PROPUESTA EJECUTIVA DE CONSULTORÍA

Modernización inteligente de SIAEM y los servicios del DCCAE

Diagnóstico, arquitectura y piloto gobernado con activos FALCONE y lecciones verificables del modelo público RUNT

Decisión propuesta

Contratar una consultoría de 14 semanas para definir el modelo objetivo de SIAEM, probar un caso de uso con agentes gobernados y entregar una decisión de adopción, ajuste o descarte sustentada en evidencia. El DCCAE conserva autoridad, datos, veredictos y aprobación de cualquier cambio.

Problema y oportunidad

Situación	Respuesta de la consultoría
Históricos, fuentes e integraciones pueden producir inconsistencias y reprocesos	Línea base, reconciliación controlada y trazabilidad extremo a extremo
La operación tecnológica no puede confundirse con la autoridad militar	Separación contractual entre autoridad, operación, analítica y auditoría
La modernización exige seguridad, continuidad y evidencia	Piloto medible con controles, recuperación, revisión humana y salida reversible

Tesis

El DCCAE puede aprovechar lecciones públicas del RUNT y activos internos de FALCONE sin trasladar competencias soberanas ni adoptar un operador predeterminado. La primera decisión no es qué tecnología comprar, sino qué problema resolver, con qué evidencia y bajo qué gobierno.

ENCAJE INSTITUCIONAL Y CAPACIDAD

Tres aportes que no deben confundirse

DCCAE	Modelo público RUNT	FALCONE
Autoridad, reglas, excepciones y decisiones	Operación de registro nacional, interoperabilidad, niveles de servicio y continuidad	Gobierno de fuentes, agentes, analítica explicable y memoria de decisiones
Custodia y clasificación de información sensible	Separación entre encargado tecnológico y autoridades que reportan o modifican	Trazabilidad, detección de anomalías y priorización para revisión humana

Agentes FALCONE para adaptar

Agente	Función	Límite
Ingestor	Verifica fuente, corte, integridad y cambios	No modifica el dato oficial
Operador	Orquesta productos, pruebas, catálogo y alertas	No decide veredictos
Cronista	Conserva reglas, decisiones y evidencia	No relaja controles
Documentador	Mantiene diccionarios, manifiestos y aprendizajes	No publica datos sensibles

Evidencia y madurez

- Lago FALCONE: 120 fuentes documentadas y 110 con manifiesto al corte interno del 02-10-2026.
- Resolución de identidad, anomalías, score, grafo y geovisor existen como motores o demostradores internos.
- Ningún activo está certificado para producción SIAEM: cada uno requiere brecha, adaptación, seguridad y prueba con muestra autorizada.
- La participación directa del equipo en el RUNT no se presume; se usan documentos y lecciones de su modelo público.

MODELO OBJETIVO

Separar autoridad operación analítica y auditoría

Capa	Responsable	Contenido
Autoridad	DCCAE	Política, autorizaciones, restricciones, excepciones y sanción
Operación	Operador contratado	Canales, expedientes, soporte, integraciones, continuidad y SLA
Analítica	Equipo mixto	Candidatos, alertas explicables y medición; nunca decisión automática
Auditoría	Control independiente	Evidencia, privilegios, desempeño, incidentes e incentivos

Trazabilidad y blockchain con criterio

Cada evento debe registrar fuente, corte, actor, regla, versión, motivo, sello de tiempo y decisión. Se comparará una bitácora inmutable convencional con un libro distribuido permisionado. Blockchain solo procede si varias entidades necesitan verificar el mismo evento y aporta más valor que costo y complejidad.

- La cadena nunca almacena personas, armas, antecedentes ni documentos: solo hashes, firmas, sellos e identificadores técnicos.
- Debe existir gobierno de nodos, rotación y revocación de llaves, rectificación del dato fuente y plan de salida.
- Se descarta si expone metadatos, dificulta la corrección legal o no mejora una auditoría firmada tradicional.

Incentivos y transparencia

La remuneración se vincula a disponibilidad, calidad, evidencia, solución y recuperación; nunca al número de permisos aprobados, negados o alertas generadas. Falsos positivos evitables, reincidencia, indisponibilidad y fallas de auditoría reducen desempeño. La ciudadanía ve estado y causas de devolución; supervisores y auditores acceden a evidencia según rol; la información reservada permanece protegida.

CASO DE USO Y PILOTO

Reconciliación y control de históricos SIAEM

Paso	Responsable	Evidencia
Autorizar muestra y finalidad	DCCAE	Campos mínimos, custodio, periodo y base de acceso
Ingerir copias controladas	Ingestor	Hash, origen, corte, diccionario y acceso
Ejecutar reglas	Motores	Versión, resultado reproducible y explicación
Priorizar candidatos	Operador	Cola de revisión sin alterar la fuente
Revisar y decidir	Analista y autoridad	Aceptación, rechazo, motivo, autor y fecha
Preservar memoria	Cronista y documentador	Bitácora, métricas, cambios y límites

Piloto gobernado de ocho semanas

Un caso de uso, una muestra controlada y máximo tres fuentes, ejecutados en infraestructura aprobada por el DCCAE. El piloto se detiene ante acceso no autorizado, pérdida de trazabilidad, uso fuera de finalidad, error sistemático no explicable o riesgo para un trámite real.

Criterios de éxito

- 100 % de alertas con fuente, regla, versión, evidencia y responsable de revisión.
- 100 % de decisiones humanas y 0 transferencias fuera del entorno autorizado.
- 100 % de la muestra auditada reconstruible desde fuente hasta decisión.
- Precisión, falsos positivos, tiempo de ciclo y reproceso comparados con línea base de semanas 2 a 4.
- Resultado por activo: adoptar, ajustar o descartar, con costo, riesgo y evidencia.

CIBERSEGURIDAD Y PRIVACIDAD

Marco colombiano obligatorio y referencia internacional

La arquitectura se alinea primero con el MSPI actualizado por la Resolución MinTIC 2277 de 2025, basado en ISO/IEC 27001:2022, y con el Decreto 338 de 2022 sobre gobernanza, riesgo, infraestructura crítica y respuesta a incidentes. NIST CSF 2.0 y NIST SP 800-207 complementan el diseño; no sustituyen las obligaciones nacionales.

Dominio	Producto y prueba
Gobernar	Perfil MSPI actual/objetivo, roles, riesgo, proveedores, datos y aprobación directiva
Identificar	Inventario y clasificación de activos, BIA, dependencias, amenazas y criticidad
Proteger	Confianza cero, MFA, PAM, mínimo privilegio, cifrado, llaves, segmentación y desarrollo seguro
Detectar	Logs íntegros, SIEM/SOC, casos de uso, alertas, sincronización de tiempo y evidencia digital
Responder	Plan probado, responsables, preservación de evidencia y reporte a CSIRT Gobierno/COLCERT cuando aplique
Recuperar	RTO/RPO por servicio, respaldos aislados, restauración probada, continuidad y comunicación

Controles de aceptación

- Pruebas de penetración y remediación; vulnerabilidades y parches con tiempos acordados.
- SBOM, evaluación de proveedores, componentes firmados y control de cadena de suministro.
- Revisión periódica de privilegios, simulacro de incidente y evidencia de restauración.
- Clasificación de información y matriz de transparencia por ciudadano, analista, supervisor, auditor y público.

OFERTA Y SIGUIENTE DECISIÓN

Catorce semanas sujetas al encuadre inicial

Etapa	Semanas	Resultado
Inicio	1	Mandato, confidencialidad, equipo, accesos y alcance
Diagnóstico	2 a 4	Línea base, MSPI, procesos, datos, contratos y riesgos
Diseño y piloto	5 a 8	Arquitectura, reglas, seguridad y ejecución controlada
Evaluación	9 a 12	Precisión, impacto, costos, incentivos, continuidad y reversibilidad
Decisión	13 a 14	Caso económico, hoja de transición y anexo técnico

Productos y frontera comercial

Se entregan diagnóstico ejecutivo, modelo operativo, arquitectura y seguridad, expediente del piloto, métricas, caso económico, transición y anexo técnico. Equipo mínimo: dirección institucional, procesos, datos, seguridad y privacidad, analítica, proyecto y calidad. No incluye operación productiva, concepto jurídico, certificación, depuración masiva, infraestructura ni migración definitiva. Diagnóstico y diseño se cotizan a precio fijo; el piloto se contrata con criterios de aceptación. Propiedad intelectual y licencias se acuerdan expresamente.

Siguiente paso

Reunión de encuadre de noventa minutos con patrocinador, proceso, tecnología, seguridad, jurídico y protección de datos para confirmar el problema prioritario, accesos, clasificación, línea base y decisión esperada. Con esa información se presenta alcance y propuesta económica cerrados.

Fuentes oficiales y límites

Información pública e interna consultada al 20 de octubre de 2026. No se revisaron arquitectura, incidentes, contratos ni datos reservados de SIAEM. El documento no constituye concepto jurídico, certificación de seguridad ni oferta económica cerrada.

DCCAE Misión funciones y SIAEM Abrir fuente

Función Pública Ley 1453 de 2011 Abrir fuente

RUNT Política y Contrato 604 de 2022 Abrir fuente

MinTIC MSPI actualizado Resolución 2277 de 2025 Abrir fuente

Función Pública Decreto 338 de 2022 Abrir fuente

MinTIC Guía blockchain para el Estado Abrir fuente