



Del hallazgo técnico a la decisión de directorio.

CRIQ consolida los hallazgos de sus escáneres, los prioriza por explotación confirmada y por plazo de remediación, y produce los informes ejecutivos y regulatorios que su organización debe presentar.

Un escáner informa qué encontró. No indica qué vence mañana, qué está siendo explotado hoy, ni qué debe presentarse al comité la próxima semana.

9

marcos normativos evaluados sobre los datos de su organización

6

escáneres reconocidos en la importación, en XLSX, XML y JSON

ES • EN

interfaz e informes completos en ambos idiomas

0

información de su organización fuera de su propia infraestructura



I Capacidades

Cuatro funciones que una hoja de cálculo no cubre

01 • POSTURA

Un indicador defendible, con su descomposición

Índice de riesgo de 0 a 10 que expone su origen: vulnerabilidades críticas abiertas, exposición a explotación confirmada y cumplimiento de plazos. Los proyectos se ordenan sobre una escala común, de modo que la comparación entre ellos sea válida.

- Tendencia de 30 días: aperturas frente a cierres
- Concentración de riesgo por activo
- MTTR y hallazgos fuera de plazo

02 • CUMPLIMIENTO

Nueve marcos, evaluados y no estimados

Cada control se evalúa de forma determinista contra los registros de la plataforma. Ningún modelo de lenguaje interviene en el dictamen: son reglas auditables, y un control sin evidencia se declara sin evidencia.

- Histórico diario del índice por marco
- Comparativo entre varios marcos
- Envío programado por correo, con el informe adjunto

03 • INFORMES

Documentos presentables, no exportaciones de tabla

Ejecutivo para el directorio, técnico para el equipo y regulatorio por marco. En PDF, con portada, índice y numeración. El informe ejecutivo se expresa en lenguaje de negocio: exposición, concentración de riesgo y decisiones prioritarias.

- Indicadores de gestión, no listados de CVE
- Metodología declarada en el propio documento
- Exportación a CSV cuando se requiere el detalle

04 • CONSULTA ASISTIDA

Preguntas en lenguaje natural, respuestas con sus registros

La respuesta se construye con lo que devuelve la consulta a la base, no con lo que el modelo supone. Cada cifra se acompaña de la tabla que la originó y del identificador de cada hallazgo.

- Solo lectura: no ejecuta ninguna acción
- Si el dato no existe, se informa; no se estima
- Cada consulta queda registrada en la auditoría

II Alcance operativo

Importación de escáneres

Nessus, OpenVAS, Nuclei, Nmap, Nikto y Acunetix, en XLSX, XML o JSON. El formato se detecta automáticamente.

SLA y MTTR por severidad

Plazo, antigüedad y cumplimiento de cada hallazgo. Una crítica de ocho días no equivale a una informativa.

Base de conocimiento

El análisis de un CVE se documenta una vez y se reutiliza en cada hallazgo que lo comparte.

Inteligencia de explotación

CISA KEV para explotación confirmada, EPSS para probabilidad y NVD para el detalle de cada CVE.

Proyectos y equipos

Operación multiproyecto con membresías propias, tareas en lista o tablero, responsables y vencimientos.

Notificaciones

Avisos a Slack, Teams o Discord ante una vulnerabilidad crítica nueva o una KEV detectada.

III Cumplimiento

Marcos internacionales y regulación local, en una misma evaluación

La mayoría de las plataformas cubre los marcos internacionales y deja fuera la exigencia regulatoria local. Esa parte termina resolviéndose en una hoja de cálculo aparte, con otro criterio y otra fecha de corte. CRIQ evalúa ambas sobre los mismos datos y con el mismo corte.



IV Despliegue y seguridad

Autoalojada, con los controles que la auditoría va a solicitar

Sus datos, su servidor

La plataforma opera dentro de su propia infraestructura. Hallazgos, proyectos e informes no salen de ahí.

Acceso en dos niveles

Roles de plataforma y roles por proyecto. Cada persona accede únicamente a los proyectos de los que es miembro, también en los informes.

Segundo factor

TOTP con código QR, y una política opcional que lo vuelve obligatorio para las cuentas administradoras.

Sesiones y auditoría

Sesiones activas listadas y revocables individualmente, y una bitácora separada para las acciones administrativas.

Respaldos bajo su control

Descargables y restaurables desde la propia plataforma, sin dependencia de terceros.

Español e inglés

Interfaz e informes completos en ambos idiomas, con paridad verificada entre ellos.



Agendamos una sesión de trabajo

En treinta minutos cargamos una exportación de su escáner y revisamos, sobre su propia información, la postura resultante, el informe ejecutivo y la evaluación de cumplimiento.

cesar@vectoraiq.dev

www.vectoraiq.dev