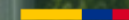




UPME



# Guía EM OCPI 2.2.1

Guía Técnica de Implementación para la  
Interoperabilidad de la  
**Movilidad Eléctrica — Resolución 40559 de 2025**

Subdirección de Gestión de la Información

Junio 2026



# Bienvenidos a la socialización

*Antes de comenzar — el espacio en el que vamos a estar las próximas 2 horas*

**90 min**

## **INTERVENCIÓN**

Recorrido por las 5 fases de la Ruta de Implementación

**30 min**

## **PREGUNTAS TÉCNICAS**

Q&A abierto a CPOs, MSPs y equipos de tecnología

**60+**

## **AUDIENCIA MIXTA**

Presencial en auditorio + transmisión virtual en vivo

**100 %**

## **COMPROMISO UPME**

La guía es viva. Toda retroalimentación cuenta.

*Para hacer preguntas en vivo durante la presentación, levanten la mano (presencial) o usen el chat (virtual). El equipo SIEM responderá al final.*

# Tabla de contenido

01

## Por qué estamos aquí

Resolución 40559 —  
contexto, plazos y actores

02

## FASE 1 — Habilitación legal

Cárgame · Notificación oficial ·  
Emisión de credenciales

03

## FASE 2 — Seguridad y acceso

mTLS · OAuth 2.1 · JWT ·  
Custodia de API Keys

07

## Demo Swagger en vivo (mocks) + cierre

Sandbox · API pública ·  
Consumo ciudadano

04

## FASE 3 — Estructura OCPI 2.2.1

Locations · Sessions ·  
Tariffs · Versions

05

## FASE 4 — Operación y reporte

Modelo basado en eventos  
· Latencia  $\leq 60$  s

06

## FASE 5 — Validación y publicación

Sandbox · API pública ·  
Consumo ciudadano

1

POR QUÉ  
ESTAMOS AQUÍ

# POR QUÉ ESTAMOS AQUÍ — EL PROBLEMA DEL CIUDADANO

Hoy un colombiano con vehículo eléctrico no puede planear un viaje con confianza.

## ¿Dónde cargo?

No existe una fuente única con todas las estaciones del país.

## ¿Cuánto cuesta?

Las tarifas no son comparables entre operadores.

## ¿Estará disponible?

No hay forma de saber el estado real en tiempo real.

LA RESOLUCIÓN 40559 RESUELVE ESTO.

**Una sola plataforma. Un solo estándar. Datos en tiempo real para todos.**

SIEM — Sistema de Interoperabilidad de Electromovilidad · [siem.upme.gov.co](http://siem.upme.gov.co)

# En 5 ideas — para ejecutivos

*Lo que su organización necesita entender de esta socialización, en una sola lámina*

## OBLIGACIÓN LEGAL

Res. 40559 de 2025

Todo CPO de acceso público debe reportar al SIEM bajo OCPI 2.2.1. No es opcional, no es diferible.

## ESTÁNDAR ABIERTO

OCPI 2.2.1

El mismo protocolo que ya usa Europa. Su backend habla un idioma estándar — no inventamos nada propietario.

## SEGURIDAD DE BANCA

mTLS + OAuth 2.1 + JWT

Mismo nivel de seguridad que el sector financiero. La UPME custodia las llaves en HSM FIPS 140-2 L3.

## REPORTE POR EVENTO

Latencia  $\leq 60$  s

El CPO solo envía datos cuando algo cambia. No es polling, no es periódico. Menos carga, más actualidad.

## AYUDA REAL

Sandbox + soporte

Ambiente de pruebas sin riesgo desde Ago/2026. Mesa de ayuda dedicada. Go-live Nov/2026.

# Cadena normativa de la electromovilidad

*La Resolución 40559 cierra un proceso de 6 años*

## 2019

### Ley 1964

Promueve el uso de vehículos eléctricos y de cero emisiones.  
Faculta a MinEnergía a reglamentar.



## 2021

### Res. 40223

Establece condiciones técnicas mínimas: conectores, niveles de carga, acceso público.



## 2024

### Res. 40123

Crea Cárgame — obligación de registro previo de toda estación de acceso público.



## 2025

### Res. 40559

Adopta OCPI 2.2.1 y crea la obligación de reporte en tiempo real al SIEM.

**ESTAMOS AQUÍ** — hoy presentamos el desarrollo técnico (Guía de Implementación) que materializa la Resolución 40559.

# ¿Qué exige la Resolución 40559 de 2025?

*Cinco obligaciones técnicas mandatorias para todo actor del ecosistema*

1

## **Adoptar OCPI 2.2.1**

Protocolo abierto mantenido por la Fundación EVRoaming. Adoptado por Colombia como el único lenguaje técnico oficial entre CPOs, MSPs y el SIEM.

2

## **Reportar al SIEM en tiempo real**

Cada CPO debe transmitir información cuando ocurra un evento relevante en su infraestructura: cambio de estado, sesión iniciada/cerrada, tarifa modificada. Latencia máxima 60 segundos.

3

## **Garantizar interoperabilidad**

Un usuario debe poder cargar en cualquier punto de carga, independientemente del operador. El estándar y la plataforma común lo permiten.

4

## **Habilitar la consulta pública**

Información de precios, disponibilidad y ubicación debe estar disponible en tiempo real para ciudadanos y autoridades, expuesta por la UPME vía API REST.

5

## **Cumplir con seguridad y auditoría**

Cifrado en tránsito y reposo, autenticación multi-capa, audit trail inmutable retención mínima 7 años (Decreto 1080/2015). Supervisión SIC.

# ¿Qué es OCPI?

*El idioma que hablan entre sí los actores del ecosistema de carga eléctrica*

## OPEN CHARGE POINT INTERFACE

Protocolo abierto y gratuito que estandariza cómo se hablan los operadores de carga (CPOs), los proveedores de servicios de movilidad (MSPs) y los hubs centrales — como el SIEM-UPME.

### MANTENIDO POR

## Fundación EVRoaming

ONG sin fines de lucro con sede en Países Bajos. Reúne a +50 países y +200 organizaciones del sector EV.

### VERSIONES

## 2.0 → 2.2.1

Histórico: 2.0 (2017), 2.1 (2018), 2.1.1 (2019), 2.2 (2020), 2.2.1 (2022). Versión 3.0 en draft.

### QUIÉN LO USA

## +50 países

Producción activa: Países Bajos, Alemania, Bélgica, Francia, Italia, España, Reino Unido. Adopción en LATAM: Brasil, Chile, México y ahora Colombia.

### NO CONFUNDIR CON

## OCPP

OCPP es cargador → backend (capa física). OCPI es backend → backend (capa de interoperabilidad). Conviven en el mismo sistema.

# ¿Por qué Colombia adoptó OCPI 2.2.1?

La versión elegida responde a criterios técnicos, regulatorios y estratégicos

| Versión | Año   | Sessions y CDRs | Tariffs      | Hub support | Adopción             |
|---------|-------|-----------------|--------------|-------------|----------------------|
| 2.1.1   | 2019  | Básico          | Limitado     | Parcial     | Legacy               |
| 2.2     | 2020  | ✓ Maduro        | ✓ Completo   | ✓ Sí        | Migración            |
| 2.2.1   | 2022  | ✓ Maduro        | ✓ Completo + | ✓ Sí        | ★ Estándar EU actual |
| 3.0     | draft | En diseño       | En diseño    | En diseño   | Sin producción       |

## RAZONES DE LA ADOPCIÓN COLOMBIANA

### Madurez

Estable en producción desde 2022 en mercados europeos

### Hub support

Diseñada para modelos centralizados como el SIEM-UPME

### Trazabilidad

Mejor soporte para audit logs e idempotencia

### Compatible

Backwards-compatible con 2.2 — migración gradual posible

# Cardinalidad en OCPI — qué es y por qué importa

Una notación de 4 símbolos que define qué campos son obligatorios, opcionales o listas en cada objeto

La cardinalidad le dice al CPO si un campo debe enviarse SIEMPRE, si es OPCIONAL, si puede ser una LISTA VACÍA o si necesita AL MENOS UN elemento. Cualquier violación = 400 Bad Request.



**OPCIONAL**

Object

El campo puede ser null o omitirse del JSON. Si no se establece, el valor por defecto del esquema aplica.

Ejemplo: `charging_when_closed?`



**REQUERIDO**

Object

El campo SIEMPRE debe estar presente con un valor válido. Su ausencia genera 400 Bad Request.

Ejemplo: `coordinates:1`



**LISTA 0..n**

[Object]

Lista que puede ser vacía. Si está vacía, puede ser null, [] o el campo puede omitirse.

Ejemplo: `facilities[:]*`



**LISTA 1..n**

[Object]

Lista REQUERIDA con al menos un objeto. No puede ser null ni vacía.

Ejemplo: `evses[:]+`

# Convenciones del body — cómo se construye cada request

Las **5 reglas** que todo CPO debe respetar al construir su payload OCPI hacia el SIEM

## HEADERS OBLIGATORIOS

### 4 headers en CADA request

#### Authorization

Bearer <jwt\_token>

*JWT vigente del CPO ( $\leq 60$  min)*

#### Content-Type

application/json

*Solo JSON soportado*

#### X-Request-ID

<UUID v4>

*Único por request — habilita idempotencia*

#### X-Correlation-ID

<UUID v4>

*Trazabilidad end-to-end en logs SIEM*

## FORMATO JSON ESTRICTO

### 5 reglas para el cuerpo

#### UTF-8

Encoding obligatorio del body

#### ISO 8601

Fechas con offset: 2026-05-28T14:32:11-05:00

#### ISO 3166-1

country\_code: "CO" (alpha-2)

#### ISO 4217

currency: "COP"

#### PUT vs PATCH

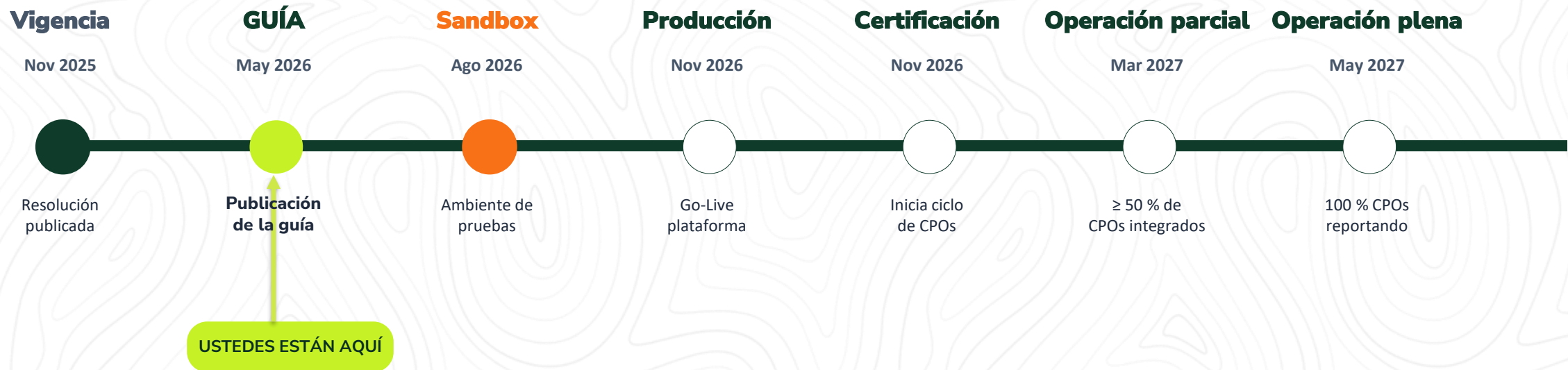
PUT reemplaza completo · PATCH solo campos enviados

```
PATCH /sessions/CO/UPM/SES-001
{ "kwh": 18.43,
  "total_cost": {"incl_vat": 13159.02},
  "last_updated": "2026-05-28T14:57:30-05:00" }
```

Especificación completa de campos y cardinalidad: ver Swagger / OpenAPI 3.1 / Ver en Sección Demo Swagger .

# Cronograma mandatorio — no negociable

*Donde estamos hoy y qué viene en los próximos 12 meses*



## PARA CPOs

Tienen ≥ 5 meses para alistar su backend antes del sandbox.

## PARA LA UPME

Compromiso vinculante de tener sandbox vivo en Ago/2026 y producción en Nov/2026.

# Actores del ecosistema — quién hace qué



# Ruta de Implementación Técnica

*Cinco fases consecutivas. Cada CPO debe completarlas en orden para llegar a producción.*



**Cada fase tiene entregables, criterios de salida y soporte UPME claros.**

2

Fase Legal

**FASE 01**

HABILITACIÓN

# FASE 1 — Habilitación y Registro Legal

*Antes de hablar de tecnología — el CPO debe estar legalmente registrado y notificado*

01

## Registro previo en Cárgame

El CPO o MSP debe registrar primero la información de sus estaciones en la plataforma Cárgame del MinEnergía.

### BASE NORMATIVA

Res. 40123 de 2024

02

## Notificación oficial a la UPME

Una vez validada la información, el MinEnergía notifica oficialmente a la UPME de la existencia del prestador habilitado.

### MECANISMO

Comunicación oficial inter-entidad

03

## Emisión de credenciales (API Key)

La UPME genera una API Key + party\_id único para el CPO, con permisos y alcances. Entrega por canales cifrados.

### CANAL

Portal seguro UPME / correo cifrado

*Sin el estado 'Habilitado' en Cárgame, la infraestructura NO es visible en la Plataforma Nacional de Electromovilidad.*

# FASE 1 — Notificación AMI (vía alternativa)

Para CPOs sin AMI plena: vía supletoria conforme al Parágrafo 3 del Art. 5 de la Res. 40559

## ¿CUÁNDO APLICA?

### AMI ausente o parcial

Cuando el CPO no cuenta con Infraestructura Avanzada de Medición plena (smart meters horarios), debe reportar la información operativa cada 1 hora por el medio habilitado.

### FALLBACK UPME

Si no entrega información en tiempo, la UPME aplica un algoritmo de aproximación basado en datos históricos de Sessions y marca los datos generados con data\_quality = ESTIMATED y source = UPME\_FALLBACK.

## METODOLOGÍA DE EVALUACIÓN

### UPME · MinEnergía · CPO

*Solicitud formal a [siem@upme.gov.co](mailto:siem@upme.gov.co) incluye:*

- ✓ Identificación del CPO (razón social, NIT, party\_id)
- ✓ Inventario de estaciones alineado a Cárgame
- ✓ Declaración del estado AMI con cronograma de despliegue
- ✓ Volumen estimado de sesiones mensuales
- ✓ Capacidades técnicas (backend, OCPP, recursos TI)

### RESOLUCIÓN UPME · 30 días

*Aprobación · Aprobación condicional · Vía alterna*

La UPME realiza revisión semestral del estado de habilitación. La vía alterna es transitoria — el objetivo es OCPI directo con AMI plena.

# FASE 1 — Criterios de salida

*Antes de pasar a la Fase 2 (Seguridad), el CPO debe poder marcar estas cinco casillas*



## **Estado Cárgame = HABILITADO**

MinEnergía ha validado y aprobado el registro de la(s) estación(es).



## **party\_id asignado por UPME**

Identificador único del CPO en el ecosistema OCPI nacional (3 caracteres).



## **API Key emitida en canal seguro**

Recibida vía portal UPME o correo cifrado. Almacenada en gestor de secretos del CPO.



## **Responsable técnico designado**

Persona de contacto registrada con correo institucional y 2FA habilitado.

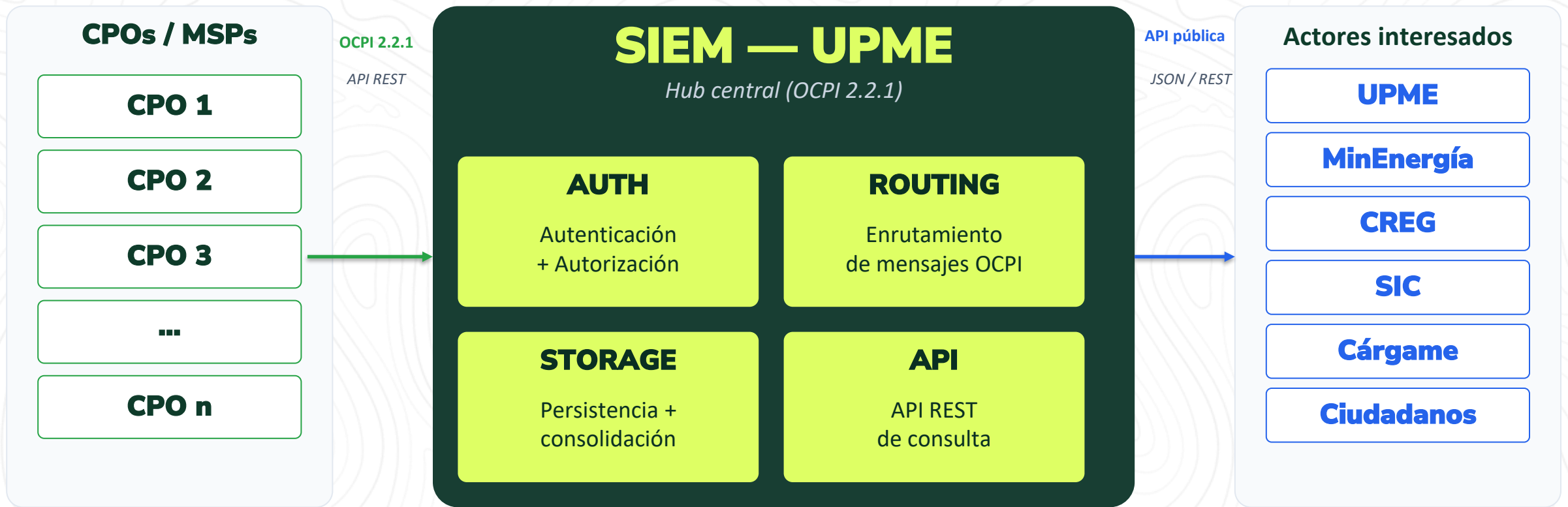


## **Vía AMI definida formalmente**

Directa (OCPI con AMI plena) o supletoria (reporte horario), documentada por escrito.

# Arquitectura SIEM — Hub central OCPI 2.2.1

Una sola plataforma. Todos los CPOs hablan con la UPME.



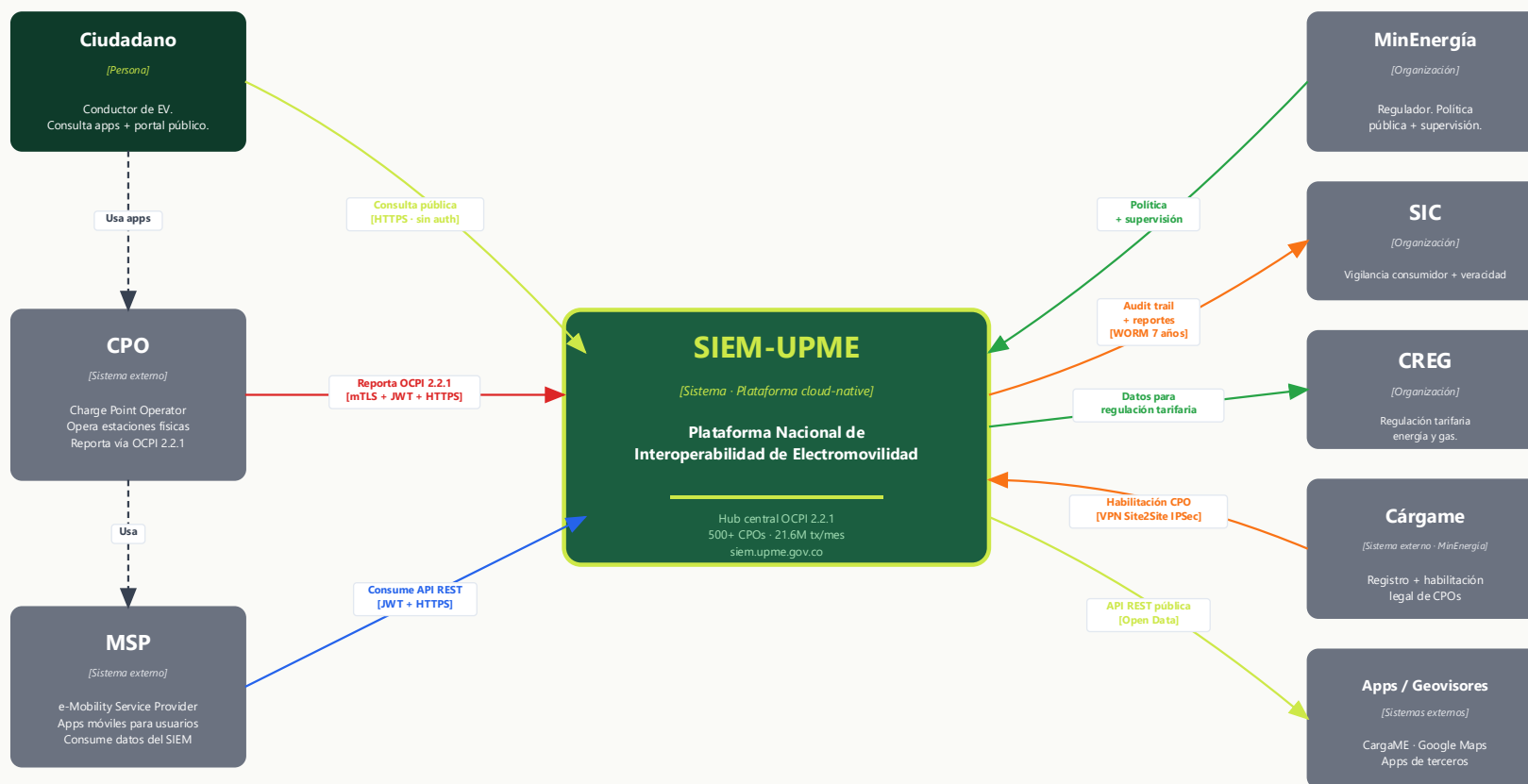
Información intercambiada: Locations · EVSEs · Connectors · Tariffs · Sessions | Endpoint productivo:  
<https://siem.upme.gov.co/ocpi/2.2.1/>

# Quién interactúa con la Plataforma SIEM

Vista de alto nivel — quiénes son los actores, qué consume cada uno y por dónde fluye la información hacia/desde la UPME

## Plataforma SIEM — Diagrama C4 · Context

Quién interactúa con la Plataforma Nacional de Interoperabilidad de Electromovilidad — UPME



### Leyenda · Notación C4

Persona

Sistema en foco

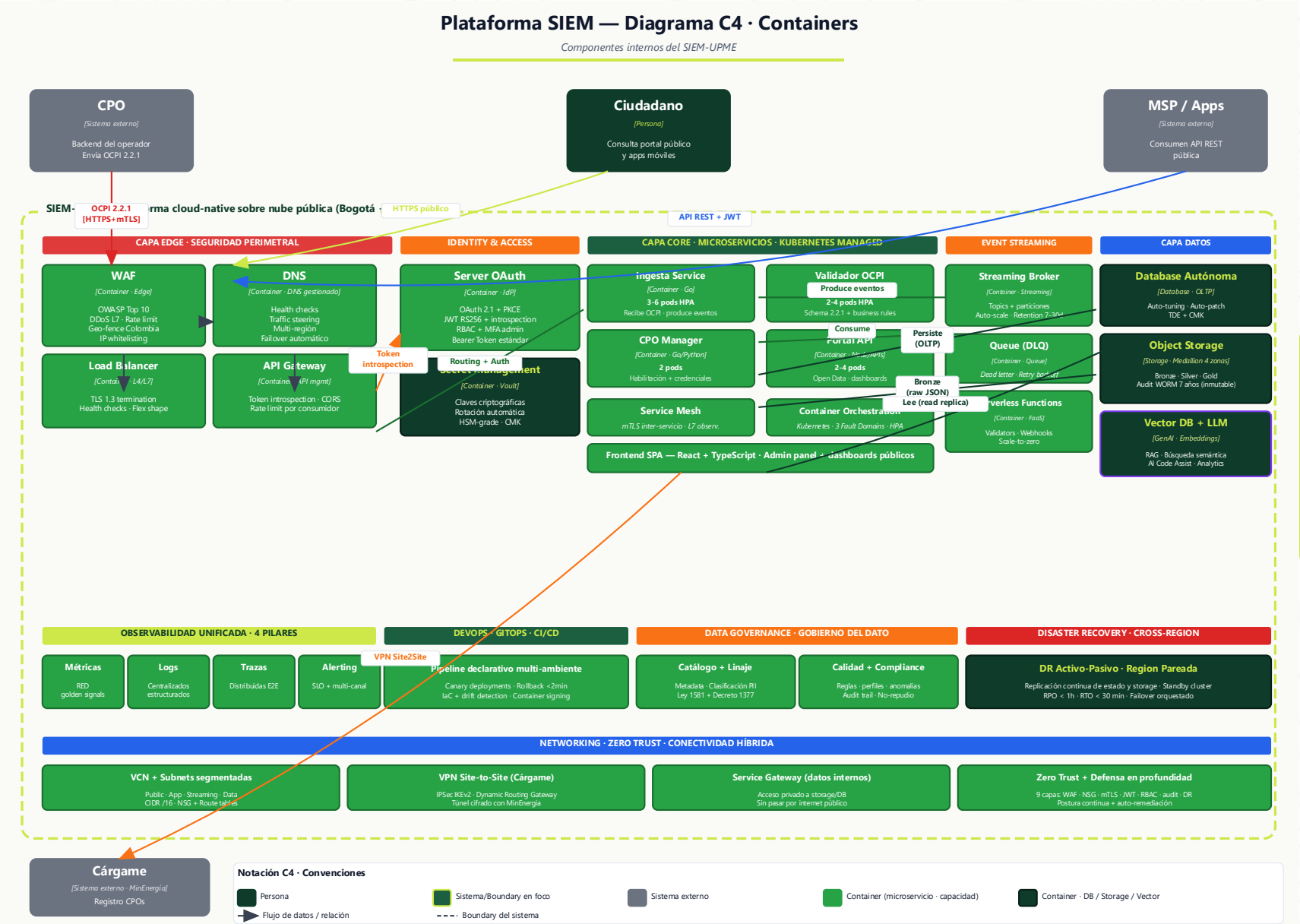
Sistema externo

Datos públicos

EL CPO reporta datos OCPI 2.2.1. · LA UPME recibe, valida, almacena, gobierna y publica. · Cárgame habilita. SIC/CREG/MinEnergía supervisan. Ciudadano consume.

# Componentes internos del SIEM-UPME

Vista detallada — los contenedores desplegados en Cloud, agrupados por capa funcional. +30 servicios. 20M tx/mes. Full Stack DR.



5 capas: Edge & Seguridad · Identity & Access · Core OKE (microservicios) · Event Streaming · Datos (Medallion + ATP) + Observabilidad transversal + DR cross-region

# Volumetría esperada y SLAs UPME

Lo que la plataforma debe sostener — y lo que la UPME se compromete a entregar

## VOLUMETRÍA PROYECTADA

**~600**

*Estaciones de carga*

**~3 000**

*Mensajes/min (pico)*

**20 M**

*Transacciones/mes*

**+30 %**

*Crecimiento anual*

## COMPROMISOS UPME

**99.9 %**

Disponibilidad anual del SIEM

**≤ 60 s**

Latencia de reporte por evento

**≤ 500 ms**

Latencia P95 endpoints API

**7 años**

Retención audit trail (Decreto 1080/2015)

**≥ 6 meses**

Compatibilidad hacia atrás en cambios

**Cross-region**

DRP activo OCI Full Stack DR

3

Fase Técnica

FASE 02

SEGURIDAD

# Seguridad y Acceso Técnico



*Cómo se autentica un CPO contra el SIEM y mantiene una conexión segura.*

## AUTENTICACIÓN MUTUA

### mTLS + Certificados

---

Conexión cifrada cliente-servidor con certificados X.509 firmados por la CA interna UPME.

## ≤ 60 MINUTOS

### Token JWT (vida corta)

---

Cada llamada incluye un Bearer JWT RS256 firmado por la UPME. Sin token, 401 Unauthorized.

## RESPONSABILIDAD DEL CPO

### Custodia API Key

---

Nunca en código fuente, URLs ni logs. Rotación inmediata si hay desvinculación de personal.

# FASE 2 — Flujo de integración segura

4 pasos desde el handshake hasta el primer mensaje OCPI

CPO Backend

MinEnergía/Cárgame

UPME Plataforma

Server OAuth

SIEM-UPME

## PASO 1 — Registro previo (offline)

Registro Cárgame (Res. 40123/2024)

Notifica prestador habilitado

Entrega party\_id + API Key

## PASO 2 — mTLS handshake

ClientHello + cert X.509

ServerHello + Finished

## PASO 3 — Token

POST /token (x-api-key, scopes)

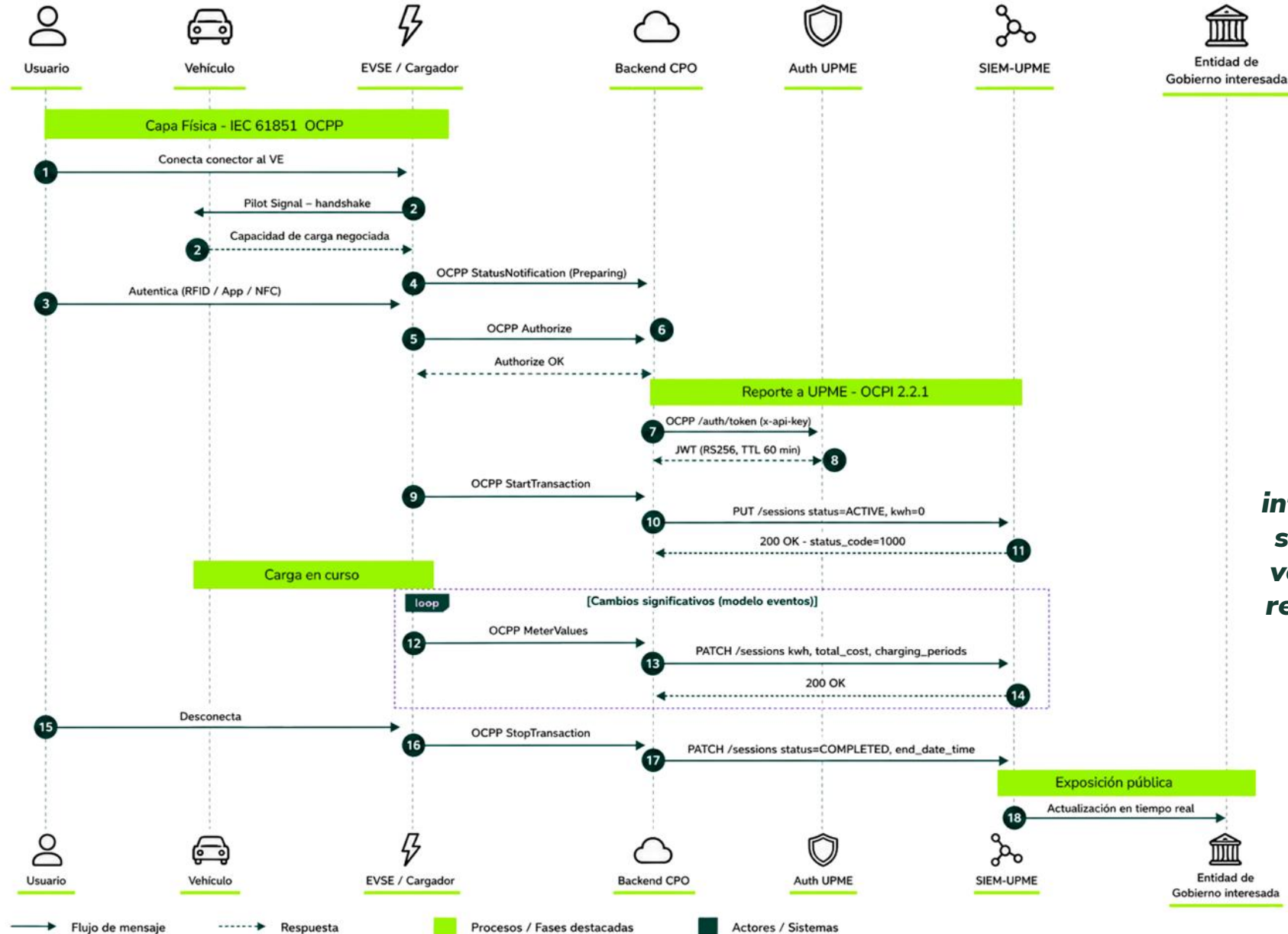
JWT RS256 (TTL 60 min)

## PASO 4 — Consumo OCPI

PUT /Locations/CO/XXX/LOC-001

200 OK status\_code=1000

# FASE 2 — Flujo de integración E2E



**Flujo de interoperabilidad para sesiones de carga de vehículos eléctricos y reporte a SIEM-UPME**

# FASE 2 — Política de rotación de credenciales

Cada credencial tiene su ciclo. La rotación es obligatoria y trazable.

| Credencial                | Frecuencia       | Mecanismo                                                                                   | Revocación de emergencia                                                      |
|---------------------------|------------------|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| API Key (long-lived)      | Cada 12 meses    | Notificación 30 días previa + entrega de nueva Key por portal + 7 días de doble Key válida. | Vía portal UPME con 2FA del responsable técnico CPO — revocación instantánea. |
| Token JWT (short-lived)   | Cada 60 min auto | CPO solicita nuevo token con API Key. No se emiten refresh tokens.                          | Lista de revocación (denylist) por jti con TTL = exp del token.               |
| Certificado mTLS cliente  | Cada 24 meses    | CSR generado por CPO, firmado por CA interna UPME (recomendado: 12 meses).                  | Lista de revocación de certificados (CRL) + OCSP stapling.                    |
| Clave de firma JWT (UPME) | Cada 90 días     | Rotación de kid con coexistencia de la clave anterior por 30 días.                          | Rotación inmediata + comunicación oficial vía circular.                       |

# FASE 2 — Responsabilidades del CPO en seguridad

*Compromisos no negociables que asume el CPO al integrarse al SIEM-UPME*

## **Custodia de API Key**



Nunca incluirla en código fuente versionado, URLs ni logs.

## **Rotación al desvincular personal**



Si un técnico con acceso deja el equipo, rotar inmediatamente.

## **Sincronización NTP**



Drift máximo  $\pm 5$  segundos para validación de iat/exp del JWT.

## **Audit logging propio**



Correlacionar con X-Correlation-ID de la PTI-UPME.

## **Notificar rango de IPs públicas**



Reportar a UPME las IPs/CIDR desde donde se enviarán requests — whitelisting WAF + geo-IP.

## **mTLS con CA interna UPME**



Implementar autenticación mutua con certificado firmado por UPME.

## **Notificación de incidentes**



Reportar a UPME en máximo 4 horas tras detección de incidente.

## **Protección de PII**



No reportar PII salvo lo estrictamente exigido por OCPI 2.2.1.

# Estructura de Datos OCPI 2.2.1



*Los 4 módulos core que Colombia adopta. Qué objetos viven dentro y cómo se relacionan.*

## Locations

*Infraestructura*

### OBJETOS

Location  
EVSE  
Connector

## Sessions

*Carga en curso*

### OBJETOS

Session  
ChargingPeriod

## Tariffs

*Precios*

### OBJETOS

Tariff  
PriceComponent  
TariffElement

## Versions

*Descubrimiento*

### OBJETOS

Version  
VersionDetail  
Endpoint

*Quedan excluidos: Tokens · Credentials · Commands · ChargingProfiles · CDR · Hub Client Info*

4

Fase Funcional

**FASE 03**

DATOS OCPI

# FASE 3 — Módulo Locations · Estados del EVSE

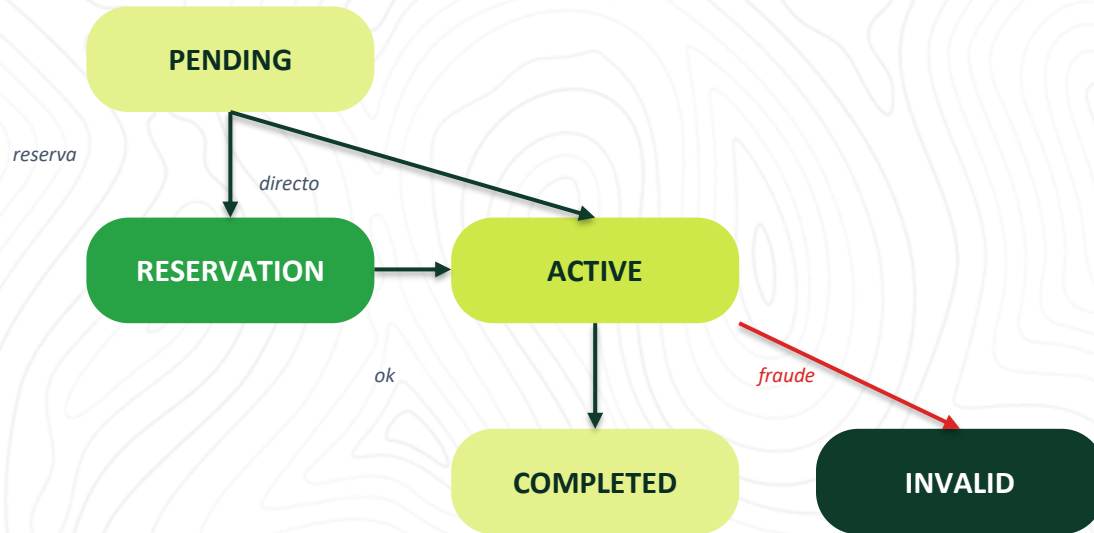
El CPO debe reportar cada cambio de estado del punto de carga. 9 estados posibles.

| ESTADO      | SIGNIFICADO PARA EL USUARIO                              |
|-------------|----------------------------------------------------------|
| AVAILABLE   | Disponible para iniciar carga inmediata                  |
| CHARGING    | En uso — el vehículo está recibiendo energía             |
| BLOCKED     | Punto no accesible por barrera física o parqueo indebido |
| OUTOFORDER  | Fuera de servicio por falla técnica o daño físico        |
| INOPERATIVE | Temporalmente no disponible (sin falla técnica)          |
| RESERVED    | Reservado por un conductor a través de una App           |
| PLANNED     | Punto planificado, estará operativo próximamente         |
| REMOVED     | Punto desinstalado permanentemente                       |
| UNKNOWN     | Estado desconocido (ej. antes de mantenimiento)          |

# FASE 3 — Módulo Sessions · Ciclo de vida

Una sesión es un evento de carga en tiempo real — desde la conexión hasta el cierre

## MÁQUINA DE ESTADOS (Sessions.status)



## EVENTOS QUE GENERAN REPORTE

### PUT status=ACTIVE

Inicio de sesión: usuario se autentica y conecta el vehículo. Envío del objeto Session completo.

### PATCH kwh, charging\_periods

Progreso de la carga: actualización de energía acumulada, períodos y costo total.

### PATCH status=COMPLETED

Fin de sesión: usuario desconecta. Se envían end\_date\_time, kwh final, total\_cost.

### PATCH status=INVALID

Sesión inválida (error técnico, fraude): no debe facturarse. Reporte inmediato.

### PATCH tariff\_id (cambio)

Cambio de tarifa activa: nuevo período de carga aplica un tariff\_id diferente.

# FASE 3 — Módulo Tariffs · Reglas comerciales

*Cómo el CPO comunica precios, IVA, restricciones y vigencia de sus tarifas*

## ESTRUCTURA DE UNA TARIFA

### Tariff

*Contenedor principal del precio*

#### PriceComponent

Precio + tipo (ENERGY, TIME, PARKING\_TIME, FLAT) + IVA

#### TariffElement

Agrupación de PriceComponents con restricciones temporales

#### TariffRestrictions

Horario · días · fechas · límites de energía/potencia

## CUÁNDO SE REPORTA

- Creación de una nueva tarifa
- Modificación de precios (price en PriceComponent)
- Modificación del IVA aplicable (vat)
- Restricciones temporales o de potencia
- Cambio de TariffType (REGULAR ↔ AD\_HOC ↔ PROFILE)
- Modificación de límites globales (min\_price / max\_price)
- Cambio de validez temporal (start\_date\_time / end\_date\_time)
- Eliminación de una tarifa

Métodos disponibles: GET · PUT (crear/actualizar) · DELETE — identificados por (country\_code, party\_id, tariff\_id)

# FASE 3 — Reporte basado en eventos

*Por qué OCPI 2.2.1 con eventos es mejor que polling — y qué implica para el CPO*

## ✗ POLLING (lo que NO hacemos)

Cliente consulta cada N segundos

- ✗ Tráfico constante incluso sin cambios
- ✗ Latencia alta (depende del intervalo)
- ✗ Sobrecarga de red y backend
- ✗ Costos de infraestructura mayores
- ✗ Datos potencialmente desactualizados

## ✓ POR EVENTOS (lo que hace SIEM)

CPO envía solo cuando algo cambia

- ✓ Cero tráfico cuando no hay cambios
- ✓ Latencia  $\leq 60$  s — casi tiempo real
- ✓ Menor uso de red y CPU del CPO
- ✓ Costos optimizados — escala mejor
- ✓ Datos siempre relevantes y frescos

*Fundamento normativo: esquema alternativo previsto en el Art. 3 de la Res. 40559 —  
reporte máximo 60 s ante cualquier cambio relevante.*

# FASE 3 — Módulo Versions · Descubrimiento

*El primer endpoint que llama todo CPO — define qué módulos están disponibles*

## GET Lista de versiones

/ocpi/2.2.1/versions

### Headers requeridos

Authorization: Bearer <jwt\_token>

### Respuesta

Array de objetos Version con number (ej. "2.2.1") y URL de detalle por cada versión soportada.

```
[{"version": "2.2.1", "url": "https://siem.upme.gov.co/ocpi/2.2.1/"}]
```

## GET Detalle de versión

/ocpi/2.2.1/

### Respuesta

VersionDetail con lista de Endpoints — cada uno con:

- identifier: LOCATIONS, SESSIONS, TARIFFS...
- role: SENDER | RECEIVER
- url: URL base del módulo

```
{
  "version": "2.2.1",
  "endpoints": [
    {
      "identifier": "locations",
      "role": "RECEIVER",
      "url": "..."
    }
  ]
}
```

*El handshake de Versions es OBLIGATORIO antes de consumir cualquier otro módulo OCPI.*

5

Fase Operativa

FASE 04

OPERACIÓN

# Operación y Reporte por Eventos

*Cómo se comporta el sistema en el día a día — flujo end-to-end de una sesión de carga.*

## Solo cambios

---

Reporte basado en eventos. El CPO transmite cuando algo cambia, no de forma periódica.

## $\leq 60$ segundos

---

Latencia máxima desde que ocurre el evento hasta que llega al SIEM.

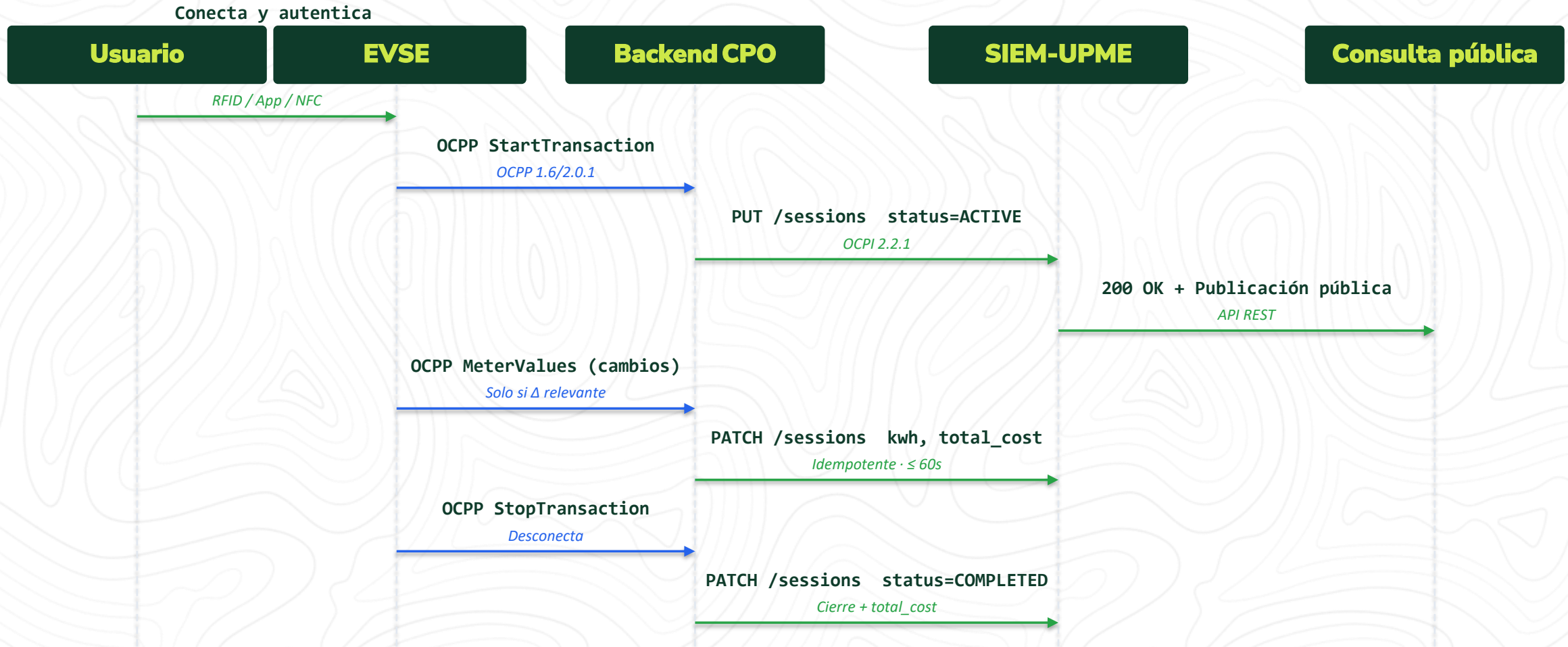
## Idempotente

---

Cada mensaje incluye X-Request-ID (UUID v4).  
Reenvíos no duplican el dato.

# FASE 4 — Flujo end-to-end de una sesión de carga

Lo que ocurre desde que el usuario llega a la estación hasta que la información se publica



# FASE 4 — Idempotencia y códigos de respuesta

Cómo garantizar que un mensaje reenviado no duplica datos — y qué significa cada respuesta

## IDEMPOTENCIA

### X-Request-ID + PUT/PATCH

Cada request del CPO incluye:

X-Request-ID: <UUID v4 único>

El SIEM cachea el resultado de cada UUID por 24 h:

- Reenvío con mismo UUID → mismo resultado
- PUT reemplaza el recurso completo
- PATCH actualiza solo los campos enviados
- POST nunca se usa para escritura de datos

## CÓDIGOS HTTP — significado SIEM

|     |                   |                                               |
|-----|-------------------|-----------------------------------------------|
| 200 | OK                | Operación exitosa                             |
| 400 | Bad Request       | Esquema JSON inválido o campos faltantes      |
| 401 | Unauthorized      | Token JWT ausente, expirado o inválido        |
| 403 | Forbidden         | Token válido pero sin scope para el recurso   |
| 404 | Not Found         | Recurso (Location / Session) no existe        |
| 409 | Conflict          | X-Request-ID ya procesado con cuerpo distinto |
| 422 | Unprocessable     | Validación de negocio falla (ej. estado)      |
| 429 | Too Many Requests | Rate limit excedido — usar Retry-After        |
| 500 | Internal Error    | Reintentar con backoff exponencial            |

# FASE 4 — Rate limiting · proteger a todos

Límites por CPO y por endpoint. La UPME devuelve 429 + Retry-After cuando se excede.

| Endpoint / Módulo    | Operación    | Límite  | Ventana     |
|----------------------|--------------|---------|-------------|
| /auth/token          | POST         | 30 req  | 5 min / CPO |
| /locations/**        | PUT / PATCH  | 60 req  | 1 min / CPO |
| /sessions/**         | PUT / PATCH  | 120 req | 1 min / CPO |
| /tariffs/**          | PUT / DELETE | 30 req  | 5 min / CPO |
| /versions, /version  | GET          | 60 req  | 1 min / CPO |
| API consulta pública | GET          | 300 req | 1 min / IP  |

Cuando recibe 429, el CPO debe aplicar backoff exponencial respetando el header Retry-After. La UPME publica ventanas ajustadas por CPO en caso de eventos masivos (festividades, etc.).

6

Fase de Salida

**FASE 05**

VALIDACIÓN

# Validación y Publicación

*Cómo se prueba la integración sin afectar producción — y cómo se hace pública la información.*

## PRUEBAS SEGURAS

### Sandbox

---

Ambiente aislado para validar interoperabilidad antes de producción. Solicita acceso a [siem@upme.gov.co](mailto:siem@upme.gov.co).

**Disponible Ago/2026**

## CONSUMO ABIERTO

### API pública

---

Endpoint REST que expone la información consolidada. Ciudadanos, MSPs y actores autorizados.

**Disponible Nov/2026**

# FASE 5 — Sandbox · cómo funciona

Lo que el CPO recibe al ser aceptado en sandbox — y qué pruebas debe pasar para producción

## QUÉ RECIBE EL CPO

- ✓ **URL Sandbox**  
*<https://sandbox.siem.upme.gov.co/ocpi/2.2.1/>*
- ✓ **API Key de pruebas**  
*Diferente a producción, sin valor regulatorio*
- ✓ **Certificado mTLS staging**  
*Emitido por CA interna UPME (entorno staging)*
- ✓ **Datos sintéticos**  
*EVSEs simuladas, tarifas y sesiones de ejemplo*
- ✓ **Validador automatizado**  
*Suite de conformidad con +120 casos OCPI 2.2.1*
- ✓ **Logs detallados**  
*Visualización de cada request, respuesta y error*
- ✓ **Soporte técnico**  
*siem@upme.gov.co · mesa de ayuda dedicada*

## CRITERIOS DE PASO A PRODUCCIÓN

- Handshake exitoso con GET /versions y /version
- $\geq 95$  % de casos de la suite de conformidad
- 0 falsos positivos en validación de esquema JSON
- Latencia P95  $\leq 60$  s en escenarios de carga
- Manejo correcto de 429, 401 y reintentos con backoff
- Audit logging con X-Correlation-ID verificado
- Sincronización NTP comprobada (drift  $\leq 5$  s)

Acta de certificación firmada por UPME

# FASE 5 — API pública · datos al ciudadano

*La UPME publica los datos validados para consumo de ciudadanos y actores autorizados*

## CONSULTA WEB

### Ciudadano

Mapa público en [upme.gov.co/electromovilidad](https://upme.gov.co/electromovilidad) — ubicaciones, disponibilidad y precios en tiempo real.

**Sin autenticación · solo lectura**

## API REST

### UPME-MSP (e-Mobility)

Endpoint `/public/v1/locations` · `/public/v1/tariffs` · datos consolidados de todos los CPOs habilitados.

**API Key MSP · rate limit**

## API PRIVADA

### Reguladores

MinEnergía · SIC · CREG: acceso completo con audit trail incluido para reportes y supervisión.

**mTLS + auditoría firmada**

7

# DEMO SWAGGER

EN VIVO (MOCKS) + CIERRE

# Sandbox SIEM en acción

*Veamos el flujo completo de una sesión OCPI 2.2.1.*

|    |                          |                                                       |
|----|--------------------------|-------------------------------------------------------|
| 01 | <b>Handshake</b>         | GET /versions → GET /version → obtención de endpoints |
| 02 | <b>Autenticación</b>     | POST /auth/token con API Key → obtención JWT          |
| 03 | <b>Registro Location</b> | PUT /locations/CO/UPM/LOC-001 con 2 EVSEs             |
| 04 | <b>Inicio sesión</b>     | PUT /sessions/CO/UPM/SES-001 status=ACTIVE            |
| 05 | <b>Progreso</b>          | PATCH /sessions/.../SES-001 con kwh y costo           |
| 06 | <b>Cierre</b>            | PATCH status=COMPLETED – validación en consola        |
| 07 | <b>Consulta</b>          | GET API pública → la sesión aparece publicada         |

# Demo • qué observar en cada paso

*Lo que sus equipos técnicos deben mirar mientras ejecuto la demo*

## Headers en cada request

*Authorization • Content-Type • X-Request-ID • X-Correlation-ID*

Toda llamada autenticada lleva 4 headers obligatorios.

## Esquema JSON exacto

*Validación contra spec OCPI 2.2.1 – campos requeridos, cardinalidad, formatos*

Un campo de más o un tipo incorrecto = 400 Bad Request.

## Idempotencia funcionando

*Repetir la misma llamada con mismo X-Request-ID → mismo resultado, no duplica*

Visible en los logs del sandbox como 'cache hit'.

## Tiempos reales del SIEM

*Latencia P50 ~120 ms – P95 ~480 ms – bien por debajo de los SLAs*

Mostrado en panel observabilidad del sandbox.

## Manejo de error 429

*Si excedo el rate limit, Retry-After indica cuánto esperar*

Demostraremos backoff exponencial en vivo.

# Cómo empezar — desde mañana

Acciones concretas para que su organización se integre al SIEM sin perder tiempo



## ESTA SEMANA

- Verificar que su(s) estación(es) estén registradas en Cárgame con estado HABILITADO.
- Designar un responsable técnico interno con correo institucional y 2FA habilitado.
- Descargar la Guía Técnica oficial: [upme.gov.co/electromovilidad](https://upme.gov.co/electromovilidad).



## ESTE MES

- Solicitar acceso al sandbox enviando correo a [siem@upme.gov.co](mailto:siem@upme.gov.co) (incluir party\_id solicitado).
- NOTIFICAR a la UPME el rango de IPs públicas desde donde el CPO hará requests al SIEM — obligatorio para whitelisting en WAF + API Gateway con filtro geo-IP.
- Hacer dry-run interno: implementar el handshake (GET /versions) contra el sandbox.
- Revisar internamente la política de custodia de API Keys y rotación.



## ANTES DE PRODUCCIÓN (Nov/2026)

- Completar suite de conformidad  $\geq 95$  % en sandbox.
- Obtener certificado mTLS de producción firmado por la CA UPME.
- Recibir acta de certificación firmada por la UPME.

# Roadmap UPME · Mayo 2026 → Mayo 2027

Los próximos 12 meses — qué hace la UPME, qué hace el CPO, en cada trimestre

**Q2 · 2026**

**MAY · JUN**

Publicación Guía

*Equipos CPO leen la guía  
y planifican*

**Q3 · 2026**

**JUL · AGO · SEP**

Sandbox vivo

*CPOs hacen dry-run y  
pruebas de conformidad*

**Q4 · 2026**

**OCT · NOV · DIC**

GO-LIVE producción

*Primeros CPOs  
certificados reportan en  
vivo*

**Q1 · 2027**

**ENE · FEB · MAR**

Onboarding masivo

*≥ 50 % CPOs integrados*

**Q2 · 2027**

**ABR · MAY**

Operación plena

*100 % CPOs habilitados  
reportando*

# Canales de contacto

Dónde escribir y para qué — la UPME atiende con SLA definido

|                                                                                                        |                                                          |              |
|--------------------------------------------------------------------------------------------------------|----------------------------------------------------------|--------------|
| <b>Integración sandbox</b><br><a href="mailto:siem@upme.gov.co">siem@upme.gov.co</a>                   | Solicitud inicial · party_id · entrega de credenciales   | 48 h hábiles |
| <b>Soporte técnico CPO</b><br><a href="mailto:siem@upme.gov.co">siem@upme.gov.co</a>                   | Bugs · errores 4xx/5xx · incidencias de integración      | 8 h hábiles  |
| <b>Mesa de ayuda operativa</b><br><a href="mailto:mesadeayuda@upme.gov.co">mesadeayuda@upme.gov.co</a> | Consultas generales · documentación · onboarding         | 24 h hábiles |
| <b>Reportes a SIC</b><br><a href="mailto:siem@upme.gov.co">siem@upme.gov.co</a>                        | Audit · trazabilidad · respuesta a requerimientos        | 72 h hábiles |
| <b>Incidentes de seguridad</b><br><a href="mailto:siem@upme.gov.co">siem@upme.gov.co</a>               | Reportar en MÁXIMO 4 horas tras detección — alto crítico | 4 h          |

# Mecanismo de actualización de la Guía

*Cómo la UPME comunica cambios — sin romper integraciones existentes*

## 30 días

*de anticipación*

Toda modificación se comunica con mínimo 30 días calendario de antelación mediante circular oficial dirigida a los CPOs, MSPs y gateways certificados.

## Portal

*[upme.gov.co/electromovilidad](https://upme.gov.co/electromovilidad)*

Se publica en el portal oficial con histórico completo de versiones. Diff visible entre versiones.

## ≥ 6 meses

*compatibilidad hacia atrás*

Cuando aplique cambios técnicos no compatibles, la UPME mantiene compatibilidad mínimo seis meses para permitir migración.

## Correo directo

*a responsables técnicos*

Notificación por correo electrónico a los responsables técnicos registrados de cada CPO.

# Lo que ustedes se llevan hoy

## **1 ES LEY**

El reporte vía OCPI 2.2.1 al SIEM es OBLIGATORIO para todo CPO de acceso público — no hay excepción técnica para postergarlo.

## **2 ES ABIERTO**

OCPI 2.2.1 es un estándar internacional documentado — su equipo no parte de cero, hay librerías y referencia oficial.

## **3 HAY APOYO**

La UPME provee sandbox, validador, mesa de ayuda y plazos amplios. No están solos en este proceso.

## **4 ES OPORTUNIDAD**

Quien integra primero, gana visibilidad pública, reputación y acceso a los MSPs nacionales antes que la competencia.

# Lo que se llevan hoy — artefactos & referencias

Documentos técnicos publicados junto con la Guía — listos para que sus equipos los usen mañana

01

## Guía Técnica de Implementación

Documento oficial (66 páginas). Marco normativo, arquitectura, módulos OCPI 2.2.1, seguridad, onboarding.

PDF

Guía Publicada

02

## Solicitud especificación OpenAPI 3.1 (Swagger)

Contrato formal de la API SIEM. Endpoints, schemas, ejemplos, códigos HTTP. Importable en Swagger UI / Stoplight.

YAML

[openapi.yaml](#)

03

## Solicitud Postman Collection

Colección ejecutable con variables de entorno, requests prearmados, ejemplos de body.

JSON

[postman-siem.json](#)

04

## Guías de Referencia (SDKs)

Implementación de SDKs.

GitHub

[sdk-ocpi-2.2.1](#)

# PREGUNTAS & RESPUESTAS

EN VIVO (MOCKS) + CIERRE

- FAQs
- Referencias normativas y técnicas
- Glosario completo de términos OCPI y UPME
- Equipo Subdirección de Gestión de la Información

*Material complementario para profundizar — disponible para Q&A o consulta posterior*

# FAQ - Impacto

## ¿Qué pasa si no nos integramos al SIEM?

La estación deja de ser visible en la API pública y para los MSPs nacionales. El MinEnergía puede sancionar al CPO conforme a la Res. 40559. La SIC supervisa veracidad de información publicada.

## ¿Cuánto cuesta integrarse?

OCPI 2.2.1 es un estándar abierto y gratuito. El sandbox y el soporte UPME son gratuitos. Costo principal: desarrollo en backend del CPO (estimable entre 2-6 meses de trabajo según madurez).

## ¿La UPME va a competir con nuestro negocio?

No. SIEM es un Hub de interoperabilidad — solo recibe, valida y publica datos. No vende energía, no opera estaciones, no tiene relación comercial con usuarios finales.

## ¿Qué información se hará pública?

Ubicación, disponibilidad y tarifas. NO se publica información comercial sensible: cuántos kWh vende, cuántas sesiones, ingresos. Eso es solo para la UPME y los reguladores.

## ¿Quién es dueño de los datos?

El CPO es el dueño de los datos operacionales. La UPME es el responsable del tratamiento bajo Ley 1581/2012 y publica solo lo exigido por la Resolución 40559.

# FAQ — Técnica

## ¿Qué necesitamos en stack tecnológico?

Un backend con capacidad de exponer HTTPS, gestionar certificados, firmar/validar JWT, persistir estados. Cualquier lenguaje moderno sirve (Java/Spring, Python/FastAPI, Node, Go, .NET).

## ¿Existen librerías OCPI 2.2.1 listas?

Sí — la Fundación EVRoaming mantiene SDKs de referencia.

## ¿Cómo manejamos los certificados?

La UPME emite certificados mTLS firmados por su CA interna. Recomendamos almacenamiento en HSM o gestor de secretos (HashiCorp Vault, AWS Secrets Manager, Azure Key Vault, OCI Vault).

## ¿Qué pasa si nuestro backend cae?

El reporte por eventos significa que datos no enviados durante la caída se acumulan. Al recuperarse, el CPO debe hacer reconciliación enviando los eventos pendientes con sus timestamps reales.

## ¿Hay impacto en nuestro OCPP existente?

No. OCPI vive en la capa CPO ↔ Hub, no en la capa cargador ↔ CPO (que sigue siendo OCPP 1.6 o 2.0.1). El CPO traduce eventos OCPP en mensajes OCPI hacia el SIEM.

## ¿Cómo manejan los eventos perdidos por red?

X-Request-ID idempotente + reintentos con backoff exponencial. La UPME no cierra conexión por errores transitorios. Caches de UUID por 24 h evitan duplicación al reenviar.

## ¿Soportan webhooks de vuelta hacia el CPO?

No en la primera versión. La comunicación es unidireccional (CPO → SIEM). El módulo Commands de OCPI (que permitiría enviar comandos al cargador) está fuera del alcance inicial.

## ¿Cuál es la política de versionado?

Semver según OCPI. SIEM-UPME mantiene 2.2.1 como versión productiva inicial. Versionado por URL: /ocpi/2.2.1/. Cambios mayores se anuncian con 30 días + 6 meses de compatibilidad.

## ¿Tienen suite de conformidad automatizada?

Sí — basada en el OCPI Test Tool oficial de EVRoaming Foundation, adaptada a las restricciones colombianas (módulos obligatorios, validación AMI, etc.). +120 casos de prueba.

## ¿Cómo se modela la zona horaria?

Todo timestamp en formato ISO 8601 con offset (-05:00 para CO). El SIEM normaliza a UTC internamente. NTP obligatorio en CPO con drift  $\leq 5$  s para validar iat/exp del JWT.

# Glosario de términos · OCPI y SIEM

## AMI

Infraestructura Avanzada de Medición — smart meters que registran demanda eléctrica con resolución horaria.

## Cárgame

Aplicativo del MinEnergía donde se registran legalmente las estaciones antes de la integración técnica.

## Conector

Puerto físico del EVSE que se enchufa al vehículo (Tipo 2, CCS2, CHAdeMO).

## DPoP

Demonstrating Proof of Possession — extensión OAuth 2.1 que ata el token al cliente.

## Hub OCPI

Plataforma intermediaria (como el SIEM) que evita conexiones N×N entre CPOs y MSPs.

## API Key

Código alfanumérico secreto que identifica al CPO ante el SIEM-UPME.

## CDR

Charge Detail Record — el 'recibo' final inmutable de una sesión de carga (facturación, auditoría).

## CPO

Charge Point Operator — empresa que instala, opera y mantiene las estaciones físicas.

## EVSE

Electric Vehicle Supply Equipment — el punto de carga individual (un cargador puede tener varios EVSEs).

## Idempotencia

Garantía de que reenviar el mismo mensaje produce el mismo resultado (X-Request-ID + UUID v4).

# Glosario de términos · OCPI y SIEM (cont.)

## JWT

JSON Web Token firmado RS256 — pase digital temporal entregado por el SIEM tras validar identidad.

## mTLS

Mutual TLS — cliente y servidor presentan certificados X.509 para cifrar y autenticar la conexión.

## OAuth 2.1

Estándar de autorización delegada — flujo Client Credentials Grant en SIEM.

## OCPP

Open Charge Point Protocol — protocolo entre el cargador físico y el backend del CPO (no SIEM).

## RFID

Radio-Frequency Identification — tarjetas que usan los conductores para iniciar carga.

## SIEM

Sistema de Interoperabilidad de Electromovilidad — la plataforma UPME (no confundir con SIEM de seguridad).

## kWh

Kilovatio-hora — unidad de energía entregada al vehículo, base del cálculo tarifario.

## MSP

e-Mobility Service Provider — empresa que gestiona la relación con el usuario final (app, pagos).

## OCPI

Open Charge Point Interface — protocolo abierto mantenido por la Fundación EVRoaming.

## party\_id

Identificador único de 3 caracteres asignado por la UPME a cada CPO (ej. UPM, ENL, CLS).

## Sesión

Session — evento de carga desde que el usuario conecta el vehículo hasta que finaliza la carga.

## Token vida corta

JWT con TTL  $\leq 60$  min — garantiza integridad, trazabilidad y no repudio.

# Ejemplo JSON — sesión OCPI 2.2.1

Estructura mínima exigida en PUT /sessions/CO/UPM/SES-001

```
{
  "country_code": "CO",
  "party_id": "UPM",
  "id": "SES-2026-05-28-000123",
  "start_date_time": "2026-05-28T14:32:11-05:00",
  "kwh": 18.43,
  "cdr_token": {
    "uid": "RFID-A1B2C3D4",
    "type": "RFID",
    "contract_id": "CO-MSP-001"
  },
  "auth_method": "WHITELIST",
  "location_id": "LOC-EL-DORADO-001",
  "evse_uid": "EVSE-001-A",
  "connector_id": "1",
  "currency": "COP",
  "charging_periods": [{
    "start_date_time": "2026-05-28T14:32:11-05:00",
    "dimensions": [
      { "type": "ENERGY", "volume": 18.43 },
      { "type": "TIME", "volume": 0.42 }
    ]
  }],
  "tariff_id": "TAR-FAST-2026-Q2"
}],
  "total_cost": { "excl_vat": 11058.0, "incl_vat": 13159.02 },
  "status": "ACTIVE",
  "last_updated": "2026-05-28T14:57:30-05:00"
}
```

# Referencias normativas y técnicas

## NORMATIVO COLOMBIANO

### Resolución 40559 de 2025

MinEnergía · 21 Nov 2025 · Marco principal

### Resolución 40123 de 2024

MinEnergía · Crea aplicativo Cárgame

### Resolución 40223 de 2021

MinEnergía · Condiciones técnicas estaciones

### Ley 1964 de 2019

Congreso · Promoción de vehículos eléctricos

### Ley 1581 de 2012

Congreso · Protección de datos personales

### Decreto 1080 de 2015

Min. Cultura · Retención de documentos 7 años

### Decreto 620 de 2020

Min. TIC · Servicios digitales del Estado

## TÉCNICO INTERNACIONAL

### OCPI 2.2.1 Spec

EVRoaming Foundation · [ocpi-protocol.org](https://ocpi-protocol.org)

### OCPP 1.6 / 2.0.1

Open Charge Alliance · [openchargealliance.org](https://openchargealliance.org)

### OAuth 2.1 (draft)

IETF · RFC en curso

### RFC 7519 — JWT

IETF · JSON Web Token

### RFC 8705 — mTLS

IETF · OAuth Mutual TLS Client Auth

### ISO 8601

Formato de fechas y horas

### IEC 61851 / IEC 62196

Carga conductiva / conectores físicos

# SLAs operativos · UPME ↔ CPO

| Métrica                  | Compromiso UPME      | Compromiso CPO      | Penalidad / Acción                 |
|--------------------------|----------------------|---------------------|------------------------------------|
| Disponibilidad SIEM      | 99.9 % mensual       | 99.0 % backend      | Plan de continuidad documentado    |
| Latencia API consulta    | P95 ≤ 500 ms         | —                   | Notificación + remediación 4 h     |
| Latencia reporte CPO     | —                    | ≤ 60 s desde evento | Suspensión temporal de party_id    |
| Tiempo respuesta soporte | 8 h hábiles          | —                   | Escalamiento a Subdirector         |
| Notificación incidente   | —                    | 4 h tras detección  | Reporte a SIC + sanción Res. 40559 |
| Mantenimiento programado | 48 h aviso previo    | Ventana acordada    | Cambio de fecha si lo solicita CPO |
| Rotación API Key         | 30 días aviso previo | —                   | Doble validez 7 días en transición |
| Compatibilidad cambios   | ≥ 6 meses            | —                   | Versionado /ocpi/2.2.1/ → /2.3/    |

## BACKUP - EQUIPO RESPONSABLE

---



**Indira Cristina Portocarrero Ospina**

*Directora General · UPME*



**John Alejandro Barrios Avila**

*Subdirector (E) Gestión de la Información*



**Cesar A. Jerez Mayorga**

*Equipo Subdirección*



**Rafael A. Domínguez Jiménez**

*Arquitecto · Expositor de hoy*



**Rafael Santos Arnedo Mendoza**

*Equipo Subdirección*



**Fabián Garzón García**

*Equipo Subdirección*



UPME



# iGracias!



@upmecol



UPME Oficial



@upmeoficial



@upmeoficial



@upmeoficial

[www.upme.gov.co](http://www.upme.gov.co)