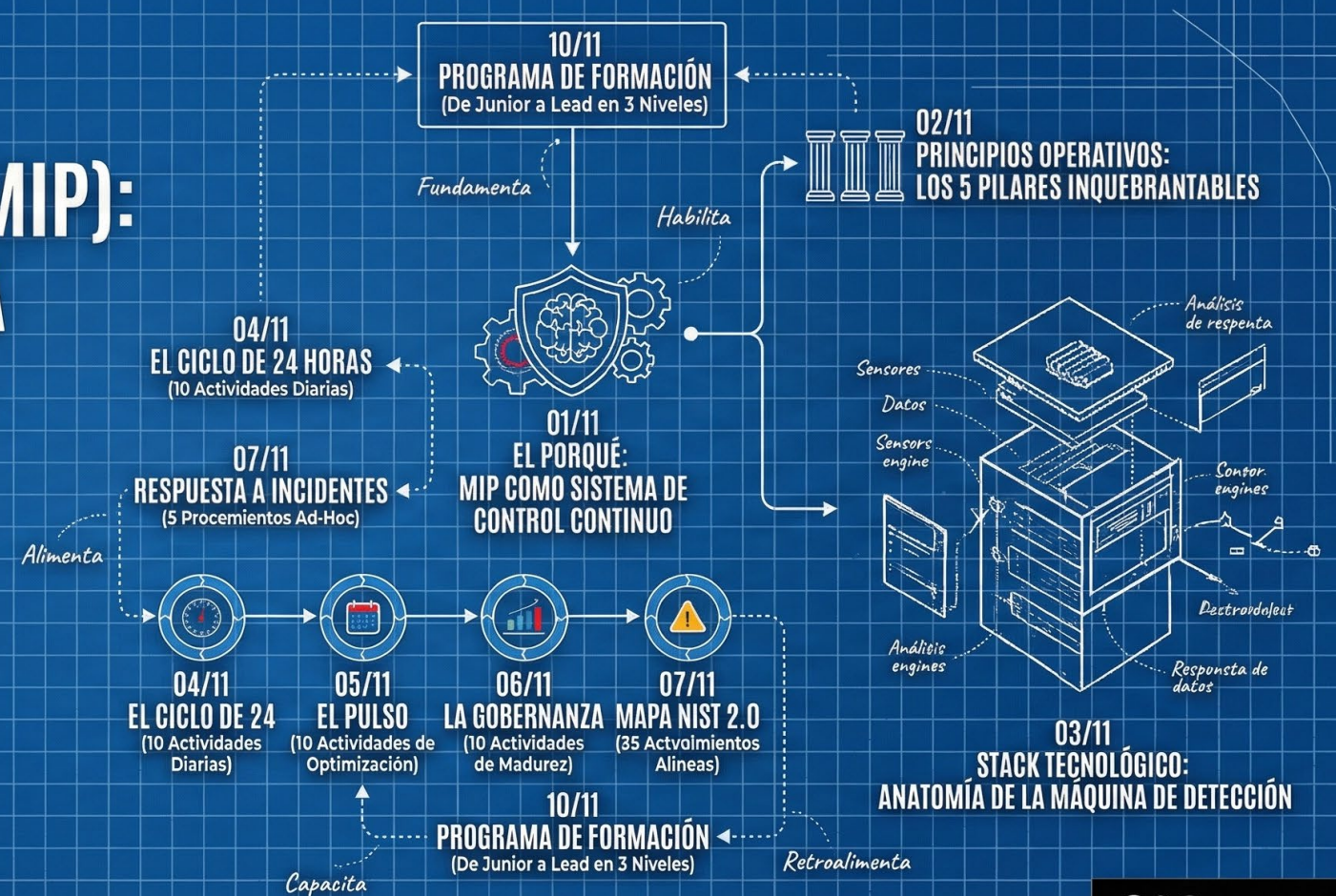
IP

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

MICROSOFT PURVIEW INFORMATION PROTECTION (MIP): GUÍA MODELO DE EXCELENCIA OPERACIONAL SOC / SECOPS

Serie Infográfica de 11 Artefactos.

P ano de Contro



Series Overview: 11-Part Framework

Blueprint Sistémico-Editorial

@SCavanna

MASTER PLAN — INFOGRAFÍAS MIP SOC OPERATIONAL EXCELLENCE

SERIE: [ÍNDICE]

Análisis Preliminar Completado y Mapa Sistémico de los 11 Nodos de Información

1/11

EL PORQUÉ: MIP COMO SISTEMA DE CONTROL CONTINUO

Fundamentos del modelo, las 3 responsabilidades simultáneas, por qué la telemetría sin operación es señal muerta.

2/11

PRINCIPIOS OPERATIVOS: LOS 5 PILARES INQUEBRANTABLES

Los 5 principios con sus implicancias prácticas — el "código genético" del modelo.

3/11

STACK TECNOLÓGICO: ANATOMÍA DE LA MÁQUINA DE DETECCIÓN

Fuentes de telemetría → plataforma de correlación → controles de mitigación como sistema de capas.

Prerrequisito Directo

4/11

EL CICLO DE 24 HORAS: 10 ACTIVIDADES DIARIAS DEL SOC

Las 10 actividades diarias como flujo operativo con dependencias internas.

Outputs Diarios Alimentan

Pueden Activarse Desde

5/11

EL PULSO SEMANAL: 10 ACTIVIDADES DE OPTIMIZACIÓN

Las 10 actividades semanales como ciclo de mejora continua que refina lo detectado en el ciclo diario.

Outputs Diarios Alimentan

6/11

LA GOBERNANZA MENSUAL: 10 ACTIVIDADES DE MADUREZ

Las 10 actividades mensuales como el nivel de gobierno que demuestra madurez ante auditorías y reguladores.

Hallazgos Semanales Alimentan

Pueden Activarse Desde

7/11

RESPUESTA A INCIDENTES: 5 PROCEDIMIENTOS AD-HOC

Los 5 procedimientos como algoritmo de decisión escalonado: triage → contención → forense → legal → post-mortem.

8/11

TABLERO DE CONTROL: KPIS Y SEÑALES DE DEGRADACIÓN

Los 11 KPIs primarios + las 6 señales de alerta temprana como panel de instrumentos de un SOC.

KPIs Transversales

9/11

MAPA NIST CSF 2.0: 35 ACTIVIDADES ALINEADAS

El mapeo completo de las 35 actividades a las 6 funciones del CSF 2.0 como ecosistema de cobertura.

Marco Normalizador

10/11

PROGRAMA DE FORMACIÓN: DE JUNIOR A LEAD EN 3 NIVELES

Los 3 niveles de competencia, recursos verificables y mapa de habilitación por actividad.

Habilita Actividades

11/11

IMPLEMENTACIÓN PROGRESIVA: DE CERO A EXCELENCIA EN 4 FASES

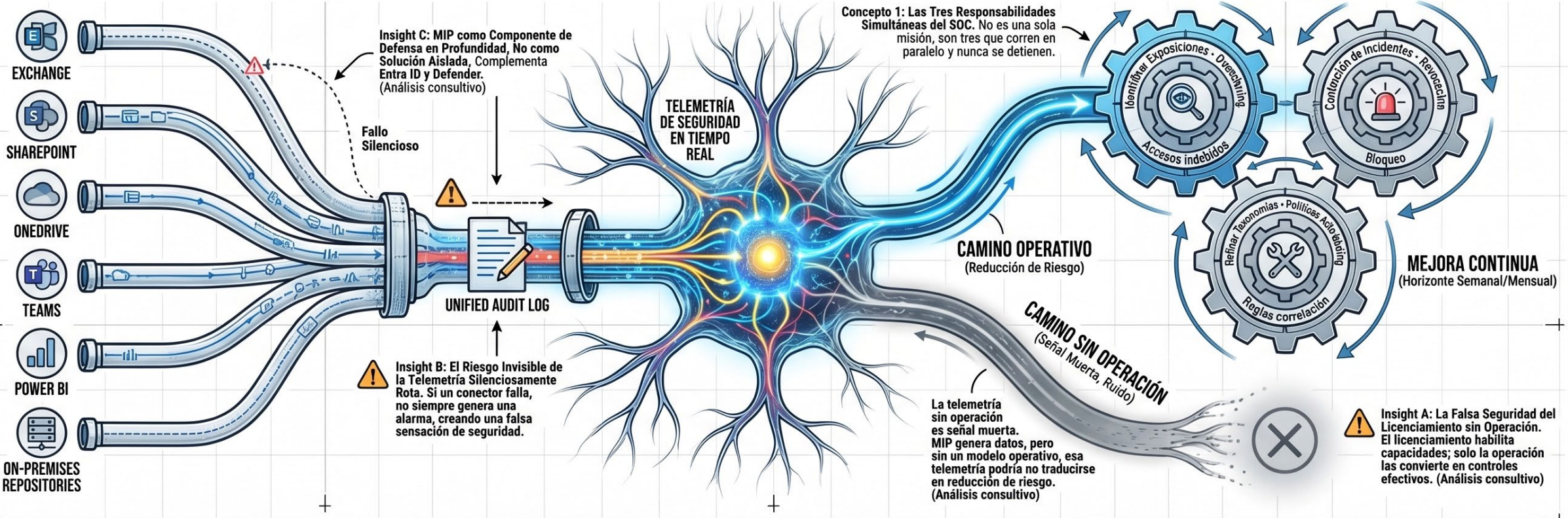
Las 4 fases de implementación + prerrequisitos técnicos + valor demostrable ante auditorías por fase.

Nota de Diseño: Asegura que cada pieza de la serie funcione como una unidad independiente pero mantenga una coherencia sistémica (mismo ADN visual y paleta funcional).

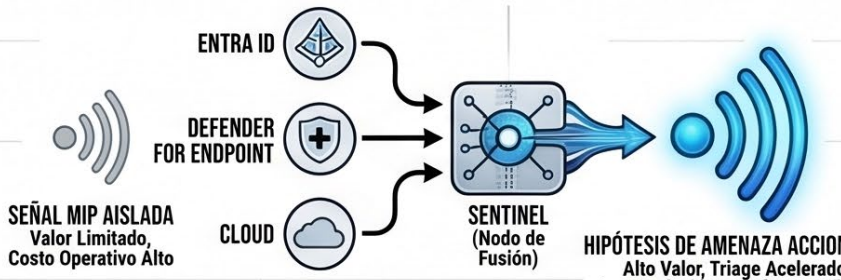
@SCavanna

EL PORQUÉ: MIP NO ES UNA CONFIGURACIÓN — ES UN SISTEMA DE CONTROL CONTINUO DE DATOS

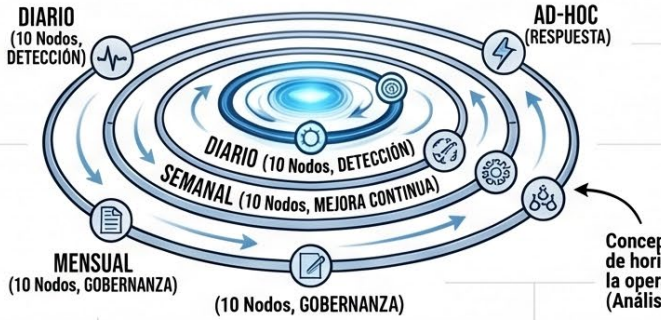
Infografía 01 de 11 · Serie: SOC Operational Excellence para Microsoft Purview Information Protection



CORRELACIÓN SOBRE AISLAMIENTO — EL MULTIPLICADOR DE VALOR



CUATRO HORIZONTES TEMPORALES, UN SOLO MODELO



Concepto 4: Uso consultivo de horizontes para estructurar la operación interna. (Análisis consultivo)

EVIDENCIA AUDITABLE POR DISEÑO — EL DOBLE PROPÓSITO

No son dos procesos separados, son el mismo acto con doble resultado. (Principio consultivo)

@SCavanna

LOS 5 PILARES INQUEBRANTABLES: CÓDIGO GENÉTICO DEL SOC QUE OPERA MIP

Infografía 02 de 11 · Serie: SOC Operational Excellence para Microsoft Purview Information Protection

Bento Box

Nota de Soporte A:
Los principios como criterio de decisión ante la ambigüedad.

CORE INSIGHT: LOS PILARES NO SON OPCIONALES

Estos cinco principios no son aspiracionales — son restricciones de diseño. Cada actividad del modelo, cada procedimiento y cada métrica existe porque estos principios lo exigen. Violar cualquiera de ellos no degrada el modelo: lo invalida.

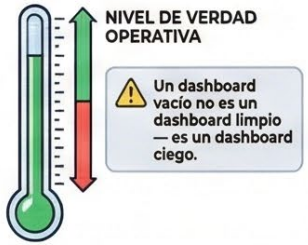
Sin estos pilares, la estructura colapsa. Son el lenguaje común entre el SOC y el Board.

Nota de Soporte B:
Interdependencia crítica: Correlación requiere Telemetría, Mejora requiere Evidencia.

TELEMETRÍA COMO FUENTE DE VERDAD

1/5

El Microsoft 365 Unified Audit Log es la fuente primaria y no negociable. Su integridad determina la capacidad operativa. Validación proactiva y monitoreo de workloads sin eventos son esenciales para evitar la ceguera operativa.

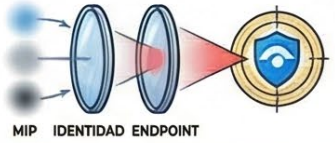


Conexión Externa:
→ Bloques 4 y 5 (Verificación y Cobertura)

CORRELACIÓN SOBRE AISLAMIENTO

2/5

Los eventos de MIP ganan valor máximo al correlacionarse con Entra ID, Defender y señales de nube en Microsoft Sentinel. La correlación reduce el ruido y revela patrones de ataque complejos.



Señal MIP sola:		Señal correlacionada:		Hipótesis:
Descarga masiva	+	IP anómala	=	Exfiltración post-compromiso

Conexión Externa:
→ Bloque 3 (Stack Tecnológico)

MEJORA ITERATIVA SIN DISRUPCIÓN

3/5

Políticas, reglas y taxonomía deben evolucionar continuamente sin causar impacto. Ciclos de tuning, simulación obligatoria y validación previa son el protocolo estricto para evitar riesgos.

Conexión Externa:
→ Bloque 5 (Tuning y Validación)

Nota de Soporte C:
Traducción para el CISO: Telemetría = Visibilidad, Correlación = Detección Avanzada.

EVIDENCIA AUDITABLE POR DISEÑO

4/5

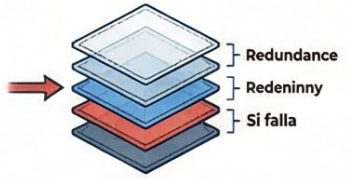
Cada actividad genera evidencia trazable y exportable como resultado intrínseco, no como un paso adicional. La operación debe estar lista para auditorías en todo momento.

Conexión Externa:
→ Bloque 8 (KPIs de Evidencia)

DEFENSA EN PROFUNDIDAD CENTRADA EN DATOS

5/5

MIP es el control primario pero complementario. La seguridad emerge de la intersección coordinada de múltiples controles en capas, no de un solo punto de fallo.



Si falla una capa, las otras contienen. Validación periódica de integración es clave.

Conexión Externa:
→ Bloque 6 (Validación de Integración)

Nota de Soporte D:
Configurar MIP es un proyecto; operar MIP es un compromiso permanente bajo estos principios.

Bento Box

@SCavanna

ANATOMÍA DE LA MÁQUINA DE DETECCIÓN: CÓMO FLUYE LA TELEMETRÍA DESDE EL DATO HASTA LA DECISIÓN

Infografía 03 de 11 · Serie: SOC Operational Excellence para Microsoft Purview Information Protection

CAPA DE MITIGACIÓN ACTIVA — LOS CONTROLES DE RESPUESTA

Defensa en profundidad: ejecución combinada en AH-B.

Conexión a Bloque 7

CONTROL 1: REVOCACIÓN DE ACCESO (PURVIEW)
Cortar acceso a documento protegido globalmente. Confirmación con RMSAccessDenied.

ACTIVAR

CONTROL 2: BLOQUEO DE CUENTA/TOKENS (ENTRA ID)
Bloqueo de sign-in y revocación de sesiones activas. Capa de identidad.

ACTIVAR

CONTROL 3: MODIFICACIÓN DE USAGE RIGHTS (AZURE RMS)
Ajuste dinámico de permisos (imprimir, copiar, etc.) sin revocar acceso total.

AJUSTAR

CONTROL 4: HOLD DE PRESERVACIÓN (EDISCOVERY)
Forense: Preserva contenido relevante para investigación legal/regulatoria.

PRESERVAR

SECUENCIA TÍPICA EN INCIDENTE CRÍTICO (<1 HORA RECOMENDADA): REVOCACIÓN → BLOQUEO → MODIFICACIÓN → HOLD

Defensa en profundidad: ejecución combinada en AH-B

Insight A: El Concor como Punto Único de Fallo Silencioso. Monitoreo D-07 es vital.

CAPA DE CORRELACIÓN E INTELIGENCIA — MICROSOFT SENTINEL COMO SISTEMA NERVIOSO

DATA CONNECTORS
Puntos de ingesta de telemetría. Estado crítico diario.

Connected
Degraded
Disconnected

ANALYTICS RULES
Correlación de señales para generar incidentes. Requiere ajuste periódico.

WORKBOOKS
Dashboards operativos para visibilidad centralizada. Interfaz visual del SOC.

PLAYBOOKS (LOGIC APPS)
Automatización de respuestas para reducir latencia en escenarios de alta confianza.

No es solo un repositorio; es el motor de inteligencia. Conexión a Bloque 4 (D-03) y Bloque 5 (S-07)

Insight D: El Stack como Prerrequisito del Modelo. Planes de mitigación para componentes faltantes.

CAPA DE GENERACIÓN DE SEÑAL — LAS FUENTES DE TELEMETRÍA

Inteligencia Operativa | Auditoría Centralizada | Ingesta y Transformación

MICROSOFT PURVIEW PORTAL
- Alert Policies (Violaciones en tiempo real)
- Content Explorer (Inventario vivo de datos sensibles)
- Activity Explorer (Registro de etiquetado y tendencias)

M365 UNIFIED AUDIT LOG
- Eventos de Sensitivity Labels (Apply, Change, Remove)
- Eventos de Azure RMS (Protect, Access Denied)
- Eventos de Oversharing (FileSensitivityLabelMismatch)

MICROSOFT SENTINEL (RECEPTOR)
- Ingesta de logs de Purview y Audit Log vía Data Connectors
- Transformación en datos consultables y correlacionables

Architects Daughter

Origen simultáneo para garantizar cobertura total. Conexión a Bloque 4: D-01, D-02, D-07

CORE INSIGHT: EL CIRCUITO CERRADO

GENERACIÓN (Señal Cruda) → CORRELACIÓN (Inteligencia) → ACCIÓN (Mitigacion) → GENERACIÓN

El stack no es un catálogo de herramientas — es un circuito cerrado de tres fases. Si cualquier fase se interrumpe, el circuito se rompe y el SOC pierde capacidad operativa sin advertencia visible. La corriente debe fluir 24/7.

VOCABULARIO DE RIESGO DEL AUDIT LOG (EVENTOS PRIORITARIOS)

EVENTO	QUÉ SIGNIFICA	NIVEL DE RIESGO	RESPUESTA ESPERADA
SensitivityLabelRemoved	Desprotección deliberada	ALTO (Rojo)	Investigar usuario/contexto
SensitivityLabelChanged (downgrade)	Reducción de protección	ALTO (Rojo)	Verificar aprobación
RMSProtectionDisabled	Remoción de cifrado	CRÍTICO (Rojo intenso)	Contención inmediata (AH-B)
FileSensitivityLabelMismatch	Oversharing	ALTO (Rojo)	Notificar propietario
Accesos anómalos	Posible exfiltración	ALTO (Rojo)	Correlacionar con Entra ID
RMSGetServersideDecryptedContent	Descifrado en servidor	MEDIO ALTO (Naranja)	Verificar legitimidad

La ausencia absoluta de estos eventos también es una alarma (falla de logging)

FLUJO END-TO-END: DE LA SEÑAL A LA DECISIÓN (EJEMPLO CONSULTIVO)

PASO 1: GENERACIÓN	PASO 2: INGESTA	PASO 3: CORRELACIÓN	PASO 4: VISUALIZACIÓN	PASO 5: TRIAGE	PASO 6: ACCIÓN	PASO 7: EVIDENCIA
Usuario remueve etiqueta. Audit Log registra.)	Connector envía a Sentinel. Latencia 5-15min.)	Analytics Rule cruza con Entra ID. Genera Incidente High.)	Aparece en Workbook/Cola. Analista revisa D-03.)	Analista evalúa contexto. Clasifica Verdadero Positivo.)	Se activa AH-B: Revocación, Bloqueo, Hold. <60 min.)	Proceso documentado con timestamps y confirmación.)

@SCavanna

EL CICLO DE 24 HORAS: 10 ACTIVIDADES QUE SEPARAN A UN SOC OPERATIVO DE UN SOC DECORATIVO

— BLOQUE 04/11: EL CICLO DE 24 HORAS: 10 ACTIVIDADES DIARIAS DEL SOC

Infografía 04 de 11 · Serie: SOC Operational Excellence para Microsoft Purview Information Protection

INSIGHT DEL CORE: 60 a 90 minutos. Ese es el tiempo que separa a un SOC que controla sus datos de uno que solo cree hacerlo. Las 10 actividades diarias no son burocracia operativa — son el sistema inmunológico del programa de protección de datos.

⚠️ (Duración aproximada basada en escenarios consultivos; puede variar por entorno y nivel de automatización)

60–90 MINS
VENTANA OPERATIVA

FLUJO CONTINUO DE TELEMETRÍA 24/7

VERIFICACIÓN DE CIMIENTOS — "¿PUEDO CONFIAR EN LO QUE VEO?"

D-07 · VERIFICACIÓN DE INTEGRIDAD DE CONECTORES (Purview → Sentinel)
INPUT: Sentinel Data Connectors (M365, Defender XDR)
OUTPUT: Estado de Conectores (Connected/Degradado)

⚠ Resultados no confiables si falla D-07

D-08 · VALIDACIÓN DE CAMBIOS ADMINISTRATIVOS DEL DÍA ANTERIOR
INPUT: Audit Log (New/Set/Remove-Label/Policy)
OUTPUT: Cambios Autorizados vs. No Autorizados (Tickets)

D-07 OK → Habilita D-08

D-07 → Habilita D-08

DETECCIÓN PRIMARIA — "¿QUÉ OCURRIÓ CON LOS DATOS SENSIBLES EN LAS ÚLTIMAS 24 HORAS?"

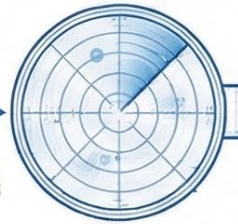
D-01 · REVISIÓN DE ALERTAS DE MICROSOFT PURVIEW

D-01 FP → Log S-01

INPUT: Purview Alerts (High → Medium → Low)
OUTPUT: Tickets (VP), Log de FP (→ S-01), Investigación (RIA)

CONSOLIDACIÓN DE DETECCIONES

D-02 · MONITOREO DEL M365 UNIFIED AUDIT LOG — EVENTOS DE INFORMATION PROTECTION

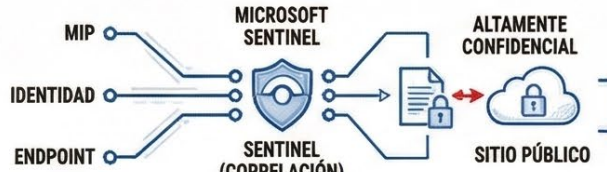


D-01 FP → Log S-01

INPUT: Audit Log (SensitivityLabelChanged, RMSProtectionDisabled, etc.)
OUTPUT: Eventos de Alto Riesgo (→ Sentinel), Baseline de Volumen

CORRELACIÓN Y CONTEXTO — "¿QUÉ HISTORIA CUENTAN LAS SEÑALES CUANDO SE CRUZAN?"

D-03 · CORRELACIÓN DE EVENTOS DE PURVIEW EN MICROSOFT SENTINEL



INPUT: Incidentes de Sentinel (Data Protection Workload)
OUTPUT: Incidentes Correlacionados (MITRE ATT&CK), Hipótesis de Amenaza

D-05 · REVISIÓN DE EVENTOS DE OVERSHARING (Teams / SharePoint)

INPUT: Audit Log (FileSensitivityLabelMismatch)
OUTPUT: Notificaciones de Remediación, Brecha de Sensibilidad

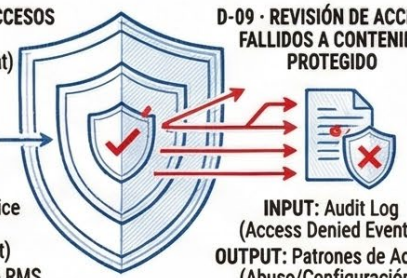
D-06 SLA Breach → Escalamiento

VALIDACIÓN DE CONTROLES ACTIVOS — "¿LOS MECANISMOS DE PROTECCIÓN SIGUEN FUNCIONANDO?"

D-04 · VALIDACIÓN DE ACCESOS A CONTENIDO CIFRADO (Azure Rights Management)

INPUT: Azure RMS Service Health, Audit Log (RMSProtect/Unprotect)
OUTPUT: Estado Operativo RMS (Activo/Degradado)

D-09 · REVISIÓN DE ACCESOS FALLIDOS A CONTENIDO PROTEGIDO



INPUT: Audit Log (Access Denied Events)
OUTPUT: Patrones de Acceso (Abuso/Configuración), Correlación (→ Entra ID)

CIERRE DE CICLO — "¿EN QUÉ ESTADO TERMINA EL DÍA?"

D-06 · SEGUIMIENTO DE INCIDENTES ABIERTOS RELACIONADOS CON DATOS

INPUT: Sistema de Ticketing (Incidentes Activos)
OUTPUT: Estado de SLA, Escalamientos (Lead/CISO)

D-10 · ACTUALIZACIÓN DEL TABLERO OPERATIVO DEL SOC

INPUT: Workbook Operativo Sentinel, Datos de D-01 a D-09
OUTPUT: Tablero RAG Consolidado, Comunicación de Cierre

OUTPUTS → CICLO SEMANAL (S-01, S-02, S-08)

NOTAS DE SOPORTE E INSIGHTS

A. LA SECUENCIA IMPORTA: No es una *checklist* plana. El orden **D-07 → D-10** es crítico para la confiabilidad.
B. 60–90 MINUTOS CON AUTOMATIZACIÓN: Tiempo estimado con automatización parcial (Sentinel Playbooks). Sin ella, se multiplica.
C. MATERIA PRIMA DEL CICLO SEMANAL: Los *outputs* diarios (FP, tendencias, correlaciones) alimentan la mejora continua semanal.
D. NIST CSF 2.0 DOMINANTE: Principalmente DETECT (DE.CM) y RESPOND (RS.CO), con elementos de GOVERN (GV.PO, GV.OC).
E. LA PREGUNTA ESENCIAL: Cada actividad responde una pregunta crítica sobre el estado de protección diario.

CONEXIONES EXTERNAS (MAPA DE SERIE)

→ Bloque 3 (Stack Tecnológico)
→ Bloque 2 (Principios Operativos)
→ Bloque 5 (Ciclo Semanal)
→ Bloque 7 (Procedimientos Ad-Hoc)
→ Bloque 8 (Métricas y KPIs)
→ Bloque 10 (Formación)
→ Bloque 9 (NIST CSF 2.0 Mapa)

@SCavanna

EL PULSO SEMANAL: 10 ACTIVIDADES QUE TRANSFORMAN DETECCIÓN EN INTELIGENCIA Y RUIDO EN PRECISIÓN

Infografía 05 de 11 · Serie: **SOC Operational Excellence para Microsoft Purview Information Protection**

INPUTS CICLO DIARIO (Log FP, Tendencias)

INPUTS:
Log FP
Tendencias
Hallazgos
Estado Conectores
Incidentes Cerrados

REFINAMIENTO DE DETECCIÓN: MENOS RUIDO, MÁS SEÑAL (S-01 + S-07)

S-01 · REVISIÓN/TUNING FALSOS POSITIVOS (PURVIEW)

Análisis de logs de FP semanales para ajustar políticas de alerta (umbral, condición) y reglas Sentinel. Validación de impacto sin reducir cobertura de riesgo real.

S-07 · AJUSTE REGLAS CORRELACIÓN (SENTINEL)

Evaluación de ratio VP/FP semanal en reglas analíticas. Ajuste de umbrales, exclusiones y cobertura MITRE ATT&CK. Priorización de nuevas reglas para brechas.

KPI (CONSULTIVO): RATIO VP MEJORADO

Insight A: Tuning semanal reduce triage diario futuro (ahorro consultivo).

SOC ESTÁTICO (SIN CICLO SEMANAL)

REPETICIÓN DE ERRORES, FATIGA, ESTANCAMIENTO. EL CICLO DIARIO DETECTA.

Sin las 10 actividades semanales, el SOC repite los mismos errores. La excelencia operacal no es hacer mejor cada nada.

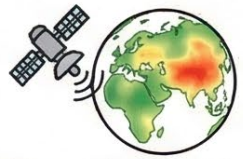
SOC EVOLUTIVO (CON CICLO SEMANAL)

APRENDIZAJE CONTINUO, PRECISIÓN, MADUREZ. EL CICLO SEMANAL APRENDE.

Sin las 10 actividades semanales, el SOC repite los mismos errores. — es hacer mejor cada semana.

INTELIGENCIA DE CLASIFICACIÓN: ¿CÓMO CAMBIAN LOS DATOS? (S-02 + S-03)

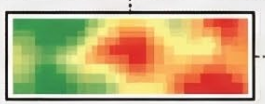
S-02 · ANÁLISIS TENDENCIAS CLASIFICACIÓN



Revisión semanal en Activity Explorer: % sin etiqueta, ratio auto/manual, top SITs, workloads con baja cobertura, downgrades. Detección temprana de degradación.

S-03 · VALIDACIÓN POLÍTICAS AUTO-LABELING

Comparación Simulación vs. Producción. Revisión de conflictos política-usuario. Identificación de nuevo contenido no cubierto. Ajuste antes de producción.



EXCHANGE (VERDE)
SHAREPOINT (ÁMBAR)
ONEDRIVE (ROJO)

OUTPUTS HACIA CICLO MENSUAL (Hallazgos, Métricas, Riesgos)

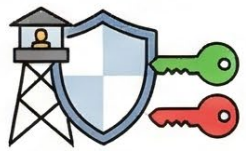
Insight C: Cero revocaciones con incidentes activos = Señal de alarma.

VALIDACIÓN EFECTIVIDAD CONTROLES: ¿FUNCIONAN LAS ARMAS? (S-04 + S-05)

S-04 · REVISIÓN EVENTOS REVOCACIÓN ACCESO

Verificación retrospectiva: ¿Cada revocación generó un bloqueo efectivo (RMSAccessDenied) en Audit Log? Fallos = incidente crítico.

S-05 · PRUEBAS ACCESO CONTROLADO (HANDS-ON)



Pruebas proactivas de acceso y usage rights en docs altamente sensibles con usuarios autorizados/no autorizados. Detección de degradación silenciosa.

KPI: % REVOCACIONES EFECTIVAS

OUTPUTS:
Hallazgos
Taxonomía
Efectividad
Revocaciones
Brechas
Logging
Riesgos
Cuentas
Reporte
Postura

Insight B: Prueba de controles detecta cambios externos (Entra ID, etc.) que degradan MIP.

CIERRE DEL CICLO SEMANAL: APRENDIZAJE Y COMUNICACIÓN (S-09 + S-10)

Insight B: Prueba de controles detecta cambios externos (Entra ID, etc.) que degradan MIP.

S-06 · REVISIÓN INCIDENTES & LECCIONES APRENDIDAS

Análisis estructurado de incidentes cerrados (causa raíz, MTTA/MTTR, efectividad). Definición de acciones de mejora (NIST CSF: RC.IM).

S-10 · REPORTE SEMANAL POSTURA SEGURIDAD DATOS

Artefacto de comunicación ejecutiva: estado RAG, métricas, incidentes, tendencias, acciones, riesgos, plan siguiente semana.

Insight D: Sesión semanal como ritual de equipo para la mejora continua.

@SCavanna

LA GOBERNANZA MENSUAL: 10 ACTIVIDADES QUE DEMUESTRAN MADUREZ ANTE CUALQUIER AUDITOR, REGULADOR O BOARD

Infografía 06 de 11 · Serie: SOC Operational Excellence para Microsoft Purview Information Protection

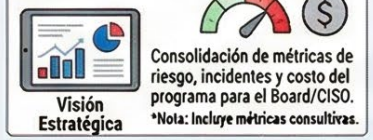
CISO · BOARD / DIRECCIÓN · AUDITORES / REGULADORES

Insight E: Los entregables mensuales como legado deben interpretarse como práctica óptima recomendada.

CONCEPTO 5: LA CÚSPIDE — REPORTE EJECUTIVO Y CUMPLIMIENTO (M-09 + M-10)

ARTEFACTOS ESTRATÉGICOS PARA AUDIENCIAS CLAVE

M-09 · REPORTE EJECUTIVO MENSUAL RIESGO DATOS



Consolidación de métricas de riesgo, incidentes y costo del programa para el Board/CISO.

*Nota: Incluye métricas consultivas.

M-10 · REVISIÓN CUMPLIMIENTO CON NIST CSF 2.0

Autoevaluación mensual del estado de madurez alineado al marco NIST CSF 2.0.

*Nota: Herramienta consultiva, no oficial Microsoft.

CONCEPTO 2: AUDITORÍA & MÉTRICAS DE EXCELENCIA (M-03 + M-04)

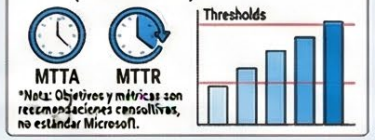
¿TENEMOS EVIDENCIA FORMAL Y CUANTIFICABLE?

M-03 · AUDITORA FORMAL AIOTOS ADMINISTRATIVO

Autoevaluación mensual del estado de madurez alineado al NIST CSF 2.0.

*Nota: Herramienta consultiva, no oficial Microsoft.

M-04 · REVISIÓN MÉTRICAS MTTA Y MTTR (CONSULTIVO)



*Nota: Objetivos y métricas son recomendaciones consultivas, no estándar Microsoft.

CONCEPTO 3: PREPARACIÓN Y RESILIENCIA (M-05 + M-06)

¿ESTAMOS LISTOS PARA EL PRÓXIMO INCIDENTE REAL?

M-05 · EJERCICIO TABLETOP: INCIDENTE FUGA DATOS

Realización mensual de escenarios de amenaza relevantes para ejercitar la respuesta del equipo.

*Nota: Recomendación consultiva.

M-06 · REVISIÓN COBERTURA IP SCANNER

Verificación del inventario de repositorios cubiertos y vigencia de credenciales del scanner local.

CONCEPTO 4: SOSTENIBILIDAD DEL PROGRAMA (M-07 + M-08)

¿ES TÉCNICAMENTE SÓLIDO Y FINANCIERAMENTE VIABLE?

M-07 · OPTIMIZACIÓN COSTOS LOGGING & RETENCIÓN

Análisis y optimización de costos entre Basic y Analytic Logs en Sentinel/M365, alineado con guías oficiales.

M-08 · VALIDACIÓN INTEGRACIÓN PURVIEW–SENTINEL–DEFENDER

Validación técnica y prueba de la correlación de eventos entre las soluciones integradas.

Insight C: El "costo por usuario protegido" es una métrica consultiva para justificar ROI interno.

Insight B: El escenario tabletop es consultivo, pero esencial para evita evitar fallos en incidentes reales.

CONCEPTO 1: GOBERNANZA TAXONOMÍA & CIFRADO (M-01 + M-02)

¿LOS FUNDAMENTOS DEL PROGRAMA SIGUEN VIGENTES?

M-01 · REVISIÓN INTEGRAL TAXONOMÍA SENSITIVITY LABELS

Revisión mensual de cambios regulatorios, de negocio y hallazgos operativos (S-02). Propuesta formal de cambios para brechas/superposiciones.

*Nota: Procedimiento consultivo recomendado.

M-02 · EVALUACIÓN EFECTIVIDAD CIFRADO PERSISTENTE

Verificación de intentos de bypass, efectividad en BYOD, usage rights y formatos no cubiertos. Informe de cobertura y anomalías.

M-03 · AUDITORÍA FORMAL CAMBIOS ADMINISTRATIVOS

Exportación y correlación mensual de eventos admin Purview con tickets de cambio aprobados. Registro firmado para auditores externos.

CONCEPTO 2: AUDITORÍA & MÉTRICAS DE EXCELENCIA (M-03 + M-04)

¿TENEMOS EVIDENCIA FORMAL Y CUANTIFICABLE?

M-03 · AUDITORÍA FORMAL CAMBIOS ADMINISTRATIVOS

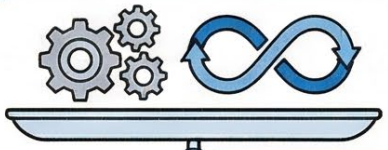
Exportación y correlación mensual de eventos admin Purview con tickets de cambio aprobados. Registro firmado para auditores externos.

M-04 · REVISIÓN MÉTRICAS MTTA Y MTTR (CONSULTIVO)

Cálculo y análisis de tiempos medios de respuesta/remediar y KPIs de cobertura/tickets.

*Nota: Objetivos y métricas son recomendaciones consultivas, no estándar Microsoft.

Insight: M-01 y M-02 validan que "sabemos qué proteger" y que "la protección funciona" simultáneamente.



GOBERNAR ES HACER VISIBLE LO INVISIBLE.

Insight Core: Sin gobernanza mensual, la excelencia operativa es un "platillo vacío" ante el Board y auditores. Se requiere tanto hacer como demostrar.

OPERACIÓN TÉCNICA (CICLOS DIARIO/SEMANAL)
FUNCIONALIDAD INVISIBLE.
El ciclo diario protege. El ciclo semanal optimiza.

ARTEFACTOS DE GOBERNANZA (CICLO MENSUAL)
EVIDENCIA DEMOSTRABLE
El ciclo mensual demuestra madurez.

@SCavanna

CUANDO LA ALARMA SUENA: 5 PROCEDIMIENTOS DE RESPUESTA QUE SEPARAN LA CONTENCIÓN DEL CAOS

Infografía 07 de 11 · Serie: SOC Operational Excellence para Microsoft Purview Information Protection

T=0 TRIGGER

T+15m Triage

T+1h Contención (AH-B)

T+4h Forense Preliminar

T+24h Com. Ejecutiva

T+72h Notificación Legal/Post-Mortem

TRIGGER: ALERTA HIGH/CRITICAL O INCIDENTE SENTINEL

TIEMPO TRANSCURRIDO: 00:00:00

EL COSTO DE LA DEMORA ES EXPONENCIAL

CORE INSIGHT: Un incidente de datos no espera. Estos 5 procedimientos no son guías, son **ALGORITMOS DE DECISIÓN** pre-diseñados. La diferencia entre contención y caos es la ejecución ensayada de este flujo.

AH-A: INVESTIGACIÓN DE ALERTA CRÍTICA (TRIAGE & CONTEXTO)

AUDIT LOG · ENTRA ID · DEFENDER · SENTINEL

Fase 1: Triage (0-15m)
Fase 2: Contexto (15-30m)
Fase 3: Alcance (30-60m)

¿VP CONFIRMADO?

NO (Falso Positivo/RIA) → DOCUMENTAR FP & TUNING SEMANAL (Bloque 5) → Bloque 5 (Tuning)

SÍ (Incidente Real)

AH-B: CONTENCIÓN INMEDIATA (CORTAR LA HEMORRAGIA)

PRINCIPIO: LA CONTENCIÓN NO ESPERA AL DIAGNÓSTICO.
Ventana Recomendada: < 1 Hora

- **REVOCAR ACCESO** (Purview/RMS)
- **BLOQUEAR CUENTA** (Entra ID)
- **PRESERVAR EVIDENCIA** (Audit/Sentinel Hold)
- **NOTIFICACIÓN INICIAL** (CISO/Legal)

Bloque 3 (Stack)

Insight C: La ejecución de AH-B define la cultura del SOC. 'Contener primero' es una mentalidad de protección activa.

AH-C: ANÁLISIS FORENSE (RECONSTRUIR LA HISTORIA)

Metódico y Exhaustivo. Sin ventana fija.
Herramientas: eDiscovery, Audit Log Extendido, Sentinel Correlación.
Output: Informe Forense Complete & Cadena de Custodia.

¿DATOS REGULADOS INVOLUCRADOS?

NO

SÍ (GDPR, CCPA, etc.)

AH-D: ESCALAMIENTO LEGAL Y COMPLIANCE (EL PUENTE TÉCNICO-JURÍDICO)

Coordinación con Legal/DPO.
Clasificación Regulatoria.
Activación Notificación (Plazos Estrictos, ej. 72h). **Hold Legal.**

Bloques 4, 5, 6 (Mejora Continua)

AH-C: ANÁLISIS FORENSE (RECONSTRUIR LA HISTORIA)

Insight B: La ventana de 72h (ej. GDPR) es una restricción de diseño crítica para organizar la respuesta.

¿EXFILTRACIÓN CONFIRMADA O POTENCIAL LEGAL?

NO (Alcance Limitado) → CIERRE INTERNO & DOCUMENTACIÓN

SÍ (Impacto Mayor)

NO

AH-E: COMUNICACIÓN EJECUTIVA Y POST-MORTEM (CERRAR EL CICLO)

COMUNICACIÓN EJECUTIVA (24h Recomendada)
Narrativa de 6 Puntos para el Board

POST-MORTEM (72h Recomendada)
Causa Raíz, Acciones Correctivas, Feedback al Modelo

Bloque 9 (NIST CSF)

Insight E: El post-mortem no es un trámite, es el mecanismo que fortalece el sistema para el próximo incidente.

⚠ **NOTA CONSULTIVA:**
Ventanas temporales basadas en mejores prácticas de industria, no son un estándar oficial de Microsoft. Adaptar al contexto organizacional.

@SCavanna

EL TABLERO DE CONTROL: 11 KPIs QUE MIDEN EXCELENCIA Y 6 SEÑALES QUE ANTICIPAN EL FRACASO

Infografía 08 de 11 · Serie: SOC Operational Excellence para Microsoft Purview Information Protection

NOTA IMPORTANTE: El modelo presentado (KPIs, señales, umbrales, benchmarks) constituye una **PROPUESTA CONSULTIVA** basada en buenas prácticas de industria (ej. NIST CSF), **NO** es un estándar oficial emitido por Microsoft para Purview, Sentinel, Azure RMS o Defender for Office 365.

HORIZONTE PRESENTE: TABLERO DE 11 KPIs PRIMARIOS (¿CÓMO ESTAMOS HOY?)

Miden la excelencia operacional. Reporte a stakeholders.

CONCEPTO 1: VELOCIDAD (DETECCIÓN Y CONTENCIÓN)

MTTA — CRITICAL
Target: <1h Consultivo
Actual: 45m
Mejorando

MTTA — HIGH
Target: <4h Consultivo
Actual: 3h 10m
Estable

MTTR — CRITICAL
Target: <4h Consultivo
Actual: 2h 30m
Mejorando

MTTR — HIGH
Target: <8h Consultivo
Actual: 6h 45m
Degradando

Tendencia 3 meses es más robusta que valor puntual. Benchmarks consultivos.

Insight A: Segmentar KPIs por audiencia es práctica recomendada, no norma Microsoft.

Insight C: El Anti-KPI. Evitar incentivos perversos midiendo lo incorrecto.

CONCEPTO 2: COBERTURA Y CALIDAD (PROTECCIÓN Y PRECISIÓN)

COBERTURA CLASIFICACIÓN

E3 Target >70%
E5 Target >85% (Ref. Consultiva)
Tamaño del escudo. % docs clasificados.

RATIO VERDADEROS POSITIVOS (VP)

>70% Saludable (Ref. Consultiva)
Precisión del radar. % alertas reales.

INCIDENTES CONTENIDOS SIN PÉRDIDA

>95% Objetivo (Ref. Consultiva)
Última línea que aguanta. Cifrado persistente efectivo.

CORE INSIGHT: Un SOC que solo tiene KPIs REACCIONA. Un SOC que también tiene señales PREVIENE.

CONCEPTO 3: GOBERNANZA Y CONTINUIDAD

CAMBIOS ADMIN APROBADOS 100%
100% (Recomendado cumplimiento)

UPTIME CONECTORES 99.8%
>99.5% (Ref. Consultiva)

TENDENCIA AUTO-LABELING
Tendencia Positiva

CONCEPTO 4 (PARTE 1): FORMACIÓN

EQUIPO CON FORMACIÓN COMPLETADA 92%
>90% (Ref. Consultiva)

CONCEPTO 5: LECTURA INTEGRADA Y DIAGNÓSTICO (PATRONES CONSULTIVOS)

SOC RÁPIDO PERO CIEGO (Buen MTTA, Mala Cobertura)
SOC EXHAUSTO (Buen VP, MTTR Degradado)
SOC MADURO (KPIs Estables, Sin Señales Activas)

Insight D: Frecuencia de revisión (Diaria/Semanal/Mensual) refleja criticidad consultiva.

HORIZONTE FUTURO: SISTEMA DE ALERTA TEMPRANA (6 SEÑALES) (¿QUÉ ESTÁ POR FALLAR?)

Anticipan problemas antes de incidentes. Monitoreo proactivo.

SEÑAL 1: CAÍDA COBERTURA CLASIFICACIÓN
→ Caída > 5% vs mes anterior — Umbral Orientativo

SEÑAL 2: AUMENTO ABRUPTO DE FALSOS POSITIVOS
→ Aumento > 10% en ratio FP — Umbral Orientativo

SEÑAL 3: CAÍDA VOLUMEN AUDIT LOG
→ Desviación negativa significativa vs línea base — Umbral Orientativo

Insight B: La señal más peligrosa. Infiere confiabilidad de todo el resto. (Ref. Consultiva)

SEÑAL 4: CRECIMIENTO SOSTENIDO MTTA
→ Tendencia negativa 3 meses consecutivos

SEÑAL 5: RECURRENCIA INCIDENTES TIPO
→ Mismo vector/actor repetido sin mitigación raíz

SEÑAL 6: CERO REVOCACIONES CON INCIDENTES ACTIVOS
→ Inactividad en respuesta técnica crítica

Insight E: Conexión Financiera. Cálculo de ROI basado en KPIs históricos es metodológico/consultivo.

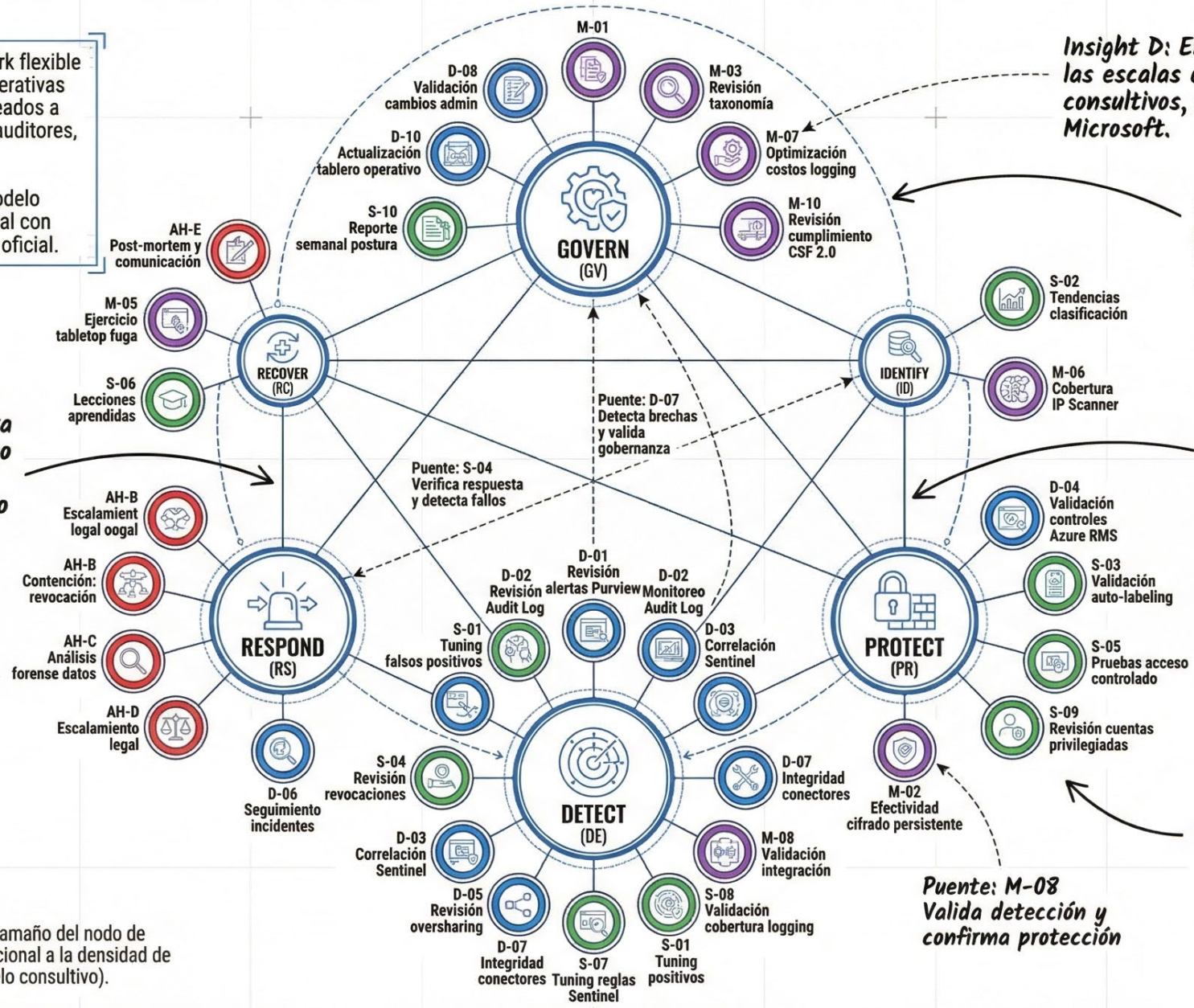
@SCavanna

EL MAPA NORMATIVO: 35 ACTIVIDADES ALINEADAS A NIST CSF 2.0 — DE LA OPERACIÓN TÉCNICA AL LENGUAJE UNIVERSAL DE CIBERSEGURIDAD

Infografía 09 de 11 · Serie: SOC Operational Excellence para Microsoft Purview Information Protection

Core Insight: NIST CSF 2.0 es un framework flexible que apoya la traducción de actividades operativas del SOC en términos comprensibles y alineados a estándares reconocidos por reguladores, auditores, aseguradoras y boards.

Subtexto estratégico: Este mapa es un modelo consultivo para alinear lenguaje operacional con comunicación estratégica, no un estándar oficial.



Insight D: El Scorecard M-10 y las escalas de madurez son consultivos, no estándar Microsoft.

Concepto 1: GOVERN envuelve y contextualiza todas las funciones (según NIST CSF 2.0 cambios).

Insight A: Perfil de Cobertura Consultivo. La distribución no uniforme es la firma del modelo (DETECT es el núcleo operativo).

Insight B: Actividades Puente. Conectan funciones primarias con secundarias, revelando interdependencias.

Insight C: Ausencia Intencional. Áreas como ID.RA, PR.AT, RC.RP no se cubren en profundidad en este modelo operativo consultivo.

Puente: M-08 Valida detección y confirma protección

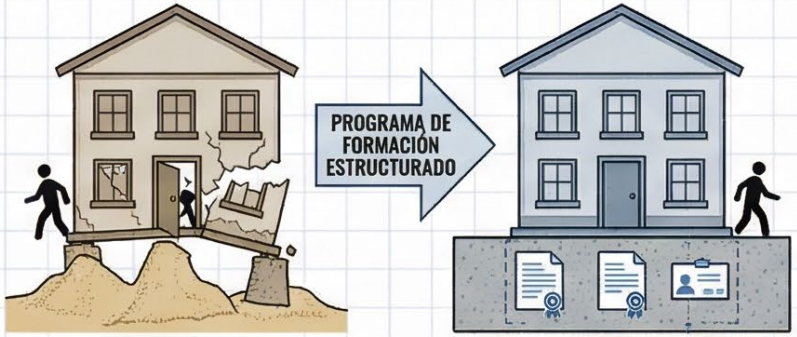
LEYENDA CADENCIA (NÚCLEO):
- DIARIA (AZUL)
- SEMANAL (VERDE)
- MENSUAL (MORADO)
- AD-HOC (ROJO)

NOTA TÉCNICA: El tamaño del nodo de función es proporcional a la densidad de actividades (modelo consultivo).

@SCavanna

DE JUNIOR A LEAD: EL PROGRAMA DE FORMACIÓN QUE TRANSFORMA CONOCIMIENTO TRIBAL EN COMPETENCIA VERIFICABLE Y AUDITABLE

Infografía 10 de 11 · Serie: SOC Operational Excellence para Microsoft Purview Information Protection



CONOCIMIENTO TRIBAL
(Frágil, No Escalable)
Depende de personas clave.
Si se van, la operación cae.

COMPETENCIA INSTITUCIONAL
(Resiliente, Auditable)
La competencia está en el sistema y la evidencia.

CORE INSIGHT: El modelo operativo es inútil sin competencia verificable. Este programa es el prerrequisito del modelo, transformando fragilidad tribal en resiliencia institucional.

NIVEL 1 — ANALISTA JUNIOR: LOS FUNDAMENTOS (Semanas 1–4)

Focus: Comprender fundamentos y ejecución básica bajo supervisión.
Ser los "ojos" del SOC.

1. SC-900 Certificación (6-8h)
2. Docs: Sensitivity Labels (2h)
3. Docs: Audit Log Activities (2h)
4. Video: Mechanics MIP (30m)
5. Docs: Teams/Groups Labels (1.5h)
6. Docs: RMS Usage Rights (1.5h)

~15h Inversión

HABILITA: COMPETENCIA BÁSICA SUPERVISADA

6-8h · 6-8h · 30m · 2h · 1.5h · 1.5h

D-01 · D-02 · D-05 · D-06 · D-09

Transcripción SC-900, Badges MS Learn

MODO: Supervisión Directa

NIVEL 2 — ANALISTA MID-LEVEL: OPERACIÓN AUTÓNOMA (Meses 2–6)

Focus: Transición crítica: de "ojos" a "cerebro + manos".
Interpretación, correlación y acción autónoma.

1. Docs: Azure RMS (3h)
2. Docs: Sentinel Ops Guide (4h)
3. Docs: Auto-labeling (2h)
4. Docs: Search Audit Log (2h)
5. Docs: Best Practices Sentinel (2h)
6. Video: Sentinel Deep Dive (1h)
7. Blog: Compliance Alerts (45m)

~16h Inversión

HABILITA: OPERACIÓN AUTÓNOMA RUTINARIA

3h · 4h · 2h · 2h · 2h · 2h

TODAS Actividades D (10) y S (10)

Participación Supervisada AH-A, AH-B

MODO: Autonomía Operativa

Sentinel Ninja (Community Route - Niveles), Registro Interno, 2x Tabletops

NIVEL 3 — ANALISTA SENIOR / LEAD SOC: LIDERAZGO OPERATIVO (Mes 6+)

Focus: Visión estratégica, gobierno del modelo, comunicación ejecutiva y respuesta compleja.

1. Sentinel Ninja Training (Community Route, Expert) (8-10h)
2. Docs: SOC Optimization (2h)
3. Docs: Deploy IP Scanner (3h)
4. CISA Expanded Cloud Logs Playbook (2h)
5. Docs: Purview Overview (2h)
6. Blog: Audit M365 (45m)

~19h Inversión

Liderazgo TODAS D, S, M, AH

HABILITA: LIDERAZGO Y GOBIERNO TOTAL

M-09 Reportes Ejecutivos

M-05 Liderazgo Tabletop

AH-D Escalamiento Legal

Mapeo Consultivo NIST CSF 2.0

8-10h · 5h

Evidencia generada: Sentinel Ninja Expert (Community), Certificados Liderazgo Tabletop, Reportes Formales

Liderazgo Estratégico y Respuesta Ad-Hoc Completa

Operación Autónoma Rutinaria (Ciclo D+S)

Ejecución Básica Supervisada

CAPACIDAD OPERATIVA HABILITADA (Incremento Progresivo)

ECOSISTEMA DE EVIDENCIA Y NOTAS TÉCNICAS

PORTAFOLIO DE EVIDENCIA AUDITABLE (SOC2 / Reguladores)

- Transcripción SC-900 (Oficial)
- Badges MS Learn (Verificable)
- Sentinel Ninja Community Route (Reconocimiento)
- Registro Interno de Formación
- Actas de Tabletop Firmadas

Insight A: Inversión Real. ~50 horas totales distribuidas en 6 meses transforman un analista junior en un Lead competente.

Insight B: Recurso Pivotal. Sentinel Ninja Training (Community Route) es crítico para el dominio de correlación, aunque no es certificación formal Microsoft.

Insight D: Anti-Patrón. La formación exitosa mapea a actividades operativas concretas, no a cursos genéricos de ciberseguridad.

Insight E: Indicador de Madurez (Consultivo). La progresión de niveles del equipo sirve como KPI de madurez del programa.

@SCavanna

DE CERO A EXCELENCIA: EL ROADMAP CONSULTIVO DE 4 FASES PARA TRANSFORMAR UN PROGRAMA DE PROTECCIÓN DE DATOS EN UNA CAPACIDAD ORGANIZACIONAL DEMOSTRABLE

Infografía 11 de 11 · Serie: SOC Operational Excellence para Microsoft Purview Information Protection

Core Insight: El modelo no se implementa de golpe — se construye en capas. Cada fase genera valor propio y demostrable antes de avanzar a la siguiente. Una organización que completa solo la Fase 1 ya tiene capacidad de detección básica operativa. Una que completa la Fase 2 puede sostener una auditoría interna. Una que completa la Fase 3 está en posición de responder ante auditorías externas o reguladores. La Fase 4 es la optimización continua de un programa ya maduro. El error más común no es ir lento — es intentar implementar todo simultáneamente y no terminar nada.

⚠ Aclaración: El carácter secuencial y acumulativo es una recomendación consultiva, no una limitación técnica impuesta por Microsoft ni existe documentación oficial que prohíba la ejecución de fases en paralelo. La secuencia es práctica recomendada.

Insight A: Escalabilidad Estructural. La arquitectura permite crecimiento, pero el diseño debe respetar límites y recomendaciones (Sentinel architecture).

Insight B: Error común: Saltar faces sin estabilizar la anterior. No avanzar a reportes ejecutivos sin un ciclo operativo estable.

Insight C: Sincronía Formación–Implementación. El retraso en formación impacta directamente la calidad de ejecución en cada face.

Insight D: Valor financiero acumulativo. Cada fase completada reduce riesgo y evita costos, aunque el ROI oficial no se publica.

Insight E: Modelo como activo organizacional transferible. La documentación y operación institucionalizada facilitan auditorías y due diligence.

NIVEL 1: Formación Base (SC-900)

NIVEL 2: Operación & Lead Nivel 3 (Consultivo)

NIVEL 3: Lead & Especialización

Formación Continua & Certificaciones Avanzadas

Fundamentos (Semanas 1–4)

Construir la Base sin la Cual Nada Funciona

En Construcción

- ON D-01 Revisión Alertas Purview
- ON Monitoreo Audit Log
- ON Correlación Sentinel
- ON Validación Azure RMS
- ON Detección Oversharing

Taxonomía Aprobada v1.0

5 actividades operativas clave

Nivel 1 Completado

Operación Estable (Meses 2–3)

El SOC Opera, No Solo Observa

- ON D-01 Revisión Alertas Purview
- ON Monitoreo Audit Log
- ON Validación Cambios
- ON Acceso Fallido
- ON Tablero Operativo
- ON Seguimiento Formal
- ON Revisión Conectores
- ON Validación Cambios
- ON Acceso Fallido
- ON Tablero Operativo

Primer Reporte Semanal de Postura (RAG)

Actividades recurrentes consultivas, alineadas a ciclo operativo

Nivel 2 Completado

Nivel 3 Lead en Progreso

Madurez Completa (Meses 4–6)

Demostrable ante Evaluadores Externos

- ON D-01 Revisión Alertas Purview
- ON Monitoreo Audit Log
- ON Ciclo Mensual de Gobernanza
- ON Procedimientos Ad-hoc Documentados
- ON Reporte Ejecutivo on Manual)
- ON Ejercicios Tabletop
- ON Reporte Ejecutivo con Métricas
- ON Scorecard CSF Consultivo (Manual)
- ON Auditoría de Cambios
- ON Revisión MTTA/MTTR

Scorecard CSF Consultivo

Reporte Ejecutivo

Auditoría Mensual

Ciclo completo y evidencia consultiva de madurez

Nivel 3 — Lead SOC Completado

Optimización Continua (Mes 7 en Adelante)

Mejora Permanente

Eje 1: Ajuste Continuo KPIs (Comparativo Consultivo)

Eje 2: Expansión Cobertura (PBI, Copilot, Multi-Cloud)

Eje 3: Contribución Corporativa (Integración SOC/Entra ID)

CSF

Optimizing (Consultivo, no oficial)

Escelencia Operacional Demostrable

La excelencia es una dirección, no un destino. Optimización y Expansión Continua.

AUDIENCIAS OBJETIVO: AUDITOR INTERNO, REGULADOR, ASEGURADORA, BOARD

PRERREQUISITOS TÉCNICOS

- M365 E5 (Recomendado)
- Sentinel + Conectores
- Audit Premium (Sugerido)
- Taxonomía Aprobada (CRÍTICO)
- Workbooks Básicos
- Workbooks Completos
- Gestión Incidentes Integrada
- Audit Premium (Necesario para forense)
- Evaluación Nuevas Capacidades

Insight E: Modelo como activo organizacional transferible. La documentación y operación institucionalizada facilitan auditorías y due diligence.

LEYENDA DE ESTADO: ☐ PENDIENTE / ☑ ACTIVO (FASE COMPLETADA) / ⏩ EN PROGRESO / ○ OPTIMIZACIÓN CONTINUA

@SCavanna