Guía de evaluación de seguridad de redes móviles

Tabla de contenido

1 Objetivos

Para mejorar la seguridad de la red de telecomunicaciones de Ecuador y ayudar a los operadores ecuatorianos a reducir los riesgos en sus redes, el Ministerio de telecomunicaciones de Ecuador ha publicado su propia guía de evaluación de redes de telecomunicación, basada en estándares internacionales, para guiar a los operadores de redes de telecomunicación de Ecuador en la evaluación y reducción de sus riesgos.

2 Ámbito de aplicación

Con base en el Balance Ecuatoriano de Economía y Eficiencia y en el MCKB GSMA, Mintel(Ministerio de Telecomunicaciones y de la Sociedad de la Información) recomienda que los operadores evalúen los riesgos en las áreas centrales de control consultando esta guía. La evaluación se divide en dos áreas: gestión de redes de radio y gestión de redes centrales.

Se puntúa la madurez de cada elemento de control y se utiliza la puntuación media como puntuación de red. Para una introducción al vencimiento, véase el capítulo 7.

3 Abreviaturas

Plazo	Descripción
3GPP	*Proyecto de asociación de tercera generación*
CA	Autoridad certificadora
CEI	Centro para la seguridad en Internet
CN	Red core
GGSN	Nodo de soporte de gateway GPRS
GPRS	Servicios generales de radio por paquetes
GSM	Sistema global para red móvil – 2G
GSMA	Asociación GSM
GTP	Protocolo de túnel GPRS
HA	Alta disponibilidad
IMEI	*Identidad internacional de equipos móviles*
IP	Protocolo de Internet
IPsec	Seguridad del protocolo de Internet
IPX	Intercambio de paquetes entre redes
LTE	Evolución a largo plazo: red 4G
MAE	Motor de automatización de redes móviles
MAPA	Parte de aplicación móvil
MMS	Servicio de mensajería multimedia
MMSC	Centro de servicios de mensajería multimedia
NE	Elemento de red

Plazo	Descripción
NIST	Instituto Nacional de Ciencia y Tecnología (Estados Unidos)
NR	Nueva radio
OTA	Por el aire
PIN	Número de identidad personal
RAN	Red de acceso por radio
RCS	Servicios de comunicación enriquecidos
RN	Red de radio
SMS	Servicio de mensajes cortos
STP	Punto de transferencia de señales
SUCI	Identificador oculto de suscripción
TMSI	Identidad de estación móvil temporal
UE	Equipos de usuario
UMTS	Servicio Universal de Telecomunicaciones Móviles - Red 3G

4 Introducción

A medida que los operadores de redes móviles (MNO) de todo el mundo introduzcan y pongan en marcha sistemas de redes móviles, las redes de comunicaciones se enfrentarán a nuevas amenazas y desafíos para la seguridad. Se ha vuelto esencial comprender, determinar y mitigar estas amenazas a la seguridad existentes y futuras de manera objetiva, rápida y eficaz.

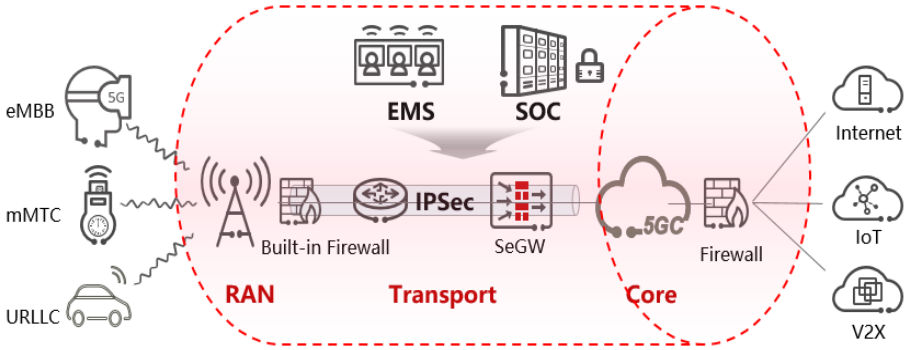
GSMA ha llevado a cabo un análisis exhaustivo de amenazas en el que han participado expertos de la industria de todo el ecosistema, incluidos MNO, vendedores, proveedores de servicios y reguladores, además de recopilar información de fuentes públicas como 3GPP, ENISA y NIST, y asignaron estas amenazas a controles de seguridad adecuados y efectivos.

La base de conocimientos proporciona información esencial para la estrategia de gestión de riesgos de las partes interesadas, así como orientación sobre las mejores prácticas y las medidas de mitigación de riesgos. La base de conocimientos facilita y fomenta la colaboración para proteger las redes y los servicios contra interrupciones y accesos no autorizados.

5 Guía de evaluación de seguridad

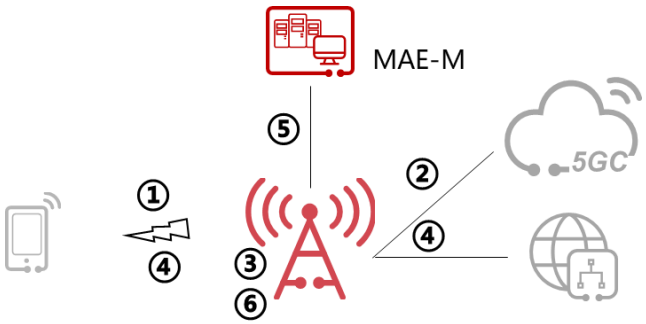
5.1 Marco general de evaluación

La evaluación de seguridad se centra en la red E2E del operador y abarca todos los elementos de red clave de la red, como se muestra en la siguiente figura. Para las evaluaciones de gestión de redes de radio y de gestión de redes core, se evalúa el E2E “RAN→Transporte→Core”.



5.2 Evaluación de la gestión de redes de radio

La seguridad de la red de radio se evalúa desde seis dimensiones.



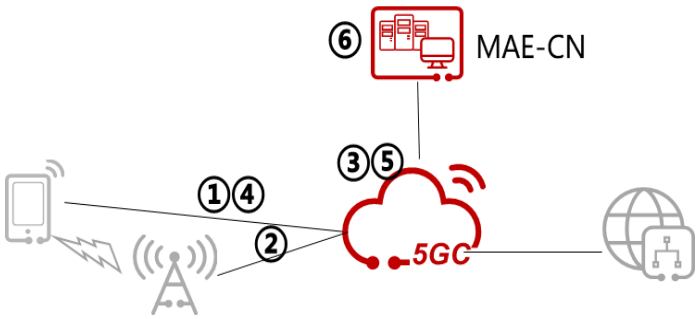
La privacidad, confidencialidad e integridad de los datos de la interfaz aérea de red están bien protegidos. En cuanto a la estructura de la red, el aislamiento de tres planos se utiliza para defenderse contra ataques entre diferentes capas de servicio.

Categoría	Descripción
① Seguridad de las comunicaciones	Evita la interceptación y manipulación no autorizadas del tráfico de usuarios y la información de señalización
②Privacidad del usuario	Uso de identificadores temporales de dispositivos para evitar el seguimiento de usuarios
③Seguridad de los equipos	Detecta y localiza ataques anormales para fines de seguridad básica/física (conocimiento del riesgo).
	Seguridad del puerto para la estación base para evitar ataques al puerto local.
④Aislamiento CP y UP	Garantiza el aislamiento del tráfico del plano de datos y del plano de control.
⑤Seguridad O&M	Las estaciones base utilizan medidas de protección de seguridad para garantizar la seguridad de O&M.

⑥Compensación de riesgos	La estación base se despliega en un entorno de riesgo. Deben añadirse medidas compensatorias para controlar los riesgos.
	La estación base se implementa compartiendo RAN. Deben añadirse medidas compensatorias para controlar los riesgos.

5.3 Evaluación de la administración de la red principal

La seguridad de la red core está protegida por la protección de señalización, la autenticación de acceso de usuarios, la protección de identidad de usuarios, la protección de IMS y el control de acceso. A través de las funciones de autenticación de identidad de usuario y cifrado de señalización, se garantiza la legitimidad de la identidad de usuario. Y las técnicas de anonimización del cliente (GUTI) se utilizan para evitar la transmisión de información de usuario no protegida. En cuanto a los datos entre la red core y la RAN, IPsec y firewall se implementan para la protección de enlaces.



Categoría	Descripción
①Autenticación de usuarios	Garantiza que solo los clientes de suscripción autorizados puedan acceder al servicio
②Protección de señalización RAN-CN	evita la interceptación no autorizada y la manipulación del tráfico de usuarios
③Protección de la identidad del usuario	Utilice la tecnología de anonimato para proteger la identidad de los usuarios individuales.
④Protección de seguridad IMS	Impide que el tráfico de mensajes no solicitados (RCS, SMS y MMS) llegue a los clientes.
⑤Validez de IMEI UE	Controla qué dispositivos pueden acceder a la red para evitar la conexión de dispositivos falsificados, robados y no calificados.
⑥Gestión de control de acceso	Procesos y herramientas para rastrear/controlar/prevenir/corregir el acceso seguro a activos críticos

6 Sugerencias para soluciones de refuerzo de la seguridad

De acuerdo con los requerimientos del elemento de control GSMA MCKB, se realizan evaluaciones y

análisis de seguridad de la red E2E. Las sugerencias detalladas de soluciones de endurecimiento son las siguientes:

Sugerencias para soluciones de refuerzo de redes de radio

Referencia	Objetivo	Descripción de la solución
RN-001	**Proteger criptográficamente el tráfico de redes** GSM, GPRS, UMTS, LTE y NR para protegerlo contra la interceptación no autorizada y la alteración del tráfico de usuarios y de la información sensible de señalización.	1. Habilite los mecanismos de encriptación recomendados en FS.35 y prohíba el uso de no encriptación, siempre que sea posible. 2. Garantizar que la protección de integridad del plano de control en UMTS, LTE o 5G se aplique correctamente 3. Garantizar que la protección de la integridad del plano de usuario se aplique cuando sea factible y necesario 4. Proteger la interfaz entre la red de acceso por radio y la red core (S1/N2), por ejemplo, implementar IPsec cuando sea apropiado 5. Proteger la interfaz de radio entre los nodos de acceso de radio, es decir, Los eNB/gNB (X2/Xn), por ejemplo, implementan IPsec cuando sea apropiado 6. Proteja la interfaz F1 y E1 en gNB con una implementación de DU-CU dividida
RN-002	**Impedir el seguimiento de usuarios** mediante el uso adecuado de identidades temporales de dispositivos, por ejemplo, antes de que el dispositivo se haya autenticado en la red	1. Utilizar identificadores temporales estándar definidos por 3GPP, por ejemplo, SUCI, TMSI, al transferir información de dispositivos no protegidos a través de la red
RN-003	Detectar ataques que puedan provocar inestabilidad en la red; **localizar actividades anómalas en la red**	1. Monitorear y responder a fluctuaciones de tráfico, patrones de traspaso inusuales, puntos muertos e interrupciones del servicio que puedan deberse a interferencias o estaciones base falsas [1][1] 2. Monitorear la distribución de los equipos de las estaciones base 3. Prevenir/detectar ataques de desvío de ofertas, autenticar en la medida de lo posible utilizando

Referencia	Objetivo	Descripción de la solución
		técnicas como las de IR.77 [2] y configurar los componentes de la red de radio para detectar la suplantación de identidad, el direccionamiento erróneo/enrutamiento erróneo y descartar el tráfico mal formado[2]
RN-004	Garantizar que las iniciativas de uso compartido de RAN **aíslen datos, usuarios y controlen el tráfico** correctamente	1. Diseñar una arquitectura RAN que incorpore la segregación adecuada de las diferentes clases de tráfico utilizando medios espectrales o lógicos 2. Segregar el tráfico de diferentes operadores mediante técnicas de aislamiento, por ejemplo, túneles seguros 3. Implementar marcos de utilización y contabilidad para compartir recursos 4. Probar rigurosamente todos los mecanismos de segregación 5. Garantizar que se conserven las características de calidad de servicio, priorización y preferencia del tráfico
RN-005	Garantizar la **seguridad y el mantenimiento de las estaciones base**	1. Garantizar que se implementen controles físicos de seguridad del sitio, por ejemplo, control de acceso a enlaces de comunicación de fibra, protección de la carcasa del equipo, componentes internos y configuraciones 2. Interfaces y canales de administración seguros 3. Garantizar que la comunicación entre los sistemas de O&M y el eNB/gNB sea confidencial, íntegra y esté protegida contra partes no autorizadas. Garantizar que las asociaciones de seguridad entre el eNb/gNB y una entidad en el núcleo 5G o en un dominio de O&M estén mutuamente autenticadas
RN-006	Cuando se despliegen **células pequeñas** en entornos hostiles, deben aplicarse controles compensatorios **para gestionar el riesgo** [32].**¡Error! No se**	1. Interfaces y canales de administración seguros 2. Garantizar que las celdas pequeñas sean inviolables y que la manipulación activa un sistema de alarma monitoreado

Referencia	Objetivo	Descripción de la solución
	encuentra el origen de la referencia.	3. Células pequeñas de origen con: a. Entorno de confianza b. Proceso de inicio confiable c. Verificación de ubicación d. Capacidad de aislamiento de red

Sugerencias para la solución de refuerzo de la administración de redes centrales

Referencia	Objetivo	Descripción de la solución
CN-001	Deben existir procesos para el **aprovisionamiento seguro y la baja de servicio de los usuarios**, a fin de garantizar que solo los clientes que se suscriban legítimamente tengan acceso a los servicios.	1. ID de usuario (sin comodines) 2. Vinculación correcta entre el cliente y el UE 3. Autentice cada usuario en cada conexión de red, actualización de ubicación, evento de tráfico, etc. 4. Implemente sistemas e iniciativas para conocer al cliente (KYC)
CN-002	**Proteger el tráfico de la red central (core)** después de su transferencia desde la ruta de radio para protegerlo contra la interceptación no autorizada y la alteración del tráfico de usuarios y de la información sensible de señalización**.**	1. Implementar cifrado para proteger la interfaz entre el eNodoB/gNodoB y la red core, por ejemplo, mediante IPsec 2. Habilitar los certificados de entidad final definidos en 3GPP TS 33.310 [3]**¡Error! No se encuentra el origen de la referencia.** 3. Gestionar activamente los firewalls GTP_U y GTP_C/SEPP entre la red core y la red IPX, descartando paquetes mal formados antes de que abandonen el núcleo [4]**¡Error! No se encuentra el origen de la referencia.**
CN-003	**Evite las escuchas, la eliminación y modificación no autorizadas del contenido del correo de voz,** la configuración y los saludos y el	1. Exigir el uso de PIN de acceso no obvios y de longitud variable [3][3] 2. Notificar a los clientes los intentos de acceso fallidos [3][3]

Referencia	Objetivo	Descripción de la solución
	estallido de llamadas para generar tráfico fraudulento.	3. Requerir la introducción del PIN para el acceso directo al correo de voz desde fuera de la red doméstica, excepto en los casos en que se pueda garantizar de forma fiable que el identificador de línea llamante es correcto [3][3] 4. Restringir el número de intentos de acceso al PIN independientemente del identificador de línea llamante [3][3] 5. Genere, distribuya y administre PIN de forma segura [3][3] 6. Establecer la frecuencia con la que se asigna un identificador temporal nuevo o de reemplazo para proporcionar una protección adecuada
CN-004	Utilice **técnicas de anonimización de clientes** para proteger identificadores que puedan utilizarse para identificar y rastrear clientes individuales.	1. Permitir el uso de identificadores temporales para los clientes, tal como se definen en las normas [5], [6][5][6]
CN-005	**Evitar que el tráfico de mensajería no solicitado (RCS, SMS y MMS)** llegue a clientes desprevenidos y cause daños potenciales a la red, incluyendo denegación de servicio a elementos de red.	1. Configure los SMSC, STP y firewalls de SMS disponibles para reducir el riesgo de ataques de SMS OTA [7], [9][7]**¡Error! No se encuentra el origen de la referencia.** 2. Implementar el enrutamiento local de SMS para garantizar la visibilidad y el control del tráfico de mensajería 3. Implementar capacidades de filtrado de tráfico en el GGSN, MMSC, SMSC, SMSF y/o STP de la red 4. Proporcionar capacidades de generación de informes y bloqueo de spam frente al cliente

Referencia	Objetivo	Descripción de la solución
CN-006	Para evitar actividades fraudulentas, se requiere una **conciliación periódica de los sistemas.**	1. Conciliar periódicamente los registros de datos de llamadas en conmutadores, sistemas de facturación, etc. 2. Realizar una conciliación periódica de los perfiles de abonado activos en redes y sistemas de facturación 3. Realizar una conciliación periódica de las suscripciones prepagadas designadas en plataformas de red inteligente
CN-007	**Controlar qué dispositivos pueden acceder** a la red para protegerse contra la conexión de dispositivos falsificados, robados y de baja calidad y los posibles impactos en la red que puedan tener.	1. Bloquear números IMEI/PEI duplicados o no válidos [8].[8] 2. Implementar el registro de identidades de equipos o tecnología equivalente capaz de monitorear y bloquear el uso de dispositivos individuales en función de sus IMEI [10]**¡Error! No se encuentra el origen de la referencia.** 3. Deben realizarse comprobaciones IMEI para confirmar la identificación del dispositivo antes de proporcionar acceso a la red móvil [8][8] 4. Valide los IMEI de los dispositivos mediante otras técnicas, como comprobaciones de perfil de agente de usuario del navegador.
CN-008	Los **procesos y herramientas utilizados para rastrear/controlar/prevenir/corregir el acceso seguro a activos críticos** (por ejemplo, infraestructura básica) según la determinación formal de qué personas, computadoras y aplicaciones tienen la necesidad y el derecho de acceder a estos activos	1. Hacer cumplir el principio de que solo las personas autorizadas deben tener acceso a la información en función de su necesidad de acceder a la información como parte de sus responsabilidades. 2. Deshabilite cualquier cuenta que no pueda asociarse con un proceso

Referencia	Objetivo	Descripción de la solución
	críticos según una clasificación aprobada.	empresarial o propietario de un negocio. 3. Asegúrese de que todas las cuentas tengan una fecha de caducidad supervisada y aplicada. Desactive automáticamente las cuentas inactivas después de un período establecido de inactividad. 4. Proteja toda la información almacenada en los sistemas con listas de control de acceso específicas para sistemas de archivos, recursos compartidos de red, reclamaciones, aplicaciones o bases de datos. 5. Aplicar un registro de auditoría detallado para el acceso a datos confidenciales o cambios en datos confidenciales.

7 Anexos

Identificar un plan para mejorar la madurez con el tiempo. Por ejemplo, un conjunto de controles más importantes podría ser objeto de mejoras en el año 1, otros controles mejorados en el año 2, dentro de un plan anual orientado a un nivel de madurez objetivo final para cada control. A continuación se indican las definiciones de los distintos niveles de vencimiento.

Marcado de madurez	Definición
N/D: no aplicable	El objetivo de control de seguridad básico GSMA no se aplica al Operador. Todas las respuestas «N/A» deben ir acompañadas de una explicación en la columna «Notas» correspondiente.
Nivel 0: ninguno	El control no está presente y aún no ha sido considerado para su implementación por el Operador. Todas las respuestas «Nivel 0» deben ir acompañadas de una explicación en la columna «Notas» correspondiente.
Nivel 1: Inicial	El Operador ha considerado el control para su implementación y ha llevado a cabo un análisis de las deficiencias del control en relación con la política y la práctica actuales. Puede haber una implementación ad hoc o localizada del control, pero el control no se soporta estratégicamente. Se ha preparado una hoja de ruta para mejorar el control a fin de aumentar el nivel de madurez hasta alcanzar un nivel de madurez objetivo aplicable. En la columna «Notas» correspondiente deberá

Marcado de madurez	Definición
	registrarse un esquema de la hoja de ruta y/o una referencia a ella.
Nivel 2: Repetible	El control ha comenzado a ser adoptado dentro de las políticas y prácticas del Operador. Se han realizado progresos en su aplicación y se incluye en un programa de trabajo detallado que está en marcha. Una junta del programa examina periódicamente los progresos realizados y, cuando se lleva a cabo el control, se ajusta a una norma coherente y repetible. Los progresos realizados en la aplicación del control de la hoja de ruta y los planes programáticos deben registrarse en la columna «Notas».
Nivel 3: Definido	El control se ha adoptado plenamente dentro de las políticas y prácticas del Operador. El control ha comenzado a integrarse en los procesos de gobernanza y gestión, pero aún no se ha completado. Los planes de recursos y capacitación abarcan la supervisión del control y han comenzado a aplicarse. Los avances en la aplicación del control de la hoja de ruta, el programa y los planes de recursos/formación deben registrarse en la columna «Notas».
Nivel 4: Gestionado	Los procesos de gobernanza y gestión que supervisan y operan el control ya están plenamente establecidos y cuentan en gran medida con personal debidamente capacitado y capacitado. Se elaboran planes para supervisar la eficacia del control y poner en marcha un proceso de revisión periódica y mejora del control. Esto incluye considerar la retroalimentación sobre la eficacia del control proveniente de investigaciones y exámenes de incidentes. Los avances en la aplicación del control de la hoja de ruta, los planes de programas/recursos/formación y los planes de revisión/mejora deben registrarse en la columna «Notas».
Nivel 5: Optimizado	Los procesos de revisión/mejora del control están integrados y funcionan con eficacia. (este nivel de vencimiento no debe reclamarse hasta que esos procesos hayan realizado varios ciclos de revisión, por ejemplo, seis meses o más) La supervisión del control ha pasado del modo de programación al modo habitual. El estado actual de la eficacia del control y los planes de mejora deben registrarse en la columna «Notas».

8 Referencias

Ref	Documento	Enlace
[1]	FF.21 Manual sobre el fraude	PRD FF.21
[2]	Req.77 de seguridad de red troncal IP de InterOperator Para proveedores de red troncal IP entre operadores y servicios	IR.77 del PRD
[3]	Pautas de seguridad del correo de voz SG.20	PRD SG.20
[4]	Seguridad del protocolo de túnel FS.20 GPRS (GTP)	Foro de células pequeñas: SCF171

Ref	Documento	Enlace
[5]	Sistema de telecomunicaciones celulares digitales (fase 2+); Sistema universal de telecomunicaciones móviles (UMTS); seguridad 3G; arquitectura de seguridad	ETSI TS 133 102
[6]	Evolución de la arquitectura del sistema (SAE) del 3GPP; arquitectura de seguridad	3GPP 33.401
[7]	Mejores prácticas y políticas de firewall de SMS	PRD SG.22
[8]	Lista negra de IMEI GSMA	Lista negra de IMEI GSMA
[9]	Especificaciones S@T de la Alianza de Conectividad Confiable	Especificaciones de S@T
[10]	Base de datos GSMA IMEI	Base de datos GSMA IMEI