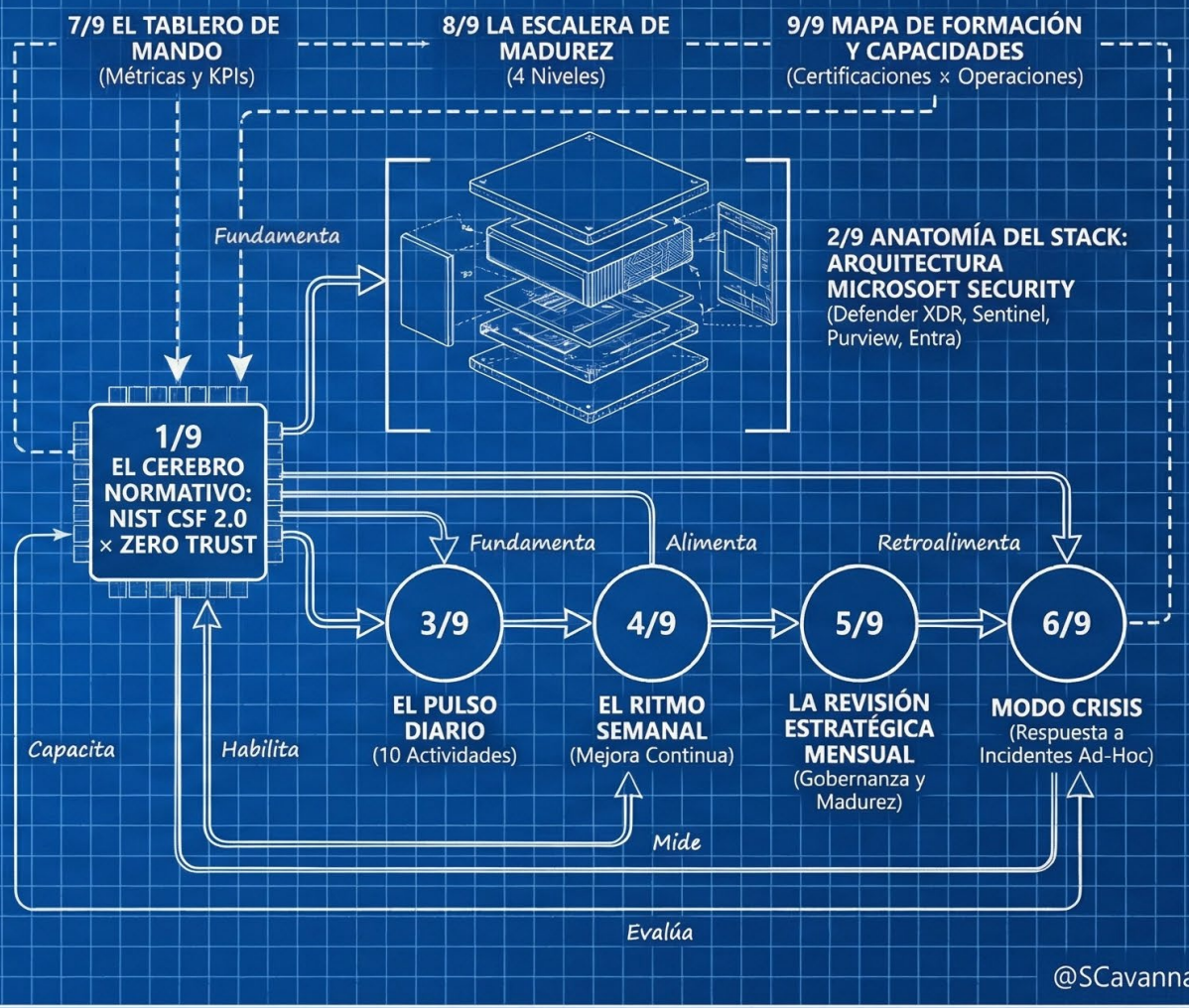
DLP

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

MICROSOFT PURVIEW DATA LOSS PREVENTION (ADVANCE DLP): GUÍA MODELO DE EXCELENCIA OPERACIONAL SOC / SECOPS

Serie Infográfica de 9 Artefactos.

Series Overview

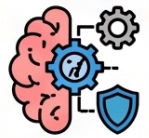


@SCavanna

Serie Infográfica: Índice de artefactos [1/9...9/9]

Microsoft Purview Data Loss Prevention (Advance DLP): Guía Modelo de Excelencia Operacional SOC / SecOps

Fundamentos y Habilitadores



1/9 El Cerebro Normativo: NIST CSF 2.0 × Zero Trust como Sistema Operativo del SOC

Cómo los marcos normativos no son "cumplimiento" sino el sistema operativo que estructura toda la actividad del SOC — las 5 funciones NIST como engranajes, los principios ZTA como reglas del juego.

Base Estructural y Tecnológica

2/9 Anatomía del Stack: Arquitectura Operacional Microsoft Security

Despiece de los 4 pilares tecnológicos (Defender XDR, Sentinel, Purview, Entra) con sus roles, artefactos de evidencia y flujo operacional de telemetría a cierre.

Fundamenta

Habilita

Ciclo Operacional y Mejora

Ciclo de Refinamiento Continuo

3/9 El Pulso Diario: 10 Actividades que Sostienen la Detección Continua

Las 10 actividades diarias como un ciclo de vigilancia 24×7 — desde la cola de incidentes hasta el handover entre turnos, con énfasis en MTTA y conciencia situacional.

Alimenta

4/9 El Ritmo Semanal: Mejora Continua y Optimización de Detecciones

Las 10 actividades semanales articuladas como un motor de refinamiento: tuning, cobertura ATT&CK, eficacia SOAR, coordinación cross-team y reporte ejecutivo.

Alimenta

5/9 La Revisión Estratégica Mensual: Gobernanza, Madurez y Resiliencia

Las 10 actividades mensuales como el ciclo de gobernanza del SOC — KPIs formales, tabletops, alineación NIST, threat intel, RBAC y reporte de riesgo al Board.

Gobernanza y Respuesta Crítica

Retroalimenta

6/9 Modo Crisis: Respuesta a Incidentes Ad-Hoc (El Playbook de Guerra)

Las 7 actividades ad-hoc como un flujo de escalamiento desde investigación profunda hasta post-mortem, con criterios de activación y estructura de lecciones aprendidas.

Retroalimenta

Retroalimenta

Medición, Madurez y Capacitación Transversal

Mide

7/9 El Tablero de Mando: Métricas, KPIs, KRIs y Umbrales Operacionales

Dashboard consolidado de métricas con objetivos, umbrales de alerta y acciones asociadas — el lenguaje cuantitativo que traduce operación a riesgo empresarial.

Evalúa

8/9 La Escalera de Madurez: De Reactivo a Adaptativo (4 Niveles)

Modelo de madurez del SOC en 4 niveles con criterios observables por nivel, como hoja de ruta de evolución estratégica para el CISO.

Capacita

9/9 Mapa de Formación y Capacidades: Rutas de Certificación × Actividades Operacionales

Cruce entre las actividades operacionales y los recursos de formación oficial (SC-200, SC-401, módulos Learn, blogs técnicos) — qué aprender para ejecutar qué.

Capas Transversales de Valor

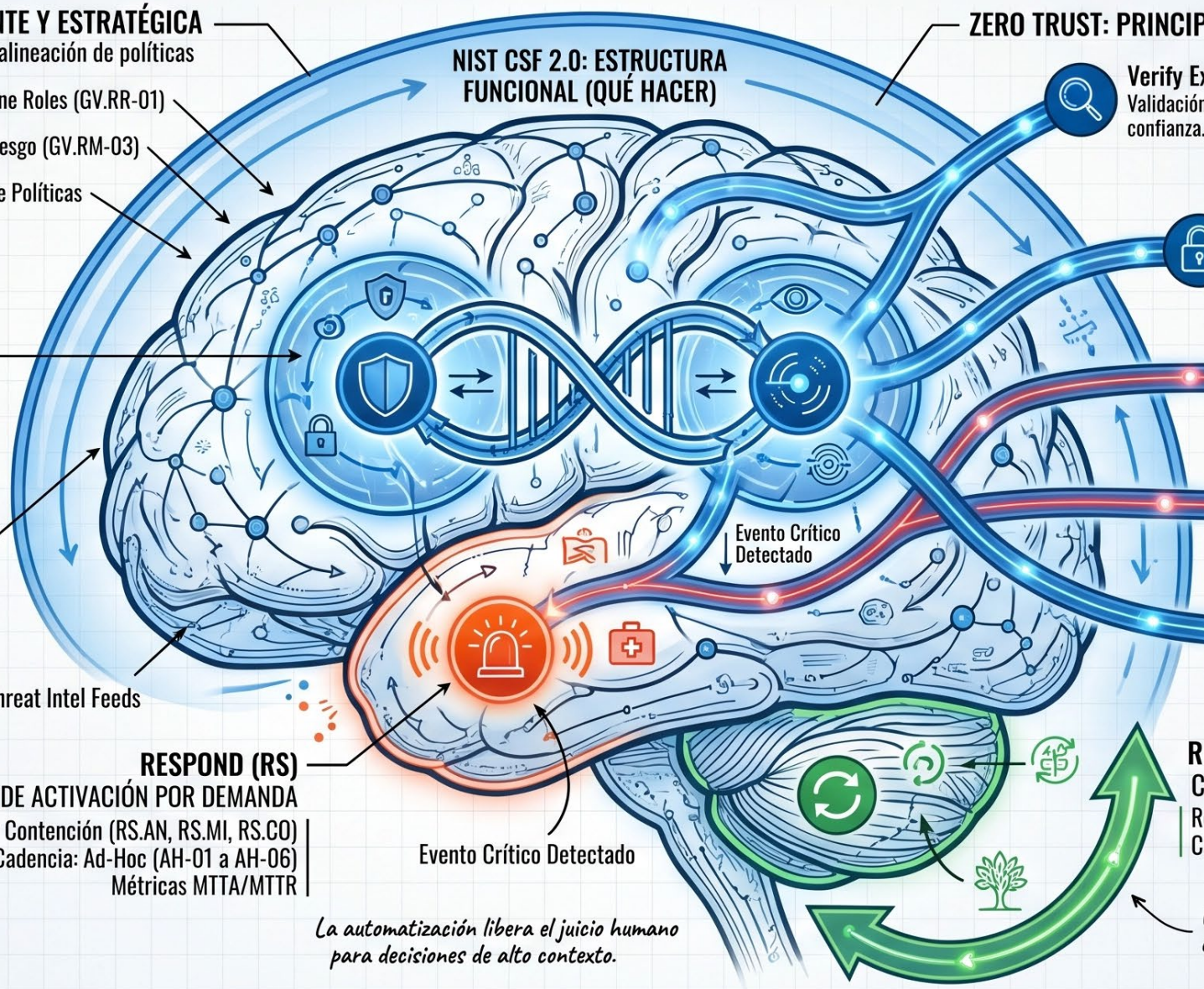
Infografía 1/9: El Cerebro Normativo — NIST CSF 2.0 × Zero Trust como Sistema Operativo del SOC

SISTEMA OPERATIVO DEL SOC: Una arquitectura viva de funciones interdependientes (NIST CSF 2.0) y principios de ejecución transversal (Zero Trust) para la ciberseguridad estratégica.

GOVERN (GV) — FUNCIÓN ENVOLVENTE Y ESTRATÉGICA

Capa de gobernanza, gestión de riesgos y alineación de políticas

Insight 1: GOVERN como diferenciador de madurez; separa lo táctico de lo estratégico.



PROTECT (PR) + DETECT (DE) — BINOMIO DE VIGILANCIA CONTINUA

Controles Activos (PR.DS, PR.AA, PR.PT)
Cadencia: Diaria/Semanal
(D-01 a D-09, S-02, S-04, S-05)

Insight 2:

DETECT (DE) — LA CHEMIO DE VIGILANCIA CONTINUA

Monitoreo de Eventos (DE.CM, DE.AE)
Cadencia: Diaria/Semanal

RESPOND (RS) — MODO DE ACTIVACIÓN POR DEMANDA

Análisis y Contención (RS.AN, RS.MI, RS.CO)
Cadencia: Ad-Hoc (AH-01 a AH-06)
Métricas MTTA/MTTR

La automatización libera el juicio humano para decisiones de alto contexto.

ZERO TRUST: PRINCIPIOS DE EJECUCIÓN (CÓMO HACERLO)

Verify Explicitly (Lupa)
Validación constante basada en evidencia, no en confianza. Contexto completo.

Insight 3: Zero Trust no es un producto, es un paradigma de decisión.

Least Privilege (Candado)
Acceso mínimo necesario (JIT/JEA).
Segmentación y RBAC estricto.

Assume Breach (Escudo Roto)
Operación bajo premisa de compromiso.
Monitoreo continuo y segmentación.

Visibility & Analytics (Ojo-Analítico)
Telemetría centralizada. Decisiones basadas en datos y detección de anomalías.

Automation (Engranaje-Rayo)
Respuesta automatizada a eventos conocidos. Orquestación eficiente.

RECOVER (RC) — CIERRE DEL CICLO Y SEMILLA DE MEJORA

Restauración y Aprendizaje (RC.RP)
Cadencia: Mensual (M-02, M-07, M-09, AH-07)

Un SOC que no ejecuta RECOVER repite errores; uno que lo ejecuta evoluciona.

ANATOMÍA DEL STACK — Los 4 Componentes Clave del SOC Microsoft y su Flujo Vital

Infografía 2/9

El sistema circulatorio del SOC: si se corta, se pierde visibilidad.

MICROSOFT DEFENDER XDR

Motor Central de Correlación y Respuesta

Capacidades Operacionales:
- Incidents Queue
- Attack Story (Narrativa Visual)
- AIR (Automatización Nativa)

Artefactos de Evidencia
- Incident Timelines
- Alert Classifications
- AIR Investigation Status
- Advanced Hunting Results

MICROSOFT SENTINEL

Plataforma SIEM/SOAR Cloud-Native

Capacidades Operacionales:
- Data Connectors (Ingesta)
- Analytics Rules (Detección)
- Playbooks (SOAR/Logic Apps)
- Workbooks (Dashboards)
- SentinelHealth (Autodiagnóstico)

Artefactos de Evidencia
- Analytics Rule Matches
- Playbook Run History
- Workbook Exports
- Connector Health Logs
- SentinelHealth Tables

MICROSOFT PURVIEW

Protección del Dato y Compliance

Capacidades Operacionales:
- DLP Policies & Alerts
- Activity Explorer (Registro Granular)
- Unified Audit Log (Registro Inmutable)
- Insider Risk Management (Comportamiento)

Artefactos de Evidencia
- DLP Alert Records
- Activity Explorer Exports
- Unified Audit Log Searches
- IRM Case Records

MICROSOFT ENTRA ID

Identidad, RBAC, PIM (Infraestructura Zero Trust)

Capacidades Operacionales
- Sign-in Logs (Autenticación)
- Audit Logs (Cambios Administrativos)
- PIM (Acceso Just-in-Time)
- RBAC & Administrative Units (Segregación)

Artefactos de Evidencia
- Sign-in Logs (w/ Risk Level)
- PIM Activation Records, Role Assignment Trails
- Conditional Access Logs

El tejido conectivo: sin identidad, no hay contexto Zero Trust.

FLUJO OPERACIONAL VITAL — De la Telemetría al Cierre Documentado

INGESTA
Conectores Sentinel + Señales Nativas

DETECCIÓN
Analytics, ML, DLP, Identity

ALERTA
Cola Unificada Defender/Sentinel
- Critical/Alert
- Warning/Caution

TRIAGE
Priorización por Severidad + Contexto
- Critical/Alert
- Warning/Caution

INSIGHT DOMINANTE

El SOC Microsoft **NO** es una colección de herramientas. Es un **SISTEMA INTEGRADO** donde la pérdida de un componente crítico (como la telemetría de Sentinel o el contexto de Entra ID) degrada la capacidad operativa global.

INVESTIGACIÓN
Attack Story, Activity Explorer, Hunting
Evidencia Cruzada

RESPUESTA
Automatizada: AIR/Playbooks | Manual: Analista

CONTENCIÓN & REMEDIACIÓN

CIERRE DOCUMENTADO

POST-INCIDENT LOOP (Tuning + Lecciones + Reporte)

INFOGRAFÍA 3/9: EL PULSO DIARIO — LAS 10 ESTACIONES DEL CICLO DE VIGILANCIA 24×7

El SOC no detecta amenazas — sostiene un estado de vigilancia continua donde las amenazas se hacen visibles. Las 10 actividades diarias no son tareas aisladas: son las estaciones de un circuito que genera detección como resultado emergente de su ejecución disciplinada.

CONCEPTO 1: APERTURA — Reconocimiento del Campo de Batalla (D-01 + D-02)

D-01 Revisión de la cola de incidentes y alertas

Revisión sistemática en Defender XDR y Sentinel. Priorización por estado, severidad y asignación. Validación de resueltos automáticamente.
Herramientas: Defender XDR Incidents, Sentinel Incidents.
NIST: DE.CM-01, RS.AN-01
Evidencia: Historial de cola con timestamps.

D-02 Triage inicial de alertas (DLP, endpoint, identidad, correo)

Clasificación por dominio (DLP, Endpoint, Identity, Office 365). Evaluación con contexto completo. Verificación explícita (ZTA).
Resultado: True Positive (Escalar), False Positive (Documentar), Informational.
Métrica: MTTA (calculado localmente).
Herramientas: DLP Dashboard, Defender for Endpoint/Identity/Office 365.
NIST: DE.AE-02, RS.AN-03

→ Bloque 2/9 (Cola Unificada),
→ Bloque 7/9 (MTTA)

→ Bloque 3/9 (D-01 Next Shift),
→ Bloque 8/9 (SOC Maturity differentiator)

CONCEPTO 2: VERIFICACIÓN — Confirmar que el Organismo Funciona (D-03 + D-05 + D-09)

D-03 Validación de salud de sensores y conectores

Verificación de conectores Sentinel operativos e ingesta continua. Revisión de dashboard de salud y métricas. Escalar si Unhealthy.
Nota Crítica: Actividad más subestimada. Sin conectores, las reglas están ciegas.
ZTA: Visibility & Analytics.
Herramientas: Sentinel Health Monitoring, SentinelHealth/Audit tables.
Evidencia: Connector health status.

→ Bloque 2/9 (Sistema Circulatorio)

D-05 Verificación de acciones automáticas ejecutadas (AIR / Playbooks)

Validación de que acciones automatizadas (AIR, Playbooks) no generaron impacto no deseado. Identificación de pendientes de aprobación.
ZTA: Assume Breach.
Herramientas: Defender XDR AIR, Sentinel Automation, Logic Apps.
NIST: GV.RM-03, PR.AA-05
Evidencia: AIR investigation status, Logic Apps run history.

→ Bloque 4/9 (S-02: Tuning)

CONCEPTO 3: OBSERVACIÓN ACTIVA — Cazar lo que las Reglas No Ven (D-04)

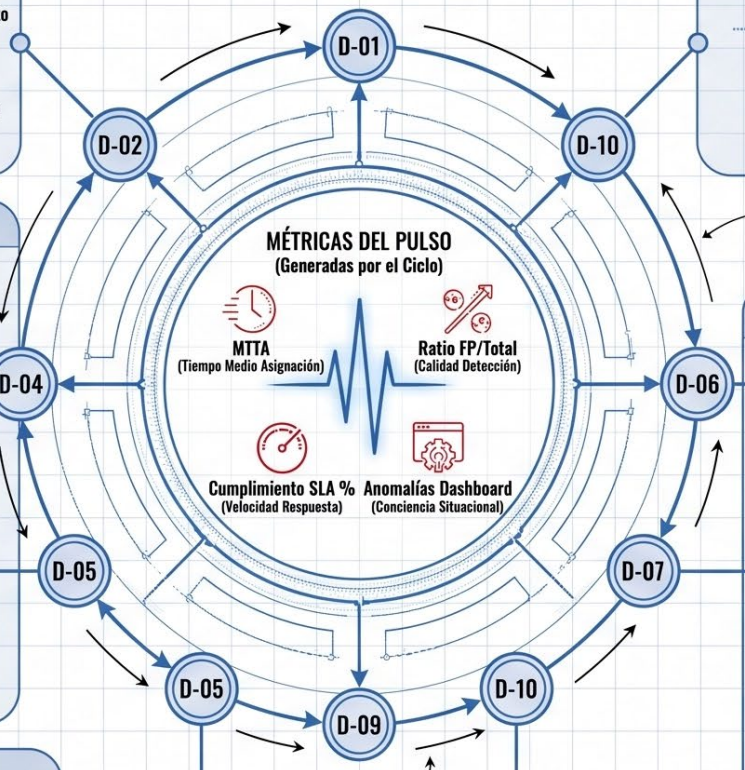
D-09 Validación de cambios recientes en políticas de seguridad

Verificación mediante Unified Audit Log de cambios no autorizados en políticas DLP, analytics rules o configuraciones.
hunting.
ZTA: Verify Explicitly
Herramientas: Unified Audit Log.
NIST: DE.CM-01, PR.PT-01
Evidencia: Audit Log searches.

D-04 Monitoreo de actividades anómalas de usuarios y endpoints

Actividad proactiva. Uso de Activity Explorer, Advanced Hunting y Insider Risk Management para
Hallazgos: Amenaza real (Escalar a incidente), Patrones nuevos (Alimentar reglas).
ZTA: Visibility & Analytics
Herramientas: Purview Activity Explorer, Advanced Hunting, Insider Risk Management.
NIST: DE.CM-03
Evidencia: Activity Explorer exports, AH queries.

→ Bloque 2/9 (Tools)
→ Bloque 4/9 (S-02: New Rules)
→ Bloque 6/9 (AH-01: Deep Dive)



CONCEPTO 5: CIERRE Y CONTINUIDAD — El Handover como Acto de Responsabilidad (D-10)

D-01 Revisión de la cola... (Turno Siguiente)

D-10 Registro operativo y handover entre turnos

Transferencia de contexto para continuidad 24×7 Shift report como evidencia y checklist de cobertura.
Nota Crítica: Handover deficiente reinicia el ciclo desde cero.
ZTA: Assume Breach (adversario no espera).
NIST: RS.CO-01
Evidencia: Shift report archivado, confirmación de recepción.

Fatiga de alertas: adversario interno combatido por D-06.
Handover: contrato de continuidad, no email de cortesía.

CONCEPTO 4: GESTIÓN DEL FLUJO — Control de Calidad y Velocidad (D-06 + D-07 + D-08)

D-06 Gestión de falsos positivos confirmados

Procesamiento formal de FPs: documentación, dismissal, encolamiento para tuning. Combate la fatiga de alertas.
Métrica: Ratio FP/Total (Tendencia)
Herramientas: Alert tuning Sentinel
NIST: DE.AE-04, DE.AE-01
Evidencia: Alert dismissal logs.

→ Bloque 4/9 (S-01/S-02: Trends & Tuning)
→ Bloque 7/9 (FP Ratio)

D-07 Seguimiento de incidentes abiertos (SLA/OLA)

Revisión del envejecimiento contra umbrales SLA definidos. Escalamiento si se esceden.
Métrica: Cumplimiento de SLA (consultivo/definido por SOC)
Herramientas: Defender XDR, Sentinel
NIST: RS.AN-03, RS.CO-01
Evidencia: Incident aging report.

→ Bloque 4/9 (S-01: Trends)
→ Bloque 7/9 (SLA Compliance)

D-08 Revisión de dashboards SOC e indicadores críticos

Verificación de conciencia situacional en Workbooks y Power BI. Identificación de anomalías no reflejadas en alertas.
Métrica: Anomalías de dashboard.
Herramientas: Sentinel Workbooks, Power BI dashboards.
NIST: DE.AE-04
Evidencia: Dashboard captures.

→ Bloque 4/9 (S-01: Trends)

El circuito late: si una estación se apaga, el pulso se debilita.
Cobertura innegociable: al final de cada turno, las 10 estaciones deben haber sido visitadas.
Fatiga de alertas: adversario interno combatido por D-06.

EL RITMO SEMANAL — 10 ENGRANAJES DE REFINAMIENTO QUE TRANSFORMAN OPERACIÓN EN INTELIGENCIA

Lo que el SOC hace cada día lo mantiene vivo. Lo que hace cada semana lo hace más inteligente. El ciclo semanal es el motor de refinamiento que transforma datos operacionales brutos en capacidad de detección mejorada, cobertura expandida y visibilidad ejecutiva.

AFINAR EL OÍDO — Tuning de Detecciones y Gestión del Ruido (S-01 + S-02)

El primer eje ataca el desbalance entre señal y ruido.

S-01 Análisis de tendencias de alertas e incidentes

Lectura epidemiológica: ¿Qué crece? ¿Dónde? Insumo para S-02.

S-02 Tuning de reglas de detección (Analytics Rules / DLP Policies)

Ajuste formal basado en FP/FN acumulado.

Pasos: Revisar Log FP Diario (D-06) → Identificar Ratio FP > Umbral → Ajustar Condiciones con Versionado → Validar en Simulación → Documentar Cambio.

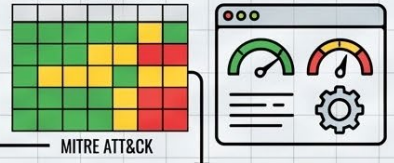
Evidencia auditable: Rule versioning, Tuning notes.

Afinar el instrumento
Architects Daughter

Pintar más verde cada semana
Architects Daughter

AMPLIAR LA VISIÓN — Cobertura ATT&CK y Eficacia de Automatización (S-03 + S-04)

Expande la capacidad del SOC en amplitud de detección y velocidad de respuesta.



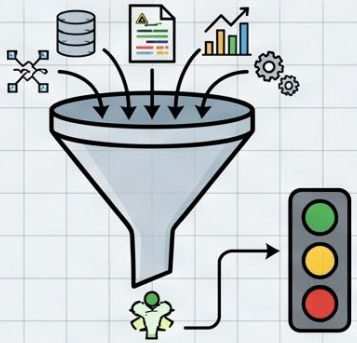
S-04 Revisión de cobertura MITRE ATT&CK

Evaluación semanal contra el framework.
Entregable: Heatmap actualizado, lista de puntos ciegos, plan de nuevas reglas.
¿Contra cuántas técnicas tenemos detección activa?

S-03 Revisión de eficacia de automatizaciones (SOAR)

Evaluación de playbooks Sentinel y acciones AIR.
Métricas: Tasa de éxito, tiempos de ejecución, fallos, override manual.
La automatización se degrada si no se revisa.

TRADUCIR A LENGUAJE DE RIESGO — El Reporte Ejecutivo Semanal (S-10)



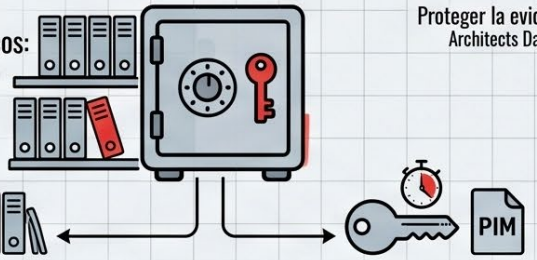
Todo el refinamiento semanal converge en el artefacto que traduce operación técnica a riesgo empresarial. El puente estratégico.

1. Semáforo ejecutivo (Verde/Amarillo/Rojo)	- Comunicación instantánea
2. Métricas clave: MTTA, MTTR, volumen	- Evidencia cuantitativa
3. Incidentes relevantes	- Impacto de negocio y acciones
4. Tendencias vs. semana anterior	- ¿Mejoramos o empeoramos?
5. DLP: Top riesgos y datos sensibles	- Dimensión de protección de datos
6. Acciones tomadas (tuning, playbooks)	- Evidencia de mejora continua
7. Recomendaciones para la semana siguiente	- Prospectiva operacional

De operación a estrategia
Architects Daughter

PROTEGER LA MEMORIA — Integridad de Logs, Retención y Cuentas Privilegiadas (S-05 + S-06)

Protege activos intangibles críticos: memoria forense y confianza en identidades.



Proteger la evidencia
Architects Daughter

S-05 Validación de integridad de logs y retención

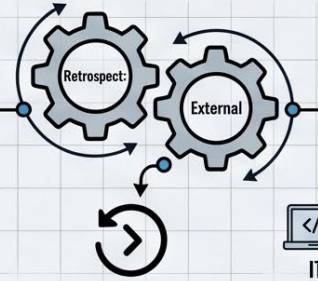
Verificación de fuentes críticas, sin gaps de ingesta.
Cumplimiento regulatorio (GDPR, PCI DSS).
Un gap es un hallazgo de alto impacto.

S-06 Revisión de cuentas privilegiadas y actividades asociadas

Revisión de actividad de roles elevados (Global Admin, PIM).
Foco en uso anómalo y expiración.
Operacionaliza Least Privilege.

SINCRONIZAR EL ECOSISTEMA — Listas, Incidentes Cerrados y Coordinación Cross-Team (S-07 + S-08 + S-09)

Asegura que el SOC no opera como isla, se coordina y aprende.



El SOC no opera solo
Architects Daughter

S-07 Actualización de listas allow/block

Revisión en Defender y Purview.
Listas desactualizadas = Falsos Positivos + Vectores Conocidos.

S-08 Revisión de incidentes cerrados

Revisión ligera post-incidente para extraer patrones y lecciones para tuning.

S-09 Coordinación con equipos de IT, Identity y Data Protection

Sincronización semanal estructurada.
Alineación para Zero Trust.
Entregable: Meeting notes y action items.

EL CICLO SEMANAL SE ALIMENTA DEL DIARIO Y NUTRE AL MENSUAL

INFOGRAFÍA 5/9: LA REVISIÓN ESTRATÉGICA MENSUAL — 10 PILARES DE GOBERNANZA QUE CONECTAN EL SOC CON EL RIESGO EMPRESARIAL

INSIGHT DOMINANTE (NIVEL 1)

Lo diario mantiene vivo al SOC. Lo semanal lo hace más inteligente. El ciclo mensual es donde el SOC deja de ser un centro de operaciones técnicas y se convierte en un órgano de gobernanza de riesgo empresarial, conectando con la estrategia de la organización.

FUNCIÓN NIST CSF 2.0 DOMINANTE

GOVERN — Capa envolvente de gobernanza materializada en acciones concretas

RECOVER RS.IM

NIVEL 4: LA CIMA — Reporte Mensual de Riesgo y Postura de Seguridad (Comunicación Estratégica)

M-10 Reporte mensual de riesgo y postura de seguridad

Audiencia: CISO, Comité de Riesgo, Board.
Propósito: Decisión, Inversión, Posición de riesgo.

Estructura del Reporte (10 Secciones):
1. Resumen ejecutivo (Semáforo)
2. Métricas (Tendencia)
3. Incidentes significativos (Impacto negocio)
4. DLP (Datos en riesgo)
5. Insider Risk (Estado)
6. Cobertura ATT&CK (Progreso/Gaps)
7. Cumplimiento regulatorio (Evidencia)
8. Riesgos emergentes
9. Inversiones/ROI
10. Plan de acción (Accountability)

Influencia en la mesa ejecutiva. Evidencia de madurez consultiva.

EL ESPEJO (Referentes Externos/Internos)

M-03 Alineación con NIST CSF 2.0 y Zero Trust

Evaluación de controles contra outcomes.
Entregable: Control mapping, lista de gaps, plan de remediación.

M-04 Evaluación de nuevas amenazas (Threat Intel)

Fuentes: MSTIC, Defender Analytics, ISACs, CISA.
Entregable: Threat intel brief, nuevas detecciones, cobertura TTPs.

M-05 Revisión de acceso y roles (RBAC)

Validación de roles (Entra ID PIM, Purview Admin Units).
¿Cada persona tiene el acceso exacto que necesita?

← Bloque 4/9 (S-04)

Puente entre el mundo exterior y el SOC (Insight 3).

FLUJO: DE LO TÁCTICO A LO ESTRATÉGICO — Insumos Operacionales → Decisión Ejecutiva

NIVEL 3: EL ESPEJO & LA EVOLUCIÓN (Alineación, Adaptación y Mejora Continua)

M-05 Revisión de acceso y roles (RBAC)

Validación de roles (Entra ID PIM, Purview Admin Units).
¿Cada persona tiene el acceso exacto que necesita?

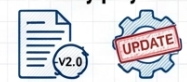
← Bloque 4/9 (S-02)

LA EVOLUCIÓN (ADN Operacional)

M-06 Revisión de políticas DLP y sensibilidad

Alineación con cambios regulatorios/negocio.
DLP Analytics para blind spots predictivos.

M-09 Actualización de runbooks y playbooks



Ciclo de actualización alimentado por: Gaps de tabletops (M-02), Lecciones aprendidas (AH-07). Cambios tecnológicos.

NIVEL 2: EL ESTRÉS — Ejercicios de Simulación y Validación de Resiliencia (Validación bajo Presión)

M-02 Ejercicios de simulación de incidentes (Tabletop)

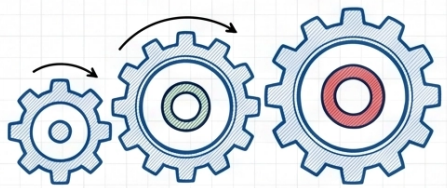
Miden preparación futura.
Escenarios: Ransomware, Insider Threat, Fuga de datos, Compromiso de identidad.

Valor en los GAPS revelados, no en "pasar el ejercicio" (Insight 2).

1. Escenario (Playbook) → 2. Activación (Triage/Investigación) → 4. Debrief (Gaps) → 5. Informe (Acciones)

→ Bloque 5/9 (M-09)

SISTEMA DE ENGRANAJES (INSIGHT 5)



DIARIO (Rápido) → SEMANAL (Intermedio) → MENSUAL (Lento/Potente)

FP diarios (D-06) → Tuning semanal (S-02) → Ratio FP mensual (M-01)
Hunting diario (D-04) → Nuevas reglas (S-02) → Cobertura ATT&CK (M-01)
Reportes semanales (S-10 x4) → Reporte mensual (M-10)
Ninguna frecuencia opera en aislamiento.

NIVEL 1: LA BASE — Medir, Respaldar y Optimizar (Fundamento Operacional)

M-01 Revisión formal de KPIs/KRIs del SOC

Histórico de 12 meses obligatorio. CISO ve tendencia, no dato puntual.

Evaluación contra objetivos. Veredicto mensual documentado.

- **MTTA/MTTR** (Desviación = Capacidad insuficiente)
- **Tasa de FP/Automatización** (Reglas/Playbooks)
- **Cobertura ATT&CK/DLP Matches** (Gaps/Riesgo emergente)

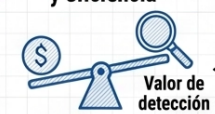
→ Bloque 4/9 (S-01/S-02)

M-07 Validación de backup y recuperación

Prueba de recuperación simulada: valida que el backup es funcional.

Configuraciones críticas: Analytics rules (Sentinel), Políticas DLP (Purview), Playbooks/Workbooks.

M-08 Revisión de costos y eficiencia



Valor de detección

Optimizar relación costo/valor.
Análisis: Ingesta Sentinel, Almacenamiento, Logic Apps.

Herramienta de negociación presupuestaria fundamentada en resultados (Insight 4).

INFOGRAFÍA 6/9: MODO CRISIS — 7 FASES DEL PLAYBOOK DE GUERRA CUANDO EL ADVERSARIO YA ESTÁ ADENTRO

EL CORE: Las actividades diarias preparan para el momento en que todo falla. El MODO CRISIS no se planifica, se ACTIVA. Su ejecución depende de la disciplina en las otras cadencias.

Bloque 3 (Diario)

Bloque 4 (Semanal)

ACTO I — COMPRENSIÓN INICIAL (AH-01)

AH-01: INVESTIGACIÓN PROFUNDA DE INCIDENTE

Objetivo: Entender la Cadena de Ataque ANTES de Contener

Herramientas Clave:
Defender XDR (Attack Story)
Advanced Hunting (KQL),
Purview Activity Explorer

Herramientas Clave:
Defender XDR (Attack Story)
Advanced Hunting (KQL),
Purview Activity Explorer

ACTO II — CONTENCIÓN Y ACTIVACIÓN (AH-02 + AH-03)

AH-02: CONTENCIÓN INMEDIATA (MANUAL)

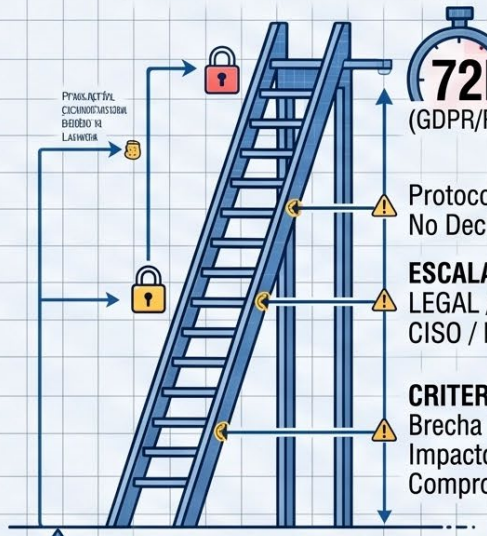
Acciones Proporcionales y Documentadas:
Aislamiento Endpoint,
Bloqueo Cuenta,
Revocación Sesiones

AH-03: ACTIVACIÓN PLAYBOOKS (AUTOMATIZADO)

Orquestación Especifica (Sentinel Logic Apps):
Ransomware, Fuga de Datos, Insider Threat

ESTADO DE CONTENCIÓN:
VERIFICADO / PARCIAL / FALLIDO

ACTO III — ESCALAMIENTO (PUNTO DE NO RETORNO) (AH-04)



72h
(GDPR/Regulatorio)

Protocolo Predefinido,
No Decisión Ad-Hoc

ESCALAR A:
LEGAL / PRIVACY /
CISO / BOARD

CRITERIO:
Brecha Datos Personales /
Impacto Financiero Material /
Compromiso C-Level

SOC OPERATIVO

ACTO IV — PROFUNDIZACIÓN FORENSE Y AJUSTE (AH-05 + AH-06)

AH-05: ANÁLISIS FORENSE MULTI-FUENTE

Reconstrucción Total:
Unified Audit Log,
Endpoint Timeline,
Email Threat Explorer,
Identity Logs

AH-06: AJUSTE URGENTE DE CONTROLES

Bloqueo Inmediato de Vector Activo:
Reglas Sentinel, Políticas DLP. Documentación Obligatoria

ACTO V — APRENDIZAJE Y CIERRE DEL CICLO (AH-07)

AH-07: LECCIONES APRENDIDAS Y ACCIONES CORRECTIVAS

1. Línea de Tiempo Objetiva
2. Causa Raíz (5 Whys)
3. Qué Funcionó / Qué Falló
4. Gaps Identificados
5. Mejoras Runbooks/Playbooks

RETROALIMENTACIÓN AL SISTEMA OPERACIONAL

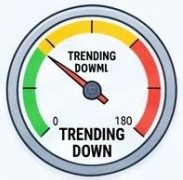
@SCavanna

INFOGRAFÍA 7/9: EL TABLERO DE MANDO — EL LENGUAJE CUANTITATIVO QUE TRADUCE OPERACIÓN TÉCNICA EN RIESGO EMPRESARIAL

ACTO I — KPIs OPERACIONALES: EL ESPEJO RETROVISOR DEL RENDIMIENTO (QUÉ PASÓ)

MTTA
(Mean Time to Acknowledge)
↑ MEJORANDO

MTTR
(Mean Time to Respond)
→ ESTABLE



MTTD
(Mean Time to Detect)
↓ DEGRADANDO

INCIDENTES CERRADOS/ABIERTOS
↑ MEJORANDO

TASA DE AUTOMATIZACIÓN ↑ MEJORANDO
40%
40% — Objetivo: >30%

RATIO FP/TOTAL ↑ MEJORANDO
12% — Objetivo: <15%

OVERRIDE RATE DLP → ESTABLE
8% — Objetivo: <10%

COBERTURA ATT&CK ↑ MEJORANDO
75%
Objetivo: >70%

Miden rendimiento pasado, no predicen el futuro.

Ningún KPI individual cuenta la historia completa.

Miden rendimiento pasado, no predicen el futuro.

SEMÁFORO EJECUTIVO

VERDE: POSTURA SÓLIDA. SOC EFICAZ. INVERSIONES CON RETORNO.
(Todos KPIs dentro de objetivo. Ningún KRI activado. Cobertura ATT&CK en marcha.)

AMARILLO: ÁREAS DE ATENCIÓN REQUIEREN SEGUIMIENTO. SOC FUNCIONAL CON MEJORAS ACTIVAS.
(Al menos un KPI fuera objetivo con plan de acción.)

ROJO: DEBILIDADES SIGNIFICATIVAS. NECESARIA DECISIÓN EJECUTIVA. RIESGO ELEVADO.
(Múltiples KPIs fuera objetivo. High impact activo.)

ESTADO ACTUAL: DETERMINADO POR: CISO — FECHA: [DD/MM/AAAA] — BASADO EN: [DATOS]

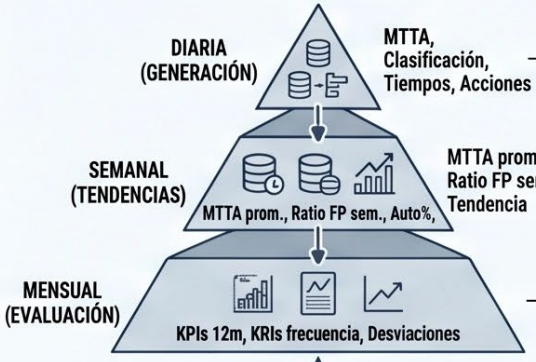
ACTO II — KRIs: EL RADAR DE ALERTA TEMPRANA (QUÉ ESTÁ A PUNTO DE FALLAR)

INCIDENTES HIGH SIN TRIAGE > 30 MIN UMBRAL: > 0	ESCALAMIENTO INMEDIATO. DOCUMENTAR CAUSA.
CONECTOR DE DATOS SIN INGESTA > 1H UMBRAL: > 0	TICKET URGENTE A SOPORTE. MONITOREO ALTERNATIVO.
RATIO FP > 25% EN REGLA/POLÍTICA UMBRAL: > 0	TUNING INMEDIATO. POSIBLE DESACTIVACIÓN TEMPORAL.
INCIDENTE HIGH ABIERTO > SLA UMBRAL: > 0	ESCALAMIENTO A CISO. REASIGNAR RECURSOS.
DLP OVERRIDE SIN JUSTIFICACIÓN UMBRAL: > 0	INVESTIGACIÓN DISCIPLINARIA/DE SEGURIDAD.

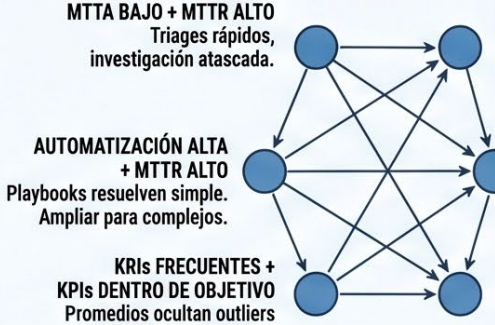
Umbrales de alarma: toda violación requiere atención inmediata. Miran hacia adelante.

ACTO III — CONSOLIDACIÓN TEMPORAL Y RELACIONES ENTRE MÉTRICAS

CONSOLIDACIÓN TEMPORAL (FLUJO ASCENDENTE)



RELACIONES (CRUCES DIAGNÓSTICOS)



Lo que no se mide no se gestiona. El peligro de los promedios, la importancia de los percentiles.

Métricas como herramienta de negociación presupuestaria.

MTTD es la más valiosa y difícil.

Override DLP como indicador cultural.

Infografía 8/9: La Escalera de Madurez —

4 Niveles que Separan un SOC que Reacciona de un SOC que Anticipa

Architects Daughter

Apagar Incendios sin Mapa

Detección: Respuesta aislada
Automatización: Inexistente/Manual
Métricas: Sin cálculo MTTA/MTTR
Documentación: Conocimiento tribal
Reporting: Sin reporte regular
Tuning: Configuración inicial y olvido
Coordinación: SOC aislado

⚠ **Trampa:** Herramientas sin proceso

Architects Daughter

Estructura que Habilita Consistencia

Detección: Triage sistematizado (TP/FP/Info)
Automatización: Playbooks básicos, AIR verificado
Métricas: MTTA/MTTR establecidos, línea base
Documentación: Runbooks documentados
Reporting: Reporte ejecutivo regular (semanal/mensual)
Tuning: Tuning semanal basado en datos
Coordinación: Reuniones semanales con IT/Identity

Architects Daughter

Inteligencia, Cobertura y Automatización a Escala

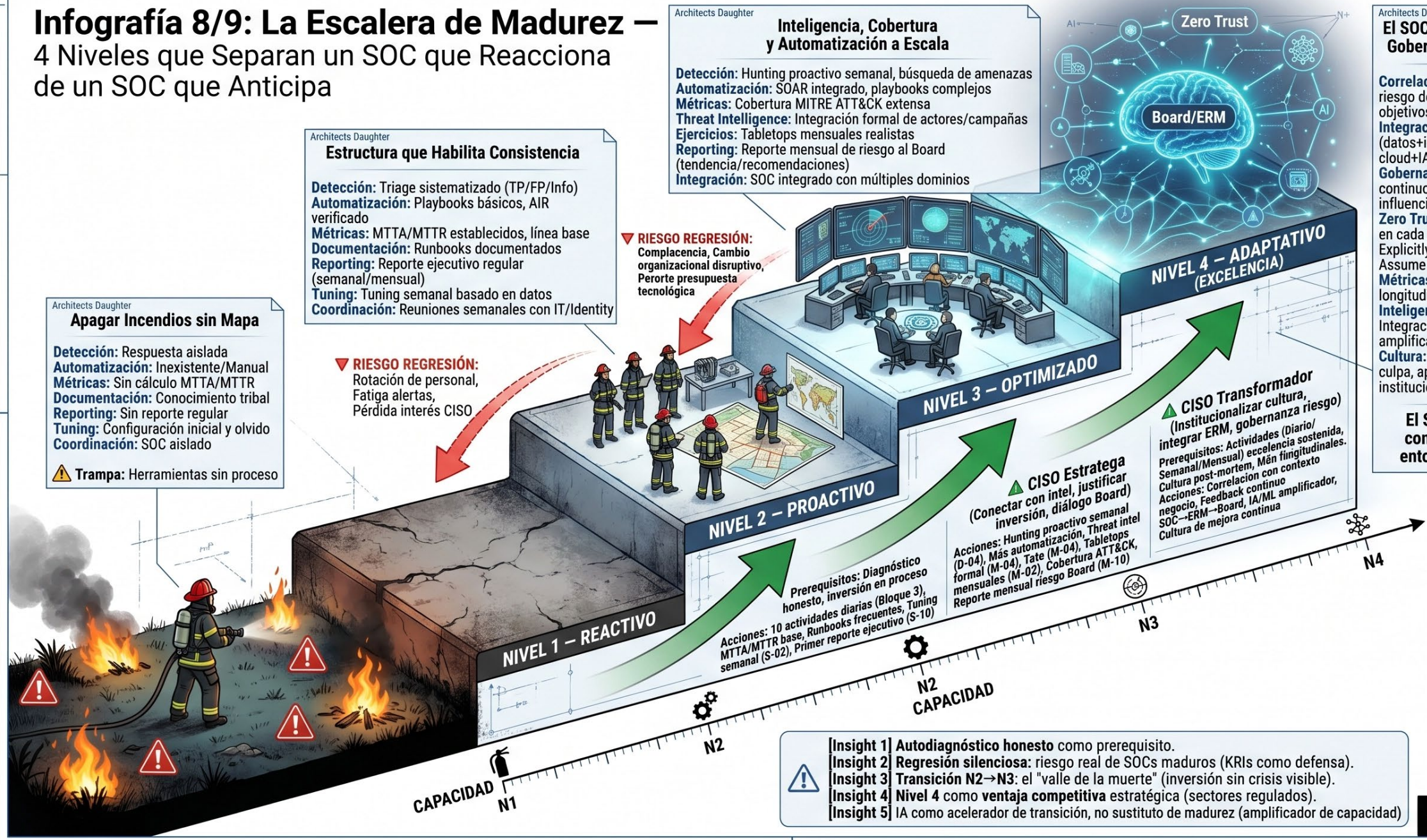
Detección: Hunting proactivo semanal, búsqueda de amenazas
Automatización: SOAR integrado, playbooks complejos
Métricas: Cobertura MITRE ATT&CK extensa
Threat Intelligence: Integración formal de actores/campañas
Ejercicios: Tabletops mensuales realistas
Reporting: Reporte mensual de riesgo al Board (tendencia/recomendaciones)
Integración: SOC integrado con múltiples dominios

Architects Daughter

El SOC como Órgano de Gobernanza de Riesgo

Correlación: Contexto de riesgo de negocio (impacto objetivos)
Integración: SOC unificado (datos+identidad+endpoint+cloud+IA)
Gobernanza: Feedback continuo a ERM y Board, influencia estratégica
Zero Trust: Operacionalizado en cada decisión (Verify Explicitly, Least Privilege, Assume Breach)
Métricas: KPIs con histórico longitudinal, ROI con datos
Inteligencia Artificial: Integración de IA/ML como amplificador humano
Cultura: Post-mortems sin culpa, aprendizaje continuo institucionalizado, resiliencia

El SOC se adapta continuamente al entorno cambiante



⚠ **[Insight 1]** **Autodiagnóstico honesto** como prerequisito.
[Insight 2] **Regresión silenciosa:** riesgo real de SOCs maduros (KRIs como defensa).
[Insight 3] **Transición N2→N3**: el "valle de la muerte" (inversión sin crisis visible).
[Insight 4] **Nivel 4** como **ventaja competitiva** estratégica (sectores regulados).
[Insight 5] IA como acelerador de transición, no sustituto de madurez (amplificador de capacidad)

@SCavanna

MAPA DE FORMACIÓN Y CAPACIDADES — Qué Aprender para Ejecutar Qué: El Cruce entre Conocimiento y Operación

MASTER PLAN — Framework Integrado MAGERIT · CCN-STIC 817 · MITRE ATT&CK · Microsoft Security Stack

Infografía 9/9