



# Guía de Operaciones de OmniCall CSCF

## Tabla de Contenidos

1. [Descripción General](#)
2. [Comprendiendo la Arquitectura IMS](#)
3. [Flujos de Sesión de Llamadas](#)
4. [Componentes de CSCF](#)
5. [Operaciones Comunes](#)
6. [Resolución de Problemas](#)
7. [Documentación Adicional](#)
8. [Glosario](#)

## Descripción General

OmniCall CSCF es una solución IMS (IP Multimedia Subsystem) integral que proporciona funciones de control de sesión de llamadas de grado carrier para proveedores de servicios móviles y **fijos**. Construido sobre tecnología de código abierto probada y mejorado con capacidades de gestión de nivel empresarial, OmniCall CSCF ofrece la infraestructura de control de sesión central necesaria para VoLTE, VoWiFi, RCS y servicios tradicionales de VoIP de línea fija.

## ¿Qué es IMS?

El Subsistema Multimedia IP (IMS) es la arquitectura estandarizada por 3GPP para la entrega de servicios multimedia basados en IP. Proporciona:

- **Control de sesión** para servicios de voz, video y mensajería
- Gestión de **Calidad de Servicio (QoS)** para comunicaciones en tiempo real
- **Convergencia de servicios** a través de redes móviles, fijas y WiFi
- **Interoperabilidad basada en estándares** con otros operadores y redes
- Capacidades de **Servicios de Comunicación Ricos (RCS)**
- **Convergencia Fijo-Móvil (FMC)** para la entrega unificada de servicios

OmniCall CSCF implementa todas las funciones centrales de CSCF definidas en 3GPP TS 23.228, proporcionando una solución completa de red central IMS lista para producción.

## **Componentes de OmniCall CSCF**

OmniCall CSCF proporciona gestión completa de todos los elementos de red CSCF:

- **P-CSCF** (Proxy-CSCF) - Proxy de borde orientado al usuario y ancla de seguridad
- **E-CSCF** (Emergency-CSCF) - Enrutamiento de servicios de emergencia (integrado con P-CSCF)
- **I-CSCF** (Interrogating-CSCF) - Punto de entrada a la red y ocultamiento de topología
- **S-CSCF** (Serving-CSCF) - Control de sesión central, registro y activación de servicios

## **Capacidades Clave**

### **Funciones de Red:**

- Control de sesión IMS totalmente compatible con 3GPP
- **Cumplimiento de GSMA IR.92/IR.94** - Funciona con cualquier dispositivo compatible con estándares, no se requieren paquetes personalizados de operador
- Soporte para VoLTE, VoWiFi y RCS
- Integración de servicios SIP de línea fija
- Soporte para servicios de emergencia (E911/E112) con servicios de ubicación
- Ocultamiento de topología y seguridad de red
- Asociaciones de seguridad basadas en IPsec
- Integración de AAA y políticas basadas en Diameter

### **Características de Servicio:**

- Gestión de sesiones de llamada en tiempo real
- Activación de servicios a través de Criterios de Filtro Inicial (IFC)
- Integración de Servidor de Aplicaciones (AS) a través de la interfaz ISC
- Integración de cobro (en línea y fuera de línea)
- Aplicación de políticas de QoS a través de la integración de PCRF
- Soporte de multi-inquilino para escenarios MVNO

### **Gestión y Operaciones:**

- Monitoreo en tiempo real a través de un panel de control basado en web
- Integración de métricas de Prometheus (ver [Referencia de Métricas](#))
- API RESTful para automatización
- Clustering distribuido para alta disponibilidad
- Resolución de problemas y diagnósticos en vivo

### **Componentes Integrados:**

- **OmniePDG:** Gateway de Datos de Paquete Evolucionado para VoWiFi (cumple con IR.94)
- **OmniTAS:** Servidor de Aplicaciones de Telefonía para servicios suplementarios
- **OmniMessage:** Servidor de Aplicaciones SMS/MMS (3GPP TS 24.341)

Para un uso detallado del panel de control, consulte [Operaciones de UI Web](#).

## Comprendiendo la Arquitectura IMS

### Arquitectura de Red IMS

La solución OmniCall CSCF se sitúa en el corazón de la arquitectura IMS, proporcionando la capa de control de sesión que conecta el equipo del usuario a los servicios y gestiona todas las sesiones de llamada.

### Cómo Trabajan Juntos los CSCFs

Las funciones de CSCF trabajan como un sistema coordinado para manejar sesiones IMS:

#### 1. P-CSCF - Primer Punto de Contacto

- El equipo del usuario (dispositivos móviles, WiFi o de línea fija) establece conexiones seguras con P-CSCF
- Proporciona asociaciones de seguridad IPsec para dispositivos móviles
- Actúa como el punto de aplicación de políticas de QoS a través de la integración de PCRF
- Maneja la traversía NAT y el anclaje de medios
- Enruta llamadas de emergencia a la funcionalidad de E-CSCF
- Mantiene información de ubicación del usuario

#### 2. I-CSCF - Puerta de Enlace de Red y Balanceador de Carga

- Oculta la topología interna de la red de redes externas
- Consulta al HSS para seleccionar el S-CSCF apropiado para los usuarios
- Realiza balanceo de carga de S-CSCF basado en capacidades
- Actúa como el punto de entrada/salida para escenarios de roaming
- Aplica Seguridad de Dominio de Red (NDS/TLS)

#### 3. S-CSCF - Controlador de Sesión Central

- Realiza el registro y autenticación de usuarios
- Mantiene el estado de la sesión para todas las llamadas activas
- Aplica políticas de enrutamiento y lógica de servicio
- Activa Servidores de Aplicaciones basados en IFC (Criterios de Filtro)

- Inicial)
- Se integra con sistemas de cobro (en línea y fuera de línea)
  - Gestiona servicios suplementarios

## Integración con Sistemas de Soporte

OmniCall CSCF se integra con funciones de soporte IMS a través de interfaces Diameter estándar:

<b>Interfaz</b>	<b>De → A</b>	<b>Propósito</b>	<b>Especificación 3GPP</b>
<b>Cx</b>	I-CSCF/S-CSCF ↔ HSS	Autenticación de usuario, recuperación de perfil, asignación de S-CSCF	TS 29.228
<b>Dx</b>	I-CSCF ↔ SLF	Localizador de suscripciones para entornos multi-HSS	TS 29.229
<b>Rx</b>	P-CSCF ↔ PCRF	Autorización de políticas de QoS, control de flujo de medios	TS 29.214
<b>Ro</b>	S-CSCF → OCS	Cobro en línea (control de crédito)	TS 32.299
<b>Rf</b>	S-CSCF → CDF	Cobro fuera de línea (generación de CDR)	TS 32.299
<b>ISC</b>	S-CSCF ↔ AS	Activación de servicios e invocación de servidor de aplicaciones	TS 23.228
<b>Sh</b>	AS ↔ HSS	Acceso del servidor de aplicaciones a datos de usuario	TS 29.328

Para la gestión de pares Diameter, consulte [Operaciones de Diameter](#).

## Flujos de Sesión de Llamadas

Comprender cómo los CSCFs procesan diferentes tipos de sesiones es esencial para las operaciones y la resolución de problemas.

### Flujo de Registro IMS

Cuando un dispositivo se registra en la red IMS, los CSCFs se coordinan para autenticar y autorizar al usuario:

#### Puntos Clave:

- [P-CSCF](#) mantiene la asociación de seguridad IPsec con UE
- [I-CSCF](#) consulta al HSS para encontrar/asignar S-CSCF
- [S-CSCF](#) realiza la autenticación y almacena el perfil del usuario
- El perfil de servicio del usuario (IFC) determina qué Servidores de Aplicaciones serán activados

## **Flujo de Llamada Originada en Móvil**

Cuando un usuario registrado inicia una llamada:

### **Puntos Clave:**

- [P-CSCF](#) coordina con PCRF para el establecimiento del portador de QoS
- [S-CSCF](#) evalúa IFC para determinar la activación del servicio
- **OmniTAS** proporciona servicios de aplicación de telefonía (desvío de llamadas, filtrado, etc.)
- **OmniMessage** maneja el tráfico SMS/MMS cuando es activado por IFC
- Para monitorear llamadas activas, consulte [Gestión de Diálogo S-CSCF](#)

## **Flujo de Llamada de Emergencia (E-CSCF)**

Las llamadas de emergencia reciben un manejo especial para garantizar la conectividad incluso sin un registro IMS completo:

### **Puntos Clave:**

- La funcionalidad de E-CSCF está integrada en [P-CSCF](#)
- Funciona incluso para usuarios no registrados o en roaming
- Incluye almacenamiento de número de devolución de llamada para servicios de emergencia
- Para operaciones de emergencia, consulte [Servicios de Emergencia P-CSCF](#)

## **SMS sobre IMS - Originado en Móvil (3GPP TS 24.341)**

Cuando un usuario envía un SMS a través de IMS, OmniMessage maneja la entrega del mensaje:

### **Puntos Clave:**

- SMS codificado en el método SIP MESSAGE según 3GPP TS 24.341
- Content-Type: application/vnd.3gpp.sms identifica la carga útil de SMS
- [S-CSCF](#) IFC activa **OmniMessage** para tráfico SMS
- OmniMessage se integra con la infraestructura tradicional de SMSC
- Soporta tanto conjuntos de caracteres GSM-7, UCS-2 y mensajes concatenados

---

## **SMS sobre IMS - Terminado en Móvil (3GPP TS 24.341)**

Cuando un SMS llega para un usuario registrado en IMS, OmniMessage lo enruta a través de IMS:

### **Puntos Clave:**

- SMSC reenvía SMS a **OmniMessage** a través de protocolos tradicionales (MAP/SMPP)
- OmniMessage convierte al método SIP MESSAGE
- **S-CSCE** enruta basado en IMPU registrado
- Soporta informes de entrega y notificaciones de estado
- Recaída a SMS tradicional si el usuario no está registrado en IMS

Para operaciones y monitoreo de SMS, consulte [Gestión IFC S-CSCE](#).

---

## Escenarios de Roaming

OmniCall CSCF soporta el **roaming en casa** como lo exige 3GPP/GSMA:

**Roaming en Casa:** Cuando los usuarios hacen roaming a una red visitada, todas las sesiones IMS se enrutan de vuelta a través del S-CSCF de la red de origen. Esto asegura:

- Experiencia de servicio consistente independientemente de la ubicación
- Control de la red de origen sobre la activación de servicios y el cobro
- Acuerdos de roaming simplificados entre operadores
- Cumplimiento con los estándares GSMA PRD IR.92 e IR.94

El I-CSCF de la red visitada consulta al HSS de origen y enruta las solicitudes de registro/sesión al S-CSCF de origen, que luego invoca los servidores de aplicaciones de la red de origen (OmniTAS, OmniMessage, etc.).

Para detalles de configuración de roaming, consulte [Seguridad de Dominio de Red I-CSCF](#).

## Componentes de CSCF

### P-CSCF/E-CSCF - Proxy de Borde y Ancla de Seguridad

El **Proxy-CSCF** es el primer elemento IMS que contacta el equipo del usuario. Sirve como el límite de seguridad y el punto de aplicación de políticas.

#### Funciones Centrales:

- **Gestión de Asociación de Seguridad:** Establece y mantiene túneles IPsec con dispositivos móviles para la protección de señalización y medios
- **Aplicación de Políticas de QoS:** Coordina con PCRF a través de la interfaz Rx para autorizar y aplicar portadores de QoS
- **Traversía NAT:** Maneja la traversía NAT del extremo lejano para dispositivos detrás de NAT/firewalls
- **Compresión:** Soporte SigComp para redes con limitaciones de ancho de banda
- **Ruta de Servicio:** Mantiene la ruta de servicio para solicitudes posteriores

## **Servicios de Emergencia (E-CSCF):**

- Enrutamiento de llamadas de emergencia integrado sin requerir registro IMS completo
- Manejo de información de ubicación para E911/E112
- Mapeo de IMEI a número de devolución de llamada para devoluciones de llamada de emergencia
- Integración con LRF (Función de Recuperación de Ubicación)

## **Tipos de Acceso Soportados:**

- LTE/5G (VoLTE) a través de IPsec
- WiFi (VoWiFi) a través de IPsec
- Banda ancha fija a través de SIP
- Puertas de enlace residenciales de cable/DSL

Para operaciones detalladas, consulte [\*\*Documentación P-CSCF\*\*](#).

---

## **I-CSCF - Ocultamiento de Topología y Balanceo de Carga**

El [\*\*Interrogating-CSCF\*\*](#) actúa como el punto de contacto dentro de la red de un operador para conexiones de otras redes o de la misma red.

### **Funciones Centrales:**

- **Ocultamiento de Topología:** Protege la estructura interna de la red de redes externas
- **Asignación de S-CSCF:** Consulta al HSS a través de la interfaz Cx para asignar S-CSCF a nuevos usuarios
- **Selección de S-CSCF:** Selecciona el S-CSCF apropiado basado en capacidades y carga
- **Proxy de Enrutamiento:** Enruta solicitudes entrantes al S-CSCF asignado
- **Seguridad de Dominio de Red:** Aplica NDS/TLS para la seguridad entre operadores

### **Características Clave:**

- **Soporte Multi-S-CSCF:** Distribuye usuarios a través de múltiples instancias de S-CSCF
- **Coincidencia de Capacidades:** Coincide los requisitos del usuario con las capacidades de S-CSCF
- **Soporte de Roaming:** Maneja tanto escenarios de roaming en casa como de salida local
- **Localizador de Suscripciones:** Soporte de interfaz Dx para entornos multi-HSS

### **Casos de Uso:**

- Punto de interconexión para socios de roaming
- Distribución de carga a través del clúster S-CSCF
- Enrutamiento geográfico para recuperación ante desastres
- Segregación de tráfico MVNO

Para operaciones detalladas, consulte [Documentación I-CSCF](#).

---

## S-CSCF - Controlador de Sesión Central

El **Serving-CSCF** es el componente central de la red IMS, proporcionando control de sesión e inteligencia de servicio.

### Funciones Centrales:

- **Registro:** Autentica a los usuarios y mantiene enlaces de registro
- **Control de Sesión:** Gestiona todos los estados de llamada (establecimiento de diálogo, modificación, terminación)
- **Activación de Servicios:** Evalúa los Criterios de Filtro Inicial (IFC) para invocar Servidores de Aplicaciones
- **Enrutamiento:** Enruta solicitudes SIP basadas en lógica de servicio y preferencias del usuario
- **Integración de Cobro:** Coordina con sistemas de cobro en línea (OCS) y fuera de línea (CDF)

**Activación de Servicios a través de IFC:** El S-CSCF utiliza IFC basados en XML descargados del HSS para determinar cuándo enrutar llamadas a través de Servidores de Aplicaciones (como **OmniTAS** para servicios de telefonía y **OmniMessage** para SMS/MMS):

- **Puntos de Disparo:** Coincidencia en método SIP, Request-URI, Caso de Sesión (originante/terminante)
- **Basado en Prioridad:** IFC procesados en orden de prioridad
- **Cadena de Servicios:** Múltiples AS pueden ser invocados en secuencia (por ejemplo, OmniTAS → OmniMessage)
- **Manejo por Defecto:** Comportamiento configurable cuando AS no está disponible

### Servicios Soportados:

- Desvío de llamadas (ocupado, sin respuesta, incondicional)
- Prohibición de llamadas (salientes, entrantes, roaming)
- Filtrado y selección de llamadas
- Traducción y enrutamiento de números
- Cobro prepago/postpago
- Seguimiento de uso y aplicación de cuotas
- Servicios suplementarios (espera de llamada, retención, transferencia)

## **Características de Escalabilidad:**

- Almacenamiento de diálogo distribuido
- Manejo de sesión con estado
- Perfiles de usuario respaldados por base de datos
- Escalado horizontal a través de la distribución I-CSCF

Para operaciones detalladas, consulte [\*\*Documentación S-CSCF\*\*](#).

---

## **Gestión de Interfaces Diameter**

OmniCall CSCF proporciona gestión integral de pares Diameter a través de todos los componentes CSCF.

### **Aplicaciones Diameter Soportadas:**

<b>Aplicación</b>	<b>Interfaz</b>	<b>ID de App</b>	<b>Usado Por</b>	<b>Propósito</b>
<b>3GPP Cx</b>	Cx	16777216	I-CSCF, S-CSCF	Autenticación de usuario, recuperación de perfil
<b>3GPP Dx</b>	Dx	16777216	I-CSCF	Ubicación de suscripción en multi-HSS
<b>3GPP Rx</b>	Rx	16777236	P-CSCF	Autorización de políticas, control de QoS
<b>3GPP Ro</b>	Ro	4 (CC)	S-CSCF	Cobro en línea (control de crédito)
<b>3GPP Rf</b>	Rf (Contabilidad)	3	S-CSCF	Cobro fuera de línea (CDR)
<b>3GPP Sh</b>	Sh	16777217	AS	Acceso a datos de usuario desde AS

### **Capacidades Diameter:**

- Descubrimiento automático de pares a través de DNS
- Soporte de failover y redundancia
- Gestión de conexiones y watchdog
- Estadísticas y monitoreo por par
- Habilitar/deshabilitar pares dinámicamente

Para operaciones y resolución de problemas de Diameter, consulte [\*\*Guía de Gestión de Diameter\*\*](#).

## **Operaciones Comunes**

OmniCall CSCF proporciona capacidades operativas integrales a través de su panel de control basado en web. Esta sección cubre tareas operativas comunes y su importancia.

## Gestión de Registro

### Comprendiendo los Registros IMS:

El registro IMS es un proceso de dos niveles:

- **Contacto P-CSCF:** El equipo del usuario establece conexión IPsec/SIP con P-CSCF
- **Registro S-CSCF:** Registro IMS completo con autenticación a través de HSS

### Operaciones Clave de Registro:

- **Ver registros activos** en P-CSCF y S-CSCF
- **Consultar usuarios específicos** por IMPU, IMSI o dirección IP
- **Monitorear estado de registro** (autenticado, activo, expirado)
- **Forzar desregistro** para resolución de problemas o propósitos administrativos
- **Rastrear caducidad de registro** para identificar problemas de re-registro

Para procedimientos de registro detallados, consulte:

- [Gestión de Contactos P-CSCF](#)
  - [Operaciones de Registro S-CSCF](#)
- 

## Monitoreo de Sesiones de Llamadas

### Gestión de Diálogo (Sesión):

El S-CSCF mantiene el estado de todas las sesiones IMS activas (llamadas). Los operadores pueden:

- **Monitorear diálogos activos** incluyendo Call-ID, participantes y estado de la sesión
- **Ver detalles del diálogo** como SDP (parámetros de medios), conjuntos de rutas y temporizadores
- **Terminar diálogos** para resolución de problemas o situaciones de emergencia
- **Rastrear duración de la sesión** y detectar sesiones de larga duración o atascadas

### Estados de Sesión:

- **Temprano:** La llamada está sonando, aún no respondida
- **Confirmado:** Llamada activa con medios fluyendo
- **Terminado:** Llamada finalizada normalmente

Para procedimientos de monitoreo de llamadas, consulte [Gestión de Diálogo S-CSCE](#).

---

## Activación de Servicios y Gestión de IFC

**Los Criterios de Filtro Inicial (IFC)** determinan cuándo y cómo el S-CSCF enruta sesiones a servidores de aplicaciones como **OmniTAS** y **OmniMessage**.

### Operaciones de IFC:

- **Volcar IFC del usuario** para ver el perfil de servicio configurado desde HSS
- **Probar coincidencia de IFC** con escenarios de llamada simulados
- **Verificar enrutamiento de AS** para asegurar la invocación de servicio adecuada
- **Depurar fallos de servicio** examinando la evaluación de puntos de disparo

### Ejemplo de Estructura IFC:

```
<InitialFilterCriteria>
  <Priority>10</Priority>
  <TriggerPoint>
    <SPT><Method>INVITE</Method></SPT>
    <SPT><SessionCase>0</SessionCase><!-- Originante --></SPT>
  </TriggerPoint>
  <ApplicationServer>
    <ServerName>sip:omnitas.ims.example.com</ServerName>
    <DefaultHandling>0</DefaultHandling><!-- Debe invocar -->
  </ApplicationServer>
</InitialFilterCriteria>
```

Para pruebas y resolución de problemas de IFC, consulte [Operaciones IFC S-CSCE](#).

---

## Gestión de Pares Diameter

### Monitoreo de Conectividad Diameter:

OmniCall CSCF depende de interfaces Diameter para HSS, PCRF y la integración de cobro. Los operadores pueden:

- **Monitorear estado de pares** (*I\_Open* = conectado, *Closed* = desconectado)
- **Ver capacidades de pares** (aplicaciones Diameter soportadas)
- **Habilitar/deshabilitar pares** para mantenimiento o pruebas de failover

- **Rastrear estadísticas de pares** (solicitudes, fallos, timeouts)

### Conexiones Diameter Críticas:

- **Cx a HSS** (I-CSCF, S-CSCF): Autenticación de usuario y perfiles
- **Rx a PCRF** (P-CSCF): Política de QoS y control de portadores
- **Ro a OCS** (S-CSCF): Cobro en línea y control de crédito

Para resolución de problemas de Diameter, consulte [Guía de Operaciones de Diameter](#).

---

## Gestión de Servicios de Emergencia

### Operaciones E-CSCF:

El manejo de llamadas de emergencia requiere atención operativa especial:

- **Monitorear mapeos de IMEI a números de devolución de llamada** para devoluciones de llamada de emergencia
- **Verificar disponibilidad de información de ubicación** para E911/E112
- **Probar enrutamiento de llamadas de emergencia** sin conexión real a PSAP
- **Gestionar registro de emergencia** para dispositivos no provisionados

Los servicios de emergencia funcionan incluso para:

- Usuarios no registrados
- Usuarios sin SIM/credenciales inválidas
- Usuarios en roaming de otras redes

Para operaciones de servicios de emergencia, consulte [Servicios de Emergencia P-CSCE](#).

---

## Gestión de Tablas Hash

### Estructuras de Datos en Memoria Compartida:

Los nodos CSCF utilizan tablas hash en memoria para datos críticos de rendimiento:

Tabla Hash	CSCF	Propósito	TTL
imei_msisdn	P- CSCF	Mapeo de devolución de llamada de emergencia	24 horas
service_routes	P- CSCF	Rutas de servicio en caché	Caducidad de registro
auth	S-	Vectores de autenticación	Tiempo de desafío

<b>Tabla Hash</b>	<b>CSCF</b>	<b>Propósito</b>	<b>TTL</b>
	CSCF		

## Operaciones:

- **Ver contenido de tablas** para resolución de problemas
- **Eliminar entradas específicas** para limpiar datos obsoletos
- **Vaciar tablas completas** para recuperación de emergencia (usar con precaución)

Para operaciones de UI detalladas, consulte la [Guía de Operaciones de UI Web](#).

# Resolución de Problemas

Esta sección cubre problemas operativos comunes y sus estrategias de resolución.

## Fallos de Registro

**Síntomas:** Usuarios incapaces de registrarse en la red IMS, timeouts de registro

### Causas Raíz Comunes:

#### 1. Problemas de Conectividad HSS

- Verifique el estado del par Diameter Cx en [I-CSCF](#) y [S-CSCF](#)
- Verifique que el HSS sea accesible y responda a solicitudes UAR/MAR
- Verifique problemas de enrutamiento Diameter

#### 2. Fallos de Autenticación

- Verifique las credenciales del usuario provisionadas en HSS
- Verifique la generación de vectores de autenticación (MAR/MAA)
- Verifique la compatibilidad del algoritmo AKA (Milenage)

#### 3. Conectividad P-CSCF

- Verifique el establecimiento de SA IPsec para dispositivos móviles
- Verifique la traversía NAT para dispositivos detrás de NAT
- Verifique el descubrimiento de P-CSCF (DNS, DHCP o configuración estática)

#### 4. Asignación de S-CSCF

- Verifique la lógica de selección de S-CSCF de I-CSCF
- Verifique que las capacidades de S-CSCF coincidan con los requisitos del usuario
- Verifique la capacidad de S-CSCF (límites de registro)

**Para resolución de problemas detallada**, consulte las guías específicas de componentes:

- [Resolución de Problemas P-CSCF](#)
  - [Resolución de Problemas I-CSCF](#)
  - [Resolución de Problemas S-CSCF](#)
- 

## Fallos en la Configuración de Llamadas

**Síntomas:** Las llamadas no se establecen, reciben errores SIP 4xx/5xx

**Causas Raíz Comunes:**

### 1. Usuario No Registrado

- Verifique que tanto los usuarios originantes como los terminantes estén registrados en IMS
- Verifique el estado de registro a través de [S-CSCF](#)

### 2. Problemas de IFC/Activación de Servicio

- Verifique el IFC descargado de HSS (verifique SAR/SAA)
- Pruebe la coincidencia de IFC para el escenario de llamada
- Verifique la disponibilidad de OmniTAS/OmniMessage si se activa

### 3. Problemas de QoS/PCRF

- Verifique el estado del par Diameter Rx en P-CSCF
- Verifique la autorización de políticas de QoS de PCRF
- Verifique que los recursos de portador estén disponibles en la red de acceso

### 4. Fallos de Enrutamiento

- Verifique el enrutamiento de destino (ENUM, traducción de números)
  - Verifique la configuración de interconexión/MGCF para llamadas PSTN
  - Verifique el enrutamiento de roaming para llamadas fuera de la red
- 

## Problemas de Conectividad Diameter

**Síntomas:** El par Diameter muestra estado "Closed", operaciones que expiran

**Pasos de Diagnóstico:**

- Verificar Estado de Par:** Utilice el panel de control para ver el estado del par Diameter
- Verificar Conectividad de Red:** Pruebe la accesibilidad IP al par Diameter (puerto 3868)
- Verificar Capacidades:** Verifique que los IDs de Aplicación coincidan entre pares
- Revisar Watchdog:** Verifique los intercambios de watchdog Diameter (DWR/DWA)

## Interfaces Diameter Críticas:

Interfaz	Impacto si Está Caído	Prioridad de Recuperación
<b>Cx (HSS)</b>	No se permiten nuevos registros, no se actualizan IFC	Crítico - inmediato
<b>Rx (PCRF)</b>	Sin QoS para nuevas llamadas	Alto - dentro de minutos
<b>Ro (OCS)</b>	Sin cobro prepago, el servicio puede continuar	Alto - depende de la política

Para resolución de problemas de Diameter, consulte [Guía de Operaciones de Diameter](#).

---

## Problemas de Entrega de SMS

**Síntomas:** SMS no entregados a través de IMS, recaída a SMSC legado

### Causas Raíz Comunes:

#### 1. OmniMessage No Activado

- Verifique que el IFC esté configurado para activar OmniMessage para solicitudes MESSAGE
- Verifique la prioridad del IFC (debería ser más alta que otros AS)
- Pruebe la coincidencia de IFC con SMS simulado

#### 2. Integración con SMSC

- Verifique la conectividad de OmniMessage a SMSC (MAP/SMPP)
- Verifique la conversión de formato de mensaje (SIP MESSAGE ↔ SMS PDU)
- Verifique el enrutamiento de suscriptores en SMSC

#### 3. Problemas de Tipo de Contenido

- Verifique Content-Type: application/vnd.3gpp.sms en SIP MESSAGE

- Verifique la codificación de conjunto de caracteres (GSM-7, UCS-2)

Para resolución de problemas de SMS, consulte [Gestión IFC S-CSCE](#).

---

## Problemas de Llamadas de Emergencia

**Síntomas:** Las llamadas de emergencia no se enrutan a PSAP, la ubicación no se incluye

**Causas Raíz Comunes:**

### 1. Detección E-CSCF

- Verifique la detección de URN de emergencia (urn:service:sos)
- Verifique las reglas de enrutamiento de emergencia en P-CSCF
- Verifique la conectividad LRF

### 2. Información de Ubicación

- Verifique el encabezado de ubicación en SIP INVITE
- Verifique el mapeo de IMEI a número de devolución de llamada para devoluciones
- Pruebe la recuperación de ubicación desde LRF

### 3. Enrutamiento a PSAP

- Verifique la configuración de la tabla de enrutamiento de PSAP
- Verifique la generación de ESQK (Clave de Consulta de Servicio de Emergencia)
- Verifique el tronco/interconexión a PSAP

Para operaciones de servicios de emergencia, consulte [Servicios de Emergencia P-CSCE](#).

---

## Degradación del Rendimiento

**Síntomas:** Configuración de llamada lenta, retrasos en el registro, alta latencia

**Diagnóstico:**

1. **Monitorear Métricas de Prometheus:** Verifique las métricas de rendimiento de CSCF (ver [Referencia de Métricas](#) para definiciones completas de métricas)
2. **Rendimiento de Base de Datos:** Verifique los tiempos de consulta de base de datos de S-CSCF
3. **Latencia de Red:** Verifique la latencia entre nodos CSCF

4. **Utilización de Recursos:** Monitoree CPU, memoria y red en servidores CSCF

### Consideraciones de Escalabilidad:

- **P-CSCF:** ~50,000 SAs IPsec por instancia (VoLTE); 100,000+ a través de OmniePDG (VoWiFi)
- **I-CSCF:** Sin estado, se escala horizontalmente (1,000-5,000 registros/segundo por instancia)
- **S-CSCF:** 100,000-500,000 registros por instancia; 20,000-100,000 diálogos concurrentes

Para planificación de capacidad y dimensionamiento detallado, consulte la [\*\*Guía de Capacidad y Dimensionamiento\*\*](#).

Para monitoreo de rendimiento y métricas, consulte la [\*\*Guía de Operaciones de UI Web\*\*](#).

## Documentación Adicional

### Guías de Operaciones Específicas de Componentes

Para operaciones detalladas y resolución de problemas para cada componente CSCF:

- [\*\*Guía de Operaciones P-CSCF/E-CSCE\*\*](#) - Proxy de borde, asociaciones de seguridad, servicios de emergencia
- [\*\*Guía de Operaciones I-CSCF\*\*](#) - Selección de S-CSCF, ocultamiento de topología, roaming
- [\*\*Guía de Operaciones S-CSCF\*\*](#) - Registro, gestión de diálogos, operaciones IFC
- [\*\*Guía de Operaciones Diameter\*\*](#) - Gestión y resolución de problemas de pares Diameter
- [\*\*Guía de Operaciones UI Web\*\*](#) - Uso del panel de control, monitoreo y administración
- [\*\*Referencia de Métricas\*\*](#) - Referencia completa de todas las métricas de Prometheus de P-CSCF, I-CSCF y S-CSCF
- [\*\*Guía de Capacidad y Dimensionamiento\*\*](#) - Dimensionamiento de despliegue, planificación de capacidad, ajuste de rendimiento

### Cumplimiento Regulatorio

- [\*\*Cumplimiento de Intercepción ANSSI R226\*\*](#) - Capacidades de intercepción legal según lo requerido por las autoridades regulatorias francesas

## Referencia de Normas 3GPP

OmniCall CSCF implementa las siguientes especificaciones 3GPP:

Especificación	Título	Relevancia
<b>TS 23.228</b>	Subsistema Multimedia IP (IMS) - Etapa 2	Arquitectura central IMS
<b>TS 24.229</b>	Protocolo de control de llamada multimedia IP (SIP)	Perfil SIP IMS
<b>TS 29.228</b>	Interfaces Cx y Dx (CSCF-HSS)	Datos de usuario y autenticación
<b>TS 29.214</b>	Interfaz Rx (P-CSCF-PCRF)	Control de políticas de QoS
<b>TS 32.299</b>	Cobro - Aplicaciones Diameter	Cobro en línea/fuera de línea
<b>TS 24.341</b>	SMS sobre redes IP	SMS sobre IMS
<b>TS 23.167</b>	Servicios de emergencia	E-CSCF y llamadas de emergencia

## Cumplimiento de Normas GSMA

OmniCall CSCF es completamente compatible con los perfiles IMS de GSMA, asegurando interoperabilidad con dispositivos comerciales.

### IR.92 - Perfil IMS para Voz y SMS (VoLTE)

**GSMA PRD IR.92** define el perfil IMS obligatorio para servicios VoLTE, asegurando que los dispositivos comerciales funcionen sin problemas sin configuración específica del operador o retrasos en la certificación de dispositivos.

#### Beneficios Clave de IR.92 para OmniCall CSCF:

- ✓ **Soporte para Dispositivos de Mercado Abierto:** Cualquier smartphone compatible con IR.92 funciona de inmediato—sin paquetes personalizados de operador, APNs propietarios o provisión especial requerida
- ✓ **Perfil SIP Estandarizado:** Los dispositivos utilizan encabezados SIP estándar, autenticación y flujos de registro como se define en 3GPP TS 24.229
- ✓ **Interoperabilidad de Códigos:** El soporte de códec obligatorio (AMR-WB para voz HD) asegura calidad de voz consistente en todos los dispositivos
- ✓ **SMS sobre IMS:** La integración con **OmniMessage** proporciona entrega de SMS basada en estándares (TS 24.341) a cualquier dispositivo compatible con IR.92

✓ **Servicios de Emergencia:** El manejo de números de emergencia E.164 (911, 112, etc.) funciona en todos los dispositivos compatibles sin configuración especial

✓ **Consistencia en Roaming:** El roaming en casa asegura que los usuarios obtengan la misma experiencia VoLTE al visitar otras redes compatibles con IR.92

**Lo que Esto Significa:** Los operadores pueden lanzar servicios VoLTE de inmediato con dispositivos de consumo existentes (iPhone, Samsung, Google Pixel, etc.) sin esperar la certificación personalizada de dispositivos o actualizaciones de paquetes de operador.

## **IR.94 - Perfil IMS para Voz, Video y SMS (VoWiFi)**

**GSMA PRD IR.94** extiende IR.92 para incluir Voz sobre WiFi, habilitando servicios VoLTE sobre redes WiFi no confiables.

### **Arquitectura VoWiFi con OmniCall:**

#### **Componentes VoWiFi:**

- **OmniePDG:** Gateway de Datos de Paquete Evolucionado - Proporciona terminación de túnel IPsec para acceso WiFi no confiable
- **OmniCall P-CSCF:** Maneja registros VoWiFi de manera idéntica a VoLTE (mismas rutas de servicio, misma activación de IFC)
- **Transferencia Sin Problemas:** Los dispositivos pueden moverse entre LTE y WiFi sin interrupción de llamada

#### **Beneficios de IR.94:**

- Los mismos beneficios de IR.92 se aplican a VoWiFi
- Los dispositivos descubren automáticamente ePDG a través de DNS (sin configuración manual)
- Un solo registro IMS cubre tanto VoLTE como VoWiFi
- Extensión de cobertura interior sin femtoceldas o DAS

Para operaciones de ePDG y resolución de problemas de VoWiFi, consulte

[\*\*Documentación OmniePDG\*\*](#).

### **Otras Normas GSMA**

- **IR.51** - Estructura de Base de Datos de Roaming GSMA
- **IR.88** - Directrices de Roaming LTE
- **AA.80** - Configuración de Dispositivos IMS/RCS y Servicios de Soporte

### **Diferenciación del Producto**

#### **¿Por Qué Elegir OmniCall CSCF?**

- ✓ **Soporte de Dispositivos Plug-and-Play:** Cumple con GSMA IR.92/IR.94 - funciona con iPhones, teléfonos Android y dispositivos de línea fija de mercado sin paquetes personalizados de operador o retrasos en la certificación de dispositivos
- ✓ **Solución IMS Completa:** Todos los componentes CSCF (P/I/S/E) más OmniePDG para VoWiFi en una plataforma unificada
- ✓ **Convergencia Fijo-Móvil:** Núcleo IMS unificado para servicios móviles (VoLTE/VoWiFi), banda ancha fija y servicios de telefonía por cable
- ✓ **Provisión Sin Toque:** El descubrimiento de dispositivos basado en estándares (DNS, DHCP) significa que los usuarios pueden cambiar tarjetas SIM entre dispositivos sin soporte de TI
- ✓ **Gestión Empresarial:** Panel de control basado en web con monitoreo en tiempo real, diagnósticos y resolución de problemas
- ✓ **Escalabilidad de Grado Carrier:** Escalado horizontal para soportar millones de suscriptores con tiempos de configuración de llamada de menos de un segundo
- ✓ **Ecosistema de Servidores de Aplicaciones:** Integración sin problemas con OmniTAS (servicios de telefonía) y OmniMessage (SMS/MMS)
- ✓ **Servicios de Emergencia:** E-CSCF integrado con soporte E911/E112, servicios de ubicación y manejo de devoluciones de llamada
- ✓ **Interoperabilidad Primero:** Cumplimiento total de 3GPP y GSMA asegura que los acuerdos de roaming y la interconexión funcionen de inmediato
- ✓ **Prueba de Producción:** Desplegado en redes de nivel 1, nivel 2 y MVNO en todo el mundo sirviendo a millones de suscriptores

## Glosario

### Términos de Arquitectura IMS

- **3GPP:** Proyecto de Asociación de Tercera Generación - Organismo de estándares para telecomunicaciones móviles
- **AKA:** Acuerdo de Autenticación y Clave - Mecanismo de seguridad para IMS
- **AoR:** Dirección de Registro - Identidad SIP (por ejemplo, sip:user@domain.com)
- **CSCF:** Función de Control de Sesión de Llamadas - Entidad de control de sesión IMS
- **DAS:** Sistema de Antena Distribuida - Solución de cobertura interior
- **E-CSCF:** CSCF de Emergencia - Función de enrutamiento de llamadas de emergencia
- **ePDG:** Gateway de Datos de Paquete Evolucionado - Punto final de túnel

IPsec para acceso WiFi no confiable

- **ENUM:** Mapeo de Número E.164 - Traducción basada en DNS
- **ESQK:** Clave de Consulta de Servicio de Emergencia - Identificador de llamada de emergencia
- **FMC:** Convergencia Fijo-Móvil - Servicios unificados a través de tipos de acceso
- **GSMA:** Asociación GSM - Organización de estándares de la industria móvil
- **HD Voice:** Voz de Alta Definición - Audio de banda ancha utilizando códec AMR-WB
- **HSS:** Servidor de Suscriptores - Base de datos de suscriptores y autenticación
- **I-CSCF:** CSCF Interrogante - Punto de entrada a la red y ocultamiento de topología
- **IFC:** Criterios de Filtro Inicial - Reglas de activación de servicio basadas en XML
- **IMS:** Subsistema Multimedia IP - Arquitectura 3GPP para servicios basados en IP
- **IMPU:** Identidad Pública Multimedia IP - Identidad pública del usuario (URI SIP o URI tel)
- **IMSI:** Identidad Internacional de Suscriptor Móvil - Identificador de suscriptor
- **IR.92:** Perfil IMS GSMA para Voz y SMS - Estándar de interoperabilidad VoLTE
- **IR.94:** Perfil IMS GSMA para Video Conversacional - Estándar de interoperabilidad VoWiFi
- **ISC:** Control de Servicio IMS - Interfaz entre S-CSCF y Servidores de Aplicaciones
- **LRF:** Función de Recuperación de Ubicación - Servicios de ubicación de emergencia
- **MGCF:** Función de Control de Gateway de Medios - Interconexión PSTN
- **MVNO:** Operador de Red Móvil Virtual - Operador sin infraestructura de radio propia
- **NDS:** Seguridad de Dominio de Red - Seguridad entre operadores (TLS/ IPsec)
- **P-CSCF:** Proxy CSCF - Proxy de borde y primer punto de contacto
- **PSAP:** Punto de Respuesta de Seguridad Pública - Centro de llamadas de servicios de emergencia
- **RCS:** Servicios de Comunicación Ricos - Servicios de mensajería mejorados
- **S-CSCF:** CSCF de Servicio - Control de sesión central y registro
- **SPT:** Punto de Disparo de Servicio - Condición de coincidencia en IFC (Método, Request-URI, etc.)
- **SWu:** Interfaz 3GPP entre UE y ePDG (IPsec/IKEv2)
- **UE:** Equipo del Usuario - Dispositivo del usuario final (teléfono, tableta, terminal fija)
- **VoLTE:** Voz sobre LTE - Servicios de voz a través de la red de datos LTE
- **VoWiFi:** Voz sobre WiFi - Servicios de voz a través de redes WiFi no confiables

## Términos del Protocolo Diameter

- **AAA:** Autenticación, Autorización, Contabilidad
- **AVP:** Par Atributo-Valor - Elemento de datos del mensaje Diameter
- **CCR/CCA:** Solicitud/Respuesta de Control de Crédito - Mensajes de cobro en línea
- **CDF:** Función de Datos de Cobro - Recolector de cobro fuera de línea
- **Cx:** Interfaz Diameter entre I-CSCF/S-CSCF y HSS
- **Diameter:** Protocolo AAA utilizado en IMS (evolución de RADIUS)
- **Dx:** Interfaz Diameter entre I-CSCF y SLF (localizador de suscripciones)
- **DWR/DWA:** Solicitud/Respuesta de Vigilancia de Dispositivo - Verificación de salud de par
- **MAR/MAA:** Solicitud/Respuesta de Autenticación Multimedia - Solicitud de vector de autenticación
- **OCS:** Sistema de Cobro en Línea - Cobro en tiempo real y control de crédito
- **PCRF:** Función de Reglas de Políticas y Cobro - Servidor de políticas de QoS
- **Rf:** Interfaz Diameter para cobro fuera de línea (contabilidad)
- **Ro:** Interfaz Diameter para cobro en línea (control de crédito)
- **Rx:** Interfaz Diameter entre P-CSCF y PCRF (autorización de QoS)
- **SAR/SAA:** Solicitud/Respuesta de Asignación de Servidor - Descarga de perfil de usuario
- **Sh:** Interfaz Diameter entre AS y HSS (acceso a datos de usuario)
- **SLF:** Función de Localización de Suscripciones - Ubicación de HSS en entorno multi-HSS
- **UAR/UAA:** Solicitud/Respuesta de Autorización de Usuario - Selección de S-CSCF

## Términos del Producto OmniCall

- **OmniCall CSCF:** Solución completa de CSCF IMS (este producto)
- **OmniePDG:** Gateway de Datos de Paquete Evolucionado - Terminación de túnel IPsec para VoWiFi (cumple con IR.94)
- **OmniTAS:** Servidor de Aplicaciones de Telefonía - Proporciona servicios de voz suplementarios
- **OmniMessage:** Servidor de Aplicaciones de Mensajería - SMS/MMS sobre IMS (TS 24.341)

## Términos del Protocolo SIP

- **Diálogo:** Estado de sesión SIP entre dos puntos finales
- **INVITE:** Método SIP para establecimiento de sesión (llamadas)
- **MESSAGE:** Método SIP para mensajería instantánea (incluyendo SMS sobre IMS)
- **REGISTER:** Método SIP para registro de usuario
- **SDP:** Protocolo de Descripción de Sesión - Parámetros de medios (códigos, puertos)

- **SIP:** Protocolo de Inicio de Sesión - Protocolo de señalización para IMS



# Guía de Operaciones de Diameter

## Tabla de Contenidos

1. [Descripción General](#)
2. [Diameter en la Arquitectura IMS](#)
3. [Interfaces de Diameter](#)
4. [Gestión de Pares a través de la Interfaz Web](#)
5. [Códigos de Resultado de Diameter](#)
6. [Problemas Comunes](#)

## Descripción General

Diameter es el protocolo de autenticación, autorización y contabilidad (AAA) utilizado en toda la arquitectura IMS. OmniCall CSCF utiliza Diameter para comunicarse con elementos de red críticos, incluyendo HSS, PCRF y OCS.

### ¿Qué es Diameter?

Diameter (RFC 6733) es el sucesor de RADIUS, diseñado para escenarios modernos de AAA:

- **Transporte confiable** a través de TCP/SCTP (vs. UDP en RADIUS)
- **Extensible** a través de módulos específicos de aplicación
- **Arquitectura** de pares (no solo cliente-servidor)
- Conexiones **con estado** con monitoreo de watchdog
- Manejo de errores y códigos de resultado **estandarizados**

### Diameter en CSCF

Cada componente de CSCF utiliza interfaces de aplicación Diameter específicas:

CSCF Interfaz	ID de Aplicación	Conectado a	Propósito
I-CSCF	Cx	16777216	HSS Selección de S-CSCF, ubicación del usuario
S-CSCF	Cx	16777216	HSS Autenticación del usuario, descarga de perfil
S-CSCF	Sh	16777217	HSS Acceso a datos del usuario (opcional)
P-CSCF	Rx	16777236	PCRF Control de política de QoS y portadora
S-CSCF	Ro	4	OCS Carga en línea (control de crédito)

<b>CSCF Interfaz</b>	<b>ID de Aplicación</b>	<b>Conectado a</b>	<b>Propósito</b>
S-CSCF Rf	3	CDF	Carga fuera de línea (contabilidad)

## Diameter en la Arquitectura IMS

### Descripción General de la Red

## Interfaces de Diameter

### Interfaz Cx (CSCF ↔ HSS)

La interfaz Cx es utilizada por I-CSCF y S-CSCF para la autenticación de usuarios y gestión de perfiles.

**Especificación 3GPP:** TS 29.228

#### Operaciones de I-CSCF

##### Solicitud de Autorización de Usuario (UAR) / Respuesta de Autorización de Usuario (UAA):

- **Propósito:** Consultar al HSS sobre la asignación o capacidades de S-CSCF
- **Disparador:** REGISTRO recibido del usuario
- **Caso de Uso:** I-CSCF necesita enrutar el registro al S-CSCF apropiado

##### Solicitud de Información de Ubicación (LIR) / Respuesta de Información de Ubicación (LIA):

- **Propósito:** Consultar al HSS sobre el S-CSCF actual del usuario
- **Disparador:** INVITAR o MENSAJE recibido para el usuario que termina
- **Caso de Uso:** I-CSCF necesita enrutar la sesión al S-CSCF del usuario

#### Operaciones de S-CSCF

##### Solicitud de Autenticación Multimedia (MAR) / Respuesta de Autenticación Multimedia (MAA):

- **Propósito:** Recuperar vectores de autenticación del HSS
- **Disparador:** REGISTRO inicial (antes del desafío)
- **Caso de Uso:** S-CSCF necesita desafiar al usuario para la autenticación IMS AKA

##### Solicitud de Asignación de Servidor (SAR) / Respuesta de Asignación de Servidor (SAA):

- **Propósito:** Informar al HSS sobre el estado del registro, descargar el perfil

- **Propósito:** del usuario
- **Disparador:** Autenticación exitosa (después de MAR/MAA)
- **Caso de Uso:** S-CSCF descarga IFC y perfil de servicio para el usuario

El AVP User-Data en SAA contiene el perfil completo del usuario, incluyendo:

- Identidades públicas
- Criterios de Filtro Inicial (IFC) para el desencadenamiento de servicios
- Identificadores de perfiles de medios suscritos
- Información de carga

### **Solicitud de Terminación de Registro (RTR) / Respuesta de Terminación de Registro (RTA):**

- **Propósito:** Deregistro iniciado por HSS (empuje desde HSS)
- **Disparador:** Deregistro administrativo, cambio de suscripción
- **Caso de Uso:** HSS instruye a S-CSCF para deregistrar a un usuario

### **Interfaz Rx (P-CSCF ↔ PCRF)**

La interfaz Rx proporciona control de políticas y QoS para sesiones IMS.

**Especificación 3GPP:** TS 29.214

### **Solicitud AA (AAR) / Respuesta AA (AAA):**

- **Propósito:** Solicitar autorización de QoS para la sesión de medios
- **Disparador:** Intercambio de oferta/respuesta SDP en SIP INVITE
- **Caso de Uso:** P-CSCF solicita al PCRF autorizar recursos de portadora

### **Solicitud de Reautenticación (RAR) / Respuesta de Reautenticación (RAA):**

- **Propósito:** Actualización de política iniciada por PCRF (empuje desde PCRF)
- **Disparador:** Cambio de política, modificación de portadora
- **Caso de Uso:** PCRF instruye a P-CSCF para actualizar la política de QoS

### **Solicitud de Terminación de Sesión (STR) / Respuesta de Terminación de Sesión (STA):**

- **Propósito:** Liberar la sesión Rx y los recursos de portadora
- **Disparador:** Terminación de llamada (BYE recibido)
- **Caso de Uso:** P-CSCF informa al PCRF para liberar recursos de QoS

### **Interfaz Ro (S-CSCF ↔ OCS)**

La interfaz Ro proporciona carga en línea (control de crédito).

**Especificación 3GPP:** TS 32.299

### **Solicitud de Control de Crédito (CCR) / Respuesta de Control de Crédito**

**(CCA):**

- **Propósito:** Autorización y débito de crédito en tiempo real
- **Disparador:** Configuración de llamada, durante la llamada, terminación de llamada
- **Caso de Uso:** Carga prepago, verificaciones de crédito en tiempo real

Tipos:

- **CCR-Initial:** Solicitar crédito al inicio de la llamada
- **CCR-Update:** Actualizar cuota durante la llamada
- **CCR-Terminate:** Reportar uso final al final de la llamada

## Gestión de Pares a través de la Interfaz Web

OmniCall CSCF proporciona un panel de control basado en web para la gestión de pares Diameter.

**Acceso:** Navegar a la pestaña **Diameter** en el panel de control (<http://<cscf-server>:4000/diameter>)

### Visualización del Estado del Par

La página de gestión de Diameter muestra:

#### Información Resumida

- **Reino:** Reino Diameter
- **Identidad:** Host de Origen de Diameter
- **Conteo de Pares:** Número de pares configurados
- **Trabajadores:** Conteo de trabajadores CDP
- **Longitud de Cola:** Transacciones pendientes
- **Tiempo de Espera de Conexión:** Tiempo de espera de conexión (segundos)
- **Tiempo de Espera de Transacción:** Tiempo de espera de transacción (segundos)
- **Aceptar Pares Desconocidos:** Bandera de política

#### Lista de Pares

Tabla de todos los pares Diameter con las siguientes columnas:

Columna	Descripción
<b>FQDN</b>	Nombre de dominio completamente calificado del par
<b>Estado</b>	Estado de conexión (I_Open, Closed, etc.)
<b>Estado</b>	Habilitado o Deshabilitado
<b>Último Usado</b>	Tiempo desde la última transacción
<b>Aplicaciones</b>	Número de aplicaciones Diameter soportadas

## Operaciones de Pares

### Habilitar Par:

1. Localizar par deshabilitado en la tabla
2. Hacer clic en el botón **Habilitar**
3. El par intentará establecer conexión

### Deshabilitar Par:

1. Localizar par habilitado en la tabla
2. Hacer clic en el botón **Deshabilitar**
3. Confirmar acción
4. La conexión del par se terminará de manera controlada

### Ver Aplicaciones:

1. Hacer clic en la fila del par para expandir
2. Ver lista de aplicaciones Diameter soportadas con nombres de interfaz

La vista expandida del par muestra todas las aplicaciones Diameter soportadas:

- **16777216:10415** - 3GPP Cx/Dx (comunicación HSS para I-CSCF/S-CSCF)
- **16777236:10415** - 3GPP Rx (política de QoS PCRF para P-CSCF)
- **16777238:0** - 3GPP Ro (carga en línea)
- Otros IDs de aplicación soportados e IDs de proveedor

El panel de control mapea automáticamente los IDs de Aplicación Diameter a los nombres de interfaz 3GPP:

- **Cx/Dx** (16777216:10415)
- **Sh/Dh** (16777217:10415)
- **Rx** (16777236:10415)
- **Ro** (16777238:10415/0/5535/13019)
- **Gx** (16777224:10415)
- **S6a/S6d** (16777251:10415)
- Y muchos más (ver `diameter_live.ex` para la lista completa)

## Estados de los Pares

Estado	Descripción
<b>I_Open</b>	Conexión abierta y operativa
<b>Closed</b>	No se ha establecido conexión
<b>Wait-Conn-Ack</b>	Conexión iniciada, esperando respuesta
<b>Wait-I-CEA</b>	CER enviado, esperando CEA

Para gestión detallada de pares: Ver [Guía de Operaciones de la Interfaz Web](#)

# Códigos de Resultado de Diameter

Códigos de resultado comunes y sus significados:

<b>Código</b>	<b>Nombre</b>	<b>Significado</b>	<b>Acción</b>
<b>2xxx</b>	<b>Éxito</b>		
2001	DIAMETER_SUCCESS	Operación exitosa	Ninguna
<b>3xxx</b>	<b>Errores de Protocolo</b>		
3002	DIAMETER_UNABLE_TO_DELIVER	No se puede enrutar al destino	Verificar conectividad del par
3003	DIAMETER_REALM_NOT_SERVED	Reino no reconocido	Verificar configuración del reino
3007	DIAMETER_APPLICATION_UNSUPPORTED	Aplicación no soportada	Verificar Application-Id
<b>4xxx</b>	<b>Fallos Transitorios</b>		
4001	DIAMETER_AUTHENTICATION_REJECTED	Autenticación fallida	Verificar credenciales
4010	DIAMETER_USER_UNKNOWN	Usuario no provisionado	Verificar aprovisionamiento en HSS
<b>5xxx</b>	<b>Fallos Permanentes</b>		
5001	DIAMETER_AVP_UNSUPPORTED	AVP no reconocido	Verificar versión del protocolo
5002	DIAMETER_UNKNOWN_SESSION_ID	Sesión no encontrada	Sesión expirada o inválida
5003	DIAMETER_AUTHORIZATION_REJECTED	No autorizado	Verificar permisos del usuario
5012	DIAMETER_UNABLE_TO_COMPLY	No se puede procesar la solicitud	Verificar registros de HSS/PCRF/OCS

## Problemas Comunes

### Fallos de Conexión de Pares

**Síntoma:** Par atascado en estado "Closed" o "Wait-Conn-Ack"

**Diagnóstico:**

1. Verificar conectividad de red:

```
ping <peer-fqdn>
telnet <peer-fqdn> 3868
```

2. Verificar reglas de firewall (el puerto 3868 TCP debe estar abierto)
3. Verificar configuración del par (dirección IP, puerto)
4. Revisar registros del par para intentos de conexión

#### Resolución:

- Corregir problemas de red/firewall
  - Verificar que el par esté en ejecución y escuchando en el puerto 3868
  - Verificar si el par tiene la configuración correcta para CSCF
  - Usar **Habilitar Par** en la interfaz web para reintentar la conexión
- 

## Fallos en el Intercambio CER/CEA

**Síntoma:** Par atascado en estado "Wait-I-CEA", o CEA con código de error

#### Errores Comunes:

- **5010 (NO\_COMMON\_APPLICATION):** Verificar que ambos pares soporten la misma aplicación (por ejemplo, Cx = 16777216)
- **3003 (REALM\_NOT\_SERVED):** Verificar que el Origin-Realm coincida con el reino esperado del par

#### Resolución:

- Verificar la configuración de Diameter para Application-Id y reino
  - Asegurarse de que la configuración del par coincide con las expectativas de CSCF
  - Revisar los registros del backend de CSCF para mensajes de error detallados
- 

## Problemas en la Interfaz Cx de HSS

**Síntoma:** Fallos de registro, tiempos de espera MAR/MAA

#### Errores Comunes:

Código de Resultado	Significado	Resolución
4010	USER_UNKNOWN	Usuario no provisionado en HSS
4001	AUTHENTICATION_REJECTED	IMPI/credenciales incorrectas
5012	UNABLE_TO_COMPLY	Error interno de HSS, verificar registros de HSS

#### Resolución:

- **USER\_UNKNOWN:** Aprovisionar usuario en HSS
- **AUTHENTICATION\_REJECTED:** Verificar IMPI y secreto compartido en HSS

- **UNABLE\_TO\_COMPLY:** Verificar registros de HSS y conectividad a la base de datos
- 

## Problemas en la Interfaz Rx de PCRF

**Síntoma:** Llamadas exitosas pero sin QoS aplicado, tiempos de espera AAR/AAA

### Problemas Comunes:

- **PCRF caído:** Verificar estado del par en la interfaz web
- **Framed-IP-Address no reconocido:** PCRF no puede mapear IP de UE al suscriptor
- **Política no aplicada:** Verificar reglas de política de PCRF, verificar integración de PCEF

### Resolución:

- Verificar que el par PCRF esté en estado "I\_Open"
  - Verificar aprovisionamiento de dirección IP de UE en PCRF
  - Verificar que la interfaz Gx (PCRF a PCEF) esté funcional
- 

## Problemas en la Interfaz Ro de OCS

**Síntoma:** Fallos en llamadas prepago, tiempos de espera CCR/CCA, llamadas bloqueadas

### Errores Comunes:

Código de Resultado	Significado	Resolución
4012	CREDIT_LIMIT_REACHED	Crédito insuficiente
5003	AUTHORIZATION_REJECTED	Usuario no autorizado para prepago

### Resolución:

- **CREDIT\_LIMIT\_REACHED:** Normal para usuarios prepago sin crédito
  - **Timeout de OCS:** Verificar disponibilidad de OCS y estado del par
  - **AUTHORIZATION\_REJECTED:** Verificar que el usuario esté aprovisionado para prepago en OCS
- 

## Degradación del Rendimiento

**Síntoma:** Tiempos de respuesta de Diameter lentos, alta latencia

### Diagnóstico:

1. Verificar la marca de tiempo "Último Usado" en la lista de pares (debería ser reciente)
2. Monitorear "Longitud de Cola" (valores altos indican acumulación)
3. Revisar registros del backend de CSCF para advertencias de tiempo de espera

#### **Resolución:**

- **Alta latencia:** Investigar la red entre CSCF y el par
- **Alta longitud de cola:** Verificar carga del sistema del par (HSS/PCRF/OCS)
- **Tiempos de espera:** Aumentar el tiempo de espera de transacción si la red tiene alta latencia

## **Mejores Prácticas**

### **Directrices Operativas**

#### **Gestión de Pares:**

- Monitorear el estado de los pares a través del panel de control de la interfaz web
- Configurar monitoreo externo para eventos de caída de pares
- Probar la conectividad de los pares durante las ventanas de mantenimiento

#### **Planificación de Capacidad:**

- Estimar la tasa de transacciones de Diameter basada en registros y volumen de llamadas
- Asegurarse de que HSS/PCRF/OCS pueda manejar tasas de transacción pico
- Considerar agentes de enrutamiento Diameter (DRA) para implementaciones grandes

#### **Solución de Problemas:**

- Verificar el estado del par primero al investigar fallos de registro o llamadas
- Correlacionar fallos de Diameter con fallos de SIP (mismo Call-ID o usuario)
- Revisar registros del backend de CSCF para trazas de transacciones Diameter detalladas

#### **Seguridad:**

- Usar TLS para conexiones Diameter en producción (si es compatible)
- Restringir el acceso a pares Diameter a través de firewall (solo pares conocidos)
- Revisar regularmente los registros de auditoría de habilitación/deshabilitación de pares

# Limitaciones y Mejoras Futuras

## Implementación Actual

El panel de control proporciona:

- ⚡ Visualización del estado de pares en tiempo real
- ⚡ Operaciones de habilitación/deshabilitación de pares
- ⚡ Mapeo de ID de aplicación a nombres de interfaz
- ⚡ Actualización automática cada 5 segundos

## No Implementado Aún

Las siguientes características **no están actualmente disponibles** pero pueden ser añadidas en versiones futuras:

- **Inspector de Mensajes Diameter:** Ver transacciones recientes de Diameter y detalles de AVP
- **Panel de Métricas de Diameter:** Integración de Grafana para latencia, tasas de error, etc.
- **Estadísticas de Pares:** Conteos de mensajes, tasas de éxito, latencia promedio por par
- **Monitoreo de Watchdog:** Estado en tiempo real de DWR/DWA
- **Reconexión Manual:** Forzar reconexión de pares a través de la interfaz web

## Soluciones Alternativas

**Para Inspección de Mensajes:** Revisar registros del backend de CSCF o habilitar el registro de depuración de Diameter

**Para Estadísticas Detalladas:** Consultar métricas desde el endpoint de Prometheus (ver [Referencia de Métricas](#) para definiciones completas de métricas de CDP/Diameter y [Guía de Operaciones de la Interfaz Web](#) para configuración de monitoreo)

**Para Reconexión Manual:** Usar la interfaz web para deshabilitar y luego volver a habilitar el par

## Documentación Relacionada

- [Guía de Operaciones de P-CSCF](#) - Operaciones de interfaz Rx de P-CSCF
- [Guía de Operaciones de I-CSCF](#) - Operaciones de interfaz Cx de I-CSCF
- [Guía de Operaciones de S-CSCF](#) - Interfaces Cx, Ro de S-CSCF
- [Guía de Operaciones de la Interfaz Web](#) - Gestión de pares Diameter a través del panel de control
- [Guía de Operaciones de CSCF](#) - Operaciones generales de CSCF

## Especificaciones 3GPP

- **TS 29.228:** Interfaces Cx y Dx (CSCF-HSS)
- **TS 29.214:** Interfaz Rx (P-CSCF-PCRF)
- **TS 32.299:** Aplicaciones de carga Diameter (Ro, Rf)
- **RFC 6733:** Protocolo Base de Diameter

## Detalles Técnicos

### Implementación

- **Pila Diameter:** Pila de protocolo Diameter integrada
- **Interfaz de Gestión:** Protocolo RPC al backend de CSCF
- **Interfaz Web:** Phoenix LiveView (`lib/cscf_web/web/diameter_live.ex`)

### Configuración

Los pares Diameter se configuran en los archivos de configuración del backend de CSCF, no a través del panel de control. El panel de control proporciona monitoreo y control operativo (habilitar/deshabilitar) únicamente.



# Guía de Capacidad y Dimensionamiento de OmniCall CSCF

## Descripción general

Esta guía proporciona información sobre la planificación de capacidad y dimensionamiento para implementaciones de OmniCall CSCF. Los números de capacidad presentados aquí son **directrices basadas en el análisis del código fuente y la experiencia en producción**, no límites estrictos.

## Estrategia de Escalado Horizontal

**OmniCall CSCF logra una escala prácticamente ilimitada a través del escalado horizontal:** simplemente despliega instancias adicionales a medida que crece tu base de suscriptores. No hay un límite superior práctico para la capacidad total de la red.

### Principios Clave de Escalado:

- ✓ **Agrega instancias, no complejidad:** ¿Necesitas soportar 1 millón de suscriptores? Despliega 3-4 instancias de S-CSCF en lugar de un servidor masivo.
- ✓ **Componentes independientes:** Cada instancia de P-CSCF, I-CSCF y S-CSCF opera de manera independiente.
- ✓ **Distribución de carga:** I-CSCF distribuye automáticamente a los usuarios entre las instancias de S-CSCF; DNS o平衡adores de carga distribuyen el tráfico a P-CSCF e I-CSCF.
- ✓ **No se requiere afinidad de sesión:** Los usuarios pueden ser distribuidos entre diferentes instancias de CSCF.
- ✓ **Distribución geográfica:** Despliega instancias de CSCF en múltiples centros de datos para resiliencia y optimización de latencia.

### Ejemplo de Ruta de Escalado:

- **10K suscriptores:** 1 P-CSCF, 1 I-CSCF, 1 S-CSCF
- **50K suscriptores:** 2 P-CSCF, 2 I-CSCF, 2 S-CSCF
- **200K suscriptores:** 6 P-CSCF, 4 I-CSCF, 4 S-CSCF
- **1M suscriptores:** 30 P-CSCF, 10 I-CSCF, 10 S-CSCF

- **10M suscriptores:** 300 P-CSCF, 50 I-CSCF, 50 S-CSCF

**Escalado Rentable:** Hardware común + escalado horizontal = menor CapEx que soluciones costosas de "gran hierro".

## Sobre Estas Directrices

Los números de capacidad en este documento son **estimaciones conservadoras** diseñadas para:

- Proporcionar margen para picos de tráfico (tormentas de registro, eventos de llamadas masivas)
- Tener en cuenta el procesamiento IFC complejo y múltiples integraciones de Servidores de Aplicaciones
- Asegurar tiempos de respuesta de menos de un segundo incluso bajo carga
- Soportar configuraciones de alta disponibilidad con capacidad de conmutación por error

**Tu experiencia puede variar** según:

- Especificaciones de hardware (velocidad de CPU, RAM, ancho de banda de red)
- Complejidad de IFC y número de Servidores de Aplicaciones
- Temporizadores de expiración de registro (más cortos = más re-registros frecuentes)
- Tiempos de espera de llamadas y patrones de tráfico en horas pico

**Recomendación:** Usa estas directrices como punto de partida, luego monitorea métricas de producción para optimizar el número de instancias y la configuración para tu implementación específica.

---

## Tabla de Contenidos

1. [Resumen Ejecutivo](#)
  2. [Capacidad de P-CSCF](#)
  3. [Capacidad de I-CSCF](#)
  4. [Capacidad de S-CSCF](#)
  5. [Dimensionamiento de Implementación](#)
  6. [Optimización del Rendimiento](#)
  7. [Monitoreo y Alertas](#)
  8. [Resumen: Escala Ilimitada a Través del Escalado Horizontal](#)
-

# Resumen Ejecutivo

## Principales Restricciones de Capacidad

Tipo de CSCF	Restricción Principal	Máximo por Instancia	Implementación Típica
P-CSCF	Asociaciones de Seguridad IPsec	~50,000 UEs	10,000-30,000 UEs
I-CSCF	CPU/Red (sin estado)	Limitado por rendimiento	100,000+ req/sec
S-CSCF	Registros de Usuarios	~500,000 IMPUs	100,000-300,000 IMPUs
Diálogos	Estado de Llamada Activa	~100,000 diálogos	20,000-50,000 concurrentes

## Límites Técnicos (Por Instancia)

OmniCall CSCF tiene algunos límites técnicos por instancia. Estos **no son límites de implementación**: la capacidad total es ilimitada a través del escalado horizontal:

Límite	Valor	Lo Que Significa	Solución
Seguimiento 10,000 de Hash SPI entradas		Estructura de seguimiento interno para SPIs IPsec	Esto NO limita los registros a 10K. P-CSCF puede manejar 40K-50K registros con la configuración adecuada. Despliega más VMs de P-CSCF para mayor escala.
Contactos por IMPU	100	Máximo de contactos SIP por identidad pública	Rara vez se alcanza en la práctica (típico: 1-5 contactos por usuario). Agrega VMs de S-CSCF si es necesario.
Rutas de Servicio	10 por contacto	Máximo de encabezados de ruta de servicio	Uso típico: 1-3. No es una restricción.
Tamaño del Cuerpo NOTIFY	16 KB	Tamaño máximo del mensaje de notificación	Divide listas de suscriptores grandes entre instancias de S-CSCF.

### Aclaración sobre el Límite de Hash SPI:

- El límite de 10,000 hashes SPI es una **estructura de seguimiento interna**, no un límite de registro estricto.
- Las instancias de P-CSCF manejan regularmente **40,000-50,000 registros concurrentes** en producción.

- El hash SPI se utiliza para búsquedas rápidas; los SAs IPsec reales son gestionados por separado por el kernel.
- Si te acercas a los límites de capacidad, simplemente despliega VMs adicionales de P-CSCF.

**Punto Clave:** Estos son límites de ingeniería para una sola instancia de VM. Para escala ilimitada, despliega más VMs.

---

## Capacidad de P-CSCF

El **Proxy-CSCF** es típicamente el componente más restringido en capacidad debido a la sobrecarga de las asociaciones de seguridad IPsec.

### Factores de Capacidad

#### 1. Asociaciones de Seguridad IPsec

##### Huella de Memoria por UE:

Cada SA IPsec consume aproximadamente:

- Seguimiento de SPI: ~200 bytes (entrada de tabla hash)
- Vinculación de socket: ~1-2 KB (recursos del kernel)
- Estado de contacto: ~500-1000 bytes (datos de registro)
- Total por UE: ~2-3 KB en memoria compartida

##### Directrices de Capacidad por Instancia:

- **Agresivo:** 40,000-50,000 UEs (se acerca al límite de hash SPI)
- **Recomendado:** 20,000-30,000 UEs (rendimiento equilibrado y margen)
- **Conservador:** 10,000-15,000 UEs (máximo margen de HA para conmutación por error)

##### Escalado Más Allá de una Sola Instancia:

- **100K suscriptores:** Despliega 3-5 instancias de P-CSCF detrás de balanceo de carga DNS.
- **500K suscriptores:** Despliega 15-25 instancias de P-CSCF en múltiples sitios.
- **1M+ suscriptores:** Despliega 30-50+ instancias de P-CSCF con distribución geográfica.

**Nota:** Estas son directrices, no límites. Las implementaciones en producción han ejecutado con éxito instancias de P-CSCF a 40K+ UEs con el ajuste adecuado.

## 2. Servicios de Emergencia

El manejo de llamadas de emergencia utiliza almacenamiento en memoria para mapeos de IMEI a devoluciones de llamada (TTL de 24 horas) para soportar devoluciones de llamada de emergencia.

### Requisitos de VM de P-CSCF

**Especificación Estándar de VM:** 8 vCPU, 8 GB de RAM como mínimo

Tamaño de Implementación	UEs por VM	VMs Necesarias para Implementaciones de Ejemplo
<b>Conservador</b>	10,000-15,000	10K subs = 1 VM, 50K subs = 4 VMs, 100K subs = 7 VMs
<b>Recomendado</b>	20,000-30,000	10K subs = 1 VM, 50K subs = 2 VMs, 100K subs = 4 VMs
<b>Agresivo</b>	40,000-50,000	10K subs = 1 VM, 50K subs = 1 VM, 100K subs = 2 VMs

### VoWiFi con OmniePDG:

- OmniePDG termina IPsec, P-CSCF maneja solo SIP.
- La capacidad aumenta a **80,000-100,000 UEs por VM de P-CSCF**.
- 100K usuarios de VoWiFi = 1-2 VMs de P-CSCF (vs. 4 VMs para VoLTE).

---

## Capacidad de I-CSCF

El **Interrogating-CSCF** es sin estado y está limitado principalmente por el rendimiento de CPU y red en lugar de memoria.

### Factores de Capacidad

#### 1. Diseño Sin Estado

- **Sin estado de sesión:** I-CSCF no mantiene registros de usuarios ni diálogos.
- **Consultas HSS:** Cada registro requiere 1 intercambio Cx UAR/UAA.
- **Basado en rendimiento:** Limitado por la tasa de procesamiento de REGISTER/INVITE.

### Rendimiento Típico:

- **Tasa de Registro:** 1,000-5,000 registros/segundo (dependiendo de la latencia de HSS).
- **Tasa de Configuración de Llamadas:** 5,000-10,000 INVITE/segundo.

- **Suscriptores Simultáneos:** Efectivamente ilimitados (no se mantiene estado).

## 2. Selección de S-CSCF

I-CSCF mantiene un grupo de instancias de S-CSCF disponibles (típicamente 2-10) para balanceo de carga basado en capacidades y carga actual.

### Requisitos de VM de I-CSCF

**Especificación Estándar de VM:** 4 vCPU, 8 GB de RAM como mínimo

Tamaño de Implementación	Rendimiento por VM	VMs Necesarias para Implementaciones de Ejemplo
<b>Conservador</b>	1,000 reg/sec	10K subs = 1 VM, 100K subs = 2 VMs, 500K subs = 4 VMs
<b>Recomendado</b>	2,000 reg/sec	10K subs = 1 VM, 100K subs = 1 VM, 500K subs = 2 VMs
<b>Agresivo</b>	5,000 reg/sec	10K subs = 1 VM, 100K subs = 1 VM, 500K subs = 1 VM

**Estrategia de Escalado:** Despliega múltiples instancias de I-CSCF detrás de round-robin DNS o balanceador de carga de hardware. Cada instancia es independiente y sin estado.

---

## Capacidad de S-CSCF

El **Serving-CSCF** mantiene el estado de registro y diálogos activos, lo que lo convierte en el componente central de escalabilidad.

### Factores de Capacidad

#### 1. Registros de Usuarios

##### Huella de Memoria por IMPU:

Cada IMPU registrado consume aproximadamente:

- Entrada de hash: ~1-2 KB (IMPU, contactos, expira)
- IFC (Criterios de Filtro Inicial): ~5-20 KB (perfil de servicio de HSS)
- Vectores de autenticación: ~1-2 KB
- Total por IMPU: ~7-25 KB dependiendo de la complejidad del servicio

##### Directrices de Capacidad por Instancia:

- **Agresivo:** 400,000-500,000 IMPUs (con hash\_size=14+, hardware de alta especificación)
- **Recomendado:** 200,000-300,000 IMPUs (carga equilibrada, complejidad típica de IFC)
- **Conservador:** 100,000-150,000 IMPUs (IFC compleja, múltiples AS, margen de HA)

## **Escalado para Implementaciones Grandes:**

- **1M suscriptores:** Despliega 3-5 instancias de S-CSCF, I-CSCF distribuye a través de HSS.
- **5M suscriptores:** Despliega 15-25 instancias de S-CSCF en múltiples centros de datos.
- **10M+ suscriptores:** Despliega 30-50+ instancias de S-CSCF.

**Nota:** Estas son directrices iniciales. La capacidad real depende de la complejidad de IFC, integración de AS y especificaciones de hardware. Algunas implementaciones en producción ejecutan 400K+ IMPUs por instancia con configuraciones optimizadas.

## **2. Diálogos Activos (Sesiones de Llamadas)**

### **Huella de Memoria por Diálogo:**

Cada diálogo activo consume aproximadamente:

- Estado del diálogo: ~2-4 KB (Call-ID, etiquetas From/To, conjunto de rutas)
- Información SDP: ~1-2 KB (parámetros de medios)
- Perfiles/variables: ~1-2 KB
- Total por diálogo: ~4-8 KB

### **Directrices de Capacidad por Instancia:**

- **Agresivo:** 80,000-100,000 diálogos concurrentes (con dlg\_hash\_size=15+)
- **Recomendado:** 40,000-60,000 diálogos concurrentes (implementación típica)
- **Conservador:** 20,000-30,000 diálogos concurrentes (máximo margen de HA)

### **Escalado para Alto Volumen de Llamadas:**

- **100K llamadas concurrentes:** Despliega 2-3 instancias de S-CSCF.
- **500K llamadas concurrentes:** Despliega 10-15 instancias de S-CSCF.
- **1M+ llamadas concurrentes:** Despliega 20-30+ instancias de S-CSCF.

**Nota:** La capacidad de diálogo suele ser mayor que la capacidad de registro, ya que los diálogos son de corta duración (segundos a minutos) mientras que los registros son de larga duración (minutos a horas). Monitorea las tasas de

llamadas concurrentes en horas pico reales para optimizar.

### 3. Procesamiento de Criterios de Filtro Inicial (IFC)

#### Impacto de la Complejidad de IFC:

- IFC simple (1-5 puntos de activación): Sobrecarga mínima.
- IFC compleja (10+ puntos de activación, múltiples AS): 5-10 ms de procesamiento adicional por llamada.
- Memoria: 5-20 KB por usuario dependiendo de la complejidad del perfil de servicio.

### Requisitos de VM de S-CSCF

Especificación Estándar de VM: 8 vCPU, 8 GB de RAM como mínimo

Tamaño de Implementación	IMPUs por VM	Concurrentes por VM	Diálogos	VMs Necesarias para Implementaciones de Ejemplo
<b>Conservador</b>	100,000-150,000	20,000-30,000		10K subs = 1 VM, 100K subs = 1 VM, 500K subs = 4 VMs
<b>Recomendado</b>	200,000-300,000	40,000-60,000		10K subs = 1 VM, 100K subs = 1 VM, 500K subs = 2 VMs
<b>Agresivo</b>	400,000-500,000	80,000-100,000		10K subs = 1 VM, 100K subs = 1 VM, 500K subs = 1 VM

### Dimensionamiento de Implementación

#### Implementación Pequeña (< 10,000 Suscriptores)

**Escenario:** MVNO, pequeña empresa, entorno de laboratorio/prueba

Componente	Cantidad de VMs	Especificación de VMs	Capacidad por VM
P-CSCF	1	8 vCPU, 8 GB RAM	10,000-15,000 UEs
I-CSCF	1	4 vCPU, 8 GB RAM	1,000-2,000 reg/sec
S-CSCF	1	8 vCPU, 8 GB RAM	100,000-200,000 IMPUs
<b>Total VMs</b>	<b>3</b>		
<b>Capacidad Total</b>			<b>Hasta 15,000 suscriptores</b>

#### Implementación Mediana (10,000-100,000 Suscriptores)

**Escenario:** Operador regional, operador de nivel 2, gran empresa

### **Dimensionamiento Conservador (100K suscriptores):**

<b>Componente</b>	<b>Cantidad de VMs</b>	<b>Especificación de VMs</b>	<b>Capacidad por VM</b>
P-CSCF	4	8 vCPU, 8 GB RAM	25,000 UEs cada uno
I-CSCF	2	4 vCPU, 8 GB RAM	2,000 reg/sec cada uno
S-CSCF	2	8 vCPU, 8 GB RAM	150,000 IMPUs cada uno
<b>Total VMs</b>	<b>8</b>		
<b>Capacidad Total</b>			<b>100,000 suscriptores</b>

### **Dimensionamiento Recomendado (100K suscriptores):**

<b>Componente</b>	<b>Cantidad de VMs</b>	<b>Especificación de VMs</b>	<b>Capacidad por VM</b>
P-CSCF	2	8 vCPU, 8 GB RAM	50,000 UEs cada uno
I-CSCF	1	4 vCPU, 8 GB RAM	5,000 reg/sec
S-CSCF	1	8 vCPU, 8 GB RAM	300,000 IMPUs
<b>Total VMs</b>	<b>4</b>		
<b>Capacidad Total</b>			<b>100,000 suscriptores</b>

### **Alta Disponibilidad:**

- Despliega I-CSCF detrás de round-robin DNS o balanceador de carga.
- I-CSCF distribuye usuarios a través del grupo de S-CSCF.
- Se recomienda distribución geográfica para resiliencia.

## **Implementación Grande (500,000 Suscriptores)**

**Escenario:** Operador de nivel 1, operador nacional

### **Dimensionamiento Conservador:**

<b>Componente</b>	<b>Cantidad de VMs</b>	<b>Especificación de VMs</b>	<b>Capacidad por VM</b>
P-CSCF	25	8 vCPU, 8 GB RAM	20,000 UEs cada uno
I-CSCF	4	4 vCPU, 8 GB RAM	2,000 reg/sec cada uno
S-CSCF	4	8 vCPU, 8 GB RAM	150,000 IMPUs cada uno
<b>Total VMs</b>	<b>33</b>		
<b>Capacidad Total</b>			<b>500,000 suscriptores</b>

## **Dimensionamiento Recomendado:**

<b>Componente</b>	<b>Cantidad de VMs</b>	<b>Especificación de VMs</b>	<b>Capacidad por VM</b>
<b>P-CSCF</b>	15	8 vCPU, 8 GB RAM	33,000 UEs cada uno
<b>I-CSCF</b>	2	4 vCPU, 8 GB RAM	5,000 reg/sec cada uno
<b>S-CSCF</b>	2	8 vCPU, 8 GB RAM	250,000 IMPUs cada uno
<b>Total VMs</b>	<b>19</b>		
<b>Capacidad Total</b>			<b>500,000 suscriptores</b>

## **Dimensionamiento Agresivo:**

<b>Componente</b>	<b>Cantidad de VMs</b>	<b>Especificación de VMs</b>	<b>Capacidad por VM</b>
<b>P-CSCF</b>	10	8 vCPU, 8 GB RAM	50,000 UEs cada uno
<b>I-CSCF</b>	1	4 vCPU, 8 GB RAM	5,000 reg/sec
<b>S-CSCF</b>	1	8 vCPU, 8 GB RAM	500,000 IMPUs
<b>Total VMs</b>	<b>12</b>		
<b>Capacidad Total</b>			<b>500,000 suscriptores</b>

## **Alta Disponibilidad:**

- P-CSCF activo-activo entre centros de datos.
- I-CSCF geo-redundante con DNS o BGP anycast.
- Múltiples instancias de S-CSCF con distribución de carga de I-CSCF.

---

## **Consideraciones de Implementación de VoWiFi**

### **Con OmniePDG:**

- La capacidad de P-CSCF aumenta significativamente (sin sobrecarga de IPsec en P-CSCF).
- ePDG maneja la terminación del túnel IPsec.
- P-CSCF puede soportar más de 100,000 usuarios de VoWiFi (limitado por CPU/red, no por IPsec).

### **Arquitectura:**

```
VoWiFi UE → (IPsec) → OmniePDG → (SIP) → P-CSCF → I-CSCF → S-CSCF  
VoLTE UE → (IPsec) → P-CSCF → I-CSCF → S-CSCF
```

**Recomendación:** Para grandes implementaciones de VoWiFi (>50K usuarios), despliega instancias dedicadas de P-CSCF detrás de OmniePDG sin el módulo

IPsec cargado para un máximo rendimiento.

---

## Optimización del Rendimiento

OmniCall CSCF se entrega pre-optimizado para uso en producción. La afinación del rendimiento es manejada por la ingeniería de OmniCall durante la implementación.

### Configuración Estándar de VM

Todas las VMs de OmniCall CSCF están configuradas con:

- **SO:** Ajuste del kernel de Linux para un alto rendimiento de red.
- **Memoria:** Asignación optimizada de memoria compartida para tablas hash y estado de sesión.
- **Red:** Ajuste de la pila TCP/IP para tráfico SIP y Diameter.

### Ajustes Específicos de Implementación

Para ajustes personalizados según los requisitos específicos de tu implementación, contacta al soporte de OmniCall. Los escenarios de ajuste comunes incluyen:

- **Alto volumen de llamadas:** Ajustando procesos de trabajo y capacidad de diálogo.
  - **Gran base de suscriptores:** Optimizando tablas hash de registro.
  - **IFC compleja:** Ajustando procesos de notificación para la integración del Servidor de Aplicaciones.
  - **Distribución geográfica:** Optimizando conmutación por error y redundancia.
- 

## Monitoreo y Alertas

### Indicadores Clave de Rendimiento (KPIs)

#### Métricas de P-CSCF

Métrica	Descripción	Umbral de Advertencia	Umbral Crítico
<b>Conteo de SA IPsec</b>	Asociaciones de seguridad activas	> 25,000	> 40,000
<b>Utilización de Hash SPI</b>	Porcentaje del rango de SPI utilizado	> 70%	> 90%
<b>Tasa de Registro</b>	Solicitudes REGISTER/	> 100/sec	> 500/sec

Métrica	Descripción	Umbral de Advertencia	Umbral Crítico
<b>Carga de Hash de Contacto</b>	Promedio de contactos por ranura hash	> 20	> 50
<b>Uso de Memoria</b>	Consumo de memoria compartida	> 70%	> 90%

### Consultas de Prometheus:

```
# Conteo de SA IPsec (desde monitoreo de tabla hash)
ipsec_sa_count{cscf="pcscf01"}  
  

# Tasa de registro
rate(sip_register_requests_total{cscf="pcscf01"}[5m])
```

### Métricas de S-CSCF

Métrica	Descripción	Umbral de Advertencia	Umbral Crítico
<b>IMPUs Registrados</b>	Total de usuarios registrados	> 300,000	> 450,000
<b>Diálogos Activos</b>	Sesiones de llamadas concurrentes	> 40,000	> 70,000
<b>Carga de Hash de IMPU</b>	Promedio de IMPUs por ranura hash	> 50	> 100
<b>Carga de Hash de Diálogo</b>	Promedio de diálogos por ranura hash	> 10	> 20
<b>Tiempo de Procesamiento de IFC</b>	Tiempo promedio de evaluación de IFC	> 10 ms	> 50 ms

### Consultas de Prometheus:

```
# Usuarios registrados
impu_registered_count{cscf="scscf01"}  
  

# Diálogos activos
dialog_active_count{cscf="scscf01"}  

```

### Métricas de I-CSCF

Métrica	Descripción	Umbral de Advertencia	Umbral Crítico
<b>TPS de Registro</b>	Transacciones REGISTER/segundo	> 1,000/sec	> 2,000/sec
<b>Latencia de</b>	Tiempo de respuesta de	> 50 ms	> 200 ms

Métrica	Descripción	Umbral de Advertencia	Umbral Crítico
<b>Consulta HSS</b>	Diameter Cx		
<b>Tasa de Fallos de HSS</b>	Porcentaje de consultas HSS fallidas	> 1%	> 5%

## Comprobaciones de Salud

**Monitoreo de Salud del Sistema:** OmniCall CSCF exporta métricas de salud completas a través del panel de control y los puntos finales de Prometheus (<http://<host>:9090/metrics>). Monitorea:

- Conteos de SA IPsec (P-CSCF)
- Conteos de registro (P-CSCF, S-CSCF)
- Conteos de diálogos activos (S-CSCF)
- Utilización de memoria
- Utilización de CPU

Para una lista completa de todas las métricas disponibles, consulta la [Referencia de Métricas](#).

## Reglas de Alerta (Prometheus/Alertmanager)

```
groups:
  - name: cscf_capacity
    rules:
      - alert: PCSCFIPsecSAHigh
        expr: ipsec_sa_count > 40000
        for: 5m
        annotations:
          summary: "P-CSCF {{ $labels.instance }} tiene un alto conteo de SA IPsec"

      - alert: SCSCFRegistrationHigh
        expr: impu_registered_count > 450000
        for: 10m
        annotations:
          summary: "S-CSCF {{ $labels.instance }} se acerca a la capacidad de registro"

      - alert: SCSCFDialoHigh
        expr: dialog_active_count > 70000
        for: 5m
        annotations:
          summary: "S-CSCF {{ $labels.instance }} tiene un alto conteo de diálogos activos"
```

# Apéndice: Metodología de Planificación de Capacidad

Esta guía de dimensionamiento se basa en:

1. **Implementaciones en Producción:** Análisis de implementaciones del mundo real de OmniCall CSCF que van desde 5K hasta 500K+ suscriptores.
2. **Pruebas de Rendimiento:** Pruebas de carga y benchmarking en varias configuraciones de hardware.
3. **Estándares 3GPP:** Cumplimiento con las especificaciones de 3GPP para capacidad y rendimiento de IMS.
4. **Análisis de Ingeniería:** Revisión técnica detallada de la arquitectura de CSCF y la utilización de recursos.

**Validación:** Todos los números de capacidad han sido validados en redes de operadores en producción.

---

## Resumen: Escala Ilimitada a Través del Escalado Horizontal

### Puntos Clave

1. **Sin Límites Estrictos en la Capacidad Total:** Los límites por instancia documentados en esta guía son **directrices conservadoras**, no techos absolutos. La capacidad total de la red es ilimitada a través del escalado horizontal.
2. **Modelo de Escalado Simple:**

¿Necesitas más capacidad? → Despliega más instancias  
¿Alcanzaste un límite por instancia? → Agrega otra instancia  
¿El tráfico está creciendo? → Activa más VMs
3. **Probado a Gran Escala:** Las implementaciones de OmniCall CSCF varían desde:
  - Pequeños MVNOs: 5K-10K suscriptores en 3-5 VMs.
  - Operadores regionales: 50K-200K suscriptores en 10-30 VMs.
  - Operadores de nivel 1: 1M+ suscriptores en 100+ VMs.
4. **Crecimiento Rentable:** Escala de manera incremental con hardware común en lugar de costosas actualizaciones masivas. Agrega capacidad a medida que crece el ingreso.

**5. Directrices, No Reglas:** Los números de capacidad en este documento son:

- Estimaciones conservadoras con margen incorporado.
- Basadas en análisis de código fuente y experiencia en producción.
- Puntos de partida útiles para la planificación.
- NO límites estrictos que no pueden ser superados.
- NO prescripciones de talla única.

## Ejemplo de Escalado en el Mundo Real

**Escenario:** Creciendo de 10K a 1M suscriptores en 3 años

Año	Suscriptores	P-CSCF	I-CSCF	S-CSCF	Acción
<b>Año 0</b>	10,000	1	1	1	Implementación inicial (3 VMs)
<b>Año 1</b>	50,000	2	2	2	Crecimiento 2x: Agregar 3 VMs
<b>Año 1.5</b>	100,000	4	3	3	Crecimiento 2x: Agregar 4 VMs
<b>Año 2</b>	250,000	8	4	5	Crecimiento 2.5x: Agregar 6 VMs
<b>Año 3</b>	500,000	15	6	8	Crecimiento 2x: Agregar 13 VMs
<b>Futuro</b>	1,000,000	30	10	10	Crecimiento 2x: Agregar 24 VMs

**Inversión Total:** Adiciones de VM incrementales a medida que crece el ingreso, no un gran CapEx inicial.

## Cuándo Agregar Instancias

Monitorea estas señales para saber cuándo escalar horizontalmente:

### P-CSCF:

- Conteo de SA IPsec consistentemente >30K (>70% de la capacidad recomendada).
- Utilización de CPU >70% durante la hora pico.
- Tiempos de respuesta de registro >500ms.

### S-CSCF:

- Conteo de IMPU consistentemente >250K (>70% de la capacidad recomendada).
- Conteo de diálogos acercándose a 50K concurrentes.
- Utilización de CPU >70% durante la hora pico.

### I-CSCF:

- Tasa de solicitudes consistentemente >2,000/sec por instancia.
- Utilización de CPU >80% durante la hora pico.
- Aumento de la latencia de consulta HSS.

**Acción:** Agrega 1-2 instancias proactivamente antes de alcanzar límites. El escalado horizontal es un seguro económico contra problemas de capacidad.

## Filosofía de Configuración

### Comienza Conservador, Ajusta a Medida que Creces:

1. Comienza con configuraciones recomendadas de esta guía.
2. Monitorea métricas de producción (ver [Monitoreo](#)).
3. Ajusta tamaños de hash y procesos de trabajo según la carga real.
4. Agrega instancias antes de alcanzar el 80% de los límites de capacidad observados.
5. Prueba configuraciones en staging antes de la implementación en producción.

**Recuerda:** Estas directrices proporcionan un punto de partida probado, pero cada implementación es única. Tu capacidad real puede ser mayor o menor dependiendo de tu entorno específico, patrones de tráfico y requisitos.



# Guía de Operaciones del I-CSCF

## Tabla de Contenidos

1. [Descripción General](#)
2. [Rol en la Arquitectura IMS](#)
3. [Funciones del I-CSCF](#)
4. [Operaciones de la Interfaz Web](#)
5. [Flujos de Llamadas](#)
6. [Solución de Problemas](#)

## Descripción General

El **I-CSCF** (Interrogating Call Session Control Function) sirve como el punto de entrada a la red de un operador IMS desde redes externas y desde el P-CSCF. Su responsabilidad principal es consultar el HSS (Home Subscriber Server) para descubrir el S-CSCF apropiado para un usuario y ocultar la topología de la red interna de entidades externas.

## Especificaciones 3GPP

- **3GPP TS 23.228:** Subsistema Multimedia IP (IMS) Etapa 2
- **3GPP TS 24.229:** Protocolo de Control de Llamadas IMS
- **3GPP TS 29.228:** Interfaz Cx (I-CSCF a HSS)
- **3GPP TS 29.229:** Protocolo Cx

## Responsabilidades Clave

1. **Interrogación HSS:** Consulta al HSS para la ubicación del usuario y la asignación del S-CSCF
2. **Selección del S-CSCF:** Elige el S-CSCF apropiado basado en capacidades
3. **Ocultación de Topología:** Protege las direcciones internas del S-CSCF de la vista externa
4. **Balanceo de Carga:** Distribuye la carga entre múltiples instancias del S-CSCF
5. **Proxy de Enrutamiento:** Enruta solicitudes al S-CSCF seleccionado
6. **Punto de Entrada de Red:** Primer salto para mensajes SIP externos

## Características Clave

- **Operación Sin Estado:** Retención mínima de estado
- **Cliente Diameter:** Interfaz Cx al HSS
- **Sin Manejo de Medios:** Proxy de señalización pura

- **Sin Autenticación:** Delegado al S-CSCF
- **Alto Rendimiento:** Optimizado para consulta y reenvío

## Rol en la Arquitectura IMS

### Posición en la Red

### Puntos de Referencia 3GPP

Interfaz	Protocolo	Propósito	Conectado a
Mw	SIP	P-CSCF/Externo a I-CSCF	P-CSCF, IMS Externo
Mw	SIP	I-CSCF a S-CSCF	S-CSCF
Cx	Diameter	Consultas de datos de usuario	HSS

## Funciones del I-CSCF

### 1. Interrogación HSS (Interfaz Cx)

El I-CSCF utiliza la interfaz Cx de Diameter para consultar el HSS para dos operaciones principales:

#### Solicitud de Autorización de Usuario (UAR)

Utilizada durante **REGISTER** para determinar qué S-CSCF debe atender al usuario.

#### Propósito:

- Verificar si el usuario puede registrarse
- Obtener el nombre del S-CSCF si ya está asignado
- Obtener las capacidades del S-CSCF si no está asignado

#### Comando Diameter:

```

UAR (User-Authorization-Request)
Session-Id
Vendor-Specific-Application-Id
  Vendor-Id: 10415 (3GPP)
  Auth-Application-Id: 16777216 (Cx)
Auth-Session-State: NO_STATE_MAINTAINED
Origin-Host: icscf.ims.mnc001.mcc001.3gppnetwork.org
Origin-Realm: ims.mnc001.mcc001.3gppnetwork.org
Destination-Realm: ims.mnc001.mcc001.3gppnetwork.org
User-Name: sip:user@ims.mnc001.mcc001.3gppnetwork.org
Public-Identity: sip:user@ims.mnc001.mcc001.3gppnetwork.org
Visited-Network-Identifier: ims.mnc001.mcc001.3gppnetwork.org

```

UAR-Flags: 0

### Respuesta HSS (UAA):

```
UAA (User-Authorization-Answer)
Result-Code: 2001 (DIAMETER_SUCCESS)
Experimental-Result-Code: 2001 (FIRST_REGISTRATION)
Server-Name: sip:scscf.ims.mnc001.mcc001.3gppnetwork.org
Server-Capabilities:
  Mandatory-Capability: 1
  Optional-Capability: 2
  Server-Name: sip:scscf-backup.ims.mnc001.mcc001.3gppnetwork.org
```

### Códigos de Resultado:

- 2001: Éxito (usuario autorizado)
- 5003: Usuario Desconocido
- 5004: Las Identidades No Coincidan
- 5042: No Hay S-CSCF Disponible

### Solicitud de Información de Ubicación (LIR)

Utilizada para **INVITE** y otras solicitudes para encontrar qué S-CSCF está atendiendo actualmente al usuario.

### Propósito:

- Encontrar el S-CSCF que atiende a un usuario registrado
- Enrutar correctamente las llamadas terminantes

### Comando Diameter:

```
LIR (Location-Info-Request)
Session-Id
Vendor-Specific-Application-Id
  Vendor-Id: 10415 (3GPP)
  Auth-Application-Id: 16777216 (Cx)
Auth-Session-State: NO_STATE_MAINTAINED
Origin-Host: icscf.ims.mnc001.mcc001.3gppnetwork.org
Origin-Realm: ims.mnc001.mcc001.3gppnetwork.org
Destination-Realm: ims.mnc001.mcc001.3gppnetwork.org
Public-Identity: sip:user@ims.mnc001.mcc001.3gppnetwork.org
Originating-Request: 0 # 0=terminating, 1=originating
```

### Respuesta HSS (LIA):

```
LIA (Location-Info-Answer)
Result-Code: 2001 (DIAMETER_SUCCESS)
```

## Códigos de Resultado:

- 2001: Éxito (usuario registrado, S-CSCF devuelto)
- 5401: Usuario No Registrado
- 5003: Usuario Desconocido

## 2. Selección del S-CSCF

Cuando el HSS no devuelve un S-CSCF específico (por ejemplo, primer registro), el I-CSCF debe seleccionar uno basado en **coincidencia de capacidades**.

### Algoritmo de Coincidencia de Capacidades

1. **Recuperar capacidades** del HSS UAA
2. **Consultar base de datos local** para S-CSCFs disponibles
3. **Coincidir capacidades obligatorias** (todas deben coincidir)
4. **Coincidir capacidades opcionales** (mejor esfuerzo)
5. **Aplicar balanceo de carga** si hay múltiples coincidencias
6. **Seleccionar S-CSCF** con mejor ajuste

### Estructura de la Base de Datos del S-CSCF

El I-CSCF mantiene una base de datos con dos tablas relacionadas:

**Tabla S-CSCF:** Almacena información sobre los servidores S-CSCF disponibles:

- **ID:** Identificador único para cada S-CSCF
- **Nombre:** Nombre descriptivo (por ejemplo, "S-CSCF Primario")
- **URI del S-CSCF:** URI SIP del S-CSCF (por ejemplo, sip:scscf.ims.mnc001.mcc001.3gppnetwork.org:5060;transport=tcp)

**Tabla de Capacidades del S-CSCF:** Mapea los S-CSCF a sus capacidades soportadas:

- **ID:** Identificador único para el mapeo de capacidades
- **ID del S-CSCF:** Hace referencia al S-CSCF en la primera tabla
- **Capacidad:** ID de capacidad entera que este S-CSCF soporta

**Ejemplo de Configuración:** Una implementación típica podría tener:

- S-CSCF #1: "S-CSCF Primario" con URI  
sip:scscf.ims.mnc001.mcc001.3gppnetwork.org:5060
  - Soporta capacidad 0 (capacidad obligatoria)
  - Soporta capacidad 1 (capacidad opcional)

Puedes ver la lista actual de S-CSCF a través de: Interfaz Web → I-CSCF →

## pestaña Lista de S-CSCF

La lista de S-CSCF muestra los servidores S-CSCF disponibles y sus capacidades para balanceo de carga y asignación.

### Lógica de Selección

**Proceso de Selección del S-CSCF:** El I-CSCF realiza la selección del S-CSCF basada en capacidades utilizando la siguiente lógica:

1. **Extraer Capacidades:** Recupera los requisitos de capacidades obligatorias y opcionales de la respuesta UAA del HSS (User Authorization Answer) y los almacena en variables AVP
2. **Consulta a la Base de Datos:** Consulta la base de datos con los requisitos de capacidades para encontrar servidores S-CSCF que coincidan con las capacidades requeridas
3. **Manejo de Resultados:**
  - Si se encuentra un S-CSCF coincidente, la URI se almacena en \$avp(scscf\_uri) y se establece como la URI de destino (\$du) para el reenvío de la solicitud
  - Si no hay un S-CSCF coincidente disponible, responde a la solicitud original con 503 Servicio No Disponible

### 3. Ocultación de Topología

El I-CSCF oculta las direcciones internas del S-CSCF de las redes externas mediante:

1. **Eliminación de Record-Route:** No agrega el encabezado Record-Route
2. **Proxy de respuestas:** Elimina los encabezados Via que revelan el S-CSCF
3. **Reescritura de contacto:** (opcional) Reemplaza el contacto del S-CSCF con el I-CSCF
4. **Eliminación de ruta:** Elimina la información de ruta interna

#### Ejemplo:

El externo ve:

```
Via: SIP/2.0/UDP icscf.example.com:5060
```

La realidad interna:

```
Via: SIP/2.0/UDP scscf.example.com:5060
Via: SIP/2.0/UDP icscf.example.com:5060
```

## **4. Lógica de Enrutamiento**

### **Procesamiento de REGISTER**

#### **Procesamiento de INVITE (Terminante)**

## **5. NDS (Seguridad del Dominio de Red)**

El I-CSCF mantiene una lista de **dominios de confianza** para la seguridad entre operadores.

**Base de Datos de Dominios de Confianza:** Contiene una lista de nombres de dominio que son de confianza para la comunicación entre operadores:

- **ID:** Identificador único para cada dominio de confianza
- **Dominio de Confianza:** Nombre de dominio (por ejemplo, "ims.mnc001.mcc001.3gppnetwork.org")

**Ejemplo de Configuración:** Una implementación típica incluye el dominio IMS local y cualquier dominio de socio de peering:

- ims.mnc001.mcc001.3gppnetwork.org (red local)
- ims.mnc002.mcc001.3gppnetwork.org (socio de roaming)

#### **Propósito:**

- Validar solicitudes entrantes de redes de peering
- Aplicar políticas de seguridad basadas en relaciones de confianza
- Implementar limitación de tasa por dominio
- Controlar qué redes externas pueden acceder al núcleo IMS

Puedes ver los dominios de confianza a través de: Interfaz Web → I-CSCF → pestaña Dominios de Confianza

## **6. Failover y Balanceo de Carga**

### **Failover del S-CSCF**

**Condiciones de Activación** - El failover al siguiente S-CSCF se activa por:

- 408 Request Timeout
- Respuestas de error del servidor 5xx
- Respuestas de fallo global 6xx (excepto 600 Busy Everywhere, que indica rechazo del usuario en lugar de fallo del servidor)

**Lógica de Failover:** El I-CSCF implementa un failover automático utilizando una ruta de fallo:

1. **Verificación de Estado:** Cuando se recibe una respuesta, verifica si el código de estado coincide con los criterios de failover (408, 5xx, o 6xx)
2. **Selección del S-CSCF Siguiente:** Si se activa el failover, selecciona el siguiente S-CSCF disponible de la lista
3. **Reintentar o Fallar:**
  - Si hay otro S-CSCF disponible, reenvía la solicitud a él
  - Si todos los S-CSCF han sido probados y fallaron, responde con 503 Servicio No Disponible al originador

### **Gestión de Lista de S-CSCF con Estado:**

- La lista de S-CSCFs candidatos se mantiene en la memoria de la transacción
- La posición en la lista se mantiene a través de múltiples intentos
- La lista se borra cuando se recibe una respuesta final exitosa (éxito 2xx o error del cliente 4xx)
- La lista se preserva al recibir 401 Unauthorized (desafío de autenticación), ya que el mismo S-CSCF debe manejar la solicitud autenticada subsiguiente

### **Balanceo de Carga**

#### **Configuración de Balanceo de Carga:**

Cuando múltiples S-CSCFs soportan las mismas capacidades:

- S-CSCF 1: sip:scscf1.example.com:5060 - capacidad 0
- S-CSCF 2: sip:scscf2.example.com:5060 - capacidad 0
- S-CSCF 3: sip:scscf3.example.com:5060 - capacidad 0

El I-CSCF utiliza selección **round-robin** o **aleatoria** para distribuir la carga de manera uniforme entre todos los S-CSCF coincidentes.

Ver distribución de carga a través de: Interfaz Web → I-CSCF → Lista de S-CSCF (muestra todos los servidores configurados)

## **Operaciones de la Interfaz Web**

### **Accediendo a la Página del I-CSCF**

Navega a: <https://<control-panel>/icscf>

## Diseño de la Página

La página del I-CSCF tiene cuatro pestañas principales:

1. **Servidores S-CSCF** - S-CSCFs configurados y capacidades
2. **Dominios de Confianza NDS** - Seguridad del dominio de red
3. **Sesiones** - Sesiones activas del I-CSCF con selección de S-CSCF
4. **Tablas Hash** - Tablas de memoria compartida

## Visualizando Servidores S-CSCF

**Propósito:** Ver qué S-CSCFs están disponibles para la asignación de usuarios

### Columnas de Visualización:

- **ID:** ID de la base de datos
- **Nombre:** Nombre descriptivo
- **URI del S-CSCF:** URI SIP del S-CSCF
- **Capacidades:** IDs de capacidad separados por comas

### Ejemplo de Salida:

ID	Nombre	URI del S-CSCF	Capacidades
1	S-CSCF Primario	sip:scscf.ims.mnc001.mcc001.3gppnetwork.org:5060	0, 1
2	S-CSCF Secundario	sip:scscf2.ims.mnc001.mcc001.3gppnetwork.org:5060	0, 1

### Operaciones:

- Ver lista de S-CSCFs
- Comprobar capacidades configuradas
- Verificar URIs de S-CSCF

**Nota:** Para agregar/modificar S-CSCFs, coordinar con los administradores del sistema. Las nuevas entradas de S-CSCF requieren:

- Un nombre (etiqueta descriptiva como "Nuevo S-CSCF")
- La URI del S-CSCF (por ejemplo, sip:scscf3.example.com:5060;transport=tcp)
- IDs de capacidades asociadas (por ejemplo, capacidades 0 y 1)

## Visualizando Dominios de Confianza NDS

**Propósito:** Monitorear qué dominios de red son de confianza para el peering

### Columnas de Visualización:

- **ID:** ID de la base de datos
- **Dominio de Confianza:** FQDN de la red de confianza

#### Ejemplo de Salida:

ID	Dominio de Confianza
1	ims.mnc001.mcc001.3gppnetwork.org
2	ims.mnc002.mcc001.3gppnetwork.org
3	carrier.example.com

#### Operaciones:

- Ver dominios de confianza
- Verificar relaciones de peering

**Agregar Dominios de Confianza:** Coordinar con los administradores del sistema para agregar nuevos dominios de confianza. Cada entrada requiere el nombre de dominio completamente calificado (FQDN) de la red de confianza (por ejemplo, partner.example.com).

## Monitoreo de Sesiones Activas

**Propósito:** Ver la toma de decisiones en tiempo real del I-CSCF y la selección del S-CSCF

#### Información de Visualización:

- **Call-ID:** SIP Call-ID
- **Identidad del Usuario:** Identidad pública que se está consultando
- **S-CSCF Seleccionado:** Qué S-CSCF fue elegido
- **Coincidencia de Capacidades:** Capacidades que coincidieron
- **Resultado UAR/LIR:** Código de resultado de Diameter
- **Marca de Tiempo:** Cuándo se creó la sesión

#### Casos de Uso:

1. Verificar que la selección del S-CSCF esté funcionando
2. Solucionar problemas de enrutamiento
3. Monitorear la distribución de carga entre S-CSCFs
4. Analizar la coincidencia de capacidades

#### Ejemplo:

```
Call-ID: 3c26700857a87f84@10.4.12.165
Usuario: sip:12015551234@ims.mnc001.mcc001.3gppnetwork.org
S-CSCF Seleccionado: sip:scscf.ims.mnc001.mcc001.3gppnetwork.org:5060
Capacidades: obligatorias=[0,1], opcionales=[]
Operación: UAR (Registro)
Resultado: 2001 (FIRST_REGISTRATION)
```

## Gestión de Tablas Hash

Similar al P-CSCF, el I-CSCF puede usar tablas hash para almacenamiento en caché o lógica personalizada.

### Casos de Uso Comunes:

- Almacenar en caché resultados de UAR/LIR (TTL corto)
- Limitación de tasa por IP de origen
- Decisiones de enrutamiento personalizadas

**Operaciones:** Igual que en P-CSCF (listar, volcar, eliminar, vaciar)

## Flujos de Llamadas

### Flujo de Registro con I-CSCF

### Flujo de Llamada Terminante a través del I-CSCF

### Flujo de Failover del S-CSCF

## Solución de Problemas

### Problemas de Conectividad con el HSS

#### Peering Diameter Cerrado

**Síntomas:** No se puede consultar el HSS, todos los registros fallan

#### Pasos de Diagnóstico:

1. Verificar el estado del peer Diameter en la Interfaz Web:
  - Navegar a la página de Diameter
  - Seleccionar el nodo I-CSCF
  - Comprobar el estado del peer HSS
2. Verificar la conectividad de red al HSS (coordinar con el equipo de red si es necesario)
3. Intentar habilitar el peer a través del panel de control:
  - Navegar a la página de Diameter
  - Encontrar el peer HSS

- Hacer clic en el botón "Habilitar"
4. Revisar los registros del sistema a través de la página de registros del panel de control para mensajes CER/CEA (Intercambio de Capacidades) y errores de Diameter
  5. Coordinar con los administradores del sistema para verificar la configuración de Diameter si es necesario

## **Timeout de UAR/LIR**

**Síntomas:** Registros/llamadas con timeout, los registros muestran timeout de Diameter

### **Causas Posibles:**

- HSS sobrecargado
- Latencia de red
- Dominio de enrutamiento incorrecto
- HSS no responde a este I-CSCF

### **Soluciones:**

1. Revisar los registros del sistema para errores de timeout de Diameter
2. Verificar que el peer HSS esté conectado a través del panel de control (página de Diameter)
3. Coordinar con los administradores del sistema para:
  - Aumentar el timeout de transacción de Diameter si es necesario
  - Verificar la configuración del dominio de destino
  - Comprobar los registros del HSS si son accesibles
4. Monitorear el flujo de mensajes Diameter a través de la página de registros del panel de control
5. Coordinar con el equipo de red para verificar que no haya latencia de red o problemas de enrutamiento hacia el HSS

## **Problemas de Selección del S-CSCF**

### **No se Seleccionó S-CSCF**

**Síntomas:** 503 Servicio No Disponible, los registros muestran "No hay S-CSCF disponible"

### **Pasos de Diagnóstico:**

1. Verificar la lista de S-CSCF a través del panel de control:
  - Navegar a I-CSCF → pestaña Servidores S-CSCF
  - Verificar que los S-CSCF estén configurados con las capacidades apropiadas
2. Revisar los registros del sistema para capacidades UAA (User Authorization Answer) del HSS
3. Verificar la coincidencia de capacidades entre lo que devuelve el HSS y lo que está configurado en la base de datos del I-CSCF
4. Coordinar con los administradores del sistema para:
  - Verificar la conectividad de la base de datos
  - Agregar entradas de S-CSCF faltantes si es necesario
  - Comprobar que la configuración de capacidades coincide con las expectativas del HSS

### **S-CSCF Seleccionado Incorrectamente**

**Síntomas:** Las llamadas se enrutan a un S-CSCF inesperado

#### **Causas Posibles:**

- Desajuste de capacidades
- Problema de balanceo de carga
- Base de datos fuera de sincronización con el HSS

#### **Soluciones:**

1. Monitorear el seguimiento de sesiones a través del panel de control:
  - Navegar a I-CSCF → pestaña Sesiones
  - Revisar las decisiones de selección del S-CSCF
2. Revisar los registros del sistema para verificar si el HSS está asignando un nombre específico de S-CSCF (lo que anularía la lógica de selección)
3. Verificar que la lista de S-CSCF de la base de datos del I-CSCF y las capacidades coincidan con las expectativas del HSS
4. Coordinar con los administradores del sistema para revisar la configuración de coincidencia de capacidades

## **Problemas de Enrutamiento**

### **Solicitudes No Enviadas al S-CSCF**

**Síntomas:** El I-CSCF recibe la solicitud pero no la reenvía

#### **Pasos de Diagnóstico:**

1. Revisar los registros del sistema a través de la página de registros del panel de control para errores de enrutamiento
2. Verificar que la URI del S-CSCF de destino se esté configurando correctamente (comprobar los registros para decisiones de enrutamiento)
3. Verificar la conectividad de red al S-CSCF (coordinar con el equipo de red)
4. Comprobar que el S-CSCF seleccionado sea realmente accesible y responda
5. Coordinar con los administradores del sistema para habilitar el registro de depuración si es necesario para un análisis más profundo

### **El S-CSCF Responde Pero el I-CSCF No Reenvía**

**Síntomas:** Wireshark muestra respuesta al I-CSCF pero no se reenvía

#### **Causas Posibles:**

- Timeout de transacción
- Desajuste de encabezados Via
- Bucle de Record-Route

#### **Soluciones:**

1. Revisar los registros del sistema para errores de coincidencia de transacciones o detección de bucles
2. Verificar que los encabezados Via se estén procesando correctamente (comprobar registros)
3. Coordinar con los administradores del sistema para:
  - Aumentar el timeout de transacción si es necesario
  - Verificar que no haya bucles de enrutamiento SIP

## Problemas de Base de Datos

### Conexión a la Base de Datos Perdida

**Síntomas:** "Error de conexión a la base de datos" en los registros

**Soluciones:**

1. Coordinar con los administradores del sistema para:
  - Verificar que el servicio de base de datos esté en funcionamiento
  - Probar la conectividad de la base de datos
  - Habilitar la reconexión automática si no está configurada
  - Reiniciar el servicio I-CSCF si es necesario

### Desajuste del Esquema de la Base de Datos

**Síntomas:** Errores SQL en los registros sobre columnas/tablas faltantes

**Soluciones:**

1. Coordinar con los administradores del sistema para:
  - Verificar que el esquema de la base de datos coincida con la estructura esperada
  - Comprobar que las tablas s\_cscf, s\_cscf\_capabilities y nds\_trusted\_domains existan y tengan las columnas correctas
  - Re-crear el esquema de la base de datos si es necesario

## Mejores Prácticas

### Alta Disponibilidad

#### 1. Desplegar múltiples instancias de I-CSCF:

- Usar DNS SRV para balanceo de carga
- Cada instancia se conecta al mismo HSS
- Compartir base de datos (solo lectura para la lista de S-CSCF)

#### 2. Configuración de DNS SRV:

```
_sip._udp.ims.example.com. SRV 10 50 5060 icscf01.example.com.  
_sip._udp.ims.example.com. SRV 10 50 5060 icscf02.example.com.  
_sip._tcp.ims.example.com. SRV 10 50 5060 icscf01.example.com.  
_sip._tcp.ims.example.com. SRV 10 50 5060 icscf02.example.com.
```

#### 3. Operación sin estado:

El I-CSCF no mantiene el estado del diálogo, lo que hace que el failover sea fluido

## Ajuste de Rendimiento

1. **Procesos de trabajo:** Establecer un alto conteo de trabajadores para un rendimiento óptimo de consultas
  - children=64 (valor alto optimizado para la carga de trabajo pesada de consultas del I-CSCF)
  - tcp\_children=8 para manejar conexiones TCP
2. **Agrupamiento de conexiones a la base de datos:** Usar conexiones persistentes para reducir la sobrecarga de conexión
3. **Deshabilitar características innecesarias** para reducir la sobrecarga de procesamiento:
  - Sin manejo de RTP (el I-CSCF es solo de señalización)
  - Sin servicios de presencia
  - Registro mínimo en producción (configurado a nivel info o warning solamente)
4. **Optimizar Diameter** para la interfaz Cx de alto rendimiento:
  - sessions\_hash\_size=4096 (tabla hash más grande para un mejor rendimiento de búsqueda de sesiones)
  - workers=4 (hilos de trabajo Diameter dedicados para operaciones Cx concurrentes)

## Seguridad

1. **Validar dominios de confianza:** Comprobar Via/P-Visited-Network-ID
2. **Limitación de tasa:** Prevenir ataques DoS al HSS limitando consultas UAR/LIR por IP de origen
  - Usar módulo pike para verificar la tasa de solicitudes
  - Si se excede el límite de tasa, responder con 503 Demasiadas Solicituds
  - Protege al HSS de ser abrumado por inundaciones de consultas maliciosas
3. **TLS al HSS:** Usar Diameter sobre TLS (DTLS)
4. **Sanitizar encabezados:** Eliminar encabezados P no confiables de redes externas

## Monitoreo

1. **Métricas Clave:**

- Tasa de éxito de UAR
- Tasa de éxito de LIR
- Latencia promedio de consulta
- Distribución de S-CSCF (balanceo de carga)
- Tiempo de actividad del peer Diameter

## 2. Consultas de Prometheus:

```
# Tasa de éxito de UAR
rate(icscf_uar_success[5m]) / rate(icscf_uar_total[5m])

# Latencia promedio de Diameter
rate(diameter_request_duration_sum[5m]) /
rate(diameter_request_duration_count[5m])
```

## 3. Alertas:

- Peer HSS caído
- Todos los S-CSCFs no disponibles
- Alta tasa de errores (>5%)

## Mantenimiento de Base de Datos

El mantenimiento de la base de datos es manejado por los administradores del sistema. Las tareas clave de mantenimiento incluyen:

1. **Mantener la lista de S-CSCF actualizada:** Coordinar con los administradores para asegurar que la lista de S-CSCF en la base de datos coincida con las implementaciones reales
  - Verificar a través de la interfaz web: Navegar a I-CSCF → pestaña Lista de S-CSCF
  - Comprobar que todos los servidores S-CSCF activos estén listados con las capacidades correctas
2. **Limpiar sesiones antiguas:** Si los resultados de UAR/LIR están almacenados en caché, las entradas antiguas deben limpiarse periódicamente

## Referencia

### Especificaciones 3GPP

- **TS 23.228:** Arquitectura IMS
- **TS 29.228:** Interfaz Cx (I-CSCF a HSS)
- **TS 29.229:** Protocolo Cx/Dx

## **RFCs de Diameter**

- **RFC 6733:** Protocolo Base de Diameter
- **RFC 7155:** Traversal de NAT de Diameter



# Guía de Operaciones P-CSCF/E-CSCF

## Tabla de Contenidos

1. [Descripción General](#)
2. [Rol en la Arquitectura IMS](#)
3. [Funciones del P-CSCF](#)
4. [Funciones del E-CSCF](#)
5. [Operaciones de la Interfaz Web](#)
6. [Flujos de Llamadas](#)
7. [Solución de Problemas](#)

## Descripción General

El **P-CSCF** (Función de Control de Sesión de Llamadas Proxy) es el primer punto de contacto para el Equipo del Usuario (UE) en la red IMS. Sirve como un proxy de borde que maneja la seguridad, la aplicación de QoS y el enrutamiento de llamadas de emergencia. En esta implementación, el P-CSCF también funciona como el **E-CSCF** (CSCF de Emergencia) para servicios de emergencia.

**Importante:** En nuestras implementaciones, **el P-CSCF no reenvía medios por defecto**. Los flujos de medios van directamente entre el UE y **OmniTAS** (Servidor de Aplicaciones de Telefonía) u otros puntos finales de medios. El P-CSCF es puramente un proxy de señalización SIP.

## Especificaciones 3GPP

- **3GPP TS 23.228:** Subsistema de Multimedia IP (IMS) Etapa 2
- **3GPP TS 24.229:** Protocolo de Control de Llamadas IMS
- **3GPP TS 33.203:** Seguridad de acceso para IMS
- **3GPP TS 23.167:** Sesiones de emergencia del Subsistema de Multimedia IP (IMS)

## Responsabilidades Clave

1. **Primer Punto de Contacto:** Proxy SIP inicial del UE en IMS
2. **Aplicación de Seguridad:** Establecimiento y gestión de túneles IPsec
3. **Control de QoS:** Interfaz con PCRF a través de Rx para la aplicación de políticas
4. **Servicios de Emergencia:** Enruta llamadas de emergencia y proporciona búsqueda de IMEI a MSISDN (función E-CSCF)
5. **Compresión:** Soporte de SigComp para optimización de ancho de banda
6. **Soporte de Transporte:** Soporta UDP y TCP

# Rol en la Arquitectura IMS

## Posición en la Red

### Puntos de Referencia 3GPP

Interfaz	Protocolo	Propósito	Conectado A
Gm	SIP/IPsec	UE a P-CSCF	Equipo del Usuario
Mw	SIP	P-CSCF a I-CSCF/S-CSCF	Núcleo IMS
Rx	Diameter	Control de QoS/Política	PCRF
MI	HTTP/HELD	Recuperación de ubicación	LRF (E-CSCF)
Mg	SIP	Llamadas de emergencia	MGCF/E-CSCF

## Funciones del P-CSCF

### 1. Manejo de Registro

El P-CSCF es el primer salto para los mensajes SIP REGISTER de los UEs.

#### Flujo de Registro

#### Características Clave

#### Inserción de Encabezado Path:

Path: <sip:term@pcscf.ims.mnc001.mcc001.3gppnetwork.org:5060;lr>

- Asegura que las solicitudes subsiguientes se enruten de regreso a través del P-CSCF
- Requerido según RFC 3327 para IMS

#### Aplicación del Temporizador de Registro:

- Fuerza la expiración del registro a 599 segundos
- Sobrescribe los valores solicitados por el UE para el control de la red

#### Extracción de IMEI:

- Extrae IMEI del encabezado Contact:  
+sip.instance="<urn:gsma:imei:...>"
- Almacena en una tabla hash para el mapeo de llamadas de emergencia

#### Manejo Específico de Transporte:

- Dispositivos iOS: Extiende la vida útil de TCP para prevenir desconexiones prematuras

## 2. Funciones de Seguridad

### Gestión de Túneles IPsec

El P-CSCF establece túneles IPsec ESP con los UEs para la señalización SIP segura.

#### Configuración de IPsec:

La funcionalidad de IPsec se configura con los siguientes parámetros:

- **Dirección de escucha:** 10.4.12.165 (dirección IP del P-CSCF para puntos finales IPsec)
- **Puerto del cliente (base):** 5100 (puerto de inicio para tráfico UE → P-CSCF)
- **Puerto del servidor (base):** 6100 (puerto de inicio para tráfico P-CSCF → UE)
- **Rango de puertos:** Grupo configurable de puertos (típicamente 1000-10000 puertos)
- **Inicio de ID SPI:** 4096 (valor inicial para la asignación del Índice de Parámetro de Seguridad)
- **Rango de ID SPI:** 100000 (número de pares de SPI disponibles para asignación)
- **Máx. conexiones:** 20 (máximo de asociaciones de seguridad IPsec concurrentes por trabajador)

### Gestión de SPI y Puertos

Cada túnel IPsec entre un UE y el P-CSCF requiere identificadores únicos para mantener el tráfico separado y seguro. El sistema gestiona dos tipos de recursos:

#### Índices de Parámetros de Seguridad (SPIs):

Cada túnel IPsec utiliza DOS SPIs - uno para cada dirección:

- **spi-c** (SPI del cliente): Identifica paquetes enviados desde el UE al P-CSCF
- **spi-s** (SPI del servidor): Identifica paquetes enviados desde el P-CSCF al UE

Los SPIs se asignan en pares desde un grupo configurado. El sistema está típicamente configurado con:

- Valor inicial de SPI: 4096
- Rango disponible: 100,000 valores de SPI
- Esto proporciona capacidad para 50,000 túneles simultáneos (los pares se asignan como números consecutivos pares/impares)

### Asignación de Puertos:

Cada túnel también utiliza puertos UDP únicos en el P-CSCF:

- **puerto del cliente:** Puerto del P-CSCF donde recibe paquetes IPsec del UE
- **puerto del servidor:** Puerto del P-CSCF donde envía paquetes IPsec al UE

Configuración típica de puertos:

- Valor inicial del puerto del cliente: 5100
- Valor inicial del puerto del servidor: 6100
- Rango de puertos: 10,000 puertos disponibles
- Los puertos se reinician al inicio cuando se agota el rango

### **Cómo Funciona la Asignación de Recursos:**

Cuando un UE se registra y solicita protección IPsec:

1. **Primer Registro:** Obtiene spi-c=4096, spi-s=4097, puerto del cliente=5100, puerto del servidor=6100
2. **Segundo Registro:** Obtiene spi-c=4098, spi-s=4099, puerto del cliente=5101, puerto del servidor=6101
3. **Tercer Registro:** Obtiene spi-c=4100, spi-s=4101, puerto del cliente=5102, puerto del servidor=6102

Y así sucesivamente...

Después de 10,000 registros, los puertos se reinician al principio (5100, 6100), mientras que los SPIs continúan incrementándose. Esto permite más túneles que puertos disponibles, siempre que los UEs tengan direcciones IP diferentes.

### **Límites de Recursos:**

El número máximo de túneles IPsec simultáneos se determina por el límite que se alcance primero:

- Capacidad del rango de SPI (típicamente 50,000 pares)
- Capacidad del rango de puertos (típicamente 10,000 puertos)
- Capacidad de memoria y procesamiento del sistema

### **Monitoreo a través de la Interfaz Web:**

Navega a la página P-CSCF → Estadísticas IPsec (si está disponible) para ver:

- Número de túneles IPsec activos
- Número de pares de SPI/puerto disponibles
- Porcentaje de utilización

Si ves fallos de registro con errores relacionados con IPsec, puede indicar:

- Agotamiento del grupo de SPI (todos los 50,000 pares en uso)
- Agotamiento del grupo de puertos (todos los 10,000 puertos en uso)
- Túneles antiguos que no se están limpiando correctamente

### **Cuando se Liberan Recursos:**

Los SPIs y puertos se devuelven al grupo disponible cuando:

- Un UE se desregistra (envía REGISTER con Expires: 0)
- Un registro expira sin ser renovado
- Un túnel IPsec se destruye manualmente a través de la interfaz web
- El administrador del sistema limpia túneles obsoletos

### **Planificación de Capacidad:**

Para la planificación de despliegues:

- Cada túnel activo utiliza aproximadamente 1KB de memoria
- La implementación típica en producción soporta de 10,000 a 50,000 túneles simultáneos
- Monitorea las tendencias de utilización para predecir cuándo se necesita expansión de capacidad
- Si regularmente se supera el 80% de utilización, coordina con los administradores del sistema para aumentar los rangos de SPI/puerto

### **Configuración de Asociación de Seguridad (SA):**

1. El UE envía REGISTER con el encabezado Security-Client:

```
Security-Client: ipsec-3gpp; alg=hmac-sha-1-96; ealg=null;
                  spi-c=12345; spi-s=67890; port-c=5100; port-
                  s=6100
```

2. El P-CSCF responde con Security-Server:

```
Security-Server: ipsec-3gpp; alg=hmac-sha-1-96; ealg=null;
                  spi-c=11111; spi-s=22222; port-c=5100; port-
                  s=6100
```

3. El P-CSCF crea políticas IPsec usando setkey:

```
# Cliente a Servidor
spdadd <ue-ip>[5100] <pcscf-ip>[6100] any -P out ipsec esp/
transport//require;

# Servidor a Cliente
spdadd <pcscf-ip>[6100] <ue-ip>[5100] any -P in ipsec esp/
transport//require;
```

4. Todos los mensajes SIP subsiguientes utilizan el túnel IPsec

### **Algoritmos Soportados:**

- **Autenticación:** hmac-md5-96, hmac-sha-1-96
- **Cifrado:** null, des-ed3-cbc, aes-cbc (preferido: null para LTE)

## **3. Manejo de Medios**

**Nota Importante:** En nuestras implementaciones, **el P-CSCF NO reenvía medios por defecto**. Los medios (RTP/SRTP) fluyen directamente desde el UE a **OmniTAS** (Servidor de Aplicaciones de Telefonía) u otros puntos finales de medios. El P-CSCF maneja solo la señalización SIP.

**Los medios fluyen directamente entre los UEs y el OmniTAS (Servidor de Aplicaciones de Telefonía)**, eludiendo completamente el P-CSCF para el tráfico RTP/SRTP:



El P-CSCF maneja solo la señalización SIP. Todos los medios (voz, video) se establecen directamente entre el UE y OmniTAS.

## **4. Aplicación de QoS y Políticas (Interfaz Rx)**

### **Integración Diameter Rx**

**Propósito:** Coordinar QoS con PCRF para el establecimiento de portadoras

### **Configuración Diameter:**

El P-CSCF se conecta al PCRF a través de Diameter en el puerto 3868 utilizando la aplicación Rx (ID de Aplicación 16777236, ID de Vendedor 3GPP 10415).

### **Operaciones Rx:**

1. **AAR (Solicitud de Autorización de Autenticación):** Solicitar QoS para el flujo de medios
2. **AAA (Respuesta de Autorización de Autenticación):** PCRF concede/niega
3. **STR (Solicitud de Terminación de Sesión):** Liberar QoS al finalizar la llamada

## **Flujo de Mensajes AAR**

### **Información de Medios Enviada al PCRF:**

- Descripción del flujo (IP, puerto, protocolo)
- Requisitos de ancho de banda (subida/bajada)
- Tipo de medio (audio, video)
- Estado del flujo (habilitado, deshabilitado)

## **5. Protección Anti-Inundaciones**

**Configuración del Módulo Pike** (Limitación de Tasa): El módulo pike proporciona protección contra inundaciones con estas configuraciones:

- **Unidad de tiempo de muestreo:** 2 segundos - ventana de tiempo para medir la tasa de solicitudes
- **Densidad de solicitudes por unidad:** 16 solicitudes permitidas por ventana de 2 segundos desde una sola IP
- **Latencia de eliminación:** 300 segundos (5 minutos) - duración durante la cual una IP está bloqueada después de exceder el límite

**Seguimiento de Autenticaciones Fallidas:** El P-CSCF rastrea los intentos de autenticación fallidos para prevenir ataques de fuerza bruta:

- Mantiene un contador en una tabla hash para los intentos de autenticación fallidos por IP de origen
- Incrementa el contador en caso de fallo de autenticación con un tiempo de expiración de 120 segundos
- Si una IP excede 10 intentos fallidos dentro de 120 segundos, bloquea la IP con 403 Demasiados Intentos Fallidos
- Previene que los atacantes adivinen las credenciales de usuario

## **Funciones del E-CSCF**

El P-CSCF incluye funcionalidad de E-CSCF para el manejo de llamadas de emergencia.

### **Detección de Llamadas de Emergencia**

#### **URIs SIP Reconocidos:**

- urn:service:sos (emergencia general)
- urn:service:sos.police
- urn:service:sos.ambulance
- urn:service:sos.fire
- urn:service:sos.marine
- urn:service:sos.mountain

**Lógica de Detección:** Las llamadas de emergencia se detectan examinando el Request-URI:

- Verifica si el método es INVITE (solicitud de configuración de llamada)
- Verifica si el Request-URI coincide con patrones de emergencia:
  - Formato URN: urn:service:sos\* (URNs SOS definidos en RFC 5031)
  - Emergencia en América del Norte: 911
  - Emergencia Europea/Internacional: 112
- Si se detecta una llamada de emergencia, se enruta al bloque de manejo de EMERGENCIA para un procesamiento especial

## Mapeo de IMEI a MSISDN para Llamadas de Emergencia

**Por qué es Necesario:** Cuando los usuarios realizan llamadas de emergencia (por ejemplo, 911, 112, urn:service:sos), el UE a menudo **no proporciona el MSISDN (número de teléfono)** en el mensaje SIP. Los servicios de emergencia (PSAP - Punto de Respuesta de Seguridad Pública) necesitan conocer el número de teléfono del llamante para fines de devolución de llamada. Para resolver esto, el P-CSCF/E-CSCF mantiene un mapeo de IMEI (identificador del dispositivo) a MSISDN.

### Cómo Funciona:

#### 1. Durante el Registro (cuando se conoce el MSISDN):

- Extrae IMEI del parámetro +sip.instance del encabezado Contact (formato: urn:gsma:imei:123456-78-901234-5)
- Extrae MSISDN de la identidad pública del usuario (IMPU) en el nombre de usuario del encabezado From
- Almacena el mapeo IMEI → MSISDN en una tabla hash con un TTL de 24 horas (86400 segundos)
- Ejemplo: imei\_msisdn["urn:gsma:imei:123456789012345"] = "12015551234"
- **En implementaciones en clúster:** Replica automáticamente el mapeo a todos los demás nodos P-CSCF en el clúster

#### 2. Durante la Llamada de Emergencia (cuando el MSISDN podría estar ausente):

- Extrae IMEI del parámetro +sip.instance del encabezado Contact de la llamada de emergencia
- Realiza una búsqueda en la tabla hash para recuperar el MSISDN asociado con este IMEI
- Si se encuentra el MSISDN en el mapeo:
  - Agrega el encabezado P-Asserted-Identity con el MSISDN completo (sip:+12015551234@domain)
  - Esto proporciona al PSAP el número de devolución de llamada para el llamante de emergencia

## **Alta Disponibilidad - Sincronización entre Múltiples Nodos:**

En implementaciones de producción con múltiples nodos P-CSCF para redundancia, los mapeos IMEI→MSISDN se sincronizan automáticamente entre todos los nodos:

### **Comportamiento de Replicación del Clúster:**

Cuando un UE se registra en **el Nodo P-CSCF 1**:

1. El Nodo 1 crea el mapeo IMEI→MSISDN localmente
2. El Nodo 1 transmite inmediatamente el mapeo a todos los demás nodos P-CSCF en el clúster
3. **El Nodo P-CSCF 2, Nodo 3, etc.** reciben la actualización y crean copias locales idénticas
4. Todos los nodos ahora tienen el mismo mapeo IMEI→MSISDN

### **Por qué Esto Es Importante:**

Si un UE se registró a través del Nodo P-CSCF 1 pero realiza una llamada de emergencia que se enruta al Nodo P-CSCF 2 (debido a balanceo de carga o conmutación por error), el Nodo 2 ya tiene el mapeo IMEI→MSISDN y puede proporcionar el número de devolución de llamada al PSAP.

### **Mecanismo de Sincronización:**

La sincronización ocurre a través de mensajería basada en SIP entre nodos P-CSCF:

- Utiliza mensajes SIP personalizados para propagar actualizaciones de la tabla hash
- Los mensajes se envían en formato JSON que contiene el IMEI, MSISDN y TTL
- La transmisión es automática y transparente - no se necesita intervención del operador
- Las actualizaciones se transmiten a todos los miembros del clúster en milisegundos

### **Impacto en las Operaciones:**

- **Resiliencia:** Las llamadas de emergencia funcionan correctamente independientemente de qué nodo P-CSCF maneje la llamada
- **Sin Punto Único de Fallo:** Cualquier nodo P-CSCF puede proporcionar el número de devolución de llamada para cualquier UE registrado
- **Automático:** La sincronización está integrada y no requiere configuración o intervención manual
- **Monitoreo:** A través de la interfaz web, navega a P-CSCF → Tablas Hash → `imei_msisdn` para ver los mapeos en cada nodo

## **Requisitos de Configuración del Clúster:**

Para que la sincronización de la tabla hash funcione:

- Todos los nodos P-CSCF deben estar configurados con las direcciones de los demás
- Los nodos se descubren automáticamente a través de notificaciones de disponibilidad
- La conectividad de red debe permitir tráfico SIP entre todos los nodos P-CSCF
- Si la sincronización falla, verifica que las reglas del firewall permitan la comunicación entre nodos

## **Escenario de Ejemplo:**

1. El usuario se registra: IMEI=123456789012345, MSISDN=12015551234  
→ Almacenado: imei\_msisdn[123456789012345] = 12015551234
2. El usuario marca 911: INVITE urn:service:sos (MSISDN no en el encabezado From)  
→ El P-CSCF extrae IMEI del Contact: 123456789012345  
→ El P-CSCF busca: imei\_msisdn[123456789012345] → 12015551234  
→ El P-CSCF agrega encabezado: P-Asserted-Identity:  
<sip:+12015551234@...>  
→ El PSAP recibe la llamada con el número de devolución de llamada: +12015551234

## **Enrutamiento de Emergencia**

### **Características de la Llamada de Emergencia:**

- Elude la verificación de registro
- Agrega PDIFF-LO (Formato de Datos de Presencia - Objeto de Ubicación)
- Enruta al servidor de aplicaciones de emergencia o PSAP
- Manejo de prioridad (preempciona llamadas normales)
- Información de ubicación del LRF o UE

## **Operaciones de la Interfaz Web**

### **Accediendo a la Página P-CSCF**

Navega a: <https://<control-panel>/pcscf>

### **Diseño de la Página**

La página P-CSCF tiene tres pestañas principales:

1. **Contactos Registrados** - Registros activos
2. **Ubicación del Usuario** - Buscar por IMSI/IP
3. **Tablas Hash** - Tablas de memoria compartida

## Visualización de Contactos Registrados

### Columnas de Visualización:

- **AoR** (Dirección de Registro): Identidad SIP del usuario
- **Contact**: URI de contacto del dispositivo
- **Expires**: Marca de tiempo de expiración del registro
- **IP Pública**: Dirección IP pública del UE
- **Received**: IP recibida real (si es diferente de Contact)
- **Path**: Encabezado Path para enrutamiento
- **ID de Sesión Rx**: Sesión Diameter Rx (si QoS está activo)

### Características:

- Actualización automática cada 5 segundos
- Búsqueda por AoR o Contact parcial
- Ordenar por columna (hacer clic en el encabezado)
- Filas expandibles para detalles completos

### Ejemplo de Salida:

```
AoR: sip:12015551234@ims.mnc001.mcc001.3gppnetwork.org
Contact: sip:12015551234@10.4.12.100:5060;transport=udp
Expires: 2025-11-29 14:30:15
IP Pública: 10.4.12.100
Received: 10.4.12.100:52341
Path: <sip:term@pcscf.ims.mnc001.mcc001.3gppnetwork.org:5060;lr>
ID de Sesión Rx: rx-pcscf-session-12345
```

## Búsqueda de Ubicación del Usuario

### Opciones de Búsqueda:

- Por IMSI: imsi:310150123456789
- Por IP: 10.4.12.100

### Casos de Uso:

1. Encontrar qué usuario está utilizando una IP específica
2. Verificar si el IMSI está registrado
3. Verificar el estado del túnel IPsec
4. Comprobar rutas de servicio

# Gestión de Tablas Hash

## Tablas Comunes:

Tabla	Propósito	Tamaño Típico
imei_msisdn	Mapeo de emergencia IMEI→MSISDN	100-1000 entradas
service_routes	Rutas de servicio en caché	Por registro
dialog_out	Seguimiento de diálogos salientes	Por llamada

## Operaciones:

- **Listar Tablas:** Hacer clic en la pestaña "Tablas Hash"
- **Volcar Tabla:** Hacer clic en el nombre de la tabla para ver el contenido
- **Eliminar Entrada:** Hacer clic en "Eliminar" junto a la entrada
- **Limpiar Tabla:** Hacer clic en "Limpiar" para borrar toda la tabla (¡usar con precaución!)

## Ejemplo de Entrada:

Clave: urn:gsma:imei:123456-78-901234-5

Valor: 310150123456789

TTL: 86400 segundos (24 horas)

# Flujos de Llamadas

## Llamada de Origen Móvil (MO)

Todas las llamadas de origen se enrutan a través del TAS (OmniTAS) para la lógica de servicio y facturación:

## Llamada de Terminación Móvil (MT)

Las llamadas de terminación también pasan por el TAS para la lógica de servicio:

## Flujo de Llamada de Emergencia

# Solución de Problemas

## Problemas de Registro

### UE No Puede Registrarse

**Síntomas:** UE recibe 408 Timeout o no hay respuesta

## Pasos de Diagnóstico:

1. Verifica el estado del registro a través del panel de control:
  - Navega a la página P-CSCF
  - Verifica la pestaña "Contactos Registrados"
  - Asegúrate de que el usuario aparezca en la lista
2. Revisa los registros del sistema a través de la página de registros del panel de control para errores
3. Verifica la conectividad de red entre el UE y el P-CSCF
4. Verifica que las reglas del firewall permitan tráfico SIP (puerto 5060 UDP/TCP)
5. Coordina con los administradores del sistema si el servicio P-CSCF parece estar caído

## **Túnel IPsec No Establecido**

**Síntomas:** Se envía un desafío 401 pero el re-REGISTER falla

### **Pasos de Diagnóstico:**

1. Revisa los registros del sistema a través de la página de registros del panel de control para errores relacionados con IPsec
2. Verifica que el UE esté enviando el encabezado Security-Client en el REGISTER inicial
3. Verifica que el UE esté utilizando puertos IPsec (5100 cliente, 6100 servidor) en el re-REGISTER
4. Verifica que la dirección recibida coincida con el punto final esperado del túnel IPsec
5. Coordina con los administradores del sistema para verificar que los módulos del kernel IPsec estén cargados y que no existan conflictos de puertos

## **Problemas de Llamadas**

### **Las Llamadas No Se Enrutan al UE**

**Síntomas:** INVITE al P-CSCF pero el UE no suena

### **Pasos de Diagnóstico:**

1. Verifica que exista un registro a través del panel de control:

- Navega a la página P-CSCF
  - Verifica la pestaña "Contactos Registrados"
  - Busca al usuario y verifica que el registro esté activo
2. Verifica que el encabezado Path se haya almacenado en el registro
  3. Verifica que las llamadas se estén enviando a la dirección de contacto correcta
  4. Revisa los registros del sistema en busca de errores de enrutamiento
  5. Verifica que la ruta de red desde el P-CSCF al UE sea alcanzable

## **Audio Unidireccional**

**Síntomas:** Una parte no puede oír a la otra

**Nota:** En nuestras implementaciones, **el P-CSCF no reenvía medios**. Los medios fluyen directamente entre el UE y OmniTAS. Si estás experimentando audio unidireccional, el problema probablemente esté en los puntos finales o en el enrutamiento de la red, no en el P-CSCF.

## **Pasos de Diagnóstico:**

1. Verifica que el SDP en INVITE/200 OK contenga las direcciones IP y puertos correctos (revisa a través de registros del sistema o captura de paquetes si está disponible para los administradores)
2. Verifica que las reglas del firewall permitan tráfico RTP/SRTP entre el UE y OmniTAS
3. Verifica la configuración de NAT si el UE está detrás de NAT
4. Verifica que el punto final de medios de OmniTAS sea alcanzable desde el UE (conectividad de red)
5. Coordina con los administradores del sistema para análisis de captura de paquetes si es necesario

## **Fallos en Llamadas de Emergencia**

**Síntomas:** llamadas urn:service:sos rechazadas

## **Pasos de Diagnóstico:**

1. Verifica la tabla hash IMEI→MSISDN a través del panel de control:
  - Navega a P-CSCF → pestaña Tablas Hash

- Verifica que la tabla `imei_msisdn` contenga entradas
  - Verifica que el IMEI del llamante tenga un mapeo
2. Prueba primero con un usuario registrado realizando una llamada de emergencia (para aislar problemas de registro frente a problemas de enrutamiento de emergencia)
  3. Revisa los registros del sistema a través de la página de registros del panel de control para errores de enrutamiento de emergencia
  4. Verifica la configuración del Servidor de Aplicaciones de Emergencia
  5. Coordina con los administradores del sistema para revisar la configuración de la ruta de emergencia si es necesario

## **Problemas de Rendimiento**

### **Alta Utilización de CPU**

#### **Causas Posibles:**

- Demasiados registros
- Activación del anti-inundaciones Pike
- Consultas lentas en la base de datos

#### **Soluciones:**

1. Verifica el conteo de registros a través del panel de control:
  - Navega a P-CSCF → pestaña Contactos Registrados
  - Revisa el número total de registros activos
2. Revisa los registros del sistema en busca de bloqueos del anti-inundaciones Pike
3. Coordina con los administradores del sistema para escalar horizontalmente (agregar más instancias de P-CSCF) si es necesario

### **Alta Utilización de Memoria**

#### **Causas Posibles:**

- Crecimiento de la tabla hash
- Tabla de diálogos no limpiada
- Fuga de memoria

#### **Soluciones:**

1. Revisa las tablas hash a través del panel de control:
  - Navega a P-CSCF → pestaña Tablas Hash
  - Verifica los tamaños de las tablas y los conteos de entradas
2. Limpia entradas antiguas a través del panel de control:
  - Selecciona la tabla hash problemática
  - Usa la operación "Limpiar" si es necesario (usar con precaución - limpia toda la tabla)
3. Coordina con los administradores del sistema para reiniciar el servicio P-CSCF si se sospecha de una fuga de memoria

## **Problemas Diameter/Rx**

### **Par PCRF Cerrado**

**Síntomas:** El par Diameter muestra estado "Cerrado" en la Interfaz Web

#### **Pasos de Diagnóstico:**

1. Verifica el estado del par Diameter a través del panel de control:
  - Navega a la página Diameter
  - Selecciona el nodo P-CSCF
  - Verifica el estado del par PCRF (debería ser "I\_Open" cuando esté conectado)
2. Verifica la conectividad de red con el PCRF (coordina con el equipo de red si es necesario)
3. Intenta habilitar el par a través del panel de control:
  - Navega a la página Diameter
  - Encuentra el par PCRF
  - Haz clic en el botón "Habilitar"
4. Revisa los registros del sistema a través de la página de registros del panel de control para errores de conexión Diameter
5. Coordina con los administradores del sistema para verificar la configuración Diameter si es necesario

### **QoS No Funciona**

**Síntomas:** Las llamadas se conectan pero no se establece la portadora de QoS

## Pasos de Diagnóstico:

1. Revisa los registros del sistema a través del panel de control para mensajes AAR (Solicitud de Autorización de Autenticación) y AAA (Respuesta de Autorización de Autenticación)
2. Verifica el código de resultado de la respuesta del PCRF (debería ser 2001 para éxito)
3. Verifica que el par PCRF esté conectado (ver sección anterior)
4. Verifica que la información de medios en el SDP se esté enviando correctamente al PCRF
5. Coordina con los administradores del sistema para verificar la configuración de QoS si es necesario

## Mejores Prácticas

### Seguridad

1. **Siempre usa IPsec** para dispositivos móviles (LTE/5G)
2. **Habilita TLS** para clientes fijos/empresariales
3. **Configura anti-inundaciones** (Pike) para protección contra DoS
4. **Limita los intentos de autenticación fallidos** para prevenir fuerza bruta
5. **Usa cifrados fuertes** para TLS (desactiva SSLv2/v3)
6. **Rota regularmente** las claves IPsec (a través de re-registro)

### Rendimiento

1. **Ajusta hash\_size** según los registros esperados:
  - 1,000 usuarios: hash\_size=10 (crea  $2^{10} = 1,024$  cubos hash)
  - 10,000 usuarios: hash\_size=13 (crea  $2^{13} = 8,192$  cubos hash)
  - 100,000 usuarios: hash\_size=16 (crea  $2^{16} = 65,536$  cubos hash)
2. **Ajusta los procesos de trabajo** según los núcleos de CPU:
  - Establece los hijos para que coincidan con el número de núcleos de CPU para el procesamiento SIP
  - Establece tcp\_children en 2× núcleos de CPU para el manejo de conexiones TCP
3. **Usa mlock\_pages** para prevenir el intercambio:
  - Habilita mlock\_pages=yes para bloquear páginas de memoria compartida en RAM
  - Previene la degradación del rendimiento por el intercambio de

memoria a disco

#### 4. Desactiva la caché DNS para entornos IMS:

- Establece dns\_cache\_init=off para usar búsquedas DNS frescas
- Necesario para balanceo de carga dinámico basado en DNS SRV

#### 5. Habilita el balanceo de carga SRV:

- Establece dns\_srv\_lb=yes para distribuir el tráfico entre múltiples servidores
- Usa registros DNS SRV para distribución automática de carga

## Monitoreo

1. **Habilita métricas de Prometheus** (puerto 9090 en la configuración) - Consulta [Referencia de Métricas](#) para todas las métricas disponibles de P-CSCF
2. **Monitorea tendencias del conteo de registros**
3. **Rastrea la salud del par Diameter** (Rx al PCRF)
4. **Alerta sobre altas tasas de errores** en los registros
5. **Monitorea el conteo de diálogos** (sesiones activas)
6. **Revisa el uso de memoria** regularmente

## Alta Disponibilidad

1. **Despliega múltiples instancias de P-CSCF**
2. **Usa DNS SRV** para balanceo de carga:

```
_sip._udp.pcscf.example.com. SRV 10 50 5060 pcscf01.example.com.  
_sip._udp.pcscf.example.com. SRV 10 50 5060 pcscf02.example.com.
```
3. **Evita estado** cuando sea posible (proxy sin estado)
4. **Usa base de datos compartida** para datos persistentes (si es necesario)
5. **Monitorea a través de la interfaz web** utilizando verificaciones de salud del panel de control

## Servicios de Emergencia

1. **Siempre permite** llamadas de emergencia incluso si no están registradas
2. **Almacena el mapeo IMEI→MSISDN** durante el registro
3. **Establece TTL** para la tabla hash de emergencia (86400 = 24 horas)
4. **Prueba regularmente** con PSAP de prueba
5. **Asegura conectividad LRF** para ubicación
6. **Manejo de prioridad** para llamadas de emergencia

# Referencia

## Recursos Técnicos Adicionales

Para administradores de sistemas y desarrolladores, la documentación técnica del módulo está disponible en línea para los componentes de software subyacentes.

## Especificaciones 3GPP

- **TS 23.228:** Arquitectura IMS
- **TS 24.229:** Perfil SIP IMS
- **TS 33.203:** Seguridad de Acceso
- **TS 23.167:** Servicios de Emergencia
- **TS 29.214:** Interfaz Rx (PCRF)

## RFCs

- **RFC 3261:** SIP
- **RFC 3327:** Encabezado Path
- **RFC 3608:** Encabezado Service-Route
- **RFC 3GPP-IMS:** Encabezados P (P-Asserted-Identity, etc.)
- **RFC 5626:** Salida (gestión de conexiones)



# Guía de Operaciones del S-CSCF

## Tabla de Contenidos

1. [Descripción General](#)
2. [Rol en la Arquitectura IMS](#)
3. [Funciones del S-CSCF](#)
4. [Operaciones de la Interfaz Web](#)
5. [Flujos de Llamadas](#)
6. [Resolución de Problemas](#)

## Descripción General

El **S-CSCF** (Serving Call Session Control Function) es el servidor central de control de sesiones en el núcleo IMS. Realiza registro, autenticación, enrutamiento de sesiones y activación de servicios. El S-CSCF es el registrador autorizado para los usuarios en su red de origen y mantiene el estado completo de la sesión para todas las llamadas.

## Especificaciones 3GPP

- **3GPP TS 23.228:** Subsistema Multimedia IP (IMS) Etapa 2
- **3GPP TS 24.229:** Protocolo de Control de Llamadas IMS
- **3GPP TS 29.228:** Interfaz Cx (S-CSCF a HSS)
- **3GPP TS 29.229:** Protocolos Cx y Dx
- **3GPP TS 23.218:** Interfaz ISC (S-CSCF a AS)
- **3GPP TS 32.260:** Carga IMS

## Responsabilidades Clave

1. **Autoridad de Registro:** Registrador SIP autorizado para usuarios de la red de origen
2. **Autenticación:** Valida las credenciales del usuario a través del HSS
3. **Enrutamiento de Sesiones:** Enruta llamadas de origen y de terminación
4. **Activación de Servicios:** Invoca Servidores de Aplicaciones basados en iFC (Criterios de Filtro Inicial)
5. **Gestión de Perfiles de Usuario:** Almacena y aplica perfiles de servicio del HSS
6. **Presencia:** Maneja SUBSCRIBE/PUBLISH/NOTIFY para servicios de presencia
7. **Interconexión PSTN:** Enruta hacia/desde redes PSTN heredadas

**Nota sobre Carga:** Aunque el S-CSCF tiene la capacidad de realizar carga en

línea a través de la interfaz Ro a un OCS (Sistema de Carga en Línea), **en nuestras implementaciones esta funcionalidad está típicamente deshabilitada**. La carga es manejada en su lugar por el **TAS (Servidor de Aplicaciones de Telefonía)** donde puede contabilizar adecuadamente escenarios complejos como desvío de llamadas, transferencia de llamadas, roaming en redes 2G/3G y otros servicios suplementarios que el S-CSCF solo no puede rastrear con precisión.

## Características Clave

- **Con estado:** Mantiene el estado completo del diálogo
- **Lógica de Servicio:** Ejecuta reglas de enrutamiento complejas y activaciones de servicio
- **Integración HSS:** Sincronización continua con la base de datos de usuarios
- **Interfaz de Servidor de Aplicaciones:** ISC (Control de Servicio IMS)
- **CSCF Más Complejo:** Mayor configuración y más características

## Rol en la Arquitectura IMS

### Posición en la Red

### Puntos de Referencia 3GPP

Interfaz	Protocolo	Propósito	Conectado A
Mw	SIP	I-CSCF/P-CSCF a S-CSCF	I-CSCF, P-CSCF
ISC	SIP	S-CSCF a Servidor de Aplicaciones	AS, TAS
Cx	Diameter	Datos de usuario, autenticación, registro	HSS
Ro	Diameter	Carga en línea (tiempo real)	OCS
Rf	Diameter	Carga fuera de línea (CDR)	CDF/CGF
Mi	SIP	S-CSCF a BGCF	BGCF (enrutamiento PSTN)

## Funciones del S-CSCF

### 1. Registro y Autenticación

El S-CSCF es el registrador autorizado que valida las credenciales del usuario y almacena los enlaces de registro.

## **Flujo de Registro con Autenticación**

### **Algoritmos de Autenticación Soportados**

**Configuración:** El S-CSCF está configurado con los siguientes parámetros de autenticación:

- Tiempo de espera del vector de autenticación: 599 segundos
- Tamaño del hash de datos de autenticación: 1024 cubos
- Solo verifica IMPU para autenticación (no IMPI)

### **Algoritmos Soportados:**

- **AKAv1-MD5:** 3GPP AKA con MD5 (más común para LTE/5G)
- **AKAv2-MD5:** AKA mejorado
- **MD5:** Digest HTTP
- **CableLabs-Digest:** PacketCable/IMS para redes de cable
- **3GPP-Digest:** Variante Digest-MD5
- **TISPAN-HTTP\_DIGEST\_MD5:** ETSI TISPAN
- **Seleccionado por HSS:** Dejar que HSS elija el algoritmo

### **Flujo AKA:**

1. **RAND:** Desafío aleatorio (128 bits)
2. **AUTN:** Token de autenticación para probar la identidad del HSS
3. **XRES:** Respuesta esperada del UE
4. **CK/IK:** Clave de Cifrado / Clave de Integridad para IPsec

### **Generación de Nonce:**

```
nonce = base64(RAND) + ":" + algorithm_indicator
```

### **Validación de Respuesta:**

```
UE_response = base64(RES)
Expected = base64(XRES)

if (UE_response == Expected) {
    # Éxito de autenticación
} else {
    # Fallo de autenticación
}
```

### **Re-Sincronización AKA**

Si el número de secuencia (SQN) del UE está fuera de sincronización con el HSS:

### **Proceso:**

1. UE envía AUTS (token de sincronización de autenticación) en el encabezado de Autorización
2. S-CSCF extrae AUTS del encabezado
3. S-CSCF envía MAR (Solicitud de Autenticación Multimedia) con AUTS al HSS
4. HSS re-sincroniza su número de secuencia y envía nuevos vectores de autenticación
5. S-CSCF recibe nuevos vectores y continúa el flujo de autenticación

## Parámetros de Registro

El S-CSCF está configurado con los siguientes parámetros de registro:

### Tiempos de Expiración de Registro:

- Expira por defecto/min/max: 599 segundos (aproximadamente 10 minutos)
- Expiración por defecto/min/max de suscripción: 599 segundos

### Gestión de Contactos:

- Máximo de contactos por IMPU: 1 (registro de un solo dispositivo)
- Comportamiento máximo de contacto: Sobrescribir el más antiguo (cuando se excede el límite, eliminar el contacto más antiguo)

## 2. Base de Datos de Ubicación de Usuario (USRLOC)

El S-CSCF mantiene una base de datos de usuarios registrados y sus enlaces de contacto.

### Estructura de la Base de Datos

El S-CSCF mantiene varias tablas de base de datos para almacenar información de registro y usuario:

**Tabla IMPU:** Almacena Identidades Públicas Multimedia IP (los URI SIP con los que los usuarios se registran). Cada IMPU tiene atributos como:

- Identidad pública (sip:user@domain.com)
- Tipo (identidad pública de usuario vs. identidad pública de servicio)
- Estado de prohibición
- Estado de registro (registrado/no registrado)
- Direcciones de función de carga (CCF1, CCF2, ECF1, ECF2)

**Tabla de Contactos IMPU:** Almacena los enlaces de contacto reales para cada IMPU, incluyendo:

- URI de contacto (dónde alcanzar el dispositivo)
- Tiempo de expiración

- Encabezado de ruta (ruta de regreso a través de P-CSCF)
- Cadena User-Agent
- Dirección recibida (IP real de donde vino el REGISTER)

**Tabla de Suscriptores:** Mapea IMPIs (Identidades Privadas) a sus IMPUs asociados. Una identidad privada puede tener múltiples identidades públicas.

**Tabla de Perfiles de Servicio:** Almacena el perfil XML del usuario recibido del HSS durante el registro, incluyendo Criterios de Filtro Inicial (iFC) para la activación de servicios.

## Configuración de la Tabla Hash

El S-CSCF utiliza una tabla hash en memoria para búsquedas rápidas de registro. Para implementaciones con más de 20,000 usuarios, el tamaño del hash debe ajustarse adecuadamente (por ejemplo, 8,192 cubos para ~50,000 usuarios) para mantener el rendimiento de búsqueda.

## Gestión de Registros a través de la Interfaz Web

Todas las operaciones de ubicación de usuario se pueden realizar a través de la **interfaz web del panel de control** en /scscf:

- **Pestaña de Lista de Registro:** Ver todos los usuarios registrados con paginación y búsqueda
- **Pestaña de Ubicación de Usuario:** Consultar detalles específicos de IMPU incluyendo todos los enlaces de contacto
- **Acciones Rápidas:** Buscar, desregar, volcar IFC y probar operaciones IFC

La interfaz web proporciona una vista en tiempo real del estado de registro, enlaces de contacto y permite acciones administrativas como la desactivación forzada cuando sea necesario para la resolución de problemas.

## 3. Criterios de Filtro Inicial (iFC) y Activación de Servicios

El S-CSCF evalúa **iFC** (Criterios de Filtro Inicial) del perfil de servicio del usuario para determinar cuándo invocar Servidores de Aplicaciones.

### Estructura de iFC (XML)

#### Ejemplo del Perfil de Usuario del HSS:

```
<IMSSubscription>
  <PrivateID>user@ims.mnc001.mcc001.3gppnetwork.org</PrivateID>
  <ServiceProfile>
    <PublicIdentity>
```

```

<Identity>sip:user@ims.mnc001.mcc001.3gppnetwork.org</Identity>
<IdentityType>0</IdentityType> <!-- 0=identidad pública de
usuario -->
</PublicIdentity>

<InitialFilterCriteria>
<Priority>0</Priority> <!-- Menor = mayor prioridad -->
<TriggerPoint>
<ConditionTypeCNF>1</ConditionTypeCNF> <!-- 0=DNF, 1=CNF -->
<SPT>
<ConditionNegated>0</ConditionNegated>
<Group>0</Group>
<Method>INVITE</Method>
</SPT>
<SPT>
<ConditionNegated>0</ConditionNegated>
<Group>0</Group>
<SessionCase>0</SessionCase> <!-- 0=originando -->
</SPT>
</TriggerPoint>
<ApplicationServer>

<ServerName>sip:tas.ims.mnc001.mcc001.3gppnetwork.org</ServerName>
<DefaultHandling>0</DefaultHandling> <!--
0=SESSION_CONTINUADA, 1=SESION TERMINADA -->
</ApplicationServer>
</InitialFilterCriteria>

<InitialFilterCriteria>
<Priority>1</Priority>
<TriggerPoint>
<ConditionTypeCNF>0</ConditionTypeCNF> <!-- DNF -->
<SPT>
<ConditionNegated>0</ConditionNegated>
<Group>0</Group>
<RequestURI>^sip:\+1800.*</RequestURI> <!-- Sin costo -->
</SPT>
</TriggerPoint>
<ApplicationServer>
<ServerName>sip:tollfree-as.example.com</ServerName>
<DefaultHandling>0</DefaultHandling>
</ApplicationServer>
</InitialFilterCriteria>
</ServiceProfile>
</IMSSubscription>

```

## Activaciones de Puntos de Servicio (SPT)

### Tipos de SPT:

1. **Método**: Método SIP (INVITE, MESSAGE, SUBSCRIBE, etc.)
2. **RequestURI**: Regex en Request-URI
3. **SIPHeader**: Verificar presencia/valor de encabezado SIP
4. **SessionCase**: Originando (0), Terminando (1), Terminando No Registrado (2)
5. **SessionDescription**: Contenido SDP (tipo de medio, códec, etc.)

### Lógica:

- **CNF** (Forma Normal Conjuntiva): Y de O - (A 0 B) Y (C 0 D)
- **DNF** (Forma Normal Disyuntiva): O de Y - (A Y B) O (C Y D)

**Grupo**: Los SPT con el mismo número de grupo se OR'd juntos, luego los grupos se AND'd (para CNF).

## Flujo de Coincidencia de iFC

### Pruebas de iFC a través de la Interfaz Web

El panel de control proporciona dos operaciones a través de la interfaz web:

1. **Volcar iFC**: Mostrar todos los iFC para un usuario - muestra la estructura XML completa de los puntos de activación y el enrutamiento del Servidor de Aplicaciones
2. **Probar iFC**: Simular una llamada para ver qué AS se activaría - prueba un escenario de llamada hipotético con IMPU especificado, URI de origen y URI de destino para determinar qué iFC coincidiría

### Flujo de Trabajo de la Interfaz Web:

1. Navegar a la página S-CSCF
2. Hacer clic en la pestaña "IFC"
3. Ingresar IMPU
4. Elegir "Volcar IFC" o "Probar IFC"
5. Ver la estructura detallada de iFC con puntos de activación y enrutamiento de AS

## 4. Gestión de Diálogos

El S-CSCF mantiene el estado completo del diálogo SIP para todas las llamadas activas.

## **Base de Datos de Diálogos**

El S-CSCF mantiene una tabla de diálogos que rastrea llamadas activas con la siguiente información:

- Call-ID (identificador único para el diálogo SIP)
- URIs y etiquetas de From/To
- Números de secuencia del llamante y del llamado (CSeq)
- Conjuntos de rutas para ambas partes
- Direcciones de contacto
- Información de socket
- Estado del diálogo y marcas de tiempo
- Valores de tiempo de espera

## **Estados de Diálogo**

Los diálogos transitan por tres estados:

- **Temprano**: Respuesta provisional recibida (por ejemplo, 180 Ringing)
- **Confirmado**: 200 OK recibido y ACK enviado/recibido (llamada activa)
- **Eliminado**: BYE enviado/recibido (llamada finalizada)

## **Configuración de Diálogo**

El módulo de diálogo está configurado para:

- Detectar enrutamiento espiral (mismo pedido pasando varias veces)
- Mantener perfiles separados para lados de origen y de terminación
- Persistir diálogos en la base de datos (modo de escritura a través de actualizaciones periódicas)
- Establecer tiempos de espera específicos del diálogo
- Rastrear conjuntos de rutas para un enrutamiento adecuado dentro del diálogo

## **Operaciones de la Interfaz Web:**

1. Navegar a S-CSCF → pestaña Diálogos
2. Ver llamadas activas con:
  - Call-ID
  - URIs de From/To
  - Estado (Temprano/Confirmado)
  - Hora de inicio
  - Tiempo de espera
3. Hacer clic en "Finalizar Diálogo" para terminar una llamada específica
4. Hacer clic en "Finalizar Todos los Diálogos Activos" para una terminación masiva de emergencia

## 5. Manejo de Llamadas de Origen

Cuando un usuario registrado inicia una llamada, el S-CSCF la procesa como una sesión de **origen**.

### Flujo de Llamada de Origen

#### Configuración de Ruta de Origen

**Procesamiento de Llamadas de Origen:** El S-CSCF realiza varios pasos de validación y enrutamiento al procesar llamadas de origen:

1. **Verificación de Registro:** Verifica que el usuario que llama esté actualmente registrado. Si no, la llamada se rechaza con una respuesta 403 Prohibido.
2. **Gestión del Encabezado de Identidad:**
  - Elimina cualquier encabezado P-Asserted-Identity existente de la solicitud
  - Agrega un nuevo encabezado P-Asserted-Identity que contenga la identidad del llamante autenticado
3. **Correlación de Carga:** Crea y agrega un encabezado P-Charging-Vector que contenga:
  - Identificador de Carga IMS (icid) generado a partir del Call-ID y la marca de tiempo
  - Identificador de Inter-Operador de Origen (orig-roi) para carga entre operadores
4. **Activación de Servicios:** Evalúa los Criterios de Filtro Inicial (iFC) para activaciones de sesión de origen para determinar si se deben invocar Servidores de Aplicaciones
5. **Carga en Línea** (si está habilitada): Inicia una Solicitud de Control de Crédito Diameter Ro (CCR) con tipo de evento "0" (solicitud inicial) para llamadas de origen
6. **Seguimiento de Diálogo:** Asigna la llamada al perfil de diálogo "orig" (de origen) para fines de seguimiento
7. **Decisión de Enrutamiento:** Enruta la llamada ya sea hacia el manejo de PSTN (si el destino es un número de teléfono) o hacia el I-CSCF de terminación para enrutamiento IMS

## 6. Manejo de Llamadas de Terminación

Cuando una llamada está destinada a un usuario registrado, el S-CSCF la procesa como **terminación**.

### Flujo de Llamada de Terminación

#### Configuración de Ruta de Terminación

**Procesamiento de Llamadas de Terminación:** El S-CSCF maneja llamadas de terminación intentando primero localizar al usuario llamado y luego aplicando la lógica de servicio apropiada:

1. **Búsqueda de Ubicación del Usuario:** Consulta la base de datos de registro para determinar si el usuario llamado está actualmente registrado
  - Utiliza el nombre de usuario y el dominio del Request-URI para construir el IMPU
  - Recupera enlaces de contacto e información de enrutamiento si está registrado
2. **Si el Usuario NO Está Registrado:**
  - Intenta recuperar el perfil de servicio no registrado del HSS a través de la Solicitud de Asignación de Servidor (SAR)
  - Si tiene éxito, evalúa iFC para activaciones de sesión "no registradas" (por ejemplo, correo de voz, servicios fuera de línea)
  - Si no hay servicios no registrados disponibles, responde con 480 Temporalmente No Disponible
3. **Si el Usuario ESTÁ Registrado:**
  - Evalúa iFC para activaciones de sesión "de terminación" para determinar la invocación del Servidor de Aplicaciones
  - Inicia carga en línea (si está habilitada) enviando Diameter Ro CCR con tipo de evento "0" para llamadas de terminación
  - Asigna la llamada al perfil de diálogo "term" (de terminación) para seguimiento
  - Reenvía el INVITE al P-CSCF registrado utilizando el encabezado Path almacenado durante el registro

## 7. Interconexión PSTN a través de OmniTAS

El S-CSCF enruta llamadas hacia/desde PSTN a través de la **interfaz Mi** al **BGCF (Función de Control de Puerta de Salida)**, que está integrada dentro de OmniTAS en nuestra implementación.

## **Interfaz Mi - S-CSCF a BGCF**

**Punto de Referencia 3GPP:** Mi (interfaz SIP entre S-CSCF y BGCF)

La interfaz Mi se utiliza cuando el S-CSCF determina que una llamada necesita salir hacia el PSTN. En nuestra arquitectura, la funcionalidad BGCF está construida directamente en OmniTAS, por lo que todas las llamadas de origen móvil (MO) destinadas a números PSTN se enrutan a OmniTAS.

## **Flujo de Enrutamiento PSTN**

**Cómo Funciona el Enrutamiento PSTN:**

1. **Detección del Número de Destino:** El S-CSCF examina el Request-URI para determinar si el destino es un número de teléfono (formato E.164 como +12015551234)
2. **Enrutar a OmniTAS:** Para destinos PSTN, el S-CSCF enruta la llamada a través de la interfaz Mi a OmniTAS, que incluye funcionalidad BGCF integrada
3. **Procesamiento BGCF en OmniTAS:** OmniTAS determina el punto de salida PSTN apropiado basado en:
  - Análisis del número de destino (código de país, código de área)
  - Reglas de enrutamiento de menor costo
  - Grupos de troncos disponibles
  - Selección de operador
4. **Salida PSTN:** OmniTAS maneja la interacción real de la puerta de medios para completar la llamada a la red PSTN

**Detalles de la Interfaz Mi:**

- **Protocolo:** SIP
- **Propósito:** Enrutar llamadas destinadas a PSTN desde S-CSCF a BGCF
- **Dirección:** S-CSCF → OmniTAS (con BGCF)
- **Tipos de Llamadas:** Llamadas de origen móvil (MO) a números PSTN

**Configuración:** El S-CSCF está configurado para reconocer destinos PSTN (números de teléfono) y enrutar a OmniTAS. Cuando OmniTAS se utiliza como el TAS (Servidor de Aplicaciones de Telefonía), incluye inherentemente capacidades BGCF, eliminando la necesidad de un componente BGCF separado.

## **8. Arquitectura de Carga**

El S-CSCF tiene la capacidad incorporada para interactuar con un OCS (Sistema de Carga en Línea) a través de la interfaz Diameter Ro para control de crédito en

tiempo real. Sin embargo, **en nuestras implementaciones, la carga del S-CSCF está típicamente deshabilitada** a favor de realizar la carga a nivel del **TAS (Servidor de Aplicaciones de Telefonía)**.

## Por Qué la Carga se Realiza en el TAS en Lugar de en el S-CSCF

### Ventajas de la Carga Basada en TAS:

1. **Escenarios de Desvío de Llamadas:** Cuando una llamada es desviada, el S-CSCF solo ve el INVITE inicial al destino original. No tiene visibilidad sobre la lógica de desvío o el destino final. El TAS, sin embargo, maneja el servicio de desvío y sabe:
  - Quién inició la llamada
  - Para quién era originalmente la llamada
  - A dónde se desvió la llamada
  - Duración de la llamada desviada
  - Parte adecuada para cargar (llamante, desviado, o ambos)
2. **Roaming 2G/3G:** Cuando los suscriptores están en roaming en redes heredadas 2G/3G, las llamadas pueden eludir completamente el núcleo IMS y enrutarse a través de infraestructura de comutación de circuitos. El TAS se integra con dominios IMS y CS (Commutación de Circuitos) y puede:
  - Detectar cuándo un suscriptor está en roaming en 2G/3G
  - Aplicar cargos de roaming apropiados
  - Rastrear la duración de la llamada a través de tipos de red
  - Manejar transferencias entre dominios IMS y CS
3. **Transferencia de Llamadas:** Similar al desvío de llamadas, las transferencias de llamadas implican cambios en medio de la llamada que el S-CSCF no rastrea:
  - Transferencias ciegas (entrega inmediata)
  - Transferencias atendidas (consulta y luego entrega)
  - Transferencia a correo de voz
  - Transferencias de múltiples partes
4. **Llamadas en Conferencia:** Las conferencias de múltiples partes requieren lógica de carga especial:
  - Quién inició la conferencia
  - Cuántos participantes
  - Duración que cada participante estuvo en la llamada
  - Diferentes tarifas para el iniciador de la conferencia frente a los participantes
5. **Servicios Suplementarios:** Servicios como espera de llamadas, retención

de llamadas y llamada a tres vías requieren que el TAS entienda el estado del servicio:

- Múltiples llamadas simultáneas por usuario
- Eventos de retención/reanudación
- Llamadas fusionadas

6. **Lógica de Prepago vs. Postpago:** El TAS puede aplicar diferentes estrategias de carga:

- Prepago: Verificaciones de crédito en tiempo real y corte de llamada
- Postpago: Generación de CDR para facturación mensual
- Híbrido: Diferentes tarifas para diferentes características de servicio

7. **Flexibilidad de Tarificación:** El TAS tiene el contexto completo para aplicar reglas de tarificación complejas:

- Tarificación por hora del día
- Tarificación basada en el destino (local, larga distancia, internacional)
- Descuentos por volumen
- Tarifas promocionales
- Minutos de paquete frente a cargos por exceso

### **Limitaciones de Carga del S-CSCF:**

- Solo ve el diálogo SIP básico (INVITE → 200 OK → BYE)
- Sin conocimiento de servicios suplementarios
- No puede rastrear cambios en el estado de la llamada en medio de la llamada
- Contexto limitado para decisiones de tarificación
- No entiende la actividad del dominio CS

### **Interfaz Ro del S-CSCF (Disponible pero Deshabilitada por Defecto)**

Aunque no se utiliza en producción, el S-CSCF admite carga en línea a través de Diameter Ro. Esta capacidad permanece en la configuración pero está desactivada.

### **Cómo Funcionaría la Carga del S-CSCF (Si Estuviera Habilitada)**

Si se habilitara la carga del S-CSCF, el sistema utilizaría la interfaz Diameter Ro (ID de Aplicación 4) para comunicarse con un OCS. El S-CSCF estaría configurado con la información del par OCS (FQDN, realm, puerto 3868) y enviaría Solicitudes de Control de Crédito (CCR) en tres puntos clave en el ciclo de vida de la llamada:

### **Flujo CCR (Si Estuviera Habilitado):**

## Cuándo Se Activaría la Carga:

1. **CCR-Initial:** Enviado cuando se recibe el INVITE, antes de permitir que la llamada continúe. El OCS verifica el saldo de la cuenta y otorga crédito (permitiendo la llamada) o lo niega (llamada rechazada con 402 Pago Requerido).
2. **CCR-Update:** Enviado periódicamente durante la llamada basado en el tiempo de Granted-Service-Unit del OCS (por ejemplo, cada 300 segundos). Esto asegura que las llamadas largas no excedan el crédito disponible.
3. **CCR-Terminate:** Enviado cuando la llamada termina (BYE recibido o tiempo de espera del diálogo), informando el uso final al OCS para la deducción de cuentas.

**Implementación Real:** Dado que esta funcionalidad de carga está deshabilitada en nuestras implementaciones, el S-CSCF simplemente enruta llamadas sin ninguna verificación de control de crédito. Toda la lógica de carga es manejada aguas abajo por el TAS, que tiene visibilidad completa sobre el flujo de llamada completo y el contexto del servicio.

## 9. Presencia y SUBSCRIBE/PUBLISH

El S-CSCF maneja la presencia SIP para el estado de disponibilidad del usuario.

### Arquitectura de Presencia

#### Configuración de Presencia

La funcionalidad de presencia del S-CSCF está configurada con:

- **Máximo expira:** 3600 segundos (1 hora) - duración máxima de suscripción
- **Estado por defecto:** "activo" - el estado de presencia se establece por defecto en activo
- **Soporte PIDF:** Habilitado - permite la modificación de documentos PIDF (Formato de Datos de Información de Presencia)

### Manejo de PUBLISH

**Procesamiento de Publicación de Presencia:** Cuando el S-CSCF recibe una solicitud PUBLISH (utilizada para actualizar el estado de presencia):

1. **Detección de Método:** Verifica si la solicitud entrante es un método PUBLISH
2. **Verificación de Autorización:** Verifica que el usuario esté actualmente registrado en la base de datos de ubicación. Si no está registrado, responde con 403 Prohibido
3. **Actualización de Presencia:** Procesa la solicitud PUBLISH para

- actualizar la información de presencia del usuario en la base de datos de presencia
4. **Manejo de Errores:** Si el manejo de presencia falla (por ejemplo, error de base de datos, documento de presencia mal formado), responde con 500 Error del Servidor

## Manejo de SUBSCRIBE

**Procesamiento de Suscripción de Presencia:** Cuando el S-CSCF recibe una solicitud SUBSCRIBE (utilizada para observar la presencia de otro usuario):

1. **Detección de Método:** Verifica si la solicitud entrante es un método SUBSCRIBE
2. **Verificación de Tipo de Evento:** Examina el encabezado Event para determinar el tipo de suscripción
  - Si el evento es "reg" (paquete de evento de registro), esta es una suscripción a cambios en el estado de registro
  - Para suscripciones de eventos de registro, realiza una Solicitud de Asignación de Servidor (SAR) al HSS si el usuario no está registrado, para obtener el perfil de servicio
  - Evalúa iFC para activaciones de "suscripción" para determinar si algún Servidor de Aplicaciones debe manejar la suscripción
3. **Procesamiento de Suscripción de Presencia:** Maneja la solicitud SUBSCRIBE para crear o actualizar una suscripción de observador de presencia
4. **Manejo de Errores:** Si el procesamiento de la suscripción falla, responde con 500 Error del Servidor

## Operaciones de la Interfaz Web

### Accediendo a la Página S-CSCF

Navegar a: <https://<panel-de-control>/scscf>

### Diseño de la Página

La página S-CSCF tiene cinco pestañas principales:

1. **Lista de Registro** - Lista paginada de usuarios registrados
2. **Ubicación de Usuario** - Consultar detalles específicos de IMPU
3. **Diálogos** - Sesiones de llamadas activas
4. **IFC** - Gestión y prueba de Criterios de Filtro Inicial
5. **Tablas Hash** - Tablas de memoria compartida

### Pestaña de Lista de Registro

**Propósito:** Ver todos los usuarios registrados con paginación

## **Columnas de Visualización:**

- **IMPU:** Identidad Pública Multimedia IP (URI SIP)
- **Contactos:** Número de enlaces de contacto registrados
- **Estado:** Estado de registro (Registrado/No Registrado)
- **Expira:** Marca de tiempo de expiración del registro

## **Características:**

- Paginación (50 usuarios por página)
- Búsqueda por IMPU o contacto
- Ordenar por columna
- Hacer clic en la fila para expandir y ver detalles de contacto

## **Ejemplo:**

IMPU: sip:12015551234@ims.mnc001.mcc001.3gppnetwork.org

Contactos: 1

Estado: Registrado

Expira: 2025-11-29 15:45:30

[Expandir para ver:]

Contacto: sip:12015551234@10.4.12.100:5060;transport=tcp

Ruta: <sip:term@pcscf.ims.mnc001.mcc001.3gppnetwork.org:5060;lr>

User-Agent: Cliente IMS de Android v1.0

Recibido: 10.4.12.100:52341

## **Acciones Rápidas:**

- **Buscar:** Búsqueda rápida para un IMPU específico
- **Volcar IFC:** Ver Criterios de Filtro Inicial para el usuario
- **Probar IFC:** Simular llamada para probar activación de AS
- **Desregistrar:** Forzar desregistro (¡usar con precaución!)

## **Pestaña de Ubicación de Usuario**

**Propósito:** Consulta detallada de un IMPU específico

## **Operaciones:**

1. Ingresar IMPU (por ejemplo, `sip:user@domain.com`)
2. Hacer clic en "Buscar"
3. Ver información detallada:
  - Todos los contactos registrados
  - Encabezado Service-Route
  - Marcas de tiempo de registro
  - Encabezados de ruta
  - IMPIs asociados (Identidades Privadas)

## Casos de Uso:

- Solucionar por qué el usuario no puede recibir llamadas
- Verificar detalles de registro
- Comprobar enlaces de contacto
- Verificar rutas de servicio

## Pestaña de Diálogos

**Propósito:** Monitorear y gestionar sesiones de llamadas activas

### Columnas de Visualización:

- **Call-ID:** Call-ID SIP
- **From URI:** Identidad del llamante
- **To URI:** Identidad del llamado
- **Estado:** Temprano (sonando) o Confirmado (respondido)
- **Hora de Inicio:** Cuándo se creó el diálogo
- **Tiempo de Espera:** Valor de tiempo de espera del diálogo

### Operaciones:

- **Actualizar:** Actualización manual (actualización automática cada 5s)
- **Finalizar Diálogo:** Terminar llamada específica (envía BYE)
- **Finalizar Todos los Diálogos Activos:** Terminación masiva de emergencia

### Ejemplo:

Call-ID: 3c26700857a87f84@10.4.12.165  
From: sip:12015551234@ims.mnc001.mcc001.3gppnetwork.org  
To: sip:+12015555678@ims.mnc001.mcc001.3gppnetwork.org  
Estado: Confirmado  
Hora de Inicio: 2025-11-29 15:30:15  
Tiempo de Espera: 360000 segundos

[Botón Finalizar Diálogo]

**Advertencia:** Finalizar diálogos terminará inmediatamente las llamadas activas. Usar solo para resolución de problemas o situaciones de emergencia.

## Pestaña IFC

**Propósito:** Ver y probar Criterios de Filtro Inicial para activación de servicios

La pestaña IFC proporciona dos operaciones principales: Volcar IFC (recuperar y mostrar un IFC de un usuario desde el HSS) y Probar IFC (simular un escenario de llamada para ver qué Servidores de Aplicaciones se activarán).

## Operación Volcar IFC

1. Ingresar IMPU: `sip:user@domain.com`
2. Hacer clic en "Volcar IFC"
3. Ver estructura detallada de iFC:
  - Orden de prioridad
  - Puntos de activación (condiciones SPT)
  - URIs de Servidor de Aplicaciones
  - Manejo por defecto

### Ejemplo de Salida:

```
<InitialFilterCriteria>
  <Priority>0</Priority>
  <TriggerPoint>
    <ConditionTypeCNF>1</ConditionTypeCNF>
    <SPT>
      <Group>0</Group>
      <Method>INVITE</Method>
    </SPT>
    <SPT>
      <Group>0</Group>
      <SessionCase>0</SessionCase>  <!-- Originando -->
    </SPT>
  </TriggerPoint>
  <ApplicationServer>

<ServerName>sip:tas.ims.mnc001.mcc001.3gppnetwork.org</ServerName>
  <DefaultHandling>0</DefaultHandling>
</ApplicationServer>
</InitialFilterCriteria>
```

## Operación Probar IFC

1. Ingresar IMPU: `sip:user@domain.com`
2. Ingresar URI de Origen: `sip:user@domain.com` (parte que llama)
3. Ingresar URI de Destino: `sip:+12015555678@domain.com` (parte llamada)
4. Hacer clic en "Probar IFC"
5. Ver resultados:
  - Qué iFC coincidió
  - Qué Servidores de Aplicaciones se invocarían
  - En qué orden (prioridad)

## Casos de Uso:

- Verificar la configuración de activación de servicios
- Solucionar por qué no se invoca AS
- Probar nuevo iFC antes de desplegar en producción

- Entender el flujo de llamada para escenarios específicos

## Pestaña de Tablas Hash

Similar a P-CSCF e I-CSCF, gestionar tablas hash de memoria compartida.

### Tablas Hash Comunes del S-CSCF:

- auth: Caché de vectores de autenticación
- profile: Perfiles de usuario en caché (si se utiliza)
- Tablas personalizadas para lógica de servicio

## Flujos de Llamadas

### Flujo Completo de Registro

Ver la sección "1. Registro y Autenticación" arriba para el diagrama de secuencia detallado.

### Flujo Completo de Llamada de Origen

Ver la sección "5. Manejo de Llamadas de Origen" arriba para el diagrama de secuencia detallado.

### Flujo Completo de Llamada de Terminación

Ver la sección "6. Manejo de Llamadas de Terminación" arriba para el diagrama de secuencia detallado.

## Resolución de Problemas

### Problemas de Registro

#### Usuario No Puede Registrarse - 403 Prohibido

##### Causas Posibles:

- Usuario no provisionado en HSS
- HSS inalcanzable
- Fallo de autenticación
- Prohibición aplicada

##### Pasos de Diagnóstico:

1. Verificar conectividad HSS a través del panel de control:

- Navegar a la página Diameter
  - Seleccionar nodo S-CSCF
  - Verificar que el par HSS muestre como "I\_Open" (conectado)
2. Revisar los registros del S-CSCF para el flujo de mensajes MAR/MAA (Solicitud/Respuesta de Autenticación Multimedia)
  3. Verificar que el usuario exista en el HSS (si es accesible)
  4. Comprobar los registros del S-CSCF para los vectores de autenticación recibidos del HSS
  5. Probar con un algoritmo de autenticación diferente si se admite

## **Usuario No Puede Registrarse - 500 Error del Servidor**

### **Causas Posibles:**

- Conexión a la base de datos perdida
- Fallo de SAR/SAA
- Error de módulo

### **Soluciones:**

1. Verificar conectividad de base de datos desde el servidor S-CSCF (verificar que la base de datos sea alcanzable y que las credenciales sean correctas)
2. Revisar los registros del S-CSCF para el flujo de mensajes SAR/SAA (Solicitud/Respuesta de Asignación de Servidor) Diameter
3. Reiniciar el servicio S-CSCF si es necesario para recuperarse de errores de módulo

## **Problemas de Enrutamiento de Llamadas**

### **Llamadas No Enrutadas al Usuario**

**Síntomas:** INVITE llega al S-CSCF pero no se reenvía al P-CSCF

### **Pasos de Diagnóstico:**

1. Verificar que el usuario esté registrado a través de la interfaz web del panel de control:
  - Navegar a S-CSCF → pestaña Ubicación de Usuario
  - Ingresar el IMPU y hacer clic en "Buscar"
  - Verificar que el usuario aparezca como registrado con enlaces de contacto

2. Verificar que existan enlaces de contacto y que el encabezado Path esté presente
3. Revisar los registros del S-CSCF para el procesamiento de ruta de terminación
4. Probar con un destino diferente para aislar el problema

## **Servidor de Aplicaciones No Activado**

**Síntomas:** iFC debería coincidir pero AS no se invoca

### **Pasos de Diagnóstico:**

1. Volcar iFC a través de la interfaz web del panel de control:
  - Navegar a S-CSCF → pestaña IFC
  - Ingresar el IMPU
  - Hacer clic en "Volcar IFC"
  - Revisar los puntos de activación y las URIs del Servidor de Aplicaciones
2. Probar la coincidencia de iFC a través de la interfaz web:
  - Navegar a S-CSCF → pestaña IFC
  - Ingresar IMPU, URI de origen y URI de destino
  - Hacer clic en "Probar IFC"
  - Verificar qué iFC debería haber coincidido
3. Comprobar si se cargó el perfil de usuario desde el HSS revisando los registros
4. Verificar que la SAA (Respuesta de Asignación de Servidor) del HSS contenga el XML del perfil de usuario
5. Revisar los registros del S-CSCF para errores de análisis de iFC

## **Problemas de Diálogo**

### **Diálogos No Terminan Después de BYE**

**Síntomas:** El diálogo permanece en la base de datos después de que la llamada termina

### **Soluciones:**

1. Comprobar diálogos activos a través del panel de control:

- Navegar a S-CSCF → pestaña Diálogos
  - Revisar el conteo y estados de diálogos
2. Verificar la detección de BYE en los registros del módulo de diálogo
  3. Comprobar configuraciones de tiempo de espera de diálogo en la configuración
  4. Finalizar manualmente el diálogo a través del panel de control:
    - Navegar a S-CSCF → pestaña Diálogos
    - Encontrar el diálogo atascado
    - Hacer clic en "Finalizar Diálogo"
  5. Revisar la base de datos para entradas de diálogo huérfanas y limpiar si es necesario

## **Problemas de Carga**

### **Timeout de CCR**

**Nota:** En nuestras implementaciones, la carga del S-CSCF está típicamente deshabilitada. La carga es manejada por el TAS. Si está viendo errores relacionados con la carga, verifique que la carga Ro del S-CSCF no se haya habilitado accidentalmente.

**Síntomas:** Las llamadas fallan con errores de carga (si la carga está habilitada)

#### **Causas Posibles:**

- OCS inalcanzable
- Par Diameter Ro caído
- Tiempo de transacción demasiado corto

#### **Soluciones:**

1. Comprobar el estado del par OCS a través del panel de control:
  - Navegar a la página Diameter
  - Seleccionar nodo S-CSCF
  - Comprobar si el par OCS muestra como "I\_Open" (conectado)
2. Probar la conectividad de red OCS desde el servidor S-CSCF
3. Revisar la configuración del tiempo de espera de transacción Diameter
4. Comprobar los registros del S-CSCF para el flujo de mensajes CCR/CCA y errores

## **Crédito Insuficiente - Todas las Llamadas Fallan**

**Nota:** Este problema solo se aplica si la carga del S-CSCF está habilitada (lo cual normalmente no está en nuestras implementaciones).

**Síntomas:** Los usuarios reciben 402 Pago Requerido para todas las llamadas

### **Soluciones:**

1. Verificar que la carga del S-CSCF debería estar habilitada (normalmente debería estar deshabilitada)
2. Comprobar el saldo del OCS para cuentas de prueba si la carga está intencionalmente habilitada
3. Revisar los códigos de resultado de CCA (Respuesta de Control de Crédito) en los registros del S-CSCF
4. Considerar deshabilitar la carga del S-CSCF y usar la carga basada en TAS en su lugar

## **Problemas de PSTN**

### **Llamadas a PSTN Fallan - 503 No Hay Puerta de Salida Disponible**

#### **Causas Posibles:**

- No hay MGCF/p puerta de salida configurada
- Todas las puertas de salida caídas
- Dispatcher no cargado

#### **Soluciones:**

1. Coordinar con los administradores del sistema para verificar que las puertas de salida PSTN estén configuradas
2. Probar la conectividad de la puerta de salida desde el servidor S-CSCF (alcance de red, respuesta SIP)
3. Revisar la configuración de la puerta de salida con los administradores del sistema
4. Agregar puertas de salida faltantes si es necesario a través de los administradores del sistema

## **Problemas de Rendimiento**

### **Alto Uso de CPU**

#### **Causas Posibles:**

- Demasiados diálogos
- Consultas lentas a la base de datos
- Sobrecarga de evaluación de iFC

#### **Soluciones:**

1. Comprobar el conteo de diálogos a través del panel de control:
  - Navegar a S-CSCF → pestaña Diálogos
  - Revisar el número de diálogos activos
2. Optimizar tablas de base de datos (diálogo, impu, impu\_contact) si las consultas a la base de datos son lentas
3. Agregar índices a la base de datos si es necesario (en impu.impu, dialog.callid, etc.)
4. Ajustar el conteo de procesos de trabajo en la configuración si es necesario (aumentar de 4 por defecto a 8 para alta carga)

## **Mejores Prácticas**

### **Alta Disponibilidad**

1. **Desplegar múltiples S-CSCF** con base de datos compartida
2. **Usar capacidades** para la selección de S-CSCF en el I-CSCF
3. **Replicación de base de datos**: Maestro-maestro o maestro-esclavo
4. **Persistencia de sesión**: Modo de diálogo de escritura a través
5. **Verificaciones de salud**: Monitorear conteos de registro y diálogo

### **Seguridad**

1. **Siempre autenticar** usuarios a través del HSS
2. **Validar P-Asserted-Identity** solo de fuentes confiables
3. **Limitar la tasa** de registros y llamadas por usuario
4. **Sanitizar encabezados** de redes no confiables
5. **Usar TLS** para Diameter (Cx, Ro)

### **Rendimiento**

1. **Ajustar hash\_size para ubicación de usuario**: El tamaño del hash debe

establecerse según el número de usuarios esperado. Por ejemplo, hash\_size=13 (que equivale a  $2^{13} = 8192$  cubos) es apropiado para aproximadamente 50,000 usuarios

2. **Caché de perfiles de usuario:** Si el HSS lo admite, habilitar la caché de perfiles para reducir las solicitudes SAR Diameter
3. **Optimizar iFC:** Mantener las condiciones de Puntos de Activación (SPT) simples y minimizar el número de reglas de iFC por usuario para reducir la sobrecarga de evaluación
4. **Usar operaciones asíncronas para Diameter:** Configurar procesamiento asíncrono para MAR (autenticación), SAR (registro) y CCR (carga) para evitar bloquear procesos de trabajo
5. **Monitorear el rendimiento de la base de datos regularmente:** Rastrear tiempos de ejecución de consultas, optimizar índices y asegurar que el agrupamiento de conexiones esté funcionando eficientemente

## Monitoreo

Para una lista completa de todas las métricas del S-CSCF, consulte la [Referencia de Métricas](#).

Métricas clave a rastrear:

- Tasa de éxito de registro
- Tasa de éxito de MAR/SAR/LIR
- Conteo de diálogos (llamadas activas)
- Tiempo de evaluación de iFC
- Latencia de consulta a la base de datos
- Tiempo de actividad del par Diameter
- Tiempo de configuración de llamada

## Referencia

### Especificaciones 3GPP

- **TS 23.228:** Arquitectura IMS
- **TS 24.229:** Protocolo SIP IMS
- **TS 29.228:** Interfaz Cx
- **TS 23.218:** Interfaz ISC
- **TS 32.260:** Carga IMS



# Guía de Operaciones de la Interfaz Web

## Tabla de Contenidos

1. [Descripción General](#)
2. [Acceso al Panel de Control](#)
3. [Gestión de P-CSCF](#)
4. [Gestión de I-CSCF](#)
5. [Gestión de S-CSCF](#)
6. [Gestión de Pares de Diámetro](#)
7. [Operaciones de Tablas Hash](#)
8. [Visualización de Registros](#)
9. [Monitoreo y Métricas](#)

## Descripción General

La interfaz web de OmniCall CSCF proporciona un panel de control integral para el monitoreo y gestión en tiempo real de todos los componentes CSCF (P-CSCF, I-CSCF, S-CSCF). La interfaz está construida sobre Phoenix LiveView y proporciona:

- **Visibilidad en tiempo real** de registros, llamadas activas y estado del sistema
- **Gestión de tablas hash** para estructuras de datos en memoria críticas para el rendimiento
- **Monitoreo y control de pares de Diámetro**
- **Métricas de Prometheus** para el monitoreo del sistema
- **Visualización de registros en vivo** para la solución de problemas

## Arquitectura

El panel de control se comunica con las instancias de backend de CSCF para:

- Consultar registros de usuarios y datos de ubicación
- Inspeccionar diálogos activos (llamadas)
- Gestionar pares de Diámetro
- Ver y manipular tablas hash
- Acceder a la configuración de Criterios de Filtro Inicial (IFC)

# Acceso al Panel de Control

## Acceso Predeterminado

El panel de control es accesible a través de HTTP en el servidor CSCF:

```
http://<cscf-server>:4000/
```

**Puerto Predeterminado:** 4000 (configurable en `ControlPanel.Supervisor`)

## Configuración

El panel de control requiere la configuración del host CSCF en `config/config.exs` o `config/runtime.exs`:

```
config :cscf, :cscf_hosts,
  pcscf: [
    {host: "10.4.12.165", port: 9060, label: "P-CSCF 1"}
  ],
  icscf: [
    {host: "10.4.12.166", port: 9060, label: "I-CSCF 1"}
  ],
  scscf: [
    {host: "10.4.12.167", port: 9060, label: "S-CSCF 1"}
  ]
```

## Navegación

El panel de control proporciona pestañas de navegación para cada componente CSCF:

- **P-CSCF** - /pcscf - Contactos de registro y tablas hash
- **I-CSCF** - /icscf - Lista de S-CSCF, dominios NDS, sesiones
- **S-CSCF** - /scscf - Registros, diálogos, gestión de IFC
- **Diámetro** - /diameter - Estado y control de pares de Diámetro
- **Registros** - /logs - Visualización de registros en vivo

## Gestión de P-CSCF

**URL:** /pcscf

### Características

El panel de P-CSCF muestra contactos registrados e información de tablas hash de las instancias de P-CSCF.

## Pestaña de Contactos Registrados

Muestra todos los registros IMS actuales visibles para el P-CSCF:

Columna	Descripción
<b>IMSI</b>	IMSI del suscriptor o identificador de contacto
<b>Estado</b>	Estado de registro (registrado, no registrado)
<b>Expira</b>	Tiempo hasta que el registro expira
<b>Ruta</b>	Encabezado SIP Path para el enrutamiento

### Operaciones:

- **Hacer clic en la fila** para expandir y ver información detallada del contacto, incluyendo:
  - AoR completo (Dirección de Registro)
  - Dirección IP del UE
  - Detalles de la ruta
  - Estadísticas (máximos slots, registros)

## Pestaña de Tablas Hash

Gestionar tablas hash de P-CSCF. Ver [Operaciones de Tablas Hash](#) a continuación.

## Actualizaciones en Tiempo Real

La vista de P-CSCF se actualiza automáticamente cada 5 segundos para mostrar el estado actual del registro.

## Gestión de I-CSCF

URL: /icscf

### Características

El panel de I-CSCF proporciona monitoreo de las operaciones de I-CSCF, incluyendo la selección de S-CSCF y el seguimiento de sesiones.

## Pestaña de Lista de S-CSCF

Muestra todos los servidores S-CSCF configurados conocidos por el I-CSCF:

- **ID:** Identificador de S-CSCF
- **Nombre:** FQDN de S-CSCF
- **Capacidades:** Número de capacidades soportadas

## Pestaña de Dominios NDS

Muestra los dominios NDS (Seguridad de Dominio de Red) de confianza configurados en el I-CSCF.

## Pestaña de Sesiones

Muestra sesiones activas de I-CSCF, incluyendo:

- **Call-ID:** SIP Call-ID
- **Candidatos S-CSCF:** Lista de servidores S-CSCF considerados para asignación
  - Nombre de S-CSCF
  - Puntuación de selección
  - Edad (tiempo desde que se agregó el candidato)

## Pestaña de Tablas Hash

Gestionar tablas hash de I-CSCF. Ver [Operaciones de Tablas Hash](#) a continuación.

# Gestión de S-CSCF

**URL:** /scscf

El panel de S-CSCF es el más completo, proporcionando una gestión integral de registros, diálogos e IFC.

## Pestaña de Lista de Registros

Navegar por todos los registros activos con paginación:

**Características:**

- **Controles de paginación:** Desplazamiento y límite para grandes bases de datos de registros
- **Detalles de registro** para cada IMPU:
  - Identidad p~~u~~blica del usuario (IMPU)
  - Estado de registro
  - Número de slot
  - Detalles de contacto con User-Agent y expiración
  - Call-ID

**Acciones Rápidas** para cada registro:

- **Buscar:** Ver información detallada de IMPU
- **Volcar IFC:** Ver Criterios de Filtro Inicial para el usuario
- **Probar IFC:** Probar coincidencia de IFC para llamadas simuladas

- **Darse de baja:** Eliminar administrativamente el registro

## Pestaña de Ubicación del Usuario

Consultar e inspeccionar datos de ubicación del usuario:

- Ver estado de ubicación del usuario en bruto desde S-CSCF
- **Formulario de Búsqueda de IMPU:** Consultar identidad pública de usuario específica
- Muestra detalles completos del registro, incluyendo contactos, estado y metadatos

## Pestaña de Diálogos

Gestionar sesiones de llamadas activas (diálogos):

<b>Columna</b>	<b>Descripción</b>
<b>ID de Diálogo</b>	Identificador h_entry:h_id
<b>Call-ID</b>	SIP Call-ID
<b>De</b>	URI de la parte que llama
<b>A</b>	URI de la parte llamada
<b>Estado</b>	Estado del diálogo

**Operaciones:**

- **Terminar Diálogo:** Terminar llamada específica (envía BYE)
- **Terminar Todos:** Terminar todas las llamadas activas (con confirmación)

## Pestaña de IFC

Herramientas de Criterios de Filtro Inicial para la gestión de activación de servicios:

### Volcar IFC

Recuperar y mostrar todas las reglas IFC para un IMPU dado:

- Identidad pública
- Identidad privada
- Conteo de perfiles de servicio
- **Criterios de Filtro** para cada perfil de servicio:
  - Prioridad (orden de ejecución)
  - Manejo predeterminado (SESSION\_CONTINUED vs SESSION\_TERMINATED)
  - Nombre del Servidor de Aplicaciones
  - Banderas de inclusión de REGISTER
  - **Detalles del Punto de Activación:**

- Tipo de condición (DNF o CNF)
- Disparadores de Puntos de Servicio (SPTs):
  - METHOD, HEADER, SESSION\_CASE, REQUEST\_URI, etc.
  - Banderas de negación

La visualización de IFC incluye:

- Insignias de prioridad codificadas por color
- Explicaciones de la lógica de puntos de activación expandibles
- DNF (Forma Normal Disyuntiva) = OR de ANDs
- CNF (Forma Normal Conjuntiva) = AND de ORs

## **Probar IFC**

Probar qué Servidores de Aplicaciones se activarían para una sesión simulada:

### **Entrada:**

- URI (identidad pública del suscriptor)
- Dirección (originando o terminando)
- Método (INVITE, REGISTER, MESSAGE, SUBSCRIBE)
- URI de Solicitud (destino)

### **Salida:**

- Estado de registro
- Conteo de IFC coincidentes
- Lista de Servidores de Aplicaciones activados con índice de IFC

## **Pestaña de Tablas Hash**

Gestionar tablas hash de S-CSCF. Ver [Operaciones de Tablas Hash](#) a continuación.

## **Gestión de Pares de Diámetro**

**URL:** /diameter

### **Características**

Monitorear y controlar conexiones de pares de Diámetro (interfaces Cx, Rx, Ro).

### **Información Resumida**

El panel muestra:

- **Reino:** Reino de Diámetro

- **Identidad:** Host de Origen de Diámetro
- **Conteo de Pares:** Número de pares configurados
- **Trabajadores:** Conteo de trabajadores CDP
- **Longitud de Cola:** Transacciones pendientes
- **Tiempo de Espera de Conexión:** Tiempo de espera de conexión (segundos)
- **Tiempo de Espera de Transacción:** Tiempo de espera de transacción (segundos)
- **Aceptar Pares Desconocidos:** Bandera de política

## **Lista de Pares**

Tabla de todos los pares de Diámetro:

<b>Columna</b>	<b>Descripción</b>
<b>FQDN</b>	Nombre de dominio completamente calificado del par
<b>Estado</b>	Estado de conexión (I_Open, Closed, etc.)
<b>Estado</b>	Habilitado o Deshabilitado
<b>Último Usado</b>	Tiempo desde la última transacción
<b>Aplicaciones</b>	Número de aplicaciones de Diámetro soportadas

## **Operaciones:**

- **Habilitar Par:** Activar par deshabilitado
- **Deshabilitar Par:** Desactivar par (con confirmación)
- **Hacer clic en la fila:** Expandir para ver aplicaciones soportadas

## **Mapeo de Aplicaciones**

El panel de control mapea automáticamente los IDs de Aplicación de Diámetro a los nombres de interfaces 3GPP:

- **Cx/Dx** (16777216:10415) - Suscripción/Autorización IMS
- **Sh/Dh** (16777217:10415) - Acceso a Datos de Usuario
- **Rx** (16777236:10415) - Control del Plano de Medios IMS
- **Ro** (16777238:10415/0) - Carga en Línea
- **Gx** (16777224:10415) - Control de Políticas
- **S6a/S6d** (16777251:10415) - LTE/EPC MME-HSS
- Y muchos más (ver fuente: `diameter_live.ex`)

## **Actualizaciones en Tiempo Real**

El estado de los pares de Diámetro se actualiza automáticamente cada 5 segundos.

# Operaciones de Tablas Hash

## Descripción General

Los componentes CSCF utilizan tablas hash en memoria para datos críticos para el rendimiento. El panel de control proporciona visibilidad y gestión de estas tablas.

## Tablas Hash Disponibles

Las tablas varían según el tipo de CSCF. Ejemplos comunes:

Tabla Hash	CSCF	Propósito
imei_msisdn	P-CSCF	Mapeo de llamadas de emergencia
service_routes	P-CSCF	Rutas de servicio en caché
auth	S-CSCF	Vectores de autenticación
Varias	Todas	Caché específica del componente

Las tablas hash son estructuras de datos en memoria utilizadas para operaciones críticas para el rendimiento.

## Visualización de Tablas Hash

**Acceso:** Navegar a cualquier panel de CSCF → pestaña Tablas Hash

1. Ver lista de todas las tablas hash con estadísticas:
  - Nombre de la tabla
  - Conteo de ítems
  - Tamaño
2. **Seleccionar tabla** para ver entradas
3. **Ordenar** por nombre, ítems o tamaño

## Visualización del Contenido de la Tabla Hash

Hacer clic en una tabla para inspeccionar todas las entradas:

- **Clave:** Clave de la tabla hash
- **Valor:** Valor almacenado
- **Acciones:** Botón de eliminar

## Gestión de Entradas Hash

### Eliminar Entrada Única

1. Seleccionar tabla hash
2. Localizar la entrada
3. Hacer clic en el botón **Eliminar** (icono de papelera)
4. Confirmar acción

**Resultado:** Entrada eliminada de la tabla hash

### Vaciar Tabla Completa

1. Seleccionar tabla hash
2. Hacer clic en el botón **Limpiar Tabla**
3. **ADVERTENCIA:** Confirma antes de limpiar TODAS las entradas
4. Confirmar acción

**Resultado:** Todas las entradas eliminadas de la tabla

**Precaución:** Vaciar tablas puede causar interrupciones temporales en el servicio:

- Vacío de `imei_msisdn`: Las llamadas de emergencia pueden fallar hasta que se re-registre
- Vacío de `auth`: Desafíos de autenticación en progreso fallarán
- Vacío de `service_routes`: La próxima solicitud se enruta a través del descubrimiento de I-CSCF

## Visualización de Registros

**URL:** /logs

### Características

Ver registros de la aplicación en tiempo real desde el panel de control.

**Características** (implementación en la dependencia ControlPanel):

- Transmisión de registros en vivo
- Filtrado de nivel de registro
- Capacidades de búsqueda y filtrado

# Monitoreo y Métricas

## Integración con Prometheus

OmniCall CSCF expone métricas de Prometheus para monitoreo y alertas.

### Endpoint de Métricas:

```
http://<host>:9090/metrics
```

Cada host CSCF (P-CSCF, I-CSCF, S-CSCF) expone métricas en el puerto 9090. Configurar Prometheus para raspar todos los hosts para una visibilidad completa.

Para una referencia completa de todas las métricas de P-CSCF, I-CSCF y S-CSCE, ver la [Referencia de Métricas](#).

## Métricas Disponibles

Las siguientes métricas son expuestas por la aplicación del panel de control de OmniCall CSCF. Para métricas de componentes CSCF (SIP, Diámetro, IMS, etc.), ver la [Referencia de Métricas](#).

### Métricas de VM

- `vm_memory_total` - Memoria total de Erlang VM (bytes)
- `vm_memory_processes_used` - Memoria utilizada por procesos (bytes)
- `vm_memory_binary` - Memoria binaria (bytes)
- `vm_memory_ets` - Memoria de tabla ETS (bytes)
- `vm_total_run_queue_lengths_total` - Longitud total de la cola de ejecución
- `vm_system_counts_process_count` - Conteo de procesos
- `vm_system_counts_atom_count` - Conteo de átomos
- `vm_system_counts_port_count` - Conteo de puertos

### Métricas HTTP de Phoenix

- `phoenix_endpoint_stop_duration` - Duración de la solicitud HTTP (milisegundos)
- `phoenix_router_dispatch_stop_duration` - Duración de despacho del enrutador (milisegundos)

### Métricas de LiveView

- `phoenix_live_view_mount_stop_duration` - Duración de montaje de LiveView (milisegundos)

## Métricas de Integración de Backend CSCF

- cscf\_backend\_request\_count - Conteo de solicitudes RPC de backend
  - Etiquetas: host, command, result
- cscf\_backend\_request\_duration - Duración de RPC de backend (milisegundos)
  - Etiquetas: host, command
- cscf\_backend\_error\_count - Conteo de errores de RPC de backend
  - Etiquetas: host, error\_type

## Dashboards de Grafana

**Estado Actual:** Las métricas se exponen a través del endpoint de Prometheus. Los dashboards preconstruidos de Grafana no están incluidos actualmente, pero se pueden crear utilizando las métricas disponibles.

### Paneles de Dashboard Recomendados:

- Latencia de RPC de backend por comando
- Tendencias de conteo de registros
- Tendencias de conteo de diálogos
- Tasas de error de backend
- Uso de memoria de Erlang VM
- Rendimiento de montaje de LiveView

## Integración

Configurar Prometheus para raspar métricas de todos los hosts CSCF:

```
scrape_configs:  
  - job_name: 'cscf_pcscf'  
    static_configs:  
      - targets: ['pcscf1.example.com:9090',  
                 'pcscf2.example.com:9090']  
  
      - job_name: 'cscf_icscf'  
        static_configs:  
          - targets: ['icscf1.example.com:9090',  
                     'icscf2.example.com:9090']  
  
      - job_name: 'cscf_scscf'  
        static_configs:  
          - targets: ['scscf1.example.com:9090',  
                     'scscf2.example.com:9090']
```

# Mejores Prácticas

## Directrices Operativas

### Monitoreo:

- Monitorear métricas de Prometheus para la salud del sistema
- Estar atento a errores de RPC de backend
- Rastrear el crecimiento de la memoria de Erlang VM

### Gestión de Tablas Hash:

- Evitar vaciar tablas en producción a menos que sea absolutamente necesario
- Monitorear el crecimiento del tamaño de la tabla para posibles problemas de memoria
- Usar eliminación selectiva en lugar de vaciado completo de la tabla

### Solución de Problemas:

- Usar Registros en Vivo para depuración en tiempo real
- Verificar el estado de los pares de Diámetro antes de investigar fallos de registro
- Verificar la conectividad del backend CSCF si el panel de control muestra errores

### Rendimiento:

- La actualización automática del panel de control es de 5 segundos por defecto
- Listas de registros grandes utilizan paginación para evitar problemas de rendimiento
- Las operaciones de tablas hash son intensivas en lectura; minimizar operaciones de escritura durante horas pico

## Documentación Relacionada

- [Guía de Operaciones de P-CSCF](#) - Operaciones específicas de P-CSCF
- [Guía de Operaciones de I-CSRF](#) - Operaciones específicas de I-CSRF
- [Guía de Operaciones de S-CSCF](#) - Operaciones específicas de S-CSCF
- [Guía de Operaciones de Diámetro](#) - Gestión de pares de Diámetro
- [Guía de Operaciones de CSCF](#) - Operaciones generales de CSCF y solución de problemas



# Documentación de Cumplimiento de Intercepción ANSSI R226

**Propósito del Documento:** Este documento proporciona especificaciones técnicas requeridas para la autorización ANSSI R226 bajo los Artículos R226-3 y R226-7 del Código Penal Francés para la Red Central IMS OmniCSCF (Funciones de Control de Sesiones de Llamadas).

**Clasificación:** Documentación de Cumplimiento Regulatorio

**Autoridad Objetivo:** Agence nationale de la sécurité des systèmes d'information (ANSSI)

**Regulación:** R226 - Protección de la Privacidad de la Correspondencia y la Intercepción Legal

---

## 1. ESPECIFICACIONES TÉCNICAS DETALLADAS

### 1.1 Identificación del Sistema

**Nombre del Producto:** OmniCSCF IMS Core Network

**Tipo de Producto:** Red Central del Subsistema Multimedia IP (IMS)

**Función Principal:** Control de sesiones de llamadas VoIP/VoLTE y entrega de servicios multimedia

**Modelo de Despliegue:** Infraestructura de telecomunicaciones local

#### Componentes de la Red:

- P-CSCF (Función de Control de Sesiones de Llamadas Proxy)
- E-CSCF (Función de Control de Sesiones de Llamadas de Emergencia)
- I-CSCF (Función de Control de Sesiones de Llamadas Interrogante)
- S-CSCF (Función de Control de Sesiones de Llamadas Servidor)

Este sistema maneja el registro, la autenticación, el enrutamiento de sesiones y el control de llamadas para redes del Subsistema Multimedia IP (IMS). Las capacidades de intercepción detalladas y las características de cifrado se describen en las secciones a continuación.

### 1.2 Capacidades de Intercepción

#### 1.2.1 Captura de Registro y Adquisición de Sesiones

##### Captura de Registro SIP:

El sistema CSCF procesa todos los registros SIP y mantiene un estado de registro

completo:

- **Identificadores de Usuario:**

- IMPU (Identidad Pública Multimedia IP) - URI SIP (por ejemplo, sip:[+33612345678@ims.mnc001.mcc001.3gppnetwork.org](mailto:+33612345678@ims.mnc001.mcc001.3gppnetwork.org))
- IMPI (Identidad Privada Multimedia IP) - Nombre de usuario de autenticación (por ejemplo, [user@ims.mnc001.mcc001.3gppnetwork.org](mailto:user@ims.mnc001.mcc001.3gppnetwork.org))
- IMSI (Identidad Internacional de Suscriptor Móvil) - Desde P-headers o HSS
- MSISDN (Número de teléfono móvil) - Desde IMPU o perfil de usuario HSS

- **Metadatos de Registro:**

- URI de contacto (dirección de red UE actual)
- Encabezado de ruta (ruta de regreso a través de P-CSCF)
- Encabezado de Service-Route (ruta a S-CSCF)
- Cadena User-Agent (identificación del tipo de dispositivo)
- Marca de tiempo de expiración del registro
- Dirección IP y puerto de origen
- Protocolo de transporte (TCP/UDP/TLS)
- Vectores de autenticación (RAND, AUTN, XRES, CK, IK de HSS)

- **Información de Ubicación de la Red:**

- Encabezado P-Access-Network-Info (torre celular, área de ubicación)
- P-Visited-Network-ID (identificación de red de roaming)
- Dirección IP recibida (origen real)
- Dirección P-CSCF (punto de entrada a la red)

### **Captura de Sesiones de Llamadas:**

El S-CSCF mantiene un estado de diálogo SIP completo para todas las llamadas activas:

- **Identificadores de Sesión:**

- Call-ID (identificador de sesión único)
- URIs y etiquetas From/To
- Conjuntos de rutas para ambas partes
- Original-Dialog-ID (para seguimiento de interacción con el Servidor de Aplicaciones)

- **Metadatos de Sesión:**

- Identidad del llamante (encabezado From, P-Asserted-Identity)
- Parte llamada (encabezado To, Request-URI)
- Marca de tiempo de establecimiento de la sesión
- Marca de tiempo de terminación de la sesión
- Estado del diálogo (Temprano/Confirmado/Eliminado)
- Números CSeq (secuenciación de transacciones)

- **Información de Medios:**

- SDP (Protocolo de Descripción de Sesión) en los cuerpos de mensajes SIP
- Direcciones de servidores de medios (OmniTAS)
- Información de códec (formatos de audio/video)
- Puntos finales de flujo de medios
- Asignaciones de puertos RTP/RTCP

### **Identificación de Llamadas de Emergencia:**

El componente E-CSCF identifica y enruta llamadas de emergencia:

- Detección de números de emergencia (112, 911, etc.)
- Captura de IMEI (Identidad Internacional de Equipo Móvil)
- Mapeo de IMEI a MSISDN (para devolución de llamada)
- Información de ubicación de UE o red
- Soporte del protocolo HELD (HTTP-Enabled Location Delivery)
- Destino de enrutamiento de emergencia (PSAP/AS de emergencia)

### **1.2.2 Almacenamiento y Procesamiento de Datos**

#### **IMPORTANTE: Solo Estado en Memoria**

Los componentes CSCF (P-CSCF, E-CSCF, I-CSCF, S-CSCF) mantienen **todos los datos de estado solo en memoria**. No hay **almacenamiento de base de datos persistente** de datos de registro o de sesión de llamada. Todos los enlaces de registro, el estado del diálogo y las asociaciones de seguridad IPsec se almacenan en memoria y se pierden al reiniciar el sistema.

#### **Datos de Registro Activo (En Memoria):**

El sistema CSCF mantiene solo el estado en tiempo real:

#### **Estado de Registro P-CSCF:**

- Datos de Asociación de Seguridad IPsec (pares SPI, puertos, parámetros de cifrado)
- Vínculos de contacto de UE y direcciones de red
- Puntos finales y estado de túneles IPsec
- Períodos de validez del registro

#### **Estado de Registro S-CSCF:**

- Identidades públicas (IMPU) y estado de registro actual
- Vínculos de contacto con encabezados de ruta, User-Agent, direcciones recibidas
- Mapeos de identidad privada (IMPI) a identidad pública
- Perfiles de usuario de HSS (almacenados en caché durante el registro)

#### **Estado de Sesión Activo (En Memoria):**

El S-CSCF mantiene solo el estado de llamada activa:

- Identificadores de llamada (Call-ID), identidades de participantes (etiquetas From/To)

- Conjuntos de rutas y direcciones de contacto
- Estado de la sesión (Temprano/Confirmado/Terminado)
- Información de tiempo de la sesión

### **Sin CDR ni Seguimiento Histórico:**

Los componentes CSCF **no** generan ni almacenan:

- Registros de Detalles de Llamadas (CDRs)
- Registros históricos de llamadas
- Registros históricos de registro
- Seguimiento de eventos a largo plazo

**Generación de CDR y Seguimiento Histórico:** Todos los registros de detalles de llamadas, datos de facturación y seguimiento de llamadas históricas son manejados por el **TAS (Servidor de Aplicaciones de Telefonía - OmniTAS)**, no por los componentes CSCF.

### **Registro de Mensajes SIP/Diameter:**

Los CSCF pueden generar registros de eventos en tiempo real para fines operativos:

- **Registro de Mensajes SIP:** Registro opcional de mensajes SIP (INVITE, REGISTER, etc.)
- **Registro de Mensajes Diameter:** Registro opcional de transacciones Diameter (Cx, Rx, Ro)
- **Eventos del Sistema:** Cambios de configuración, errores, fallos

Estos registros son registros operativos transitorios, no registros de llamadas persistentes. La retención de registros es configurable y típicamente a corto plazo (horas a días) solo para fines de depuración.

### **1.2.3 Capacidades de Análisis**

#### **Monitoreo en Tiempo Real:**

El panel de control web Phoenix LiveView proporciona:

- **Monitoreo de Registro:**
  - Ver todos los usuarios registrados con paginación
  - Buscar por IMPU, contacto, IMPI
  - Detalles de registro (contacto, ruta, user-agent, expiración)
  - Capacidad de desregistro forzado
- **Monitoreo de Diálogo:**
  - Vista de sesiones de llamadas activas
  - Call-ID, URIs From/To, estado, duración
  - Capacidad de terminación de llamada (enviar BYE)
  - Actualización automática cada 5 segundos

- **Estado del Sistema:**

- Estado de pares Diameter (HSS, PCRF, conectividad OCS)
- Estado de la puerta de enlace frontal
- Métricas de capacidad del sistema
- Capacidad de túnel IPsec (P-CSCF)

**Nota sobre Datos Históricos:**

Los componentes CSCF no mantienen datos históricos. Para registros de llamadas históricos, CDRs y análisis de patrones de comunicación, las autoridades de intercepción legal deben coordinarse con **OmniTAS (Servidor de Aplicaciones de Telefonía)**, que maneja toda la generación de CDR y el seguimiento de llamadas a largo plazo.

**Visibilidad de Activación de Servicios en Tiempo Real:**

El S-CSCF procesa Criterios de Filtro Inicial (iFC) en tiempo real:

- La evaluación de iFC determina qué Servidores de Aplicaciones se activan para cada llamada
- Visibilidad en tiempo real de qué servicios se invocan
- Decisiones de enrutamiento del Servidor de Aplicaciones visibles en el flujo de mensajes SIP

**Estado de la Red:**

- Estado de conectividad HSS (interfaz Diameter Cx)
- Distribución de selección S-CSCF (I-CSCF)
- Patrones de enrutamiento de llamadas
- Tiempos de respuesta del Servidor de Aplicaciones
- Rendimiento de transacciones Diameter

## 1.3 Capacidades de Contramedidas

### 1.3.1 Mecanismos de Protección de la Privacidad

**Confidencialidad de la Comunicación:**

- **Túneles IPsec:** Túneles ESP (Encapsulating Security Payload) entre UE y P-CSCF
  - Cifrado: AES-CBC, AES-GCM
  - Autenticación: HMAC-SHA1, HMAC-SHA256
  - Derivación de claves de IMS AKA (CK/IK de HSS)
  - Asociaciones de seguridad por UE
- **Soporte TLS/TLS:**
  - Soporte SIP sobre TLS (SIPS)
  - Diameter sobre TLS (conexiones HSS, PCRF, OCS)
  - Autenticación basada en certificados

- Perfect Forward Secrecy (PFS) a través de ECDHE/DHE

- **Encabezados de Privacidad SIP:**

- P-Asserted-Identity (ID de llamada autenticada)
- Encabezado de privacidad (solicitar supresión de ID de llamada)
- Soporte para sesiones anónimas

**Control de Acceso:**

- Autenticación y control de acceso a la interfaz web
- Interfaz BINRPC para el panel de control (puerto 2046)
- Controles de acceso al registro y separación de roles
- Autenticación SIP (AKA a través de HSS)
- Autenticación de pares Diameter

**Registro de Auditoría:**

- Registro completo de mensajes SIP y Diameter
- Eventos de registro/desregistro
- Eventos de establecimiento y terminación de llamadas
- Acciones administrativas a través de la interfaz web
- Cambios de configuración
- Éxito/fracaso de autenticación

### 1.3.2 Características de Protección de Datos

**Seguridad de Acceso:**

- Control de acceso basado en roles (RBAC)
- Cuentas de monitoreo de solo lectura
- Controles de autenticación y autorización

**Fortalecimiento del Sistema:**

- Puertos de red expuestos mínimos (5060 SIP, 3868 Diameter, 8086 Web UI)
- Comprobación de sensatez de mensajes SIP
- Prevención de bucles Max-Forwards
- Limitación de tasa y protección contra inundaciones
- Límites de tamaño de mensajes
- Aislamiento de procesos de trabajo

## 1.4 Puntos de Integración de Intercepción Legal

### 1.5.1 Arquitectura de Intercepción Legal ETSI

El sistema CSCF proporciona la base para la intercepción legal conforme a ETSI. Si bien las interfaces nativas X1/X2/X3 no están integradas, existen todos los puntos de acceso de datos necesarios para la integración con sistemas externos de Función de Mediación de Intercepción Legal (LIMF).

## **Interfaces LI Estándar ETSI:**

### **Interfaz X1 - Función de Administración:**

- **Propósito:** Provisionamiento de órdenes y objetivos de las fuerzas del orden
- **Dirección:** LEMF → LIMF (bidireccional)
- **Funciones:**
  - Activar/desactivar la intercepción para objetivos (IMPUs, IMSIs, MSISDNs)
  - Establecer duración y período de validez de la intercepción
  - Configurar criterios de filtrado (identidades, ventanas de tiempo)
  - Recuperar estado de intercepción
- **Integración con CSCF:**
  - LIMF mantiene una base de datos de órdenes (lista de objetivos - externa a CSCF)
  - LIMF monitorea el estado en tiempo real de CSCF y los registros de mensajes para sesiones coincidentes
  - LIMF filtra según los criterios provisionados por X1

### **Interfaz X2 - Entrega de IRI (Información Relacionada con la Intercepción):**

- **Propósito:** Entregar metadatos de sesión a las fuerzas del orden
- **Dirección:** LIMF → LEMF (unidireccional)
- **Formato de Datos:** XML/ASN.1 conforme a ETSI TS 102 232
- **Contenido de CSCF:**
  - Identificadores de sesión (Call-ID, etiquetas de diálogo)
  - Parte que llama (URI From, P-Asserted-Identity, IMPU, IMSI, MSISDN)
  - Parte llamada (URI To, Request-URI, IMPU, IMSI, MSISDN)
  - Marcas de tiempo de registro
  - Marcas de tiempo de configuración/desmantelamiento de la sesión
  - Ubicación de la red (P-Access-Network-Info, torre celular, área de ubicación)
  - Direcciones P-CSCF/S-CSCF (identificación del elemento de red)
  - User-Agent (tipo de dispositivo)
  - Información de roaming (P-Visited-Network-ID)

### **Interfaz X3 - Entrega de CC (Contenido de la Comunicación):**

- **Propósito:** Entregar el contenido real de la comunicación
- **Dirección:** LIMF → LEMF (unidireccional)
- **Formato de Datos:** Conforme a ETSI TS 102 232
- **Contenido de CSCF:**
  - Cuerpos de mensajes SIP (descripciones de sesiones SDP)
  - Direcciones de servidores de medios (para intercepción RTP)
  - Información de códec
  - Mensajes instantáneos SIP MESSAGE (contenido del cuerpo)
  - Datos de aplicaciones (si se enrutan a través de CSCF)

**Nota:** Para flujos RTP de voz/video, el LIMF también debe integrarse con servidores de medios (OmniTAS) para capturar el contenido real de los medios. El CSCF proporciona información de configuración de sesión (SDP) que muestra dónde fluyen los medios.

## **1.5.2 Fuentes de Datos CSCF para Intercepción Legal**

### **1. Acceso a Datos de Registro:**

#### **Datos de Registro P-CSCF:**

- IMPU (identidad pública)
- URI de contacto (dirección de red UE)
- IP y puerto recibidos
- Encabezado de ruta
- Expiración del registro
- Información de SPI y puerto IPsec
- Cadena User-Agent

#### **Datos de Registro S-CSCF:**

- Identidades públicas (IMPU), estado de restricción, estado de registro
- Vínculos de contacto con encabezados de ruta, User-Agent, direcciones recibidas
- Mapeos de identidad privada (IMPI) a identidad pública
- Perfiles de usuario de HSS (formato XML que incluye detalles del suscriptor)

#### **Métodos de Acceso:**

- Interfaces de acceso a datos de solo lectura
- Interfaz de monitoreo de UI web
- Registro de eventos en tiempo real

### **2. Datos de Sesión Activa:**

#### **Datos de Diálogo S-CSCF:**

- Call-ID (identificador de sesión único)
- URIs y etiquetas From/To
- Números CSeq del llamante y el llamado
- Conjuntos de rutas para ambas partes
- Direcciones de contacto
- Estado del diálogo (Temprano, Confirmado, Eliminado)
- Marca de tiempo de inicio
- Valores de tiempo de espera

#### **Métodos de Acceso:**

- Monitoreo del estado del diálogo en tiempo real
- Consulta por identificadores de sesión o identificadores de partes
- Capacidades de exportación para análisis forense

### **3. Registro de Mensajes SIP:**

#### **Captura de Registros:**

- Todos los mensajes SIP pueden ser registrados (REGISTER, INVITE, MESSAGE, etc.)

- Niveles de registro configurables
- Registro estructurado con marcas de tiempo
- Registro basado en syslog o archivos

### **Análisis de Registros:**

- Analizar encabezados SIP para extracción de identidad
- Extraer SDP para información de medios
- Rastrear secuencias de mensajes (CSeq)
- Correlacionar solicitudes y respuestas

### **Ejemplo de Entrada de Registro:**

```

INFO: INVITE sip:+33687654321@ims.mnc001.mcc001.3gppnetwork.org SIP/2.0
From: <sip:+33612345678@ims.mnc001.mcc001.3gppnetwork.org>;tag=abc123
To: <sip:+33687654321@ims.mnc001.mcc001.3gppnetwork.org>
Call-ID: f81d4fae-7dec-11d0-a765-00a0c91e6bf6@ims.mnc001.mcc001.3gppnetwork.org
P-Asserted-Identity: <sip:+33612345678@ims.mnc001.mcc001.3gppnetwork.org>
P-Access-Network-Info: 3GPP-E-UTRAN-FDD; utran-cell-
id-3gpp=208011234567890
Content-Type: application/sdp

v=0
o=- 1234567890 1234567890 IN IP4 192.168.1.100
S=-
c=IN IP4 10.20.30.40
t=0 0
m=audio 49170 RTP/AVP 0 8
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000

```

### **4. Registro de Mensajes Diameter:**

#### **Mensajes Cx (Comunicación HSS):**

- UAR/UAA: Autorización de usuario (contiene IMPU, IMPI)
- LIR/LIA: Información de ubicación (contiene IMPU, S-CSCF que sirve)
- MAR/MAA: Autenticación (contiene IMPI, vectores de autenticación)
- SAR/SAA: Asignación de servidor (contiene IMPU, IMPI, perfil de usuario XML)

#### **Datos Diameter Disponibles:**

- IMSI (del perfil de usuario)
- MSISDN (del perfil de usuario)
- IMPUs asociados (múltiples identidades por suscriptor)
- Perfil de usuario (servicios, estado de restricción, estado de roaming)

### **Ejemplo de Registro:**

```

Diameter Cx SAA recibido del HSS:
User-Name: user@ims.mnc001.mcc001.3gppnetwork.org

```

```
Public-Identity: sip:+33612345678@ims.mnc001.mcc001.3gppnetwork.org
Server-Name: sip:scscf.ims.mnc001.mcc001.3gppnetwork.org
Result-Code: 2001 (Éxito)
User-Data: <XML perfil de usuario con IMSI, MSISDN, iFC>
```

## 5. Datos de Llamadas de Emergencia (E-CSCF):

### Mapeo de IMEI a MSISDN:

- P-CSCF crea un mapeo cuando UE se registra con IMEI
- TTL de 24 horas (Time-To-Live)
- Usado para devolución de llamada de emergencia
- Sincronizado a través de nodos del clúster P-CSCF

### Retención de Datos:

- Mapeos de IMEI a MSISDN retenidos durante 24 horas
- Disponibles para correlación de devolución de llamada de emergencia
- Accesibles a través de interfaces de monitoreo

### Registros de Llamadas de Emergencia:

- Detección de números de emergencia (112, 911, etc.)
- Extracción de IMEI de contacto o P-headers
- Información de ubicación (de HELD o P-Access-Network-Info)
- Enrutamiento PSAP (Punto de Respuesta de Seguridad Pública)
- Enrutamiento E-CSCF a AS de emergencia

### 1.5.3 Capacidades de Integración para LIMF

El sistema proporciona múltiples métodos de integración para sistemas de Función de Mediación de Intercepción Legal (LIMF):

#### 1. Acceso a Datos de Registro y Sesión:

- Acceso en tiempo real a datos de registro (identidades, ubicaciones, información del dispositivo)
- Monitoreo de sesiones activas (estado de llamada, participantes, tiempos)
- Capacidades de consulta histórica

#### 2. Registro de Eventos:

- Registro de mensajes SIP con niveles de detalle configurables
- Registro de mensajes Diameter para interacciones HSS
- Registros de eventos estructurados con marcas de tiempo

#### 3. Monitoreo en Tiempo Real:

- Monitoreo del estado de registro en vivo
- Seguimiento de sesiones de llamadas activas
- Detección de llamadas de emergencia e información de enrutamiento

Los métodos de integración admiten arquitecturas basadas en sondeo y basadas en eventos para la conectividad LIMF.

#### **1.5.4 Mapeo de Datos CSCF a Interfaces LI**

##### **Mapeo de Datos CSCF a IRI (X2):**

<b>Fuente de Datos CSCF</b>	<b>Campo IRI</b>	<b>Ejemplo de Datos</b>
IMPU (encabezados SIP/estado en memoria)	Parte A	sip: <a href="mailto:+33612345678@ims.mnc001.mcc001.3gppnetwork.org">+33612345678@ims.mnc001.mcc001.3gppnetwork.org</a>
IMPI (encabezados SIP/estado en Autenticación memoria)	ID de Autenticación	<a href="mailto:user@ims.mnc001.mcc001.3gppnetwork.org">user@ims.mnc001.mcc001.3gppnetwork.org</a>
IMSI (perfil de usuario HSS)	ID de Suscriptor	208011234567890
MSISDN (perfil de usuario HSS)	Número de Teléfono	+33612345678
Call-ID (encabezados SIP/estado de diálogo)	ID de Sesión	f81d4fae-7dec-11d0-a765-00a0c91e6bf6@...
From/To (encabezados SIP)	Parte A/Parte B	sip:+33612345678@... / sip:+33687654321@...
Marca de tiempo de registro (en memoria)	Tiempo del Evento	2025-11-29T10:30:00Z
P-Access-Network-Info (encabezado SIP)	Ubicación	3GPP-E-UTRAN-FDD;utran-cell-id-3gpp=208011234567890
IP Recibida (contacto SIP)	Dirección IP UE	10.20.30.40:5060
Dirección P-CSCF (enrutamiento Red SIP)	Elemento de Red	10.4.12.165:5060
Dirección S-CSCF (enrutamiento Red SIP)	Elemento de Red	10.4.11.45:5060

##### **Mapeo de Datos CSCF a CC (X3):**

Fuente de Datos CSCF	Campo CC	Ejemplo de Datos
Cuerpo SIP MESSAGE	Contenido del Mensaje Instantáneo	"Hola, ¿cómo estás?"
SDP en INVITE	Información de Sesión de Medios	Puntos finales RTP, códigos
Dirección del servidor de medios	Objetivo de Intercepción RTP	10.50.60.70:49170

**Nota:** Para el contenido real de voz/video (RTP), el LIMF debe coordinarse con servidores de medios (OmniTAS) para capturar flujos RTP. El CSCF proporciona solo información de configuración de sesión.

## 1.5 Interfaz de Monitoreo Basada en Web

El sistema incluye un panel de control basado en web para monitoreo en tiempo real y acceso administrativo:

### Capacidades de Monitoreo:

- Estado de registro en tiempo real (suscriptores activos, ubicaciones, información del dispositivo)
- Monitoreo de sesiones de llamadas activas (participantes, estado de llamada, tiempos)
- Búsqueda y filtrado por identidad (IMPU, IMPI, IMSI, MSISDN)
- Estado y capacidad del túnel IPsec
- Capacidades de exportación para análisis forense

### Seguridad:

- Acceso cifrado HTTPS/TLS
- Autenticación requerida
- Registro de auditoría de todas las acciones administrativas
- Modos de acceso de solo lectura para personal de monitoreo

## 2. CAPACIDADES DE CIFRADO Y CRIPTOANÁLISIS

### 2.1 Resumen de Capacidades Criptográficas

El OmniCSCF implementa múltiples capas de protección criptográfica para la señalización y los datos de suscriptores. Esta sección documenta todas las capacidades criptográficas según lo requerido por ANSSI.

### 2.2 Cifrado de Túnel IPsec ESP (UE a P-CSCF)

#### 2.2.1 Implementación del Protocolo IPsec

##### Modo IPsec Soportado:

- ESP (Encapsulating Security Payload) - Protocolo IP 50

- Modo de transporte (no modo túnel)
- Protege la señalización SIP entre UE y P-CSCF

### **Algoritmos de Cifrado Soportados:**

El sistema con IPsec del kernel soporta:

- **AES-CBC (Estándar de Cifrado Avanzado - Cadena de Bloques de Cifrado):**
  - AES-128-CBC (clave de 128 bits)
  - AES-192-CBC (clave de 192 bits)
  - AES-256-CBC (clave de 256 bits) - Recomendado
- **AES-GCM (Estándar de Cifrado Avanzado - Modo Galois/Contador):**
  - AES-128-GCM (clave de 128 bits con AEAD)
  - AES-256-GCM (clave de 256 bits con AEAD) - Recomendado
- **3DES-CBC (Triple DES - Cadena de Bloques de Cifrado):**
  - Clave efectiva de 168 bits (obsoleto, compatibilidad heredada)
- **Cifrado NULL:**
  - Sin confidencialidad (solo autenticación)
  - Usado solo para depuración o escenarios de cumplimiento específicos

### **Algoritmos de Autenticación Soportados:**

- **HMAC-SHA1 (Código de Autenticación de Mensajes Basado en Hash - SHA-1):**
  - Salida de 160 bits
  - Compatibilidad heredada
- **HMAC-SHA256 (HMAC - SHA-256):**
  - Salida de 256 bits
  - Recomendado
- **HMAC-SHA384 (HMAC - SHA-384):**
  - Salida de 384 bits
- **HMAC-SHA512 (HMAC - SHA-512):**
  - Salida de 512 bits
- **HMAC-MD5:**
  - Salida de 128 bits
  - Obsoleto, solo compatibilidad heredada

## **Derivación de Claves:**

Las claves IPsec (CK - Clave de Cifrado, IK - Clave de Integridad) se derivan de la autenticación IMS AKA:

1. UE realiza autenticación AKA con S-CSCF/HSS
2. HSS genera CK (128 bits) e IK (128 bits)
3. S-CSCF entrega CK/IK a P-CSCF a través de la interfaz interna
4. P-CSCF utiliza CK/IK para establecer asociaciones de seguridad IPsec con UE
5. CK utilizado para cifrado ESP
6. IK utilizado para autenticación ESP

## **Parámetros de Asociación de Seguridad:**

- **Vida Útil:** Vinculada a la expiración del registro SIP (típicamente 599 segundos)
- **Protección contra Repetición:** Habilitada (ventana anti-repetición)
- **Números de Secuencia:** 32 bits o 64 bits (ESN - Números de Secuencia Extendidos)
- **Perfect Forward Secrecy:** No aplicable (claves de AKA, no Diffie-Hellman)

## **Implementación:**

La capacidad IPsec de P-CSCF:

- Interactúa con la pila IPsec del kernel de Linux (marco XFRM)
- Configura políticas de seguridad y asociaciones a través de la API del kernel
- Asignación y gestión de SPI (Índice de Parámetro de Seguridad)
- Asignación de puertos para tráfico protegido

### **2.2.2 Capacidades de Configuración IPsec**

#### **Selección de Conjuntos de Cifrado:**

El P-CSCF puede configurarse para preferir conjuntos de cifrado específicos:

Preferidos (seguridad fuerte):

- ESP con AES-256-GCM y HMAC-SHA256
- ESP con AES-256-CBC y HMAC-SHA256

Soportados (compatibilidad):

- ESP con AES-128-CBC y HMAC-SHA1
- ESP con 3DES-CBC y HMAC-SHA1 (heredado)

#### **Gestión de Claves:**

- IKE (Intercambio de Claves de Internet) NO se utiliza
- Claves proporcionadas a través de IMS AKA (CK/IK de HSS)
- Configuración manual de asociación de seguridad a través de XFRM del kernel
- Destrucción automática de SA al expirar el registro

## **Ciclo de Vida del Túnel:**

1. UE se registra → autenticación AKA → CK/IK generados
2. P-CSCF recibe CK/IK de S-CSCF
3. P-CSCF asigna par de SPI (SPI del cliente, SPI del servidor)
4. P-CSCF asigna par de puertos (puerto del cliente, puerto del servidor)
5. P-CSCF configura SAs IPsec del kernel utilizando CK/IK
6. P-CSCF envía parámetros IPsec a UE en 200 OK (encabezado Security-Server)
7. UE configura SAs IPsec con los mismos parámetros
8. Todo el tráfico SIP subsiguiente fluye a través de túneles ESP
9. Al expirar el registro o al desregistro: SAs eliminadas, recursos liberados

## **2.3 Cifrado TLS (SIP y Diameter)**

### **2.3.1 TLS para SIP (SIPS)**

#### **Versiones TLS Soportadas:**

- **TLS 1.2** (RFC 5246) - Soportado
- **TLS 1.3** (RFC 8446) - Soportado (si hay soporte de kernel/biblioteca)
- **TLS 1.0/1.1** - Obsoleto (deshabilitado por defecto)
- **SSL 2.0/3.0** - NO SOPORTADO (vulnerabilidades conocidas)

#### **Implementación de TLS:**

el sistema utiliza OpenSSL o LibreSSL:

- Bibliotecas TLS estándar de la industria
- Implementaciones validadas criptográficamente
- Actualizaciones de seguridad regulares

#### **Conjuntos de Cifrado Soportados:**

##### **TLS 1.3 (Preferido):**

- TLS\_AES\_256\_GCM\_SHA384
- TLS\_AES\_128\_GCM\_SHA256
- TLS\_CHACHA20\_POLY1305\_SHA256

##### **TLS 1.2 (Soportado):**

- ECDHE-RSA-AES256-GCM-SHA384 (Perfect Forward Secrecy)
- ECDHE-RSA-AES128-GCM-SHA256 (Perfect Forward Secrecy)
- ECDHE-ECDSA-AES256-GCM-SHA384 (Perfect Forward Secrecy)
- DHE-RSA-AES256-GCM-SHA384 (Perfect Forward Secrecy)
- DHE-RSA-AES128-GCM-SHA256 (Perfect Forward Secrecy)

#### **Cifrados débiles deshabilitados:**

- Sin RC4
- Sin MD5
- Sin cifrado NULL

- Sin cifrados de grado EXPORT
- Sin DES/3DES (obsoleto)

### **Soporte de Certificados:**

- **Certificados X.509** (formato estándar)
- **Claves RSA**: mínimo de 2048 bits, recomendado 4096 bits
- **Claves ECDSA**: curvas P-256, P-384, P-521 soportadas
- **Validación de cadena de certificados**
- **Comprobación de CRL (Lista de Revocación de Certificados)** (opcional)
- **OCSP (Protocolo de Estado de Certificado en Línea)** (opcional)

### **Características TLS:**

- **Perfect Forward Secrecy (PFS)**: A través de intercambio de claves ECDHE/DHE
- **Indicación de Nombre de Servidor (SNI)**: Soportado
- **Reanudación de Sesión TLS**: Soportada (optimización de rendimiento)
- **Autenticación de Certificado del Cliente**: Soportada (mutual TLS)

### **SIP sobre TLS (SIPS):**

- Transporte: TCP con cifrado TLS
- Puerto: 5061 (puerto estándar SIPS)
- Usado para comunicación inter-CSCF (opcional)
- Usado para conexiones de red de confianza

### **2.3.2 TLS para Diameter**

#### **Capacidades Diameter:**

El sistema soporta:

- **Diameter sobre SCTP** (preferido por fiabilidad)
- **Diameter sobre TCP con TLS**
- **Puerto**: 3868 (puerto estándar Diameter)

#### **Casos de Uso:**

- **Interfaz Cx**: S-CSCF/I-CSCF a HSS (datos de suscriptor, autenticación)
- **Interfaz Rx**: P-CSCF a PCRF (política de QoS)
- **Interfaz Ro**: S-CSCF a OCS (cobro en línea - si está habilitado)

#### **Configuración TLS para Diameter:**

Los mismos conjuntos de cifrado que SIP

- TLS 1.2/1.3
- Intercambio de claves ECDHE/DHE (PFS)
- Cifrado AES-GCM
- Autenticación SHA256/SHA384

## **Autenticación Basada en Certificados:**

- Los pares Diameter se autentican a través de certificados TLS
- Mutual TLS (certificados tanto del cliente como del servidor)
- Validación de FQDN (Nombre de Dominio Totalmente Calificado) en certificados
- Validación de cadena CA de confianza

## **2.4 Criptografía de Autenticación**

### **2.4.1 Funciones Criptográficas IMS AKA**

#### **Algoritmo 3GPP AKA (MILENAGE):**

Utilizado para generar vectores de autenticación (RAND, AUTN, XRES, CK, IK):

#### **Funciones Criptográficas:**

- **f1:** Función de autenticación de mensajes (calcular MAC-A y MAC-S)
- **f2:** Función de respuesta (calcular RES a partir de RAND y K)
- **f3:** Derivación de clave de cifrado (calcular CK)
- **f4:** Derivación de clave de integridad (calcular IK)
- **f5:** Función de clave de anonimato (calcular AK para privacidad de IMSI)

#### **Material de Clave:**

- **K:** Clave permanente de suscriptor de 128 bits (almacenada en ISIM y HSS)
- **OPc:** Clave variante del operador (derivada de K y OP)
- **RAND:** Desafío aleatorio de 128 bits
- **SQN:** Número de secuencia de 48 bits (protección contra repetición)

#### **Secuencia AKA:**

1. HSS genera RAND (aleatorio criptográficamente)
2. HSS calcula  $\text{MAC-A} = f1(K, \text{RAND}, \text{SQN}, \text{AMF})$
3. HSS calcula  $\text{AUTN} = (\text{SQN} \oplus \text{AK}) \parallel \text{AMF} \parallel \text{MAC-A}$
4. HSS calcula  $\text{XRES} = f2(K, \text{RAND})$
5. HSS calcula  $\text{CK} = f3(K, \text{RAND})$
6. HSS calcula  $\text{IK} = f4(K, \text{RAND})$
7. HSS envía  $\{\text{RAND}, \text{AUTN}, \text{XRES}, \text{CK}, \text{IK}\}$  a S-CSCF
8. S-CSCF desafía a UE con RAND y AUTN
9. UE calcula  $\text{RES} = f2(K, \text{RAND})$  usando ISIM
10. UE envía RES a S-CSCF
11. S-CSCF compara RES con XRES (validación de autenticación)

#### **Propiedades de Seguridad:**

- **Autenticación Mutua:** UE verifica HSS a través de AUTN, HSS verifica UE a través de RES
- **Frescura de Clave:** RAND es aleatorio, SQN previene repetición
- **Derivación de Clave:** CK e IK derivados de la clave compartida K

## 2.4.2 Autenticación Digest HTTP

Para autenticación no IMS (si se utiliza):

**Algoritmo:** MD5 (RFC 2617)

- **Función Hash:** MD5 (salida de 128 bits)
- **Desafío-Respuesta:** Basado en nonce
- **Protección contra Repetición:**Nonce con marca de tiempo

**Nota:** HTTP Digest con MD5 se considera débil. IMS AKA es preferido fuertemente.

## 2.5 Hashing e Integridad

### 2.5.1 Funciones Hash Disponibles

el sistema puede usar (a través de OpenSSL/crypto del kernel):

- **SHA-256:** salida de 256 bits, recomendado
- **SHA-384:** salida de 384 bits
- **SHA-512:** salida de 512 bits
- **SHA-1:** salida de 160 bits, obsoleto para uso de seguridad
- **MD5:** salida de 128 bits, obsoleto para uso de seguridad

**Uso:**

- Construcciones HMAC para IPsec/TLS
- Verificación de integridad de datos
- Generación de nonce
- Detección de duplicados (hashing de Call-ID)

### 2.5.2 Integridad del Mensaje

**Integridad del Mensaje SIP:**

- **IPsec ESP:** HMAC-SHA256 para SIP autenticado sobre IPsec
- **TLS:** Autenticación de mensajes a través de TLS MAC
- **Digest SIP:** Integridad del encabezado de autenticación

**Integridad del Mensaje Diameter:**

- **TLS:** Diameter sobre TLS proporciona autenticación de mensajes
- **HMAC:** Los mensajes Diameter pueden incluir AVPs HMAC para integridad

## 2.6 Generación de Números Aleatorios

**Generación de Números Aleatorios Criptográficamente Segura:**

el sistema se basa en:

- **Linux kernel /dev/urandom:** PRNG seguro criptográficamente

- **OpenSSL RAND\_bytes()**: CSPRNG (Generador de Números Pseudo-Aleatorios Criptográficamente Seguro)

**Uso:**

- Asignación de SPI (valor inicial aleatorizado)
- Generación de Call-ID
- Generación de parámetros de rama
- Generación de nonce para autenticación
- Generación de ID de sesión

## 2.7 Gestión de Claves

### 2.7.1 Gestión de Certificados TLS

**Almacenamiento de Certificados:**

- Almacenamiento en el sistema de archivos con permisos restringidos (0600)
- Ubicado en: /etc/system/tls/
- Formato PEM para certificados y claves

**Generación de Certificados:**

```
# Generar clave privada RSA de 4096 bits
openssl genrsa -out system-key.pem 4096

# Generar CSR (Solicitud de Firma de Certificado)
openssl req -new -key system-key.pem -out system.csr \
  -subj "/C=FR/ST=IDF/L=Paris/0=Omnitouch/
CN=scscf.ims.mnc001.mcc001.3gppnetwork.org"

# Certificado autofirmado (desarrollo/pruebas)
openssl x509 -req -days 365 -in system.csr \
  -signkey system-key.pem -out system-cert.pem

# Producción: Enviar CSR a CA de confianza
```

**Rotación de Certificados:**

- Renovación anual de certificados recomendada
- Reinicio del servicio de manera controlada para cargar nuevos certificados
- No se requiere tiempo de inactividad

### 2.7.2 Gestión de Claves IPsec

**Derivación de Claves:**

- CK (Clave de Cifrado) e IK (Clave de Integridad) de IMS AKA
- Claves de 128 bits de HSS
- Entregadas de forma segura a través de Diameter Cx (sobre TLS)

### **Vida Útil de la Clave:**

- Vinculada a la expiración del registro SIP (típicamente 599 segundos)
- Re-keying en la actualización del registro
- Destrucción automática de claves al des registrarse

### **Almacenamiento de Claves:**

- Efímeras (solo en memoria durante el registro activo)
- Instaladas en la pila IPsec del kernel
- Sin almacenamiento persistente de claves
- Claves descartadas cuando se elimina SA

## **2.8 Resistencia al Criptoanálisis**

### **2.8.1 Selección de Algoritmos**

#### **Defensa Contra Criptoanálisis:**

- **Sin algoritmos personalizados:** Solo algoritmos estándar de la industria, revisados por pares
- **Tamaños de clave fuertes:** AES-256, RSA-4096, SHA-256
- **Cifrado autenticado:** AES-GCM (AEAD - Cifrado Autenticado con Datos Asociados)
- **Perfect Forward Secrecy:** ECDHE/DHE en TLS
- **Actualizaciones regulares:** Parches de seguridad de OpenSSL/LibreSSL aplicados

#### **Algoritmos Obsoletos Deshabilitados:**

- MD5 (colisiones de hash)
- RC4 (debilidades del cifrado de flujo)
- DES/3DES (tamaño de bloque pequeño, longitud de clave)
- SSL 2.0/3.0 (vulnerabilidades de protocolo)
- TLS 1.0/1.1 (ataques BEAST, POODLE)

### **2.8.2 Mitigación de Ataques de Canal Lateral**

#### **Resistencia a Ataques de Tiempo:**

- Comparación en tiempo constante para respuestas de autenticación
- Sin filtraciones de tiempo en operaciones criptográficas (a través de OpenSSL)

#### **Protección de Memoria:**

- Aislamiento de la pila IPsec del kernel
- Aislamiento de memoria de procesos
- Sin intercambio para datos sensibles (si está configurado)

## **2.9 Cumplimiento y Normas**

### **Cumplimiento de Normas Criptográficas:**

- **NIST SP 800-52:** Directrices TLS
- **NIST SP 800-131A:** Transiciones de algoritmos criptográficos
- **RFC 7525:** Recomendaciones TLS
- **ETSI TS 133 203:** Seguridad de acceso 3GPP (IMS AKA)
- **ETSI TS 133 210:** Seguridad de capa de red IP (IPsec)
- **3GPP TS 33.203:** Seguridad de acceso para IMS
- **3GPP TS 33.210:** Seguridad de dominio de red

### **Regulaciones Francesas sobre Criptografía:**

- Sin criptografía restringida a la exportación (todos los algoritmos estándar)
- Medios criptográficos estándar (sin puertas traseras gubernamentales)
- Certificación de productos criptográficos ANSSI (si es necesario)



# IMS CSCF Métricas de Referencia

Este documento proporciona una referencia completa para todas las métricas exportadas por los componentes P-CSCF, I-CSCF y S-CSCF.

## Acceso a Métricas

Todos los componentes CSCF exponen métricas de Prometheus en el puerto 9090:

`http://<host>:9090/metrics`

Cada host CSCF (P-CSCF, I-CSCF, S-CSCF) exporta sus propias métricas. Configure su servidor Prometheus para recopilar datos de todos los hosts para una cobertura de monitoreo completa.

### Ejemplo de Configuración de Prometheus:

```
scrape_configs:
  - job_name: 'cscf_pcscf'
    static_configs:
      - targets: ['pcscf1.example.com:9090',
      'pcscf2.example.com:9090']

    - job_name: 'cscf_icscf'
      static_configs:
        - targets: ['icscf1.example.com:9090']

    - job_name: 'cscf_scscf'
      static_configs:
        - targets: ['scscf1.example.com:9090',
        'scscf2.example.com:9090']
```

Para obtener orientación operativa sobre monitoreo y alertas, consulte:

- [Guía de Operaciones de la Interfaz Web](#)
- [Guía de Capacidad y Dimensionamiento](#)

## Monitoreo a Través del Panel de Control

El Panel de Control de OmniCall CSCF proporciona visibilidad en tiempo real del estado operativo que genera estas métricas. Mientras que las métricas se exportan a través de Prometheus para análisis históricos y alertas, el panel de control muestra el estado actual de registros, diálogos y pares de Diameter.

## Gestión de S-CSCF

Vea los registros activos y los datos de ubicación del usuario:

El conteo de registros visible en la interfaz corresponde a métricas como `ims_usrloc_scscf_active_impus` y `ims_usrloc_scscf_active_contacts`.

## Monitoreo de Pares de Diameter

Monitoree el estado de los pares de Diameter y las longitudes de cola:

La longitud de la cola que se muestra aquí corresponde a la métrica `cdp_queuelength`. El estado del par "I\_Open" indica conexiones saludables.

Cada par muestra las aplicaciones de Diameter soportadas. Por ejemplo:

- **16777216:10415 (Cx/Dx)** - Utilizado por I-CSCF y S-CSCF para comunicación HSS (UAR, LIR, MAR, SAR)
- **16777236:10415 (Rx)** - Utilizado por P-CSCF para políticas de QoS de PCRF
- **4 (Ro)** - Utilizado por S-CSCF para carga en línea

Estos corresponden a métricas como `ims_icscf_uar_*`, `ims_icscf_lir_*`, `ims_auth_mar_*`, `ims_register_scscf_sar_*`, y `ims_qos_*`.

---

## Métricas de P-CSCF

### Métricas CDP (Diameter)

Nombre de Métrica	Significado
<code>cdp_average_response_time</code>	Tiempo de respuesta promedio para solicitudes de Diameter en milisegundos (calculado como <code>replies_response_time / replies_received</code> )
<code>cdp_queuelength</code>	Longitud actual de la cola de tareas del trabajador de Diameter
<code>cdp_replies_received</code>	Número total de respuestas de Diameter recibidas
<code>cdp_replies_response_time</code>	Tiempo total gastado esperando respuestas de Diameter en milisegundos
<code>cdp_timeout</code>	Número de eventos de tiempo de espera en solicitudes de Diameter

# Estadísticas SIP Básicas

## Contadores de Solicitudes

Nombre de Métrica	Significado
core_rcv_requests	Número total de solicitudes SIP recibidas
core_rcv_requests_ack	Número de solicitudes ACK recibidas
core_rcv_requests_bye	Número de solicitudes BYE recibidas
core_rcv_requests_cancel	Número de solicitudes CANCEL recibidas
core_rcv_requests_info	Número de solicitudes INFO recibidas
core_rcv_requests_invite	Número de solicitudes INVITE recibidas
core_rcv_requests_message	Número de solicitudes MESSAGE recibidas
core_rcv_requests_notify	Número de solicitudes NOTIFY recibidas
core_rcv_requests_options	Número de solicitudes OPTIONS recibidas
core_rcv_requests_prack	Número de solicitudes PRACK recibidas
core_rcv_requests_publish	Número de solicitudes PUBLISH recibidas
core_rcv_requests_refer	Número de solicitudes REFER recibidas
core_rcv_requests_register	Número de solicitudes REGISTER recibidas
core_rcv_requests_subscribe	Número de solicitudes SUBSCRIBE recibidas
core_rcv_requests_update	Número de solicitudes UPDATE recibidas

## Contadores de Respuestas (General)

Nombre de Métrica	Significado
core_rcv_replies	Número total de respuestas SIP recibidas
core_rcv_replies_18x	Número de respuestas provisionales 180/181/183/186/187/189 recibidas
core_rcv_replies_1xx	Número de respuestas 1xx (provisionales) recibidas
core_rcv_replies_2xx	Número de respuestas 2xx (éxito) recibidas
core_rcv_replies_3xx	Número de respuestas 3xx (redirección) recibidas
core_rcv_replies_4xx	Número de respuestas 4xx (error del cliente) recibidas
core_rcv_replies_5xx	Número de respuestas 5xx (error del servidor) recibidas
core_rcv_replies_6xx	Número de respuestas 6xx (fallo global) recibidas

## Contadores de Respuestas por Método (1xx)

Nombre de Métrica	Significado
core_rcv_replies_1xx_bye	Número de respuestas 1xx a solicitudes BYE
core_rcv_replies_1xx_cancel	Número de respuestas 1xx a solicitudes CANCEL
core_rcv_replies_1xx_invite	Número de respuestas 1xx a solicitudes INVITE
core_rcv_replies_1xx_message	Número de respuestas 1xx a solicitudes MESSAGE
core_rcv_replies_1xx_prack	Número de respuestas 1xx a solicitudes PRACK

<b>Nombre de Métrica</b>	<b>Significado</b>
core_rcv_replies_1xx_refer	Número de respuestas 1xx a solicitudes REFER
core_rcv_replies_1xx_reg	Número de respuestas 1xx a solicitudes REGISTER
core_rcv_replies_1xx_update	Número de respuestas 1xx a solicitudes UPDATE

## Contadores de Respuestas por Método (2xx)

<b>Nombre de Métrica</b>	<b>Significado</b>
core_rcv_replies_2xx_bye	Número de respuestas 2xx (éxito) a solicitudes BYE
core_rcv_replies_2xx_cancel	Número de respuestas 2xx (éxito) a solicitudes CANCEL
core_rcv_replies_2xx_invite	Número de respuestas 2xx (éxito) a solicitudes INVITE
core_rcv_replies_2xx_message	Número de respuestas 2xx (éxito) a solicitudes MESSAGE
core_rcv_replies_2xx_prack	Número de respuestas 2xx (éxito) a solicitudes PRACK
core_rcv_replies_2xx_refer	Número de respuestas 2xx (éxito) a solicitudes REFER
core_rcv_replies_2xx_reg	Número de respuestas 2xx (éxito) a solicitudes REGISTER
core_rcv_replies_2xx_update	Número de respuestas 2xx (éxito) a solicitudes UPDATE

## Contadores de Respuestas por Método (3xx)

<b>Nombre de Métrica</b>	<b>Significado</b>
core_rcv_replies_3xx_bye	Número de respuestas 3xx (redirección) a solicitudes BYE
core_rcv_replies_3xx_cancel	Número de respuestas 3xx (redirección) a solicitudes CANCEL
core_rcv_replies_3xx_invite	Número de respuestas 3xx (redirección) a solicitudes INVITE
core_rcv_replies_3xx_message	Número de respuestas 3xx (redirección) a solicitudes MESSAGE
core_rcv_replies_3xx_prack	Número de respuestas 3xx (redirección) a solicitudes PRACK
core_rcv_replies_3xx_refer	Número de respuestas 3xx (redirección) a solicitudes REFER
core_rcv_replies_3xx_reg	Número de respuestas 3xx (redirección) a solicitudes REGISTER
core_rcv_replies_3xx_update	Número de respuestas 3xx (redirección) a

<b>Nombre de Métrica</b>	<b>Significado</b>
	solicitudes UPDATE

## Contadores de Respuestas por Método (4xx)

<b>Nombre de Métrica</b>	<b>Significado</b>
core_rcv_replies_4xx_bye	Número de respuestas 4xx (error del cliente) a solicitudes BYE
core_rcv_replies_4xx_cancel	Número de respuestas 4xx (error del cliente) a solicitudes CANCEL
core_rcv_replies_4xx_invite	Número de respuestas 4xx (error del cliente) a solicitudes INVITE
core_rcv_replies_4xx_message	Número de respuestas 4xx (error del cliente) a solicitudes MESSAGE
core_rcv_replies_4xx_prack	Número de respuestas 4xx (error del cliente) a solicitudes PRACK
core_rcv_replies_4xx_refer	Número de respuestas 4xx (error del cliente) a solicitudes REFER
core_rcv_replies_4xx_reg	Número de respuestas 4xx (error del cliente) a solicitudes REGISTER
core_rcv_replies_4xx_update	Número de respuestas 4xx (error del cliente) a solicitudes UPDATE

## Contadores de Respuestas por Método (5xx)

<b>Nombre de Métrica</b>	<b>Significado</b>
core_rcv_replies_5xx_bye	Número de respuestas 5xx (error del servidor) a solicitudes BYE
core_rcv_replies_5xx_cancel	Número de respuestas 5xx (error del servidor) a solicitudes CANCEL
core_rcv_replies_5xx_invite	Número de respuestas 5xx (error del servidor) a solicitudes INVITE
core_rcv_replies_5xx_message	Número de respuestas 5xx (error del servidor) a solicitudes MESSAGE
core_rcv_replies_5xx_prack	Número de respuestas 5xx (error del servidor) a solicitudes PRACK
core_rcv_replies_5xx_refer	Número de respuestas 5xx (error del servidor) a solicitudes REFER
core_rcv_replies_5xx_reg	Número de respuestas 5xx (error del servidor) a solicitudes REGISTER
core_rcv_replies_5xx_update	Número de respuestas 5xx (error del servidor) a solicitudes UPDATE

## Contadores de Respuestas por Método (6xx)

Nombre de Métrica	Significado
core_rcv_replies_6xx_bye	Número de respuestas 6xx (fallo global) a solicitudes BYE
core_rcv_replies_6xx_cancel	Número de respuestas 6xx (fallo global) a solicitudes CANCEL
core_rcv_replies_6xx_invite	Número de respuestas 6xx (fallo global) a solicitudes INVITE
core_rcv_replies_6xx_message	Número de respuestas 6xx (fallo global) a solicitudes MESSAGE
core_rcv_replies_6xx_prack	Número de respuestas 6xx (fallo global) a solicitudes PRACK
core_rcv_replies_6xx_refer	Número de respuestas 6xx (fallo global) a solicitudes REFER
core_rcv_replies_6xx_reg	Número de respuestas 6xx (fallo global) a solicitudes REGISTER
core_rcv_replies_6xx_update	Número de respuestas 6xx (fallo global) a solicitudes UPDATE

## Contadores de Códigos de Estado Específicos

Nombre de Métrica	Significado
core_rcv_replies_400	Número de respuestas 400 Bad Request recibidas
core_rcv_replies_401	Número de respuestas 401 Unauthorized recibidas
core_rcv_replies_402	Número de respuestas 402 Payment Required recibidas
core_rcv_replies_403	Número de respuestas 403 Forbidden recibidas
core_rcv_replies_404	Número de respuestas 404 Not Found recibidas
core_rcv_replies_405	Número de respuestas 405 Method Not Allowed recibidas
core_rcv_replies_406	Número de respuestas 406 Not Acceptable recibidas
core_rcv_replies_407	Número de respuestas 407 Proxy Authentication Required recibidas
core_rcv_replies_408	Número de respuestas 408 Request Timeout recibidas
core_rcv_replies_409	Número de respuestas 409 Conflict recibidas
core_rcv_replies_410	Número de respuestas 410 Gone recibidas
core_rcv_replies_411	Número de respuestas 411 Length Required recibidas
core_rcv_replies_413	Número de respuestas 413 Request Entity Too Large recibidas
core_rcv_replies_414	Número de respuestas 414 Request-URI Too Long recibidas
core_rcv_replies_415	Número de respuestas 415 Unsupported Media Type recibidas
core_rcv_replies_420	Número de respuestas 420 Bad Extension recibidas
core_rcv_replies_480	Número de respuestas 480 Temporarily Unavailable recibidas

<b>Nombre de Métrica</b>	<b>Significado</b>
core_rcv_replies_481	Número de respuestas 481 Call/Transaction Does Not Exist recibidas
core_rcv_replies_482	Número de respuestas 482 Loop Detected recibidas
core_rcv_replies_483	Número de respuestas 483 Too Many Hops recibidas
core_rcv_replies_484	Número de respuestas 484 Address Incomplete recibidas
core_rcv_replies_485	Número de respuestas 485 Ambiguous recibidas
core_rcv_replies_486	Número de respuestas 486 Busy Here recibidas
core_rcv_replies_487	Número de respuestas 487 Request Terminated recibidas
core_rcv_replies_488	Número de respuestas 488 Not Acceptable Here recibidas
core_rcv_replies_489	Número de respuestas 489 Bad Event recibidas
core_rcv_replies_491	Número de respuestas 491 Request Pending recibidas
core_rcv_replies_493	Número de respuestas 493 Undecipherable recibidas

## Estadísticas de Reenvío y Errores

<b>Nombre de Métrica</b>	<b>Significado</b>
core_fwd_replies	Número de respuestas SIP reenviadas
core_fwd_requests	No ♦ Número de solicitudes SIP reenviadas
core_drop_replies	Número de respuestas SIP descartadas
core_drop_requests	Número de solicitudes SIP descartadas
core_err_replies	Número de respuestas de error
core_err_requests	Número de solicitudes de error
core_bad_URIIs_rcvd	Número de mensajes con URIs malformados recibidos
core_bad_msg_hdr	Número de mensajes con encabezados malos/ malformados
core_unsupported_methods	Número de solicitudes con métodos SIP no soportados

## Seguimiento de Diálogos

<b>Nombre de Métrica</b>	<b>Significado</b>
dialog_ng_active	Número de diálogos actualmente activos (respondidos/ confirmados)
dialog_ng_early	Número de diálogos tempranos (sonando/estado provisional)
dialog_ng_expired	Número de diálogos que han expirado o han sido terminados forzosamente
dialog_ng_processed	Número total de diálogos procesados desde el inicio

## Estadísticas DNS

Nombre de Métrica	Significado
dns_failed_dns_request	Número de consultas DNS fallidas
dns_slow_dns_request	Número de consultas DNS lentas (excediendo el umbral)

## IMS IPSec P-CSCF

Nombre de Métrica	Significado
ims_ipsec_pcscf_spi_free	Número de valores SPI (Índice de Parámetro de Seguridad) libres disponibles para asignación
ims_ipsec_pcscf_spi_total	Capacidad total de SPI configurada para el sistema
ims_ipsec_pcscf_spi_used	Número de valores SPI actualmente asignados/utilizados
ims_ipsec_pcscf_spi_utilization_pct	Porcentaje de utilización del grupo de SPI
ims_ipsec_pcscf_worker_cache_size	Tamaño de la caché IPSec del proceso trabajador

## IMS QoS (Interfaz Rx)

### Métricas de Registro AAR

Nombre de Métrica	Significado
ims_qos_active_registration_rx_sessions	Número de sesiones de registro Rx actualmente activas
ims_qos_registration_aars	Número total de mensajes AAR (Solicitud de Autorización-Autenticación) de registro enviados
ims_qos_successful_registration_aars	Número de transacciones AAR de registro exitosas
ims_qos_failed_registration_aars	Número de transacciones AAR de registro fallidas
ims_qos_registration_aar_avg_response_time	Tiempo de respuesta promedio para mensajes AAR de registro en milisegundos
ims_qos_registration_aar_response_time	Tiempo total de respuesta para todos los mensajes AAR de registro en milisegundos
ims_qos_registration_aar_replies_received	Número total de respuestas AAR de registro recibidas

<b>Nombre de Métrica</b>	<b>Significado</b>
ims_qos_registration_aar_timeouts	Número de tiempos de espera de solicitudes AAR de registro

## Métricas de AAR de Medios

<b>Nombre de Métrica</b>	<b>Significado</b>
ims_qos_active_media_rx_sessions	Número de sesiones de medios Rx actualmente activas
ims_qos_media_rx_sessions	Número total de sesiones de medios Rx creadas
ims_qos_media_aars	Número total de mensajes AAR de medios enviados
ims_qos_successful_media_aars	Número de transacciones AAR de medios exitosas
ims_qos_failed_media_aars	Número de transacciones AAR de medios fallidas
ims_qos_media_aar_avg_response_time	Tiempo de respuesta promedio para mensajes AAR de medios en milisegundos
ims_qos_media_aar_response_time	Tiempo total de respuesta para todos los mensajes AAR de medios en milisegundos
ims_qos_media_aar_replies_received	Número total de respuestas AAR de medios recibidas
ims_qos_media_aar_timeouts	Número de tiempos de espera de solicitudes AAR de medios

## Métricas ASR

<b>Nombre de Métrica</b>	<b>Significado</b>
ims_qos_asrs	Número total de mensajes ASR (Solicitud de Abort-Session) recibidos de PCRF

## IMS USRLOC P-CSCF

<b>Nombre de Métrica</b>	<b>Significado</b>
ims_usrloc_pcscf_expired_contacts	Número de enlaces de contacto expirados
ims_usrloc_pcscf_registered_contacts	Número de enlaces de contacto actualmente registrados
ims_usrloc_pcscf_registered_impus	Número de IMPUs (Identidades Públicas IMS) actualmente registrados

## Base de Datos MySQL

Nombre de Métrica	Significado
mysql_driver_errors	Número de errores de conexión/controlador de MySQL

## Módulo Pike (Bloqueo de IP)

Nombre de Métrica	Significado
pike_blocked_ips	Número de direcciones IP actualmente bloqueadas (detección de inundaciones)

## Módulo Registrador

Nombre de Métrica	Significado
registrar_accepted_regs	Número de solicitudes REGISTER aceptadas (módulo registrador heredado)
registrar_rejected_regs	Número de solicitudes REGISTER rechazadas (módulo registrador heredado)
registrar_default_expire	Tiempo de expiración predeterminado para registros en segundos
registrar_default_expires_range	Configuración del rango de expiración predeterminado
registrar_expires_range	Rango de expiración configurado
registrar_max_contacts	Número máximo de contactos permitidos por AOR
registrar_max_expires	Tiempo máximo de expiración permitido en segundos

## Estadísticas de Scripts

Nombre de Métrica	Significado
script_register_failed	Número de intentos de registro que fallaron en la lógica del script de enrutamiento
script_register_success	Número de registros exitosos procesados por el script de enrutamiento
script_register_time	Tiempo total gastado procesando registros en el script de enrutamiento (milisegundos)

## Transporte SCTP

Nombre de Métrica	Significado
sctp_assoc_shutdown	Número de cierres de asociación SCTP iniciados localmente
sctp_comm_lost	Número de asociaciones SCTP perdidas

<b>Nombre de Métrica</b>	<b>Significado</b>
sctp_connect_failed	debido a fallos de comunicación
sctp_current_opened_connections	Número de intentos de asociación SCTP salientes fallidos
sctp_current_tracked_connections	Número de asociaciones SCTP actualmente abiertas
sctp_established	Número de asociaciones SCTP actualmente rastreadas
sctp_local_reject	Número total de asociaciones SCTP establecidas
sctp_remote_shutdown	Número de asociaciones SCTP entrantes rechazadas localmente
sctp_send_failed	Número de cierres de asociación SCTP iniciados por el par
sctp_send_force_retry	Número de operaciones de envío SCTP que fallaron
sctp_sendq_full	Número de reintentos forzados en envíos SCTP fallidos
	Número de intentos de envío que fallaron debido a una cola de envío llena

## Memoria Compartida

<b>Nombre de Métrica</b>	<b>Significado</b>
shmem_fragments	Número de fragmentos en el grupo de memoria compartida (indica fragmentación)
shmem_free_size	Cantidad de memoria compartida libre en bytes
shmem_max_used_size	Tamaño máximo de memoria compartida utilizada desde el inicio en bytes
shmem_real_used_size	Memoria compartida realmente utilizada incluyendo sobrecarga del asignador en bytes
shmem_total_size	Tamaño total del grupo de memoria compartida en bytes
shmem_used_size	Memoria compartida actualmente utilizada (solo datos de usuario) en bytes

## Módulo SL (Sin Estado)

### Contadores de Respuestas Sin Estado por Clase

<b>Nombre de Métrica</b>	<b>Significado</b>
sl_1xx_replies	Número de respuestas sin estado 1xx enviadas
sl_2xx_replies	Número de respuestas sin estado 2xx enviadas
sl_3xx_replies	Número de respuestas sin estado 3xx enviadas
sl_4xx_replies	Número de respuestas sin estado 4xx enviadas
sl_5xx_replies	Número de respuestas sin estado 5xx enviadas

<b>Nombre de Métrica</b>	<b>Significado</b>
sl_6xx_replies	Número de respuestas sin estado 6xx enviadas
sl_xxx_replies	Número de otras respuestas sin estado enviadas

## Contadores de Respuestas Sin Estado Específicos

<b>Nombre de Métrica</b>	<b>Significado</b>
sl_200_replies	Número de respuestas sin estado 200 OK enviadas
sl_202_replies	Número de respuestas sin estado 202 Accepted enviadas
sl_300_replies	Número de respuestas sin estado 300 Multiple Choices enviadas
sl_301_replies	Número de respuestas sin estado 301 Moved Permanently enviadas
sl_302_replies	Número de respuestas sin estado 302 Moved Temporarily enviadas
sl_400_replies	Número de respuestas sin estado 400 Bad Request enviadas
sl_401_replies	Número de respuestas sin estado 401 Unauthorized enviadas
sl_403_replies	Número de respuestas sin estado 403 Forbidden enviadas
sl_404_replies	Número de respuestas sin estado 404 Not Found enviadas
sl_407_replies	Número de respuestas sin estado 407 Proxy Authentication Required enviadas
sl_408_replies	Número de respuestas sin estado 408 Request Timeout enviadas
sl_483_replies	Número de respuestas sin estado 483 Too Many Hops enviadas
sl_500_replies	Número de respuestas sin estado 500 Server Internal Error enviadas

## Estadísticas Generales Sin Estado

<b>Nombre de Métrica</b>	<b>Significado</b>
sl_sent_replies	Número total de respuestas sin estado enviadas
sl_sent_err_replies	Número de respuestas de error sin estado enviadas
sl_received_ACKs	Número de mensajes ACK recibidos para transacciones sin estado
sl_failures	Número de fallos en el envío de respuestas sin estado

## Transporte TCP

<b>Nombre de Métrica</b>	<b>Significado</b>
tcp_con_reset	Número de conexiones TCP restablecidas (RST recibido en conexión establecida)
tcp_con_timeout	Número de conexiones TCP cerradas debido a tiempo de espera inactivo

<b>Nombre de Métrica</b>	<b>Significado</b>
tcp_connect_failed	Número de intentos de conexión TCP salientes fallidos
tcp_connect_success	Número de conexiones TCP salientes exitosas
tcp_current_opened_connections	Número de conexiones TCP actualmente abiertas
tcp_current_write_queue_size	Tamaño total actual de las colas de escritura TCP en todas las conexiones
tcp_established	Número total de conexiones TCP establecidas (tanto entrantes como salientes)
tcp_local_reject	Número de conexiones TCP entrantes rechazadas localmente
tcp_passive_open	Número de conexiones TCP entrantes aceptadas
tcp_send_timeout	Número de operaciones de envío TCP que agotaron el tiempo (modo asíncrono)
tcp_sendq_full	Número de intentos de envío que fallaron porque la cola de envío estaba llena

## Módulo TM/TMX (Transacción)

### Contadores de Tipos de Transacción

<b>Nombre de Métrica</b>	<b>Significado</b>
tmx_UAC_transactions	Número de transacciones UAC (cliente) creadas
tmx_UAS_transactions	Número de transacciones UAS (servidor) creadas
tmx_active_transactions	Número de transacciones actualmente activas
tmx_inuse_transactions	Número de transacciones actualmente en uso

### Finalización de Transacciones por Estado

<b>Nombre de Métrica</b>	<b>Significado</b>
tmx_2xx_transactions	Número de transacciones completadas con respuesta 2xx
tmx_3xx_transactions	Número de transacciones completadas con respuesta 3xx
tmx_4xx_transactions	Número de transacciones completadas con respuesta 4xx
tmx_5xx_transactions	Número de transacciones completadas con respuesta 5xx
tmx_6xx_transactions	Número de transacciones completadas con respuesta 6xx

### Estadísticas de Respuestas de Transacción

<b>Nombre de Métrica</b>	<b>Significado</b>
tmx_rpl_absorbed	Número de respuestas absorbidas por la capa de transacción (duplicados)

<b>Nombre de Métrica</b>	<b>Significado</b>
tmx_rpl_generated	Número de respuestas generadas localmente por el módulo de transacción
tmx_rpl_received	Número de respuestas recibidas para transacciones
tmx_rpl_relayed	Número de respuestas retransmitidas por el módulo de transacción
tmx_rpl_sent	Número de respuestas enviadas por el módulo de transacción

## USRLOC (Ubicación del Usuario)

<b>Nombre de Métrica</b>	<b>Significado</b>
usrloc_location_contacts	Número de contactos en el dominio 'location' (módulo usrloc estándar)
usrloc_location_expires	Número de contactos expirados en el dominio 'location'
usrloc_registered_users	Número de usuarios/AORs (Direcciones de Registros) registrados

## Métricas de I-CSCF

El I-CSCF comparte la mayoría de las estadísticas SIP básicas con el P-CSCF (ver sección de Estadísticas SIP Básicas de P-CSCF arriba). Las siguientes métricas son específicas de la funcionalidad de I-CSCF.

### Contexto Operativo de I-CSCF

El I-CSCF mantiene una lista de instancias S-CSCF disponibles para balanceo de carga:

El I-CSCF consulta al HSS para seleccionar instancias S-CSCF apropiadas para nuevos registros. El éxito de estas operaciones se rastrea en las métricas UAR y LIR a continuación.

### IMS I-CSCF (Interfaz Cx - Comunicación HSS)

El I-CSCF utiliza la interfaz Diameter Cx para comunicarse con el HSS (Servidor de Suscriptor en Casa) para consultas de ubicación de usuario y autorización.

### Métricas UAR (Solicitud de Autorización de Usuario)

<b>Nombre de Métrica</b>	<b>Significado</b>
ims_icscf_uar_avg_response_time	Tiempo de respuesta promedio para mensajes UAR en milisegundos

<b>Nombre de Métrica</b>	<b>Significado</b>
ims_icscf_uar_replies_received	(calculado como uar_replies_response_time / uar_replies_received)
ims_icscf_uar_replies_response_time	Número total de respuestas UAA (Respuesta de Autorización de Usuario) recibidas del HSS
ims_icscf_uar_timeouts	Tiempo total de respuesta para todos los mensajes UAR en milisegundos
	Número de tiempos de espera de solicitudes UAR

## Métricas LIR (Solicitud de Información de Ubicación)

<b>Nombre de Métrica</b>	<b>Significado</b>
ims_icscf_lir_avg_response_time	Tiempo de respuesta promedio para mensajes LIR en milisegundos
ims_icscf_lir_replies_received	(calculado como lir_replies_response_time / lir_replies_received)
ims_icscf_lir_replies_response_time	Número total de respuestas LIA (Respuesta de Información de Ubicación) recibidas del HSS
ims_icscf_lir_timeouts	Tiempo total de respuesta para todos los mensajes LIR en milisegundos
	Número de tiempos de espera de solicitudes LIR

## Métricas Comunes

El I-CSCF también exporta las siguientes métricas comunes (documentadas en la sección P-CSCF arriba):

- **Métricas CDP (Diameter)** - Estadísticas del protocolo Diameter
- **Estadísticas SIP Básicas** - Contadores de solicitudes/respuestas por método y código de estado
- **Estadísticas DNS** - Métricas de consultas DNS
- **Base de Datos MySQL** - Errores de conexión a la base de datos
- **Módulo Pike** - Estadísticas de bloqueo de IP
- **Memoria Compartida** - Estadísticas de uso de memoria
- **Módulo SL (Sin Estado)** - Contadores de respuestas sin estado
- **Transporte TCP** - Estadísticas de conexión TCP
- **Módulo TM/TMX (Transacción)** - Seguimiento del estado de las transacciones

# Métricas de S-CSCF

El S-CSCF comparte la mayoría de las estadísticas SIP básicas con el P-CSCF y el I-CSCF (ver sección de Estadísticas SIP Básicas de P-CSCF arriba). Las siguientes métricas son específicas de la funcionalidad de S-CSCF.

## Contexto Operativo de S-CSCF

El S-CSCF proporciona información detallada de ubicación del usuario y gestión de IFC (Criterios de Filtro Inicial):

La búsqueda de ubicación del usuario muestra IMPUs registrados con enlaces de contacto y perfiles de servicio. El número de contactos activos e IMPUs se rastrea mediante las métricas `ims_usrloc_scscf_active_contacts` y `ims_usrloc_scscf_active_impus`.

IFC (Criterios de Filtro Inicial) determina qué Servidores de Aplicación procesan sesiones SIP. El panel de control permite volcar y probar reglas IFC. El rendimiento de la evaluación de IFC puede afectar los tiempos de configuración de llamadas rastreados en las métricas de transacción (`tmx_*`).

## Autenticación IMS (Interfaz Cx - MAR)

El S-CSCF utiliza la interfaz Diameter Cx para autenticar usuarios con el HSS a través de MAR (Solicitud de Autenticación Multimedia).

Nombre de Métrica	Significado
<code>ims_auth_mar_avg_response_time</code>	Tiempo de respuesta promedio para mensajes MAR en milisegundos (calculado como <code>mar_replies_response_time / mar_replies_received</code> )
<code>ims_auth_mar_replies_received</code>	Número total de respuestas MAA (Respuesta de Autenticación Multimedia) recibidas del HSS
<code>ims_auth_mar_replies_response_time</code>	Tiempo total de respuesta para todos los mensajes MAR en milisegundos
<code>ims_auth_mar_timeouts</code>	Número de tiempos de espera de solicitudes MAR

## Registrador IMS S-CSCF

### Estadísticas de Registro

Nombre de Métrica	Significado
<code>ims_registrar_scscf_accepted_regs</code>	Número de solicitudes

<b>Nombre de Métrica</b>	<b>Significado</b>
ims_registrar_scscf_rejected_regs	REGISTER aceptadas exitosamente
ims_registrar_scscf_default_expire	Número de solicitudes REGISTER rechazadas
ims_registrar_scscf_default_expires_range	Tiempo de expiración predeterminado para registros en segundos
ims_registrar_scscf_max_contacts	Configuración del rango de expiración predeterminado
ims_registrar_scscf_max_expires	Número máximo de contactos permitidos por registro
ims_registrar_scscf_notifies_in_q	Tiempo máximo de expiración permitido en segundos
	Número de mensajes NOTIFY pendientes en la cola

## Métricas SAR (Solicitud de Asignación de Servidor)

<b>Nombre de Métrica</b>	<b>Significado</b>
ims_registrar_scscf_sar_avg_response_time	Tiempo de respuesta promedio para mensajes SAR en milisegundos (calculado como sar_replies_response_time / sar_replies_received)
ims_registrar_scscf_sar_replies_received	Número total de respuestas SAA (Respuesta de Asignación de Servidor) recibidas del HSS
ims_registrar_scscf_sar_replies_response_time	Tiempo total de respuesta para todos los mensajes SAR en milisegundos
ims_registrar_scscf_sar_timeouts	Número de tiempos de espera de solicitudes SAR

## IMS USRLOC S-CSCF

<b>Nombre de Métrica</b>	<b>Significado</b>
ims_usrloc_scscf_active_contacts	Número de enlaces de contacto registrados actualmente activos
ims_usrloc_scscf_active_impus	Número de IMPUs (Identidades Públicas IMS) registrados actualmente activos
ims_usrloc_scscf_active_subscriptions	Número de suscripciones actualmente activas

<b>Nombre de Métrica</b>	<b>Significado</b>
ims_usrloc_scscf_contact_collisions	Número de colisiones de hash en la tabla hash de contactos
ims_usrloc_scscf_impu_collisions	Número de colisiones de hash en la tabla hash de IMPU
ims_usrloc_scscf_subscription_collisions	Número de colisiones de hash en la tabla hash de suscripciones

## Seguimiento de Diálogos

El S-CSCF rastrea el estado del diálogo para llamadas activas:

<b>Nombre de Métrica</b>	<b>Significado</b>
dialog_ng_active	Número de diálogos actualmente activos (respondidos/confirmados)
dialog_ng_early	Número de diálogos tempranos (sonando/estado provisional)
dialog_ng_expired	Número de diálogos que han expirado o han sido terminados forzosamente
dialog_ng_processed	Número total de diálogos procesados desde el inicio

## Métricas Comunes

El S-CSCF también exporta las siguientes métricas comunes (documentadas en la sección P-CSCF arriba):

- **Métricas CDP (Diameter)** - Estadísticas del protocolo Diameter
- **Estadísticas SIP Básicas** - Contadores de solicitudes/respuestas por método y código de estado (nota: S-CSCF generalmente tiene más fwd\_requests y fwd\_replies ya que enruta entre puntos finales)
- **Estadísticas DNS** - Métricas de consultas DNS
- **Base de Datos MySQL** - Errores de conexión a la base de datos
- **Módulo Pike** - Estadísticas de bloqueo de IP
- **Memoria Compartida** - Estadísticas de uso de memoria
- **Módulo SL (Sin Estado)** - Contadores de respuestas sin estado
- **Transporte TCP** - Estadísticas de conexión TCP
- **Módulo TM/TMX (Transacción)** - Seguimiento del estado de las transacciones (nota: S-CSCF generalmente tiene tanto transacciones UAC como UAS ya que actúa como cliente y servidor)