MilpaSec

Seguridad solida a través de interdependencia.

Servicios MilpaSec

De la exposición a la capacidad operativa

Modelo técnico-ejecutivo para diagnosticar, implementar, validar y sostener capacidades de ciberseguridad.

GUI-SVC-GEN-001 | v1.0 | 2026

DOCUMENTO TÉCNICO | PÚBLICO

MilpaSec

engage@milpasec.com

Resumen ejecutivo

La ciberseguridad se vuelve operable cuando una organización puede observar su entorno, controlar los accesos, entender su exposición y sostener decisiones con evidencia. Comprar herramientas, ejecutar revisiones aisladas o acumular recomendaciones no garantiza esa capacidad. El problema central es conectar diagnóstico, implementación, validación y seguimiento dentro de una secuencia que tenga responsables y criterios de cierre.

MilpaSec estructura sus servicios para cerrar esa brecha. La cartera combina evaluación, arquitectura, defensa, validación adversarial, continuidad operativa y acompañamiento especializado. Cada servicio resuelve un problema delimitado, produce evidencia verificable y debe dejar una decisión o siguiente acción más clara que al inicio.

El problema que resuelve la cartera

Las organizaciones compactas y en crecimiento suelen operar con infraestructura híbrida, proveedores externos, servicios en nube, identidades dispersas y equipos de TI con responsabilidades amplias. En ese contexto aparecen inventarios incompletos, privilegios difíciles de justificar, respaldos no probados, exposición externa desconocida y controles que dependen de conocimiento informal. El riesgo no proviene únicamente de una vulnerabilidad: también nace de no saber qué existe, quién responde y cómo verificar que una corrección realmente quedó operativa.

La lógica MilpaSec

La cartera se organiza en cuatro movimientos complementarios:

- **Diagnosticar:** determinar el estado actual, las dependencias y las prioridades antes de intervenir;
- **Implementar:** convertir prioridades en controles, arquitectura, procedimientos y responsables;
- **Validar:** comprobar exposición, funcionamiento y límites mediante evidencia técnica;
- **Sostener:** mantener seguimiento, métricas, decisiones y ciclos de mejora.

Estos movimientos no representan una venta lineal obligatoria. Permiten iniciar donde existe evidencia suficiente y establecen dependencias cuando comenzar en una etapa posterior generaría una falsa sensación de avance.

OC2G como marco de orientación

OC2G — Observa, Controla, Caza y Gobierna — aporta el marco de progresión que conecta los servicios con dependencias reales: primero visibilidad, después control, luego validación de exposición y finalmente gobierno. No todos los servicios de MilpaSec se fuerzan dentro de **OC2G**; el framework se utiliza cuando ayuda a explicar madurez, continuidad y priorización. Los servicios especializados conservan su propia lógica cuando una etiqueta de dominio reduciría precisión.

Una cartera, ocho puntos de intervención

- **01 — «Diagnóstico OC2G Express»:** establece una lectura inicial y una hoja de ruta (**roadmap**) 30/60/90.

- **02 — «OC2G por Dominio»:** convierte un dominio priorizado en un sprint operativo.
- **03 — «Blue Team Starter»:** construye controles defensivos, endurecimiento (hardening) y telemetría útil.
- **04 — «Red Team Starter»:** valida exposición, simula escenarios adversarios autorizados y refuerza cultura de seguridad.
- **05 — «Mesa Operativa»:** sostiene seguimiento, coordinación y mejora recurrente.
- **06 — «Arquitectura y Segmentación»:** ordena arquitectura, flujos, segmentación y accesos de red.
- **07 — «Respaldos y Recuperación Operativa»:** define y prueba recuperación con objetivos RPO/RTO.
- **08 — «Criptoactivos y Custodia»:** construye criterio sobre blockchain, privacidad, mercados y tokenización, y lo convierte en soberanía, custodia y operación responsable.

Evidencia, trazabilidad y cierre

Los entregables separan lectura ejecutiva y detalle técnico. Cuando existen hallazgos, evidencias, recomendaciones o decisiones vinculadas con **OC2G**, **MilpaSec** conserva trazabilidad operativa mediante identificadores internos de trabajo. Esa trazabilidad no reemplaza la explicación; impide que el objeto cambie de nombre o desaparezca entre documentos sin dejar relación con su evidencia, prioridad y remediación.

Para quién es

Este paper se dirige a dirección, tecnología, seguridad, operaciones y compras técnicas. Explica qué problema atiende cada servicio, qué resultado puede esperarse y cómo se conecta con una ruta de mejora.

1 — Introducción

1.1 – La brecha entre herramientas y capacidad

Una organización puede tener antivirus, firewall, respaldos, un proveedor de nube y políticas escritas **sin disponer de una capacidad de seguridad coherente.** Las **herramientas** son **componentes**; una capacidad exige cobertura conocida, responsables, operación repetible, evidencia y una forma de decidir cuándo el control funciona o debe cambiar.

La diferencia importa porque los incidentes rara vez respetan los límites administrativos. Una **identidad comprometida** puede atravesar correo, nube, VPN y aplicaciones; una **dependencia no inventariada** puede impedir una restauración; un **servicio externo** puede quedar expuesto después de un cambio legítimo. **Cuando cada control se administra como una pieza aislada, la organización pierde la relación entre activos, accesos, exposición y decisiones.**

1.2 – Limitaciones de los servicios aislados

Una revisión puntual puede producir una lista técnicamente correcta y aun así no cambiar el riesgo. Esto ocurre cuando los hallazgos no tienen dueño, la evidencia no indica alcance o confianza, la prioridad se basa solo en severidad técnica, o la remediación no considera dependencias operativas. También ocurre cuando se implementa una herramienta sin definir qué señal importa, quién la revisa y qué decisión debe detonar.

MilpaSec trata el servicio como una intervención con inicio y cierre verificables. La pregunta no es únicamente qué se encontró o instaló, sino qué capacidad queda disponible, para qué activos, bajo qué límites y con qué evidencia puede demostrarse.

1.3 – Propósito y alcance del documento

Este documento explica la razón de ser de la cartera MilpaSec, la relación entre sus servicios y el tipo de resultados que busca producir. Su alcance es técnico-ejecutivo: ofrece suficiente profundidad para evaluar el enfoque sin publicar procedimientos internos, bandas de precio, listas de verificación sensibles ni técnicas que dependan de un entorno real.

El paper no sustituye un acuerdo de confidencialidad, contrato, reglas de participación (Rules of Engagement, **ROE**), **SOW**, propuesta económica o plan de trabajo. Esos documentos convierten la lógica general en obligaciones, activos, ventanas, exclusiones y criterios de aceptación específicos para cada cliente.

2 — Modelo de servicio MilpaSec

2.1 – Qué significa construir capacidad

MilpaSec considera operable una capacidad cuando reúne, de forma proporcional al riesgo, cinco elementos:

- **Cobertura:** se conocen los activos, identidades, flujos o procesos a los que aplica.
- **Responsabilidad:** existe una persona o función que decide y que ejecuta cuando corresponde.
- **Procedimiento:** la actividad puede repetirse sin depender exclusivamente de memoria informal.
- **Evidencia:** el estado y los resultados pueden verificarse.
- **Gobierno:** hay condiciones para aceptar, corregir, escalar o revisar el resultado.

No todos los servicios completan por sí solos los cinco elementos. Un **diagnóstico** puede establecer cobertura y prioridad; un **sprint** puede implementar el control; una **validación** puede demostrar exposición; una **mesa operativa** puede sostener el ciclo. El diseño del portafolio hace visibles esas transiciones.

2.2 – Diagnosticar, implementar, validar y sostener

Diagnosticar reduce incertidumbre antes de invertir. Implementar convierte una prioridad en configuración, arquitectura, procedimiento o decisión. Validar comprueba el comportamiento real y distingue una declaración de una condición demostrable. Sostener evita que los controles se degraden cuando cambian personas, proveedores, activos o necesidades.

La secuencia puede ser iterativa. Una validación puede descubrir una dependencia y regresar a diagnóstico; una implementación puede requerir redefinir alcance; la operación continua puede detectar que una métrica dejó de representar riesgo. **La madurez no es una línea recta, pero sí necesita estados comparables y decisiones registradas.**

2.3 – Relación con OC2G

OC2G organiza el programa en cuatro dominios con dependencias explícitas. **D1 - Observa** produce la base de realidad: activos, dependencias, superficie y contexto operativo. **D2 - Controla** toma esa base y reduce abuso de identidades, privilegios, configuraciones inseguras y accesos no justificados. **D3 - Caza** valida lo que está expuesto, lo que puede explotarse y lo que la organización puede detectar. **D4 - Gobierna** convierte evidencia, métricas y decisiones en políticas mínimas, aceptación de riesgo, continuidad y mejora. **La secuencia importa porque un control aplicado sin visibilidad, identidad o evidencia termina operando sobre supuestos.**

Para la cartera de servicios, **OC2G** funciona como mapa de decisión. Permite explicar por qué un cliente puede necesitar inventario antes de endurecimiento, identidad antes de pruebas más profundas, telemetría antes de caza de amenazas **(threat hunting)** o gobierno antes de sostener auditoría. En México y Latinoamérica, donde muchas organizaciones conocen referencias como **NIST**, **CIS** o **ISO** pero no cuentan con equipos ni presupuesto para traducirlas de inmediato en operación diaria, **OC2G** aterriza esas referencias en dependencias, decisiones y entregables proporcionales.

«Criptoactivos y Custodia» conserva lógica propia; puede usar principios de evidencia, control y gobierno, pero no debe reducirse a una etiqueta **OC2G** cuando el alcance exige arquitectura de custodia, contraparte, mercado y soberanía operativa.

3 — Arquitectura del portafolio

3.1 – Capas de intervención

La cartera no es una colección plana. Sus servicios ocupan capas distintas y pueden combinarse sin perder sus límites.

- **Orientación y priorización: «Diagnóstico OC2G Express»** ofrece una lectura transversal, mientras «**OC2G por Dominio»** profundiza una prioridad ya reconocida.
- **Construcción: «Blue Team Starter», «Arquitectura y Segmentación», «Respaldos y Recuperación Operativa»**, y determinados **sprints OC2G** convierten prioridades en controles y capacidades.
- **Validación: «Red Team Starter»** comprueba exposición y rutas de abuso dentro de un alcance autorizado; también puede **simular escenarios adversarios para cultura de seguridad**, apoyar ejercicios de caza de amenazas y validar si una restauración o control defensivo deja evidencia útil.
- **Continuidad y especialización: «Mesa Operativa»** conserva seguimiento y decisión recurrente. **«Criptoactivos y Custodia»** atiende gobierno de tesorería digital, soberanía operativa y seguridad blockchain con límites propios de acceso, custodia y responsabilidad financiera.

3.2 – Dependencias explícitas

La dependencia más común es la visibilidad. No puede afirmarse cobertura de **endurecimiento** si no existe una lista razonable de activos; no puede diseñarse **segmentación** sin entender flujos; no puede evaluarse **recuperación** sin identificar servicios, datos, responsables y tolerancias; no puede ejecutarse una **prueba ofensiva** sin autorización y superficie delimitada.

Hacer visible una dependencia no significa bloquear todo avance hasta alcanzar perfección. Significa declarar qué se sabe, qué se asume y qué limitación afecta la confianza del resultado. **Un alcance parcial puede ser útil si no se presenta como cobertura total.**

3.3 – Transiciones entre servicios

Un cliente puede comenzar con **«Diagnóstico OC2G Express»** y continuar con un **sprint** por dominio, **«Blue Team Starter», «Arquitectura y Segmentación» o «Mesa Operativa».** También puede iniciar directamente en un servicio especializado **cuando ya dispone de inventario, responsables y una necesidad suficientemente delimitada.** En ambos casos, la transición debe heredar evidencia útil y no reiniciar el análisis sin motivo.

La continuidad no es una venta automática. Se propone cuando existe un pendiente definido, un resultado que debe sostenerse o una nueva pregunta que justifica otro alcance. **El cierre de cada servicio debe permitir al cliente detenerse, operar por cuenta propia o avanzar con información suficiente.**

3.4 – Matriz rápida del portafolio

La siguiente referencia ayuda a ubicar cada servicio antes de leer el catálogo detallado. **No sustituye una calificación de alcance:** resume la pregunta que atiende, la relación con **OC2G**, el perfil típico de adopción y el entregable principal que debe quedar al cierre.

Para leer la matriz desde este punto: **Perfil A** describe **micro/PYME** sin área formal de **TI** o con operación muy compacta; **Perfil B** describe **PYME** con equipo pequeño de **TI**; **Perfil C** describe **mediana empresa con equipo de TI más establecido**. La sección 8.6 retoma estos perfiles como criterio de adopción.

Servicio	Pregunta que responde	OC2G / perfil típico	Entregable principal
01 Diagnóstico OC2G Express	¿Dónde estamos y qué debe atenderse primero?	D1-D4 / A-B-C	Matriz, hallazgos y hoja de ruta 30/60/90
02 OC2G por Dominio	¿Cómo convertimos una prioridad en capacidad operativa?	Dominio elegido / A-B-C	Sprint con criterios de cierre y evidencia
03 Blue Team Starter	¿Qué telemetría y endurecimiento mínimo necesitamos operar?	D1-D2 / A-B	Cobertura defensiva y lista priorizada
04 Red Team Starter	¿Qué puede explotarse y qué cultura o detección debemos reforzar?	D3 / B-C	Reporte, rutas de abuso y escenarios controlados
05 Mesa Operativa	¿Cómo sostenemos evidencias, pendientes y decisiones?	D4 / A-B-C	Lista priorizada viva, métricas y decisiones
06 Arquitectura y Segmentación	¿Qué flujos deben existir y qué confianza debe reducirse?	D1-D2 / B-C	Diagramas, matriz de flujos y plan de cambio
07 Respaldos y Recuperación Operativa	¿Podemos restaurar lo crítico con objetivos claros?	D1-D4 / A-B-C	RPO/RTO, pruebas y guía de recuperación
08 Criptoactivos, Custodia y Soberanía	¿Cómo entender, usar y gobernar activos digitales sin exponer secretos?	Especializado / A-B-C	Ruta de conocimiento, mapa de custodia y hoja de ruta

4 — Catálogo de servicios

4.1 – OC2G EXPRESS | Diagnóstico OC2G Express

«Diagnóstico OC2G Express» es la oferta de entrada para organizaciones que reconocen riesgos o controles parciales, pero no tienen una secuencia defendible de prioridades. Su función no es vender una herramienta ni producir una lista aislada de hallazgos: establece una lectura inicial de visibilidad, control, exposición y gobierno para decidir qué construir primero.

Cuando aplica: cuando dirección necesita justificar inversión, cuando TI tiene demasiados pendientes sin orden, cuando un cliente exige evidencia mínima o cuando existe preocupación por accesos, respaldos, exposición o cumplimiento, pero no hay una línea base común.

Qué revisa: activos conocidos, dependencias críticas, identidad y privilegios, configuración y endurecimiento observable, exposición externa básica, respaldo y recuperación declarada, evidencia disponible, responsables y criterios de gobierno. La profundidad se ajusta al alcance autorizado y al perfil de adopción del cliente.

Qué entrega: reporte ejecutivo, matriz de madurez **OC2G**, hallazgos priorizados, evidencia resumida, limitaciones de confianza, hoja de ruta 30/60/90 y recomendación de siguiente sprint. **Su valor está en separar urgencia, importancia y dependencia: una condición crítica no siempre es la primera acción si antes falta control sobre activos, identidades o continuidad.**

Qué no promete: no sustituye una auditoría regulatoria, un pentest profundo, una certificación ni una implementación. El cierre debe permitir detenerse con claridad, operar internamente o avanzar a servicios de la cartera según la evidencia.

4.2 – OC2G X DOMINIO | OC2G por Dominio

«OC2G por Dominio» convierte una prioridad concreta en un sprint de construcción o mejora dentro de **D1, D2, D3 o D4**. Puede partir de **un «Diagnóstico OC2G Express»** o de evidencia equivalente proporcionada por el cliente. **Si esa evidencia no existe, el servicio inicia con una delimitación breve para evitar implementar controles sobre supuestos.**

D1 - Observa no es una lista de activos: es la capacidad de saber qué existe, quién lo posee, qué función cumple, dónde vive, de qué depende y qué tan confiable es esa información.

D2 - Controla no es solo MFA: es el gobierno de identidades humanas, dispositivos, cuentas privilegiadas y cuentas de servicio, con privilegios justificados, configuración segura y capacidad de revocación.

D3 - Caza no es únicamente un escaneo: es la validación continua de exposición, vulnerabilidades, rutas probables de abuso, señales defensivas y brechas entre activos descubiertos y activos realmente controlados.

D4 - Gobierna no es documentación por cumplir: es el mecanismo que convierte evidencia en políticas mínimas, métricas, aceptación de riesgo, responsables, auditoría y mejora continua.

Cada **sprint** define un estado objetivo, entradas requeridas, responsables, alcance de activos, criterios de aceptación y evidencia mínima. La implementación puede combinar documentación, configuración, revisión, automatización ligera, validación y transferencia operativa.

Qué entrega: guía de dominio, matriz de objetos, lista priorizada, cambios aplicados o recomendados, evidencias, pendientes fuera de alcance y criterio de cierre. **Cuando corresponde, cada objeto operativo conserva trazabilidad mediante identificadores internos de trabajo.**

Qué no promete: no equivale a implementar todo **OC2G** ni a resolver todos los dominios. Su propósito es avanzar una capacidad delimitada sin perder la relación con el programa completo. Si el dominio depende de visibilidad o autorización inexistente, esa limitación se declara antes de ejecutar.

4.3 – BLUE STARTER | Blue Team Starter

«Blue Team Starter» construye una base defensiva proporcionada al entorno: telemetría útil, endurecimiento, revisión de accesos, configuraciones seguras y criterios básicos de atención. No busca instrumentar cada activo ni generar el mayor volumen posible de alertas; busca producir señales que alguien pueda interpretar y controles cuyo estado pueda verificarse.

Cuando aplica: cuando la organización tiene herramientas dispersas, agentes sin lectura operativa, logs que nadie revisa, endpoints críticos sin línea base (baseline) o servicios importantes cuya configuración depende del conocimiento informal. **Es especialmente útil después de un diagnóstico o cuando ya existen activos prioritarios definidos.**

Qué puede incluir: selección de fuentes de logs, endurecimiento de endpoints y servidores críticos, revisión de cuentas privilegiadas, línea base de configuración, reglas o criterios iniciales de detección, documentación de cobertura y recomendaciones para operación mínima.

Qué entrega: lista de activos cubiertos, cambios aplicados o recomendados, fuentes habilitadas, evidencia técnica, limitaciones, lista priorizada de trabajo defensivo y criterios de seguimiento. La entrega debe dejar claro qué señal importa, quién debe revisarla y qué decisión debe detonar.

Qué no promete: no reemplaza un SOC, un EDR administrado ni una respuesta 24/7 a incidentes. Sin seguimiento posterior, la telemetría envejece, el endurecimiento se degrada y las excepciones se vuelven invisibles; **por eso puede continuar con «Mesa Operativa», «OC2G por Dominio» o una validación ofensiva autorizada.**

4.4 – RED STARTER | Red Team Starter

«Red Team Starter» evalúa superficie externa, aplicaciones o infraestructura para determinar qué condiciones son explotables, qué señales defensivas aparecen y qué decisiones deben tomarse. Su valor no está en dramatizar una intrusión, sino en conectar una ruta de abuso plausible con evidencia, impacto técnico, prioridad operativa, remediación y aprendizaje organizacional.

Cuando aplica: cuando existe una superficie autorizada, un aplicativo expuesto, presión de cliente, necesidad de validar controles o dudas sobre qué tan explotable es una condición observada. También puede usarse después de implementaciones de seguridad para comprobar si la defensa implementada produce evidencia útil, para apoyar ejercicios de **caza de amenazas** en equipos **SOC**, o para validar si procedimientos de restauración y continuidad responden ante escenarios adversarios razonables.

Requisitos mínimos: autorización escrita, alcance técnico exacto, reglas de participación (**ROE**), ventanas, contacto de emergencia, condiciones de paro, exclusiones y manejo de evidencia. La ausencia de cualquiera de estos elementos impide ejecutar. Cuando el alcance incluya cultura de seguridad, las simulaciones se diseñan como ejercicios controlados de aprendizaje, no como humillación pública ni vigilancia encubierta.

Qué puede incluir: evaluación de exposición externa, pruebas web o de infraestructura, simulación adversarial, simulaciones controladas de phishing e ingeniería social, ejercicios de concientización sobre malware y sesiones de sensibilización, validación de alertas defensivas, apoyo a la caza de amenazas y repetición de prueba para verificar correcciones cuando se acuerde.

Qué entrega: resumen ejecutivo, reporte técnico, evidencia sanitizada, rutas probables de ataque, severidad, prioridad operativa, recomendaciones, lista priorizada de remediación, aprendizajes para cultura de seguridad y señales esperadas para equipos defensivos.

Qué no promete: no garantiza ausencia de vulnerabilidades, no autoriza pruebas fuera de alcance y no busca persistencia, movimiento lateral o acceso a información que no sean necesarios para demostrar el riesgo acordado. La prueba termina donde termina la autorización.

4.5 – MESA OPERATIVA | Mesa Operativa

«Mesa Operativa» proporciona seguimiento recurrente para organizaciones que necesitan sostener prioridades, coordinar responsables y convertir evidencia dispersa en decisiones periódicas. **Es la pieza que evita que un diagnóstico, sprint o validación se convierta en un documento archivado.**

Cuando aplica: cuando existe una hoja de ruta, lista priorizada, hallazgos abiertos, varias áreas involucradas o presión de auditoría, cliente o dirección. También aplica cuando el equipo interno ejecuta parte del trabajo (o nada) pero necesita criterio, estructura y seguimiento externo.

Qué puede incluir: revisión de avances, gestión de evidencias, priorización mensual, minutas ejecutivas, actualización de riesgos, políticas mínimas, procedimientos, playbooks, seguimiento de remediación, preparación de decisiones y soporte especializado.

Qué entrega: lista priorizada viva, matriz de pendientes, decisiones registradas, evidencias validadas, métricas útiles, escalamiento oportuno y documentación lista para sostener operación o auditoría. El resultado no se mide por número de reuniones, sino por pendientes cerrados con evidencia y riesgos con responsable.

Qué no promete: no sustituye una mesa de ayuda general, un SOC, administración integral de sistemas ni responsabilidad operativa del cliente.

4.6 – NETWORKING SEGMENTACION | Arquitectura y Segmentación

«Arquitectura y Segmentación» ordena la arquitectura de conectividad para reducir confianza implícita, limitar movimiento lateral y hacer comprensibles los flujos entre usuarios, dispositivos, servicios y zonas. La segmentación no consiste únicamente en crear **VLANs** o reglas: requiere entender dependencias, administración, resolución de nombres, autenticación, monitoreo y continuidad.

Cuando aplica: cuando la red creció de forma orgánica, existen accesos amplios, se incorporan sedes o servicios, hay reglas de firewall difíciles de justificar o un hallazgo revela que la arquitectura amplifica el impacto.

Qué puede incluir: inventario lógico, revisión de topología, matriz de flujos, propuesta de zonas, reglas priorizadas, revisión de firewall y ACLs, validación de administración remota, respaldo de configuración, plan de migración y mecanismos de reversa.

Qué entrega: diagramas actualizados, matriz de flujos permitidos, riesgos de arquitectura, cambios recomendados, plan de implementación por ventanas, evidencias de validación y excepciones documentadas. Cuando incluye implementación, el control de cambio forma parte del alcance.

Qué no promete: no garantiza aislamiento absoluto ni elimina la necesidad de identidad, monitoreo o operación. **Una segmentación sin documentación y sin dueño se degrada con cada excepción**; por eso puede conectarse con **D1, D2**, «**Blue Team Starter» o «Mesa Operativa».**

4.7 – RESPALDOS | Respaldos y Recuperación Operativa

«Respaldos y Recuperación Operativa» transforma la existencia de copias en una capacidad de recuperación verificable. Parte de servicios y datos críticos, objetivos de punto de recuperación **(RPO)**, objetivos de tiempo de recuperación **(RTO)**, retención, rotación, responsables y dependencias necesarias para restaurar.

Cuando aplica: cuando existen tareas de respaldo no probadas, restauraciones que dependen de una sola persona, servicios críticos sin **RPO/RTO**, copias sin aislamiento suficiente o dudas sobre qué ocurriría ante **ransomware, error humano o pérdida de infraestructura.**

Qué puede incluir: arquitectura de respaldo, cobertura de datos críticos, revisión de accesos, copias fuera de línea o inmutables cuando sean viables, monitoreo de tareas, documentación de restauración, pruebas controladas y matriz de dependencias.

Qué entrega: cobertura y exclusiones, **RPO/RTO** acordados, resultados de pruebas, evidencia de restauración, limitaciones, costos operativos relevantes, responsables y guía de recuperación. **Una tarea exitosa no demuestra por sí sola que el servicio puede recuperarse; la validación debe considerar integridad, tiempo, permisos y secuencia.**

Qué no promete: no ofrece recuperación garantizada, no sustituye al propietario del dato y no elimina la necesidad de pruebas periódicas. **Si las pruebas no se repiten, la capacidad se degrada cuando cambian sistemas, usuarios, proveedores o volumen de información.**

4.8 – CRIPTO | Criptoactivos y Custodia

Es una especialidad independiente para personas u organizaciones que necesitan comprender, usar o gobernar activos digitales sin entrar a ciegas en un ecosistema que todavía está madurando. El servicio no parte de recomendar compra o venta: parte de construir criterio técnico, lectura de riesgos, privacidad proporcional, control de secretos y capacidad de decidir con más soberanía.

La ruta de fundamentos puede cubrir historia de Bitcoin y del protocolo Bitcoin, el problema que buscaba resolver, eventos macroeconómicos y tecnológicos relevantes (históricos), tipos de criptoactivos, filosofía y tesis de redes principales, blockchain, protocolos de consenso, contratos inteligentes, stablecoins y usos como ahorro, pagos, remesas o tesorería. El objetivo es que el cliente entienda qué promete cada arquitectura, qué riesgos introduce y qué supuestos debe aceptar antes de usarla.

La ruta de mercados explica P2P, CEX, DEX y OTC; ejecución, liquidación, spot, futuros, apalancamiento, contraparte, comisiones, liquidez y mecánica operativa de trading. Puede incluir lectura educativa de indicadores como presión de compra/venta, funding rate, open interest e históricos mensuales, siempre como alfabetización de mercado y gestión de riesgo, no como señal de entrada, recomendación financiera, promesa de rendimiento ni administración de portafolio.

La ruta de usos de tecnología aborda aplicaciones de blockchain, Web3, tokenización, protocolos para IA, mercados de predicción, identidad descentralizada, NFT y otros casos de uso reales o emergentes. El criterio de análisis no es entusiasmo por la novedad, sino utilidad, permisos, custodia, dependencia de terceros, superficie de ataque, sostenibilidad operativa y valor verificable para una persona u organización.

La ruta de privacidad y soberanía aborda trazabilidad, autocustodia, billeteras (wallets), multisig, modelos de recuperación, segregación de roles, dispositivos, listas de retiro, permisos, API keys, continuidad y escenarios de pérdida o compromiso. Cuando ya existe exposición, **MilpaSec** puede revisar CEX/DEX, billeteras, permisos, firma, concentración y continuidad. No solicita seed phrases, llaves privadas, códigos de recuperación, credenciales, tokens de sesión ni otros secretos; trabaja con evidencia sanitizada y demostraciones controladas.

Los entregables pueden incluir ruta de conocimiento, mapa del ecosistema relevante, criterios de plataforma y contraparte, mapa de custodia y tesorería, matriz de roles, escenarios de pérdida o compromiso, checklist de privacidad y hoja de ruta de soberanía y control. No incluye custodia de fondos, administración de inversiones, ejecución de operaciones por cuenta del cliente ni asesoría financiera, fiscal o legal final.

5 — Entregables, evidencia y trazabilidad

5.1 – Dos niveles de lectura

Los entregables deben permitir que dirección decida sin ocultar la base técnica y que el equipo técnico actúe sin perder el contexto de negocio. Por eso se separan, cuando el alcance lo justifica, un reporte ejecutivo y un reporte o anexo técnico. El primero explica estado, impacto, prioridad, dependencias y decisiones. El segundo conserva alcance, método, evidencia, limitaciones y detalle de remediación.

Otros entregables pueden incluir matriz de madurez, inventario, diagramas, lista priorizada, bitácora de cambios, resultados de restauración, matriz de flujos, hoja de ruta 30/60/90 o propuesta de siguiente sprint. La lista exacta depende del **SOW**; mencionar un artefacto en este paper no lo incorpora automáticamente a todos los servicios.

5.2 – Evidencia proporcional

La evidencia debe ser suficiente para sostener una afirmación y mínima para reducir exposición innecesaria. Una captura, salida de herramienta o fragmento de configuración adquiere valor cuando incluye origen, fecha, alcance, interpretación y limitación. Acumular datos sin propósito aumenta riesgo de custodia y dificulta distinguir lo relevante.

Cuando una condición no puede verificarse directamente, se declara la fuente y el nivel de confianza. La ausencia de evidencia no siempre demuestra ausencia de control; puede significar que el alcance, acceso o tiempo no permitieron confirmarlo. Esa diferencia debe permanecer visible.

5.3 – Trazabilidad operativa

La trazabilidad operativa conecta objetos relacionados sin convertir el reporte en una tabla ilegible. Un hallazgo conserva un identificador; las evidencias y recomendaciones asociadas pueden referenciarlo; una

acción de la hoja de ruta puede heredar la relación; una decisión de aceptación de riesgo puede conservar vínculo con el objeto original.

La estabilidad del identificador no congela la comprensión. El título puede mejorar y la prioridad puede cambiar con nueva evidencia. Si el objeto cambia de forma sustancial, se crea uno nuevo y se conserva la relación histórica.

5.4 – Hoja de ruta y criterio de cierre

Una hoja de ruta útil distingue urgencia inmediata, construcción de capacidad y mejoras posteriores. El horizonte 30/60/90 no es una promesa universal de tiempo: es una forma de ordenar decisiones conforme a dependencias, esfuerzo, riesgo y responsables.

El cierre verifica entregables acordados, limitaciones, pendientes y aceptación. Cuando existe implementación, también debe quedar claro qué fue aplicado, qué requiere monitoreo y qué condición obliga a revisar o revertir.

El cierre también debe declarar qué puede degradarse si no existe seguimiento: inventarios que envejecen, reglas que acumulan excepciones, respaldos no probados, cuentas que conservan privilegios y evidencias que pierden vigencia. Nombrar esa degradación no es presión comercial; es una condición técnica para que el cliente decida si operará internamente o si requiere **«Mesa Operativa».**

6 — Ciclo de una intervención

6.1 – Calificación y alcance

La intervención comienza determinando problema, propietario, activos, restricciones, urgencia y resultado esperado. Esta fase evita ofrecer una prueba ofensiva cuando se necesita inventario, instrumentar telemetría sin responsable o diseñar respaldos sin objetivos de recuperación. También identifica requisitos de confidencialidad, autorización y acceso.

El alcance final se expresa en una propuesta o **SOW** con inclusiones, exclusiones, supuestos, entregables, calendario, responsabilidades y criterios de aceptación. Las ambigüedades que cambien riesgo, esfuerzo o autorización se resuelven antes de ejecutar.

La cotización se define por alcance, profundidad técnica, criticidad operativa, evidencia requerida, ventanas de trabajo, número de activos o dominios incluidos, nivel de acompañamiento y responsabilidades asumidas por cada parte. Este paper no publica precios porque la economía real de la intervención depende de esos factores y debe quedar expresada en propuesta o **SOW**.

6.2 – Preparación y kickoff

Antes de comenzar se confirman contactos, canales, ventanas, evidencia inicial, accesos temporales, manejo de incidentes y dependencias. El **kickoff** alinea lenguaje y decisiones: quién puede aprobar un cambio, quién recibe un hallazgo sensible, qué ocurre si aparece un riesgo crítico y cómo se documenta una desviación del alcance.

6.3 – Ejecución y control de cambios

Durante la ejecución se registra qué se revisa o modifica, con qué evidencia y bajo qué limitación. Los cambios que amplían activos, profundidad, ventanas o impacto potencial se evalúan antes de incorporarse. En actividades técnicas se priorizan mecanismos de reversa, mínima exposición y comunicación proporcional al riesgo.

Un avance no se reporta únicamente como porcentaje. Debe indicar objetos completados, decisiones pendientes, impedimentos y efecto sobre el criterio de cierre.

6.4 – QA, entrega y sesión de cierre

Antes de entregar se revisan consistencia de alcance, trazabilidad, lenguaje, evidencia, severidad, prioridad, límites y recomendaciones. Un hallazgo no debe exagerar impacto ni esconder incertidumbre. Una recomendación debe ser ejecutable o declarar qué decisión previa necesita.

La sesión de cierre explica resultados, responde preguntas y confirma aceptación o pendientes. El cliente recibe una ruta comprensible para operar, remediar o profundizar. La continuidad se propone después de explicar qué valor adicional produciría.

7 — Ejecución responsable y límites

7.1 – Autorización y reglas de participación (ROE)

MilpaSec trabaja únicamente sobre activos y procesos respecto de los cuales el cliente puede demostrar autoridad. Las actividades ofensivas requieren autorización escrita y reglas de participación (**ROE**) antes de iniciar. El alcance identifica objetivos, exclusiones, técnicas permitidas, ventanas, contacto de emergencia y condiciones de paro.

Una solicitud de evaluar, acceder, vigilar o recuperar información de terceros sin autorización no se ejecuta. **La urgencia comercial no sustituye el consentimiento ni amplía permisos técnicos.**

7.2 – Minimización y custodia de evidencia

Se recolecta la evidencia necesaria para demostrar el resultado acordado, no todo lo que una herramienta permita obtener. **Credenciales, secretos, llaves privadas, seed phrases, tokens, contenido personal o bases completas no se solicitan como insumo normal.** Si aparece información sensible de forma incidental, se limita exposición y se aplica el canal acordado.

Los plazos de conservación, transferencia y destrucción deben definirse contractualmente cuando el tipo de servicio lo requiera.

7.3 – Límites de las afirmaciones

Una evaluación representa el alcance, tiempo y evidencia disponibles. No prueba ausencia total de vulnerabilidades, no garantiza que un incidente no ocurrirá y no certifica cumplimiento salvo que un servicio y una autoridad competente lo establezcan expresamente. La seguridad es una condición operativa que cambia con el entorno.

MilpaSec distingue severidad técnica de prioridad operativa. Una condición puede ser técnicamente grave, pero requerir una dependencia previa; otra puede tener severidad moderada y merecer atención inmediata por alcance, facilidad de abuso o criticidad del activo. La recomendación debe explicar esa lógica.

7.4 – Límites especializados

«Red Team Starter» no se ejecuta sin **ROE** y condiciones de paro. «**Criptoactivos y Custodia»** no implica recibir fondos, operar billeteras, ejecutar estrategias de trading ni custodiar secretos. **«Respaldos y Recuperación Operativa»** no promete recuperación absoluta: define y prueba capacidades bajo escenarios acordados. **«Mesa Operativa»** no sustituye un servicio de respuesta a incidentes permanente si ese alcance no fue contratado.

7.5 – Criterios de no ejecución

MilpaSec puede rechazar o pausar una solicitud cuando no exista autoridad demostrable sobre los activos, cuando el alcance sea ambiguo, cuando se solicite acceso a terceros sin autorización, cuando el cliente pretenda omitir reglas de participación (**ROE**) o cuando la evidencia requerida implique recolectar secretos innecesarios.

También puede detener un trabajo si aparecen condiciones no declaradas que cambian el riesgo, si un cambio operativo amenaza continuidad sin ventana aprobada, si se detecta conflicto legal o si la solicitud desplaza el servicio hacia custodia de fondos, operación financiera, vigilancia no autorizada o recuperación de información ajena.

Rechazar o pausar no es falta de flexibilidad: protege al cliente, a terceros y a MilpaSec. La urgencia comercial no sustituye autorización, evidencia mínima, responsabilidad definida ni límites técnicos claros.

8 — Rutas de adopción

8.1 – Cuando no existe una prioridad clara

«Diagnóstico OC2G Express» es el punto de entrada recomendado cuando la organización tiene múltiples preocupaciones, evidencia fragmentada o presión para invertir sin una lectura común. El resultado permite decidir si el siguiente paso debe ser identidad, arquitectura, defensa, exposición, continuidad o gobierno.

8.2 – Cuando el problema ya está delimitado

«OC2G por Dominio» es apropiado si existe evidencia suficiente y una capacidad concreta por construir. «**Blue Team Starter»** sirve cuando la prioridad es defensa mínima y telemetría; «**Arquitectura y Segmentación»** cuando los flujos y la confianza de red amplifican riesgo; **«Respaldos y Recuperación Operativa**» cuando la continuidad necesita objetivos y pruebas.

8.3 – Cuando se necesita validar exposición

«Red Team Starter» responde si la pregunta es qué puede explotarse dentro de una superficie autorizada y qué ruta de abuso merece remediación. Puede seguir a una fase defensiva para probar controles o comenzar de forma independiente si existen propiedad, alcance, autorización y condiciones técnicas suficientes.

8.4 – Cuando el reto es sostener

«Mesa Operativa» es adecuada cuando ya existe una lista priorizada, varias personas deben coordinar decisiones o los controles se degradan por falta de seguimiento. Puede sostener resultados de un diagnóstico, una implementación, una prueba ofensiva o un programa ya existente.

8.5 – Cuando se necesita comprender y gobernar activos digitales

«Criptoactivos y Custodia» se considera tanto para construir criterio desde cero como para gobernar una exposición existente. La ruta puede comenzar en Bitcoin, fundamentos de blockchain, tipos de activos, mercados, privacidad, Web3 y usos reales de tecnología, y avanzar hacia plataforma, contraparte, firma, autocustodia, recuperación y continuidad. Es independiente de **OC2G** y mantiene fuera del alcance las recomendaciones de inversión, la ejecución por cuenta del cliente y las decisiones fiscales o legales finales.

8.6 – Criterio para elegir

El mejor punto de entrada es el servicio más pequeño que pueda responder la pregunta real sin ocultar dependencias críticas. Como orientación transversal:

Perfil A - describe micro/PYME sin área formal de TI.

Perfil B - PYME con equipo pequeño de TI.

Perfil C - mediana empresa con equipo de TI más establecido.

Los perfiles no prescriben herramientas ni presupuesto: ayudan a calibrar profundidad, evidencia, cadencia y expectativas. Si la pregunta aún no puede formularse con activos, responsables y resultado esperado, el punto de entrada más sano suele ser «**Diagnóstico OC2G Express».**

9 – Referencias

MilpaSec. **OC2G** Cybersecurity Framework. **FRM-OC2G-GEN-001**, versión 1.0, 2026.

National Institute of Standards and Technology. The **NIST** Cybersecurity Framework (**CSF**) 2.0. 2024.

Center for Internet Security. CIS Critical Security Controls, Version 8.

International Organization for Standardization. **ISO/IEC 27001:2022**, Information security management systems — Requirements.

MITRE. ATT&CK: Adversarial Tactics, Techniques, and Common Knowledge.

OWASP Foundation. **OWASP** Top 10: The Ten Most Critical Web Application Security Risks.