DOC ID: EN6-8P-SOC-001

REV 1.0 - DATE: 2024-05-20

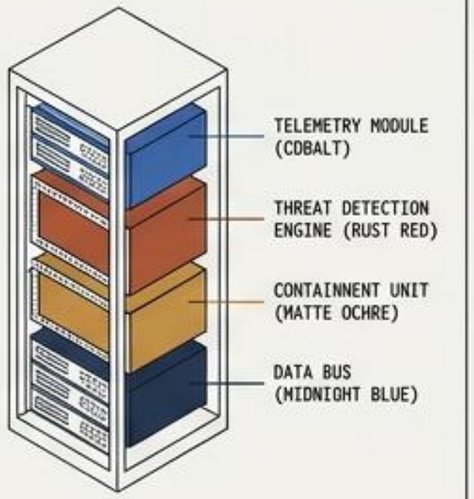
X-AXIS: 125.58mm

Y-AXIS: 66.30mm

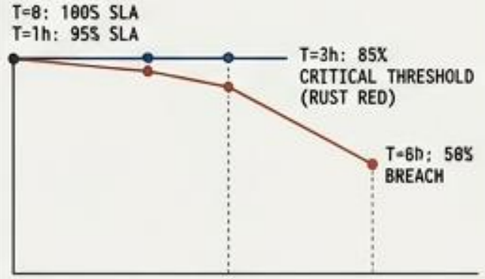
3 HORAS PARA DETECTAR

Rediseñando la arquitectura del SOC mediante SLAs estrictos y telemetría de precisión.

De la narrativa retrospectiva del Dwell Time a la disciplina de la ingeniería en la respuesta a incidentes.



SLA CONPLIANCE METRICS



SPECIFICATION OVERVIEW

ARCH: ISONETRIC NETWORK GRID
GRID: 5mm PITCH GRAPHITE
COLOR: DEEP GRAPHITE/NIDNIGHT BLUE/COBALT/OCHRE/RUST
TYPEFACE: GEOMETRIC SANS / TABULAR MONOSPACE

SYSTEM STATUS LOG

00:00:00: STARTUP SEQUENCE INITIATED > OK
00:05:32: NETNORK SCANNING ACTIVE (COBALT) > OK
01:15:20: ANONALY DETECTED (RUST RED) > PENDING
03:00:01: DETECTION NINDON CLOSED > CRITICAL

DOC ID: EN6-8P-SOC-001

Mg. Ing. Sebastián Vargas

Liderazgo Estratégico, Maestría Técnica y Formación Académica en Ciberseguridad IT/OT

[CEO TTPSEC] [vCISO LATAM] [+18 Años Experiencia]

+18 Años

Experiencia en Ciberseguridad IT/OT/ICS

10 Roles

De Liderazgo Ejecutivo e Institucional

5 Sectores

De Infraestructura Crítica Protegidos

4 Ingenierías

Informática y Ciberseguridad

13 Grados

10 Másteres Titulados + 3 Doctorados en curso

94+

Credenciales y Certificaciones Técnicas Internacionales

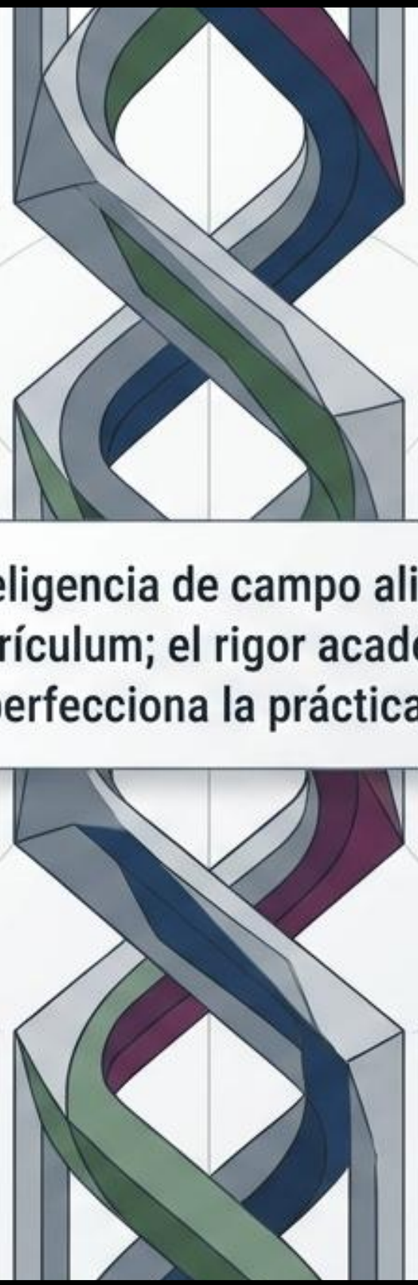
El Consultor Ejecutivo (Práctica)

Roles:

CEO TTPSEC, vCISO,
Ex-Jefe CSIRT.

Capacidades:

CISO as a Service,
Arquitectura Segura Cloud,
Protección OT/ICS,
Auditorías CIS/ISO 27001.



La inteligencia de campo alimenta el currículum; el rigor académico perfecciona la práctica.

El Director Académico (Teoría)

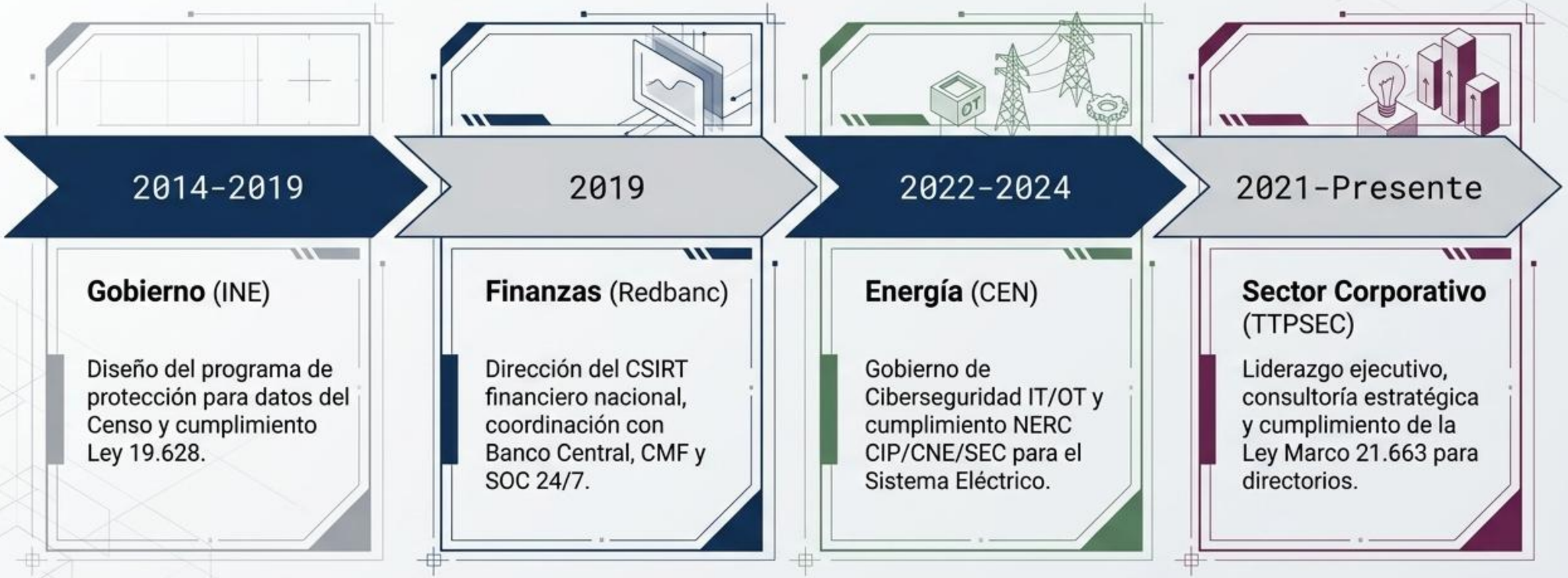
Roles:

Profesor de Posgrado
(U. de Chile, PUC),
Director Académico
(USACH, 8dot8).

Capacidades:

Creador de Diplomados
(Blue/Purple Team),
Especialista en
Ciberinteligencia y
Ransomware.

Evolución Estratégica en Infraestructura Crítica Nacional



Mapa de Cobertura Sectorial y Normativa

Energía & Utilities

[NERC CIP] [CNE] [SEC]

[Ciberseguridad OT/ICS]

Banca & Finanzas

[CMF] [BCCh] [Monitoreo SOC 24/7]

[Fintech & Blockchain]

Sector Público

[Ley Marco 21.663] [Ley 19.628]

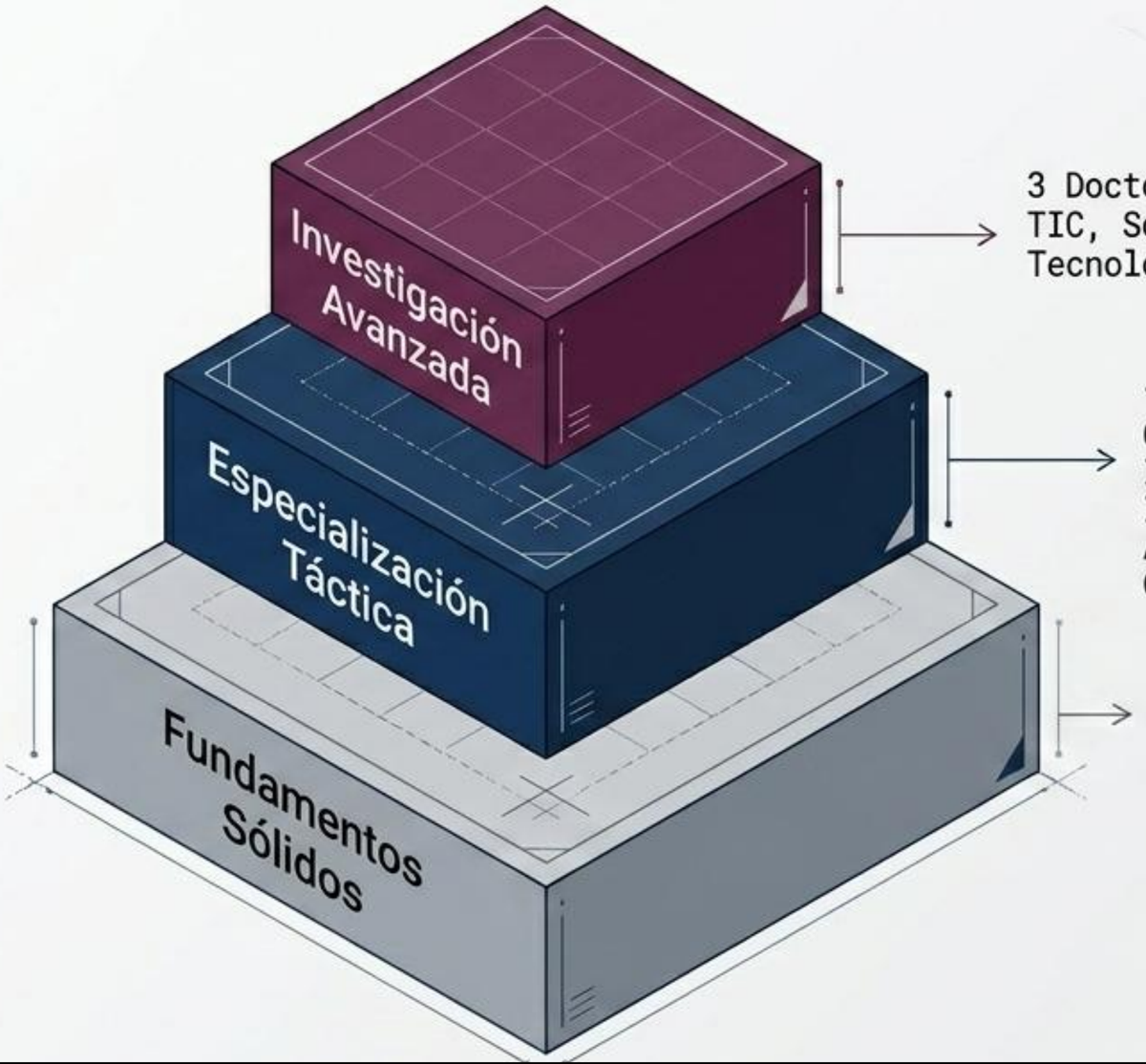
[Políticas Gubernamentales]

Minería e Industria

[Redes IIoT] [Automatismos Industriales]

[CCI Black Level]

Arquitectura Académica



3 Doctorados en curso: TIC, Socioformación, Tecnología Educativa.

10 Másteres y Magísteres: Ciberseguridad y Ciberguerra, IA, Ciberseguridad Industrial, Robótica, Automatismos Industriales, Gestión TI, MBA, Fintech.

4 Títulos de Ingeniería (Ciberseguridad, Civil en Informática, Informática, Licenciatura). Nota 6.9, Mejor Alumno.

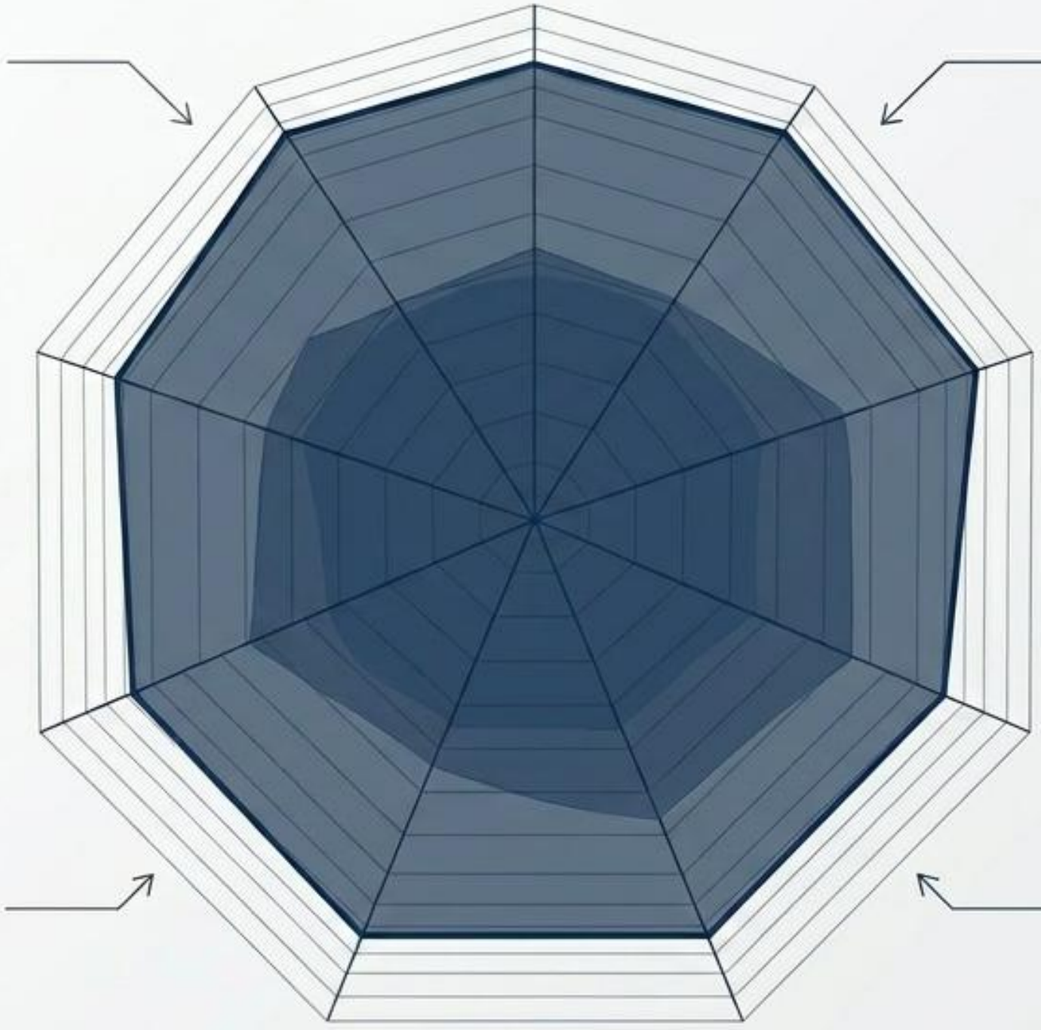
Radar de Capacidades Técnicas Especializadas (94+ Credenciales)

Threat-Informed Defense

32 AttackIQ, 25 MITRE Engenuity (MAD20), 4 eLearnSecurity.

Gobernanza y Riesgo

EC-Council C|CISO, 4 ISO Standards (Auditor Líder 27001/42001), Secure Controls Framework.



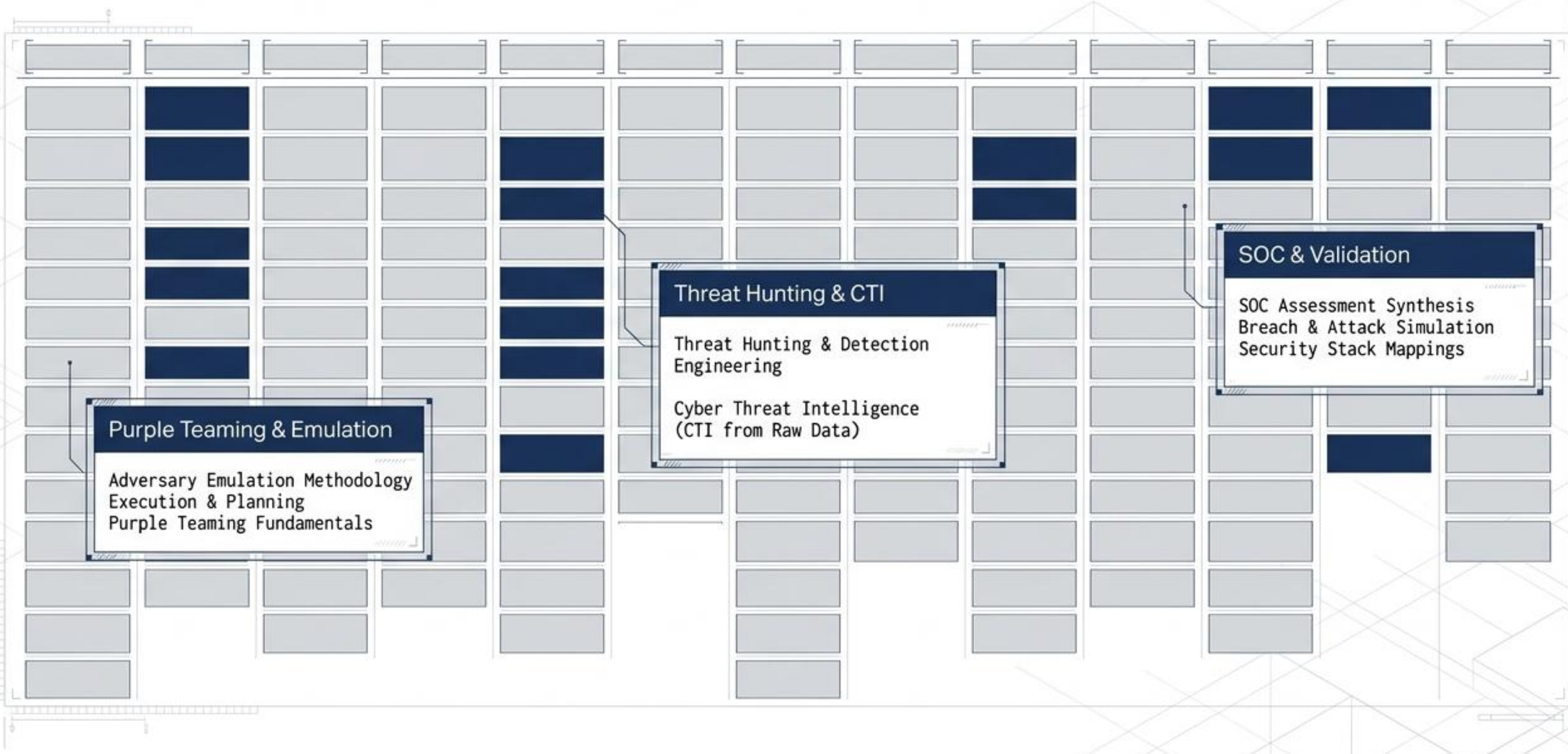
Cloud & Zero Trust

Cloud Security Alliance (CCSK, CCZT), AWS, Google Cloud, Cisco.

IA e Innovación

18 Anthropic Certifications, Certiprof AI Expert, IBM Deep Learning.

Dominio Táctico: El Ecosistema MITRE ATT&CK & AttackIQ



La Frontera: Inteligencia Artificial y Automatización

Fundamentos Académicos

Máster en Inteligencia Artificial (CEUPE).

Maestría en Robótica (ESNECA - Sobresaliente).

Maestría en Automatismos Industriales.

Implementación y Seguridad

18 Certificaciones Anthropic (Claude Code 101, Model Context Protocol, Building with API).

Cloud Security Alliance Trusted AI Safety Expert (TAISE).

ISO/IEC 42001 Internal Auditor (Gestión de Sistemas de IA).

Impacto Académico y Formación de Talentos

Perú

USIL (Programa Defensiva/Ofensiva),
UCV (Especialización Hacking Ético).

Bolivia

UCB (Diplomado Forense Digital, Pentesting OT/IoT).

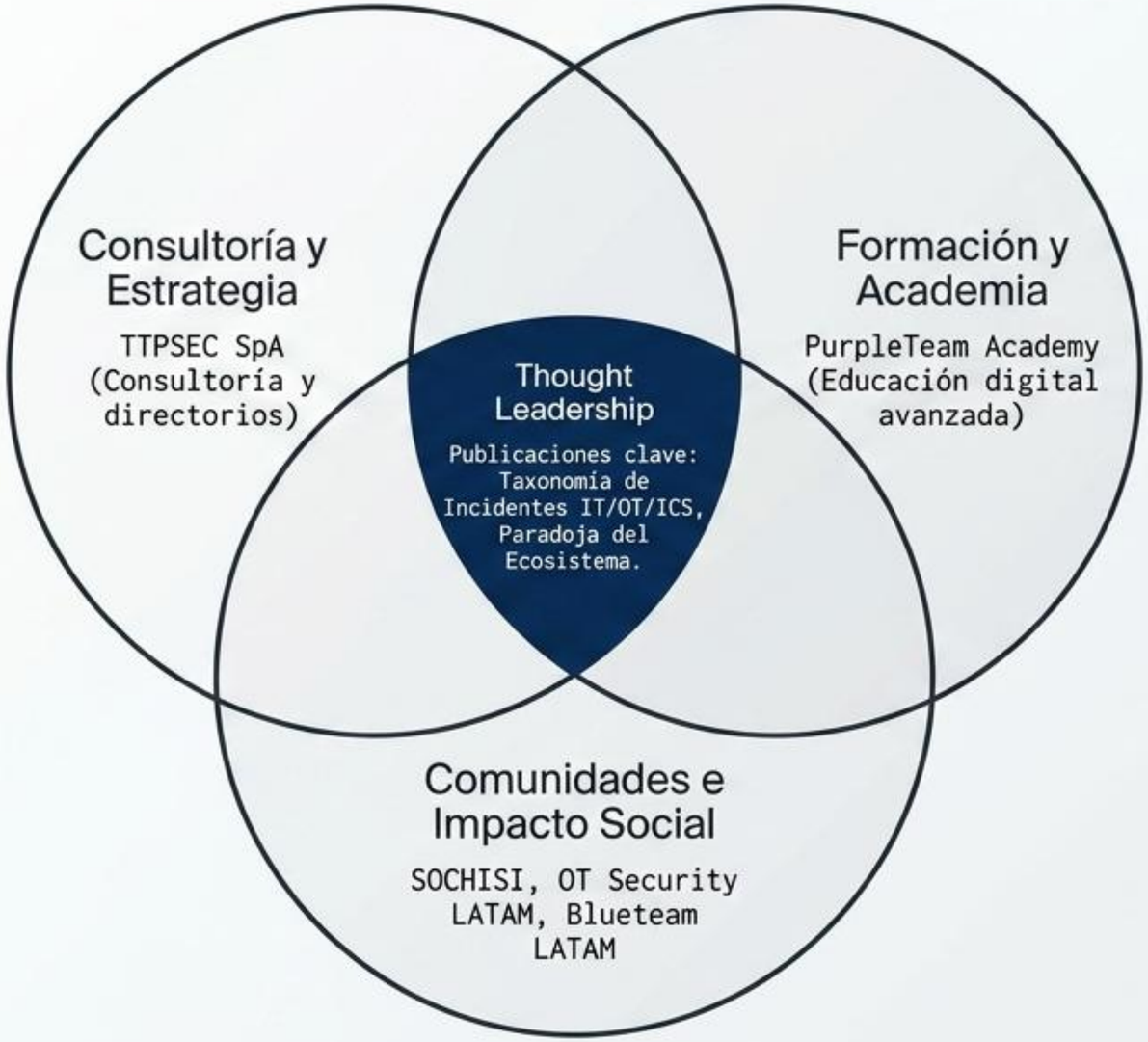
Chile

U. de Chile (Profesor Posgrado),
PUC (Creador Diplomado Ethical Hacking),
USACH (Ex-Director Académico).

Ecosistema Digital

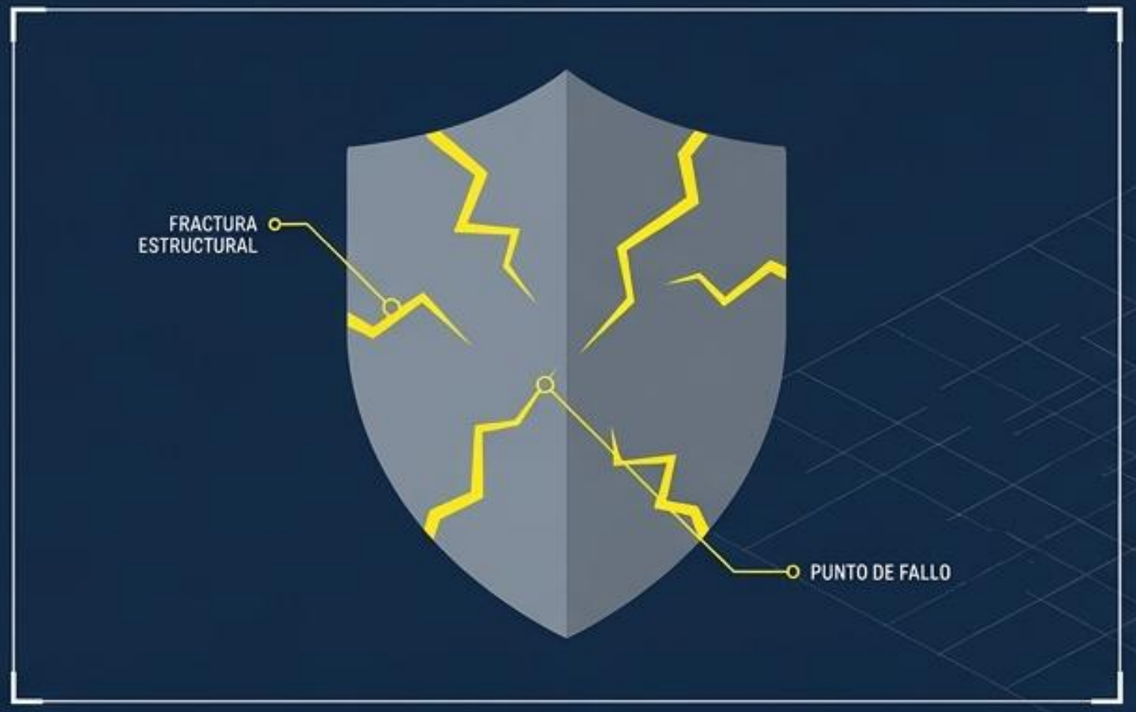
8dot8 Academy (Director Académico),
PurpleTeam Academy (Gerente General).

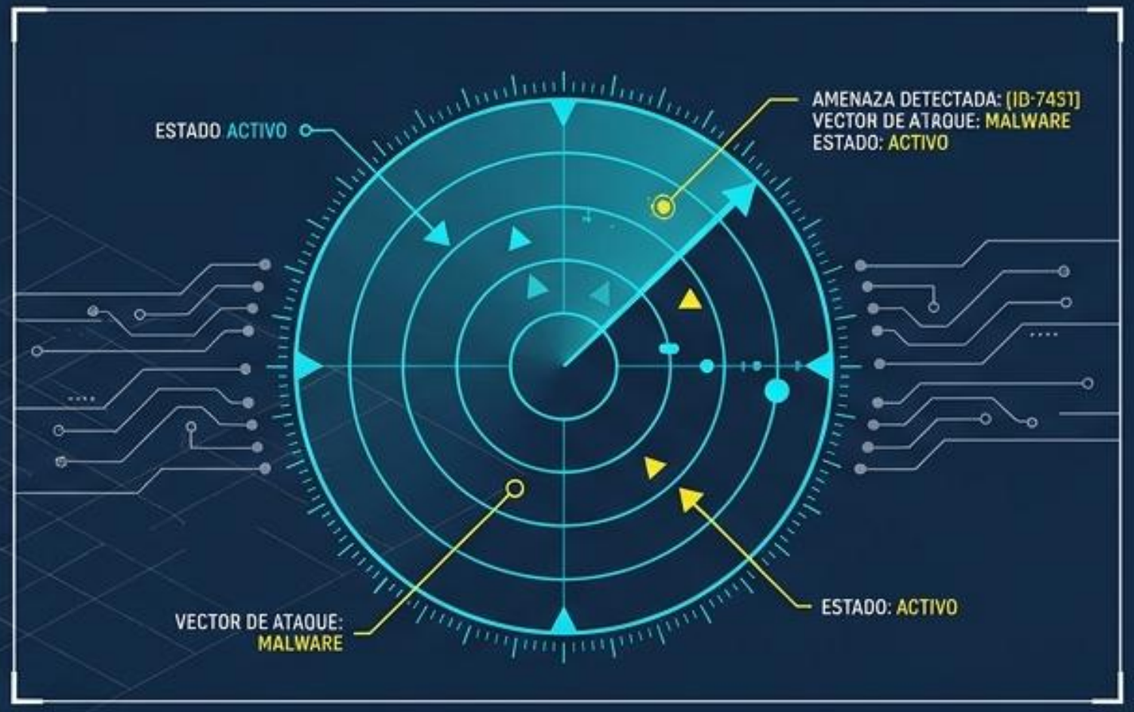
El Multiplicador: Comunidades y Ecosistema



EL PARADIGMA DE LA INEVITABILIDAD

SYSTEM STATUS: ONLINE
NETWORK LOAD: 52%
LAST UPDATE: 2024-10-27 14:35:22





Las políticas de seguridad y los controles por sí solos no garantizan la protección total. Siempre existirán vulnerabilidades residuales.

Las amenazas no identificadas previamente causarán incidentes. La falta de preparación hace que cualquier respuesta sea menos efectiva y aumenta el impacto adverso en el negocio.

FASE: PREPARACIÓN

La preparación estructurada no es opcional; es el único mecanismo para minimizar la disrupción y prevenir catástrofes operativas.

FASE: PREPARACIÓN

ESTADO: CRÍTICO
TIEMPO DE RESPUESTA: 00:00:00
ANÁLISIS: EN CURSO

Diagnóstico: Evento vs. Incidente

	Evento de Seguridad de la Información	Incidente de Seguridad de la Información
Definición	Anomalías técnicas, fallos de sistemas o errores humanos.	Uno o múltiples eventos que tienen una probabilidad significativa de comprometer las operaciones del negocio.
Implicación	Su ocurrencia no significa necesariamente que un ataque haya sido exitoso o que existan consecuencias para el negocio.	Amenaza directa a la confidencialidad, integridad o disponibilidad.
Naturaleza	Puede ser eliminado, ignorado o registrado para análisis.	Requiere activación inmediata de protocolos de respuesta, mitigación y recuperación.

No todos los eventos se convierten en incidentes, pero todos los incidentes comienzan como eventos.

La Anatomía de un Incidente

Las amenazas explotan debilidades tecnológicas, organizacionales o físicas, transformando un riesgo teórico en una disrupción operativa real.

Beneficios de un Enfoque Estructurado

Mejora de Seguridad General

Identificación rápida y resoluciones consistentes.

Reducción de Impacto

42% ↗
17% ↘

Minimiza pérdidas financieras y daño reputacional.

Prevención Proactiva

Identifica patrones y tendencias para defensas futuras.

Priorización Efectiva

Priority
LOW
MED
HIGH
CRITICAL

Escala incidentes basada en impacto, no en reactividad.

Admisibilidad de Evidencia

Timestamp Pol → Checksum → Chain of Custody
Chain of Custody
Timestamp 223 ← Checksum 301 ← Checksum

Recolección legalmente válida para acciones disciplinarias.

Justificación de Presupuesto

Resource Allocation
BDI Tracking

Rastreo de recursos y tiempos para optimizar la inversión en el SOC.

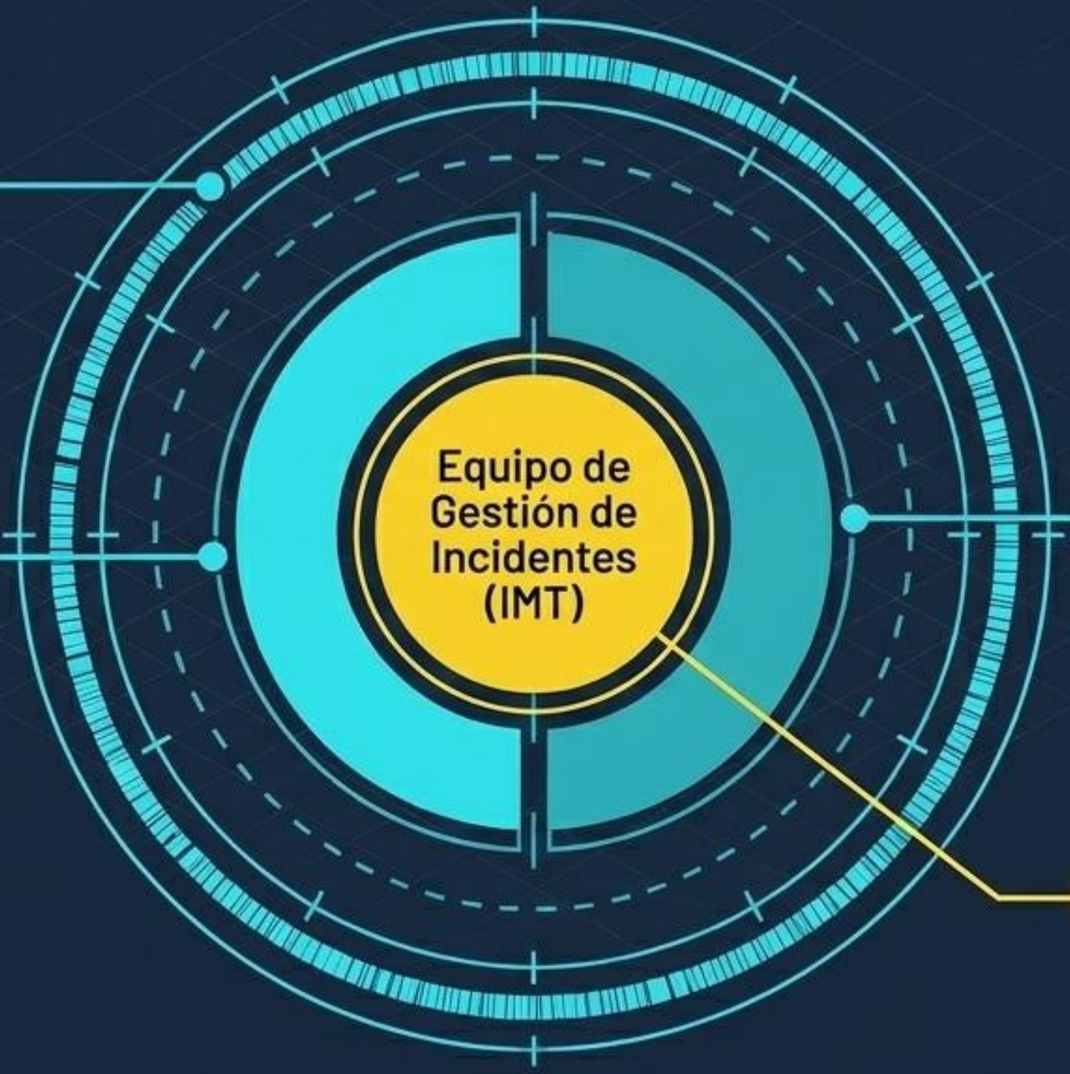
Arquitectura del Equipo de Respuesta

Punto de Contacto (PoC)

El primer eslabón. Recibe alertas y anomalías iniciales (sistemas o individuos).

Coordinador del Incidente

Evalúa eventos, declara formalmente el incidente y activa a los equipos.



Taíta de la respuesta me come se quipo al rnorreno.

Equipos de Respuesta (IRTs)

Ejecutan procedimientos técnicos, investigan la causa raíz y contienen la amenaza.

Liderazgo estratégico. Asigna recursos, coordina partes externas y escala a Gestión de Crisis si el impacto supera los límites.

El Ciclo de Vida del Incidente (Proceso de 5 Fases)

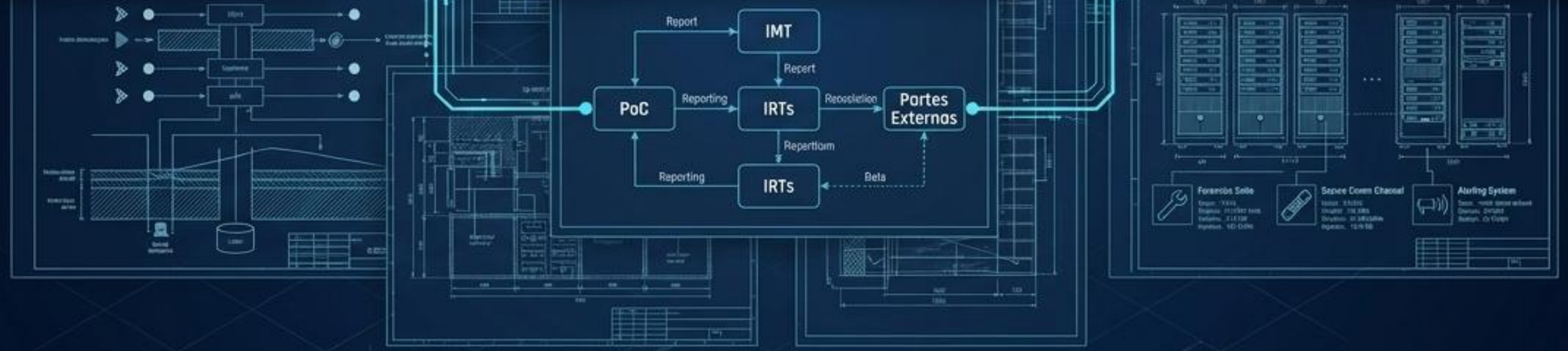
Fase 1 - Planificar y Preparar

Fase 1 | Fase 2 | Fase 3 | Fase 4 | Fase 5

Formular políticas de gestión alineadas con la gestión de riesgos global.

Establecer la estructura (IMT, PoC, IRTs) y sus conexiones organizacionales.

Desarrollar el soporte técnico y operativo (herramientas forenses, canales de comunicación).



La fase de preparación incluye obligatoriamente la capacitación de habilidades y la prueba constante del plan de gestión de incidentes antes de que ocurra una crisis.

Mg. Ing. Sebastián Vargas – profesor@sebastianvargas.cl + 56920063713

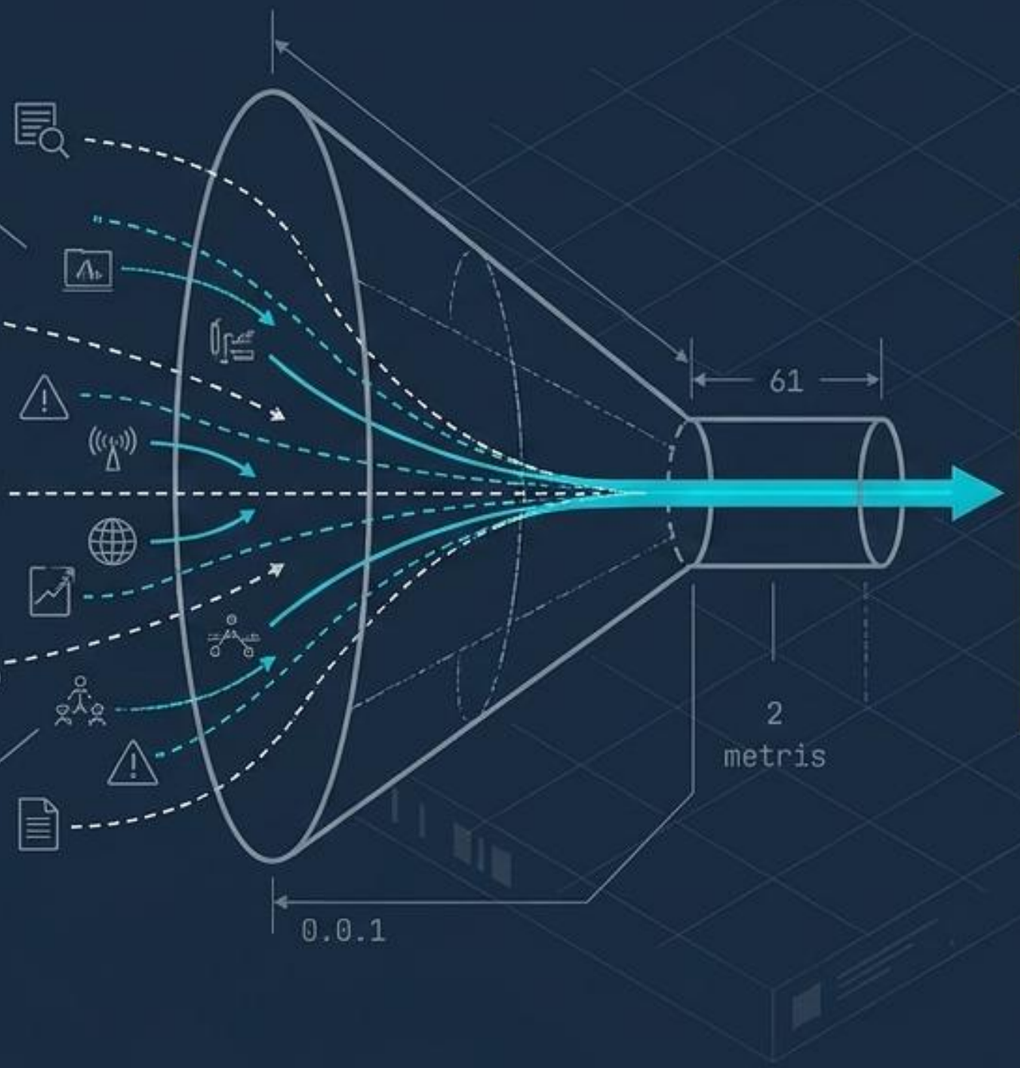
Fase 2 - Detectar y Reportar

Acciones Clave:

Recolectar inteligencia de fuentes locales y externas.

Monitorear redes y sistemas en busca de actividades anómalas, sospechosas o maliciosas.

Canalizar reportes de usuarios, proveedores y sensores de seguridad.



Regla de Oro:

Detección: lo antes posible.

Reporte: sin retrasos innecesarios, utilizando métodos automatizados siempre que sea factible.

Fase 3 - Evaluar y Decidir

El Momento de Decisión:

1. Evaluar

Determinar formalmente si el evento constituye un incidente de seguridad real.

2. Categorizar y Correlacionar

Agrupar incidentes relacionados para entender el alcance.

3. Priorizar

Asignar nivel de urgencia basado en el impacto al negocio (no solo en la severidad técnica).

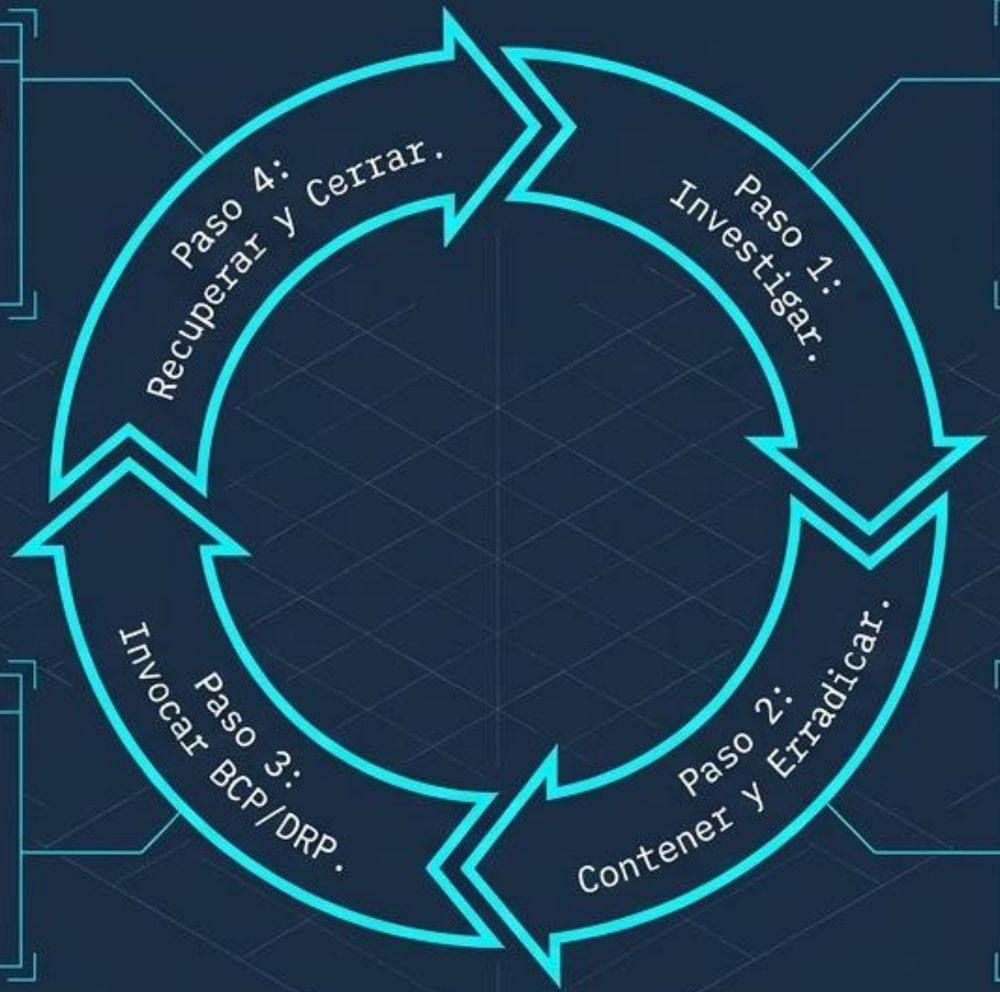
4. Activar

Establecer y desplegar los Equipos de Respuesta a Incidentes (IRTs) necesarios.

Fase 4 - Responder

Fase 1 | Fase 2 | Fase 3 | **Fase 4** | Fase 5

Restaurar los servicios a la normalidad y declarar el cierre formal del incidente de seguridad.

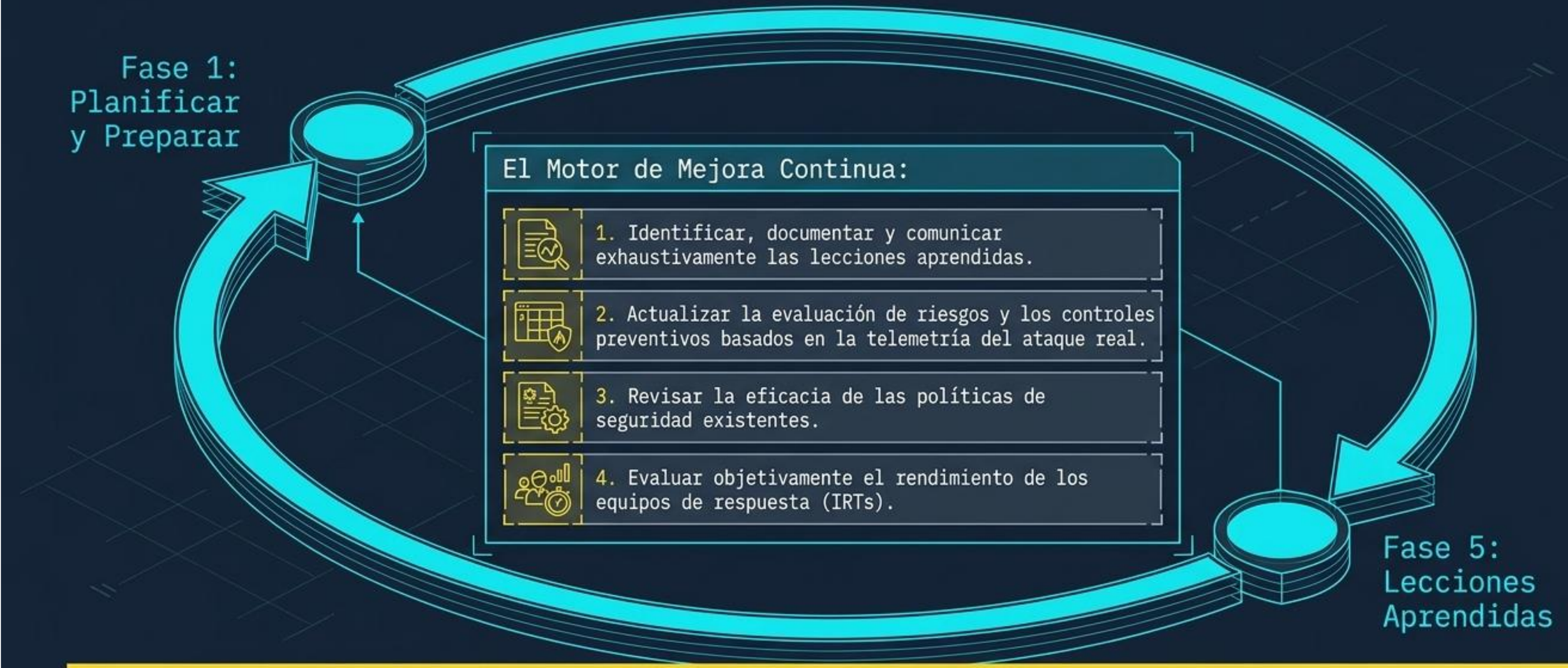


Determinar el alcance operativo y si la amenaza está bajo control.

Si los daños superan los límites aceptables, escalar a Continuidad de Negocio o Recuperación de Desastres.

Detener la hemorragia de datos y eliminar el acceso no autorizado o el malware.

Fase 5 - Aprender Lecciones



Un incidente resuelto sin lecciones implementadas es una vulnerabilidad garantizada para el futuro.

Reglas Críticas de Operación

Comunicación “Sin Culpa” (No-Fault)

El reporte inicial de incidentes debe estar libre de culpa o represalias para garantizar la divulgación inmediata por parte del personal.

Toda comunicación externa (RP, entidades legales) es estrictamente controlada por personal mandatado.

Documentación Rigurosa

Reporte de Eventos: Síntesis de circunstancias, hora de detección y hechos para comprender la magnitud.

Registro de Incidentes (Log): Todo dato y acción (fecha/hora/decisión) debe centralizarse para análisis legal, forense y de optimización.

Síntesis Sistémica: Integración con el Negocio

MITRE

Core Insight

La gestión de incidentes no opera en el vacío; es la prueba de estrés en tiempo real de todo el Sistema de Gestión de Seguridad de la Información.

Resumen Ejecutivo y Próximos Pasos

01 La Preparación es la Única Defensa.

Un centro de operaciones de clase mundial se diseña, entrena y prueba antes de que ocurra la brecha.

02 Claridad Absoluta de Roles.

La ambigüedad operativa durante una crisis es fatal. Defina y empodere hoy a su PoC, IMT e IRTs.

03 Retroalimentación Obligatoria.

Cada incidente debe convertirse en inteligencia accionable que modifique la matriz de riesgos y mejore los controles preventivos.

Evalúe sus protocolos actuales contra los estándares de la serie ISO/IEC 27035 para transicionar de una postura reactiva a una arquitectura de resiliencia total.

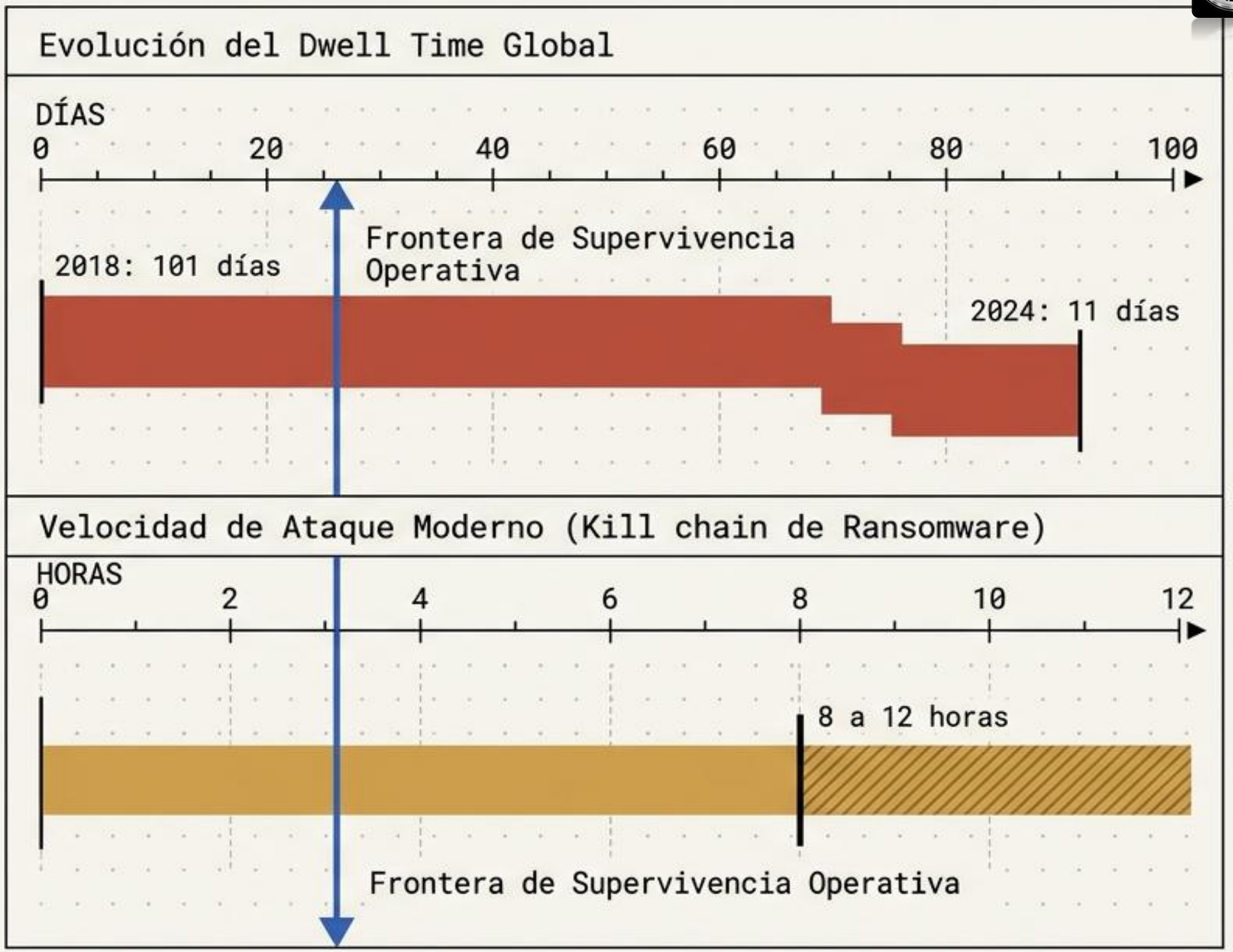
La falla matemática del SOC reactivo

TECHNICAL LOG READOUT

[!] ERROR: Operar sin métrica convierte a la seguridad en un estado binario ilusorio (protegido vs comprometido).

[!] LATENCIA: Aunque el dwell time bajó a 11 días (Mandiant 2025), el adversario cifra en 8-12 horas (Sophos 2024).

[+] RESOLUCIÓN: La frontera realista y exigible para un programa maduro es detectar incidentes materiales en <= 3 horas.



DOC: SOC-ENG-MAN-2025.1B | REV: 3.0 | SEC: LATENCY ANALYSIS | STATUS: CRITICAL REVIEW

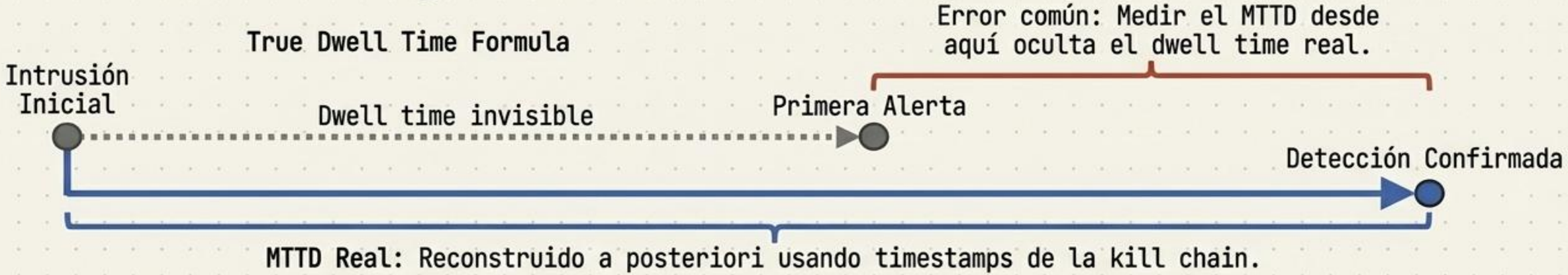
El déficit de ingeniería en los marcos tradicionales

Marcos de Referencia	NIST SP 800-61	ISO/IEC 27035	SANS PICERL	MITRE ATT&CK	TTP-IRT (Propuesto)
SLA Prescrito de Detección	✗ Depende de criticidad	✗ Depende del ISMS	✗ Mnemotécnico sin reloj	✗ Mapa de tácticas	✓ <= 3 horas P1/P2
Integración SOAR / Automatización	! Adaptativo pero manual	✗ Documental	! Fases claras	! D3FEND incipiente	✓ Orquestación MTTC <= 1h
Requisito de Telemetría Activa	! Asume telemetría irreal	✗ Foco en proceso	! Identificación teórica	✓ Guía el triage	✓ Hunting proactivo
Foco en SLA de Contención	✗ SLA invisible	✗ Sin umbral	✗ Sin SLA	✗ No aplica	✓ SLAs por severidad

⚠ Ningún marco público prescribe un SLA temporal explícito. Esta ausencia permite que la madurez retórica supere la capacidad técnica real del SOC.

DOC: SOC-ENG-MAN-2025.1B | REV: 3.0 | SEC: FRAMEWORK ANALYSIS | STATUS: CRITICAL REVIEW

Recalibrando la telemetría: El léxico del ingeniero



MTTC (Mean Time To Contain)

<= 1 HORA

Sensible a automatización SOAR.

MTTR (Mean Time To Recover)

Operación normal de negocio, no solo cerrar el ticket en el sistema.

FPR (False Positive Rate)

> 95%

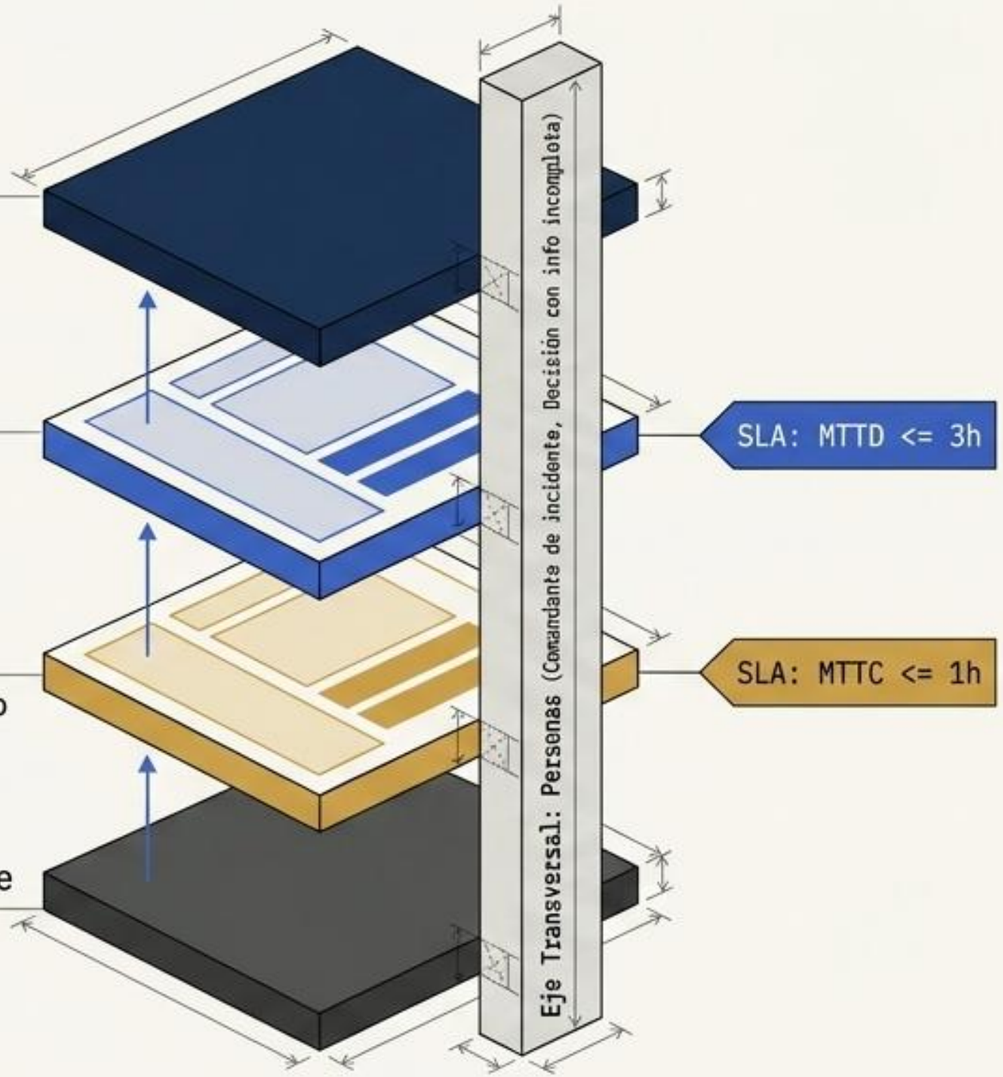
FPR alto es la norma esperada de una detección amplia, no una disfunción.

Nota Arquitectónica: Las métricas de detección dependen del adversario; las métricas de respuesta dependen puramente de la arquitectura interna del SOC.

La economía de la latencia: Tasa de quema por hora

Reducir el MTTD de 12 a 3 horas justifica económicamente cualquier inversión en XDR/SIEM. Con 4 incidentes al año (Ahorro USD 180k), el ROI sobre un EDR Enterprise es inmediato y matemáticamente irrefutable.

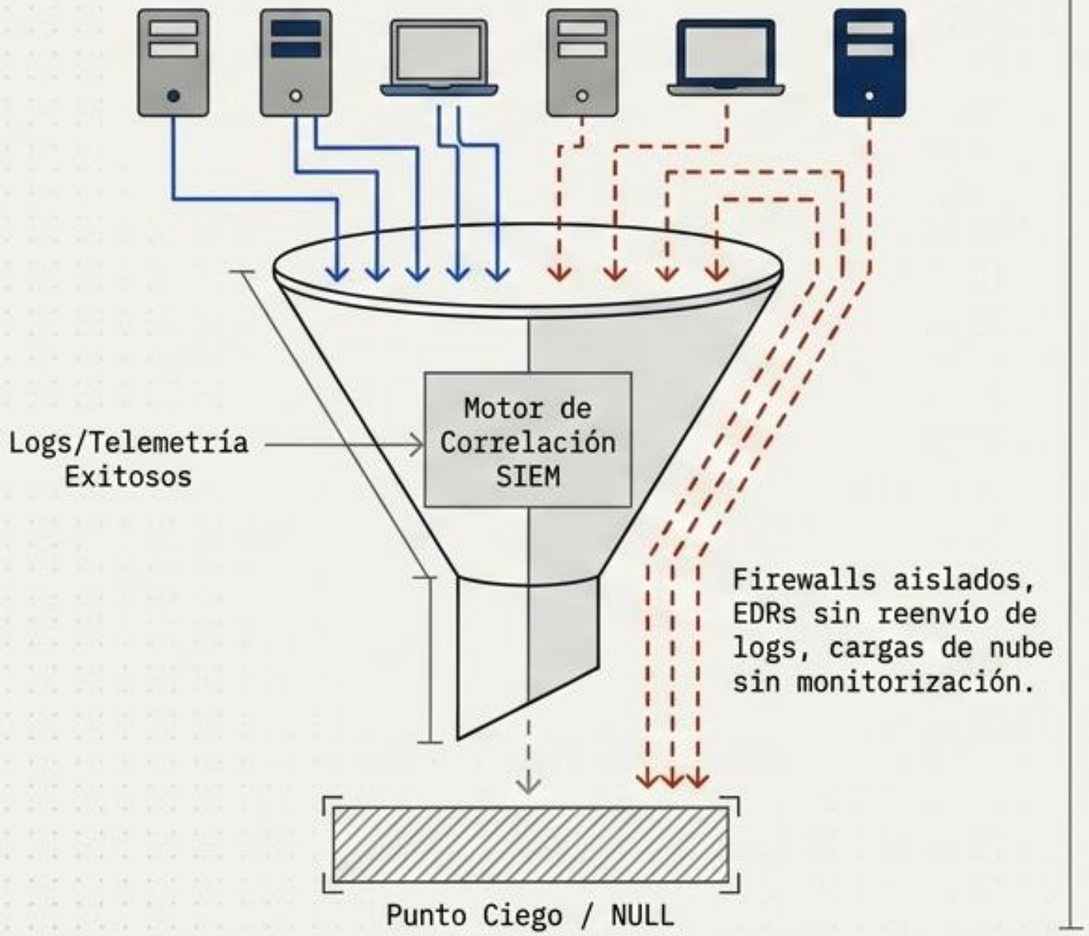
Arquitectura del Framework TTP-IRT



Un flujo de datos estructurado donde la telemetría cruda en la Capa 2 se transforma en acciones orquestadas en la Capa 3, gobernadas por decisiones ejecutivas pre-aprobadas en la Capa 1.

NESO Revisión	REVESIÓN 1	SEGORIDAD -	PÓSUMIAN 1/1
SOGUASOAN Ieistd Oaca de le dz 13 2023		CLASITIEACIÓR DE SEOGRAR Seguridad	

El embudo de visibilidad y el Control Invisible



Regla de Ingeniería

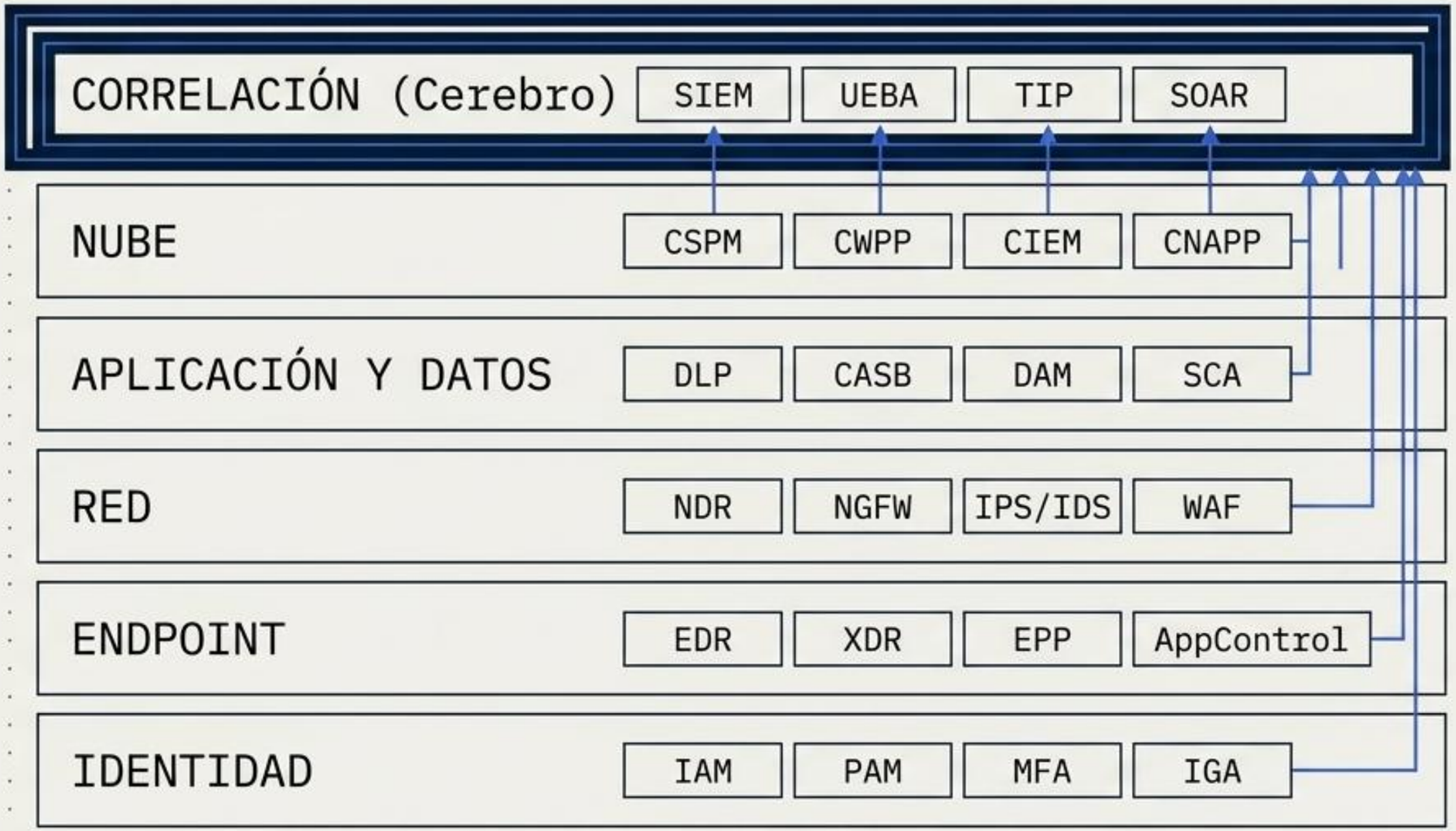
Control sin telemetría centralizada = Punto Ciego Operativo.

Un EDR que no reenvía eventos a la plataforma de correlación reduce el riesgo local, pero es completamente invisible para la métrica global de MTTD.

Vale más una cobertura de logs extensa en un SIEM modesto, que desplegar múltiples EDRs de gama alta aislados y sin integración.

El 70% de la kill chain ocurre en el endpoint.

Stack de Detección: Planos de Control y Caza



Cumplir el SLA de 3 horas exige un stack maduro donde cada plano de control actúa como un sensor activo. La integración SOAR en la capa de correlación es obligatoria y no opcional para lograr el MTTC de 1 hora.

MICRO-003 ENGINEERING BLUEPRINT - IVC.NEIL.

DOCUMENT NO:	PORT	STATUS	STATUS	STATUS

Matriz de Efectos Observables vs. Tácticas MITRE

Efecto Técnico Observable	Impacto CIA	Mapeo MITRE ATT&CK	SLA TTP-IRT
Indisponibilidad Total (E02) / Ejecución No Autorizada (E10)	Disponibilidad / Acceso	TA0040 (Impact)	1 Hora
Exfiltración de Datos (E04)	Confidencialidad	TA0010 (Exfiltration)	1 Hora
Modificación de Datos (E07) / Ejecución Parcial (E11)	Integridad	TA0005 (Defense Evasion)	2-3 Horas
Exposición de Config/Código (E03, E05)	Confidencialidad	TA0009 (Collection)	3 Horas
Manipulación Config (E06) / Degradación (E01)	Integridad / Disp.	Tácticas Diversas	4 Horas

Clasificación técnica exigida en < 15 minutos post-confirmación. Un analista entrenado reconocee que un evento de configuración suele preceder a un TA0040 (Impacto), orientando inmediatamente el threat hunting forense.

Calibración de Sensores: Telemetría vs. Tiempos de Tolerancia

Ransomware

10%

MTTD ~45 min

[EDR] [File Integrity]

El reto es detectar en discovery/exfiltración, antes del cifrado.

DDoS

1%

MTTD < 5 min

[NDR] [WAF] [Borde]

Web Application

5%

MTTD ~30 min

[WAF] [App Logging]

BEC / Phishing

15%

MTTD ~90 min

[Email GW] [UEBA]

Cloud Misconfig

25% 25%

MTTD ~2 horas

[CSPM Continuo]

APT con Lateralidad

35% 35%

MTTD 2-3 horas

[NDR] [Active Hunting]

Sin hunting activo, demora días.

Amenaza Insider

75%

MTTD 6-12 horas

[UEBA] [PAM Logs]

[Baselines]

Supply Chain

100%

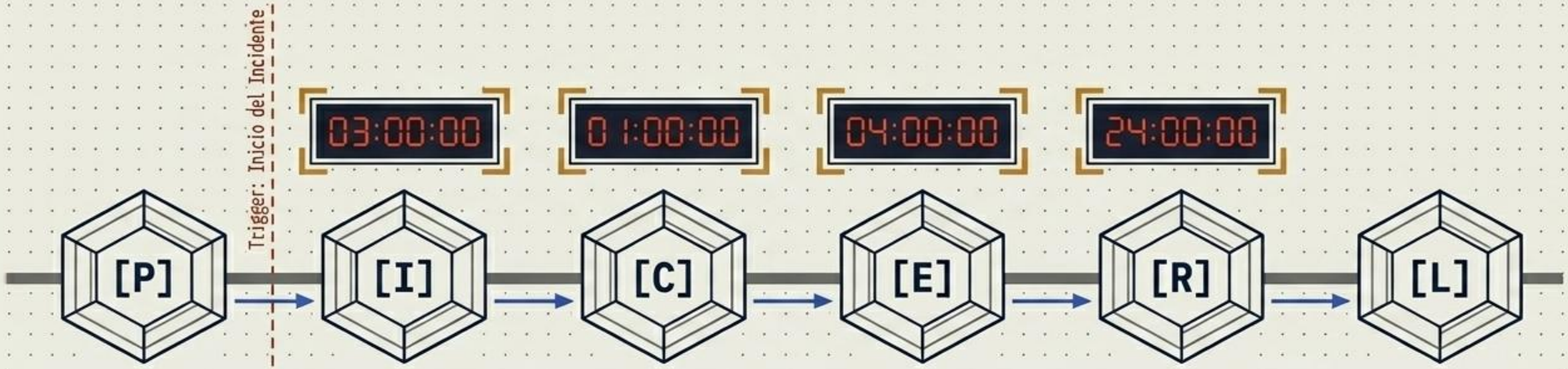
MTTD Semanas

[EDR Perímetro]

SLA aplica a la propagación interna.

MICRO-064 ENGINEERING BLUEPRINT - IVC.NEIL. | DOCUMENT NO: 5 | PORT (ES/2N) | STATUS 1 | STATUS ●●●●● | STATUS ○○○

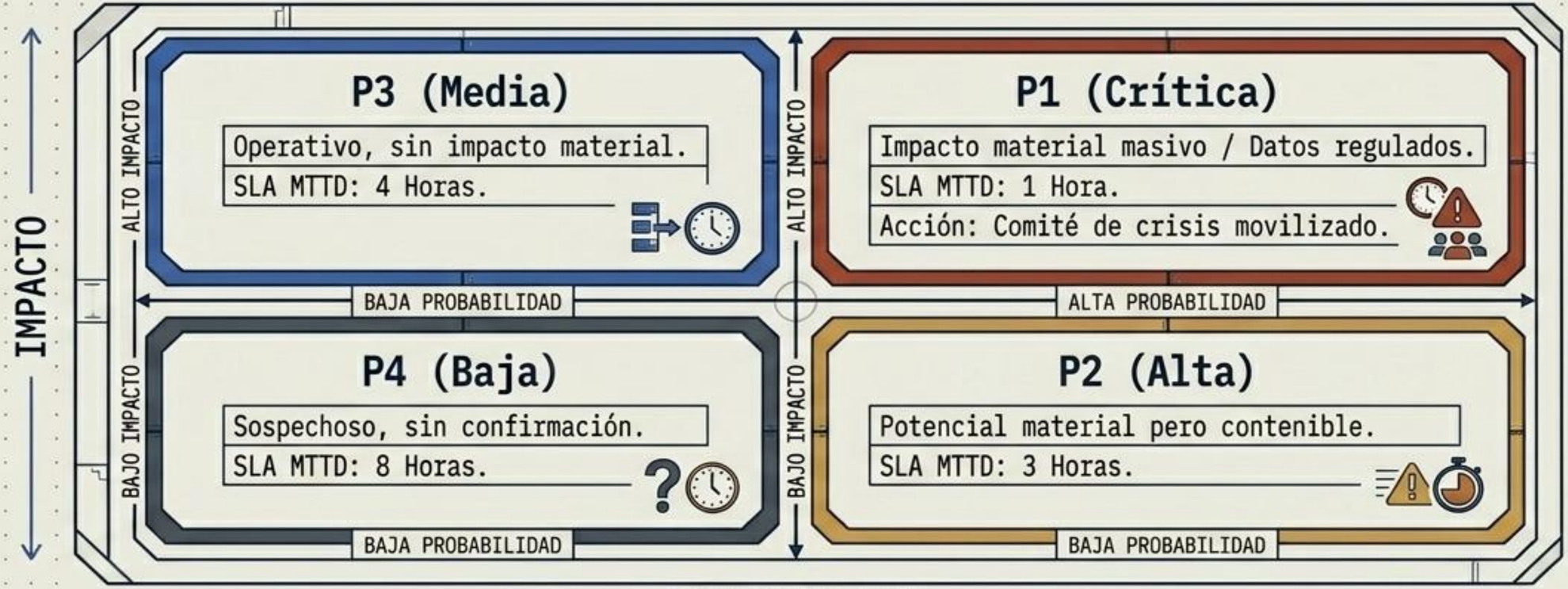
El Pipeline PICERL Sincronizado



Convertimos un ciclo conceptual en una cadena de montaje temporal. La pregunta del Comandante de Incidente ya no es '¿Qué pasó?', sino '¿En qué fase estamos y cuánto tiempo nos queda?'.

MICRO-D64 ENGINEERING BLUEPRINT - IVC.NEIL. | DOCUMENT NO: 5 | PORT (ES/2N) | STATUS 1 | STATUS ●●●●● | STATUS ○○○

Matriz de Tolerancias: Triggers de Severidad



The Responder's Rule

La regla práctica del primer nivel: en caso de duda, elevar. Errar a la baja le regala tiempo al adversario. Un comandante de incidente puede degradar un evento a posteriori, pero raramente debe escalar uno tarde.

MICRO-D64 ENGINEERING BLUEPRINT - IVC.NEIL. | DOCUMENT NO: 5 | PORT (ES/2N) | STATUS 1 | STATUS ●●●●● | STATUS ○○○

NotebookLM

Refactorización del SOC: Legacy vs. Arquitectura Moderna

Legacy SOC	
MTTD Comprometido	No declarado
MTTC Comprometido	Lo antes posible
Cobertura ATT&CK	< 30% técnicas
Threat Hunting	Reactivo/Inexistente
Orquestación (SOAR)	Pilotos aislados
Comité de Crisis	Documentado, nunca probado
Cultura Forense	Punitiva (buscar culpable)

TTP-IRT SOC	
MTTD Comprometido	**<= 3 horas para P1/P2**
MTTC Comprometido	**<= 1 hora desde detección**
Cobertura ATT&CK	**> 70% técnicas relevantes**
Threat Hunting	**Programado, mínimo 16 hrs/semana**
Orquestación (SOAR)	**60% de casos automatizables**
Comité de Crisis	**Probado cada trimestre**
Cultura Forense	**No-culpa, iterativa**

DOCUMENT NO: 6 STATUS

El Algoritmo del Responder: Ejecución bajo presión

Decidir con Incertidumbre

Actuar con el 60% de la información. Esperar al 100% es regalarle la red al adversario.

Ritmo de Sitreps

Emitir reportes cada 30-60 min. Incluso si el mensaje es "sin novedades". El silencio destruye confianza.

Aislar la Carga Cognitiva

Separar estrictamente al equipo que caza (causa raíz) del equipo que contiene (respuesta).

Preservación Forense Previa

Capturar imagen forense antes de mitigar. Restaurar sin evidencia impide litigios.

Loggeo en Tiempo Real

Llenar el casebook durante el incidente. La memoria humana es pésima reconstruyendo timelines.

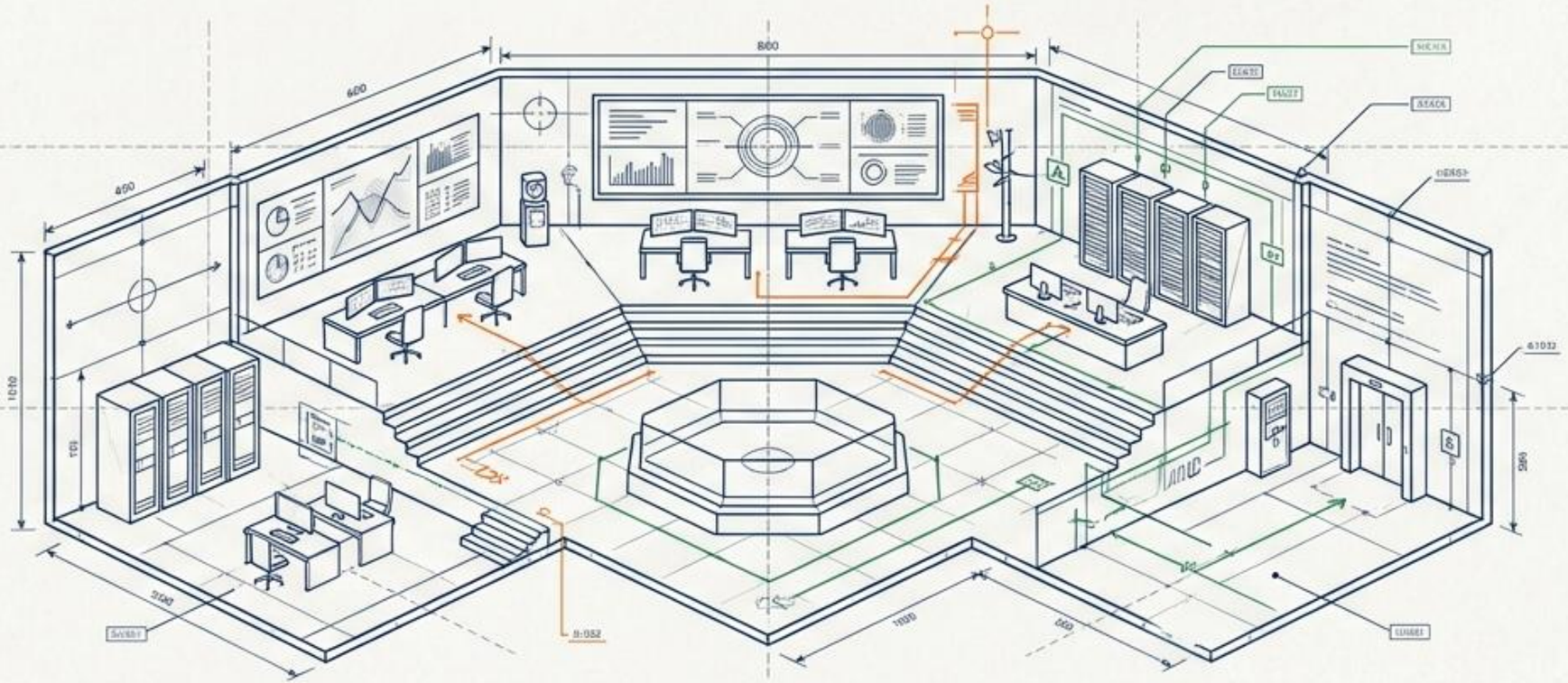
Contexto

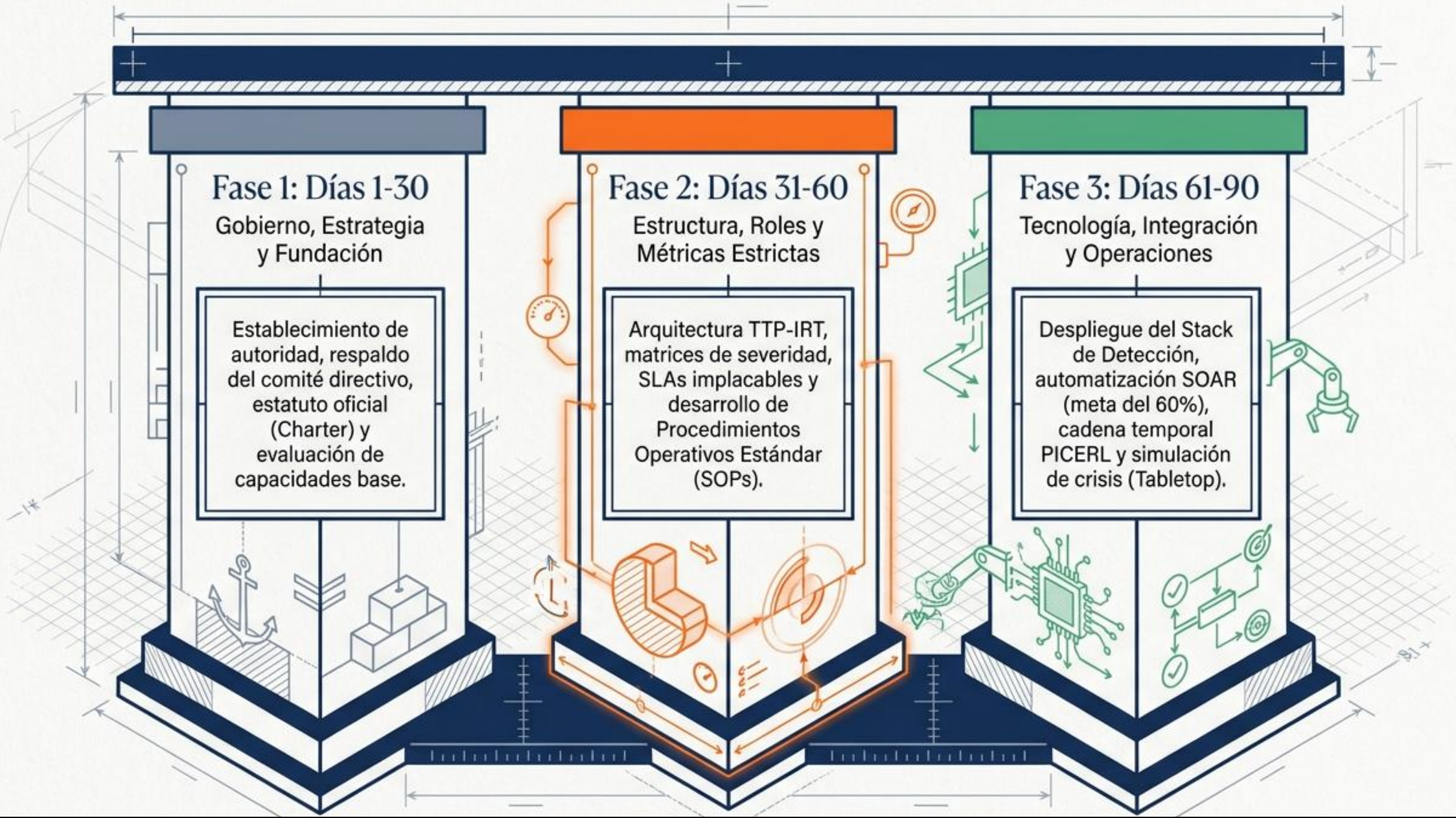
La gestión de incidentes combina disciplina técnica con juicio entrenado. La capa humana sostiene la arquitectura.

DOCUMENT NO: 7 | STATUS

Blueprint del SOC de 90 Días: De la Fundación a la Operación

Ingeniería de precisión para centros de operaciones de seguridad, basada en el estándar ISO/IEC 27035.




Fase 1: Días 1-30
Gobierno, Estrategia y Fundación
Establecimiento de autoridad, respaldo del comité directivo, estatuto oficial (Charter) y evaluación de capacidades base.
Fase 2: Días 31-60
Estructura, Roles y Métricas Estrictas
Arquitectura TTP-IRT, matrices de severidad, SLAs implacables y desarrollo de Procedimientos Operativos Estándar (SOPs).
Fase 3: Días 61-90
Tecnología, Integración y Operaciones
Despliegue del Stack de Detección, automatización SOAR (meta del 60%), cadena temporal PICERL y simulación de crisis (Tabletop).

El Mandato de Precisión

El Mandato de Precisión: Un SOC moderno no es solo monitoreo pasivo; es un motor de respuesta calibrado para neutralizar amenazas críticas en una ventana máxima de 4 horas.

DÍAS 1-30

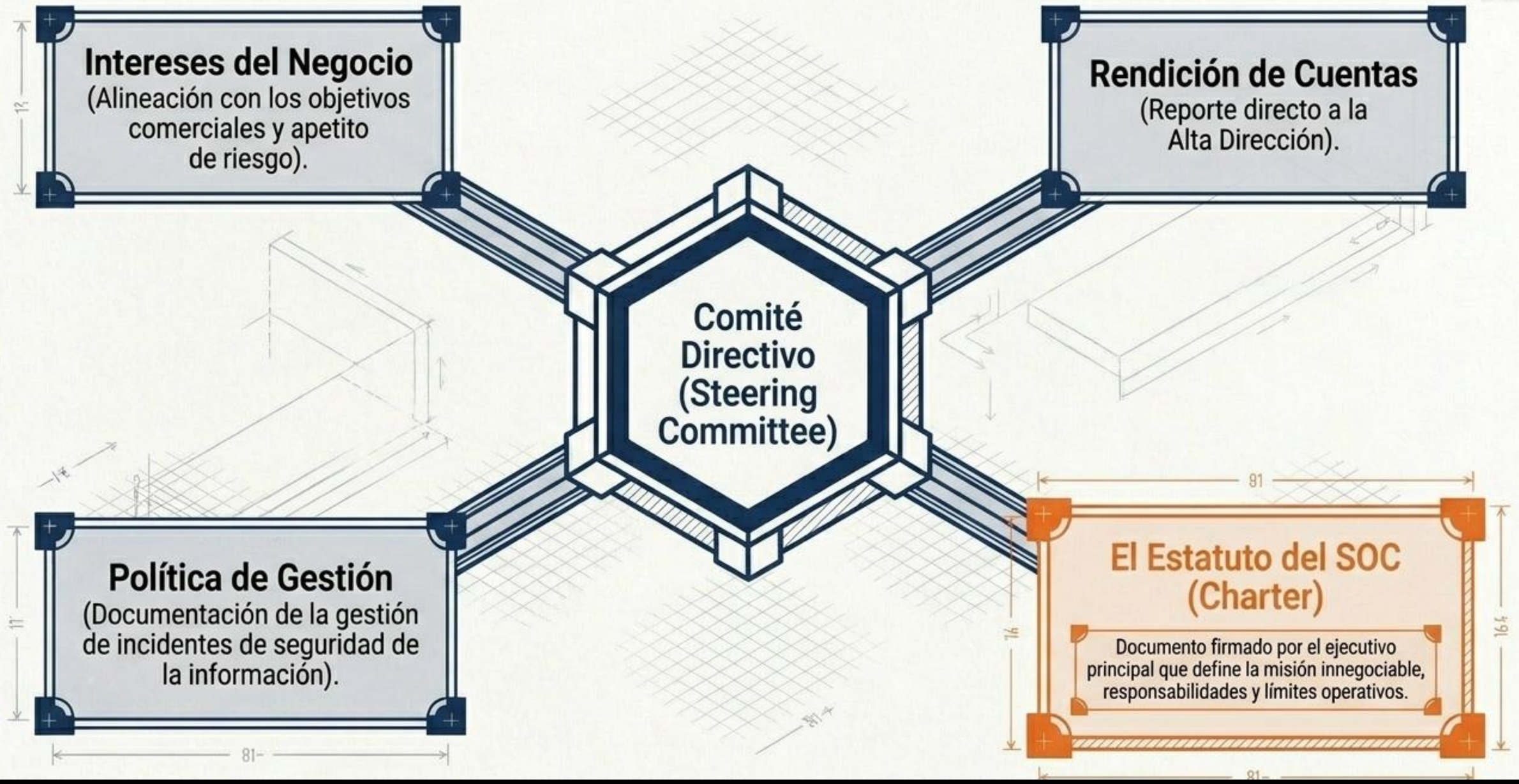
Fase 1: Gobierno, Estrategia y Fundación

Objetivo Central

Establecer la autoridad inquebrantable del SOC y asegurar los recursos iniciales antes de encender un solo servidor.

Hitos Clave

1. **1.** Formación del Comité Directivo.
2. **2.** Firma del Estatuto del SOC (Charter) por la Alta Gerencia.
3. **3.** Evaluación de capacidades existentes e inyección de presupuesto inicial.


Intereses del Negocio
(Alineación con los objetivos comerciales y apetito de riesgo).
Rendición de Cuentas
(Reporte directo a la Alta Dirección).
Comité Directivo (Steering Committee)
Política de Gestión
(Documentación de la gestión de incidentes de seguridad de la información).
El Estatuto del SOC (Charter)
Documento firmado por el ejecutivo principal que define la misión innegociable, responsabilidades y límites operativos.

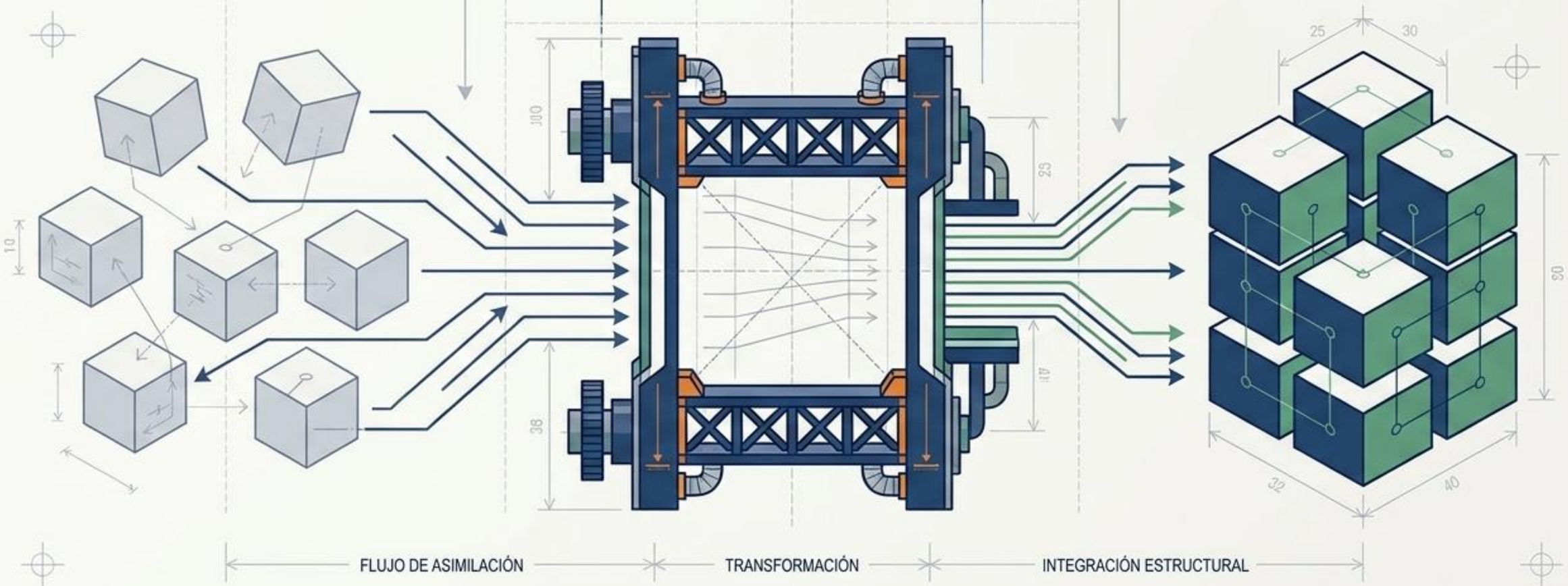
Estado Actual

Identificación de herramientas, funciones y talento existente en la organización.

El Puente: Asimilación y Justificación

Estado Futuro: Presupuesto Asegurado

Financiamiento inicial desbloqueado para personal clave y tecnología crítica basada en las brechas detectadas.



DÍAS 31-60

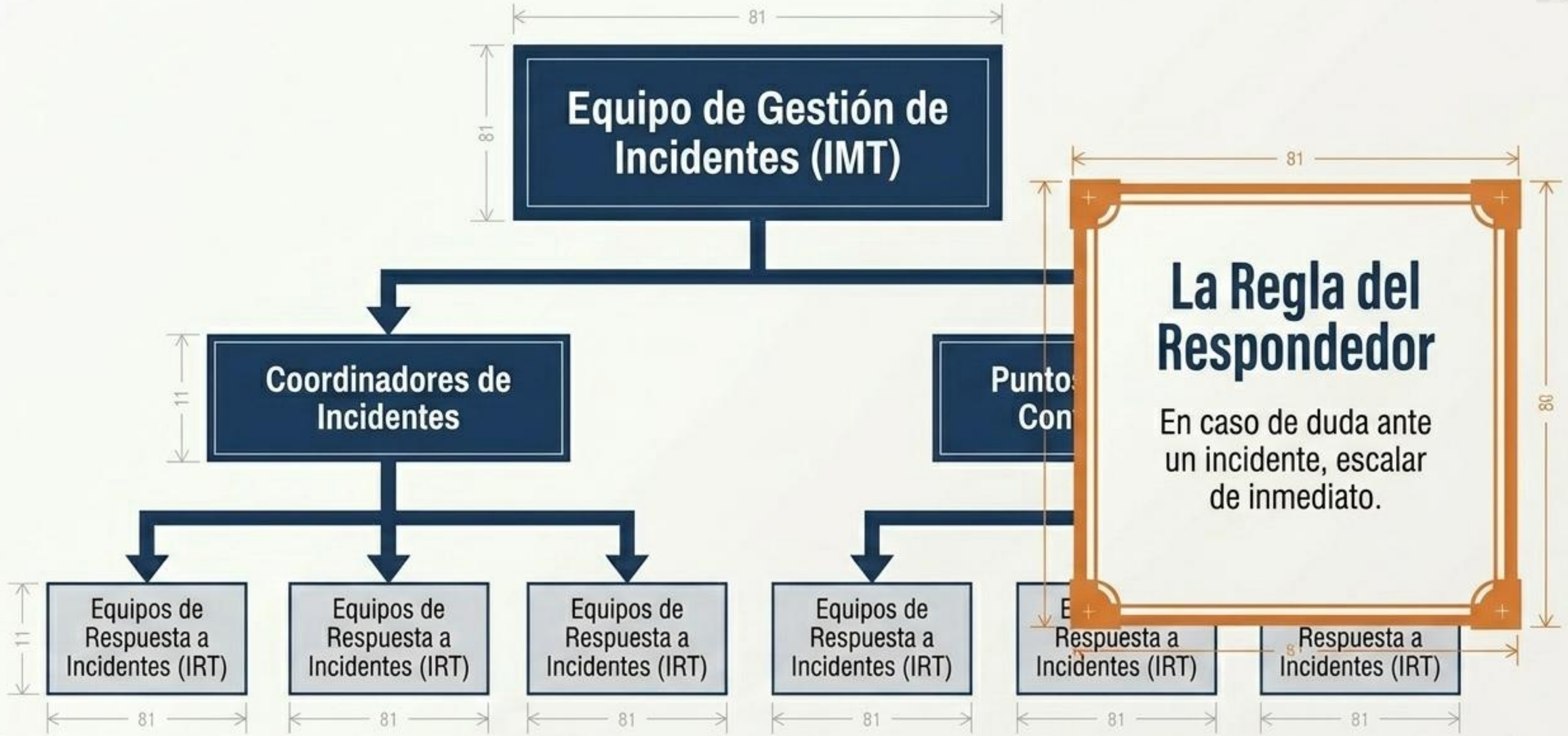
Fase 2: Estructura, Roles y Métricas Estrictas

Objetivo Central

Transformar el mandato ejecutivo en un motor táctico. Definir la cadena de mando, los umbrales de severidad y las reglas de movilización.

Hitos Clave

1. Despliegue de la estructura IMT e IRT.
2. Calibración de la Matriz de Tolerancias.
3. Reclutamiento e inicio de la Fábrica de Playbooks (SOPs).



Separación estricta entre la toma de decisiones estratégicas (IMT) y la mitigación técnica en la trinchera (IRT).

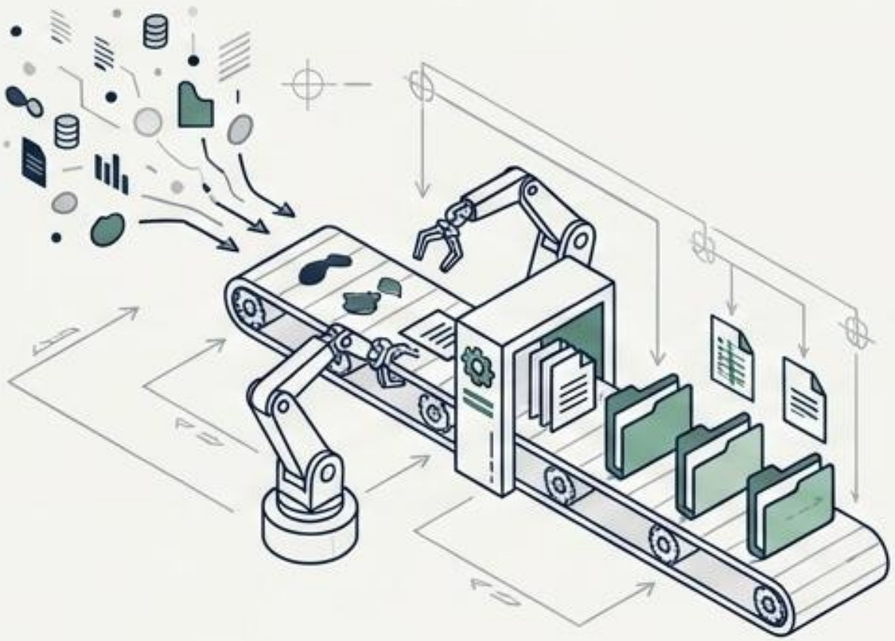
MATRIZ DIAGNÓSTICA: PROTOCOLO DE MOVILIZACIÓN DE INCIDENTES

NIVEL DE SEVERIDAD	IMPACTO AL NEGOCIO	PROBABILIDAD	PROTOCOLO DE MOVILIZACIÓN
P1 (Crítica)	Paralización del negocio / Fuga de datos masiva.	Certeza inminente.	Movilización total del IMT/IRT, escalamiento directo al CEO.
P2 (Alta)	Degradación severa de servicios críticos.	Alta.	Activación de IRT especializado, notificación al Comité Directivo.
P3 (Media)	Interrupción contenida, sin impacto masivo a clientes.	Moderada.	Manejo estandarizado por analistas tier 2, playbooks automatizados.
P4 (Baja)	Anomalías aisladas, eventos de ruido.	Baja/Incierta.	Resolución mediante automatización SOAR, revisión periódica.

Reclutamiento de Élite

Contratación de analistas principales e ingenieros de respuesta especializados en el modelo TTP-IRT.

Procedimientos Operativos Estándar (SOPs)



Desarrollo del Plan de Gestión de Incidentes y playbooks que guiarán la respuesta paso a paso, eliminando la improvisación.

Fase 3: Tecnología, Integración y Operaciones Iniciales

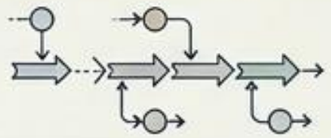
Objetivo Central

Encender la infraestructura tecnológica, forzar la automatización extrema y probar el ecosistema bajo fuego simulado.

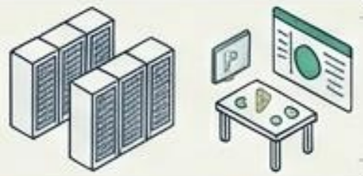
Hitos Clave

1. Despliegue del Stack de Detección (SIEM, UEBA, SOAR).

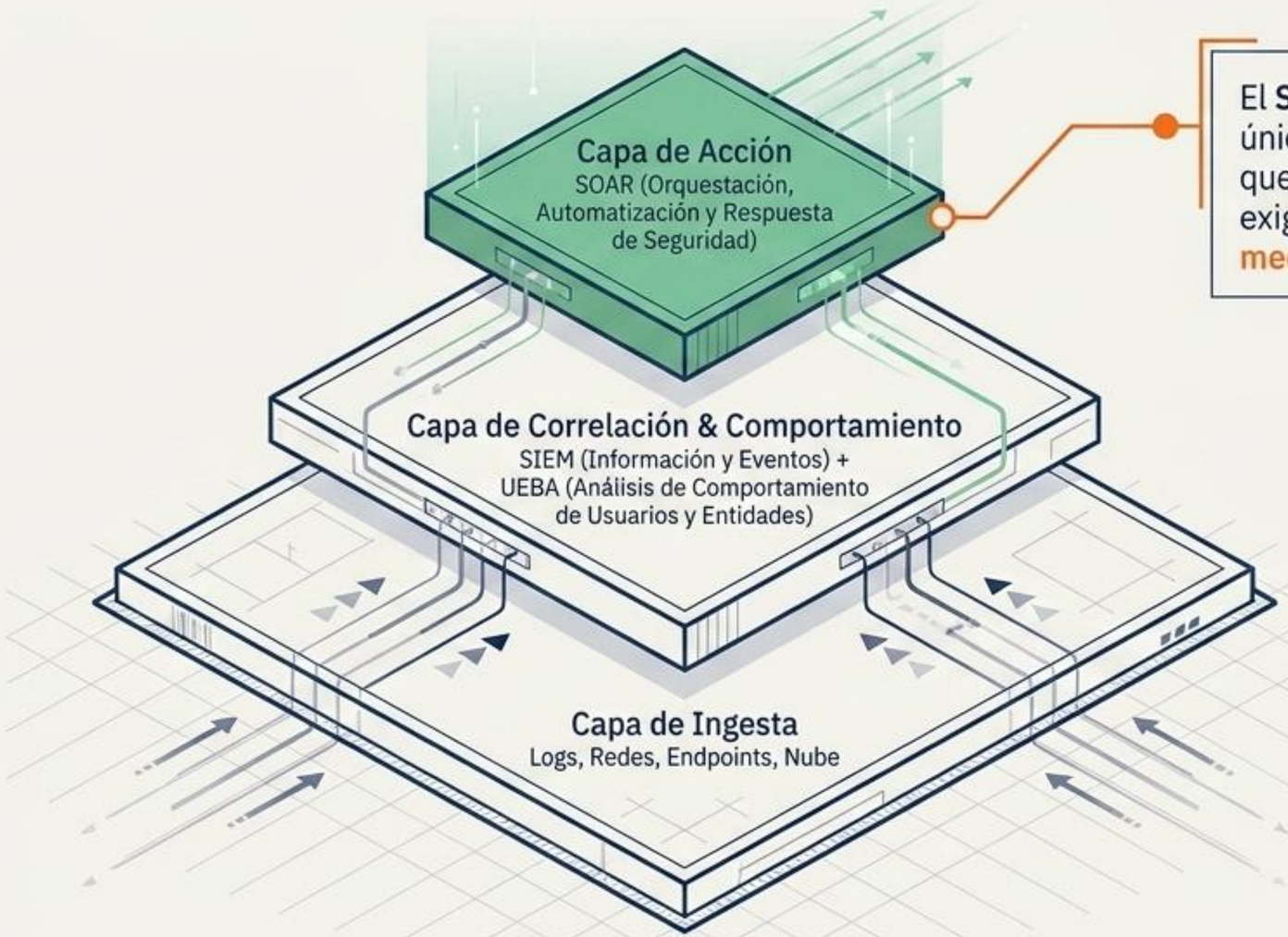
2. Sincronización temporal del pipeline PICERL.



3. Adecuación del entorno físico/virtual y simulación Tabletop.



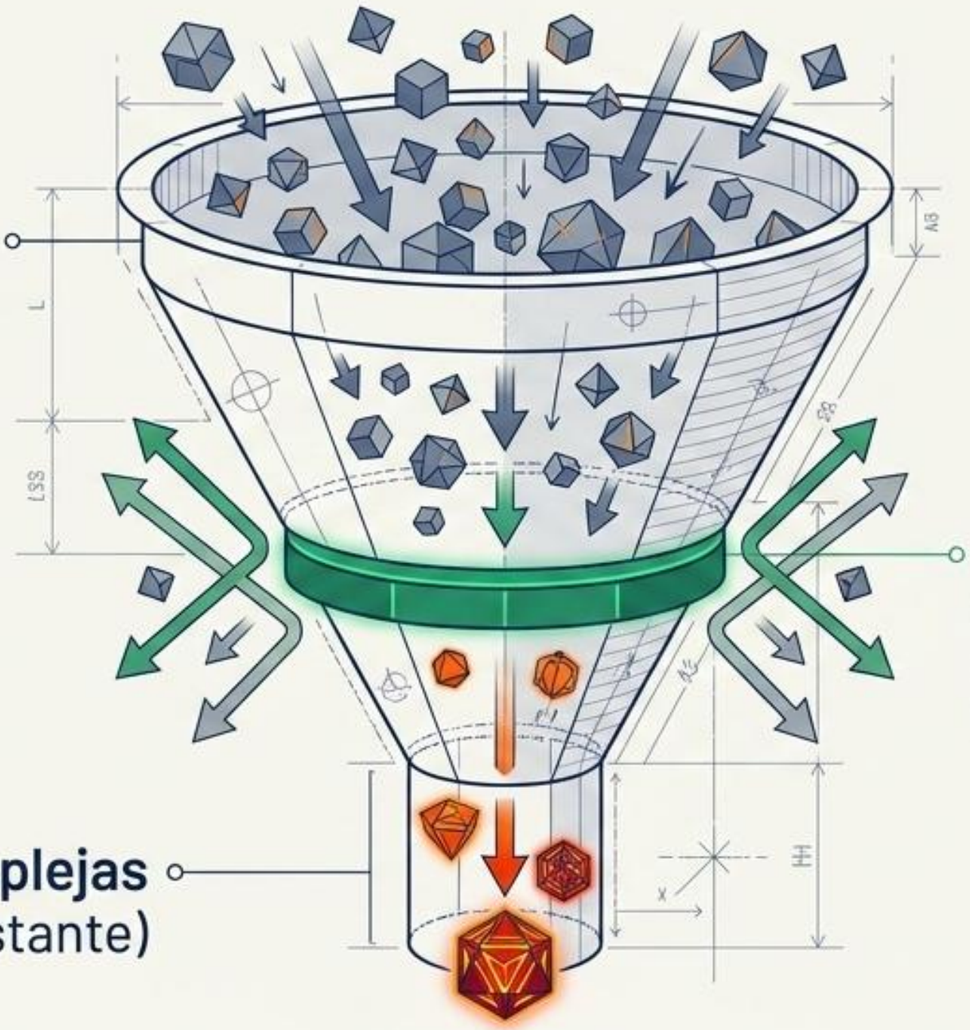
El Stack de Detección



El **SOAR es obligatorio**. Es la única pieza de la arquitectura que permite ejecutar el exigente **SLA de contención mecánica de 1 hora.**

Lluvia de Alertas Crudas

Volumen masivo ingresado por el SIEM/UEBA.



El Escudo SOAR

Meta: 60% de los casos automatizables. Resolución y desvío inmediato mediante playbooks.

Amenazas Complejas
(El 40% restante)

Al filtrar mecánicamente el ruido y las amenazas repetitivas, los ingenieros elite del IRT dedican su carga cognitiva exclusivamente a los incidentes de alto impacto.

Cadena de montaje temporal

Preparación
(Estado base constante)

Identificación
(Gatilla el reloj de 3h MTTD)

Contención
(Gatilla el reloj de 1h MTTC)

Erradicación
(Eliminación de la amenaza de la red)

Recuperación
(Restauración de sistemas a producción)

Lecciones
(Post-mortem y actualización de SOPs)

PICERL no es un concepto teórico; es una cadena de montaje cronometrada. Cada fase tiene plazos estrictos diseñados por ingeniería para evitar la parálisis operativa.

Día 90: Preparación del Ecosistema y Validación

El SOC virtual o físico está establecido. Los flujos de trabajo externos están formalizados. El flujo de información hacia el comité de crisis ha sido validado mediante el primer ejercicio de simulación de crisis (Tabletop).

El Blueprint está completo.
Operaciones Iniciadas.

03:00:00

La excelencia, cuando llega, se mide en minutos.

Cumplir las tres horas no requiere el presupuesto más alto del mercado.
Requiere la integración disciplinada de un stack mínimo viable,
cobertura honesta de telemetría y una matriz de autoridad delegada.

Tres horas es la regla del oficio. Rediseñe su SOC para medir latencia, no solo alertas.

DOCUMENT NO: 8 | STATUS

Protegiendo el presente, diseñando la resiliencia del futuro en LATAM.

MAIL: profesor@sebastianvargas.cl

TEL: +56 9 2006 3713

LINK: linkedin.com/in/profesorsvargasy

WEB: ttpsec.cl / purpleteamacademy.net

ORCID: 0000-0003-1782-3153 | ID-A1SCAN ✓