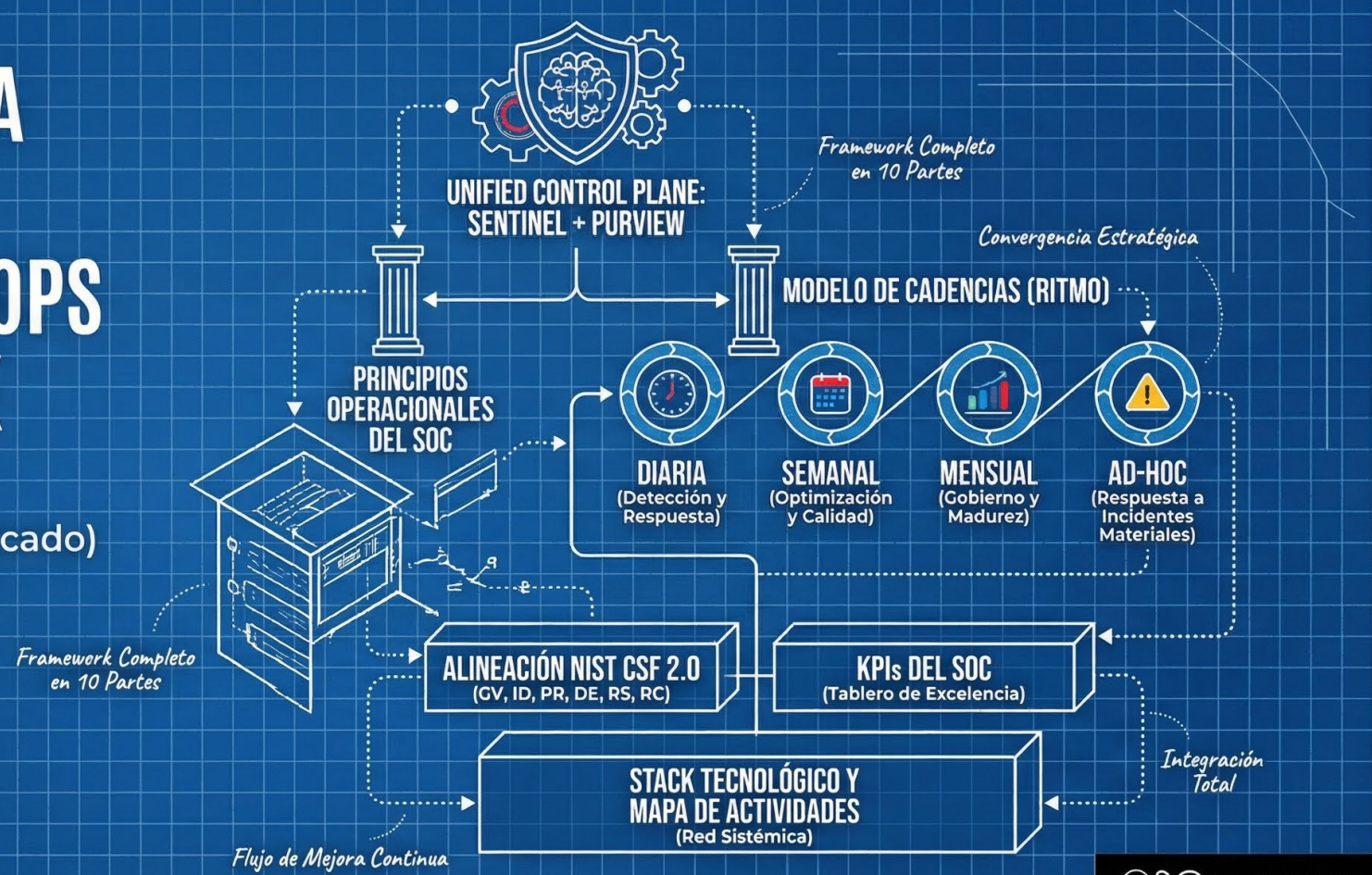
DLCM

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

MICROSOFT PURVIEW DATA LIFECYCLE & RECORDS MANAGEMENT - SOC / SECOPS EXCELLENCE FRAMEWORK

(SCavanna - Versión 1.0 - 2603)

(Serie de 10 Artefactos - Plano de Control Unificado)



SERIES OVERVIEW: 10-PART FRAMEWORK

Blueprint Sistémico-Editorial

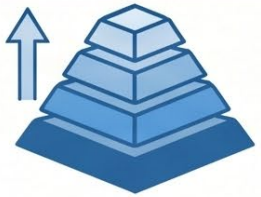
@SCavanna

MICROSOFT PURVIEW DATA LIFECYCLE MANAGEMENT & RECORDS MANAGEMENT MANAGEMENT (ADVANCED) - SOC / SECOPS: EXCELENCIA OPERACIONAL DEL SOC

SERIE: [ÍNDICE]

Arquitectura de Información y Flujo Lógico: De la Estrategia a la Ejecución y la Medición

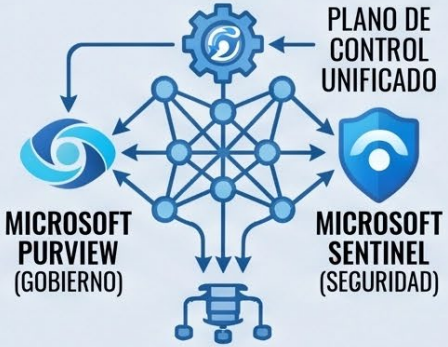
ESTRUCTURA Y PRINCIPIOS



2/10: **Principios Operacionales del SOC de Excelencia.** Los 5 principios rectores contra los que se mide la madurez.

Define la Medición

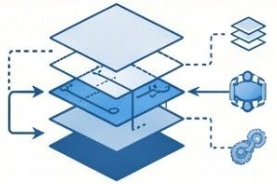
SISTEMA CENTRAL: MARCO ESTRATÉGICO



1/10: **La Convergencia.** El "por qué" estratégico: dos plataformas, un ecosistema que se retroalimenta.

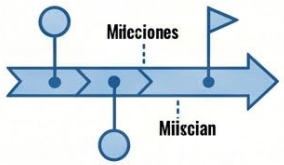
Alimenta la lógica de todos

EJECUCIÓN DIARIA: MOTOR DE RESPUESTA



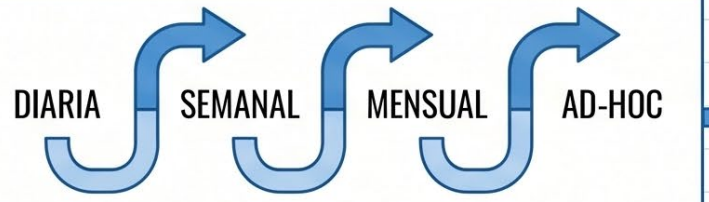
4/10: **Cadencia Diaria.** Actividades diarias organizadas como flujo integrado entre Sentinel, Purview y el ciclo de incidentes.

GOBIERNO Y ESTRATEGIA MENSUAL



6/10: **Cadencia Mensual.** Ciclo de accountability ante CISO, reguladores y junta directiva.

RITMO OPERACIONAL (COLUMNA VERTEBRAL)



3/10: **Modelo de Cadencias.** El engranaje de mejora continua, no una lista de tareas.

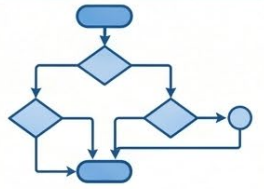
Estructura de Ejecución

FUNDAMENTO LÓGICO TRANSVERSAL

CALIDAD Y CONTROL SEMANAL

5/10: **Cadencia Semanal.** Feedback que alimenta la mejora de regias, automatización y cobertura.

PROTOCOLO DE ACTIVACIÓN AD-HOC



7/10: **Respuesta Ad-Hoc.** Árhol de decisión integrando SOC + Legal + Privacidad + Regulador.

Columna vertebral que conecta cadencias

Output medible de actividades

Acsesement de 30 días como primer paso.

FUNCTIOIS	EVIDENCA ITIONAL	EVIDENCIA DFENRTIVA		
		GV Surpkck 1	ED Vurriose Duna	RC Sepsetis C
GV	-	-	-	-
IG	-	-	-	-
PR	-	-	-	-
DE	-	-	-	-
RS	-	-	-	-
RC	-	-	-	-

8/10: **Alineación NIST CSF 2.0.** Mapeo bidireccional entre funciones y actividades SOC con evidencia nativa.

MÉTRICAS Y RESULTADOS: DASHBOARD EJECUTIVO

9/10: **KPis del SOC.** Tablero de excelencia operacional dividido en dos pianos.

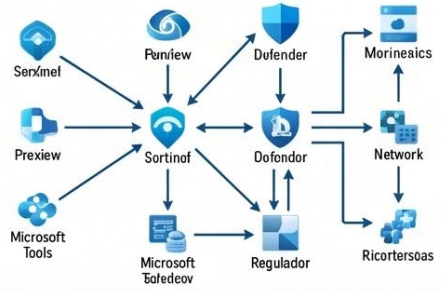
Referencia Cruzada

Referencia cruzada NIST

Complemento Técnico

Vista técnica complementaria

TECNOLOGÍA E INTEGRACIÓN: MAPA DE HERRAMIENTAS



10/10: **Stack Tecnológico y Mapa de Actividades.** Qué hace cada herramienta y cómo se conectan en el flujo real.

@50avanna

MICROSOFT PURVIEW DATA LIFECYCLE & RECORDS MANAGEMENT (ADVANCED) - SOC / SECOPS EXCELLENCE FRAMEWORK

(SCavanna - Versión 1.0)

BLOQUE 1/10: LA CONVERGENCIA — SENTINEL + PURVIEW COMO PLANO DE CONTROL UNIFICADO

NOTAS DE SOPORTE / INSIGHTS

M365 E5 | Sentinel | Entra ID PIM

STACK TECNOLÓGICO COMPLETO

Modelo asume E5 + licenciamiento adicional para Sentinel y Entra ID PIM. La ausencia reduce cobertura.

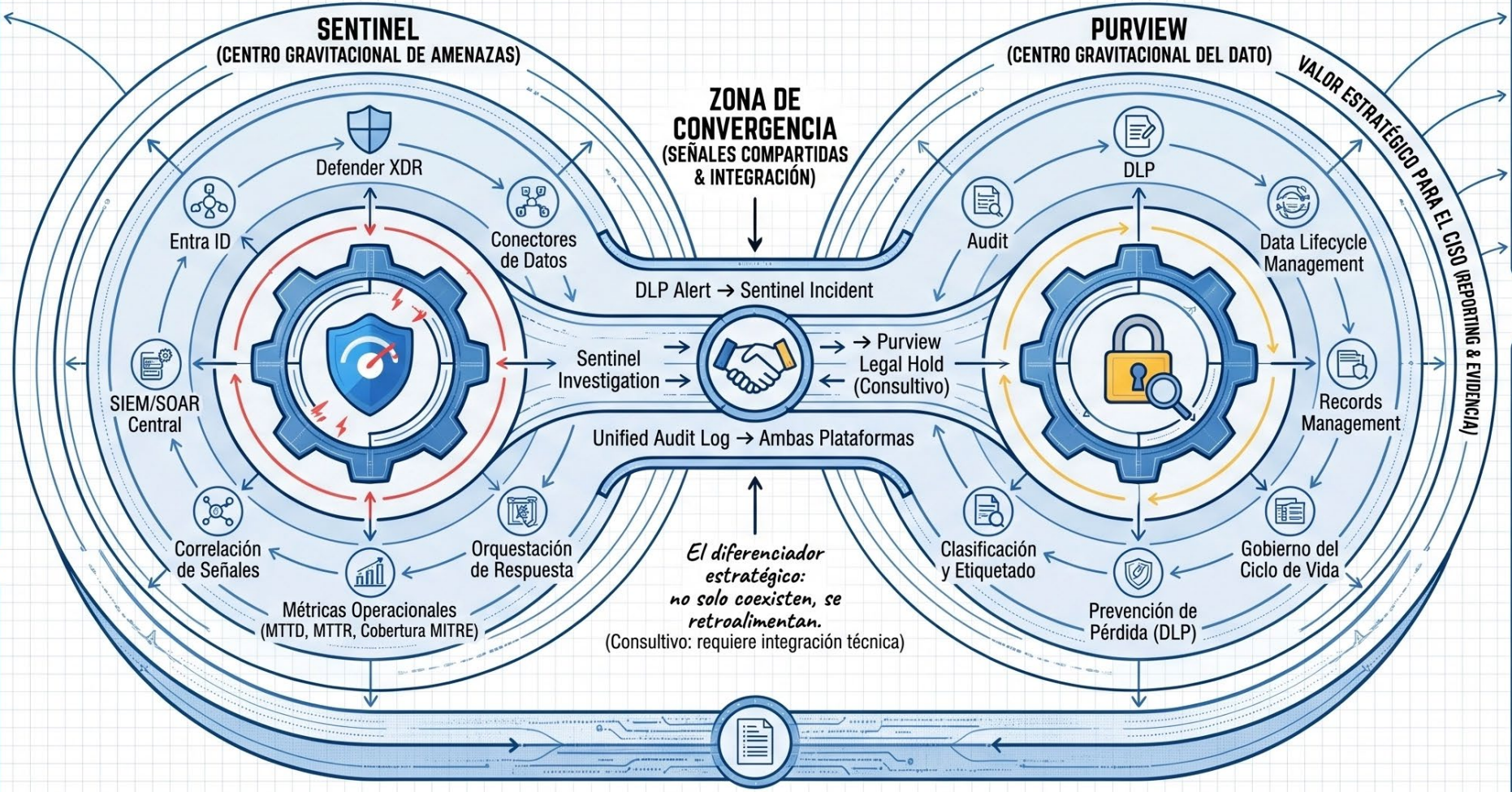
Verificar requisitos.

DEFENDER PORTAL (EXPERIENCIA UNIFICADA)

Evolución hacia Unified SecOps en Defender Portal para gestión conjunta de incidentes.

ANÁLISIS CONSULTIVO (NO REPLICABLE)

Convergencia facilita cobertura y evidencia; otras herramientas requieren integraciones complejas. (Análisis consultivo, no claim oficial).



UNIFIED AUDIT LOG: EL TEJIDO CONECTIVO

Infraestructura de trazabilidad que alimenta ambos núcleos.
Registro de cada acción administrativa, acceso, cambio de política.
Retención hasta 10 años (Audit Premium) para cumplimiento y soporte de litigios.

CONEXIONES EXTERNAS (SERIES OVERVIEW)

- **Junta Directiva** (Postura de Seguridad)
- **Reguladores** (Cumplimiento Normativo)
- **Auditoría Externa** (Evidencia Trazable)
- **Decisiones de Inversión**

CONEXIONES EXTERNAS (SERIES OVERVIEW)

→ **Bloque 2 (Principios):** Consecuencia directa de esta arquitectura.

→ **Bloque 3 (Cadencias):** Operacionalización práctica de la convergencia.

→ **Bloque 8 (NIST CSF 2.0):** Alineación con evidencia de ambas plataformas (Detect/Respond + Govern/Identify/Protect).

→ **Bloque 9 (KPIs):** Tablero ejecutivo con métricas de eficiencia y gobierno.

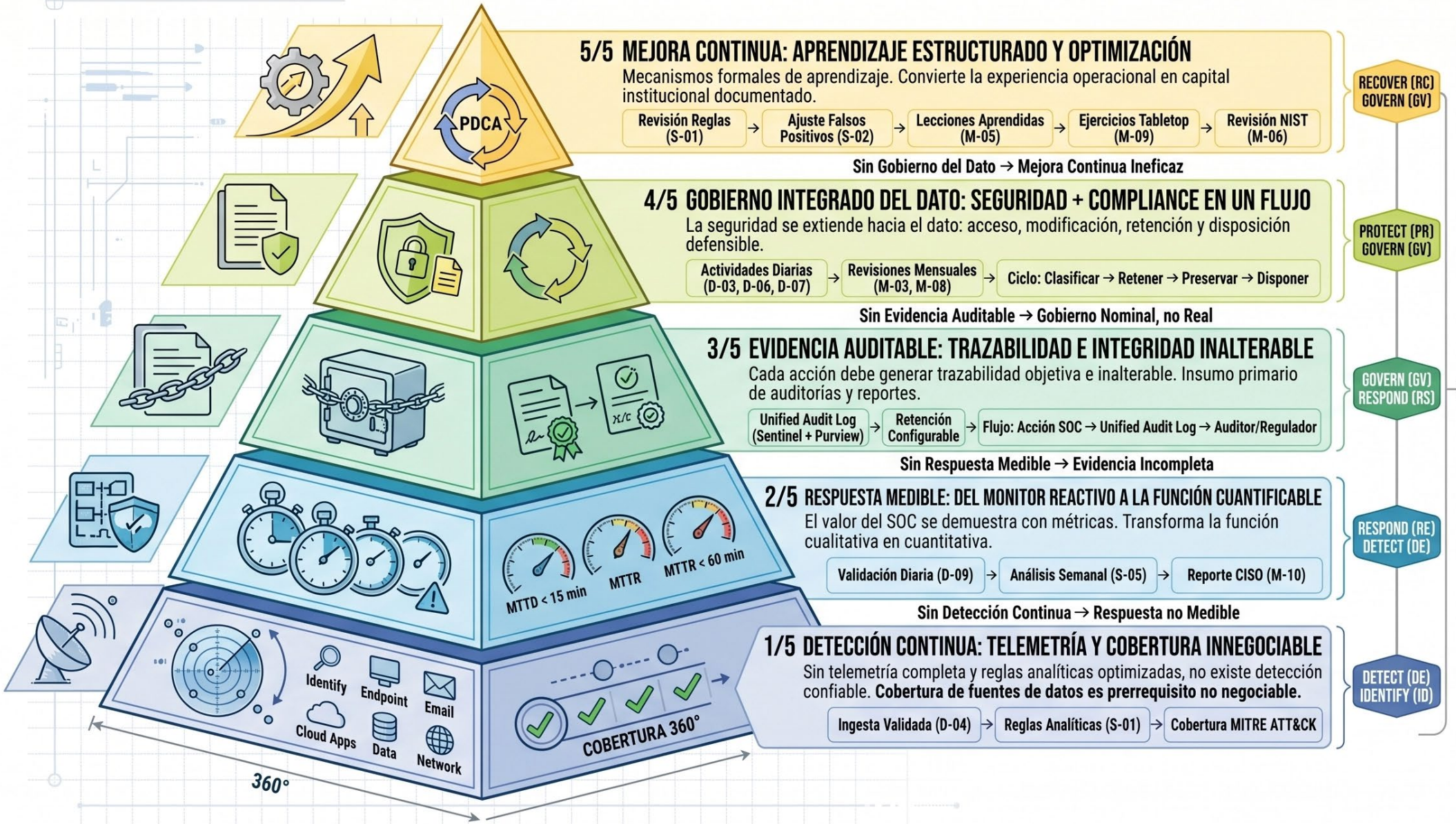
→ **Bloque 10 (Stack por Herramienta):** Detalle del "quién hace qué".

MICROSOFT PURVIEW DATA LIFECYCLE & RECORDS MANAGEMENT (ADVANCED) - SOC / SECOPS EXCELLENCE FRAMEWORK

(SCavanna - Versión 1.0)

PRINCIPIOS OPERACIONALES DEL SOC DE EXCELENCIA

Un SOC no se mide por la cantidad de alertas, sino por la calidad de la detección y la velocidad de la respuesta.



5/5 MEJORA CONTINUA: APRENDIZAJE ESTRUCTURADO Y OPTIMIZACIÓN

Mecanismos formales de aprendizaje. Convierte la experiencia operacional en capital institucional documentado.

Revisión Reglas (S-01) → Ajuste Falsos Positivos (S-02) → Lecciones Aprendidas (M-05) → Ejercicios Tabletop (M-09) → Revisión NIST (M-06)

RECOVER (RC) GOVERN (GV)

Sin Gobierno del Dato → Mejora Continua Ineficaz

4/5 GOBIERNO INTEGRADO DEL DATO: SEGURIDAD + COMPLIANCE EN UN FLUJO

La seguridad se extiende hacia el dato: acceso, modificación, retención y disposición defensible.

Actividades Diarias (D-03, D-06, D-07) → Revisiones Mensuales (M-03, M-08) → Ciclo: Clasificar → Retener → Preservar → Disponer

PROTECT (PR) GOVERN (GV)

Sin Evidencia Auditable → Gobierno Nominal, no Real

3/5 EVIDENCIA AUDITABLE: TRAZABILIDAD E INTEGRIDAD INALTERABLE

Cada acción debe generar trazabilidad objetiva e inalterable. Insumo primario de auditorías y reportes.

Unified Audit Log (Sentinel + Purview) → Retención Configurable → Flujo: Acción SOC → Unified Audit Log → Auditor/Regulador

GOVERN (GV) RESPOND (RS)

Sin Respuesta Medible → Evidencia Incompleta

2/5 RESPUESTA MEDIBLE: DEL MONITOR REACTIVO A LA FUNCIÓN CUANTIFICABLE

El valor del SOC se demuestra con métricas. Transforma la función cualitativa en cuantitativa.

Validación Diaria (D-09) → Análisis Semanal (S-05) → Reporte CISO (M-10)

RESPOND (RE) DETECT (DE)

Sin Detección Continua → Respuesta no Medible

1/5 DETECCIÓN CONTINUA: TELEMETRÍA Y COBERTURA INNEGOCIABLE

Sin telemetría completa y reglas analíticas optimizadas, no existe detección confiable. **Cobertura de fuentes de datos es prerrequisito no negociable.**

Ingesta Validada (D-04) → Reglas Analíticas (S-01) → Cobertura MITRE ATT&CK

DETECT (DE) IDENTIFY (ID)

MAPEO NIST CSF 2.0 & SEÑALES DE ALERTA

ANTI-PATRONES: SEÑALES DE UN SOC SIN PRINCIPIOS

- ⚠ **Conectores fallidos no detectados** (Principio 1 comprometido)
- ⚠ **Ausencia de métricas MTTD/MTTR** (Respuesta no medible)
- ⚠ **Incidentes sin documentación** (Evidencia inexistente)
- ⚠ **Purview no monitoreado** (Gobierno nominal)
- ⚠ **Mismos errores repetidos** (Mejora continua ausente)

@SCavanna

MICROSOFT PURVIEW DATA LIFECYCLE & RECORDS MANAGEMENT (ADVANCED) - SOC / SECOPS EXCELLENCE FRAMEWORK

(SCavanna - Versión 1.0)

CADENCIA MENSUAL: EL CICLO DE GOBIERNO Y ACCOUNTABILITY

10 actividades ejecutadas por Team Lead y CISO.
Propósito: Revisión estratégica de postura, cumplimiento regulatorio, madurez del programa y reporte ejecutivo.
Traduce operación técnica a gobierno.

- M-01 Evaluación postura global
- M-02 Mapeo cobertura MITRE
- M-03 Revisión políticas retención
- M-04 Auditoría accesos administrativos
- M-05 Ejecución lecciones aprendidas
- M-06 Evaluación alineación NIST
- M-07 Optimización costos ingesta
- M-08 Validación cumplimiento regulatorio
- M-09 Ejecución ejercicios tabletop
- M-10 Entrega reporte ejecutivo

10 ACTIVIDADES
TEAM LEAD + CISO
NIST: GOVERN + RECOVER

Prioridades estratégicas → Ajustes operacionales

Prioridades estratégicas → Ajustes operacionales

CADENCIA SEMANAL: EL CICLO DE OPTIMIZACIÓN

10 actividades ejecutadas por analistas L2/L3 y Team Lead.
Propósito: Optimizar detección, controlar calidad de automatización, gestionar accesos y revisar métricas.
Transforma datos brutos en inteligencia.

- S-01 Revisión reglas analíticas
- S-02 Ajuste falsos positivos
- S-03 Revisión eventos gobierno datos (Purview)
- S-04 Validación cobertura telemetría
- S-05 Análisis métricas
- S-06 Estudio tendencias
- S-07 Verificación playbooks
- S-08 Revisión accesos privilegiados
- S-09 Actualización documentación
- S-10 Revisión backlog incidentes

10 ACTIVIDADES
ANALISTAS L2/L3 + TEAM LEAD
NIST: IDENTIFY + GOVERN

Datos brutos → Inteligencia de mejora

CADENCIA AD-HOC: LA PRUEBA DE FUEGO

10 actividades activadas ante eventos materiales. Involucra SOC, IR, Legal, Privacidad y Reguladores. Pone a prueba la madurez bajo presión real.

- AH-01 Investigación forense
- AH-02 Legal holds
- AH-03 Acceso indebido records
- AH-04 Exfiltración DLP
- AH-05 Ajuste urgente políticas
- AH-06 Escalamiento legal
- AH-07 Soporte auditorías externas
- AH-08 Contención amenazas
- AH-09 Coordinación lecess· Legal/Privacidar stakeholders

SOC + IR + LEGAL + REGULADOR
ACCIONA MÚLTIPLES FUNCIONES NIST

Puede activarse desde cualquier cadencia

Prioridades estratégicas → Ajustes operacionales

3/10 CADENCIA DIARIA: EL PULSO OPERACIONAL

10 actividades ejecutadas por analistas L1/L2 en cada turno.
Propósito: Detección temprana, contención oportuna y visibilidad operacional. Genera el mayor volumen de evidencia granular.

- D-01 Revisión incidentes activos
- D-02 Triage alertas
- D-03 Validación auditoría activos/logs (inc. Purview)
- D-04 Verificación ingesta
- D-05 Revisión playbooks
- D-06 Monitoreo cambios admin
- D-07 Alertas DLP
- D-08 Actualización tickets
- D-09 Validación SLA
- D-10 Escalamiento al CISO

10 ACTIVIDADES
ANALISTAS L1/L2
NIST: DETECT + RESPOND

Datos brutos → Inteligencia de mejora

TABLA DE REFERENCIA RÁPIDA — ANATOMÍA DE CADA CADENCIA

Dimensión	Diaria	Semanal	Mensual	Ad-Hoc
Propósito	10 actividades ejecutadas por analistas L1/L2 en cada turno.	Propósito: Optimizar eettor, conouriación inidentes, pérdida granularidad.	10 actividades posturo cumplimiente regulatorio, madures del programa y ejecutivo.	10 actividades activadas ante eventos materiales. Involucra SOC, IR, Legal, Privacidad y Reguladores.
Actor principal	Analista L1/L2	Analista L2/L3 + TL	Team Lead + CISO	SOC + IR + Legal + Reg
Actividades	Validación auditoría activos/logs (inc. Purview)	Reglas desactualizadas, falsos positivos.	Postura no medida, apro auditoría.	Postura o medida, gaps auditoctiva.
Evidencia tipo	Evidencia tipo	Fvidencia	Actividaia	Posturzo no medida.
NIST CSF dominante	NIST CSF	NIST	Mensual	NIST
Plataforma primaria	Plataforma	Plameria	Plantarra	SOC + IR + Legal + Reg

EFECTO CASCADA DE UNA CADENCIA ROTA

- Todas Activas — Flujo Óptimo
- Sin Diaria — Acumulación incidentes, pérdida granularidad
- Sin Semanal — Reglas desactualizadas, falsos positivos
- Sin Mensual — Postura no medida, gaps auditoría
- Sin Ad-Hoc — Respuesta caótica, evidencia insuficiante

ESCALAMIENTO PROGRESIVO DE ACTORES

- Diario — Analista L1/L2
- Semanal — Analista L2/L3 + TL
- Mensual — Team Lead + CISO
- Ad-Hoc — SOC + IR + Legal + Reg

CÓDIGO DEL SISTEMA

La nomenclatura caos cnar D / 9 / M / AH es las actividades, un sistema de codiga consalta-la consultaria para referencia interno.

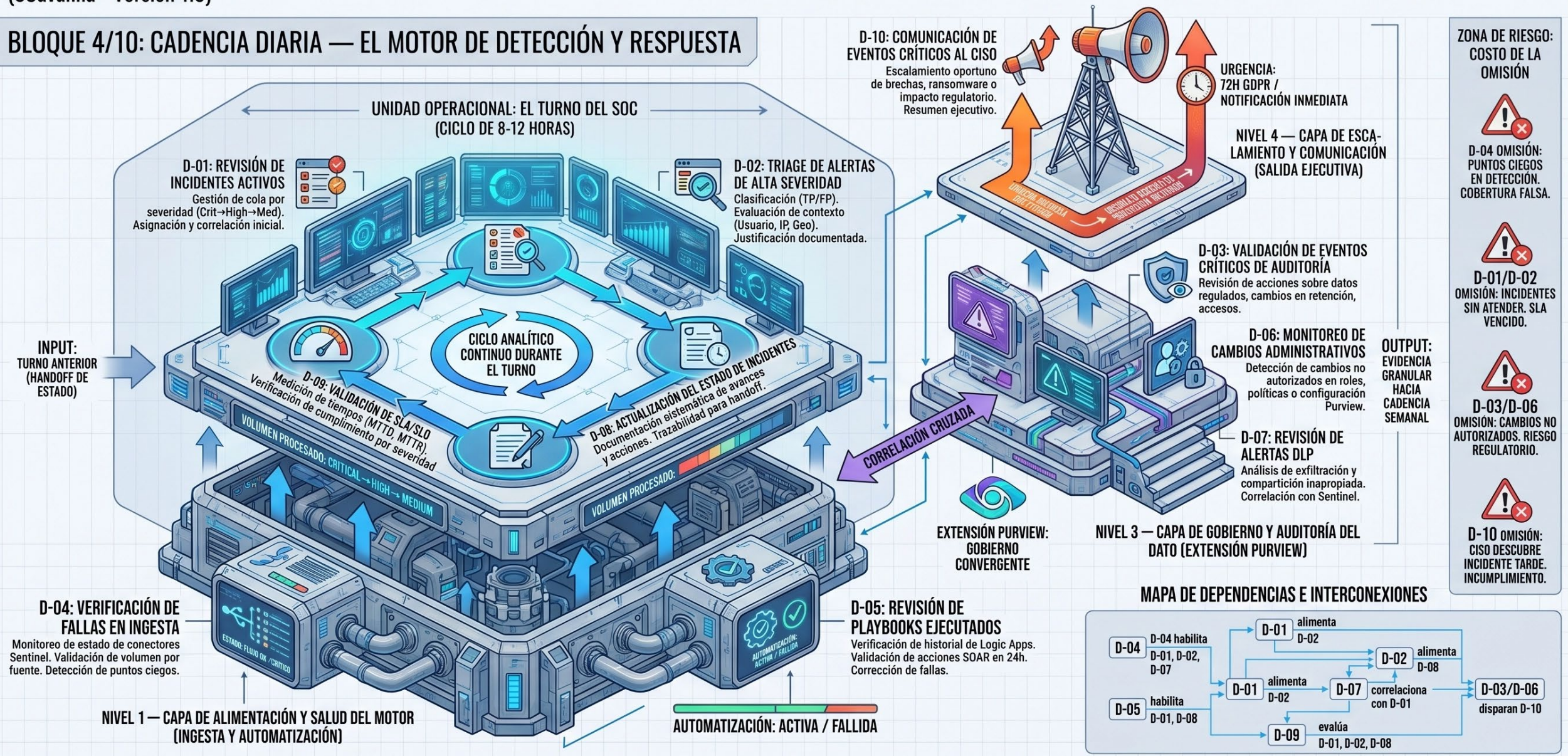
SERIES OVERVIEW: 10-PART FRAMEWORK

@SCavanna

MICROSOFT PURVIEW DATA LIFECYCLE & RECORDS MANAGEMENT (ADVANCED) - SOC/SECOPS EXCELLENCE FRAMEWORK

(SCavanna - Versión 1.0)

BLOQUE 4/10: CADENCIA DIARIA — EL MOTOR DE DETECCIÓN Y RESPUESTA



MAPA DE DEPENDENCIAS E INTERCONEXIONES

SERIES OVERVIEW: 10-PART FRAMEWORK

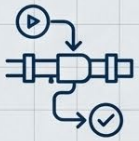
SERIES OVERVIEW: 10-PART FRAMEWORK
(SCavanna - Versión 1.0)

5/10 CADENCIA SEMANAL: OPTIMIZACIÓN, CALIDAD Y CONTROL

EN TRANSICIÓN: DEFENDER PORTAL

MÓDULO DE SALUD DE INFRAESTRUCTURA Y AUTOMATIZACIÓN

S-04 COBERTURA DE TELEMETRÍA
Validación de ingesta, identificación de brechas.



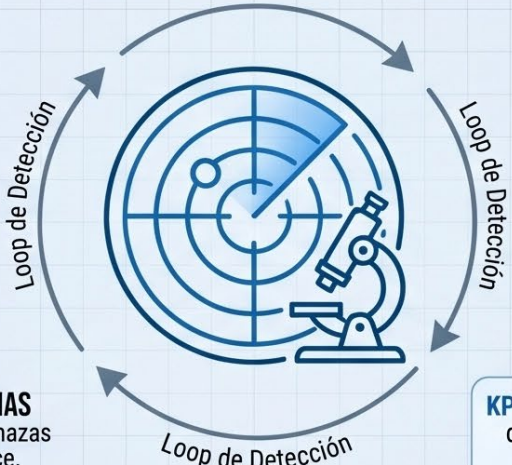
S-07 SALUD SOAR
Validación de playbooks, conectores y dependencias.

ESTADO: Monitoreo del estado de conectores y playbooks activos.

MÓDULO DE OPTIMIZACIÓN DE DETECCIÓN (EL CORE)

S-01 CATÁLOGO DE REGLAS
Revisión de reglas activas, nuevas plantillas, baja fidelidad.

S-06 ANÁLISIS DE TENDENCIAS
Identificación de patrones, amenazas recurrentes, threat intelligence.



S-02 AJUSTE DE UMBRALES
Reducción de falsos positivos, ajuste de condiciones.

KPI: Monitoreo continuo del ratio de falsos positivos semana a semana.

MÓDULO DE GOBIERNO Y AUDITORÍA PURVIEW

S-03 AUDITORÍA DEL DATO
Revisión de alertas Purview, ciclo de vida, disposición.

S-08 ACCESOS PRIVILEGIADOS
Revisión de roles críticos, PIM, permission drift.

GOBIERNO: Monitoreo de accesos proporcionales, PIM en uso.

MÓDULO DE MÉTRICAS Y RENDIMIENTO

Diario actividad

Data

S-05 DASHBOARD DE MÉTRICAS
Análisis de eficiencia operacional, tendencias semanales.

S-10 CALIDAD DE CIERRE
Auditoría de incidentes cerrados, detección de cierres prematuros.

RENDIMIENTO: Monitoreo y análisis de métricas semana a semana.

MÓDULO DE DOCUMENTACIÓN Y CONOCIMIENTO

S-09 ACTUALIZACIÓN DE RUNBOOKS
Incorporación de aprendizajes, versionado de procedimientos.

CAPITAL: Número de runbooks actualizados y lecciones incorporadas.

Número de repositorios

Governancia

Maturitad assessmentos

DIARIO (INPUTS) → SEMANAL (PROCESAMIENTO) → MENSUAL (OUTPUTS)

Nota: La cadencia semanal procesa inputs diarios y genera outputs para el gobierno mensual.

MICROSOFT PURVIEW DATA LIFECYCLE & RECORDS MANAGEMENT (ADVANCED) - SOC / SECOPS EXCELLENCE FRAMEWORK (SCavanna - Versión 1.0)

Bloque 6/10: Cadencia Mensual — Gobierno, Madurez y Reporte Estratégico

HITO 1: EVALUACIÓN DE POSTURA
(¿DÓNDE ESTAMOS?)

M-01 POSTURA GLOBAL
Secure Score + Optimización SOC. Brechas top 3. ↑ Mejora

M-02 COBERTURA MITRE ATT&CK
Mapeo de tácticas/técnicas. Priorización de nuevos casos.

M-07 COSTOS DE INGESTA
Análisis de volumen/valor. Proyección de eficiencia.

MARCO REGULATORIO APLICABLE
- Argentina (Ley 25.326)
- UE (GDPR)
- US (SOX)

Postura evaluada → **Hacia la auditoría**

HITO 2: AUDITORÍA Y CUMPLIMIENTO
(¿ESTAMOS CUMPLIENDO?)

M-03 POLÍTICAS DE RETENCIÓN
Revisión contra obligaciones. Clasificadores entrenables.

M-04 ACCESOS ADMINISTRATIVOS
Auditoría de roles y cambios. Segregación de funciones.

M-08 VALIDACIÓN REGULATORIA (INTERNA)
Ley 25.326, GDPR, SOX

Estado de controles técnicos y legales. Legal Holds.

Cumplimiento validado → **Hacia la simulación**

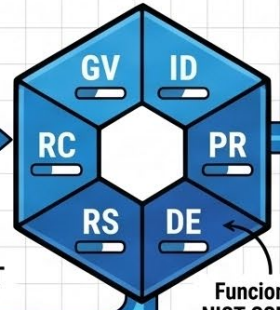
HITO 3: SIMULACIÓN Y APRENDIZAJE
(¿ESTAMOS PREPARADOS?)

M-05 LECCIONES APRENDIDAS
Análisis de incidentes reales. Acciones correctivas definidas.

M-09 EJERCICIO TABLETOP
Simulación de escenarios de alto impacto. Validación de runbooks.

Preparación probada → **Hacia la alineación NIST**

HITO 4: ALINEACIÓN ESTRATÉGICA NIST CSF 2.0
(¿CÓMO LO COMUNICAMOS?)



Funciones NIST CSF 2.0

M-06 REVISIÓN DE ALINEACIÓN NIST
Evaluación consultiva de madurez por función. Traducción a lenguaje ejecutivo.

Madurez traducida → **Convergencia en el reporte final**

Madurez traducida → **Convergencia en el reporte final**

Hitos 1-4 → 5 Secciones del Reporte

Atención del CISO: Ventana de 30 min

HITO 5: SÍNTESIS Y REPORTE EJECUTIVO
(EL ENTREGABLE FINAL)

M-10 REPORTE AL CISO Y LIDERAZGO

PANEL SENTINEL (EFICIENCIA)
MTTD/MTTR, Volumen, SLA, Cobertura MITRE, Costos.

PANEL PURVIEW (GOBIERNO)
Datos ROT eliminados, Clasificación, Legal Holds, Disposiciones.

CISO · JUNTA DIRECTIVA · REGULADORES

- Decisiones de Inversión
- Capacitación
- Herramientas

Motor de Inversión Estratégica

MICROSOFT PURVIEW DATA LIFECYCLE & RECORDS MANAGEMENT (ADVANCED) - SOC / SECOPS EXCELLENCE FRAMEWORK (SCavanna - Versión 1.0)

(7/10) RESPUESTA AD-HOC: PROTOCOLO DE ACTIVACIÓN ANTE INCIDENTES MATERIALES

Architects Daughter
Prueba ácida de la convergencia Sentinel + Purview bajo presión.

ACTIVACIÓN: INCIDENTE MATERIAL DETECTADO

1. INVESTIGACIÓN Y DETERMINACIÓN DE ALCANCE

Reconstruir lo sucedido y delimitar alcance real.
- Forense de datos con Purview Audit Premium (timeline de accesos, modificaciones).
- Análisis de acceso indebido a registros (correlación usuario/ubicación con Sentinel).

Tools: Purview Audit Premium, eDiscovery Premium

Architects Daughter
La calidad forense determina la solidez de las siguientes fases.

2. CONTENCIÓN Y ERRADICACIÓN TÉCNICA

Detener amenaza y eliminar presencia.
- Aislamiento de dispositivos, bloqueo de cuentas, revocación de tokens desde Defender Portal.
- Respuesta a exfiltración (DLP): Bloqueo de canal.

Tools: Defender XDR, Sentinel SOAR (Playbooks), DLP

Velocidad crítica.
MTTR reducido vía integración sin cambio de consola.

CONVERGENCIA SENTINEL + PURVIEW

Narrativa unificada: Timeline de Amenazas (Sentinel) + Timeline de Datos (Purview). Ej: Compromiso -> Acceso Docs -> Intento Exfiltración.

2. CONTENCIÓN Y ERRADICACIÓN TÉCNICA

Detener amenaza y eliminar presencia.
- Aislamiento de dispositivos, bloqueo de cuentas, revocación de tokens desde Defender Portal.
- Respuesta a exfiltración (DLP): Bloqueo de canal.

Tools: Defender XDR, Sentinel SOAR, DLP

Architects Daughter
Determina la rense de las cuansestiases.

3. PRESERVACIÓN LEGAL Y COMPLIANCE

Activar controles legales en paralelo.
- Activación de Legal Hold en Purview (custodios, fechas, keywords).
- Ajuste inmediato de políticas de retención ante cambios regulatorios.

Tools: Purview Legal Hold, Retention Policies

Protege contra riesgos jurídicos (spoliation) por hold tardío.

4. ESCALAMIENTO Y COORDINACIÓN MULTI-ACTOR

- Protocolo formal de notificación si supera umbrales.
- Coordinación SOC, Legal, DPO, Regulador.
- Comunicación estructurada a stakeholders.

Respuesta multidisciplinaria; incumplimiento de plazos amplifica consecuencias.

5. SOPORTE A AUDITORÍA Y CIERRE

Provisión de evidencia y cierre formal.
- Proveer logs técnicos, acceso controlado a plataformas y documentación de interacciones para auditores externos.

Evidencia estructurada reduce hallazgos adversos.

RETROALIMENTACIÓN A CADENCIAS REGULARES

- PIR mensual (lecciones aprendidas)
- Actualización Runbooks/ Reglas Detección
- Ejercicios Tabletop
- Revisión NIST RESPOND/RECOVER

Architects Daughter:
El aprendizaje institucional solo ocurre si el incidente se documenta.

ÁRBOL DE DECISIÓN: ACTIVACIÓN SEGÚN ESCENARIO

Tipo de Incidente	Ramas Activadas	Actores Involucrados
Ransomware activo	Investigación, Contención, Escalamiento, Auditoría	SOC, IR, CISO, Legal, Comms
Exfiltración datos sensibles	Investigación, Contención DLP, Preservación Legal, Escalamiento Reg., Auditoría	SOC, DLP Team, Legal, DPO, Regulador
Compromiso cuenta privilegiada	Investigación, Contención, Escalamiento CISO	SOC, IR, Identity Team, CISO
Acceso indebido records regulados	Investigación, Preservación Legal, Escalamiento Legal	SOC, Purview Admin, Legal, Data Gov
Solicitud Legal Hold (Litigio)	Preservación Legal (directo)	Legal -> SOC/Purview Admin

PLAZOS REGULATORIOS CRÍTICOS

Obligación	Plazo	Consecuencia Incumplimiento
Notificación GDPR	72 horas	Multa hasta 4% volumen global
Notificación LGPD	30 días	Sanciones admin/reputacionales
Activación Legal Hold (US)	Inmediato al litigio	Riesgo spoliation (legal)
Preservación evidencia forense	Antes de remediación	Pérdida admisibilidad legal

ANTI-PATRÓN VS. SOC PREPARADO

Dimensión	SOC Preparado ✓	SOC Reactivo ✗
Investigación	Timeline en horas	Búsqueda manual días
Contención	Playbook automático	Acciones manuales
Preservación Legal	Inmediato	Tardío
Escalamiento	Protocolo con evidencia	Notificación improvisada

CONEXIONES EXTERNAS: Alimenta Bloques 2, 3, 4, 6, 8, 9 del framework.

MICROSOFT PURVIEW DATA LIFECYCLE & RECORDS MANAGEMENT (ADVANCED) - SOC / SECOPS EXCELLENCE FRAMEWORK

(SCavanna - Versión 1.0) - BLOQUE 8/10: **ALINEACIÓN NIST CSF 2.0 — DE LAS 6 FUNCIONES A LA EVIDENCIA OPERACIONAL**

NIST CSF 2.0 ANALYTIC MATRIX	CADENCIA DIARIA (D)	CADENCIA SEMANAL (S)	CADENCIA MENSUAL (M)	CADENCIA AD-HOC (AH)	EVIDENCIA NATIVA GENERADA (SUBPRODUCTO OPERACIONAL)
GOVERN (GV) - GOBIERNO DEL PROGRAMA DE SEGURIDAD	**D-10** Escalamiento al CISO (Reporte Ejecutivo)	**S-08** Revisión de Accesos Privilegiados (Auditoría)	**M-06** Revisión Alineación NIST (Evaluación); **M-08** Auditoría Interna (Cumplimiento); **M-10** Reporte Ejecutivo (KPIs y Madurez)	**CONVERGENCIA PLENA: SENTINEL + PURVIEW**	Políticas Config., Aprobaciones Disposición, Reportes Eliminación ROT, Logs Escalamiento, Reportes Ejecutivos
IDENTIFY (ID) - CONOCER LOS ACTIVOS Y EL RIESGO		**S-04** Validación Cobertura Telemetría (Mapa de Ingesta)	**M-02** Evaluación Cobertura MITRE ATT&CK (Gap Analysis); **M-03** Revisión Políticas Retención (File Plan)		Inventario Clasificado, Mapa Cobertura Ingesta, Mapa Cobertura MITRE, File Plan Actualizado
PROTECT (PR) - SALVAGUARDAR LOS ACTIVOS CRÍTICOS	**D-03** Validación Eventos Críticos Auditoría (Purview); **D-06** Monitoreo Cambios Admin (Entra ID)		**DOMINIO PURVIEW: GOBIERNO DEL DATO**	**AH-02** Activación Legal Hold (Preservación); **AH-05** Ajuste Inmediato Políticas Retención (Reducción Superficie)	Records Declarados, Historial Legal Holds, Logs Acceso Admin/RBAC, Políticas Retención Activas
DETECT (DE) - IDENTIFICAR EVENTOS DE SEGURIDAD	**D-01** Revisión Incidentes (Triage); **D-02** Triage de Alertas (Análisis); **D-04** Verificación de Ingesta (Salud); **D-07** Alertas DLP (Fuga de Datos)	**S-01** Revisión Reglas Analíticas (Optimización)	**DOMINIO SENTINEL: OPERACIONES DE SEGURIDAD**		Unified Audit Log, SentinelHealth Status, Logs Ejecución Playbooks, Historial Reglas & Fidelidad
RESPOND (RS) - ACTUAR ANTE INCIDENTES DETECTADOS	**D-10** Escalamiento al CISO (Notificación)			**AH-04** Respuesta a Exfiltración (Contención); **AH-06** Escalamiento Legal/Regulatorio (Notificación); **AH-08** Contención y Erradicación (Playbooks)	Logs Contención & Timestamp, Reportes Preservación, Timeline Completo Incidente, Registros Notificación
RECOVER (RC) - RESTAURAR Y APRENDER	**CONVERGENCIA PLENA: SENTINEL + PURVIEW**		**M-05** Lecciones Aprendidas / PIR (Mejora Continua); **M-09** Ejercicios Tabletop (Simulación)	**AH-07** Soporte a Auditorías Externas (Evidencia)	Versionado Histórico Políticas/Runbooks, Reportes PIR & Acciones, Métricas Comparativas Pre/Post, Hallazgos Tabletop

NIST CSF 2.0: Lenguaje vivo de madurez, no solo compliance.

Evidencia generada automáticamente por la operación diaria.

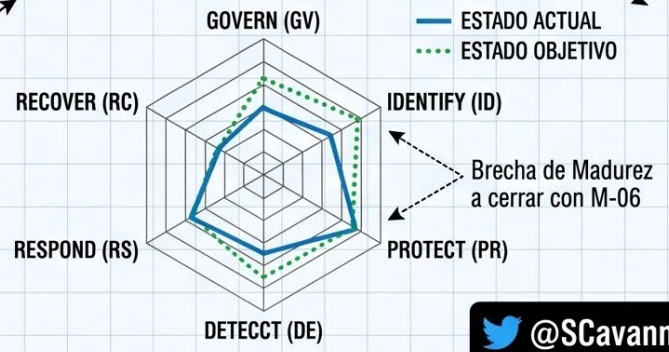
EL ARGUMENTO ESTRATÉGICO: COMPLIANCE COMO SUBPRODUCTO

Reducción Significativa del Esfuerzo Manual

La operación de seguridad automatiza parte de la generación de evidencia de compliance.

Las revisiones mensuales (M-06) transforman la operación en un lenguaje de madurez NIST verificable.

BRÚJULA DE MADUREZ NIST CSF 2.0



SERIES OVERVIEW: 10-PART FRAMEWORK

8/10: ALINEACIÓN NIST CSF 2.0

@SCavanna

MICROSOFT PURVIEW DATA LIFECYCLE & RECORDS MANAGEMENT (ADVANCED) - SOC/SECOPS EXCELLENCE FRAMEWORK

(SCavanna – Versión 1.0) - SERIES OVERVIEW: 10-PART FRAMEWORK - BLOQUE 9/10: KPIs DEL SOC — TABLERO DE EXCELENCIA OPERACIONAL

PANEL DE VELOCIDAD (TIEMPO - MTTD/MTTR)

MTTD (Mean Time to Detect)
Tiempo promedio ocurrencia a detección. Mide priorización. **Target Excelencia: <5 min (Critical).**

MTTR (Mean Time to Respond)
Tiempo detección a cierre (triage, respuesta). Evidencia mejora operacional. **Target Excelencia: <30 min (Critical).**

Ciclo de vida del incidente en tiempo.
¿Cuánto tardamos en ver y detener la amenaza?

Architects Daughter

PANEL DE CALIDAD (FIDELIDAD - RULE HEALTH)

RATIO FALSOS POSITIVOS
% alertas clasificadas falso positivo. **>30%** indica reglas mal calibradas o fatiga. **Target Excelencia: <10%.**

SLA PRIMERA RESPUESTA
% incidentes respondidos en tiempo definido. Demuestra constancia. **Target Excelencia: >99% (Critical).**

Control de calidad: velocidad sin fidelidad genera ruido.

TABLERO CENTRAL DE EXCELENCIA (SOC + GOBIERNO)

Convergencia de Métricas: Velocidad, Calidad, Alcance, Compliance y Escala como instrumento de decisión.

PANEL DE COBERTURA (ALCANCE - VISIBILIDAD)

COBERTURA MITRE ATT&CK
% tácticas/técnicas con detección activa. Seguimiento de mejora gradual. **Target Excelencia: >80%.**

FALLAS DE INGESTA
Conectores con interrupción >1h. Puntos ciegos críticos a minimizar.

FALLAS DE INGESTA
Conectores con interrupción >1h. Puntos ciegos críticos a minimizar.

TASA DE AUTOMATIZACIÓN
% incidentes con acciones SOAR. Escala de respuesta. **Target Excelencia: >70%.**

Métrica Invisible: Costo del Incidente No Detectado
(aproximado por brechas en MITRE e Ingesta).

PANEL DE CONTEXTO OPERACIONAL (ESCALA/COSTO)

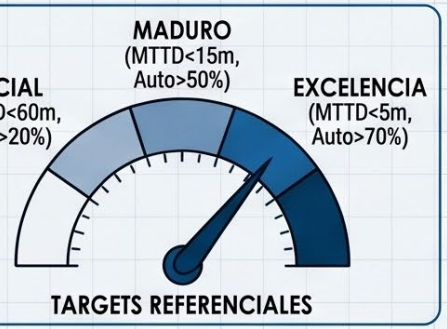
VOLUMEN INCIDENTES (SEVERIDAD)
Distribución mensual. Revela tendencias e inflación por nuevas reglas.

COSTOS DE INGESTA (SENTINEL)
Volumen/costo por fuente. Proyección de gastos y justificación de inversión.

Transforma Purview en una herramienta medible y accionable para el CISO.

PANEL DE GOBIERNO DEL DATO (METRICAS PURVIEW - COMPLIANCE)

ROT DATA ELIMINADA	COBERTURA CLASIFICACIÓN	AUTOMATIZACIÓN ETIQUETADO	LEGAL HOLDS ACTIVOS	TIEMPO ACTIVACIÓN HOLD	INCIDENTES AUDITORÍA
Reducción superficie riesgo.	% docs con etiqueta Target Exc: >85%.	% aplicado vs. manual.	Volumen preservado.	Solicitud a activación. Target Exc: <1h.	Accesos anómalos detectados.



CADENCIA DE REVISIÓN Y NIVELES DE MADUREZ (INTEGRACIÓN)

DIARIA (Analista/Lead) — MTTD, MTTR, SLA, Fallas → **DASHBOARD OPERACIONAL**

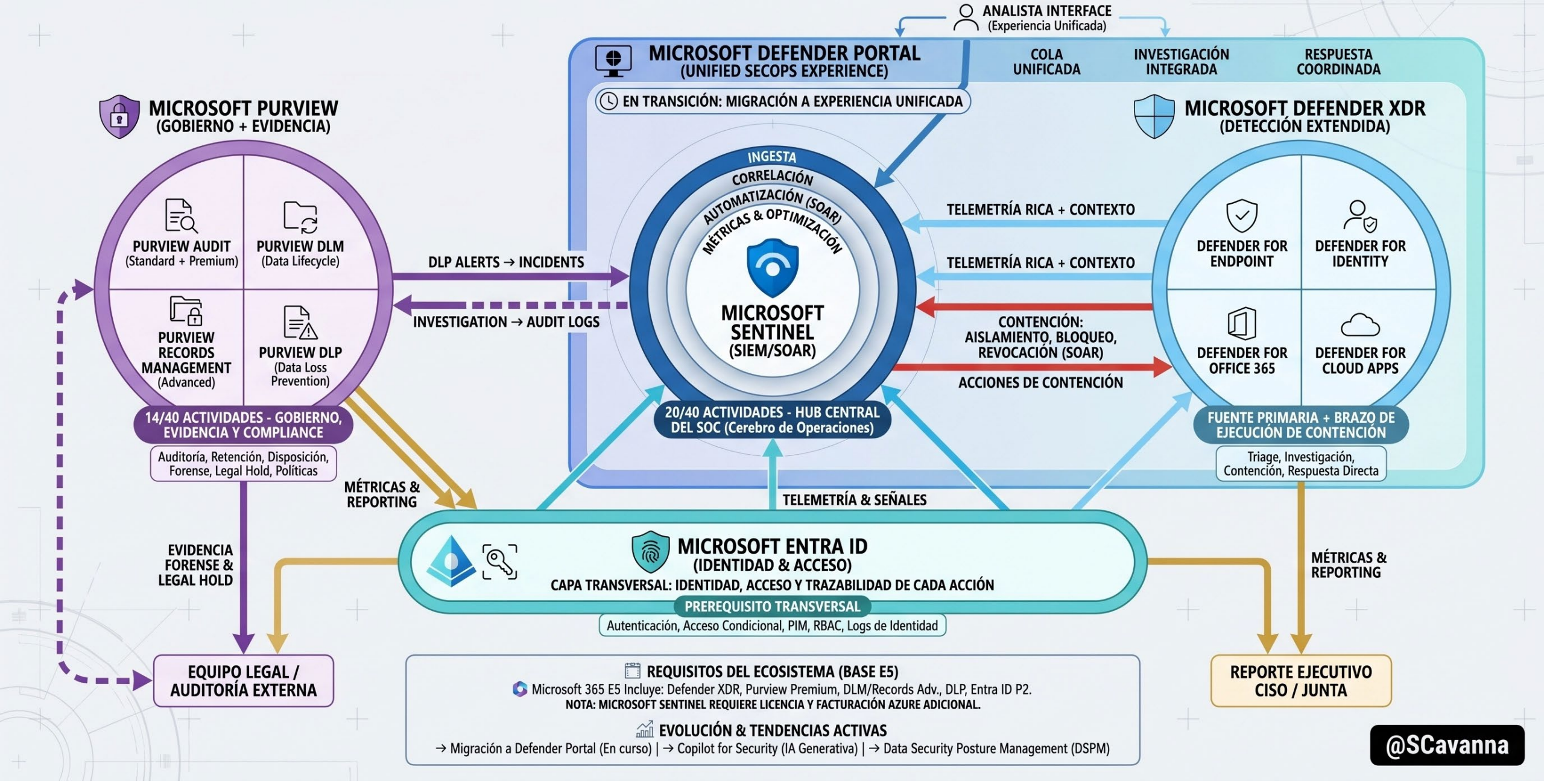
SEMANAL (Lead/L2-L3) — Falsos Positivos, Automatización, Tendencias → **REPORTE OPTIMIZACIÓN**

MENSUAL (CISO/GRC) — MITRE, Gobierno Purview, Costos, Resumen Ejecutivo → **REPORTE EJECUTIVO ESTRATÉGICO**

CONEXIONES EXTERNAS DE LA SERIE: Cuantifica principio de respuesta (Bloque 2).
Alimenta cadencias diaria/semanal/mensual (Bloques 4, 5, 6). Mide funciones NIST (Bloque 8).

MICROSOFT PURVIEW DATA LIFECYCLE & RECORDS MANAGEMENT (ADVANCED) - SOC/SECOPS EXCELLENCE FRAMEWORK (SCavanna - Versión 1.0)

10/10 STACK TECNOLÓGICO Y MAPA DE ACTIVIDADES POR HERRAMIENTA - Qué hace cada herramienta, cuándo se usa y cómo se conectan.



@SCavanna