SecurityScorecard cedia

CASE STUDY

IN PARTNERSHIP WITH LSG Company Line Solutions Gateway

Cómo CEDIA transformó la ciberresiliencia del ecosistema académico ecuatoriano con SecurityScorecard

CASO DE USO

Monitoreo Continuo del Ecosistema Académico

Gestión Centralizada del Riesgo Digital (VOC)

CSIRT Académico y Respuesta a Incidentes

Reporting Ejecutivo y Gobernanza Institucional

Alineamiento con Marcos de Cumplimiento (ISO 27001, EGSI, LOPDP

CEDIA, red académica del Ecuador y CSIRT del sector universitario, integró SecurityScorecard como feed externo en su Centro de Operaciones de Vulnerabilidades (VOC), transformando un modelo reactivo de gestión de riesgo en una operación continua, automatizada y escalable para más de 90 instituciones de educación superior.

EL RESULTADO: El porcentaje de instituciones con calificación F bajó de ~63% a menos del 20%, más del 18% superan ya los 90 puntos, y el equipo liberó más del 60% de su tiempo operativo para tareas de mayor valor.

Sobre CEDIA

CEDIA es la red académica y de investigación de Ecuador, con más de 20 años de trayectoria conectando y fortaleciendo el ecosistema de educación superior del país. Opera el VOC (Centro de Operaciones de Vulnerabilidades), el SOC-CSIRT académico y el área de GRC, siendo miembro pleno de FIRST. Su misión es elevar de forma colectiva y sostenible la ciberresiliencia de las más de 90 instituciones de educación superior que integran su red.

El Desafío

CEDIA debía proteger un ecosistema extraordinariamente diverso: universidades grandes con equipos maduros, institutos técnicos donde una sola persona gestiona toda la infraestructura, y pequeñas unidades académicas con recursos limitados.

Cuatro desafíos estructurales:

- Visibilidad fragmentada: muchas instituciones desconocían qué activos estaban expuestos públicamente.
- Asimetría presupuestaria: no era viable exigir el mismo conjunto de herramientas a todas las Instituciones de Educación Superior (IES).
- Alta rotación del personal técnico, que debilitaba la continuidad operativa.
- Crecimiento permanente de la superficie de ataque: portales, repositorios, servicios cloud y plataformas de IA.

La Solución

SecurityScorecard se integró como feed externo dentro del VOC de CEDIA, convirtiéndose en pieza central del modelo operativo junto al SOC, CSIRT y GRC. La plataforma automatiza la visibilidad, la priorización y la notificación a escala para más de 90 instituciones.

Operación continua automatizada

El equipo de Ciberseguridad:

- Revisa semanalmente el panel del VOC con alertas ya filtradas y priorizadas.
- Notifica automáticamente a la IES cuando se detecta un nuevo problema.
- Genera fotografías comparativas semanales de la evolución de las instituciones.
- Envía reportes ejecutivos mensuales automatizados a CIOs y autoridades.
- Recibe alertas automáticas ante credenciales filtradas o cambios críticos.

Resultados

Mejora medible de la postura de seguridad

El porcentaje de instituciones con calificación F bajó de ~63% a menos del 20% desde la integración en marzo de 2024. Más del 18% de las IES superan ya los 90 puntos sobre 100. La ventana entre detección y acción se redujo de días o semanas a horas; en casos críticos, a minutos. Este logro fue posible mediante la colaboración coordinada entre el VOC, el CSIRT y los equipos de TI de las instituciones.

Monitoreo continuo a escala

SecurityScorecard permitió a CEDIA:

Visualizar todas las IES en un único panel centralizado

Detectar caídas de score de forma temprana

Priorizar acciones según nivel de riesgo

Reducir el esfuerzo manual en monitoreo

Decisiones más rápidas e informadas

La plataforma hizo posible:

Acelerar go/no-go con nuevos proveedores

Priorizar remediaciones según impacto real

Mantener conversaciones basadas en datos

Estandarizar criterios de evaluación

Mayor eficiencia operativa

Alertas, reportes y seguimiento histórico:

Liberaron más del 60% del tiempo operativo

Automatizaron notificaciones e informes ejecutivos

Redujeron ruido mediante correlación con IA

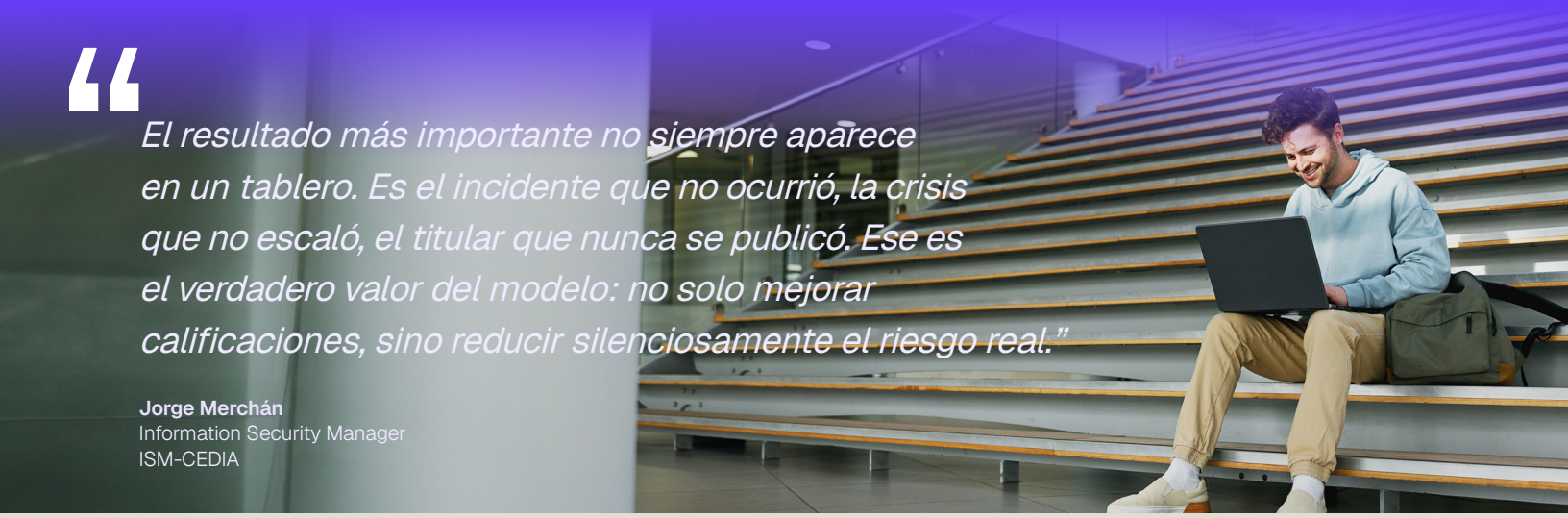
Enfocaron al equipo en los riesgos que exigen acción

~63% → <20%
Instituciones con calificación F

>18%
IES superan 90 puntos

+60%
Tiempo operativo liberado

Horas → Minutos
De detección a acción crítica



"El resultado más importante no siempre aparece en un tablero. Es el incidente que no ocurrió, la crisis que no escaló, el titular que nunca se publicó. Ese es el verdadero valor del modelo: no solo mejorar calificaciones, sino reducir silenciosamente el riesgo real."

Jorge Merchán
Information Security Manager
ISM-CEDIA

Estandarización y cambio operativo

SecurityScorecard transformó la manera en que CEDIA estructura y comparte la información de ciberseguridad con su ecosistema:

- **CIOs y autoridades:** reporte ejecutivo mensual con calificación A-F, en lenguaje orientado a decisión.
- **Equipos TI de las IES:** acceso operativo a alertas, hallazgos y remediaciones junto al VOC y CSIRT.
- **CSIRT de CEDIA:** orquestación para priorizar y traducir riesgo técnico en gobernanza.
- **Compras/Contratos:** la calificación se integra como criterio objetivo en la selección de proveedores.

La trazabilidad del modelo fortaleció la certificación ISO/IEC 27001:2022 de CEDIA y aceleró el alineamiento de las IES con el EGSI y la LOPDP.

Incidentes prevenidos antes de ocurrir:

- Credenciales filtradas identificadas y mitigadas a tiempo.
- Campañas de typosquatting interceptadas antes de convertirse en phishing activo.
- Certificados renovados y brechas cerradas antes de ser aprovechadas.

FUNCIONALIDADES UTILIZADAS

APIs y notificaciones: Feed vivo en tiempo real integrado al VOC como columna vertebral del modelo.

Planes de acción: Simula remediaciones y prioriza inversiones por retorno en reducción de riesgo.

Marcos de cumplimiento: Mapea cada IES frente a ISO/IEC 27001, EGSI ecuatoriano y LOPDP.

Reportes ejecutivos: Cierran el ciclo de gobernanza mensual sin construcción manual.

Portfolio: Prioriza el monitoreo de instituciones con mayor variación o riesgo crítico.

Mirando al futuro

CEDIA prevé expandir este modelo al ecosistema académico latinoamericano.

- Ampliar la cobertura a más instituciones miembro.
- Consolidar benchmarking interno entre IES del ecosistema.
- Posicionar a CEDIA como interlocutor estratégico ante el Ministerio de Educación, Deporte y Cultura, el CSIRT Nacional y entidades de regulación y control.
- Documentar la arquitectura VOC + SecurityScorecard como modelo replicable para otras NREN.