DATOS PREVIOS PARA REALIZAR ANALISIS E IMPLEMENTACION A MEDIDA

Preguntas de Descubrimiento para Petroil (Modelo de Venta de Soluciones)

5.1. Situación Actual

- ¿Cómo monitorea y protege actualmente Petroil su flota durante el transporte?
- ¿Qué tecnologías tienen ya implementadas (GPS, RFID, ERP, sensores IoT, NFC, cámaras de tablero)?
- ¿Cómo rastrean y responden hoy a las desviaciones de ruta o a la manipulación de la carga?
- ¿Qué sistemas están integrados (ERP, gestión de flotas, monitoreo de seguridad) o están aislados?
- ¿Cómo se recopilan y utilizan los datos de camiones, conductores y depósitos?

5.2. Problemas / Puntos de Dolor

- ¿Cuántos camiones fueron robados o secuestrados el año pasado?
- ¿Cuál es la pérdida promedio por camión robado (valor del vehículo + carga de combustible + tiempo de inactividad + seguro)?
- ¿Cuánto le cuestan estos robos a Petroil por año?
- ¿Cuál es el mayor riesgo operativo en su flota hoy en día: secuestradores externos, colusión de conductores o puntos ciegos en los sistemas?
- ¿Los bloqueadores de señal inhabilitan por completo su rastreo GPS actual?
- Más allá de las pérdidas financieras directas, ¿cómo afectan estos incidentes las primas de seguro, la reputación y la confiabilidad de las entregas?

5.3. Implicaciones (Costo de la Inacción)

- Si los incidentes de robo se mantienen al ritmo actual, ¿cuál será el impacto financiero a 3 años?
- ¿Cómo afecta el robo de combustible la confianza del cliente y el cumplimiento de las normativas?
- ¿Qué impacto tiene el tiempo de inactividad por los camiones robados en las operaciones y los contratos?
- Si las primas de seguro continúan subiendo, ¿cuál será el costo para Petroil en los próximos 1-2 años?

5.4. Necesidades y Resultados Deseados

- Si Petroil pudiera reducir los robos en un 30-50%, ¿cómo cambiaría su estado de pérdidas y ganancias (P&L)?
- ¿Sería valiosa para sus equipos de seguridad y operaciones una plataforma de inteligencia en tiempo real (alertas predictivas, puntuación de riesgos, información basada en IA)?
- ¿Qué tan importante es para Petroil integrar la seguridad de la flota con paneles de inteligencia de negocios para los ejecutivos?
- ¿Qué sería el éxito para ustedes: menos robos, menores costos, mayor seguridad o una transformación digital completa?

5.5. Proceso de Decisión y Criterios de Compra

- ¿Quién tiene el presupuesto para la seguridad de la flota y la transformación digital: Operaciones, Seguridad, TI o Finanzas?

- ¿Quiénes son los tomadores de decisiones clave e influyentes en la selección de nuevos proveedores de tecnología?
- ¿Cuál es el proceso de Petroil para evaluar y aprobar nueva tecnología de seguridad (piloto, solicitud de propuestas, prueba de concepto)?
- ¿Se ha asignado un presupuesto este año para iniciativas antirrobo o de transformación digital? Si es así, ¿cuánto?
- ¿Cuál es el plazo esperado para la implementación (piloto inmediato vs. estrategia a largo plazo)?

5.6. Visión de Futuro

- Más allá de la prevención de robos, ¿qué otros objetivos de transformación digital tiene Petroil en logística y cadena de suministro?
- ¿Está Petroil interesado en la analítica predictiva (anticipar riesgos antes de que ocurran)?
- ¿Un gemelo digital de su red logística (camiones, depósitos, oleoductos) ayudaría en la estrategia a largo plazo?
- ¿Qué tan abierto está Petroil a trabajar con socios tecnológicos para la innovación en lugar de solo comprar herramientas?

5.7 Preguntas sobre fuentes de datos y disponibilidad:

- ¿Qué tipos de datos operativos y de seguridad recopilan actualmente de sus camiones y depósitos?
- ¿Monitorean en tiempo real el comportamiento del conductor, las desviaciones de ruta o la manipulación de la carga?
- ¿Rastrean conversaciones en la web/dark web sobre combustible o camiones robados?

Preguntas sobre integración y sistemas:

- ¿Sus sistemas ERP y de gestión de flotas son capaces de integrar fuentes de datos externas (IoT, monitoreo web, sensores)?
- ¿Tienen un **data lake** o una plataforma de **big data** interna?

Preguntas sobre toma de decisiones y alertas:

- ¿Quién recibe las alertas de robo hoy y cómo se actúa ante ellas?
- ¿Necesitan alertas en tiempo real impulsadas por IA, o prefieren informes programados?
- ¿Se beneficiarían de un único centro de mando que consolide todos los hallazgos?

Preguntas sobre cuantificación de riesgos y pérdidas:

- ¿Cuál es el valor promedio de combustible y camiones perdidos por año?
- ¿Cómo miden actualmente el costo de la inseguridad más allá de los camiones (seguro, reputación, tiempo de inactividad, asuntos legales)?
- Si pudieran reducir los robos en un 30-50%, ¿qué significaría eso financieramente?

Preguntas sobre la visión de futuro:

- Más allá de resolver el robo, ¿estaría Petroil interesado en un gemelo digital completo de sus operaciones logísticas?
- ¿Existe interés en monitorear no solo los camiones, sino también los depósitos de combustible, oleoductos y puntos de distribución?
- ¿Quién en su organización es responsable de la estrategia de transformación digital: es TI, operaciones o estrategia corporativa?

A Evaluar / Pregunta Específica	Cumple (Sí/No/N.A.)	Hallazgo / Respuesta	Observaciones / Nivel de Riesgo (Bajo, Medio, Alto)
1.1. Auditoría de Hardware e Instalación Física			
	Inventario de Dispositivos: ¿Se tiene un listado completo de todos los dispositivos a bordo por unidad? (GPS/AVL, cámaras, módems, sensores, teclados, etc.).		
	Ocultamiento (GPS/Módem): ¿Están los dispositivos críticos instalados en ubicaciones no obvias y de difícil acceso?		
	Ocultamiento (Calidad): ¿La instalación requiere desmontaje de componentes del vehículo para ser alcanzada?		
	Endurecimiento (Cableado): ¿El cableado está protegido y mimetizado con el arnés original del vehículo?		
	Endurecimiento (Fijación): ¿Se utilizan precintos, cajas de seguridad o tornillería especializada (ej. Torx de seguridad) en la instalación?		
	Ubicación de Antenas (GPS/Celular): ¿Están las antenas instaladas de forma encubierta y protegida dentro de la estructura del vehículo?		
1.2. Análisis de Software, Firmware y Configuración			
	Versión de Firmware/SO: ¿Se conoce y documenta la versión de firmware/SO de cada dispositivo inteligente?		
	Política de Actualización: ¿Existe una política y proceso documentado para la actualización y parcheo de firmware?		
	Acceso a Configuración: ¿Se tiene acceso a los archivos de configuración o código para análisis? Si no, ¿existen resultados de auditorías de seguridad externas?		
	Vulnerabilidades Conocidas: ¿Se han identificado vulnerabilidades como credenciales codificadas (hardcoded) o puertas traseras?		
	Control de Acceso (Admin): ¿Quién posee los derechos de administrador para configurar los dispositivos?		
	Auditoría de Acceso: ¿Cómo se controla, audita y revoca el acceso a la configuración de los dispositivos?		
1.3. Suministro Eléctrico y Redundancia			
	Fuente Primaria: ¿Los dispositivos están conectados a un circuito dedicado y protegido con fusibles directamente de la batería?		
	Batería de Respaldo: ¿Los dispositivos críticos (GPS primario, señuelos) cuentan con batería interna de respaldo?		
	Duración Batería Respaldo: ¿Cuál es la duración especificada y probada de la batería de respaldo (ej. 4, 6, 8 horas)?		
	Monitoreo de Batería: ¿Existe un mecanismo para monitorear el estado de salud y nivel de carga de la batería de respaldo?		
	Alerta de Sabotaje Eléctrico: ¿El sistema genera una alerta inmediata de sabotaje al perder la alimentación principal, transmitiendo con la batería de respaldo?		
2.1. Arquitectura de Red y Redundancia			
	Canal Primario: ¿Cuál es el proveedor de red celular principal (ej. Telcel, AT&T)?		
	Redundancia Celular (Dual-SIM): ¿Las SIMs pertenecen a operadores con infraestructura de red independiente en las rutas clave? (Evitar "falsa redundancia")		
	Redundancia Tecnológica: ¿Existe un canal de respaldo satelital que opere en frecuencias distintas?		
	Canales Alternativos: ¿Se utilizan tecnologías adicionales como LPWAN (LoRaWAN, Sigfox) para alertas?		
Lógica de Conmutación (Failover): ¿El cambio al canal de respaldo es automático? ¿Cuál es la latencia (retraso) de esta conmutación?			
2.2. Protocolos de Datos y Seguridad			
	Protocolos de Transmisión: ¿Qué protocolos se utilizan (TCP/IP, UDP, MQTT)?		
	Cifrado en Tránsito: ¿Los datos se cifran desde el vehículo hasta el servidor? ¿Qué estándar se usa (TLS 1.2, AES-256)?		
	Integridad de Datos: ¿Se utilizan sumas de verificación (checksums) para proteger la integridad de los datos contra manipulación?		
2.3. Plataforma y Procesamiento de Datos			
	Tipo de Plataforma: ¿La plataforma de monitoreo es propietaria o de un tercero (ej. Navixy, RedGPS)?		
	Control de Acceso (Plataforma): ¿Existen roles y permisos de usuario bien definidos?		
	Registro de Auditoría: ¿Existe un registro inmutable que documente todas las acciones en la plataforma (quién, qué, cuándo)?		
	Configuración de Alertas: ¿Cómo y quién define las reglas de negocio (geocercas, detección de jammer, etc.)?		
	Responsabilidad 24/7: ¿Está claramente definido y cubierto 24/7 el rol responsable de interpretar alertas y tomar acciones?		
3.1. Protocolos Anti-Jamming			
	Mecanismo de Detección: ¿La detección de jamming es pasiva (reactiva a pérdida de señal) o activa (escaneo de espectro RF)?		
	Diferenciación de Señal: ¿El sistema puede diferenciar fiablemente entre un jammer y una zona sin cobertura (ej. túnel)?		
	Acciones Locales Automatizadas: Al detectar jamming, ¿se activan contramedidas en el vehículo (paro de motor, sirena, bloqueo de puertas)?		
	Comunicación de Alerta: ¿El sistema intenta enviar una alerta de "jamming detectado" por un canal de respaldo (satelital) antes del bloqueo total?		
3.2. Anti-Sabotaje y Dispositivos Señuelo			
	Dispositivo Señuelo ("Canary"): ¿Existe una segunda unidad de rastreo, encubierta y con batería propia?		
	Lógica de Activación del Señuelo: ¿Cómo se activa el señuelo (temporizador, falta de "heartbeat" del GPS principal, etc.)?		
	Alertas de Manipulación (Tamper): ¿Los dispositivos tienen sensores que alertan sobre apertura de carcasa o desconexión?		
3.3. Redundancia de Localización (Anti-GPS Spoofing/Jamming)			
	Navegación Inercial (Dead Reckoning): ¿El sistema incluye una Unidad de Medición Inercial (IMU) con acelerómetros y giroscopios para estimar la posición sin GPS?		
Calidad del Dead Reckoning: ¿Cuál es la tasa de deriva (drift rate) especificada? (ej. % de distancia recorrida o metros/minuto)			

	Pruebas de Campo: ¿Pueden proporcionar datos de pruebas de campo que muestren la precisión del sistema tras 15-30 min de denegación de GPS?		
	Almacenamiento de Ruta Estimada: ¿La ruta estimada durante el jamming se almacena y transmite una vez se recupera la comunicación para análisis forense?		
4.1. Procedimientos del Centro de Monitoreo			
	Certificación del Personal: ¿Los monitoristas tienen alguna certificación de la industria (ej. ANERPV)?		
	SOPs Documentados: ¿Existen y se pueden revisar los Procedimientos Operativos Estándar para cada tipo de alerta (jammer, pánico, sabotaje)?		
	Simulacros Periódicos: ¿Se realizan simulacros periódicos y sin previo aviso para probar los protocolos y al personal?		
	Prueba de Escenario Práctico: (Realizar la simulación) "Jamming a las 3 AM en Arco Norte. Describan paso a paso su actuación en los primeros 15 min."		
4.2. Protocolos y Capacitación del Conductor			
	Capacitación en Amenazas: ¿Se capacita a los conductores para reconocer señales previas a un ataque (vehículos sospechosos, etc.)?		
	Protocolo de Actuación (Asalto): ¿El protocolo principal es claro en priorizar la vida y no oponer resistencia?		
	Uso de Botón de Pánico: ¿Están capacitados para usar el botón de pánico de forma discreta y preventiva? ¿Se entrena la memoria muscular para su uso bajo estrés?		
	Políticas de Operación: ¿Existen y se hacen cumplir políticas estrictas sobre paradas no autorizadas y desvíos de ruta?		
4.3. Gobernanza y Cadena de Mando			
	Cadena de Mando: ¿Está claramente definida y mapeada la ruta de escalamiento para un incidente?		
	Autoridad para Acciones Críticas: ¿Quién tiene la autoridad para aprobar un paro de motor remoto u otras acciones críticas?		
	Enlace con Autoridades: ¿Quién es el enlace designado para coordinarse con las fuerzas del orden?		
	Responsabilidad (Accountability): ¿Quién es el responsable último de la seguridad de la flotilla (Gerente de Seguridad, Logística, etc.)?		
5.1. Integración de Sistemas Internos			
	Integración con TMS/ERP: ¿La plataforma de seguridad está integrada con otros sistemas (TMS, ERP) para contextualizar las alertas?		
	Disponibilidad de API: ¿La plataforma ofrece una API robusta y documentada para permitir integraciones a medida?		
5.2. Colaboración con Autoridades			
	Proceso de Reporte a Autoridades: ¿El proceso actual es una llamada manual al 911 o existe un canal más directo?		
	Certificación ANERPV: ¿El proveedor de seguridad actual es socio certificado y activo de la ANERPV?		
	Integración con Plataforma Centinela: ¿La plataforma de monitoreo está integrada a nivel API y en tiempo real con la "Plataforma Centinela" de ANERPV para un enlace directo con C4/C5 y		
5.3. Contexto Legal y Regulatorio			
	Conocimiento Ley Anti-Jammer: ¿El equipo de seguridad y el proveedor conocen y aprovechan la "Ley Anti-Jammer" en sus reportes a las autoridades?		
	Homologación de Equipos (IFT): ¿Todos los dispositivos de radiofrecuencia están debidamente homologados por el IFT?		