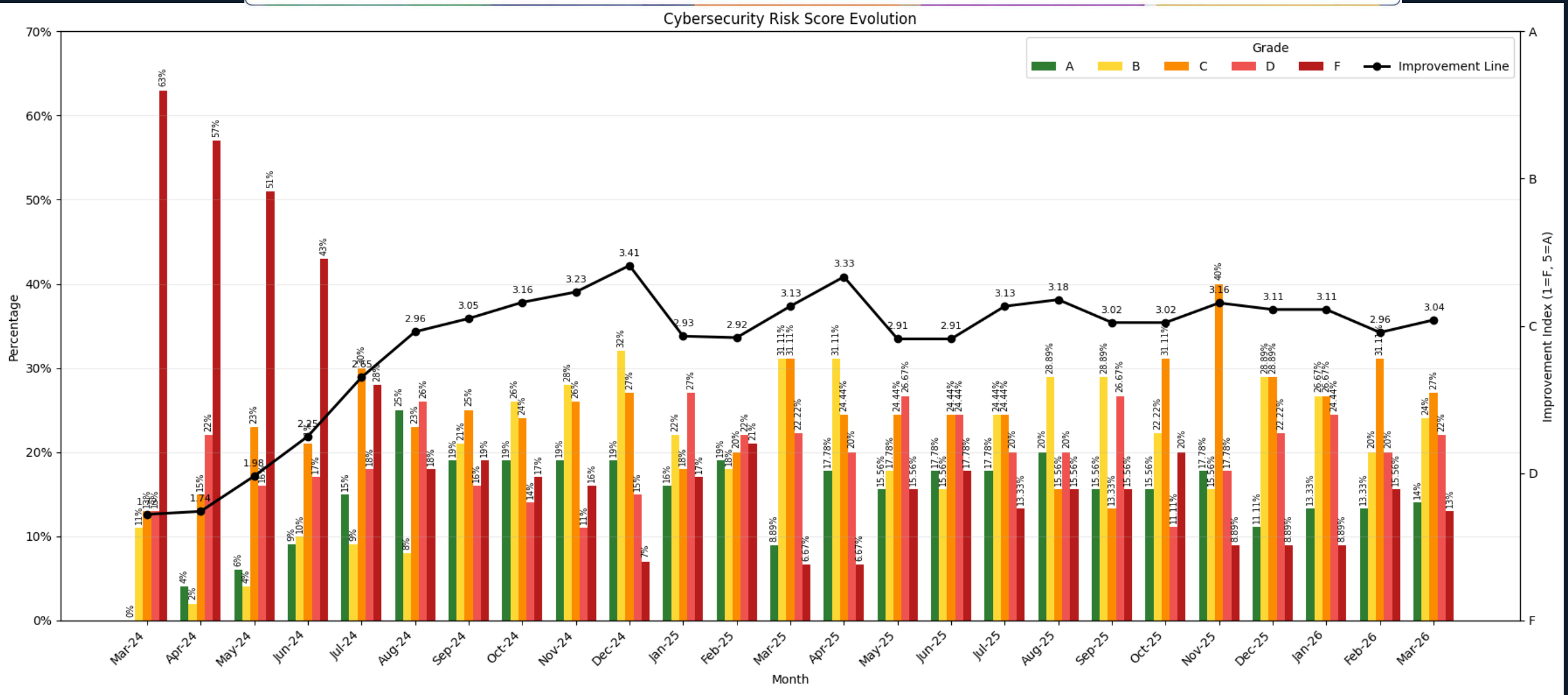
213,063
CUENTAS PROTEGIDAS
(notificadas y filtradas)

35,260
ALERTAS PROCESADAS
(alertas de seguridad)

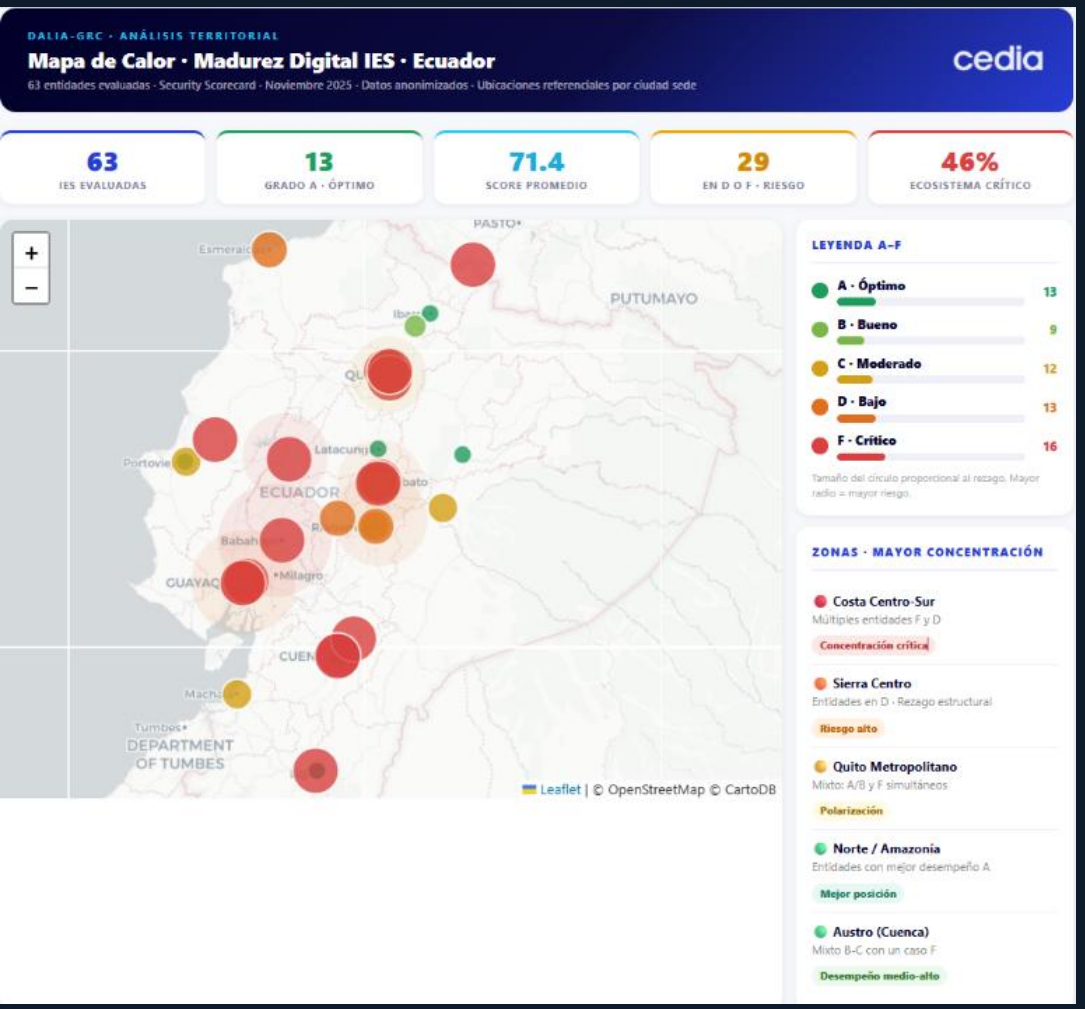
176
ATAQUES CRÍTICOS MITIGADOS
(antes de materializarse)

3,100
PERSONAS FORMADAS
(capacitaciones realizadas)

$3.16M
AHORRO ESTIMADO EN PREVENCIÓN
(pérdidas evitadas)



RESULTADOS


DALIA-GRC · ANÁLISIS TERRITORIAL
Mapa de Calor · Madurez Digital IES · Ecuador
cedia
63 entidades evaluadas · Security Scorecard · Noviembre 2025 · Datos anonimizados · Ubicaciones referenciales por ciudad sede
63
IES EVALUADAS
13
GRADO A · ÓPTIMO
71.4
SCORE PROMEDIO
29
EN D O F · RIESGO
46%
ECOSISTEMA CRÍTICO
PASTO
PUTUMAYO
ECUADOR
Latacunga
Portoviejo
Babahoyo
Milagro
GUAYAQUIL
CUENCA
Machala
Tumbes
DEPARTMENT OF TUMBES
Leaflet | © OpenStreetMap © CartoDB
LEYENDA A–F
A · Óptimo 13
B · Bueno 9
C · Moderado 12
D · Bajo 13
F · Crítico 16
Tamaño del círculo proporcional al rezago. Mayor radio = mayor riesgo.
ZONAS · MAYOR CONCENTRACIÓN
Costa Centro-Sur
Múltiples entidades F y D
Concentración crítica
Sierra Centro
Entidades en D · Rezago estructural
Riesgo alto
Quito Metropolitano
Mixto: A/B y F simultáneos
Polarización
Norte / Amazonía
Entidades con mejor desempeño A
Mejor posición
Austro (Cuenca)
Mixto B-C con un caso F
Desempeño medio-alto


cedia
Panorama de Seguridad - IES Ecuador
75
15
27
97.25
0.0
Distribución por Calificación
A 15
B 15
C 18
D 14
F 13
Top 10 IES Mejor Posicionadas
1 UTN A 97.25
2 ACAC A 97.00
3 ISTE A 95.00
4 PUCE - SA A 94.00
5 IBAM A 93.75
RELACIÓN MADUREZ DIGITAL — EXPOSICIÓN ECONÓMICA POR GRUPO
CÓMO LA MADUREZ REDUCE MULTAS Y ACELERA LA RECUPERACIÓN · 5 GRUPOS ANONIMIZADOS
A
15
Instituciones
Score: 90–99
Multa estimada
$0–$50K
Recuperación
< 48 horas
Exposición mínima
B
15
Instituciones
Score: 80–89
Multa estimada
$50K–$200K
Recuperación
3–7 días
Exposición baja
C
18
Instituciones
Score: 70–79
Multa estimada
$200K–$500K
Recuperación
15–30 días
Exposición moderada
D
14
Instituciones
Score: 60–69
Multa estimada
$500K–$1.5M
Recuperación
30–90 días
Exposición alta
F
13
Instituciones
Score: 39–59
Multa estimada
$1.5M–$5M+
Recuperación
90–180 días
Exposición crítica
Relación inversa confirmada: ↑ Madurez = ↓ Multas + ↓ Tiempo de recuperación
Una IES que pasa de grado F a grado A reduce su exposición económica en hasta $4.95M y acorta su tiempo de recuperación de 180 días a < 48 horas. La madurez digital es el mejor seguro regulatorio disponible.
BRECHAS CRÍTICAS DEL ECOSISTEMA
25 % del ecosistema en grado F — Score mínimo: 39
16 IES con score entre 39 y 59 representan el grupo de mayor exposición. Una brecha de incidente en cualquiera de ellas activa responsabilidad LOPDP directa y puede generar multas superiores a $1.5M por evento.
0 % de issues resueltas en el período octubre-diciembre 2025
Ninguna de las 15,766 issues activas fue cerrada en el período evaluado. Este dato indica ausencia de procesos formales de remediación y gestión del ciclo de vida de vulnerabilidades a nivel de ecosistema.
591 credenciales comprometidas activas · sin remediación
Credenciales institucionales expuestas en dark web. Constituyen infracciones graves bajo LOPDP Art. 39 (deber de seguridad) y pueden derivar en acceso no autorizado a datos de estudiantes, docentes y registros académicos.
737 certificados TLS autofirmados — Confianza digital comprometida
Certificados sin validación de autoridad confiable exponen portales institucionales, plataformas académicas y sistemas de gestión. Incrementan superficie de ataque MitM y pueden afectar acuerdos de intercambio de datos con terceros.
719 parches críticos pendientes — Cadencia de parcheo deficiente
Alta concentración en IES grado D y F. La falta de parcheo oportuno eleva el riesgo de explotación de vulnerabilidades conocidas (CVE) y constituye incumplimiento EGSI v3.0 control de gestión de vulnerabilidades.
600 sitios sin política CSP — Exposición a inyección y XSS
Ausencia de Content Security Policy en plataformas académicas y portales públicos. Favorece ataques de scripting e inyección de contenido. Brecha de control básico de seguridad web (NIST CSF PR.IP-1).

CINCO ACCIONES PARA EL PROXIMO LUNES

Sin presupuesto adicional

1	**Verifique cobertura detectiva**	Tome los 3 escenarios de mayor impacto de su BIA y confirme si cada uno tiene un caso de uso detectivo probado.
2	**Pida MTTD y MTTR reales**	De los últimos 12 meses, por escenario. Si nadie los tiene, ese es su hallazgo número uno.
3	**Agende un ejercicio de crisis**	En 90 días, con el comité de riesgos en la sala, con reloj corriendo y con decisiones que se registran.
4	**Interrogue a sus 5 terceros críticos**	¿RTO verificado o declarado? ¿Cuándo lo probaron? ¿Con qué evidencia? ¿Le notifican en cuántas horas?
5	**Abra un canal con dos pares**	Intercambio de indicadores anonimizados con dos entidades del sector. Empiece por lo que no le cuesta nada revelar.

Ninguna de estas cinco requiere una compra. Las cinco requieren una decisión.

El atacante ya entendió el valor de la colaboración.

Comparte herramientas. Vende accesos. Opera como afiliado. Trabaja en red.
Nosotros seguimos trabajando en silos, y lo llamamos confidencialidad.

La pregunta no es si podrán evitar la próxima crisis.
Es cuánto tardarán en darse cuenta — y quién estará del otro lado del teléfono cuando llamen.

Gracias.

Jorge Merchán Lima · CISM, CISSP · CEDIA · linkedin.com/in/jorge-merchán-lima-85a581164