Matriz simple para priorizar pruebas ofensivas

Un marco práctico para decidir qué evaluar primero cuando existen varios activos relevantes y el equipo necesita enfocar esfuerzos.

Objetivo

Ordenar web pública, APIs, accesos remotos y red interna según riesgo real para definir por dónde partir.

Uso recomendado

Aplicar el puntaje antes de una evaluación ofensiva o cuando existe presupuesto, discusión interna o urgencia técnica.

Resultado

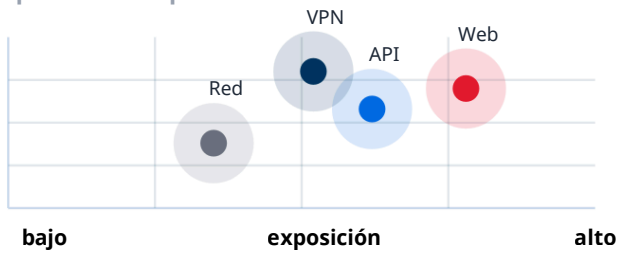
Una prioridad clara, simple de explicar y más fácil de defender frente a gerencia o equipos técnicos.

Cómo aplicar el marco

1	Selecciona los activos que hoy están en discusión o generan mayor preocupación
2	Asigna un puntaje de 1 a 3 según exposición, impacto y nivel de validación
3	Suma el total y prioriza el activo con mayor puntaje. Ese debería revisarse primero

Priorización de activos

Exposición + impacto + validación



La prioridad no depende solo de lo más visible. Depende de la combinación entre exposición, criticidad, datos involucrados y controles que no han sido validados recientemente.

MATRIZ DE PRIORIZACIÓN

Evalúa cada opción con puntaje de 1 a 3

1 bajo | 2 medio | 3 alto. Luego suma el total por columna y parte por el activo con mayor puntaje.

Criterio	Web pública	APIs	Acceso remoto / VPN	Red interna
Está expuesto a internet				
Maneja datos sensibles				
Tiene cambios recientes				
Es crítico para la operación				
Tiene controles poco validados				
Total				

12 a 15 puntos
Prioridad alta. Conviene revisarlo primero.

8 a 11 puntos
Prioridad media. Planificación cercana.

5 a 7 puntos
Prioridad baja. No debe salir del radar.

Recomendación práctica
Empieza por el activo con mayor exposición, datos sensibles, impacto operativo y poca validación reciente.
Enfoca la ciberseguridad ofensiva donde entrega más valor.

Validamos tus defensas como lo haría un atacante real.