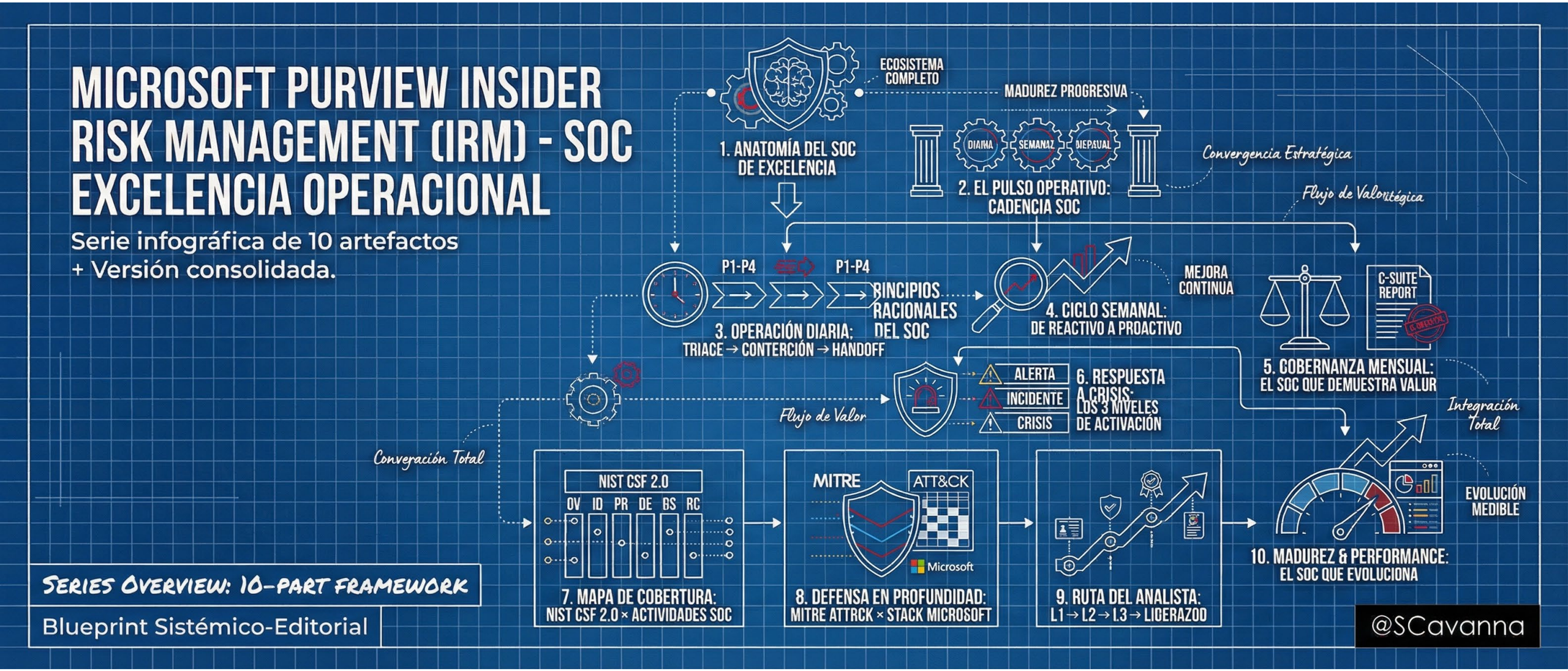
IRM

https://www.linkedin.com/....

MICROSOFT PURVIEW INSIDER RISK MANAGEMENT (IRM) - SOC EXCELENCIA OPERACIONAL

Serie infográfica de 10 artefactos
+ Versión consolidada.



Series Overview: 10-part framework

Blueprint Sistémico-Editorial

@SCavanna

— MASTER PLAN —

Microsoft Purview Insider Risk Management & SecOps: Excelencia Operacional del SOC

SISTEMA INTEGRADO DE OPERACIONES DE SEGURIDAD (1/10 → 10/10)

BLOCK 3/10: OPERACIÓN DIARIA: TRIAGE → CONTENCIÓN → HANDOFF

Sequencial/Narrativo

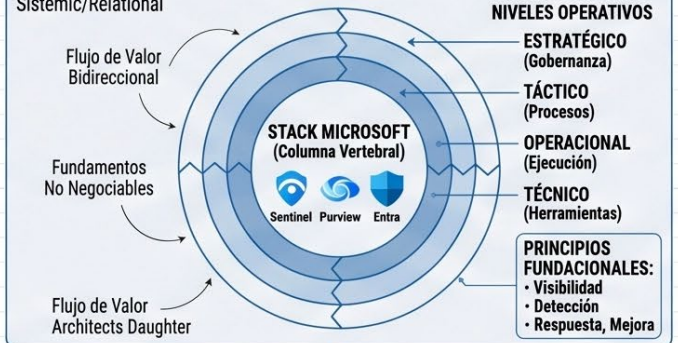
1. TRIAGE (Priorización)
- Criterios P1-P4
- SLA Triage: <15m

2. CONTENCIÓN (Respuesta Rápida)
- Acciones Inmediatas
- SLA Contención: <60m (P1)

3. HANDOFF (Transición de Turno)
- Documentación, Comunicación
- SLA Handoff: Fin de Turno

BLOCK 1/10: ANATOMÍA DEL SOC DE EXCELENCIA

Sistemic/Relational



PRINCIPIOS FUNDACIONALES:
- Visibilidad
- Detección
- Respuesta, Mejora

BLOCK 5/10: GOBERNANZA MENSUAL: EL SOC QUE DEMUESTRA VALOR

Analítico/Jerárquico

BLOCK 4/10: CICLO SEMANAL: DE REACTIVO A PROACTIVO

Editorial/Modular

TUNING (Afinar Detecciones)
- Reducción Falsos Positivos
- Optimización Reglas KQL

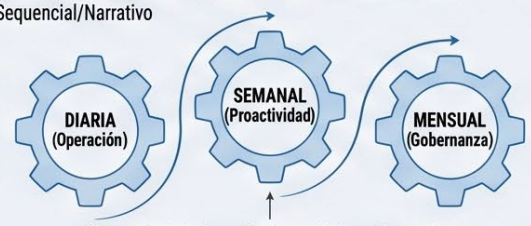
HUNTING (Caza de Amenazas)
- Búsqueda Hipótesis-Driven
- Identificación de Tácticas

UEBA (Análisis Comportamiento)
- Detección de Desviaciones
- Riesgo de Usuario

LESSONS LEARNED (Aprendizaje Continuo)
- Análisis Post-Incidente
- Actualización de Procedimientos

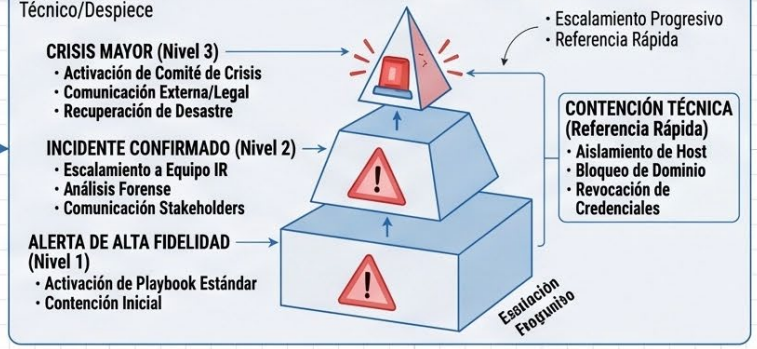
BLOCK 3/10: EL PULSO OPERATIVO: CADENCIA SOC

Sequencial/Narrativo



BLOCK 6/10: RESPUESTA A CRISIS: LOS 3 NIVELES DE ACTIVACIÓN

Técnico/Despiece



- Flujo Operativo de Turno
- Velocidad y Precisión

- Escalamiento Progresivo
- Referencia Rápida

BLOCK 7/10: MAPA DE COBERTURA: NIST CSF 2.0 × ACTIVIDADES SOC

Sistémico

	SOC					
	Monitoreo (Detectar)	Triage (Responder)	Hunting (Detectar)	Tuning (Proteger)	IR Plan (Gobernar)	Lessons Learned (Recuperar)
GOBERNAR	✓	✓	✓	✓		
IDENTIFICAR	✓	✓	✓	✓		✓
PROTEGER	✓	✓		✓	✓	
DETECTAR	✓	✓	✓			
RESPONDER		✓	✓	✓		✓
RECUPERAR					✓	✓

Cobertura Core (Azul Fuerte) | Cobertura Complementaria (Azul Claro)

BLOCK 8/10: DEFENSA EN PROFUNDIDAD: MITRE ATT&CK × STACK MICROSOFT

Analítico/Jerárquico

	Reconnaissance	Resource Development	Initial Access	Execution	Prisistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collecion	Command and Control	Exfiltration	Impact
Detecciones SOC	✓	✓	✓		✓		✓		✓	✓				✓
Herramientas Microsoft Específicas (Sentinel, Defender)													…	
Evaluación de Brechas (Rojo/Amarillo/Verde)													…	

BLOCK 10/10: MADUREZ & PERFORMANCE: EL SOC QUE EVOLUCIONA

Analítico/Jerárquico

Analítico/Jerárquico

ANATOMÍA DEL SOC DE EXCELENCIA [1/10]

LOS 4 PRINCIPIOS FUNDACIONALES (EL CORE)

DETECCIÓN TEMPRANA
Métrica: MTTD ≤ Umbral Definido.
Alineación: ISO 27001 / NIST CSF 2.0 (Controles Documentados).

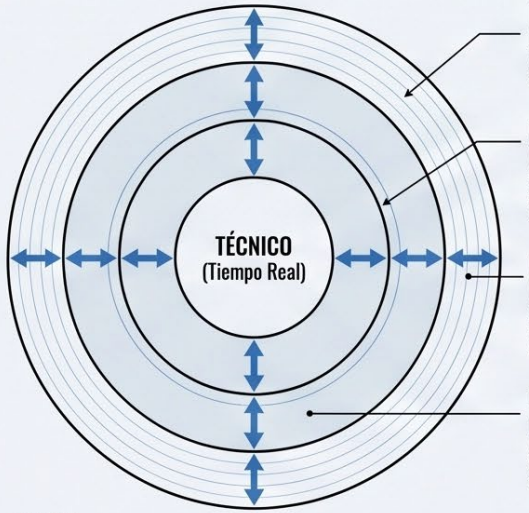
CONTENCIÓN EFECTIVA
Métrica: MTTR Medido y Decreciente.
Foco: Reducción de Impacto.

CONTINUIDAD OPERACIONAL
Métrica: Uptime de Conectores/ Playbooks.
Resiliencia del Sistema.

MEJORA CONTINUA
Métrica: Ciclos de Tuning, Lessons Learned.
Optimización Constante.

Base para la Madurez & Performance

ARQUITECTURA DE 4 NIVELES OPERATIVOS



ESTRATÉGICO (Trimestral/Anual)
¿Cómo está nuestra postura de seguridad? Cadena:

OPERATIVO (Diario/Semanal)
¿Detectamos y contenemos eficazmente?
Cadena: Diaria/Semanal.

TÁCTICO (Mensual)
¿Mejoramos nuestra capacidad de detección?
Cadena: Semanal/Mensual.

ESTRATÉGICO (Trimestral/Anual)
¿Cómo está nuestra postura de seguridad?
Cadena: Mensual.

Operación en paralelo, no en cascada. Evita vacíos de visibilidad.

STACK TECNOLÓGICO MICROSOFT: TEJIDO CONECTIVO

UN SOC DE EXCELENCIA NO SE DEFINE POR SUS HERRAMIENTAS, SINO POR LA CONSISTENCIA, TRAZABILIDAD Y MEJORA CONTINUA DE SUS OPERACIONES.

Flujo de Datos Bidireccional

El cerebro que centraliza y orquesta la inteligencia

MICROSOFT DEFENDER XDR
(Endpoints, Email, Identity, Cloud Apps)
- Detección Nativa Multivector

MICROSOFT ENTRA ID
(Identity Risk, Sign-in Risk, PIM)
- Primera Línea de Detección de Identidad

MICROSOFT SENTINEL
(SIEM / SOAR / UEBA)
- Correlación, Automatización, Hunting

Integración Vía Conectores

Flujo de Señales y Alertas

Cobertura de Dominios Específicos

MICROSOFT PURVIEW
(Compliance, IRM, DLP)
- Protección de Datos y Gobierno

Alineación Estratégica

Evolución Constante

ROLES Y RESPONSABILIDADES: LA CADENA HUMANA

L1 — JUNIOR
(Triage y Monitoreo)
70% Triage, 20% Doc, 10% Formación.
Volumen de Incidentes.

L2 — SENIOR
(Investigación y Correlación)
40% Investigación, 30% Tuning, 20% Contención, 10% Mentoría
Profundidad Analítica.

L3 — ESPECIALISTA
(Detección Avanzada)
40% Hunting, 30% Ingeniería, 20% Arquitectura, 10% Crisis.
Especialización.

SOC LEAD
(Gobernanza y Mejora)
30% Gobernanza. 30% Comunicación. 30% Mejora. 20% Estrategia.
Visión Transversal

Ruta de Desarrollo y Madurez

Evitar "Fábricas de Escalamiento" con desequilibrio de roles.

EL CICLO VIRTUOSO: DE OPERAR A EVOLUCIONAR

OPERAR
(Con Capacidad Mejorada)

MEDIR
(Semanal/Mensual)
Evaluación de desempeño y métricas.

APRENDER
(Post-Incident Reviews)
Análisis de lecciones y brechas.

MEJORAR
(Tuning, Nuevos Playbooks).
Implementación de optimizaciones.

Mecanismo de Transición de Madurez

@SCavanna

EL PULSO OPERATIVO: CADENCIA SOC

Bloque 2/10 — Diario · Semanal · Mensual · Ad-hoc

01. ENGRANAJE DIARIO
(Velocidad y Consistencia)

Foco: Detección temprana, contención, continuidad
Ritmo: Ciclo de Turno (Inicio → Operación → Cierre)
Output: Cola priorizada, Alertas clasificadas (TP/FP)
Responsable: L1 (triage) + L2 (análisis)

Architects Daughter: Genera datos crudos para análisis de tendencias.

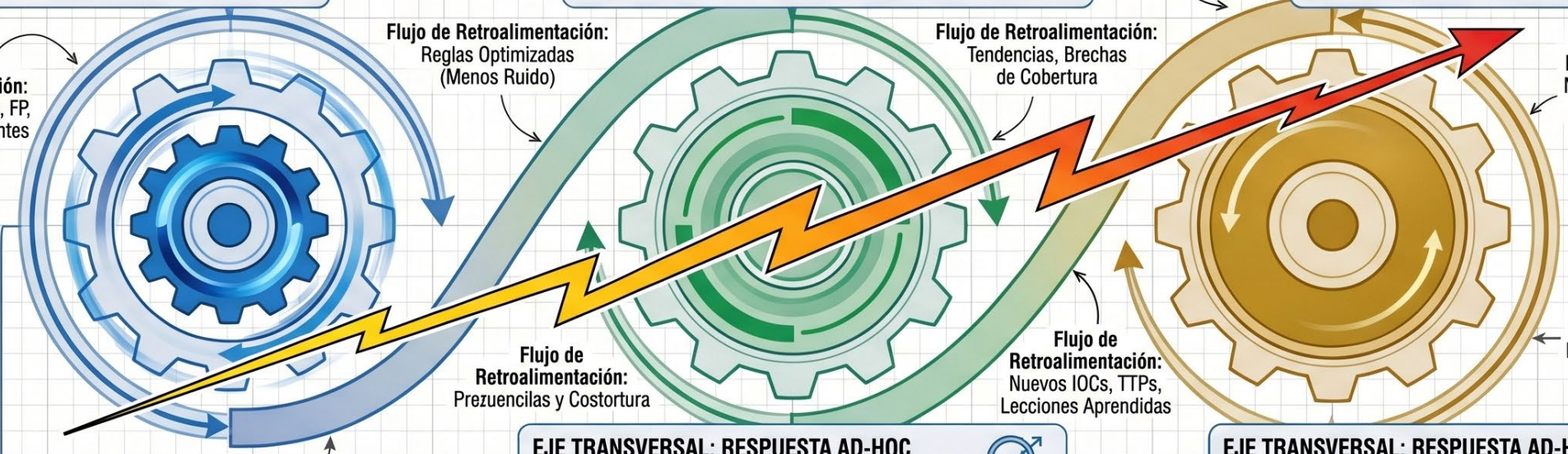
02. ENGRANAJE SEMANAL
(Inteligencia y Calibración)

Foco: Calidad de detección, reducción de ruido, mejora continua
Ritmo: Sesiones estructuradas
Output: Reglas optimizadas, Hipótesis hunting, Lessons learned
Responsable: L2 (tuning) + L3 (hunting) + SOC Lead

Architects Daughter: Diferenciador: reactivo vs proactivo. Alimenta el reporte ejecutivo.

03. ENGRANAJE MENSUAL
(Gobernanza y Evolución)

Foco: Gobernanza, madurez, valor ejecutivo, costos
Ritmo: Revisiones estructuradas (1ª semana)
Output: Reporte Ejecutivo, KPIs, Roadmap, Compliance
Responsable: SOC Lead (gobierno) + L3 (evaluación)



EJE TRANSVERSAL: RESPUESTA AD-HOC
(Activación por Crisis)

Nivel 1 (Alerta Alta Fidelidad): Absorbe L2/L3 temporalmente (Amarillo)
Nivel 2 (Incidente Confirmado): Prioridad sobre Semanal (Naranja)
Nivel 3 (Crisis Mayor): Suspende Cadencias Regulares (Rojo)

EJE TRANSVERSAL: RESPUESTA AD-HOC
(Activación por Crisis)

- **Foco:** Gobernanza, madurez, valor ejecutivo, costos
- **Ritmo:** Revisiones estructuradas (1ª semana)
- **Output:** Reporte Ejecutivo, KPIs, Roadmap, Compliance
- **Responsable:** SOC Lead (gobierno) + L3 (evaluación)

INSIGHTS OPERATIVOS CRÍTICOS (Consultivo)

- Bloquear tiempo calendario para Semanal/Mensual (evitar “cuando haya tiempo”).
- Operar 24/7 ≠ Madurez (requiere Tuning y Gobernanza).
- Cadencias = Evidencia de Cumplimiento (NIST CSF, ISO 27001).

MÉTRICAS & CAPACIDAD (Estimación Consultiva)

Reserva de capacidad para Ad-hoc es clave para evitar colapso.

OPERACIÓN DIARIA SOC: TRIAGE → CONTENCIÓN → HANDOFF [Bloque 3/10]

El Ciclo de Turno como Motor de Excelencia: Disciplina, Trazabilidad y Flujo Continuo.

La excelencia diaria no se construye con heroísmo individual sino con disciplina de turno: cada analista ejecuta el mismo flujo, con el mismo rigor, generando trazabilidad completa independientemente de quién opera.

CONCEPT 3: EL HANDOFF: CONTRATO EXPLÍCITO

- ☑ Incidentes Activos
- ☑ Alertas Pendientes
- ☑ Contexto Crítico
- ☑ Estado Infraestructura
- ☑ Escalamientos

Architects Daughter:
Anti-patrón mortal: El handoff verbal. Si no está escrito, no existe.

FASE 1: INICIO — PREPARAR EL TERRENO (Primeros 30 min)

S-Pattern

- **E1: Revisar Handoff** (Sentinel/Teams)
- **E2: Verificar Conectores** (Sentinel Data Connectors)
- **E3: Revisar Playbooks Fallidos** (Logic Apps History)

Architects Daughter:
Insight: Los primeros 30 min son críticos. Operar sin revisar es operar a ciegas.

FASE 2: OPERACIÓN — EJECUCIÓN DISCIPLINADA (Durante el Turno)

- **E4: Triage Priorizado** (Sentinel Incidents)
- **E5: Análisis y Clasificación** (Sentinel/Defender XDR)
- **E6: Validación de Correlaciones** (Sentinel)
- **E7: Revisión de Riesgo de Identidad** (Entra ID)
- **E8: Documentación en Tiempo Real** (Sentinel Notes)
- **E9: Escalamiento según SOP** (Canal Definido)

Concepto 2: La Matriz de Priorización

Concepto 5: Documentación

CONCEPT 2: MATRIZ DE PRIORIZACIÓN: URGENCIA vs. IMPACTO

- **P1 Critical (<15 min*)** Impacto Inminente. Acción Inmediata.
- **P2 High (<1 hour*)** Alta Fidelidad. Investigación Profunda.
- **P3 Medium (<4 hours*)** Comportamiento Sospechoso. Análisis L2.
- **P4 Low/Info (<24 hours*)** Bajo Riesgo. Documentar/Monitorear.

Architects Daughter:
Regla de Oro: Ante la duda, asignar la prioridad más alta.

MÉTRICAS DIARIAS OBSERVABLES (CONSULTIVAS*)

- **Alertas vs Procesadas** (Ratio > 1.5 = Alerta)
- **Tiempo Primer Triage P1** (>30 min = Alerta)
- **Playbooks Fallidos** (>3 = Alerta)

FASE 3: CIERRE — TRANSICIÓN ESTRUCTURADA (Últimos 30 min)

- **E10a: Actualizar Estado de Incidentes** (Sentinel Incidents)
- **E10b: Preparar Handoff** (Formato Estandarizado)
- **E10c: Comunicar al Negocio** (Email/Teams)

Architects Daughter:
Loop Infinito: El cierre alimenta el inicio del siguiente turno.

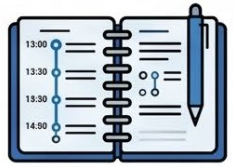
CONCEPT 4: CLASIFICACIÓN: EL VOCABULARIO COMÚN

Real/No Real vs. Malicioso/Legítimo

TP (True Positive). Malicioso Confirmado. Acción Requerida.	**BP*** (Benign Positive*). Real pero Legítimo. Excepción.
FP (False Positive). Alerta Incorrecta. Candidata a Tuning.	**TN*** (True Negative*). No Alerta, No Amenaza. (No visible en operación diaria)

Architects Daughter:
***BP y TN son términos consultivos, no estándar oficial Microsoft.**

CONCEPT 5: DOCUMENTACIÓN: AUDIT TRAIL VIVIENTE



Qué documentar:
Decisión de Clasificación,
Evidencia Consultada,
Acciones de Contención,
Contexto Verbal,
Razón de Escalamiento.

Architects Daughter:
Regla del "Analista Ausente": ¿Puede otro reconstruir el análisis solo leyendo la documentación?

Advertencia: Métricas y tiempos marcados con * son consultivos, no estándar oficial Microsoft.

BLOQUE 4/10 — CICLO SEMANAL: DE REACTIVO A PROACTIVO

El organismo que aprende: Transformando el ruido en inteligencia estructural.

REACTIVO (Diario)
Temperatura Pasada

Architects Daughter
El salto cualitativo: De fábrica de triage a radar estratégico

PROACTIVO (Semanal)
Amenazas Futuras

CLUSTER A: CALIDAD DE DETECCIÓN
"¿Estamos detectando bien?"

1. Tuning de Reglas Analíticas
(Sentinel Analytics)

Reducir FP/FN

FRAMEWORK DE TUNING
(El Arte de Reducir Ruido)

1. **Identificar** (Top 10 Vol.) → 2. **Clasificar** (TP/FP/Benign)
3. **Diagnosticar** (KQL/Umbral) ← 4. **Ajustar** (Refinar lógica)
5. **Validar** (Monitoreo) → 6. **Documentar** (Historial)

Architects Daughter
Si FP alto: Candidata urgente.
No deshabilitar, **¡tunear!**

3. Threat Hunting Manual
(Sentinel Hunting)

FRAMEWORK DE HUNTING
(6 Pasos)

1. **Hipótesis** (Pregunta falsificable)
2. **Datos** (Disponibilidad tablas)
4. **Análisis** (Descartar FP)
5. **Documentación** (Bookmarks)
6. **Acción** (Hallazgo o "Caza sin hallazgo")

Architects Daughter
Inputs: ATT&CK Gaps, TI Sectorial, Anomalías UEBA

→ **Nueva Regla Analítica**
→ **Evidencia de Ausencia**

4. Revisión UEBA Insights
(Anomalías de comportamiento)

5. Evaluación Cobertura MITRE ATT&CK
(Gaps tácticos)

CLUSTER B: VISIBILIDAD Y POSTURA
"¿Estamos viendo todo?"

6. Health de Conectores/Fuentes
(Gaps silenciosos)

Architects Daughter
Sensores de Deriva:
Alertan degradación silenciosa

7. Validación Integración XDR ↔ Sentinel
(Ingesta correcta Defender)

8. Revisión Secure Score
(Posture Drift)

Alerta de Degradación

CLUSTER C: APRENDIZAJE Y EVOLUCIÓN
"¿Estamos mejorando?"

2. Análisis Tendencias Incidentes
(Patrones semanales)

9. Actualización Runbooks Operativos
(Reflejar realidad)

10. SESIÓN LESSONS LEARNED
(El Motor de Evolución)

1. **Contexto** (10m, Hechos)
2. **Detección** (10m, ¿Fue temprano?)
3. **Respuesta** (10m, ¿Qué mejorar?)
4. **Impacto** (5m, Negocio)
5. **Acciones** (15m, Concretas)
6. **Asignación** (5m, Dueño/Plazo)

Architects Daughter
Regla de oro: No blame.
Cada sesión genera al menos **UNA acción concreta.**

OUTPUTS DE LA SESIÓN

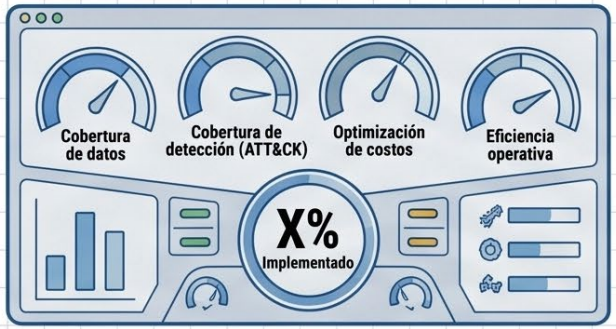
→ **Ajuste Tuning** (Bloque 3)
→ **Actualización Playbooks** (Bloque 3)
→ **Input Reporte Ejecutivo** (Bloque 5)

Montserrat/Inter

GOBERNANZA MENSUAL: EL SOC QUE DEMUESTRA VALOR

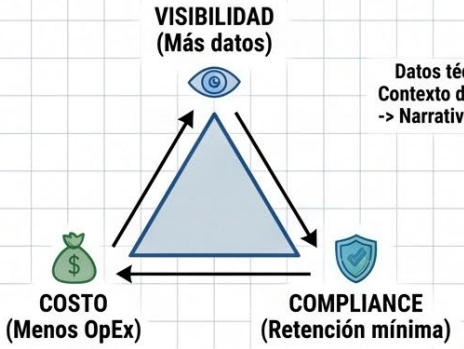
Transformando datos operativos en narrativa de valor — el lenguaje que entiende la C-Suite

SOC OPTIMIZATION: EL COPILOTO ESTRATÉGICO

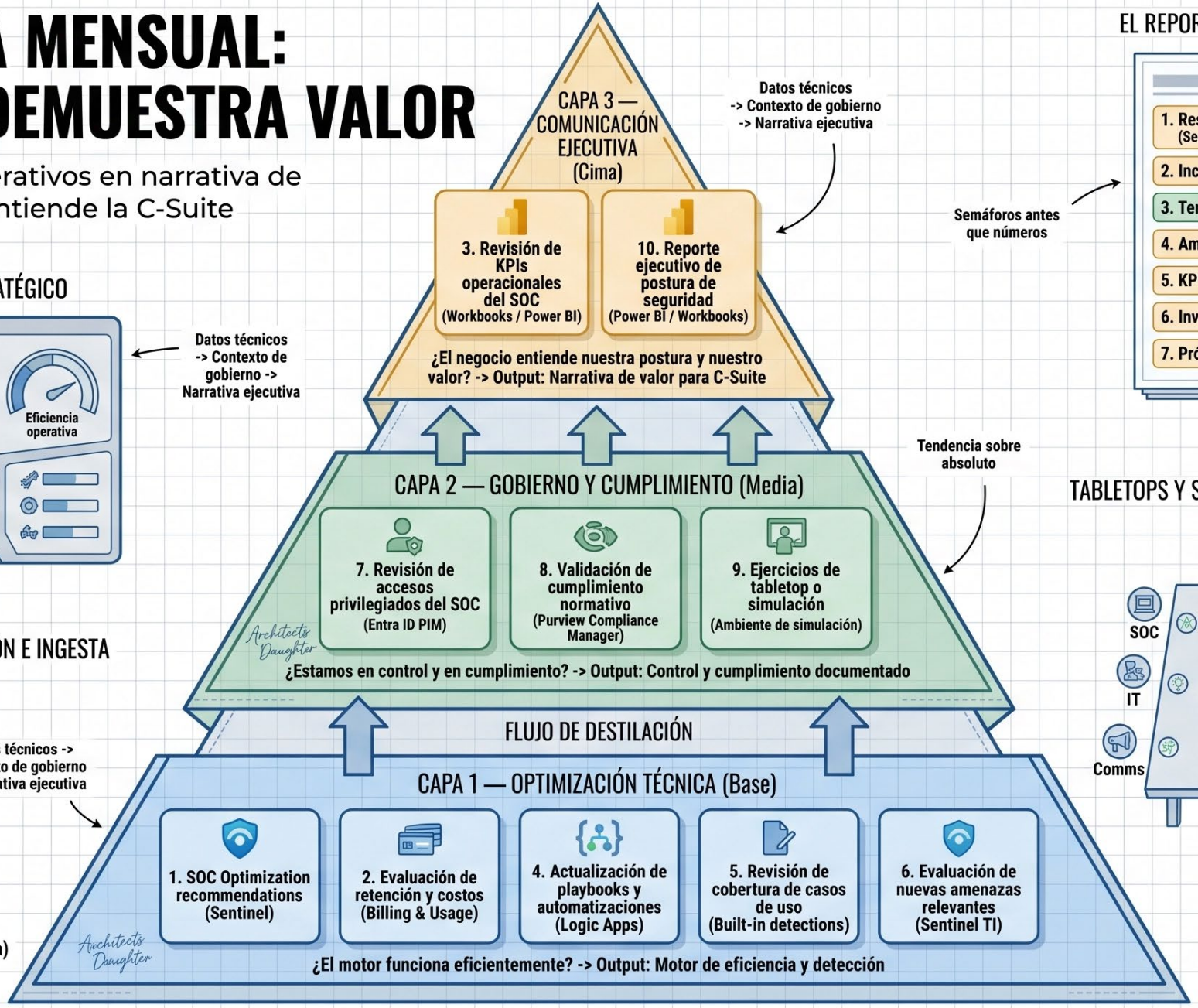


Datos técnicos -> Contexto de gobierno -> Narrativa ejecutiva

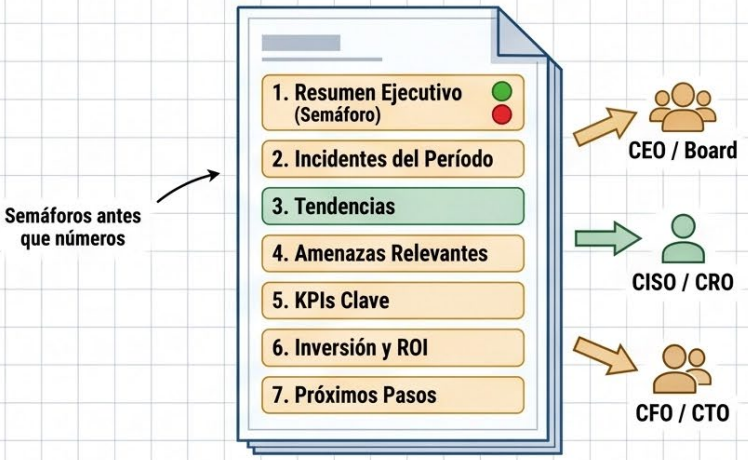
ECONOMÍA DEL SOC: COSTOS, RETENCIÓN E INGESTA



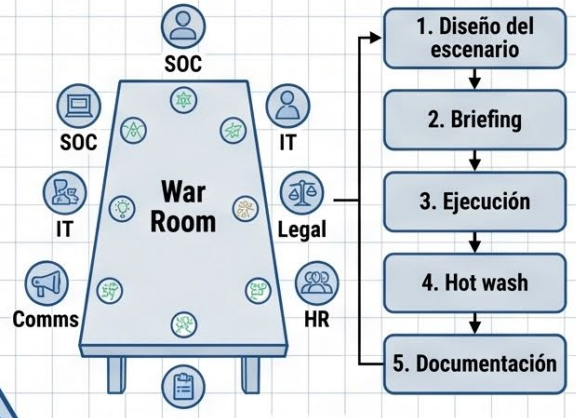
Equilibrio mensual: Filtrar sin perder cobertura, retener según regulación



EL REPORTE EJECUTIVO: NARRATIVA DE VALOR



TABLETOPS Y SIMULACIONES: PROBAR SIN ROMPER



Revela:

- Roles confusos
- Brechas de comunicación
- Tiempos reales

ACTO 6/10 — RESPUESTA A CRISIS: LOS 3 NIVELES DE ACTIVACIÓN

La improvisación en respuesta a incidentes es uno de los principales vectores de error operativo. Los 3 niveles existen para que cada escalamiento sea una decisión predefinida, no una reacción bajo estrés. (⚠ **Consultivo**)

NIVEL 1 — ALERTA DE ALTA FIDELIDAD (SOC L2/L3)

TRIGGER: Alerta alta confianza TP, sin impacto confirmado.
OBJETIVO: Validar y contener rápido.
PERÍMETRO: SOC únicamente.
1-4 horas (⚠)

1. Análisis profundo (Sentinel Graph) → 2. Correlación Logs (KQL) → 3. Enriquecimiento TI (VirusTotal/MSTIC) → 4. Evaluación Impacto (Risk Scoring) → 5. Escalamiento (SOP) → 6. Documentación (Case Notes)

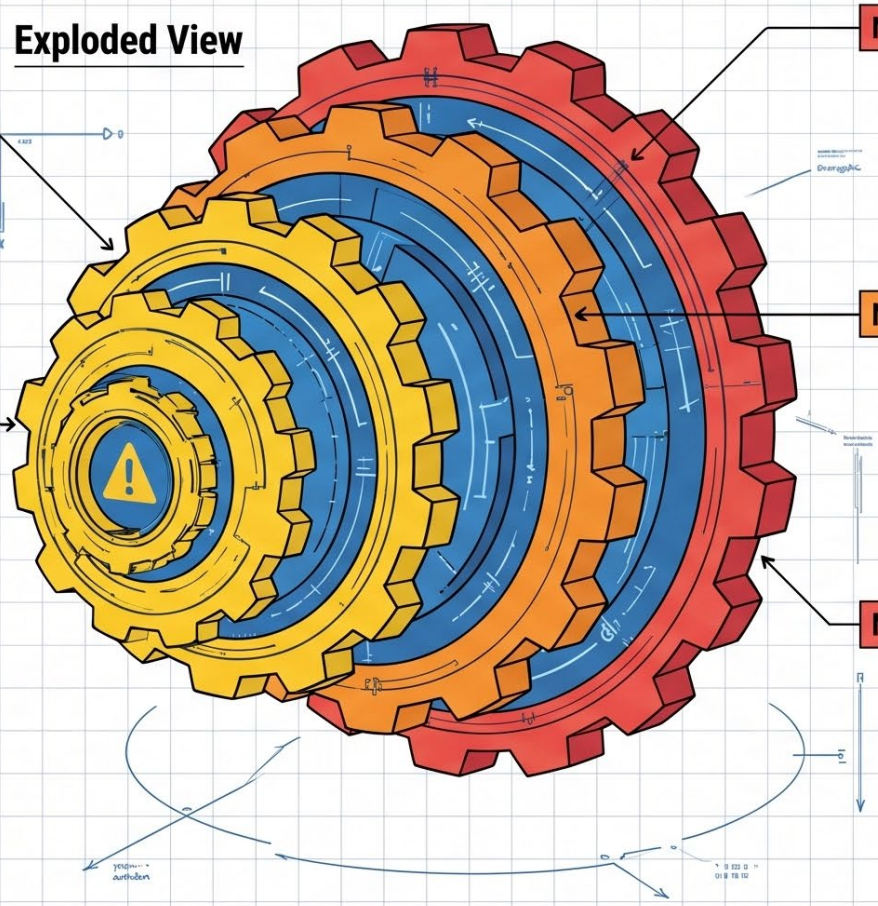
↓ **Decisión Explícita: SOC Lead** (si impacto confirmado)

NIVEL 1 — ALERTA DE ALTA FIDELIDAD (SOC L2/L3)

TRIGGER: Alerta alta confianza TP, sin impacto confirmado.
OBJETIVO: Validar y contener rápido.
PERÍMETRO: SOC únicamente. **1-4 horas (⚠)**

1. Análisis profundo (Sentinel Graph) → 2. Correlación Logs (KQL) → 3. Enriquecimiento TI (VirusTotal/MSTIC) → 4. Evaluación Impacto (Risk Scoring) → 5. Escalamiento (SOP) → 6. Documentación (Case Notes)

Exploded View



NIVEL 3 — CRISIS / INCIDENTE MAYOR (Organización Completa)

TRIGGER: Impacto amplio, sistemas críticos comprometidos.
OBJETIVO: Activar IR Plan completo, coordinación organizacional.
PERÍMETRO: CISO, SOC, IT, Legal, Comms, HR, Mgmt.
Días a semanas (⚠)

1. Activar IR Plan → 2. Convocar IR Team → 3. Establecer War Room → 5. Updates 30-60 min → 6. Coord. Legal → 7. Comms Externas → 8. PIR Completo

NIVEL 2 — INCIDENTE CONFIRMADO (SOC + IT + Stakeholders)

TRIGGER: Impacto confirmado en sistemas/datos/usuarios.
OBJETIVO: Contener, erradicar, recuperar con mínimo impacto.
PERÍMETRO: SOC, IT, afectados directos. **4-48 horas (⚠)**

1. Creación Caso Formal → 4. Deshabilitar Cuenta (Entra ID) → 6. Preservación Forense (Live Response) → 7. RCA (KQL) → 8. Comunicación Ejecutiva → 9. Cierre Formal → 10. Post-Incident Review

↓ **Decisión Explícita: CISO** (si impacto crítico)

NIVEL 3 — CRISIS / INCIDENTE MAYOR (Organización Completa)

TRIGGER: Impacto amplio, sistemas críticos comprometidos.
OBJETIVO: Días horas (⚠)

1. Activar IR Plan → 2. Convocar IR Team → 3. Establecer War Room → **WAR ROOM** EY eteam (Teams Dedicado) → 6. Coord. Legal → 7. Comms Externas → 8. PIR Completo

PRIORIDAD DE CONTENCIÓN (Regla de Oro ⚠)

P1: DETENER	P2: PRESERVAR	P3: ERRADICAR
(Aislar endpoint, Deshabilitar cuenta, Revocar sesiones)	(Evidencia forense **ANTES** de remediar)	(Eliminar persistencia, Restablecer, Restaurar)

⚠ **REGLA: PRESERVAR EVIDENCIA ANTES DE REMEDIAR**

ARSENAL DE CONTENCIÓN — REFERENCIA RÁPIDA DE HERRAMIENTAS (⚠ Consultivo)

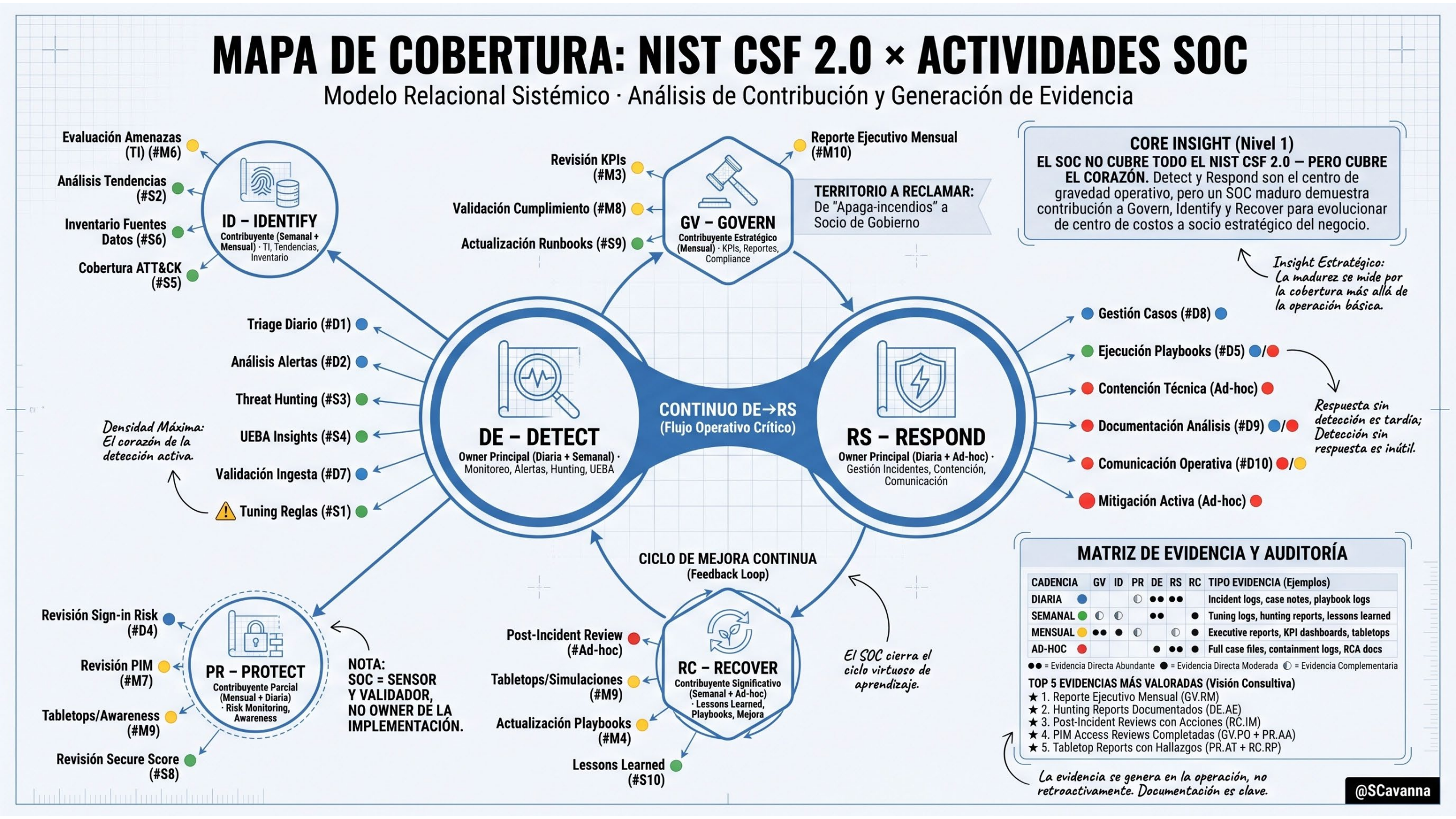
ENDPOINT (Defender)	IDENTIDAD (Entra ID)	EMAIL (Defender for Office)	CLOUD APPS (Defender for Cloud Apps)	RED/PERÍMETRO (Sentinel/FW)	DATOS/COMPLIANCE (Purview)
→ Aislar device → Collect package → Live Response	→ Block sign-in → Revoke sessions → Revoke MFA → Revoke OAuth	→ Quarantine emails → Block sender	→ Disable app → Revoke 3rd party access	→ Block IP (Playbook) → Block domain	→ Forensic/Insider actions → eDiscovery hold

IR TEAM (Nivel 3)

CISO (Estrategia) ↔ **SOC Lead** (Coord.) ↔ **L3/IT** (Técnica)
Legal (Regulat.) · **Comms** (Mensaje) · **HR** (Personal) ↔ **Management** (Negocio)

MAPA DE COBERTURA: NIST CSF 2.0 × ACTIVIDADES SOC

Modelo Relacional Sistémico · Análisis de Contribución y Generación de Evidencia



MATRIZ DE EVIDENCIA Y AUDITORÍA

CADENCIA	GV	ID	PR	DE	RS	RC	TIPO EVIDENCIA (Ejemplos)
DIARIA			◐	●●	●●		Incident logs, case notes, playbook logs
SEMANAL	◐	◐		●●		●	Tuning logs, hunting reports, lessons learned
MENSUAL	●●	●	◐		◐	●	Executive reports, KPI dashboards, tabletops
AD-HOC				●	●●	●	Full case files, containment logs, RCA docs

●● = Evidencia Directa Abundante ● = Evidencia Directa Moderada ◐ = Evidencia Complementaria

TOP 5 EVIDENCIAS MÁS VALORADAS (Visión Consultiva)

★ 1. Reporte Ejecutivo Mensual (GV.RM)
★ 2. Hunting Reports Documentados (DE.AE)
★ 3. Post-Incident Reviews con Acciones (RC.IM)
★ 4. PIM Access Reviews Completadas (GV.PO + PR.AA)
★ 5. Tabletop Reports con Hallazgos (PR.AT + RC.RP)

La evidencia se genera en la operación, no retroactivamente. Documentación es clave.

@SCavanna

DEFENSA EN PROFUNDIDAD: MITRE ATT&CK × STACK MICROSOFT

KILL CHAIN DEL ADVERSARIO (11 Tácticas: Flujo de Detección Temprana a Tardía)

Detección temprana = Máximo valor

Detección tardía = Mínimo margen

TA0001 Initial Access → TA0002 Execution → TA0003 Persistence → TA0004 Privilege Escalation → TA0005 Defense Evasion → TA0006 Credential Access → TA0007 Discovery → TA0008 Lateral Movement → TA0009 Collection → TA0010 Exfiltration → TA0040 Impact

Ventana de Oportunidad

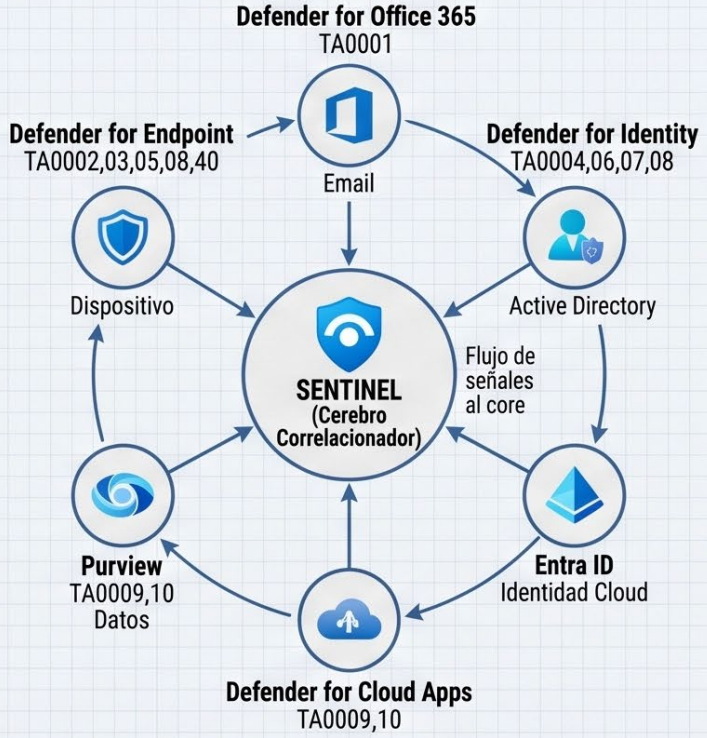
MATRIZ DE CONTRAMEDIDAS (Táctica × Herramienta Microsoft)

	Defender for Endpoint	Defender for Office 365	Defender for Identity	Defender for Cloud Apps	Entra ID	Purview	Sentinel (Correlación Transversal)
TA0001	○	●	○	○	●	◑	Complementario/ Transversal en TODAS las tácticas
TA0002	●	○	○	○	○	◑	
TA0003	●	○	○	○	◑	◑	
TA0004	◑	○	●	○	●	◑	
TA0005	●	○	○	○	○	●	
TA0006	◑	○	●	○	●	◑	
TA0007	◑	○	●	○	○	◑	
TA0008	●	○	●	○	◑	●	
TA0009	◑	○	○	●	○	●	
TA0010	○	○	○	●	○	●	
TA0040	●	○	○	○	○	◑	

Centraliza, correlaciona y analiza señales de múltiples fuentes

● Primaria ■ ◑ Complementaria ■ ○ Sin cobertura directa □

DOMINIOS DE DETECCIÓN POR HERRAMIENTA



EVALUACIÓN MENSUAL DE COBERTURA (Funnel de Priorización)

1. Inventariar (Todas las brechas)
2. Priorizar por Amenaza Real (Threat Intel Sectorial)
3. Priorizar por Factibilidad (Disponibilidad de Logs)
4. Planificar (Implementación Mensual)

Implementación de Reglas Analíticas

Meta: +2-3 detecciones/mes → +24-36/año (Consultivo)

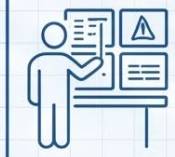
Proceso estratégico, no inventario pasivo. Enfoque en adversarios reales, no en cobertura 100%.

BLOQUE 9/10 — RUTA DEL ANALISTA: L1 → L2 → L3 → LIDERAZGO

"La madurez de un SOC no se mide solo por sus herramientas, sino por la profundidad de talento... Cada nivel es una transformación de mentalidad: de ejecutar procedimientos a cuestionar supuestos."

MAPA DE COMPETENCIAS TÉCNICAS (SKILL TREE)

	L1	L2	L3	Lead
KQL Básico	●	●	●	●
KQL Avanzado	●	●	●	◐
Defender XDR	●	●	●	◐
Playbooks Design	●	●	◐	○
ATT&CK Mapping	●	●	◐	○
ATT&CK Mapping	●	●	◐	○
Comunicación Ejecutiva	●	●	○	○
KQL Bretico	●	◐	○	○
Liderantes Extención	●	◐	○	○
Sestsme Analítica	●	◐	○	○
Comunicación Ejecutiva	●	○	○	○



NIVEL 1 (L1) — EL CENTINELA

Foco: Alerta individual (¿Real o Falso?)
Pregunta Guía: "¿Requiere acción o cierre?"
Actividades Core: Triage, Actualización estados
Mentalidad: Consistencia mecánica (Filtro de primera línea)
Tiempo: 70% Triage, 20% Doc, 10% Formación

GATE/HITO DE TRANSICIÓN (Puerta L1→L2)

- ☑ Dominio KQL básico (Correlación simple)
- ☑ Triage autónomo (<10% escalamiento)
- ☑ Comprensión Tácticas ATT&CK
- ☑ SC-200 (Recomendable, no obligatorio)
- ☑ Documentación consistente (Audit trail)

No es automático; verificación práctica requerida.

NIVEL 2 (L2) — EL INVESTIGADOR

Foco: Patrón y contexto (¿Qué historia cuentan?)
Pregunta Guía: "¿Qué ocurre más allá de la alerta?"
Actividades Core: Análisis profundo, Tuning reglas, UEBA, Contención
Mentalidad: Curiosidad estructurada (Profundidad analítica)
Tiempo: 40% Investigación, 30% Tuning, 20% Contención

GATE/HITO DE TRANSICIÓN (Puerta L2→L3)

- ☑ Hunting con hipótesis estructuradas
- ☑ Creación reglas analíticas custom (Producción)
- ☑ Comprensión profunda cobertura ATT&CK
- ☑ Liderazgo Incidentes Nivel 2 (RCA)
- ☑ Mentoría activa a L1

Salto de la reacción a la proactividad.

NIVEL 3 (L3) — EL ESTRATEGA TÉCNICO

Foco: Adversario y sistema (Thinking Red)
Pregunta Guía: "¿Dónde están las brechas sistémicas?"
Actividades Core: Threat Hunting, Evaluación ATT&CK, Ingeniería detecciones
Mentalidad: Pensamiento adversarial (Capacidad predictiva)
Tiempo: 40% Hunting, 30% Ingeniería, 20% Arquitectura

BIFURCACIÓN DE CARRERA

SOC LEAD / MANAGER (El Gobernante)

Foco: Valor Organizacional Comunicación Ejecutiva, KPIs, Gobierno
Mentalidad: Traducción bidireccional (Negocio ↔ Técnico), 30% Gobernanza, 30% Comunicación, 20% Estrategia

THREAT HUNTER (Especialista Dedicado)

Pasión investigación profunda
KQL avanzado, CTI aplicada
Destino Técnico Puro

MODELO DE FORMACIÓN 70-20-10

- 70% Experiencia Práctica (Doing)
- 20% Aprendizaje Social (Peers/Mentoría)
- 10% Formación Formal (Cursos/Certs)

MAPA DE CERTIFICACIONES (MAPA DE CREDENCIALES)

Track 1 (Fundamentos L1→L2): AZ-900 → SC-900 → SC-200* *Recomendado

Track 2 (Especialización L2→L3): AZ-500 | ISC-300 | [GCIA] | [GCIH]

Track 3 (Avanzado L3→): GCFE/GCFA | CISSP/CISM — *Inversión incremental; valida experiencia, no la sustituye.*

@SCavanna

MASTER PLAN — Bloque 10/10: Madurez & Performance: El SOC que Evoluciona

MODELO CONSULTIVO DE MADUREZ SOC (5 Niveles)

NIVEL 5 — ADAPTATIVO: "El SOC Inteligente"
Identidad: Incorpora IA/ML para detección predictiva y mejora autónoma.
Pregunta: ¿UEBA avanzado, Copilot y detección predictiva activa? (Si sí → Nivel 5)

Características: IA/ML integrado, aprendizaje continuo.
Riesgo: Sobreconfianza en automatización.

NIVEL 4 — OPTIMIZADO: "El SOC Proactivo"
Identidad: Anticipa amenazas, optimiza con inteligencia.
Pregunta: ¿Uso activo de recomendaciones, cobertura ATT&CK y threat intelligence? (Si sí → Nivel 4).
Características: Hunting avanzado, automatización, cobertura ATT&CK, TI integrada.
Riesgo: Complejidad operativa creciente.

NIVEL 3 — MEDIDO: "El SOC Orientado a Métricas"
Identidad: Opera y mide, ciclo de mejora con datos.
Pregunta: ¿Medimos MTTD/MTTR mensual y tuning semanal documentado? (Si sí → Nivel 3).
Características: KPIs activos, tuning continuo, hunting básico, playbooks críticos.
Riesgo: Estancamiento en "medir sin transformar".

NIVEL 2 — DEFINIDO: "El SOC Estructurado"
Identidad: Procesos documentados, roles claros, sin medición formal.
Pregunta: ¿Runbooks y roles definidos pero no medimos MTTD/MTTR? (Si sí → Nivel 2).
Características: Procesos/Roles definidos, herramientas integradas, SLAs establecidos.
Riesgo: Operación estable sin visibilidad de eficacia.

NIVEL 1 — INICIAL: "El SOC Reactivo"
Identidad: SOC existe sin estructura formal.
Pregunta: ¿Las respuestas dependen de quién esté de turno? (Si sí → Nivel 1).
Características: Sin procesos, respuesta ad-hoc, herramientas desconectadas, sin KPIs.
Riesgo: Incidentes mal gestionados, sin trazabilidad.

GATES DE TRANSICIÓN (Criterios Consultivos)

Nivel 4 → 5 Gate
- UEBA avanzado (modelos calibrados)
- Automatización creciente
- Copilot/AI integrado (triage/hunting)
- Detecciones predictivas activas

Architects Daughter

Architects Daughter

Nivel 3 → 4 Gate
- Implementación recomendaciones optimización
- Evaluación cobertura ATT&CK
- Threat Intelligence integrada
- Ejecución de tabletops

Architects Daughter

Nivel 2 → 3 Gate
- KPIs operativos medidos (MTTD, MTTR, FP rate)
- Tuning semanal documentado
- Playbooks activos (críticos)
- Hunting semanal documentado

Architects Daughter

Nivel 2 → 2 Gate
- Runbooks documentados (5 escenarios)
- Roles SOC definidos (RACI)
- Integración Sentinel + Defender XDR
- SLAs definidos

Architects Daughter

Nivel 1 → 2 Gate
- Runbooks documentados (5 escenarios)
- Roles SOC definidos (RACI)
- Integración Sentinel + Defender XDR
- SLAs definidos

TABLERO DE CONTROL: 10 KPIs OPERATIVOS (Consultivo)

DIMENSIÓN	KPIs ASOCIADOS & DEFINICIÓN
EFICACIA DE DETECCIÓN	1. MTTD (Tiempo promedio detección) - Nivel 3
	3. Alert Volume (Cantidad alertas/período) - Nivel 2
	4. False Positive Rate (% alertas descartadas) - Nivel 3
EFICACIA DE RESPUESTA	2. MTTR (Tiempo promedio respuesta) - Nivel 3
	8. Incident Resolution Rate (% resueltos en SLA) - Nivel 3
SALUD OPERACIONAL	6. Connector Health (% conectores activos) - Nivel 2
	5. Playbook Success Rate (% playbooks exitosos) - Nivel 2
EFICIENCIA Y CAPACIDAD	9. Cases per Analyst (Carga promedio) - Nivel 2
	10. Cost per Alert (Costo SOC / alertas) - Nivel 4
MADUREZ DE PROGRAMA	7. ATT&CK Coverage (% tácticas cubiertas) - Nivel 4

KPIs desbloqueados por madurez

Medición progresiva

Architects Daughter

NOTA: Los niveles, criterios de transición y KPIs aquí presentados son marcos de referencia consultivos y de mejores prácticas de la industria, NO constituyen estándares oficiales publicados por Microsoft.

CICLO DE MEJORA CONTINUA (Best Practice)

OPERAR (Ejecutar procesos) → MEDIR (Capturar KPIs) → APRENDER (Analizar datos/gaps) → MEJORAR (Implementar cambios/tuning)