10 Señales de que tus Controles de Seguridad No Están Funcionando

Checklist para CISO · Validación de controles con Picus Security · Nuvol Cybersecurity

Si marcas 3 o más señales, tu postura de seguridad tiene brechas críticas no visibles.

¿Para qué sirve este checklist?

La mayoría de las organizaciones asumen que sus controles de seguridad funcionan porque los compraron e instalaron. **Picus Security Control Validation** demuestra cuáles realmente bloquean ataques reales — y cuáles no. Este checklist te ayuda a identificar las señales de alerta antes de que lo descubra un atacante.

01 Señales 1–5 — Brechas en Detección y Respuesta

1 ☐ Tu pentesting anual no generó alertas en el SIEM

Si el red team logró moverse lateralmente sin que ningún control lo detectara, tu SIEM no está correlacionando correctamente o tus reglas de detección están desactualizadas.

Síntoma: 0 alertas durante un ejercicio de pentest activo
Riesgo: Atacante real puede operar semanas sin ser detectado

2 ☐ No sabes qué porcentaje de técnicas MITRE ATT&CK bloqueas

Si no puedes responder cuántos TTPs del top 10 de tu sector bloqueas hoy, no tienes visibilidad real de tu postura. Picus SCV entrega ese número en horas.

Síntoma: Sin métrica de cobertura MITRE ATT&CK documentada
Riesgo: Brecha invisible para el board y los reguladores

3 ☐ Tu EDR no detectó malware en pruebas de simulación

Los EDR bien configurados deben detectar ransomware moderno, loaders y RATs. Si en una simulación controlada el EDR no generó alerta, hay un gap de configuración crítico.

Síntoma: Malware simulado ejecutado sin alerta del EDR
Riesgo: Ransomware real puede cifrar activos antes de ser contenido

4 ☐ El firewall tiene reglas sin revisar de más de 6 meses

Las reglas de firewall obsoletas acumulan excepciones que nunca se cierran. Cada excepción sin revisar es una puerta potencialmente abierta para un atacante.

Síntoma: Reglas con fecha de creación mayor a 180 días sin auditoría
Riesgo: Tráfico malicioso puede pasar por excepciones olvidadas

5 ☐ No tienes métricas de MTTD y MTTR documentadas

Si no mides cuánto tarda tu SOC en detectar (MTTD) y contener (MTTR) un incidente, no puedes demostrar mejora ni cumplir con requerimientos regulatorios de CNBV y Banxico.

Síntoma: Sin SLA de respuesta medido ni reportado al board
Riesgo: Incumplimiento regulatorio y exposición prolongada

02 Señales 6–10 — Brechas en Prevención, ROI y Visibilidad

6 ☐ Tu email gateway dejó pasar un correo BEC en prueba

Los ataques BEC generados por IA no contienen malware ni dominios maliciosos. Si tu gateway filtra solo por firmas, un correo que suplanta al CFO llegará a la bandeja.

Síntoma: Correo de phishing sin payload pasó el gateway sin alerta
Riesgo: Fraude por transferencia no autorizada — pérdida directa

7 ☐ Tienes herramientas de seguridad con agentes desactualizados

Un EDR, DLP o endpoint con agente de más de 30 días sin actualizar no aplica las últimas reglas de detección. La cobertura real es menor a la cobertura contractual.

Síntoma: Agentes desactualizados en más del 15% de endpoints
Riesgo: Falsa sensación de cobertura — brechas reales no visibles

8 ☐ No puedes demostrar el ROI de tus herramientas al CFO

Si el CFO pregunta para qué sirve cada herramienta del stack y no tienes métricas de valor por herramienta, estás en riesgo de recortes de presupuesto en seguridad.

Síntoma: Sin reporte de valor por herramienta para la dirección
Riesgo: Presupuesto de seguridad vulnerable a recortes injustificados

9 ☐ Tu SIEM genera más de 500 alertas al día sin priorización

Un SIEM que genera cientos de alertas sin contexto ni severidad crea fatiga de alertas. Los analistas priorizan mal y un incidente crítico puede perderse entre el ruido.

Síntoma: Tasa de falsos positivos superior al 70% en alertas SIEM
Riesgo: Incidentes reales ignorados por saturación del equipo SOC

10 ☐ No tienes validación continua — solo auditorías anuales

Una auditoría anual es una fotografía del ambiente en un día específico. En 365 días el ambiente cambia: actualizaciones, nuevas integraciones, cambios de configuración. Sin validación continua, la seguridad entre auditorías es un punto ciego total.

Síntoma: Última prueba técnica hace más de 90 días
Riesgo: El ambiente cambió — los controles ya no son los auditados

¿Cuántas señales marcaste?

0 – 2 señales	3 – 5 señales	6 o más señales
Postura saludable. Mantén la validación continua para sostenerla.	Brechas moderadas. Agenda una evaluación técnica con Nuvol + Picus.	Brechas críticas. Tus controles tienen gaps que un atacante puede explotar hoy.

¿Identificaste brechas? Picus Security Control Validation las cierra.

Nuvol Cybersecurity es el partner certificado de Picus Security en México, Panamá y Colombia.

Implementamos Security Control Validation para que sepas con exactitud qué herramientas funcionan, cuáles optimizar y cómo demostrarlo al board y al regulador con métricas auditables.

cybernuvol.com/breach-attack-simulation-bas-mexico

info@cybernuvol.com · MX +52 55 9124 0158 ·