

INICIATIVA: PROTOCOLO DE SEGURIDAD 120M

RAZÓN SOCIAL: ENGINEERING INVERSE CORP S.A. DE C.V. RFC: EIC2212275C3 PÁGINA: www.eicacademy.mx
TELÉFONO: 664 219 5591 WHATSAPP: 686 188 4648 CORREO: jesuscampos@eicacademy.mx
DIRECCIÓN: AV. REPÚBLICA DE BRASIL 598 INT. 7, COL. CUAUHTÉMOC, C.P. 21200, MEXICALI B.C.

1. RESUMEN EJECUTIVO

Esta Iniciativa propone dotar a las personas suscriptoras de un Protocolo de Seguridad, capacitación tecnológica y un esquema de evidencia trazable (generación, resguardo y entrega). Con ello, y en coordinación con las autoridades competentes, se busca contribuir a la reducción de la incidencia delictiva y a la prevención de la privación ilegal de la libertad, mediante tiempos de respuesta definidos y mecanismos de verificación.

ETAPA 1: Entrega oficial del protocolo sin respaldo.

ETAPA 2: Inicia enlace con la autoridad local.

ETAPA 3: Se trabaja en colaboración con autoridad local.

ETAPA 4: Autonomía del proceso.

Más información en <https://www.eicacademy.mx/protocolo-de-seguridad-120m>

2. OBJETIVOS DEL PROYECTO

A).- Sistema (Software, apps y hardware)

Desarrollar e implementar un sistema que sistematice los procesos del Protocolo de Seguridad 120M, incorporando funcionalidades avanzadas hoy no implementadas, para fortalecer la seguridad y la privacidad de los datos personales mediante cifrado en la nube (en tránsito y en reposo) y controles de acceso basados en roles. Con ello, ofrecer un servicio confiable y escalable, capaz de adaptarse a las necesidades cambiantes de las personas usuarias y a los requerimientos operativos, manteniendo tiempos de respuesta definidos y evidencia verificable.

B).- Puntos de Atención y Servicio Técnico (P.A.S.T.):

Establecer una red territorial de puntos de atención y servicio técnico por delegación para:

- Tener contacto directo con el cliente (proximidad ≤ 2.5 km en zonas urbanas).
- Capturar necesidades locales y adaptar inventario/servicios por distrito.
- Generar empleo en cada sector (ventas, técnico, cambaceo, logística).
- Reducir tiempos de respuesta y costo de última milla.
- Instalar plataformas vertiport para Drones en cada sucursal.

C).- Central de Monitoreo (CM)

Establecer una Central de Monitoreo por localidad encargada de recabar, resguardar, analizar y compartir información con el sistema de seguridad pública, como complemento operativo para la prevención, atención y seguimiento de incidentes.

Propósitos específicos.

- Complementar la operación del sistema de seguridad pública.
- Recabar evidencias complementarias para investigaciones (bitácoras, georreferencias, imágenes, metadatos, testimonios documentados).
- Asegurar el resguardo y entrega oportuna de la información a las autoridades.

D).- Departamento de Seguridad e Inteligencia (D.S.I.)

- Establecer un Departamento de Seguridad e Inteligencia (DSI), orientado a la protección integral de sucursales, personal y clientela, y a la coadyuvancia con autoridades, con apego estricto al marco legal.

3. ALCANCE DEL PROYECTO

A).- Sistema (Software, apps y hardware):

- **Geovallas:** alta/edición de zonas; clasificación por nivel de riesgo; reglas por zona (avisos, escalamiento, restricciones).
- **Asistencia audiovisual:** apoyo en llamada/videollamada desde zonas de riesgo; bajo cifrado y con consentimiento.
- **Evidencia audiovisual:** generación, resguardo y entrega sólo a autoridad competente vinculada al caso; hash e inmutabilidad (WORM).
- **Rastreo forense:** en investigaciones, reconstrucción de co-presencias (suscriptor–suscriptores) antes/después de incidentes, con consentimiento y base legal.
- **Protocolo de emergencia:** disparadores y escalamiento con tiempos ($MTTA \leq 1$ min, puesta en marcha ≤ 1 min). Sin modificar la ley, las evidencias agilizan actuaciones y coordinación.

B).- Puntos de Atención y Servicio técnico (PAST):

- La apertura de cada sucursal en el mismo lugar donde las personas se suscriben constituye un acto tangible de cumplimiento y un símbolo de respaldo inmediato. No solo representa un punto de atención, sino una señal visible de apoyo y compromiso: el suscriptor ve, experimenta y valida que la promesa se cumple en su propia comunidad.
- Este modelo genera un vínculo emocional positivo, al ofrecer un espacio donde los clientes pueden constatar resultados, recibir acompañamiento y “saborear” el beneficio de su decisión desde el primer día. Con ello, se fortalece la confianza mutua, la pertenencia comunitaria y la lealtad hacia el servicio, al transformar cada sucursal en un testimonio vivo de cercanía, apoyo y cumplimiento.

C).- Central de Monitoreo (CM)

- La CM canaliza alertas, activaciones de protocolo y evidencias verificables hacia las autoridades competentes, conforme a convenios de coordinación y a la normativa aplicable en protección de datos personales y cadena de custodia.
- La CM es responsable de validar, priorizar y correlacionar cada alerta, enlazando geolocalización (GNSS) y contenido audiovisual con los dispositivos de rastreo y expedientes del caso, dejando sello de tiempo y trazabilidad completa.
- Conciencia situacional para la autoridad (en tránsito). La CM provee transmisión audiovisual cifrada y mapa operativo en tiempo real para que las y los oficiales conozcan el contexto desde su punto de partida hasta el punto del suscriptor.
- Automatización con drones. La CM implementará un algoritmo de despacho autónomo de drones para despegar, sobrevolar, recargarse y dirigirse automáticamente a las coordenadas del suscriptor que lo solicite, sujeto a:
 - Geocercas y zonas de no vuelo, verificación de NOTAM/clima, detección y evasión de obstáculos, retorno automático y reserva de batería.
 - Gestión de pads de recarga (turnos y prioridades) y registro de misión (telemetría, video, bitácora y hash de integridad).
 - Cumplimiento de normativa aeronáutica vigente y de privacidad.

D).- Departamento de Seguridad e Inteligencia (D.S.I.)

- Seguridad física y monitoreo 24/7; prevención, disuasión, reacción y resguardo de evidencias verificables.
- Coordinación con autoridades locales, estatales y federales mediante convenios y canales C2/C4/C5, sin sustituir funciones de seguridad pública.
- Desarrollo tecnológico para asegurar cifrado (en tránsito y reposo), controles de acceso por rol, bitácoras de auditoría y cadena de custodia digital.

- Observancia de legalidad, necesidad y proporcionalidad en el uso de la fuerza y respeto a derechos humanos.

4. METODOLOGÍA

4.1 Enfoque general

- **Gobernanza del proyecto (PMO):** Comité con responsables de Legal/Privacidad, Operaciones (PAST/CM/DSI), Tecnología, Seguridad de la Información y RH. Reunión quincenal y reporte mensual.
- **Marcos de trabajo:** Privacy & Security by Design, gestión de riesgos (matriz legal–operativo–tecnológico), SLA/KPI y mejora continua
- **Etapas:** Diagnóstico → Diseño → Piloto → Despliegue → Evaluación (con stage–gates).

4.2 Fases por Etapa.

1. Sistema (Software, apps y hardware)

- **F0 Diagnóstico:** casos de uso, análisis legal de datos, threat modeling, arquitectura inicial (cloud, cifrado en tránsito/reposo, RBAC/MFA).
- **F1 Diseño + MVP:** MVP con alertas + geovallas + ubicación en vivo + registro audiovisual. Ensayo con 1–2 delegaciones.
- **F2 Endurecimiento:** rastro forense (copresencias con base legal/consentimiento), telemetría WORM, rotación de llaves, pruebas de carga.
- **F3 Integración externa:** formatos de entrega a autoridad (según convenios), disponibilidad $\geq 99.5\%$. Cierre de Año 1: sistema en producción y enlace con policía.
- **KPI/SLA:** MTTA ≤ 1 min, TPP ≤ 1 min, latencia de video ≤ 2 s, evidencia completa $\geq 95\%$.

2. P.A.S.T. (Puntos de Atención y Servicio Técnico)

- **F1:** zonificación por demanda y accesibilidad; layouts; accesibilidad física/ comunicacional.
- **F1 (Mes 3–6):** apertura piloto 2–3 PAST; SOPs (recepción, diagnóstico, pick-up/drop-off) y atención incluyente.
- **F2 (Año 2 en adelante):** expansión progresiva a partir de 20,000 suscriptores (ver cronograma).
- **KPI:** espera mostrador ≤ 10 min, resolución básica ≤ 24 –48 h, NPS ≥ 65 , cobertura cambaceo $\geq 90\%$.

3. C.M. (Central de Monitoreo)

- **F0 (Mes 6–9):** SOPs, plantillas, cadena de custodia digital, turnos, cifrado E2E.
- **F1 (Año 3, al llegar a 40k suscriptores):** apertura de la 1ª CM (24/7) con trazabilidad y enlace a C2/C4/C5 (si hay convenio).
- **F2 (Año 4–5):** automatizaciones (colas de casos, analítica de riesgo).
- **SLA:** acuse ≤ 1 min, puesta en marcha ≤ 1 min, expediente a autoridad ≤ 5 min, disponibilidad $\geq 99.5\%$.

4. D.S.I. (Departamento de Seguridad e Inteligencia)

- **F1:** contratación de servicio de seguridad privada con licencias y protocolos de uso de la fuerza/DDHH; coordinación con CM.
- **F1:** madurez operativa (aperturas/cierres, acompañamientos, analítica).
- **F2:** célula de inteligencia (tendencias, MO, OSINT).

Hito drones (Año 4, 50k suscriptores): piloto controlado BVLOS/VLOS donde la norma lo permita; pads de recarga y telemetría integradas; always-on compliance.

5. RECURSOS NECESARIOS

5.1 Humanos

SISTEMA:

- Ingeniería en animación y efectos visuales
- Ingeniería en marketing digital
- Desarrollo y programación
- Ciberseguridad / análisis de riesgos

PAST:

- Gerencia
- Técnico en microsoldadura
- Técnico en remanufactura
- Ventas y Atención al cliente

DSI:

- Proveedor externo (SLA)
- Enlace interno de coordinación

Corporativo:

- Recursos Humanos
- Finanzas
- Compras
- Jurídico
- Ciberseguridad

CM (Central de Monitoreo 24/7):

- 1 Coordinador
- 6–8 Operadores en rotación
- 1 Analista (08:00–18:00)

5.2 Materiales/Infraestructura

SISTEMA:

- Software y plataforma
- Aplicación móvil
- Dispositivos de rastreo
- Servidores / nube
- Redundancia de energía y enlaces

PAST:

- Mobiliario y mostrador
- Estaciones de trabajo
- Kits de diagnóstico
- CCTV
- UPS

CM:

- Video wall / monitores
- Estaciones de monitoreo
- Drones
- Dispositivos de rastreo
- Servidores lógicos (nube)
- Almacenamiento WORM
- Redundancia 24/7

DSI:

- Equipamiento operativo según proveedor externo
- Protocolos
- Servicios especializados bajo SLA

5.3 Tecnológicos

Nube y servicios:

- Orquestación
- Base de datos cifrada
- CDN
- Métricas
- Colas

Plataforma app/web:

- Autenticación MFA
- RBAC
- Geofencing
- Streaming cifrado

Observabilidad:

- Logs inmutables
- SIEM
- Panel de SLA/KPI

Laboratorio:

- Desarrollo de tecnología química y electrónica para drones.

Normatividad y cumplimiento:

- Protección de datos
- Gestión de vulnerabilidades
- Pruebas de penetración periódicas
- Auditorías.

6. CRONOGRAMA TENTATIVO (1–5 años ó 50,000 suscriptores activos)

ETAPA 1 / Sistema (Software, apps y hardware)

- F1: Desarrollo de sistema centralizado.
- F2: Desarrollo de App y funciones avanzadas.
- F3: Sistema robusto de cifrado.

- F4: Ejercicios, pruebas.
- F5: Lanzamiento .

ETAPA 2 / P.A.S.T (Puntos de Atención y Servicio Técnico)

- F1: 3 P.A.S.T en un Radio de 2.5km entre sucursal.
- F2: Plataformas Vertiport para Drones.
- F3: 6 P.A.S.T en un Radio de 2.5km entre sucursal.
- F4: Dispositivos de Rastreo para autoridad local.
- F5: Inician operaciones en coordinacion con autoridades local.

ETAPA 3 / C.M. (Central de Monitoreo)

- F1: Sucursal con control y monitoreo de drones.
- F2: Automatizaciones y autorecargas
- F3: Desarrollo de tecnologia anti inhivision RF para Dron
- F4: Desarrollo de tecnologia ligera y térmica para Dron
- F5: Sobrevuelo 24/7 por perimetros automatizados

ETAPA 4 / D.S.I. (Departamento de Seguridad e Inteligencia)

- F1: Selección y adiestramiento
- F2: Adquisición de equipo táctico
- F3: Primer equipo de servicios especializados bajo SLA
- F4: Automatización de drones y Sistema
- F5: Inicio formal de operaciones bajo el esquema de iniciativa ciudadana (independiente)

7. PRESUPUESTO (modelo paramétrico y rangos)

Nota: valores de referencia en MXN; se ajustan por ciudad, renta, nómina y licencias. Este esquema convierte recursos + cronograma en cifras CAPEX/OPEX y escala por suscriptores.

7.1 CAPEX (inversión)

- **Sistema:** desarrollo inicial y puesta en producción: **\$6–12 M** (equipo propio/mixto).
- **P.A.S.T. por punto (apertura):** adecuación + equipamiento: **\$180–350 mil c/u.**
- **C.M.:** adecuación, monitores, estaciones, redundancias: **\$1.8–3.0 M.**
- **Drones:** 3–6 unidades + pads + software: **\$1.2–2.5 M.**

7.2 OPEX (mensual estimado)

- **Nube/servicios plataforma:** **\$120–200 mil** (escala por uso).
- **Equipo de tecnología (10 FTE):** **\$600–900 mil.**
- **P.A.S.T. (por punto):** nómina **\$90–130 mil**, renta/servicios **\$25–60 mil** → **\$115–190 mil c/u.**
- **C.M. (operación 24/7):** **\$280–420 mil** (personal + conectividad/energía).
- **D.S.I. (proveedor):** **\$150–300 mil** (según cobertura).
- **Drones (si activos):** **\$60–120 mil** (mantenimiento, seguros, licencias).

La información de gastos e inversiones conforme al avance del proyecto serán publicados en <https://www.eicacademy.mx/protocolo-de-seguridad-120m>

8. BENEFICIOS ESPERADOS

- A) **Solución integral y confiable.** Brindar a las personas usuarias una plataforma robusta para el rastreo y recuperación de objetos y personas, integrando tecnología avanzada, protocolos de seguridad y evidencia verificable.
- B) **Seguridad y tranquilidad.** Fortalecer la confianza y la paz mental de los suscriptores, al ofrecerles un sistema completo de reacción sobre lo que consideran más valioso.

- C) **Modelo de negocio sostenible.** Generar ingresos mediante esquemas de suscripción escalables, que permitan garantizar la continuidad del servicio y su constante innovación.
- D) **Posicionamiento de marca.** Construir una marca sólida, confiable y reconocida en el mercado de localización, rastreo y recuperación, con proyección nacional e internacional.
- E) **Compromiso social y nacional.** Consolidarse como una empresa incluyente, que genera oportunidades para adultos mayores, personas con discapacidad y con TEA, y que a la vez contribuye a la seguridad nacional mediante colaboración con autoridades y apego a la normativa vigente.

9. EVALUACIÓN Y SEGUIMIENTO

9.1 Evaluación del Avance de la Iniciativa (Roadmap)

La evaluación del proyecto Protocolo de Seguridad 120M se realizará midiendo el avance de sus fases y la consolidación progresiva de infraestructura, sistema, personal y cobertura.

Elementos evaluados:	Indicadores sugeridos:
• Cumplimiento de fases y etapas. • Implementación y expansión de PAST por distrito. • Apertura y madurez de la Central de Monitoreo. • Integración de drones y laboratorio. • Crecimiento de suscriptores. • Productividad, costos y sostenibilidad financiera. • Cumplimiento de metas 3–6–9–12 meses.	• % de avance por fase. • Recursos instalados vs proyectados. • Suscriptores activos por mes. • Ticket promedio mayorista/usuario. • Breakeven por delegación.

Se establecerán métricas clave de rendimiento KPIs (desempeño, satisfacción e impacto) para evaluar el éxito del proyecto, como el número de usuarios activos, la retención de usuarios, el crecimiento de los ingresos y la satisfacción del cliente. Se realizarán evaluaciones periódicas para realizar ajustes y mejoras según sea necesario

9.2 Evaluación del Funcionamiento del Protocolo de Seguridad 120M (SLA/KPI)

Se evaluará el rendimiento operativo del Protocolo de Seguridad 120M mediante los siguientes indicadores:

- **T0:** instante en que el sistema recibe la alerta.
- **VAS** (Ventana de activación del suscriptor): ≤ 120 minutos desde T0.
Periodo máximo para que la persona suscriptora confirme y active el protocolo.
- **MTTA** (Tiempo medio de acuse): ≤ 1 minuto desde T0.
Acuse automático/operador que confirma la recepción de la alerta.
- **TPP** (Tiempo de puesta en marcha del protocolo): ≤ 1 minuto tras la activación.
Una vez que el suscriptor activa, el protocolo queda operativo en ≤ 60 segundos.
- **EPI** (Evidencia predispuesta): disponibilidad inmediata.
100% de expedientes con evidencia base pre-cargada (fichas del suscriptor, georreferencias, plantillas de reporte, formatos de cadena de custodia).
KPI: publicación/adjunto al expediente ≤ 1 minuto posterior a la activación.
- **MTTR** (Tiempo medio para resultados por autoridad): objetivo ≤ 120 minutos tras la activación.

Resultado = reporte con folio y evidencias remitidas/validadas conforme al protocolo de coordinación.

Nota: este plazo es objetivo de coordinación interinstitucional y queda sujeto a disponibilidad y determinaciones de la autoridad competente o a los convenios que se suscriban.

9.3 Evaluaciones periódicas

- **Mensual:** Tablero integral (SLA/KPI), incidentes, riesgos y acciones correctivas.
- **Trimestral:** Auditoría de seguridad/privacidad, pruebas de carga, revisión legal (convenios).

- **Semestral:** Evaluación de expansión PAST (demanda por distrito, productividad, NPS).
- **Anual:** post-mortem estratégico, ROI, actualización de metas 3–6–9–12 y plan año siguiente.

9.4 Criterios de éxito por hito

- AÑO 1 o 10,000 suscriptores activos – FASE 1 – **SISTEMA** – Etapa 1 - 5.
- AÑO 2 o 20,000 suscriptores activos – FASE 2 – **P.A.S.T.** – Etapa 1 - 5.
- AÑO 3 o 30,000 suscriptores activos – FASE 3 – **C.M.** – Etapa 1 - 5.
- AÑO 4 o 40,000 suscriptores activos – FASE 4A – **INTEGRACIÓN D.S.I.**
- AÑO 5 o 50,000 suscriptores activos – FASE 4B – **D.S.I.** – Etapa 1 - 5.

10. ACLARACIONES

A) Permisos del usuario en la App.

El suscriptor será libre de otorgar o negar permisos en relación con:

- | | | |
|-------------------|----------------------|------------|
| • Notificaciones. | • Ubicación en vivo. | • Rastreo. |
| • Geovallas. | • Cámaras. | • Audio. |

Nota: La negativa a otorgar alguno de estos permisos puede derivar en una reducción en la eficacia de los resultados, ya que para el óptimo desempeño del protocolo de seguridad 120m es indispensable la activación de estas funciones. En caso de no habilitarlas, el servicio se prestará con las limitaciones actuales, sin alcanzar el nivel máximo de prevención y respuesta previsto.

B) Restricciones de acceso.

El sistema no solicitará, bajo ninguna circunstancia, acceso a:

- | | | |
|---------------------------|---|-----------------------------|
| • Fotografías. | • Contraseñas. | • Historial de navegación. |
| • Contactos. | • Correos electrónicos. | • Descargas. |
| • Historial de llamadas. | • Mensajes de texto o mensajería instantánea. | • Aplicaciones de terceros. |
| • Ajustes de dispositivo. | | |

C) Confidencialidad operativa

El suscriptor no podrá visualizar la ubicación en tiempo real de las unidades u operadores. Únicamente recibirá estatus del caso, folio de seguimiento y reportes conforme al protocolo.

D) Colaboración y confidencialidad de la ubicación de la autoridad

- La Central de Monitoreo (CM) no requerirá ni condicionará la operación del protocolo a que las autoridades compartan su geolocalización en tiempo real. La decisión de compartir o no dicha información corresponde exclusivamente a la autoridad competente, conforme a sus propios protocolos operativos y de seguridad.
- Se hace del conocimiento que la ausencia de geolocalización oficial puede limitar la visibilidad operativa y afectar el desempeño (estimaciones de arribo, optimización de rutas, coordinación en tránsito). La respuesta a esta petición de compartir ubicación quedará documentada, y su impacto será evaluado mediante métricas y resultados, sin menoscabo de la autonomía de la autoridad.
- Protección de datos. En caso de que la autoridad decida compartir geolocalización, la CM aplicará medidas de cifrado, controles de acceso por rol y registro de auditoría, utilizándola únicamente para los fines del caso, con retención limitada y cadena de custodia digital.

Nota final: La CM no instruye operativos, no impone obligaciones a las autoridades y actúa como complemento técnico y de coadyuvancia dentro del marco legal aplicable.

11. PETICIÓN (a todo el público en general)

1. EXPOSICIÓN

Engineering Inverse Corp S.A. de C.V., en el marco de la **Iniciativa Protocolo de Seguridad 120M**, autoriza a toda persona física o moral, medio de comunicación o creador de contenido a compartir, difundir o emitir opiniones públicas positivas relacionadas con la iniciativa, siempre que se respeten los siguientes lineamientos:

1. **Citar la fuente original:** se deberá mencionar claramente el nombre de la iniciativa (“Protocolo de Seguridad 120M”) y su titular (“Engineering Inverse Corp S.A. de C.V.”).
2. **No alterar el contenido técnico ni el mensaje oficial**, ni usarlo con fines políticos, partidistas o contrarios a los valores de seguridad y comunidad.
3. **Mantener visibles los enlaces o documentos originales** de EIC, preferentemente dirigiendo a la fuente principal: www.eicacademy.mx/protocolo-de-seguridad-120m
4. **El uso de materiales gráficos, logotipos o documentos oficiales** requerirá autorización escrita previa del titular.

Toda exposición pública que cumpla estas condiciones se considerará una colaboración legítima de difusión ciudadana y será bienvenida como parte del fortalecimiento de esta iniciativa social y tecnológica.

2. RELACIÓN

Esta propuesta se alinea con los objetivos de seguridad y bienestar ciudadano establecidos tanto en el Gobierno de México como en los Estados Unidos, fomentando:

- **Colaboración interinstitucional** para la atención de incidentes.
- **Complemento operativo** a los sistemas de seguridad pública.
- **Generación de empleo incluyente**, incluyendo a personas de la tercera edad, con discapacidad(es) y con TEA.
- **Uso de tecnología avanzada** (cifrado, inmutabilidad, drones automatizados, evidencias digitales) para elevar la eficacia de la coordinación binacional.

3. AGRADECIMIENTOS

Engineering Inverse Corp S.A. de C.V. agradece la atención, el interés y el tiempo dedicado a conocer esta iniciativa.

El **Protocolo de Seguridad 120M** nace con el propósito de fortalecer la unión ciudadana, impulsar la innovación tecnológica en favor de la seguridad y demostrar que la prevención también puede ser ciencia y comunidad.

Gracias por su atención y por formar parte de esta visión.