Machine Translated by Google
RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 30/09/2026 | Aceptado: 03/10/2026 | Publicación: 06/10/2026

Itinerancia internacional en redes 5G independientes.
Itinerancia internacional en redes 5G independientes
Itinerancia internacional en redes 5G independientes

Danyell Teixeira Soares

Ingeniero de Telecomunicaciones con 16 años de experiencia. MBA en Gestión Empresarial por la Fundação Getulio Vargas (FGV-SP, 2015). Licenciatura en Ingeniería Eléctrica con énfasis en Telecomunicaciones por la Pontifícia Universidad Católica de São Paulo (PUC-SP, 2008).

Resumen

Este artículo investiga los mecanismos arquitectónicos, los protocolos de seguridad y los requisitos de gobernanza necesarios para garantizar la continuidad del servicio internacional en las redes 5G Standalone (5G SA).
Este estudio examina la diferenciación entre las topologías Home Routed (HR) y Local Breakout (LBO), el rol del Security Edge Protection Proxy (SEPP) en el borde entre PLMN y la protección de la interfaz N32 mediante las especificaciones 3GPP TS 29.573. También analiza el esquema de privacidad de la identidad del suscriptor basado en el cifrado SUPI en SUCI, mitigando las vulnerabilidades de seguimiento histórico. La metodología se basa en una revisión analítica de los estándares 3GPP (Release 18), las especificaciones GSMA (NG.113), los informes ENISA y artículos científicos revisados por pares. Concluye que el éxito operativo del roaming 5G depende de una cadena de confianza punto a punto rigurosamente validada mediante pruebas bilaterales y observabilidad segmentada por socios.

Palabras clave: Roaming 5G. Enrutamiento a domicilio. Salida de ubicación. SEPP. Interfaz N32. SUCI.

Abstracto

Este documento investiga los mecanismos arquitectónicos, los protocolos de seguridad y los marcos de gobernanza necesarios para garantizar la continuidad del servicio internacional en redes 5G Standalone (5G SA). Detalla las diferencias operativas entre las topologías Home Routed (HR) y Local Breakout (LBO), el papel del Security Edge Protection Proxy (SEPP) en el límite entre PLMN y la protección de la interfaz N32 según las especificaciones 3GPP TS 29.573. También analiza los mecanismos de privacidad de la identidad del suscriptor basados en el cifrado del SUPI en un SUCI, mitigando las vulnerabilidades de seguimiento heredadas. La metodología se basa en una revisión analítica de los estándares 3GPP Release 18, las directrices GSMA (NG.113), los informes de amenazas de ENISA y la literatura científica revisada por pares. El estudio concluye que el éxito operativo en el roaming 5G depende de una cadena de confianza de extremo a extremo validada mediante pruebas bilaterales y observabilidad segmentada por socios.

Palabras clave: Roaming 5G. Enrutamiento a domicilio. Salida de ubicación. SEPP. Interfaz N32. SUCI.

1. Introducción

La itinerancia internacional en las redes de telecomunicaciones móviles es la piedra angular que permite la continuidad.
Gama global de servicios de voz, mensajería y datos para usuarios que se desplazan fuera de sus redes.
origen (Home Public Land Mobile Network - HPLMN). En las generaciones de redes heredadas (2G, 3G y
4G), la señalización entre redes asociadas dependía en gran medida de los protocolos SS7 y Diameter,
transportado por redes de intercambio de tráfico conocidas como IPX (IP Exchange) (BASIN et al., 2018;
ENISA, 2020).

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 30/09/2026 | Aceptado: 03/10/2026 | Publicación: 06/10/2026

Sin embargo, las arquitecturas de señalización tradicionales presentaban graves vulnerabilidades estructurales.
Los protocolos SS7 y Diameter fueron concebidos originalmente bajo la premisa ingenua de que la red de
El transporte IPX era un entorno implícitamente confiable. Esta vulnerabilidad permitió que agentes maliciosos accedieran al servicio.
llevaron a cabo ataques que implicaban suplantación de origen, interceptación no autorizada de
Llamadas y mensajes SMS, y seguimiento en tiempo real de la ubicación geográfica de los suscriptores.
(ENISA, 2020).
La introducción de 5G Standalone (5G SA) altera radicalmente este escenario al reemplazar los protocolos.
legados de la arquitectura basada en servicios (SBA). En 5G SA, toda la comunicación del plan de
El control entre la red visitada (PLMN visitada - VPLMN) y la red de origen (HPLMN) se convierte en
gestionado a través de llamadas a la API RESTful sobre HTTP/2, lo que requiere nuevos paradigmas para el
protección de las fronteras entre operadores (3GPP, 2024c; GSMA, 2024).
Para garantizar la seguridad del ecosistema de roaming entre PLMN, el estándar 3GPP TS 29.573 define
El Proxy de Protección de Borde de Seguridad (SEPP) es una función de borde obligatoria. SEPP actúa como...
Punto único de entrada y salida para la señalización del plano de control, que protege la topología interna.
desde el operador y gestionando el cifrado de los mensajes transmitidos a través de la interfaz N32.
(3GPP, 2024c).
La interfaz N32 implementa el protocolo PRINS (Protocol-specific Application Layer Security), un
Una innovación crucial que resuelve el dilema entre el cifrado de extremo a extremo y la necesidad de intermediarios.
La red IPX permite a los usuarios modificar ciertos encabezados de transporte. Esto garantiza la integridad de los datos.
y la confidencialidad de los datos del usuario, permitiendo únicamente modificaciones expresamente indicadas.
autorizado por contratos de señalización.
El objetivo de este artículo es examinar exhaustivamente la arquitectura de roaming en 5G SA, analizando
topologías de transporte de datos, el papel de SEPP en la interfaz N32, el esquema criptográfico de
Privacidad de la identidad (SUPI/SUCI), interoperabilidad de múltiples proveedores y modelos de
Gobernanza bilateral. El análisis se basa estrictamente en las especificaciones y directrices oficiales del 3GPP.
de la GSMA y de literatura científica de alto impacto.

2 Metodología

Este estudio se basa en una revisión analítica y sistemática de la literatura técnica.
Conocimientos estandarizados y científicos especializados en seguridad de redes móviles y arquitectura de telecomunicaciones.
El proceso de selección del corpus documental se guió por el rigor metodológico y la verificación.
autoridad de las fuentes.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 30/09/2026 | Aceptado: 03/10/2026 | Publicación: 06/10/2026

El primer eje de la encuesta abarca las especificaciones normativas primarias publicadas por
3GPP (Versión 18). Se analizaron en profundidad los documentos TS 23.501 (arquitectura general).
TS 23.502 (flujos de procedimiento), TS 29.573 (interconexión de red PLMN a través de SEPP) y TS
33.501 (Arquitectura y procedimientos de seguridad 5G).
El segundo eje metodológico abarca las directrices operativas y orientaciones consolidadas por
Asociación Internacional de Operadores Móviles (GSMA). El enfoque se centró en el estándar GSMA NG.113 (5GS).
Directrices de itinerancia), que establece los requisitos prácticos para la implementación de acuerdos.
Itinerancia bilateral en redes de quinta generación.
El tercer eje incluye informes de evaluación de amenazas técnicas y marcos para...
directrices de ciberseguridad emitidas por organismos gubernamentales e internacionales, con especial énfasis en
Publicaciones de la Agencia de la Unión Europea para la Ciberseguridad (ENISA - *Panorama de amenazas 5G*)
y NIST (Marco de Ciberseguridad 2.0).
El cuarto eje comprende artículos científicos revisados por pares presentados en conferencias.
Un referente en el campo de la seguridad de la información y las redes móviles, como la Conferencia ACM SIGSAC.
sobre seguridad informática y de las comunicaciones (CCS) y revistas selectas de IEEE/Elsevier.
mediante la validación directa del DOI.
La síntesis de la información se organizó en una matriz analítica centrada en cuatro dimensiones.
Aspectos operativos: topología del plano de usuario, seguridad del plano de control en la interfaz N32,
Cifrado de privacidad del suscriptor y requisitos de gobernanza bilateral. El texto final fue
Totalmente estandarizado según las directrices de redacción científica y citación de ABNT.

3 modelos arquitectónicos para roaming 5G

Establecer una sesión de roaming en 5G SA requiere una coordinación precisa entre las funciones.
Redes de control y transporte ubicadas en la red visitada (VPLMN) y en la red doméstica del abonado.
(HPLMN). 3GPP estandariza dos modelos arquitectónicos para el manejo del tráfico de datos.
Usuario: Home Routed (HR) y Local Breakout (LBO) (3GPP, 2024a; GSMA, 2024).
En el modelo Home Routed (HR), el anclaje principal del plano de usuario permanece en la red de
se origina a través de H-UPF (Home UPF). Cuando el usuario accede a la red en la VPLMN, el tráfico de
Los datos son recibidos por el V-UPF local y encapsulados en un túnel GTP-U que atraviesa la interfaz N9.
inter-PLMN a través de la red IPX hasta llegar al H-UPF en el país de origen, desde donde finalmente se realiza el tráfico...
enrutado a Internet (3GPP, 2024a).

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 30/09/2026 | Aceptado: 03/10/2026 | Publicación: 06/10/2026

Figura 1 – Arquitetura de Interconexão e Segurança de Roaming 5G SA com SEPP

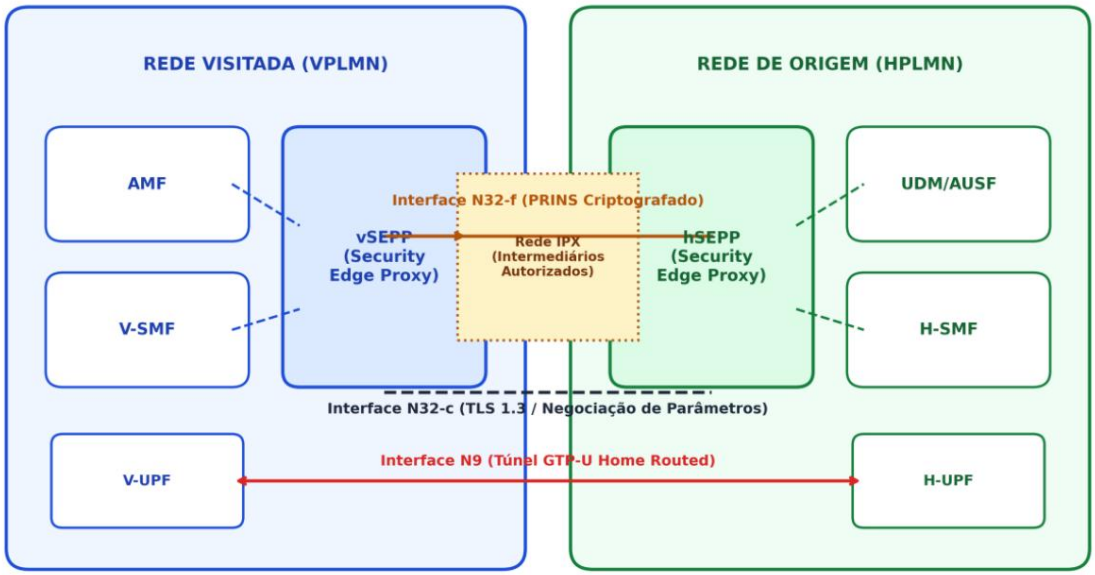

Figura 1 – Arquitectura de seguridad e interconexión de roaming 5G SA con SEPP.

Fuente: Elaborado con base en 3GPP TS 29.573 (2024).

La arquitectura HR es la opción preferida por los operadores de telecomunicaciones para Servicios de datos convencionales. La centralización del plan de usuario en HPLMN garantiza el control. absoluto con respecto a la aplicación de políticas de precios en tiempo real, auditoría de consumo y estricto cumplimiento de los requisitos reglamentarios locales para la interceptación legal (*legal interceptación*), sin depender de las políticas del socio visitado.

Sin embargo, la principal desventaja del modelo Home Routed es la latencia adicional introducida por Enrutamiento circular (*tromboning*). El tráfico de datos se ve obligado a viajar geográficamente al país. origen y regreso al destino, lo que puede hacer inviable las aplicaciones en tiempo real que lo requieren. Latencia ultrabaja (URLLC), como la automatización industrial avanzada y la telemedicina (GSMA, 2024).

Para superar esta limitación, 3GPP define el modelo Local Breakout (LBO). En LBO, el tráfico Los datos de sesión PDU se descargan directamente a la red de datos de destino desde el V-UPF ubicada en VPLMN, eliminando la necesidad de que el tráfico viaje al país de origen. HPLMN mantiene El control sobre las reglas de política y la autorización de sesión se realiza únicamente a través de H-PCF y H-SMF (3GPP, 2024a).

A pesar de su superioridad técnica en cuanto a latencia, el modelo LBO presenta una complejidad significativa. operativo y comercial. Requiere acuerdos bilaterales de emisión de billetes altamente complejos para La facturación cruzada entre operadores plantea desafíos regulatorios en materia de responsabilidad. El tráfico se descarga en la red visitada, razón por la cual su adopción inicial se limita a los servicios. empresa específica (GSMA, 2024).

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 30/09/2026 | Aceptado: 03/10/2026 | Publicación: 06/10/2026

4 SEPP, N32 Seguridad de interfaz e interconexión

Para eliminar las vulnerabilidades históricas de las redes de señalización SS7 y Diameter, el 3GPP TS

El Reglamento 29.573 establece el Proxy de Protección de Borde de Seguridad (SEPP, por sus siglas en inglés) como la función de protección de borde obligatoria.

En 5G SA, todos los flujos de señalización desde el plano de control entre la VPLMN y la HPLMN son gestionados por cualquier sistema de señalización.

debe transitar obligatoriamente a través de los SEPP de ambas redes (vSEPP y hSEPP) (3GPP, 2024c;

ENISA, 2020).

SEPP desempeña funciones vitales de ciberseguridad en el borde entre PLMN. Actúa como

Un cortafuegos de aplicación de señalización que realiza el enmascaramiento de la topología de la red interna.

(*ocultación de topología*), filtrado de mensajes no autorizados, control de velocidad para la prevención de

Ataques de denegación de servicio (DoS) y validación estricta del formato de esquemas JSON (3GPP,

2024c).

La interconexión entre vSEPP y hSEPP se produce a través de la interfaz N32, que es lógicamente...

subdividido en dos canales operativos con funciones complementarias: la interfaz N32-c (Control

Plano) y la interfaz N32-f (Plano de reenvío) (3GPP, 2024c).

La interfaz N32-c se utiliza para la fase de control inicial. A través de ella, los dos SEPP realizan la...

Autenticación mutua mediante TLS 1.3 utilizando certificados digitales x.509, con capacidad de negociación.

Métodos criptográficos admitidos, intercambio de claves de sesión y establecimiento de los parámetros de la Asociación de

Asociación de Seguridad (SA) que regirá el intercambio de mensajes de la aplicación.

La interfaz N32-f está dedicada a la transmisión eficaz de mensajes de señalización desde las funciones de red internas.

(como llamadas entre V-SMF y H-SMF o AMF y UDM). Para proteger estos mensajes mientras

Para el tránsito a través de la red IPX, el N32-f implementa el protocolo PRINS (Protocol-specific Application Layer).

Seguridad) (3GPP, 2024c; BASIN et al., 2018).

El protocolo PRINS resuelve elegantemente el dilema del transporte itinerante. ¿Cómo?

Los proveedores de redes IPX intermedias a menudo necesitan modificar ciertos encabezados.

Para el enrutamiento HTTP/2, PRINS divide el mensaje en bloques: los datos confidenciales del suscriptor.

permanecen totalmente encriptados e inaccesibles, mientras que los encabezados modificables pueden ser

Modificado por nosotros con nuestra autorización y reasignado criptográficamente, lo que garantiza una auditabilidad completa.

(BASIN et al., 2018).

5. Identidad, autenticación y privacidad del suscriptor

Una de las debilidades más graves de las redes móviles de segunda, tercera y cuarta generación fue...

Transmisión de la identidad permanente del abonado (IMSI) en texto plano a través del canal de radio.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 30/09/2026 | Aceptado: 03/10/2026 | Publicación: 06/10/2026

durante los procedimientos iniciales de conexión de red. Esta limitación facilitó la proliferación de
equipo de interceptación malicioso conocido como *IMSI Catchers* (Stingrays) (BASIN et
et al., 2018; ENISA, 2020).

En 5G Standalone, la especificación 3GPP TS 33.501 elimina esta vulnerabilidad al redefinir la
Estructura de identidad del usuario. La identidad permanente del suscriptor ahora se llamará
SUPI (Identificador Permanente de Suscripción). La normativa prohíbe expresamente que el SUPI sea...
transmitido en texto plano en cualquier interfaz de radio (3GPP, 2024d).

En lugar de enviar directamente datos SUPI, la tarjeta SIM/eSIM del terminal del usuario genera un
Una identidad temporal y encriptada llamada SUCI (Identificador Oculto de Suscripción). La generación de
SUCI se basa en un esquema de criptografía de clave pública asimétrica basado en curvas.
elíptica (ECIES - Esquema de cifrado integrado de curva elíptica) (BASIN et al., 2018).

La tarjeta SIM almacena en su memoria segura la clave pública de la red de origen.
(HPLMN). Al solicitar acceso a la red visitada (VPLMN), el terminal utiliza la clave pública para
El cifrado de SUPI produce SUCI. La clave privada correspondiente se mantiene exclusivamente...
Dentro del HPLMN UDM, ni la red de radio ni el VPLMN AMF pueden descifrar el
identidad real del usuario.

Al recibir el SUCI enviado por el terminal, el AMF en el VPLMN reenvía esta identidad cifrada a
Se accede al HPLMN hSEPP a través de la interfaz N32. El HPLMN UDM utiliza su clave privada para...
Descifra el SUCI, recupera el SUPI original e inicia el procedimiento de autenticación mutua 5G-AKA.
(o EAP-AKA') (3GPP, 2024d).

Este mecanismo garantiza que la privacidad del suscriptor se mantenga preservada de extremo a extremo. Incluso
que la red de radio visitada o la infraestructura del socio de itinerancia se vean comprometidas por escuchas ilegales.
Incluso ante actividades maliciosas, la identidad permanente del usuario permanece totalmente protegida contra el rastreo.
indebido (BASIN et al., 2018).

6. Interoperabilidad y señalización entre operadores

La habilitación del roaming internacional en redes 5G SA requiere un estricto cumplimiento técnico y
semántica entre funciones de red desarrolladas por diferentes proveedores de tecnología (*multi-
(proveedor*). Las llamadas a la API intercambiadas en la SBA deben cumplir estrictamente con los esquemas OpenAPI.
3.0 estandarizado por 3GPP en la serie TS 29500 (3GPP, 2024c; GSMA, 2024).

En escenarios operativos del mundo real, pequeñas discrepancias en la interpretación de parámetros opcionales en
Los documentos JSON o el manejo específico de encabezados HTTP/2 pueden provocar el rechazo.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 30/09/2026 | Aceptado: 03/10/2026 | Publicación: 06/10/2026

solicitudes en el borde SEPP. Esto da como resultado la terminación prematura del intento de conexión y en
Pérdida de conectividad para los suscriptores mientras están en roaming.

Para mitigar estos riesgos de interoperabilidad, el estándar GSMA NG.113 establece un protocolo.
Instrucciones detalladas para realizar pruebas bilaterales continuas (*Pruebas IREG*) antes de su lanzamiento.
rutas de roaming comercial entre dos operadores (GSMA, 2024).

Las pruebas bilaterales abarcan la validación sintáctica y semántica en SEPP, verificando si las reglas de
Los firewalls de señalización están configurados para permitir el paso de API autorizadas sin
Alterar indebidamente la carga útil de los mensajes cifrados mediante PRINS.

Otro aspecto fundamental es la estandarización de la asignación de códigos de causas de error.
Cuando falla una solicitud de sesión PDU en HPLMN, H-SMF debe devolver un código de error.
HTTP estandarizado (por ejemplo, `403 Prohibido` o `504 Tiempo de espera de puerta de enlace`) seguido del código de
La causa 5GSM correspondiente, según TS 24.501, permite que el AMF en VPLMN guíe el
terminal correctamente (GSMA, 2024).

Finalmente, los equipos de ingeniería de redes deben ajustar los temporizadores.
Llamadas de reconexión TCP y comprobación de integridad del bus HTTP/2 (*PING*)
interfaz N32. Esta medida evita que pequeñas fluctuaciones de latencia en la red IPX provoquen la
Desmantelamiento masivo de asociaciones de seguridad entre SEPP (GSMA, 2024).

7. Calidad, continuidad y experiencia en el roaming

La experiencia percibida por el usuario en el roaming internacional depende directamente de la calidad.
La técnica se mantiene en ambas redes implicadas (VPLMN y HPLMN) y en el segmento de transporte.
interconectado a través de IPX. El monitoreo continuo de esta experiencia requiere seguimiento por
Indicadores de nivel de servicio (SLI) altamente específicos (ITU, 2024; GSMA, 2024).

La evaluación de la calidad se divide entre las métricas del plan de control y las métricas del plan de riesgos.
usuario. En el plan de control, el indicador principal es la tasa de éxito en los procedimientos de
Autenticación 5G-AKA y tiempo de respuesta total para establecer sesiones de datos PDU.
en la topología Home Routed.

A nivel de usuario, las métricas se centran en la latencia de ida y vuelta (RTT) del túnel GTP-U.
interfaz N9, en la tasa de cambio del retardo de paquetes (*jitter*) y en el porcentaje de pérdida accidental
de paquetes durante la transmisión transfronteriza.

Para identificar los cuellos de botella en el rendimiento de las redes internacionales, es necesario tener la capacidad de segmentar.
Datos de observabilidad por socio itinerante (identificado por PLMN-ID). Una elevación
Latencia atípica observada exclusivamente en la interfaz N32 asociada a una específica

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 30/09/2026 | Aceptado: 03/10/2026 | Publicación: 06/10/2026

El operador asociado indica saturación en el SEPP remoto o degradación en la ruta de red IPX contratada. (GSMA, 2024).

El uso de sistemas automatizados de monitoreo de la experiencia en tiempo real permite que El operador de origen realiza una conmutación de tráfico proactiva (dirección de roaming). En caso de que el Si la calidad de un socio VPLMN cae por debajo de los límites SLO aceptables, HPLMN aconseja conectar dinámicamente los terminales de sus suscriptores a otra red de socios disponible en misma región.

De esta forma, la integración de las métricas de calidad del plano de control y del plano de datos garantiza la continuidad transparente de los servicios, minimizando las interrupciones de navegación y garantizando la cumplimiento de los acuerdos de nivel de servicio (SLA) comerciales (UIT, 2024).

8. Gobernanza bilateral, fraude y respuesta a incidentes

El funcionamiento fiable de los acuerdos de roaming en 5G SA va más allá del despliegue de soluciones. Es puramente tecnológico. Requiere una estructura de gobernanza organizativa y contractual bilateral. Los operadores asociados se caracterizan por una alta disciplina y por estar alineados con los principios de ciberseguridad del NIST. Marco 2.0 y recomendaciones de la GSMA (GSMA, 2024; NIST, 2024).

Los contratos operativos de itinerancia deben definir con precisión una matriz de responsabilidades. (RACI) que abarca todos los puntos de contacto técnico, ventanas de mantenimiento programadas y Procedimientos estandarizados para la notificación anticipada de cambios de software en el extremo de la red PLMN.

Uno de los pilares de la gobernanza técnica es la gestión continua del ciclo de vida del certificado. Las firmas digitales x.509 se utilizan para el cifrado TLS en la interfaz N32-c y la firma PRINS en la interfaz N32-f. falta de un control riguroso de las fechas de vencimiento claves o fallos en la rotación de las mismas. Los certificados PKI pueden provocar la interrupción completa e inmediata del tráfico de roaming entre dos redes.

En el contexto de la prevención del fraude, la migración a 5G SA requiere nuevos mecanismos para Monitorización en el SEPP. El tráfico de señalización debe ser analizado continuamente mediante algoritmos. detección de anomalías para identificar intentos de eludir la facturación, llamadas fantasma o Ataques de explotación de API dirigidos al consumo no autorizado de datos.

Además, el intercambio mutuo de registros de facturación y uso debería producirse en plazos más breves. a través del formato estandarizado SDR (Registro de Datos Estándar), lo que permite una rápida conciliación de Facturación entre operadores y contención ágil de incidentes financieros (GSMA, 2024).

Finalmente, la gobernanza requiere el establecimiento de canales de comunicación directos para responder a Respuesta a incidentes de ciberseguridad (CSIRT). En caso de compromiso de claves privadas o

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 30/09/2026 | Aceptado: 03/10/2026 | Publicación: 06/10/2026

Identificación de patrones de ataque originados en la red del socio y protocolos de contención.

Se deben activar las medidas de emergencia y el aislamiento de rutas, con tiempos de respuesta que se miden en minutos.

(NIST, 2024).

Consideraciones finales

La activación del roaming internacional en redes 5G Standalone representa una transición histórica.

al nivel de seguridad, privacidad y eficiencia que se ofrece a los usuarios en la movilidad global.

reemplazo definitivo de las redes heredadas SS7 y Diameter con una infraestructura basada en

Los microservicios y las llamadas a la API a través del protocolo HTTP/2 abordan las vulnerabilidades estructurales de

La señalización ha afectado al sector de las telecomunicaciones durante décadas.

Como se demuestra en esta investigación, la presencia obligatoria del proxy de protección de borde de seguridad es fundamental.

(SEPP) en el borde inter-PLMN constituye la piedra angular de la seguridad en 5G SA. Al actuar como

Mediante el uso del cortafuegos de aplicaciones y la gestión del protocolo PRINS en la interfaz N32, SEPP garantiza la integridad del protocolo.

y la confidencialidad de los mensajes del plan de control incluso en presencia de intermediarios.

en la red de transporte IPX.

El análisis de las topologías del plano de usuario revela que la arquitectura Home Routed (HR)

Sigue siendo la opción predominante para los operadores a la hora de proporcionar servicios de datos.

convencional. La capacidad de mantener el anclaje UPF en HPLMN garantiza la auditabilidad.

Precios y cumplimiento de la normativa local sin depender del socio que se visite.

A su vez, el modelo de compra apalancada local (LBO, por sus siglas en inglés) se está consolidando como una opción estratégica indispensable.

para habilitar servicios de ultra alta velocidad y ultrabaja latencia (URLLC). La descarga

El enrutamiento del tráfico directamente en la red visitada elimina los retrasos inherentes al enrutamiento circular, lo que abre...

Una vía para aplicaciones industriales y corporativas transfronterizas.

En lo que respecta a la privacidad del usuario, el avance proporcionado por el esquema de cifrado

El protocolo SUPI/SUCI asintótico elimina de forma permanente la exposición del identificador del abonado en el canal.

radio. El hecho de que SUCI se descifre exclusivamente mediante la clave privada almacenada en el UDM de

La red de origen protege a los suscriptores contra escaneos maliciosos y seguimiento indebido mediante

Dispositivos *IMSI Catchers*.

Garantizar una interoperabilidad perfecta en entornos de múltiples proveedores.

Esto refuerza la importancia de adherirse estrictamente a los esquemas y rutinas de prueba de OpenAPI 3.0.

ajustes bilaterales según lo recomendado por GSMA NG.113. La configuración de los temporizadores del bus HTTP/2 y el

La estandarización de los códigos de causa de error es esencial para evitar fallos en la señalización.

intermitente.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 30/09/2026 | Aceptado: 03/10/2026 | Publicación: 06/10/2026

Paralelamente, la gobernanza operativa y contractual se reafirma como un elemento inseparable de Arquitectura de red. Gestión disciplinada del ciclo de vida y monitorización de los certificados PKI. La prevención del fraude en el SEPP y la coordinación de incidentes cibernéticos en tiempo real son las condiciones que garanticen la estabilidad de las alianzas internacionales.

En conclusión, el éxito del roaming en 5G SA depende de la construcción de una cadena de confianza. Integración técnica e institucional integral. Integración armoniosa entre mecanismos criptográficos. En el extremo, la observabilidad segmentada por socios y la gobernanza bilateral continua son lo que garantiza... Ofreciendo una experiencia de conectividad verdaderamente sólida, segura e internacional. resiliente.

Referencias

3GPP. TS 23.501: Arquitectura del sistema para el sistema 5G; Etapa 2 (Versión 18). Sophia Antipolis: 3GPP, 2024a. Disponible en: https://www.3gpp.org/dynareport/23501.htm.
3GPP. TS 23.502: Procedimientos para el sistema 5G; Etapa 2 (Versión 18). Sophia Antipolis: 3GPP, 2024b. Disponible en: https://www.3gpp.org/dynareport/23502.htm.
3GPP. TS 29.573: Interconexión de redes móviles terrestres públicas (PLMN); Etapa 3 (Versión 18). Sophia Antipolis: 3GPP, 2024c. Disponible en: https://www.3gpp.org/dynareport/29573.htm.
3GPP. TS 33.501: Arquitectura y procedimientos de seguridad para el sistema 5G (Versión 18). Sophia Antipolis: 3GPP, 2024d. Disponible en: https://www.3gpp.org/dynareport/23501.htm.
BASIN, D. et al. Un análisis formal de la autenticación 5G. En: Actas de la Conferencia ACM SIGSAC de 2018 sobre Seguridad Informática y de las Comunicaciones (CCS '18), 2018, Toronto. Anales [...]. Nueva York: ACM, 2018. págs. 1383-1396. DOI: https://doi.org/10.1145/3243734.3243846.

ENISA. Panorama de amenazas de ENISA para redes 5G. Atenas: Agencia de Ciberseguridad de la Unión Europea, 2020. DOI: https://doi.org/10.2824/49299.
GSMA. NG.113: Directrices de roaming 5GS. Versión 10.0. Londres: GSMA, 2024. Disponible en: https://www.gsma.com/newsroom/wp-content/uploads/NG.113-v10.0.pdf. Consultado el 10 de septiembre de 2026.
UIT. Medición del desarrollo digital: Datos y cifras 2024. Ginebra: Unión Internacional de Telecomunicaciones, 2024. Disponible en: https://www.itu.int/itu-d/reports/statistics/facts-figures-2024/.

NIST. Marco de Ciberseguridad 2.0. https://doi.org/ Gaithersburg: NIST, 2024. DOI: 10.6028/NIST.CSWP.29.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.