Guía de buenas prácticas de **ciberseguridad para redes privadas 5G**

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

universidad de león

Guía de buenas prácticas de ciberseguridad para redes privadas 5G

Diciembre 2025

Contenido

Índice de figuras

Índice de tablas

Glosario de términos

#

- **3GPP (3rd Generation Partnership Project):** Es un consorcio de organismos de estandarización que desarrollan las especificaciones técnicas para las telecomunicaciones móviles, incluyendo las tecnologías 3G, 4G y 5G. Define la arquitectura de seguridad y los requisitos para los equipos de red.
- **5G-ACIA (5G Alliance for Connected Industry and Automation / Alianza 5G para la Industria Conectada y la Automatización)**: Organización que define escenarios de despliegue para redes privadas 5G integradas en redes públicas (PNI-NPN).
- **5GC (5G Core / Núcleo 5G)**: Es el "cerebro" de la red 5G, diseñado con una arquitectura basada en servicios (SBA) y nativa en la nube. Es responsable de todas las funciones de control, gestión de sesiones y enrutamiento del tráfico.

A

- **AGV (Automated Guided Vehicle / Vehículo Guiado Automático)**: Vehículos que se utilizan en entornos industriales, como fábricas o almacenes, para transportar materiales sin necesidad de un conductor. Las redes 5G privadas son ideales para controlarlos debido a su baja latencia y alta fiabilidad.
- **AMF (Access and Mobility Management Function / Función de Gestión del Acceso y la Movilidad)**: Es una función de red clave en el núcleo 5G. Actúa como punto de entrada para la señalización de los dispositivos, gestionando su registro en la red, la conexión, la movilidad entre distintas zonas de cobertura y la autenticación inicial.
- **AP (Access Point / Punto de Acceso)**: Dispositivo que crea una red de área local inalámbrica (WLAN), comúnmente usado en tecnologías como Wi-Fi. En el texto, se compara su cobertura limitada con la de las células 5G.
- **API (Application Programming Interface / Interfaz de Programación de Aplicaciones)**: Conjunto de reglas y herramientas que permiten que diferentes aplicaciones de software se comuniquen entre sí. En la arquitectura 5G, las funciones de red se comunican mediante APIs, lo que introduce una nueva superficie de ataque que debe protegerse.
- **AppSec (Application Security / Seguridad de Aplicaciones)**: Disciplina de la ciberseguridad centrada en proteger las aplicaciones contra amenazas mediante la identificación y corrección de vulnerabilidades en su diseño, desarrollo y despliegue. Es crucial para la seguridad 5G debido a su nueva arquitectura.
- **APT (Advanced Persistent Threat / Amenaza Persistente Avanzada)**: Tipo de ciberataque sigiloso y continuo, a menudo orquestado por actores sofisticados, en el que un atacante establece una presencia a largo plazo en una red para robar datos o espiar.
- **AUSF (Authentication Server Function / Función de Servidor de Autenticación)**: Función del núcleo 5G responsable de llevar a cabo la autenticación de un dispositivo, verificando sus credenciales para autorizar su acceso a la red. Colabora con la UDM para este fin.

C

- **CCB (Change Control Board / Comité de Revisión de Cambios)**: Grupo de personas, generalmente de diferentes áreas de una organización (seguridad, redes, operaciones), responsable de evaluar, aprobar o rechazar las solicitudes de cambio en la configuración de un sistema o en las líneas base de seguridad.
- **CI (Configuration Item / Elemento de Configuración)**: Cualquier componente de un sistema (hardware, software, documentación) que es gestionado para controlar su estado y configuración.
- **CIS (Center for Internet Security)**: Organización sin ánimo de lucro que desarrolla y promueve las mejores prácticas de ciberseguridad. Sus *CIS Benchmarks* son guías de configuración segura para diversos sistemas

y productos.

- **CNF (Cloud-native Network Function / Función de Red Nativa en la Nube)**: Funciones de red diseñadas específicamente para operar en un entorno de nube, utilizando tecnologías como contenedores y microservicios. El sistema MANO gestiona su ciclo de vida.
- **COTS (Commercial Off-The-Shelf / Comercial Estándar)**: Hardware o software que está disponible comercialmente y no está diseñado a medida. Las redes 5G pueden utilizar hardware COTS, lo que reduce costes pero requiere un enfoque de seguridad adaptado.
- **CU (Centralized Unit / Unidad Centralizada)**: En arquitecturas O-RAN, es uno de los dos componentes en los que se puede dividir una estación base 5G (gNB). Gestiona los protocolos de nivel superior y puede centralizarse para controlar varias Unidades Distribuidas (DU).
- **CUPS (Control and User Plane Separation / Separación del Plano de Control y de Usuario)**: Principio de diseño fundamental en la arquitectura del núcleo 5G que separa el tráfico de señalización (control) del tráfico de datos del usuario. Esta separación permite una mayor flexibilidad, como desplegar el plano de usuario cerca del dispositivo (*edge computing*) para reducir la latencia.

D

- **DDoS (Distributed Denial of Service / Denegación de Servicio Distribuida)**: Ataque en el que múltiples sistemas comprometidos se utilizan para sobrecargar un único sistema (como una estación base o un servidor) con tráfico, provocando que deje de funcionar para los usuarios legítimos.
- **DNN (Data Network Name / Nombre de Red de Datos)**: Identificador que especifica la red de datos a la que un dispositivo desea conectarse (p. ej., "internet" o "red_corporativa"). Es un parámetro clave para segmentar el tráfico y aplicar políticas de seguridad, similar al APN en 4G.
- **DRB (Data Radio Bearer / Portador de Radio de Datos)**: Túnel o canal lógico que se establece en la interfaz de radio para transportar los datos del usuario entre el dispositivo (UE) y la estación base (gNB) una vez que se ha establecido una sesión PDU.
- **DU (Distributed Unit / Unidad Distribuida)**: En arquitecturas O-RAN, es el componente de la estación base 5G que maneja las funciones de radio de bajo nivel, más cercanas a la señal física. Se controla desde una Unidad Centralizada (CU).

E

- **EAP-AKA' (Extensible Authentication Protocol - Revised Authentication and Key Agreement)**: Protocolo de autenticación mejorado utilizado en redes 5G. Permite una verificación segura de los dispositivos que se conectan a la red y es un estándar desarrollado por el IETF.
- **eMBB (enhanced Mobile Broadband / Banda Ancha Móvil Mejorada)**: Uno de los tres principales casos de uso de 5G, enfocado en proporcionar velocidades de datos muy altas y mayor capacidad. Es ideal para aplicaciones como la transmisión de vídeo en 4K/8K o la realidad aumentada.
- **EMS (Element Management System / Sistema de Gestión de Elementos)**: Sistema utilizado para la operación y mantenimiento de los elementos de una red de telecomunicaciones. Su compromiso puede dar a un atacante el control total sobre la red.
- **ENS (Esquema Nacional de Seguridad)**: Marco legal en España (Real Decreto 311/2022) que establece la política de seguridad en el uso de medios electrónicos. Exige medidas como la configuración segura y la gestión continua de la configuración.
- **ENS5G (Esquema Nacional de Seguridad de redes y servicios 5G)**: Desarrollo reglamentario específico para la seguridad 5G en España (Real Decreto 443/2024). Es de obligado cumplimiento para operadores y empresas que desplieguen redes 5G, tanto públicas como privadas.
- **EOS (End of Support / Fin de Soporte)**: Fecha a partir de la cual un fabricante deja de proporcionar soporte

técnico, actualizaciones de software o parches de seguridad para un producto. Gestionar la retirada de productos en EOS es crucial para la seguridad.

- **eSIM (embedded SIM / SIM embebida)**: Versión digital de una tarjeta SIM que está integrada en el propio dispositivo y puede programarse de forma remota, eliminando la necesidad de una tarjeta física.
- **ETSI (European Telecommunications Standards Institute / Instituto Europeo de Normas de Telecomunicaciones)**: Organismo de estandarización que desarrolla normas para las tecnologías de la información y la comunicación en Europa, incluyendo la arquitectura de virtualización (NFV MANO).

G

- **gNB / gNodeB (next-generation NodeB)**: Término técnico para una estación base 5G. Es el elemento de la red de acceso radioeléctrico (RAN) que se comunica de forma inalámbrica con los dispositivos de usuario (UE).
- **GSMA (GSM Association)**: Organización que representa los intereses de los operadores de redes móviles de todo el mundo. Publica documentos de referencia sobre ciberseguridad, como la *Mobile Cybersecurity Knowledge Base* (MCKB).

H

- **HIPS (Host Intrusion Prevention System / Sistema de Prevención de Intrusiones Basado en Host)**: Software de seguridad que se instala en un dispositivo o servidor individual para monitorizar su actividad en busca de comportamientos maliciosos y bloquearlos.
- **HMTC (High-Performance Machine-Type Communications / Comunicaciones de Tipo Máquina de Alto Rendimiento)**: Un tipo de servicio 5G estandarizado diseñado para comunicaciones entre máquinas que requieren un alto rendimiento, como en la automatización industrial avanzada.

I

- **IETF (Internet Engineering Task Force / Grupo de Trabajo de Ingeniería de Internet)**: Organización que desarrolla y promueve estándares de Internet, muchos de los cuales son fundamentales para el funcionamiento y la seguridad de las redes 5G, como IPsec o EAP-AKA'.
- **IMSI (International Mobile Subscriber Identity / Identidad Internacional de Abonado Móvil)**: Identificador único asociado a cada usuario de una red móvil. Su suplantación es una amenaza de seguridad que permite a dispositivos no autorizados acceder a la red.
- **IPsec (Internet Protocol Security)**: Conjunto de protocolos para asegurar las comunicaciones por Internet mediante la autenticación y el cifrado de cada paquete IP. Se usa en 5G para proteger el tráfico en segmentos no confiables de la red.
- **iSIM (integrated SIM / SIM integrada)**: Evolución de la eSIM donde la funcionalidad de la SIM está integrada directamente en el System-on-a-Chip (SoC) del dispositivo, ofreciendo mayor seguridad y eficiencia.

L

- **LADN (Local Area Data Network / Red de Datos de Área Local)**: Funcionalidad 5G que permite que el tráfico generado localmente (p. ej., dentro de una fábrica) permanezca dentro de la red local sin necesidad de salir a redes externas. Se configura mediante un DNN específico.
- **LMT (Local Maintenance Terminal / Terminal de Mantenimiento Local)**: Dispositivo utilizado por el personal técnico para configurar, gestionar y mantener los equipos de red directamente en su ubicación física.
- **LTE (Long-Term Evolution)**: Tecnología de comunicación móvil de cuarta generación (4G) que ofrece alta velocidad de transmisión de datos y baja latencia. Fue diseñada como evolución del 3G para mejorar la eficiencia de la red y la experiencia del usuario.

M

- **MANO (Management and Orchestration / Gestión y Orquestación)**: Marco, estandarizado por ETSI, que se encarga de automatizar la gestión del ciclo de vida de las funciones de red virtualizadas (NFV) en un entorno 5G, desde su despliegue hasta su finalización.
- **MCKB (Mobile Cybersecurity Knowledge Base / Base de Conocimientos sobre Ciberseguridad Móvil)**: Recurso de la GSMA que recopila información sobre amenazas, riesgos y mejores prácticas de seguridad para el ecosistema móvil, promoviendo un modelo de responsabilidad compartida.
- **MEC (Multi-access Edge Computing / Computación en el Borde de Múltiple Acceso)**: Arquitectura de red que acerca las capacidades de cómputo y almacenamiento al borde de la red, más cerca del usuario final. Esto reduce la latencia y es fundamental para aplicaciones en tiempo real, pero requiere medidas de seguridad específicas.
- **mMTC (massive Machine Type Communications / Comunicación Masiva de Tipo Máquina)**: Caso de uso de 5G diseñado para conectar una gran cantidad de dispositivos (hasta millones por kilómetro cuadrado) que transmiten pequeños volúmenes de datos, como sensores en entornos de Internet de las Cosas (Internet of Things, IoT).

N

- **NAS (Non-Access Stratum / Estrato de No Acceso)**: Capa de protocolo en las redes móviles que gestiona la comunicación de señalización entre el dispositivo (UE) y el núcleo de la red (específicamente, la AMF), independientemente de la tecnología de acceso radio. Se usa para procesos como el registro en la red.
- **NE (Network Element / Elemento de Red)**: Componente individual de la infraestructura de una red de telecomunicaciones, como una estación base, un router o una función del núcleo 5G.
- **NESAS (Network Equipment Security Assurance Scheme / Esquema de Garantía de Seguridad para Equipos de Red)**: Esquema de certificación estandarizado por la GSMA y el 3GPP para garantizar que los equipos de redes móviles cumplen con unos requisitos de seguridad y desarrollo seguro definidos.
- **NF (Network Function / Función de Red)**: En 5G, es un bloque funcional de la red que proporciona una capacidad específica. En la arquitectura 5G, las NFs se implementan como software (virtualizadas o en contenedores) y se comunican entre sí a través de APIs.
- **NFV (Network Functions Virtualization / Virtualización de Funciones de Red)**: Paradigma tecnológico que consiste en separar las funciones de red (como el enrutamiento o el balanceo de carga) del hardware dedicado y ejecutarlas como software en hardware comercial estándar (COTS). Es un pilar de la arquitectura 5G.
- **NG-RAN (Next-Generation Radio Access Network / Red de Acceso Radioeléctrico de Nueva Generación)**: Es la red de acceso radioeléctrico específica de 5G, compuesta principalmente por estaciones base gNodeB.
- **NIPS (Network Intrusion Prevention System / Sistema de Prevención de Intrusiones en Red)**: Dispositivo de seguridad que monitoriza el tráfico de una red para detectar y bloquear actividades maliciosas o violaciones de políticas de seguridad.
- **NIS2 (Network and Information Security Directive 2 / Directiva de Seguridad de Redes y Sistemas de Información 2)**: Directiva de la Unión Europea (UE 2022/2555) que establece obligaciones de ciberseguridad para una amplia gama de sectores considerados "esenciales" o "importantes", incluyendo las redes 5G públicas.
- **NPN (Non-Public Network / Red No Pública)**: Término técnico utilizado por el 3GPP para referirse a una red privada 5G.
- **NR (New Radio)**: Especificación de la interfaz de radio del 5G. Es la tecnología que permite la comunicación inalámbrica entre los dispositivos y las estaciones base gNodeB.

- **NRF (Network Repository Function / Función de Repositorio de Red)**: Función del núcleo 5G que actúa como un catálogo o registro de servicios. Permite que las funciones de red (NF) se descubran dinámicamente entre sí, facilitando la arquitectura basada en servicios.
- **NSA (Non-Standalone / No Autónoma)**: Uno de los dos modos de despliegue de 5G, donde la infraestructura 5G depende de una red 4G existente para gestionar funciones como el control de señalización y el acceso. Esto permite una transición más rápida hacia 5G sin necesidad de desplegar toda la red 5G desde el inicio.
- **NSSAI (Network Slice Selection Assistance Information / Información de Ayuda a la Selección de Segmento de Red)**: Parámetro que un dispositivo utiliza para solicitar el acceso a un *slice* o segmento de red específico. Es fundamental para implementar el *network slicing*.

O

- **O&M (Operation and Maintenance / Operación y Mantenimiento)**: Conjunto de tareas y procesos necesarios para gestionar, supervisar y mantener una red en funcionamiento. La seguridad en O&M es un aspecto crítico que abarca desde la gestión de acceso del personal hasta la auditoría de configuraciones.
- **O-RAN (Open RAN / RAN Abierta)**: Iniciativa de la industria que promueve arquitecturas de red de acceso radio abiertas e interoperables, permitiendo que los componentes de diferentes proveedores (como CU y DU) funcionen juntos.
- **OT (Operational Technology / Tecnología de Operación)**: Conjunto de sistemas y dispositivos utilizados para monitorizar, controlar y gestionar procesos físicos en entornos industriales, como fábricas, plantas de energía o infraestructuras críticas. Abarca equipos como sensores, controladores y sistemas SCADA, diferenciándose de la Tecnología de la Información (IT) por su enfoque en operaciones físicas y en tiempo real. La integración de 5G con sistemas OT en entornos industriales amplía la superficie de ataque.

P

- **PCF (Policy Control Function / Función de Control de Políticas)**: Función del núcleo 5G que proporciona un marco unificado para definir y aplicar políticas de red, como las reglas de calidad de servicio (QoS) o las políticas de tarificación para las diferentes sesiones de datos.
- **PDU (Packet Data Unit / Unidad de Datos de Paquete)**: En el contexto 5G, una "sesión PDU" es una conexión de datos que se establece entre un dispositivo y una red de datos externa (como Internet o una red corporativa). El proceso de establecimiento de esta sesión es un flujo de señalización fundamental.
- **PKI (Public Key Infrastructure / Infraestructura de Clave Pública)**: Sistema de hardware, software, políticas y procedimientos necesarios para crear, gestionar, distribuir, usar, almacenar y revocar certificados digitales. Se utiliza en 5G para la autenticación mutua entre componentes de red.
- **PLMN (Public Land Mobile Network / Red Móvil Terrestre Pública)**: Red de telecomunicaciones establecida y operada por un operador para proporcionar servicios móviles al público en general. Las redes privadas SNPN son independientes de las PLMN.
- **PNI-NPN (Public Network Integrated Non-Public Network / Red No Pública Integrada en la Red Pública)**: Un modelo de despliegue de red privada 5G en el que la red privada comparte parte de la infraestructura de una red pública, como la red de acceso (RAN) o el plano de control.

R

- **RAN (Radio Access Network / Red de Acceso Radioeléctrico)**: Parte de un sistema de telecomunicaciones móviles que conecta los dispositivos de los usuarios a la red principal (core network). En 5G, se denomina NG-RAN y está formada por las estaciones base gNB.
- **RBAC (Role-Based Access Control / Control de Acceso Basado en Roles)**: Modelo de seguridad en el que el acceso a los recursos se asigna a los usuarios en función de sus roles dentro de una organización. Es una práctica recomendada para aplicar el principio de mínimo privilegio.

- **RRC (Radio Resource Control / Control de Recursos de Radio)**: Protocolo utilizado en la interfaz de radio para gestionar la señalización entre el dispositivo y la estación base. Se encarga de establecer, mantener y liberar la conexión de radio.

S

- **SA (Standalone / Autónoma)**: El modo de despliegue completo y definitivo de 5G, que utiliza tanto una red de acceso radio 5G (NR) como un núcleo de red 5G (5GC), operando de forma independiente de las redes 4G.
- **SBA (Service-Based Architecture / Arquitectura Basada en Servicios)**: El modelo de diseño del núcleo 5G (5GC), en el que las funciones de red se descomponen en un conjunto de servicios modulares que se comunican entre sí a través de APIs. Esto proporciona flexibilidad y escalabilidad, pero también crea nuevos vectores de ataque.
- **SCAS (Security Assurance Specifications / Especificaciones de Garantía de Seguridad)**: Conjunto de documentos definidos dentro del marco NESAS (Network Equipment Security Assurance Scheme) que especifican los requisitos técnicos de seguridad y las pruebas necesarias para certificar los equipos de red, garantizando que cumplan con los estándares de seguridad establecidos por el 3GPP..
- **SD (Slice Differentiator / Diferenciador de Segmento)**: Identificador que forma parte del S-NSSAI. Permite distinguir entre diferentes segmentos de red (*slices*) que comparten el mismo tipo de servicio (SST).
- **SDN (Software Defined Networks / Redes Definidas por Software)**: Enfoque de la arquitectura de red que permite que la red sea controlada de forma inteligente y centralizada mediante software, desacoplando el plano de control del plano de datos. La complejidad de esta arquitectura produce también un incremento en la posible superficie de ataque en entornos de redes 5G.
- **SIEM (Security Information and Event Management / Gestión de Eventos e Información de Seguridad)**: Sistema que recopila, agrega y analiza datos de eventos y registros de múltiples fuentes (dispositivos de red, servidores, etc.) para detectar amenazas de seguridad y facilitar la respuesta a incidentes.
- **SIM (Subscriber Identity Module / Módulo de Identidad del Suscriptor)**: Es un dispositivo que almacena la información necesaria para identificar y autenticar a un abonado en una red móvil. En 5G, puede presentarse en tres formas: física (SIM), embebida (eSIM) o integrada (iSIM), adaptándose a diferentes necesidades de conectividad y gestión.
- **SMF (Session Management Function / Función de Gestión de Sesiones)**: Función del núcleo 5G responsable de establecer, modificar y liberar las sesiones de datos de los usuarios (sesiones PDU). Asigna direcciones IP y selecciona el UPF adecuado para enrutar el tráfico.
- **S-NSSAI (Single-NSSAI)**: Identificador único para un solo segmento de red (*network slice*). Está compuesto por un tipo de servicio (SST) y, opcionalmente, un diferenciador de segmento (SD).
- **SNPN (Stand-alone Non-Public Network / Red No Pública Independiente)**: Es un tipo de red privada 5G que es completamente autónoma y no depende de ninguna función de una red pública.
- **SOC (Security Operations Center / Centro de Operaciones de Seguridad)**: Equipo centralizado que se encarga de monitorizar y mejorar la postura de seguridad de una organización, así como de prevenir, detectar, analizar y responder a incidentes de ciberseguridad.
- **SST (Slice/Service Type / Tipo de Segmento/Servicio)**: Valor numérico estandarizado que define el tipo de servicio principal para el que está optimizado un segmento de red (*slice*), como eMBB (valor 1), URLLC (valor 2) o mMTC (valor 3).

U

- **UDM (Unified Data Management / Gestión Unificada de Datos)**: Función del núcleo 5G que almacena de forma segura los datos de suscripción de los usuarios, incluyendo perfiles de servicio, políticas de acceso y credenciales de autenticación. Es consultada por la AMF y la SMF durante los procesos de registro y

establecimiento de sesión.

- **UE (User Equipment / Equipo de Usuario)**: Término genérico para cualquier dispositivo que se conecta a una red 5G. En redes privadas, puede ser un sensor, un robot, una cámara de seguridad, un AGV o un smartphone, entre otros.
- **UPF (User Plane Function / Función de Plano de Usuario)**: Es la función del núcleo 5G que se encarga de procesar el tráfico de datos del usuario. Sus tareas incluyen el enrutamiento y reenvío de paquetes, la inspección de tráfico y la aplicación de políticas de calidad de servicio (QoS).
- **URLLC (Ultra-Reliable and Low-Latency Communications / Comunicaciones Ulrafiables y de Baja Latencia)**: Caso de uso de 5G diseñado para aplicaciones críticas que requieren una comunicación casi instantánea y una fiabilidad extremadamente alta, como el control de robots industriales o los vehículos autónomos.

V

- **V2X (Vehicle-to-Everything / Vehículo a Todo)**: Tipo de comunicación que permite a los vehículos intercambiar información con otros vehículos, con la infraestructura vial y con peatones. Es un caso de uso de 5G relevante para la logística y el transporte.
- **VIM (Virtualized Infrastructure Manager / Gestor de Infraestructura Virtualizada)**: Componente del marco MANO que controla y gestiona los recursos de computación, almacenamiento y red de la infraestructura subyacente (p. ej., un clúster de Kubernetes) sobre la que se ejecutan las funciones de red virtualizadas.
- **VLAN (Virtual Local Area Network / Red de Área Local Virtual)**: Tecnología que permite segmentar una red física en múltiples redes lógicas independientes. Se utiliza para aislar el tráfico y mejorar la seguridad.
- **VM (Virtual Machine / Máquina Virtual)**: Emulación por software de un sistema informático completo. Las funciones de red 5G pueden desplegarse como VMs, aunque es más común el uso de contenedores.
- **VNFM (VNF Manager / Gestor de VNF)**: Componente del marco MANO responsable de gestionar el ciclo de vida de las funciones de red virtualizadas (VNF) individuales, incluyendo su creación, actualización y terminación.
- **VPN (Virtual Private Network / Red Privada Virtual)**: Tecnología que crea una conexión segura y cifrada a través de una red menos segura, como Internet. Se recomienda su uso para el acceso remoto a la red.
- **VXLAN (Virtual Extensible LAN)**: Tecnología de virtualización de red diseñada para superar las limitaciones de escala de las VLAN en entornos de centros de datos a gran escala. Permite crear redes lógicas aisladas sobre una infraestructura física compartida.

Capítulo 1: Introducción al ecosistema 5G

1.1 Tecnología 5G y redes privadas 5G

El despliegue de la tecnología 5G está impulsando una nueva generación de conectividad inalámbrica, con un potencial transformador para industrias y empresas. A la vanguardia de esta evolución se encuentran las **redes privadas 5G**: redes móviles personalizadas diseñadas para satisfacer las necesidades específicas de rendimiento, control y seguridad de una organización. A diferencia de los sistemas inalámbricos tradicionales, las redes privadas 5G ofrecen características mejoradas como ultra baja latencia, alta fiabilidad, segmentación lógica de red de extremo a extremo (network slicing) y soporte para comunicaciones masivas de tipo máquina. Estas capacidades las hacen ideales para entornos que requieren respuesta en tiempo real, transmisión segura de datos y gestión escalable de dispositivos.

La principal distinción entre redes 5G privadas y públicas radica en el grado de propiedad, personalización y gobernanza. Las redes públicas están gestionadas por operadores de telecomunicaciones y se construyen para el acceso general en amplias zonas geográficas (ejemplo: todo el país); dan servicio millones de usuarios simultáneamente (ejemplo: operadores de redes públicas a nivel nacional) y ofrecen una capacidad limitada de personalización o niveles de rendimiento garantizados. En cambio, las redes privadas se construyen para una organización concreta, con control sobre el acceso de los usuarios, la autenticación de los dispositivos, los flujos de tráfico y las políticas de seguridad, lo que permite una mayor precisión, garantía sobre el rendimiento y resiliencia en las aplicaciones críticas de la empresa.

Una amplia gama de industrias puede beneficiarse de las redes privadas 5G. En la fabricación avanzada, el 5G privado soporta vehículos guiados automatizados, control de calidad en tiempo real y comunicación de máquina a máquina en la planta de producción. En logística, mejora la automatización de almacenes y el seguimiento de activos. En energía y servicios públicos, permite el mantenimiento predictivo de infraestructuras remotas y la comunicación segura en entornos de difícil acceso físico o aislados. Las organizaciones sanitarias pueden utilizar la 5G privada para conectar dispositivos médicos, apoyar diagnósticos remotos o garantizar una transmisión de datos segura y de alta velocidad.

Sin embargo, este cambio también introduce nuevos retos de seguridad. La flexibilidad y complejidad del 5G privado -especialmente cuando se integra con entornos de TI, OT y nube- amplían la superficie de ataque y exigen medidas de seguridad especializadas. Esta guía proporciona un marco práctico de mejores prácticas para ayudar a las organizaciones a desplegar y operar redes privadas 5G con confianza y resiliencia desde una perspectiva de ciberseguridad.

1.2 Redes privadas 5G: Ventajas y oportunidades estratégicas

Como se ha mencionado anteriormente, el objetivo de la tecnología 5G no se limita a servir de infraestructura para la red pública de comunicaciones móviles, sino que pretende servir de base

para la creación de redes privadas. Una red 5G privada es una infraestructura de red, incluida la red de acceso radioeléctrico y el núcleo de red, que se dedica al uso exclusivo de una sola entidad, como una empresa, una fábrica o un campus universitario. A diferencia de las redes públicas, que son un recurso compartido entre millones de abonados, una red privada da a la organización pleno control sobre sus recursos, políticas de seguridad y calidad de servicio.

Estas redes ofrecen diferentes ventajas estratégicas sobre otras tecnologías de conectividad inalámbrica, como Wi-Fi o LTE privada (véase la tabla 1.1), lo que las posiciona como una solución superior para casos de uso complejos o exigentes. A diferencia de Wi-Fi 6/6E, cuyo acceso al medio puede provocar latencias impredecibles, 5G garantiza un rendimiento determinista y una fiabilidad constante, lo que resulta crucial para aplicaciones como la robótica o los vehículos guiados automatizados, con menor tolerancia a fallos. Además, gestiona la movilidad a alta velocidad con transiciones fluidas entre celdas y proporciona una cobertura de mayor alcance y homogénea en grandes áreas abiertas como puertos o en interiores como plantas de fabricación. Su seguridad, basada en una autenticación robusta mediante SIM, es superior al uso de credenciales tradicionales de Wi-Fi. Mientras que 4G se optimizó para la banda ancha móvil (“internet para las personas”), 5G introduce una arquitectura más flexible basada en el tipo de servicios ofrecidos "en la nube" (internet para personas, internet para dispositivos/máquinas, redes privadas, redes híbrídas, etc), una tecnología de enlace radioeléctrico más eficiente y una latencia significativamente menor.

El valor de una red 5G privada radica no solo en su velocidad, sino en su capacidad para ofrecer **un control determinista** de la conectividad. Esta capacidad de garantizar latencias específicas, anchos de banda y niveles de fiabilidad (SLAs) supone un cambio de paradigma que posibilita nuevos casos de uso, como la inspección remota con drones de alta definición, la automatización de procesos logísticos en puertos, la creación de "gemelos digitales" de fábricas enteras para simulación y optimización, o el mantenimiento predictivo basado en la recopilación masiva de datos de sensores en tiempo real.

Tabla 1.1: Comparación de tecnologías de redes privadas: 5G SA vs. LTE Privada vs. Wi-Fi 6/6E

Característica	5G SA Privada	Privada LTE	Wi-Fi 6/6E
Latencia	Muy baja (<5 ms)	Baja (10-20 ms)	Variable (depende de la congestión y sobre todo la cobertura)
Fiabilidad	Fiabilidad del 99.999% garantizada como requisito en escenarios URLLC	Alta	Media
Movilidad	Excelente (alta velocidad)	Buena	Limitada (transferencias complejas)
Cobertura	Amplia (kms por célula)	Amplia (kms por célula)	Limitada (decenas de metros por AP)
Seguridad	Muy alta (basada en SIM/eSIM)	Alta (basada en SIM)	Media (basada en credenciales)
Espectro	Licenciado / Compartido	Licenciado / Compartido	Sin licencia

Determinismo	Alto (acceso planificado)	Medio-alto	Bajo (acceso por contención)

1.3 Selección del modo de despliegue de la red privada 5G

3GPP[1] (3rd Generation Partnership Project) define dos tipos de redes privadas 5G: red no pública independiente (stand-alone non-public network, SNPN) y red no pública integrada en la red pública (public network integrated non-public network , PNI-NPN). La SNPN se refiere a una red privada que no depende de las funciones de red proporcionadas por la red pública terrestre móvil (public land mobile network, PLMN), como se muestra en la siguiente figura 1.1.[2]

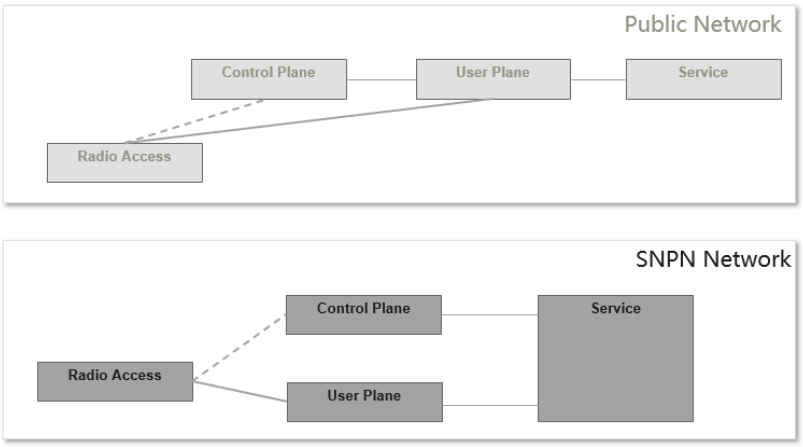


Figura 1.1 Esquema de una red no pública independiente (SNPN)

Una PNI-NPN es una red privada que proporciona funciones de red compartiendo algunas de las infraestructuras de red pública de una empresa. La Alianza 5G para la Industria Conectada y la Automatización (5G Alliance for Connected Industry and Automation, 5G-ACIA) ofrece tres escenarios típicos de despliegue de PNI-NPN.[3]

El primer escenario es una PNI-NPN con red de acceso radioeléctrico (RAN) compartida (figura 1.2), en la que una parte de la RAN es utilizada tanto por la organización empresarial como por el operador móvil, mientras que todas las demás funciones de red están aisladas entre sí, como en el caso de la SNPN.

[1] 3GPP es un consorcio de organizaciones que desarrolla los estándares mundiales para las tecnologías de comunicación móvil, incluidas las especificaciones para las redes 5G
[2] https://www.3gpp.org/technologies/npn
[3] https://5g-acia.org/insight/whitepapers/

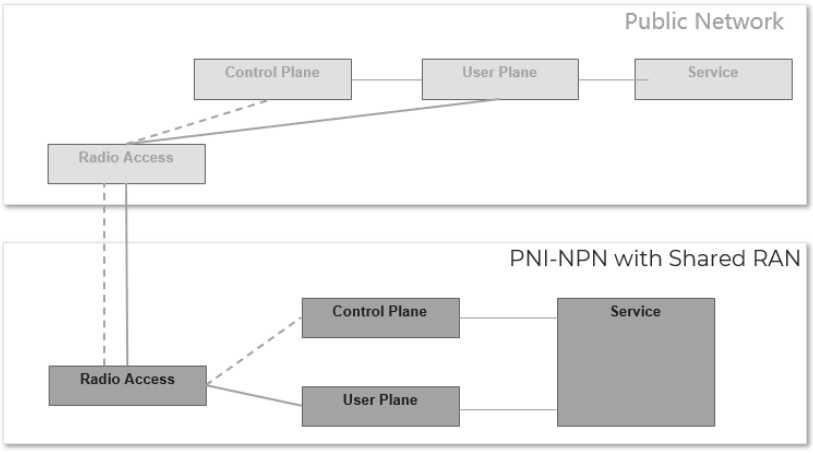


Figura 1.2 PNI-NPN con RAN compartida

El segundo escenario es el despliegue de una RAN y un plano de control compartidos (figura 1.3), donde no sólo se comparte la RAN, sino que las tareas de control de la red también son realizadas por la red pública.

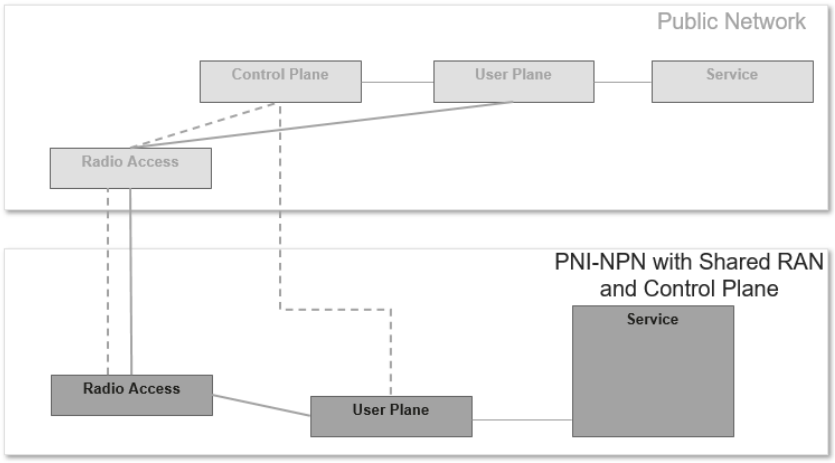


Figura 1.3 PNI-NPN con RAN y plano de control compartidos

En el tercer escenario, la red no pública (NPN) se despliega sobre la red pública y utiliza el enlace de extremo a extremo de esta para prestar los servicios de la NPN.

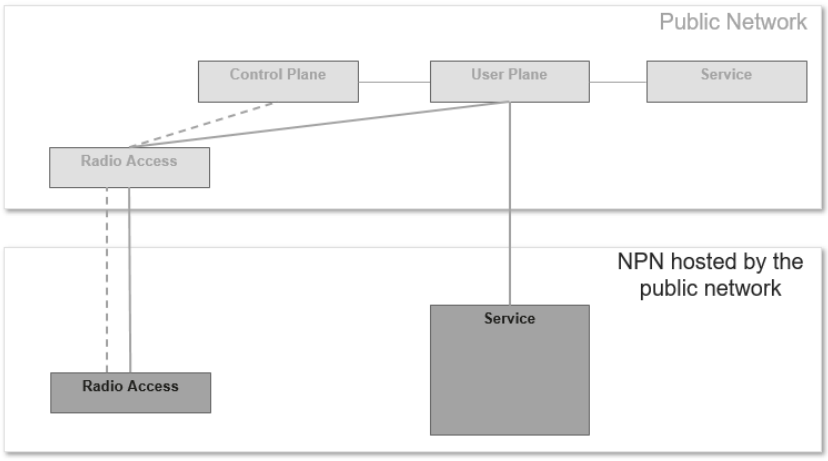


Figura 1.4 NPN alojada en la red pública

La introducción de las redes privadas 5G conlleva una amplia gama de amenazas y desafíos en ciberseguridad. Para clarificar el objetivo, esta guía utiliza la SNPN como objeto de análisis.

1.4 Principales avances de la tecnología 5G

La red 5G en modo standalone (SA) abandona el modelo monolítico y basado en hardware propietario de las generaciones anteriores para adoptar plenamente los paradigmas tecnológicos del cloud computing y del mundo de las tecnologías de la información (TI). Esta convergencia es lo que dota al 5G de su flexibilidad y potencia, pero también redefine en gran medida su superficie de ataque en lo que respecta a la ciberseguridad.

Los pilares de la transformación tecnológica del 5G son:

- **Virtualización de Funciones de Red (NFV, Network Functions Virtualization):** En una red 5G, funciones de red como la movilidad, la gestión de sesiones o la autenticación dejan de ser elementos físicos dedicados para convertirse en funciones software que se ejecutan sobre hardware comercial estándar (COTS, Commercial Off-The-Shelf). Esta virtualización, ya sea en forma de máquinas virtuales (VMs) o, más comúnmente, como contenedores, permite una agilidad sin precedentes, reduce los costes de capital (CapEx) y de operación (OpEx), y acelera el despliegue de nuevos servicios.

- **Arquitectura Basada en Servicios (SBA, Service Based Architecture):** El núcleo de la red 5G (5G Core, 5GC) está diseñado siguiendo el modelo de arquitectura basada en servicios. Esto implica que las funciones de red monolíticas se descomponen en un conjunto de servicios modulares. Cada función expone sus capacidades a otras mediante interfaces de programación de aplicaciones (APIs) bien definidas. En lugar de protocolos de señalización punto a punto y complejos como en redes anteriores, la comunicación entre funciones en 5GC se realiza mayoritariamente a través de estas APIs, que suelen ser RESTful y emplear protocolos estándar de Internet como HTTP/2 sobre TCP/IP.

- **Diseño Nativo en la Nube y Microservicios:** Las funciones de red en 5G se conciben como aplicaciones nativas en la nube. Esto significa que están diseñadas desde el inicio para ejecutarse en entornos cloud (públicos, privados o híbridos). Estas funciones se descomponen en microservicios aún más pequeños e independientes, cada uno encargado de una tarea específica. Los microservicios se empaquetan en contenedores ligeros (por ejemplo, Docker) y se gestionan y orquestan mediante plataformas como Kubernetes. Este enfoque permite que la red sea resiliente, escalable y ágil.

Una de las consecuencias de esta profunda transformación tecnológica es que la superficie de ataque de una red 5G se ha desplazado. Ya no se limita únicamente a los protocolos de telecomunicaciones, sino que abarca toda la pila tecnológica TI: desde vulnerabilidades en APIs web y contenedores, hasta errores de configuración en orquestadores como Kubernetes, pasando por riesgos en la cadena de suministro del software. Por tanto, la ciberseguridad en redes 5G no puede abordarse únicamente desde el conocimiento de los estándares 3GPP; requiere también la aplicación de disciplinas como la seguridad de aplicaciones (AppSec), la seguridad en la nube (Cloud Security) y la seguridad de la cadena de suministro de software.

1.5 Importancia de la ciberseguridad en las redes 5G públicas y privadas

La ciberseguridad no es una funcionalidad añadida en las redes 5G, sino un pilar fundamental de su diseño y operación. La propia naturaleza de esta tecnología, junto con los casos de uso que habilita, incrementa drásticamente tanto la probabilidad como el impacto potencial de un ciberataque. La convergencia con tecnologías TI, aunque aporta flexibilidad, también introduce sus vulnerabilidades en la infraestructura de telecomunicaciones.

La superficie de ataque se ha ampliado de forma generalizada. La proliferación de miles de millones de dispositivos IoT, muchos de ellos con capacidades de seguridad limitadas, crea infinidad de puntos de entrada potenciales para atacantes. La integración del 5G con infraestructuras críticas nacionales, como redes eléctricas, sistemas de transporte o instalaciones sanitarias, implica que un incidente de seguridad podría tener graves consecuencias para la seguridad pública y la economía. Amenazas como la manipulación de datos en tiempo real, antes consideradas teóricas, se vuelven críticas en entornos URLLC (comunicaciones ultrafiables y de baja latencia), donde un vehículo autónomo o un robot quirúrgico dependen de la integridad de los datos para tomar decisiones en milisegundos.

Además, la complejidad de la arquitectura 5G, basada en la virtualización, las redes definidas por software (Software Defined Networks, SDN) y el uso de software de múltiples proveedores, aumenta el riesgo de errores y malas configuraciones que pueden ser aprovechados por atacantes. Las redes privadas, aunque operan en entornos más controlados, no son inmunes. La responsabilidad de la seguridad recae directamente sobre la empresa o el operador que despliega la red, y la seguridad ya no se limita a la red en sí, sino que debe extenderse a todos los dispositivos, aplicaciones y cargas de trabajo que la utilizan.

Las arquitecturas 5G modernas requieren modelos de seguridad que trasciendan las defensas perimetrales tradicionales, incorporando controles más profundos, adaptativos y distribuidos en

toda la red. En un ecosistema 5G, donde las funciones están a menudo virtualizadas, repartidas entre centros de datos distribuidos (Edge: borde de la red local o cercano al dispositivo conectado) y o centralizados en la nube (Cloud privado, público o híbrido), y donde el tráfico entre microservicios (tráfico este-oeste) es constante, el concepto de un perímetro que separa una red interna "confiable" de una externa "no confiable" tiende a desvanecerse. Un atacante que comprometa una sola función de red podría moverse lateralmente para atacar otras si existe confianza implícita entre ellas.

Por este motivo, el modelo de seguridad considerado adecuado para las redes 5G es el de Confianza Cero (Zero Trust). Este paradigma, formalizado en documentos como la Publicación Especial SP 800-207[4] del NIST (y que también está siendo adoptado en toda la normativa europea de ciberseguridad), parte del principio de que ninguna solicitud de acceso debe ser considerada confiable por defecto, independientemente de su origen; cada intento de comunicación debe ser explícitamente verificado y autorizado. Esto implica la aplicación de principios como la autenticación mutua estricta en todas las comunicaciones, la microsegmentación para aislar componentes de red, y la aplicación de políticas de acceso de mínimo privilegio.

1.6 Panorama de las normas y recomendaciones de seguridad

La ciberseguridad 5G es un campo complejo y en evolución, respaldado por el trabajo de múltiples organismos de estandarización y agencias de seguridad. Para los operadores y administradores de red, es esencial conocer las principales fuentes de referencia que guían el diseño y la implementación de los controles de seguridad. En la Tabla 1.2 se enumeran los principales organismos de ciberseguridad en el ámbito de la tecnología 5G, junto con alguno de los documentos clave o marcos de referencia que han publicado.

Tabla 1.2: Organismos de normalización y documentos de referencia en ciberseguridad 5G

Organismo	Documento/marco clave	Área de interés principal
3GPP (3rd Generation Partnership Project)	Especificaciones técnicas (por ejemplo, TS 33.501), SCAS (Security Assurance Specifications)	Definición de arquitectura de seguridad y requisitos técnicos para equipos de red.
GSMA (GSM Association)	MCKB (Mobile Cybersecurity Knowledge Base), como FS.30 y FS.31, etc.	Amenazas a las redes móviles, directrices prácticas y controles de seguridad básicos para operadores de redes móviles.
ENISA (Agencia de Ciberseguridad de la UE)	Panorama de las amenazas para las redes 5G, caja de herramientas de la UE para la seguridad 5G.	Análisis de amenazas, evaluación de riesgos y coordinación de políticas de seguridad a escala europea.
ETSI (Instituto Europeo de Normas de Telecomunicaciones)	NFV MANO (Gestión y Orquestación)	Estandarización de la arquitectura para la virtualización de las funciones de red.
UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT)	Recomendaciones de la serie X	Normas mundiales sobre diversos aspectos de la seguridad de las telecomunicaciones.

[4] https://csrc.nist.gov/pubs/sp/800/207/final

Cabe mencionar que otras organizaciones, como el **IETF** (Internet Engineering Task Force), dedicado al desarrollo de estándares técnicos para Internet, desempeñan un papel muy relevante en la tecnología 5G, dada la importancia que tiene Internet en esta nueva generación de comunicaciones móviles.

En este sentido, el IETF ha desarrollado y adaptado diversos estándares clave para la seguridad en arquitecturas 5G, entre los que se destacan:

- **IPSec**: utilizado para cifrar y autenticar el tráfico en segmentos no confiables del sistema 5G, como las redes de transporte (o transmisión de datos) entre el acceso y el núcleo de la red (centros de datos distribudios en el Edge o en la nube), que a veces de denominan en inglés backhaul o backbone de la red, dependiendo del nivel de agregación de tráfico.

- **EAP-AKA'** (Extensible Authentication Protocol - Revised Authentication and Key Agreement): especificado en el RFC 9048, es la versión mejorada del protocolo EAP-AKA, utilizado en 5G para permitir una autenticación segura de dispositivos.

- Extensiones de **certificados X.509** para funciones de red.

1.7 Marco regulador de la ciberseguridad 5G en Europa y España

Más allá de las recomendaciones técnicas, la implantación de medidas de ciberseguridad en las redes 5G está sujeta a un marco legal cada vez más estricto, tanto a nivel europeo como nacional. El hecho de que las redes públicas de comunicaciones móviles sean consideradas infraestructuras críticas ha propiciado un rápido desarrollo normativo para garantizar la seguridad de las redes 5G en previsión de su adopción generalizada.

A nivel europeo, **la Directiva (UE) 2022/2555 (NIS2)** amplía el alcance de las obligaciones de ciberseguridad existentes a una gama más amplia de sectores y entidades, clasificando a éstas como "esenciales" e "importantes", incluyendo entre los sectores de alta criticidad (Anexo I de NIS2) a las infraestructuras digitales como las redes públicas 5G. La NIS2 exige a las entidades afectadas que adopten medidas adecuadas de gestión de riesgos de ciberseguridad, incluida la seguridad de la cadena de suministro, y establece una responsabilidad explícita para los órganos de gestión en caso de incumplimiento.

En España se ha desarrollado una legislación específica que desarrolla estas directrices europeas y establece un marco de seguridad para las redes 5G. Las dos referencias fundamentales son:

1. **Real Decreto-Ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación.** Conocida como "Ley de Ciberseguridad 5G", esta norma establece el marco general de obligaciones para los operadores y proveedores implicados en el despliegue y explotación de redes 5G en España. Incorpora la Recomendación (UE)

2019/534[5] y la caja de herramientas 5G de la Comisión Europea[6], y fija objetivos como impulsar la seguridad integral del ecosistema 5G, reforzar la protección de la seguridad nacional y diversificar la cadena de suministro.

2. **Real Decreto 443/2024, de 30 de abril, por el que se aprueba el Esquema Nacional de Seguridad de redes y servicios 5G (ENS5G).** Este real decreto es el desarrollo reglamentario de la ley anterior y constituye el núcleo de la regulación de la seguridad 5G en España. Sus objetivos son reforzar la seguridad nacional y garantizar la seguridad y el funcionamiento continuo de estas redes. El ENS5G se aplica a los operadores de redes públicas 5G, a los proveedores de equipos y software 5G y a las empresas usuarias de redes privadas 5G. Asimismo, establece la creación del Centro de Operaciones de Seguridad 5G (SOC 5G), entidad nacional encargada de dar soporte operativo a los sujetos obligados en las actividades de prevención, protección, detección y respuesta ante amenazas, incidentes y ciberataques que afecten a los sistemas, redes y servicios 5G.

1.8 Objetivos y estructura de la guía

El objetivo de esta guía es proporcionar un marco de buenas prácticas, con un enfoque didáctico, pero técnicamente riguroso, para el despliegue y gestión segura de redes 5G SNPN. Está dirigida a los operadores de este tipo de redes y al personal técnico de las empresas e industrias que las implementan, con el fin de ayudarles a comprender la tecnología, identificar los riesgos de seguridad e implementar los controles adecuados para mitigarlos, cumpliendo con el marco normativo vigente.

La guía se estructura en los siguientes capítulos. Tras esta introducción, el **Capítulo 2** detallará la arquitectura y el funcionamiento básico de una red 5G standalone, presentando sus componentes y explicando los flujos de comunicación fundamentales. El **Capítulo 3** expone las amenazas de ciberseguridad que pueden darse en una red privada 5G, así como la arquitectura de seguridad y las principales medidas que un operador de este tipo de redes debe adoptar para mitigarlas. Los **Capítulos 4 y 5** abordan dos aspectos clave de la operación segura de redes privadas 5G. El capítulo 4 se centra en las dimensiones operativas y organizativas de la seguridad, con énfasis en la cooperación entre múltiples actores y en las estrategias de protección durante todo el ciclo de vida. El capítulo 5 lo complementa proporcionando orientación práctica sobre la gestión de la configuración de seguridad, un área esencial, pero a menudo desatendida, que requiere procesos estructurados, coherentes y, en lo posible, automatizables para reducir los riesgos y garantizar el cumplimiento con normativa o políticas de seguridad.

[5] https://op.europa.eu/s/z6Wu
[6] https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security

Capítulo 2: Arquitectura y funcionamiento de una red 5G privada

2.1 Arquitectura de referencia (SA) autónoma 5G

Para abordar la ciberseguridad de una red 5G, es fundamental comprender su arquitectura. Esta guía se centra exclusivamente en la arquitectura **5G autónoma** (**standalone, SA**)[7], que representa la visión completa de la tecnología, incluyendo todas las nuevas características diseñadas específicamente para ella. A diferencia de la arquitectura no autónoma (non-standalone, NSA), que constituye una primera fase de despliegue utilizando la red de acceso radioeléctrico 5G (New Radio - NR) anclada al núcleo de red 4G existente (Evolved Packet Core - EPC), la arquitectura SA es un sistema que define las comunicaciones extremo a extremo de forma independiente de las generaciones anteriores. La arquitectura NSA se pensó para ayudar en los despliegues iniciales de 5G sobre redes 4G públicas “legacy” (existentes), pero para redes 5G privadas donde no existe una red 4G heredada, la arquitectura SA es la que permite capturar todas las bondades del 5G para los casos de uso ya mencionados.

2.2 Dominios funcionales de la red 5G

La arquitectura SA se compone de una red de acceso de nueva generación (next-generation access network, NG-RAN) y un núcleo de red 5G (5G Core - 5GC) implementado como una infraestructura "nativa en la nube" (cloud-native). Esta arquitectura puede descomponerse en cuatro dominios funcionales principales, cada uno con un papel específico en el funcionamiento de la red.

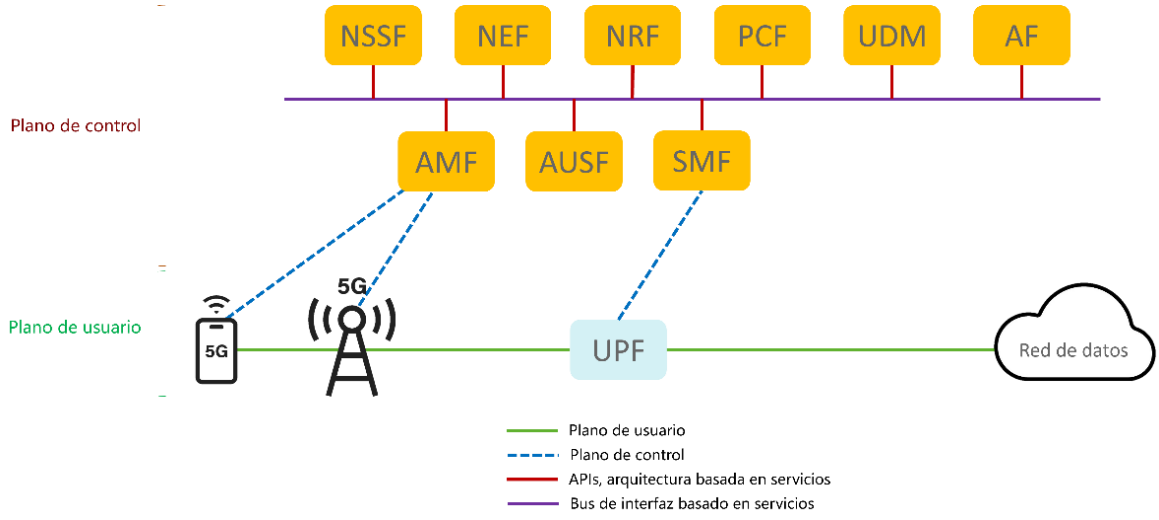


Figura 2.1. Arquitectura básica de una red 5G

- **Dominio de los Equipos de Usuario (UE)**: Este término ya no se refiere únicamente a los teléfonos inteligentes. En el contexto de una red privada, un UE (User Equipment)

[7] Los términos “standalone” y “autónoma” se utilizarán de forma indiferente para nombrar a este tipo de redes a lo largo de esta guía.

puede ser cualquier dispositivo que requiera conectividad: un sensor en una máquina, un robot en una línea de montaje, un vehículo guiado automático (AGV), una cámara de videovigilancia, un controlador lógico programable (PLC), etc. Cada UE incorpora un módulo de comunicación 5G y un Módulo de Identidad del Suscriptor (SIM), que puede consistir en una tarjeta física, una eSIM embebida (que no requiere tarjeta física) o incluso una iSIM embebida (la SIM está integrada en el mismo chip del dispositivo), lo que le permite autenticarse de forma segura en la red.

- **Red de Acceso Radioeléctrico (RAN)**: Es la parte de la red que proporciona conectividad inalámbrica a los UEs. En 5G se denomina NG-RAN (Next-Generation RAN) y está compuesta por estaciones base llamadas **gNodeB (gNB)**. Una de las innovaciones arquitectónicas del 5G es la posibilidad de dividir funcionalmente la gNB en dos componentes: la **Unidad Centralizada (CU)**, que gestiona los protocolos de nivel superior, y la **Unidad Distribuida (DU)**, que se encarga de las funciones radioeléctricas de nivel inferior, más próximas a la señal física. Esta división, promovida por iniciativas como O-RAN (Open RAN), ofrece una mayor flexibilidad en el despliegue, permitiendo, por ejemplo, centralizar múltiples CUs para gestionar varias DUs, en escenarios donde el caso de uso/negocio tenga sentido.
- **Dominio del Núcleo (5G Core – 5GC)**: Es el núcleo de la red, responsable de todas las funciones de control, la gestión de sesiones y el encaminamiento del tráfico de datos. Una de las características de diseño más relevantes del 5GC es la separación entre el plano de control y el plano de usuario (CUPS – Control and User Plane Separation):
    - **Plano de Control**: Encargado de la señalización y la gestión general de la red. Incluye un conjunto de funciones de red (NF) que gestionan el registro de dispositivos, la autenticación, la movilidad, la creación de sesiones de datos, la aplicación de políticas, entre otros.
    - **Plano de Usuario**: Responsable del transporte del tráfico de datos del usuario. Su función principal es reenviar, inspeccionar y encaminar los paquetes de datos entre el UE y la red de datos de destino.

  Esta separación entre planos facilita la implantación de sistemas de computación en el borde **(edge computing)**, permitiendo desplegar las funciones del plano de usuario de forma flexible y distribuida, muy cerca del usuario final (por ejemplo, en la propia planta o instalación industrial), mientras que el plano de control puede residir en un centro de datos más distante y centralizado. Este enfoque minimiza la latencia, ya que el tráfico local no necesita enviarse al núcleo de red remoto para ser procesado.
- **Dominio de Orquestación, Supervisión y Gestión (MANO)**: Dado que las funciones de red en 5G se implementan mediante software, se requiere un sistema robusto para gestionar su ciclo de vida. El marco de gestión y orquestación (MANO), normalizado por ETSI, se encarga de automatizar el despliegue, la configuración, el escalado y la finalización de estas funciones de red virtualizadas (VNF o CNF). Está compuesto por tres bloques principales:
    - **NFV Orchestrator (NFVO)**: Gestiona el ciclo de vida de los servicios de red

completos.

- **VNF Manager (VNFM)**: Administra el ciclo de vida de las funciones de red individuales.
- **Virtualized Infrastructure Manager (VIM)**: Controla los recursos subyacentes de computación, almacenamiento y red (por ejemplo, un clúster de Kubernetes). En una red privada, esta capa puede ser más sencilla que en la infraestructura de un gran operador público, pero su función de automatización sigue siendo esencial.

La Tabla 2.1 recoge las principales funciones de red del núcleo 5G y su funcionalidad clave dentro del servicio de comunicaciones que proporcionan.

Tabla 2.1: Principales funciones de red del núcleo 5G y su papel

Acrónimo (NF)	Nombre completo	Función principal
AMF	Función de gestión del acceso y la movilidad	Gestiona el registro, la conexión, la movilidad y la accesibilidad de los UE. Es el punto de entrada de la señalización de los UE al núcleo.
SMF	Función de gestión de sesiones	Se encarga de establecer, modificar y liberar sesiones de datos de usuario (sesiones PDU). Selecciona el UPF adecuado y asigna la dirección IP.
UPF	Función de plano de usuario	Enruta y reenvía los paquetes de datos de usuario. Realiza la inspección de paquetes y la aplicación de la política QoS. Es la única función correspondiente al plano de datos.
UDM+UDR	Gestión unificada de datos	Almacena y gestiona de forma segura los datos de suscripción del usuario, incluidos los perfiles de servicio y las políticas de acceso.
AUSF	Función de servidor de autenticación	Realiza la autenticación del UE, verificando sus credenciales para permitir el acceso a la red.
PCF	Función de control de políticas	Proporciona un marco unificado para las políticas de red, como las normas de calidad de servicio y tarificación.
NRF	Función de repositorio de red	Actúa como registro de servicios. Permite a las NF descubrir otras NF y los servicios que ofrecen.

2.3 Flujos de señalización fundamentales en redes privadas

Para que un UE se comunique a través de la red 5G, deben completarse dos procesos de señalización fundamentales. La seguridad de estos flujos es crítica, ya que se basan en una cadena de confianza que implica a múltiples componentes de la red.

- **Proceso de conexión y registro:** Es el procedimiento mediante el cual un UE se registra en la red y establece un contexto de seguridad. De forma simplificada, los pasos son los siguientes:
  1. El UE se enciende y busca una señal 5G. Se sincroniza con una célula gNB cercana descodificando el denominado Bloque de Sincronización de Señal (SSB).
  2. A través del Procedimiento de Acceso Aleatorio (RACH), el UE solicita recursos al gNB para establecer una conexión de señalización.
  3. Se establece una conexión de Control de Recursos de Radio (RRC) entre el UE y el gNB.
  4. El UE envía un mensaje NAS (Non-Access Stratum) de tipo "Registration Request" a

través del gNB. El gNB lo reenvía al **AMF**.

5. La AMF inicia el **procedimiento de autenticación**. Se comunica con la **AUSF**, que a su vez interactúa con la **UDM** para verificar las credenciales del abonado (almacenadas en la SIM/eSIM).
6. Una vez autenticado, se establecen las claves de seguridad que se utilizarán para cifrar y proteger las comunicaciones entre el UE y la red.
7. La AMF envía un mensaje de "Registration Accept" al UE, confirmando que el registro se ha completado con éxito.

- **Proceso de establecimiento de sesión PDU:** Una vez registrado, el equipo de usuario puede solicitar una conexión de datos para acceder a una red, como la red interna de la empresa/red privada o Internet. Esto se conoce como establecimiento de una sesión de unidad de paquetes de datos (Packet Data Unit, PDU).

  1. El equipo de usuario envía un mensaje NAS PDU "Solicitud de establecimiento de sesión" a la **AMF**. Este mensaje especifica a qué Red de Datos (identificada por un nombre DNN -Data Network Name-) desea conectarse.
  2. El AMF selecciona un **SMF** adecuado para gestionar esta sesión y le reenvía la solicitud.
  3. El SMF verifica en el **UDM** y el **PCF** que el usuario tiene permiso para acceder a esa red de datos.
  4. El SMF selecciona un **UPF** (que puede estar en el borde local) y asigna una dirección IP al UE.
  5. El SMF ordena al UPF (a través de la interfaz N4) que cree las reglas de encaminamiento para el tráfico de este UE.
  6. Simultáneamente, el SMF ordena al gNB (a través del AMF) que establezca los "túneles" de radio (portadores de radio de datos – Data Radio Bearers, DRB –) necesarios para transportar los datos del usuario.
  7. Una vez establecidos los túneles, el flujo de datos del usuario puede comenzar, viajando desde el UE, a través del gNB y la UPF, hasta la red de datos de destino.

La protección de estos flujos requiere un enfoque de defensa en profundidad. No basta con asegurar la interfaz de radio; es igualmente crucial proteger las interfaces entre las funciones básicas (por ejemplo, las que conectan AMF, SMF, UDM y AUSF), garantizar que las políticas de suscripción en la UDM son correctas y están protegidas contra la manipulación, y supervisar estos flujos para detectar cualquier comportamiento anómalo.

2.4 Interacción entre funciones de red (arquitectura basada en servicios)

Como ya se ha mencionado, el núcleo 5G funciona con una Arquitectura Basada en Servicios (SBA), que supone un cambio radical con respecto a las arquitecturas de red anteriores. En este modelo, las funciones de red (NF) actúan como "productoras" de servicios y también como "consumidoras" de servicios.

La pieza central que permite este dinamismo es la **NRF (Network Repository Function)**. La NRF funciona como un catálogo o registro de servicios. Cada vez que una NF se pone en marcha, se registra en la NRF, publicando los servicios que ofrece. Cuando otra NF (actuando como consumidor) necesita utilizar un servicio (por ejemplo, la AMF necesita un servicio de gestión de sesiones SMF), en lugar de tener una conexión preconfigurada, primero consulta a la NRF. La NRF devuelve una lista de instancias SMF disponibles que ofrecen ese servicio. El consumidor puede entonces seleccionar una instancia y establecer una comunicación directa con ella.

Esta comunicación se realiza a través de interfaces basadas en servicios (por ejemplo, Nsmf_PDUSession para servicios de sesión SMF), que, como se ha señalado, utilizan API RESTful sobre protocolos web estándar como HTTP/2. Esta arquitectura proporciona una gran flexibilidad, escalabilidad y capacidad de recuperación, ya que las NF pueden añadirse, eliminarse o actualizarse dinámicamente sin interrumpir el servicio. Sin embargo, también introduce una nueva superficie de ataque en las propias API, que deben protegerse adecuadamente.

2.5 Configuraciones esenciales para una red 5G privada

Para personalizar una red privada, segmentar el tráfico y aplicar políticas de seguridad granulares, son esenciales dos parámetros de configuración: la NSSAI y el DNN. La correcta configuración de estos elementos en los perfiles de suscripción de los usuarios (almacenados en el UDM) es un control de seguridad preventivo de primer orden.

- **NSSAI (Network Slice Selection Assistance Information):** *La segmentación o división en porciones de la red* es una de las capacidades más potentes de la tecnología 5G. Permite dividir una única infraestructura de red física en múltiples redes lógicas virtuales y aisladas, cada una optimizada para un caso de uso específico. Por ejemplo, en una fábrica puede haber un *segmento o porción*[8] *(slice)* para el tráfico de vídeo de alta definición de las cámaras de seguridad (eMBB), otro para el control de robots en tiempo real (URLLC) y un tercero para los miles de sensores industriales de la planta (mMTC).

  Cada *"slice"* se identifica unívocamente mediante una **S-NSSAI (Single-NSSAI)**. A su vez, la S-NSSAI se compone de dos partes:

  - **SST (Slice/Service Type):** Valor numérico normalizado que define el tipo de servicio principal del segmento (véase la Tabla 2.2).
  - **SD (Slice Differentiator):** Un identificador opcional que permite diferenciar entre segmentos o porciones que comparten el mismo tipo de servicio (SST).

  Cuando un UE se registra en la red, incluye en su solicitud el S-NSSAI del segmento o porción (red lógica virtual) al que desea acceder. La red, basándose en el perfil de suscripción del UE, autoriza o deniega el acceso a ese segmento.

- **DNN (Nombre de Red de Datos):** El DNN es un identificador, conceptualmente similar a un APN (Access Point Name) en 4G, que especifica la red de datos a la que el UE desea

[8] El término “slice” puede aparecer en español como segmento, rebanada o porción.

conectarse. En una red privada, se pueden definir varios DNN para segmentar el acceso a distintas redes. Por ejemplo, se podría tener un DNN "internet" para el acceso general, un DNN "corporate_network" para el acceso a los sistemas de la empresa y un DNN "control_ot" para la red de control industrial, que estarían completamente aisladas entre sí.

- El DNN es un parámetro clave en el proceso de establecimiento de sesión PDU, ya que permite al SMF seleccionar la UPF y las políticas de enrutamiento correctas para dirigir el tráfico UE a su destino previsto. Se puede utilizar un DNN específico para una **LADN (red de datos de área local)**, lo que garantiza que el tráfico generado y destinado a permanecer dentro de las instalaciones de la empresa nunca salga a redes externas.

La combinación de NSSAI y DNN es la herramienta fundamental para implantar **la microsegmentación**. Una política de seguridad puede definir, por ejemplo, que los UE pertenecientes al grupo "Robots de producción" sólo puedan utilizar el segmento *de* tipo URLLC (identificado por su S-NSSAI) para establecer una sesión PDU con la red de control industrial (identificada por el DNN "control_ot"). Cualquier intento por parte de uno de estos robots de acceder a otro segmento o a otro DNN sería denegado por la red. Este ejemplo muestra que la configuración segura de los perfiles de suscripción en la PDU es un control de acceso fundamental.

Tabla 2.2: Valores SST (Slice/Service Type) normalizados y sus casos de uso

Valor SST	Acrónimo	Descripción	Red privada Ejemplo de caso de uso
1	eMBB	Banda ancha móvil mejorada	Transmisión de vídeo 4K/8K desde cámaras de seguridad; aplicaciones de realidad aumentada para asistencia remota.
2	URLLC	Comunicaciones ultra fiables de baja latencia	Control en tiempo real de robots y maquinaria; vehículos de guiado automático (AGV); teleoperación de equipos.
3	mMTC	Comunicación masiva de máquinas	Conexión de miles de sensores de baja potencia para la supervisión del estado, el mantenimiento predictivo o la gestión de activos.
4	V2X	Comunicación de Vehículo a cualquier otro dispositivo	Comunicaciones entre vehículos, infraestructuras y personal en entornos como puertos, aeropuertos o centros logísticos.
5	HMTC	Comunicaciones de tipo máquina de alto rendimiento	Comunicaciones entre máquinas que requieren un alto rendimiento, como la automatización industrial avanzada.

Capítulo 3: Arquitectura de seguridad de la red privada 5G

3.1 Retos de seguridad que añade la SNPN a las redes empresariales

Tradicionalmente, las empresas utilizan sistemas con baja inteligencia (dispositivos simples, no conectados o con capacidad limitada de procesamiento y decisión). Sin embargo, con la incorporación de redes privadas 5G, una gran cantidad de dispositivos inteligentes acceden a dichas redes, lo que rompe los límites de seguridad previamente establecidos. Los cambios se ilustran en la Figura 3.1.

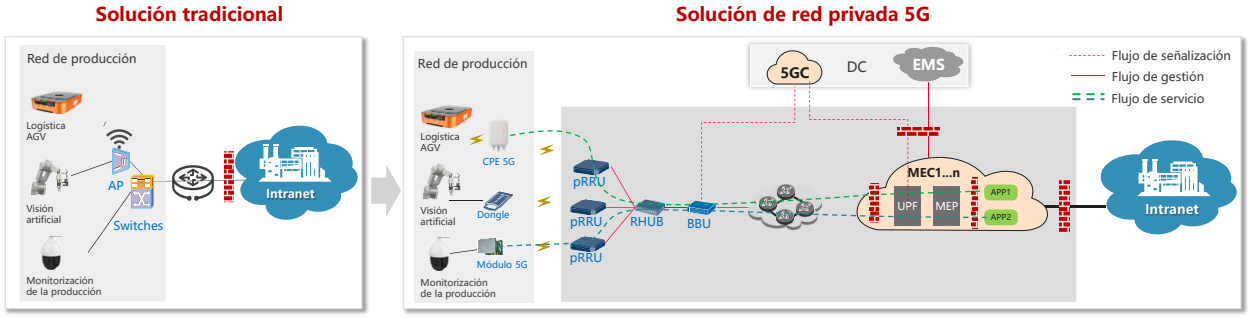


Figura 3.1 Cambios en las redes empresariales tras la introducción de SNPN

1. Desde la perspectiva de la arquitectura de red, la introducción de redes privadas 5G conduce a la adición de un gran número de dispositivos inalámbricos, incluyendo redes centrales, estaciones base y sistemas de gestión de red, a las redes empresariales, aumentando la complejidad de la arquitectura de red de esas empresas.
2. Desde la perspectiva del acceso de dispositivos, el acceso inalámbrico 5G tiene una cobertura más amplia que Wi-Fi o el acceso por cable y admite comunicaciones masivas de tipo máquina, lo que indica que el número de dispositivos que acceden a la red aumenta significativamente.
3. Desde el punto de vista técnico, las redes 5G adoptan una arquitectura virtualizada y orientada a los servicios, difuminando los límites tradicionales de la red.

Los cambios anteriores plantean una serie de retos de seguridad a las redes privadas 5G, tal como se detalla a continuación.

3.1.1 El aumento de la complejidad de la red conlleva amenazas de seguridad más habituales

Mayor probabilidad de brechas de seguridad

A medida que se integra un gran número de dispositivos en las redes empresariales, aumenta la posibilidad de vulnerabilidades en el kernel del sistema operativo de los dispositivos y servidores, la capa de virtualización de los servidores usados tanto en la red como en los centros de datos, y las aplicaciones que se ejecutan tanto en dispositivos como en los servidores. Los atacantes pueden explotar estas vulnerabilidades para obtener el control del sistema o ejecutar código malicioso. Si las empresas no instalan los parches de seguridad a tiempo, aumentarán los riesgos

de seguridad.

Las configuraciones inseguras de los dispositivos se convierten en puntos débiles de seguridad.

Al desplegar un gran número de dispositivos en redes 5G empresariales, es común que las organizaciones configuren contraseñas débiles y predecibles —como *123456* o *admin*— con el objetivo de simplificar la gestión. Sin embargo, este tipo de credenciales son altamente vulnerables a ataques por fuerza bruta mediante enumeración sistemática. Una vez comprometidas, los atacantes pueden acceder fácilmente a los dispositivos y llevar a cabo acciones maliciosas sobre los datos y servicios de la red empresarial.

Gestión de la superficie de ataque en entornos de alta densidad de dispositivos

Las redes 5G están diseñadas para ofrecer una conectividad masiva y segura a un número sin precedentes de dispositivos. Esta capacidad, si bien es una de sus grandes ventajas, amplía la superficie de ataque potencial de una organización. Por ello, es fundamental una gestión proactiva de la seguridad en todos los niveles del ecosistema. Las vulnerabilidades pueden surgir en el kernel del sistema operativo de los dispositivos, en la capa de virtualización de los servidores de red y centros de datos, o en las aplicaciones que se ejecutan en ellos. Para conseguir un despliegue adecuado, las empresas deben implementar un ciclo de vida de seguridad riguroso, incluyendo la aplicación oportuna de parches para mitigar el riesgo de que los atacantes exploten dichas vulnerabilidades.

La configuración segura como pilar de la protección en redes 5G

El despliegue a gran escala de dispositivos que permiten las redes 5G privadas introduce desafíos operativos. Una configuración inadecuada de los dispositivos puede anular las ventajas de seguridad inherentes a estas redes. Por ejemplo, el uso de contraseñas débiles y predecibles —como 123456 o admin— para simplificar la administración de miles de dispositivos podría crear un punto débil crítico. Este tipo de credenciales son altamente vulnerables a ataques de fuerza bruta. Para aprovechar la arquitectura de seguridad de 5G, es imprescindible aplicar políticas de configuración robustas y credenciales fuertes, asegurando que los atacantes no puedan obtener un acceso fácil a los dispositivos para comprometer datos y servicios de la red empresarial.

Ataques DDoS

Cuando una estación base es atacada por un gran número de dispositivos 5G a través de la interfaz de radio, puede dejar de prestar servicios debido a la limitación de los recursos del sistema. Los atacantes también pueden utilizar la red para enviar peticiones masivas a los elementos clave del núcleo 5C (Network Element – NE – como la AMF, SMF y UPF) así como al MEC, agotando el ancho de banda, los recursos de cómputo y la memoria. Como consecuencia, dichos elementos no pueden responder a las solicitudes legítimas de los abonados autorizados.

Ataques de intermediario (“Man-in-the-Middle)

La red privada 5G introduce múltiples enlaces —como las interfaces radio, la red de transmisión y los canales de operación y mantenimiento (O&M)—, lo que incrementa el riesgo de ataques de tipo man-in-the-middle sobre los enlaces de datos, al ampliar la superficie de exposición a interceptaciones y manipulaciones no autorizadas.

3.1.2 El acceso inalámbrico de un volumen masivo de dispositivos amplía la superficie de ataque en la interfaz de radio

Acceso desde dispositivos maliciosos

En un entorno de red privada 5G, existe el riesgo de suplantación de identidades legítimas de dispositivos para acceder a la red y obtener información sensible o lanzar ataques. Por ejemplo, pueden alterarse el IMSI (Identidad Internacional de Abonado Móvil) y las direcciones MAC de los dispositivos. De este modo, dispositivos no autorizados se hacen pasar por dispositivos legítimos con el objetivo de eludir los mecanismos de autenticación de acceso a la red.

Capacidades de protección de seguridad dispares en los dispositivos de acceso

Los dispositivos que carecen de capacidades básicas de protección pueden propagar y amplificar los riesgos de seguridad dentro de las redes empresariales a través de las redes privadas 5G. Además, muchos protocolos industriales heredados, diseñados para redes aisladas, carecen de cifrado o autenticación propios. Al extender su alcance con 5G, un atacante que comprometa un dispositivo o servidor puede enviar órdenes maliciosas a través de la red. La red 5G transportará esos datos, permitiendo que una vulnerabilidad local se propague y amplifique por toda la infraestructura empresarial.

3.1.3 La virtualización debilita el perímetro de protección y compromete las defensas tradicionales.

Las funciones de red en 5G se implementan mediante tecnologías de virtualización, lo que difumina los límites tradicionales de la infraestructura de comunicaciones. Como resultado, las medidas de seguridad basadas en protecciones perimetrales —habituales en redes empresariales— dejan de ser efectivas o no están disponibles en muchos casos. Además, se introducen nuevos riesgos, como vulnerabilidades propias de los entornos virtualizados o ataques dirigidos a las plataformas de virtualización que alojan las funciones de red.

3.1.4 La arquitectura orientada a servicios amplía la superficie de ataque de la red

El núcleo 5G (5GC) adopta una arquitectura basada en servicios (SBA, Service-Based Architecture), en la que las funciones tradicionales de los elementos de red (NEs) se dividen en múltiples funciones de red independientes (NFs) que se comunican entre sí mediante interfaces basadas en servicios (SBIs). Esta arquitectura mejora la flexibilidad y escalabilidad de la red, pero también incrementa su exposición a amenazas. Por ejemplo, un atacante puede aprovechar vulnerabilidades en las interfaces para atacar elementos de red, acceder de forma no autorizada a información sensible o manipular datos, afectando al funcionamiento normal del 5GC. Asimismo, una vulnerabilidad en la autenticación entre la AMF y la SMF podría permitir la suplantación de solicitudes legítimas de abonados, interfiriendo en la gestión de sesiones y provocando interrupciones del servicio.

3.1.5 Desafíos de seguridad en la operación y mantenimiento (O&M)

Desafíos de seguridad del sistema de gestión EMS

El sistema EMS (Element Management System) en una red privada 5G se encarga de la gestión de operación y mantenimiento del sistema, siendo crítico para el funcionamiento normal de los elementos de red (NEs) y la seguridad de los datos. Si este sistema es comprometido, un atacante podría tomar el control de todos los NEs de la red 5G y causar daños intencionados, como el acceso no autorizado a datos de red, modificaciones en la configuración del sistema o la instalación de software malicioso.

Desafíos en la visibilidad de eventos de seguridad

Las redes privadas 5G implican el acceso masivo de dispositivos, lo que plantea un gran reto en la detección y prevención oportuna de ataques de seguridad. La presencia de múltiples fuentes de registros heterogéneas genera volúmenes masivos de datos provenientes de diferentes *logs*, aumentando la complejidad de su gestión. En este entorno, eventos de seguridad críticos pueden quedar ocultos entre datos irrelevantes. Además, la arquitectura de red distribuida y compleja reduce la visibilidad de las amenazas y dificulta la localización precisa de fallos de seguridad, lo que puede impedir una respuesta eficaz y a tiempo ante los incidentes.

3.2 Arquitectura de seguridad en redes privadas 5G

3.2.1 Arquitectura de seguridad integral

Para mitigar los riesgos de seguridad introducidos por las redes privadas 5G, es necesario construir capacidades de seguridad de extremo a extremo. En primer lugar, se deben desplegar redes 5G utilizando productos que cumplan con los estándares del 3GPP y que habiliten las funciones de seguridad correspondientes. En segundo lugar, es fundamental garantizar la seguridad de los dispositivos mediante medidas como la protección física, el fortalecimiento del sistema frente a vulnerabilidades y configuraciones débiles (*system hardening*) y la verificación de integridad del software. Estas acciones constituyen la base de seguridad sobre la que se sostiene toda la red.

A partir de esta base, se debe implementar la seguridad específica en cada uno de los dominios: seguridad en el acceso de dispositivos, seguridad en la red de comunicaciones, seguridad en el entorno MEC, seguridad del núcleo 5G (5GC), seguridad en O&M y gestión de la seguridad. Todo ello contribuye a garantizar una arquitectura de seguridad de extremo a extremo, tal como se muestra en la Figura 3.2. Las siguientes secciones describen los principales dominios de seguridad.

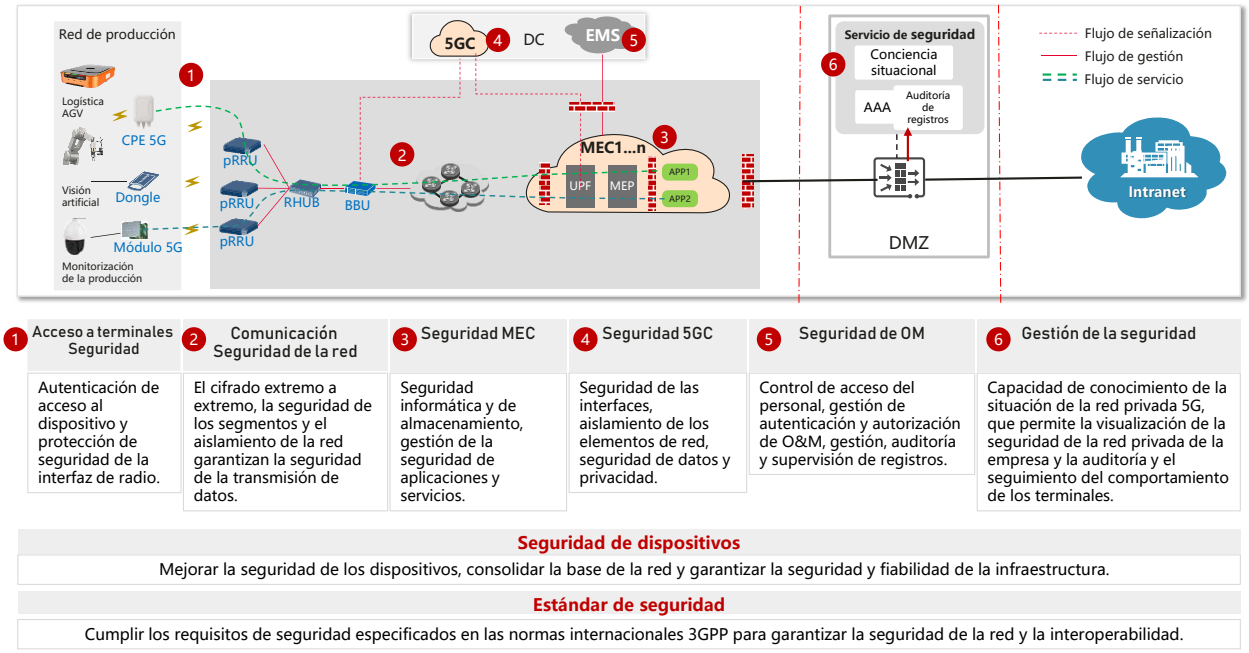


Figura 3.2 Arquitectura de seguridad de la red privada 5G

3.2.2 Estándares de seguridad

Es fundamental cumplir con los requisitos de seguridad establecidos en los estándares del 3GPP para garantizar la seguridad de las comunicaciones dentro de la red. Por ejemplo, se debe habilitar la función de autenticación definida en la especificación **3GPP TS 33.501**, que describe la arquitectura y los procedimientos de seguridad para el sistema 5G.

Asimismo, la gestión del ciclo de vida de los certificados digitales debe realizarse utilizando la infraestructura de clave pública (**PKI**) según lo definido en la **3GPP TS 33.310**. Además, la implementación de medidas de seguridad debe alinearse con las mejores prácticas del sector en ciberseguridad, como las recogidas en la base de conocimiento **GSMA MCKB**[9].

3.2.3 Seguridad del dispositivo

Protección física

La sala donde se ubiquen los equipos de red debe contar con puertas de seguridad para evitar accesos no autorizados. Los armarios deben disponer de cerraduras seguras y alarmas del estado de las puertas. Solo los usuarios autorizados podrán abrirlos. Se debe aplicar una gestión de seguridad física adecuada, así como supervisar sistemas de detección de inundaciones e incendios.

Fortalecimiento del sistema y gestión de vulnerabilidades

El sistema debe reforzarse mediante políticas estrictas de control de acceso, y desactivar

[9] https://www.gsma.com/solutions-and-impact/technologies/security/cybersecurity-knowledge-base/

servicios y puertos innecesarios siguiendo las guías de configuración segura del fabricante. Se debe establecer un mecanismo de gestión de vulnerabilidades que permita obtener, validar e implementar actualizaciones de seguridad de forma oportuna. Antes de instalar un parche, es obligatorio realizar pruebas de compatibilidad y estabilidad para evitar fallos en los dispositivos o interrupciones del servicio. Asimismo, se deben realizar escaneos periódicos del sistema para identificar y corregir vulnerabilidades de seguridad de forma proactiva.

Protección de la integridad del software

El software de los dispositivos debe obtenerse únicamente a través de canales autorizados. Durante la instalación o actualización, se debe verificar la integridad mediante firma digital para garantizar que el software no ha sido alterado de forma maliciosa.

3.2.4 Seguridad en el acceso de dispositivos

Reforzar la autenticación de dispositivos para el acceso a redes 5G

Las funciones de autenticación de la arquitectura 5G definidas en la 3GPP TS 33.501 permiten identificar y verificar rigurosamente a los dispositivos (UEs) que acceden a la red empresarial 5G, impidiendo que dispositivos no autorizados se conecten. Por ejemplo, la AMF ofrece la función SeaF (Security Anchor Function) y la AUSF permite autenticación mediante el mecanismo 5G-AKA.

Mejorar el sistema de gestión de mantenimiento de los dispositivos

Se debe establecer un sistema unificado de gestión para los dispositivos 5G, que permita dar de baja de forma inmediata aquellos que han sido retirados de la red. Esto evita que atacantes utilicen dispositivos antiguos para intentar acceder a la red. También se recomienda implementar autenticación multifactor para reforzar la seguridad en las tareas de mantenimiento, y así mitigar riesgos asociados al robo o filtración de contraseñas. Los datos almacenados en los dispositivos deben estar cifrados para evitar su exposición en caso de pérdida o robo.

Proteger los mensajes del plano de señalización en la interfaz radio

Se deben habilitar funciones de cifrado, protección de integridad y protección contra repetición (*anti-replay*) para la señalización RRC entre el UE y el gNodeB. Asimismo, aplicar cifrado, integridad, anti-replay y protección de seguridad para la señalización NAS entre el UE y la AMF (interfaz N1), incluyendo la protección de los mensajes NAS iniciales y la transmisión cifrada de los identificadores permanentes del UE.

Proteger los datos del plano de usuario en la interfaz radio

Se debe habilitar el cifrado y la protección de integridad para el tráfico del plano de usuario entre el UE y el gNodeB.

Protección anti-DDoS en la interfaz radio

Cuando el gNodeB es objetivo de tráfico malicioso, los mecanismos de control de flujo pueden mitigar los riesgos de reinicio del nodo o ataques de denegación de servicio (DoS) y denegación de servicio distribuida (DDoS), mejorando la fiabilidad del nodo y asegurando la continuidad del servicio. Además, se deben habilitar mecanismos de detección de ataques de señalización, como

solicitudes RRC consecutivas iniciadas por UEs maliciosos, para prevenir su impacto en la red.

3.2.5 Seguridad de la red de comunicaciones

Cifrado de la información en tránsito

Se debe asegurar el uso de protocolos de transmisión segura estandarizados para proteger las comunicaciones externas, evitando que atacantes intercepten, manipulen o reproduzcan de forma fraudulenta el contenido transmitido a través de la red 5G. Entre las interfaces protegidas se incluyen:

- **Las interfaces NG**, que conecta el gNodeB con el núcleo 5G (5GC), específicamente con funciones como la AMF (interfaz N2) y la UPF (interfaz N3).
- **La interfaz Xn**, que permite la comunicación directa entre distintos gNodeBs, facilitando la movilidad y la transferencia (handover) de sesiones entre celdas.
- **La interfaz OMCH** (Operation, Maintenance and Control Channel), utilizada para la gestión y supervisión remota de los equipos de red desde el sistema de operación y mantenimiento (O&M).

Además, se debe habilitar la autenticación mutua mediante certificados digitales, con el fin de verificar la identidad de los dispositivos en ambas direcciones.

Seguridad de los segmentos o porciones de red 5G (slices)

El algoritmo de asignación de recursos está optimizado para garantizar la eficacia del aislamiento de recursos entre los diferentes segmentos definidos. Además, se deben mejorar la supervisión y la gestión de los recursos de hardware para detectar y resolver a tiempo los problemas de aislamiento de recursos causados por fallos de hardware o software.

Separación de flujos de información con diferente propósito:

Se deben separar el plano de usuario, el plano de señalización y el plano de gestión. A nivel de capa de red, se utilizan múltiples tecnologías de aislamiento de red, como VLAN, VXLAN y Multiprotocol Label Switching (MPLS), así como políticas de segmentación de red, para construir un sistema de aislamiento de red multicapa y multidimensional. Además, se debe reforzar la revisión y verificación de las configuraciones de aislamiento de red, se debe comprobar periódicamente la corrección de las configuraciones de aislamiento de red y se deben detectar y rectificar a tiempo los errores de configuración.

3.2.6 Seguridad MEC

Garantizar la seguridad del cómputo y el almacenamiento.

Se deben emplear tecnologías de monitorización de seguridad en entornos virtualizados para supervisar en tiempo real el estado de ejecución de las máquinas virtuales (VM). Cuando se detectan comportamientos anómalos, se generarán alarmas de forma oportuna, garantizando así la integridad del entorno de virtualización. Los datos almacenados en los nodos MEC se deben cifrar mediante algoritmos de cifrado robustos, asegurando la confidencialidad de la información en los medios de almacenamiento. Adicionalmente, se debe reforzar la gestión de seguridad de

los dispositivos de almacenamiento, estableciendo permisos de acceso estrictos para prevenir accesos no autorizados y manipulaciones indebidas de datos.

Reforzar la gestión de la seguridad de aplicaciones y servicios

La plataforma de computación de borde o MEC (Multi-access Edge Computing) constituye uno de los pilares fundamentales de una red privada 5G en un entorno industrial o empresarial. Su función es procesar los datos cerca de donde se generan, habilitando servicios de baja latencia que son esenciales para le empresa o industria. En esta plataforma es habitual que se encuentren las aplicaciones más críticas y se gestionen los datos más sensibles, como información de producción en tiempo real o de telemetría. Su valor estratégico la convierte en un objetivo de alto impacto, por lo que su protección integral debe ser una prioridad.

La primera línea de defensa reside en la seguridad de las propias aplicaciones alojadas en el MEC, lo cual implica implantar o exigir al proveedor un ciclo de vida de desarrollo de software seguro. Una vez en producción, las aplicaciones deben ser sometidas a escaneos de seguridad periódicos para detectar y corregir posibles vulnerabilidades. Además de asegurar el código, es crucial garantizar tanto la continuidad operativa como la vigilancia de seguridad del entorno MEC. La continuidad se logra mediante una arquitectura redundante, usando técnicas como el despliegue en múltiples nodos y el balanceo de carga para hacer al sistema tolerante a fallos. Además, se debe implementar un sistema de monitorización de seguridad, supervisando logs, tráfico de red y comportamiento de las aplicaciones para detectar anomalías o patrones de ataque. Este sistema de alerta temprana es clave para activar medidas de mitigación y neutralizar amenazas antes de que afecten a los servicios implantados o a la propia red 5G.

3.2.7 Seguridad en el núcleo 5G (5GC)

Reforzar la protección de la arquitectura de red y de las interfaces

- Fortalecer la seguridad en las interfaces

  El acceso a las interfaces basadas en servicios del núcleo 5G (SBIs) debe estar estrictamente controlado. Se deben emplear mecanismos de autenticación y autorización basados en identidad, así como tecnologías de certificados digitales, para asegurar que únicamente los elementos de red autorizados (NEs) puedan comunicarse entre sí. Los datos que circulan por estas interfaces se cifran mediante protocolos seguros de cifrado, con el fin de evitar su interceptación o manipulación durante la transmisión.

- Aislamiento de elementos de red y seguridad en las comunicaciones internas

  Se deben aplicar tecnologías de aislamiento, tal como la virtualización de funciones de red (NFV) para aislar distintas funciones de red, evitando así la propagación lateral de ataques entre NEs dentro del core 5G.

Garantizar la seguridad de los datos de usuario y su privacidad

Los datos de usuario almacenados en el núcleo 5G se deben cifrar mediante algoritmos robustos. Asimismo, se debe reforzar la gestión de los dispositivos de almacenamiento, restringiendo su acceso únicamente a personal autorizado para prevenir accesos indebidos o alteraciones maliciosas. Durante la transmisión, se debe implementar cifrado extremo a extremo desde el dispositivo del usuario (UE) hasta el núcleo 5G, asegurando la confidencialidad durante todo el trayecto. Se debe utilizar también un mecanismo de verificación de integridad para asegurar que los datos no hayan sido alterados en tránsito. Finalmente, se debe optimizar el sistema de gestión de claves criptográficas para garantizar su generación, distribución, almacenamiento y actualización segura, mitigando riesgos derivados de filtraciones de claves.

3.2.8 Seguridad en operación y mantenimiento (O&M)

Segmentación por dominios de seguridad

Siguiendo la estrategia de seguridad global, la red se dividirá en dominios de seguridad diferenciados según la criticidad, función y nivel de confianza de los elementos que los componen (como NEs, sistemas EMS y servicios básicos). A cada dominio se le asignarán políticas de seguridad específicas. Los distintos dominios se aislarán entre sí mediante firewalls, con el fin de reducir la propagación de amenazas.

Gestión del control de acceso del personal

Tanto los operadores como los visitantes deben cumplir estrictamente con los requisitos de acceso definidos por la organización al ingresar a las salas donde se encuentren desplegados sistemas EMS. Se controlará el acceso mediante sistemas físicos (por ejemplo, control de acceso electrónico) y se registrará toda entrada o salida, permitiendo auditorías de seguridad posteriores. Para personal externo (por ejemplo, técnicos de terceros), se requerirá acompañamiento continuo por parte de empleados autorizados, así como verificación y registro de todas las operaciones realizadas.

Gestión de terminales de O&M

Con el objetivo de prevenir accesos no autorizados y abusos de privilegios, los terminales de operación y mantenimiento —como los clientes EMS o terminales de mantenimiento local (LMT)— deben gestionarse de forma centralizada y con políticas unificadas. En escenarios de O&M remota, se emplearán proxys de seguridad para controlar, autorizar y auditar los accesos remotos. Se implementarán políticas de control de acceso con aislamiento lógico para reducir la superficie de ataque expuesta por el sistema EMS y evitar accesos no autorizados.

Gestión de autenticación y autorización en O&M

- Mejorar los mecanismos de autenticación

  Se debe emplear autenticación multifactor para reforzar la seguridad y precisión del proceso de autenticación. Además, se deben optimizar los protocolos de autenticación para resistir ataques comunes, como los ataques por repetición (replay attacks) o los ataques de intermediación (man-in-the-middle). Se reforzará también la seguridad del servidor de autenticación para evitar su compromiso y garantizar la integridad de los datos de autenticación. En escenarios de conexión

con sistemas de terceros, se establecerá un proceso riguroso de autenticación de acceso externo.

- Gestión de autorizaciones con granularidad

  Se implementará un modelo de control de acceso basado en roles (RBAC) para asignar derechos mínimos necesarios a cada usuario o dispositivo, de acuerdo con su función y requerimientos operativos. Las autorizaciones deben ser revisadas y actualizadas periódicamente, asegurando su correspondencia con las necesidades reales. Asimismo, se establecerá un mecanismo de auditoría de cambios en los permisos, de forma que todas las modificaciones queden registradas y puedan ser analizadas en caso de incidentes. El personal encargado de las tareas O&M debe ser gestionado y autorizado exclusivamente por el administrador de seguridad, quien aplicará de forma estricta el principio de mínima autorización para no comprometer la estabilidad en el funcionamiento habitual del sistema de NEs.

3.2.9 Gestión de la seguridad

Control de acceso

Las empresas deben desplegar firewalls en la frontera entre la red privada 5G y la red corporativa (intranet) con el fin de controlar el tráfico entrante y saliente. Las políticas de seguridad del firewall deben regirse por el principio de mínimo privilegio, permitiendo únicamente el tráfico legítimo mediante reglas específicas y reduciendo así la superficie de ataque.

En la zona de operación y mantenimiento (O&M), se debe implementar un “bastion host” para gestionar de forma centralizada todos los accesos administrativos. A cada administrador se le asignan distintos roles y permisos de acceso en función de sus responsabilidades, previniendo accesos no autorizados y registrando todas las operaciones administrativas realizadas.

Detección y defensa contra amenazas

Se deben desplegar sistemas de protección avanzados como firewalls, NIPS (Network Intrusion Prevention System) y HIPS (Host Intrusion Prevention System), conformando un sistema de defensa integral contra amenazas. Estos sistemas permiten detectar comportamientos anómalos, generar alertas y bloquear actividades maliciosas en tiempo real. La base de datos de patrones o firmas para detección de anomalías debe mantenerse actualizada y es recomendable que el sistema admita la integración de fuentes externas de inteligencia de amenazas, lo que refuerza las capacidades de detección y control de seguridad.

Defensa frente a ataques DDoS

Se deben incorporar dispositivos específicos de protección contra ataques DDoS que monitoricen el tráfico de red en tiempo real y apliquen tecnologías de depuración para identificar y filtrar tráfico anómalo. Además, es esencial disponer de un mecanismo de respuesta ante emergencias provocadas por ataques DDoS, de manera que, ante un ataque masivo, se pueda activar un plan de contingencia y ajustar las políticas de red. Por ejemplo, se puede desviar el tráfico hacia enlaces de respaldo o hacia un nodo de depuración de tráfico anómalo, asegurando así el

funcionamiento continuo de funciones virtualizadas clave del core 5G. También se debe recopilar y analizar información de inteligencia sobre ataques DDoS para anticiparse y preparar medidas preventivas.

Respuesta a incidentes y conocimiento situacional

Se debe desplegar un sistema SIEM (Security Information and Event Management), que permita recolectar y analizar datos fundamentales de la red, como el tráfico y los registros de eventos generados por los distintos dispositivos. Esto facilita la detección de amenazas avanzadas persistentes (APT) y, en combinación con los sistemas de protección ya instalados, mejora la capacidad de respuesta ante incidentes de seguridad.

Capítulo 4: Operación y mantenimiento de la seguridad de la red privada 5G

4.1 La cooperación es un mecanismo importante para abordar los retos de la ciberseguridad

La arquitectura de seguridad de las redes privadas 5G presentada anteriormente permite hacer frente de manera eficaz a los riesgos de seguridad derivados de la introducción de este tipo de redes privadas en las empresas. Sin embargo, debido a la complejidad inherente de las redes 5G y a la naturaleza transversal y transfronteriza de muchas amenazas, las redes privadas 5G aún se enfrentan a desafíos de gran envergadura. Superar estos retos requiere de una colaboración coordinada entre gobiernos, organismos de estandarización, fabricantes y empresas usuarias. Un ejemplo de este esfuerzo conjunto es la GSMA Mobile Cybersecurity Knowledge Base, que ofrece conocimientos clave sobre estrategias de gestión de riesgos adoptadas por los distintos actores del ecosistema. Además, proporciona guías prácticas basadas en las mejores prácticas del sector, medidas de mitigación de riesgos, y promueve un modelo de seguridad basado en la responsabilidad compartida y la protección en capas, tal como se muestra en la Figura 4.1.

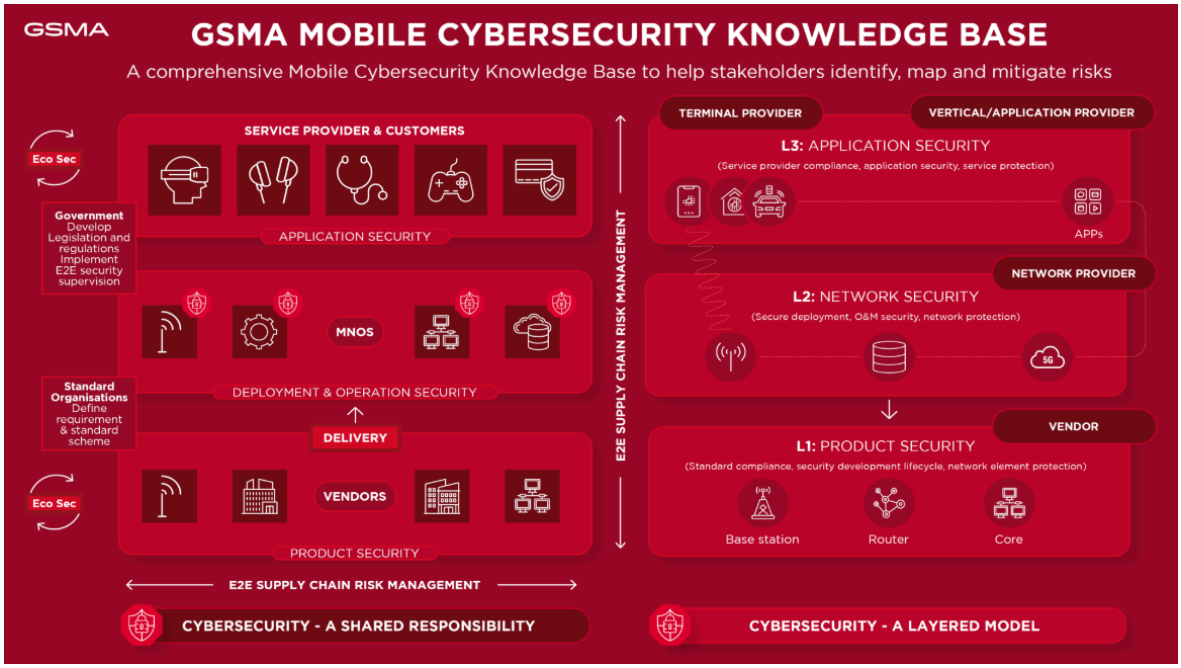


Figura 4.1 Base de conocimientos sobre ciberseguridad móvil de la GSMA[10]

En primer lugar, los organismos gubernamentales elaboran estrategias nacionales de ciberseguridad y promulgan legislación específica para implementar una supervisión integral de la seguridad en todo el ciclo de vida de las redes. Por ejemplo, los países de la Unión Europea

[10] https://www.gsma.com/solutions-and-impact/technologies/security/cybersecurity-knowledge-base/

han desarrollado leyes nacionales conforme a la Directiva NIS2, que obliga a las entidades a aplicar medidas de seguridad para gestionar los riesgos de ciberseguridad. Estas medidas incluyen la creación de sistemas de gobernanza en ciberseguridad y la obligación de notificar los incidentes de seguridad detectados. Además, se establecen sanciones específicas por el incumplimiento de dichas obligaciones.

En segundo lugar, los organismos de estandarización desarrollan normas de ciberseguridad y buenas prácticas, estableciendo referencias unificadas que sirven como plantillas técnicas reutilizables para empresas de distintos tamaños. Esto ayuda a reducir la brecha de capacidades, fomenta la gestión de riesgos estandarizada, y promueve la colaboración tecnológica y la confianza mutua dentro del ecosistema 5G.

En tercer lugar, los fabricantes de equipos deben garantizar la seguridad de los equipos a nivel de producto (L1, “Level 1”: nivel 1 en la figura 4.1), siguiendo procesos de desarrollo seguro que aseguren que los dispositivos cumplen con los requisitos normativos y los estándares de seguridad. Estos productos deben superar procesos de certificación como NESAS[11]/SCAS[12], y estar sujetos a un modelo de gestión del ciclo de vida seguro.

En cuarto lugar, los operadores de red deben cumplir con los requisitos de seguridad a nivel de red (L2, nivel 2 en la figura 4.1). Esto implica aplicar una gestión de la seguridad integral desde el despliegue hasta la operación de la red, con el objetivo de reforzar las capacidades de protección y resiliencia del entorno de red.

En quinto lugar, los proveedores de servicios y los usuarios finales son responsables de implementar medidas de seguridad en el nivel de aplicación (L3, nivel 3 en la figura 4.1). En los casos en los que una red privada 5G se despliega de forma independiente, es común que el proveedor de red asuma también la responsabilidad de la seguridad en la capa de aplicación (L3).

4.2 Mejora de la protección de redes privadas 5G mediante una operación y mantenimiento seguros

De acuerdo con el análisis previo, los pilares fundamentales para fortalecer la seguridad en redes privadas 5G son dos:

1. Que los **fabricantes de dispositivos** proporcionen productos seguros y confiables.
2. Que los **proveedores de red** gestionen de forma eficaz la operación y mantenimiento de la seguridad de la red.

La experiencia del sector demuestra que el coste de la seguridad reactiva (post-incidente) es extremadamente alto. Por ello, la seguridad debe integrarse desde el inicio del ciclo de desarrollo de los productos. El concepto clave consiste en incorporar medidas de ciberseguridad en todas las fases del ciclo de vida del producto: desde la planificación, diseño, codificación y pruebas,

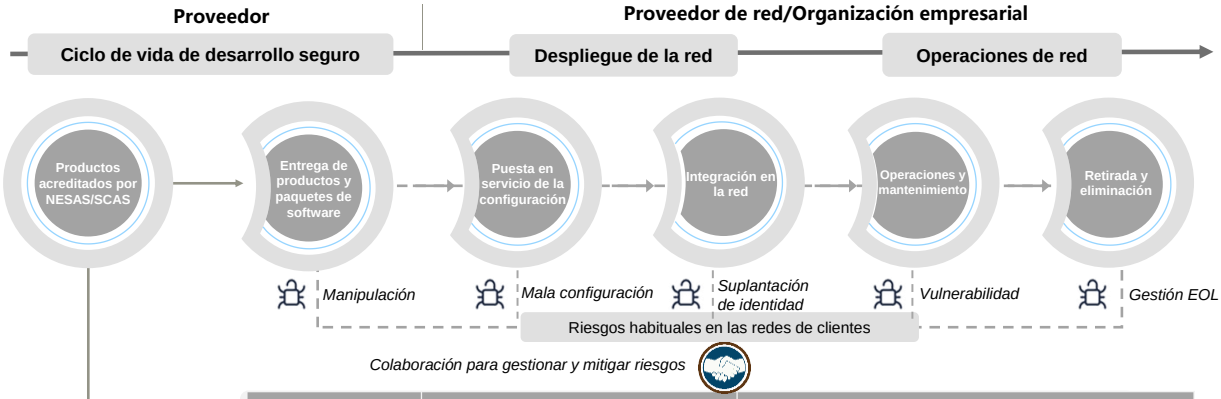
[11] https://www.gsma.com/solutions-and-impact/industry-services/assurance-services/network-equipment-security-assurance-scheme-nesas/
[12] https://www.3gpp.org/technologies/scas-cert

hasta la liberación, investigación y mantenimiento. Incluir actividades de seguridad en cada etapa reduce la probabilidad de introducir vulnerabilidades de software y refuerza la protección del producto.

La GSMA y el 3GPP han definido un esquema unificado de certificación —NESAS/SCAS— para dispositivos de red móvil, que garantiza la implementación de controles de seguridad obligatorios por parte de los fabricantes.

En cambio, la gestión operativa de la seguridad de red representa un reto mayor: cómo aplicar de forma eficaz las capacidades de seguridad disponibles en los dispositivos a la operación de red, de manera que se cumplan los requisitos establecidos por las normativas y se eleve el nivel de protección de las organizaciones empresariales.

A partir de las mejores prácticas de seguridad del sector, se proponen las siguientes medidas clave para mitigar los cinco principales riesgos del ciclo de vida de las redes 5G, tal como se muestra en la Figura 4.2.



Riesgo típico	Medidas de control	Descripción
Manipulación	Protección de la integridad del producto	Firmas digitales y plataforma de actualización en línea
Mala configuración	Gestión de la configuración de seguridad	Líneas de base de configuración de seguridad y herramientas de comprobación de la configuración
Suplantación de identidad	Gestión de certificados digitales	Soluciones de despliegue y explotación de certificados
Vulnerabilidad	Gestión de vulnerabilidades	Mecanismo de gestión de vulnerabilidades y múltiples métodos de divulgación de vulnerabilidades
Gestión del final de la vida útil (EOL)	Gestión del ciclo de vida	Planificación y criterios del fin de la vida útil, desmantelamiento de productos, supervisión posterior al fin de la vida útil

Figura 4.2 Cinco riesgos principales y medidas de seguridad clave en el ciclo de vida de redes 5G

4.2.1 Protección de la integridad

Durante la fase de lanzamiento comercial del producto a usar en el despliegue de redes 5G, el fabricante de dichos productos debe proporcionar una solución de protección de integridad y emplear firmas digitales para garantizar que el software no ha sido alterado durante su distribución, instalación o actualización.

4.2.2 Gestión de la configuración de seguridad

Durante la fase de lanzamiento comercial del producto, el fabricante debe publicar la línea base de configuración de seguridad del producto y su correspondiente guía de configuración. Durante

la fase de despliegue, las organizaciones deben garantizar que la implementación no introduce riesgos de seguridad, basándose para ello en la guía de configuración de seguridad del producto. Ya en la fase de operación y mantenimiento, las organizaciones deben ser capaces de identificar y fortalecer (hardening) los elementos de configuración de seguridad para evitar que configuraciones deficientes se conviertan en vulnerabilidades del sistema.

4.2.3 Gestión de certificados digitales

El fabricante de dispositivos debe proporcionar soporte para el despliegue y administración de certificados digitales. Por su parte, las organizaciones deben gestionar la revocación y sustitución de certificados de acuerdo con el contexto de riesgo en la red.

4.2.4 Gestión de vulnerabilidades

El fabricante de dispositivos debe publicar información sobre vulnerabilidades de forma oportuna, mientras que las empresas deben aplicar las correcciones pertinentes lo antes posible, en función de la criticidad y la exposición descrita en los boletines de seguridad del proveedor.

4.2.5 Gestión del ciclo de vida del producto

El fabricante debe definir un plan claro de gestión del ciclo de vida del producto, incluyendo el plan de fin de soporte (EOS, End of Support). A su vez, las organizaciones deben elaborar estrategias de retirada segura de productos de la red, en función del plan de fin de vida, para evitar riesgos derivados de la ausencia de soporte técnico y actualizaciones de seguridad una vez finalizado su ciclo de vida.

4.3 La gestión de la configuración de seguridad es una medida de seguridad clave importante pero fácil de pasar por alto

La norma 3GPP especifica las capacidades de seguridad que debe tener un dispositivo. Sin embargo, no todas las capacidades de seguridad son obligatorias. Por ejemplo, según 3GPP TS 33.501, el gNodeB debe soportar el cifrado de datos de usuario entre el UE y el gNodeB pero la protección de la confidencialidad es opcional. La habilitación del mecanismo de protección depende de si el algoritmo de cifrado de seguridad está habilitado en la red. Esta gestión de la configuración suele ignorarse durante la operación y mantenimiento de la red, lo que conlleva riesgos para la seguridad. Además, la gestión de la configuración de seguridad es importante por las siguientes razones:

1. **Cumplir los requisitos de conformidad con normativas y políticas de seguridad:**

   Cada vez más leyes, reglamentos y normas exigen la gestión de la configuración de seguridad. El incumplimiento provocará riesgos de conformidad.

- **La ENS[13] española (Real Decreto 311/2022)**

  La certificación ENS de España exige una configuración de seguridad, como se muestra en la Tabla 4.1.

Tabla 4.1 Requisitos relacionados con la configuración de seguridad en el ENS

Medidas de seguridad	Requisitos
4.3.2 Configuración de seguridad [op.exp.2]	Los ordenadores se configurarán antes de su entrada en funcionamiento, de forma que: - [op.exp.2.1] Se retirarán las cuentas y contraseñas estándar. - [op.exp.2.2] Se aplicará la regla de "mínima funcionalidad" - [op.exp.2.3] Se aplicará la regla de "seguridad por defecto" - op.exp.2.4] Las máquinas virtuales deberán estar configuradas y gestionadas de forma segura.
4.3.3 Gestión de la configuración de seguridad [op.exp.3]	Se gestionará de forma continua la configuración de los componentes del sistema, de manera que se: - [op.exp.3.1] Mantenga siempre la regla de "funcionalidad mínima" (op.exp.2). - op.exp.3.2] Mantenga siempre la regla de "mínimo privilegio" (op.exp.2) - [op.exp.3.3] Adapte el sistema a nuevas necesidades, siempre que estén previamente autorizadas (ver op.acc.4) - [op.exp.3.4] Reaccione ante vulnerabilidades notificadas (ver op.exp.4) - op.exp.3.5] Reaccione ante incidentes de seguridad (ver op.exp.7) - [op.exp.3.6] Restringa la edición de configuración a personal debidamente autorizado.

- **ISO 27002 Control A.8.9[14]**

  La Gestión de la Configuración requiere que las organizaciones gestionen las configuraciones para asegurar la integridad y reducir las vulnerabilidades.

2. **Configuraciones inseguras ocurrirán en la red.**

   Con el avance de las nuevas tecnologías (como la IA o la computación cuántica), los algoritmos y protocolos considerados inicialmente como seguros pueden volverse inseguros cuando los productos ya han sido lanzados comercialmente y desplegados en redes de empresas. Los algoritmos originales y las configuraciones de protocolo heredadas durante la actualización de la red se convierten en la principal fuente de configuraciones inseguras. Por ejemplo:

   - La mejora de la capacidad computacional convertirá a un algoritmo seguro original en un algoritmo inseguro tal como ocurre, por ejemplo, con la longitud de la clave considerada segura para el algoritmo RSA, que a principios de los 2000 era de 1024 bits y hoy en día se recomienda que no sea menor de 3072.

[13] https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191
[14] https://www.iso.org/standard/75652.html

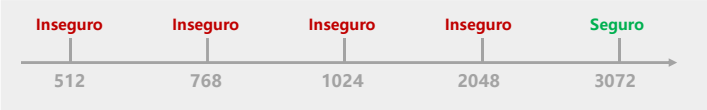


Figura 4.3 Evolución de la longitud de la clave RSA

- A medida que se revelan vulnerabilidades, los protocolos seguros originales se convertirán en protocolos inseguros, como ocurrió con la versión 3.0 de SSL y posteriormente con las versiones 1.0 y 1.1 de TLS..

Figura 4.4 Evolución del protocolo SSL/TLS

3. **Los problemas de configuración insegura también se producen cuando se despliegan nuevos productos en la red.**

   Cuando se lanza un nuevo producto, la seguridad puede implementarse por defecto. Sin embargo, cuando el producto se despliega en una red, la capacidad de seguridad del nuevo producto puede degradarse debido a las insuficientes capacidades de seguridad de los dispositivos existentes. Por ejemplo, cuando un nuevo producto necesita sincronizar su reloj con un servidor NTP, puede verse degradado a utilizar el algoritmo MD5 porque el servidor NTP sólo admite el algoritmo de “resumen de mensajes” (“hash”, usado para asegurar la integridad) MD5, aunque el nuevo producto admita el algoritmo de resumen de mensajes SHA256.

Basándose en el análisis anterior, esta guía se centra en la orientación práctica para la gestión de la configuración de seguridad en la operación de seguridad de la red privada 5G.

Capítulo 5: Buenas prácticas en la Gestión de la Configuración de Seguridad de la Red Privada 5G

5.1 Conceptos Relacionados con la Gestión de la Configuración de Seguridad

Existen diferentes definiciones para los conceptos relacionados con la gestión de la configuración de seguridad en la industria. Por ejemplo, ISO 10007:2017 define los elementos de configuración como: **Elemento de configuración (Configuration Item, CI):** entidad dentro de una configuración que satisface una función de uso final[15]. Por su parte, NIST SP 800-128 lo define como: **Elemento de configuración (CI):** es una parte identificable de un sistema (por ejemplo, hardware, software, firmware, documentación o una combinación de los mismos) que es un objetivo discreto de los procesos de control de configuración[16].

Este documento define los conceptos relacionados con la gestión de la configuración de seguridad de la siguiente manera, basándose en las definiciones de los términos en varios estándares de la industria:

- **Configuración**

  Indica los ajustes utilizados para controlar el estado de los productos y sistemas.

- **Elemento de configuración**

  Parámetro utilizado para controlar las funciones/características de productos y sistemas, por ejemplo, habilitar o deshabilitar una función o característica específica.

- **Elemento de configuración de seguridad**

  Elemento de configuración que controla el estado de seguridad de los productos y sistemas, con el objetivo de reducir los riesgos de seguridad de la red durante el uso del sistema. Los elementos de configuración de seguridad se clasifican en los siguientes tipos:

  1) Elementos de configuración que están directamente relacionados con las funciones y características de seguridad de red de los productos y sistemas, incluidas las cuentas, las contraseñas y algoritmos criptográficos; por ejemplo, como el número de intentos de inicio de sesión fallidos antes de aplicar un bloqueo de la cuenta cuyo inicio de sesión se está intentando.

  2) Elementos de configuración que no están directamente relacionados con las funciones o características de seguridad de la red en productos y sistemas, pero que están configurados incorrectamente, por ejemplo, elementos de configuración relacionados con servicios y puertos innecesarios, que aumentarán el riesgo de intrusión.

[15] https://www.iso.org/standard/70400.html
[16] https://doi.org/10.6028/NIST.SP.800-128

- **Línea base de configuración (o "configuration baseline")**

  Conjunto aprobado de normas relacionadas con los elementos de configuración (CI) que determinan la funcionalidad y las características de los productos y sistemas en un momento dado y que sólo pueden modificarse mediante el proceso de control de cambios.

- **Línea base de configuración de seguridad (o "security configuration baseline")**

  Se trata de una línea base de configuración para controlar el estado de seguridad de los productos y sistemas en función del equilibrio entre los costes de seguridad y los riesgos de seguridad asumibles. Sirve de referencia básica para las actividades de gestión y control de la seguridad en el ciclo de vida de los productos y sistemas.

- **Gestión de la configuración de seguridad**

  Conjunto de actividades de gestión y control centradas en la configuración de seguridad de productos y sistemas. El objetivo de la gestión es garantizar que los productos y sistemas cumplen los objetivos de seguridad y gestión de riesgos definidos por la organización.

5.2 Introducción al proceso de gestión de la configuración de seguridad

Como un contenido importante de la gobernanza de la seguridad de la empresa, la gestión de la configuración de seguridad debe integrarse en los procesos de operación y mantenimiento de la seguridad del sistema. Teniendo en cuenta que la industria ya dispone de estándares como *ISO/IEC 27002:2022 Control A.8.9: Gestión de la Configuración* y *NIST 800-128 Guide for Security-Focused Configuration Management of Information Systems*, y *CIS (Center for Internet Security) Benchmarks* para recomendaciones específicas de configuración de seguridad para productos y componentes generales, esta guía analiza las prácticas de la red privada 5G desde la perspectiva de la viabilidad para dichas redes. Por lo tanto, se proporciona una guía de bajo nivel para la gestión de la configuración de seguridad para la implementación de una red privada 5G, que incluye cuatro partes: planificación de la gestión de la configuración de seguridad, gestión de activos y análisis de requisitos de seguridad, gestión de la línea base de la configuración de seguridad, e implementación de la línea base de la configuración de seguridad, como se muestra en la Figura 5.1. A continuación, se describe cada uno de estos epígrafes.

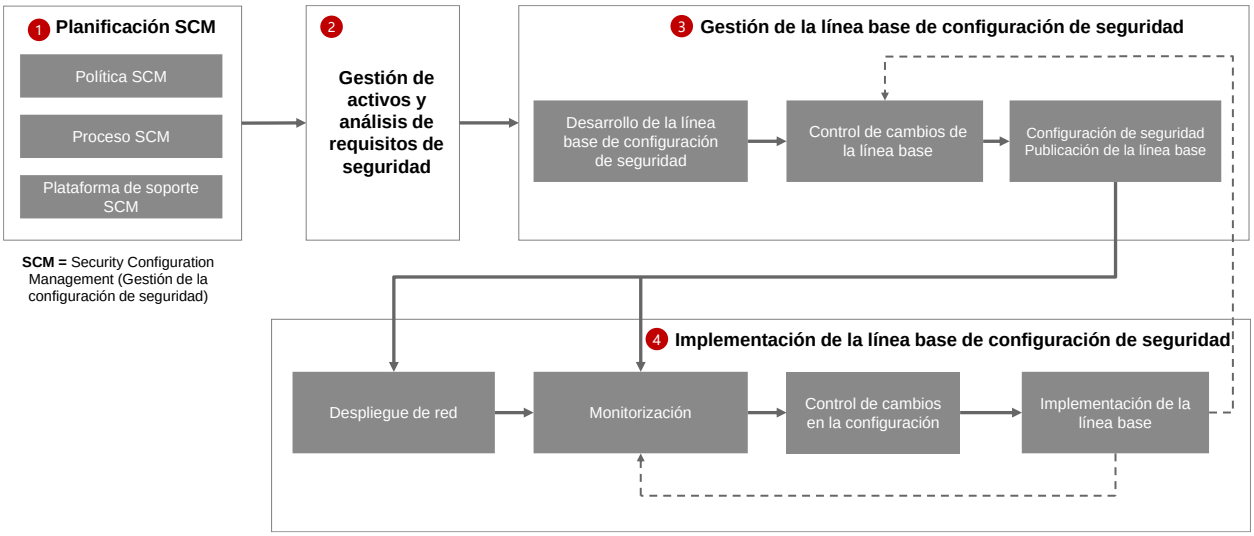


Figura 5.1 Proceso de gestión de la configuración de seguridad

5.3 Planificación de la gestión de la configuración de seguridad

La empresa debe desarrollar un modelo de gobernanza de la seguridad coherente con la estrategia y objetivos de negocio, que incluya políticas de seguridad, normas de gestión de la seguridad en el ámbito empresarial y procesos de gestión de la seguridad.

La estrategia de gobernanza de la seguridad define, en el nivel más alto, cómo la organización gestiona la seguridad de la información. Debe ser aprobada por la alta dirección y estar alineada con los objetivos estratégicos del negocio. A niveles inferiores, esta estrategia debe estar respaldada por políticas de seguridad específicas por dominios, cuando sea necesario, con el fin de reforzar los controles de seguridad de la información y dar respuesta a las necesidades de ciertos grupos dentro de la organización o a áreas de seguridad concretas. Estas políticas específicas deben estar alineadas y ser complementarias con la estrategia general de gobernanza de la seguridad de la empresa. La gestión de la configuración de seguridad es uno de estos ámbitos específicos. Por ello, al abordar esta práctica, las organizaciones deben comenzar por definir un marco de control de seguridad corporativo, tomando como referencia normas internacionales como ISO/IEC 27001.

Además, en las actividades de planificación de la gestión de la configuración de seguridad, se debe aplicar un enfoque descendente (top-down), que permita establecer objetivos de seguridad medibles, verificables y alineados con la estrategia general. Dichos objetivos deben ir acompañados de acciones concretas y resultados esperados que permitan alcanzarlos. A continuación, se detallan los elementos específicos de este enfoque.

5.3.1 Desarrollar políticas de gestión de la configuración de seguridad

Es necesario determinar la estrategia de gestión de la configuración de seguridad basándose en las leyes y regulaciones aplicables, las estrategias generales de seguridad de la empresa, los requerimientos del cliente, los estándares de seguridad de la industria y las mejores prácticas.

- Propósito

  Se deben determinar los objetivos de la política de gestión de la configuración de seguridad y definir el nivel de riesgo aceptable para la empresa. Por ejemplo, garantizar que la configuración de seguridad de todos los activos de TI (servidores, dispositivos de red, entornos de nube y dispositivos) en la red privada 5G cumple con la tolerancia al riesgo de la empresa, los requisitos de cumplimiento de la industria y las mejores prácticas, y reducir continuamente la superficie de ataque, evitando cambios no autorizados. Los objetivos pueden cuantificarse mediante indicadores clave de rendimiento (Key Performance Indicators, KPIs) si es necesario.

- Ámbito

  Se debe definir con precisión qué parte de la red privada 5G se encuentra bajo la cobertura o aplicación de la política de gestión de la configuración de seguridad.

- Organización

  Se debe establecer una estructura organizativa relacionada con las actividades de gestión de la configuración de seguridad y especificar las funciones implicadas y sus responsabilidades.

- Proceso

  Se deben especificar los procesos que deben cubrirse para apoyar las actividades de configuración de seguridad, como el proceso de gestión de activos, el proceso de cambio de línea base y el proceso de cambio de configuración.

- Capacidad de apoyo

  Se deben proponer requisitos para las capacidades de apoyo auxiliares involucradas en la gestión de la configuración de seguridad, incluyendo los requisitos para las plataformas de apoyo de TI, concienciación de seguridad y formación de capacidades, y principios de configuración de seguridad.

5.3.2 Desarrollar el proceso de gestión de configuraciones de seguridad

Para apoyar la implementación de políticas de gestión de configuraciones de seguridad, se deben establecer y mantener procedimientos de ejecución relevantes para las actividades de gestión relacionadas con estas configuraciones de seguridad. Desde la perspectiva de la gestión empresarial, las empresas deben desarrollar primero un sistema unificado de gestión de procesos para apoyar el desarrollo de procesos específicos de gestión empresarial. Por lo tanto, se recomienda establecer normas y reglamentos de gestión de procesos de acuerdo con la norma ISO 9001 y otras normas internacionales antes de desarrollar los procesos de gestión de la configuración de seguridad. Las normas y reglamentos incluyen:

- Especificar los objetivos de la gestión de procesos, guiar a los responsables de los procesos a operar de forma eficaz y mejorar la calidad de la gestión.
- Aclarar los principios de desarrollo del proceso, incluidos los principios de gestión jerárquica, los principios de establecimiento del responsable del proceso y las directrices

de operación.

- Definir las organizaciones, funciones y responsabilidades relacionadas con las operaciones de gestión de procesos.
- Operación rutinaria de procesos: Introducir las reglas básicas para la gestión de operaciones de procesos rutinarios.

Basándose en el sistema de gestión de procesos, los responsables de cada proceso deben establecer los siguientes procesos clave para las actividades de gestión de la configuración de seguridad:

- Proceso de gestión de activos: Se recomienda establecer, implementar, mantener y mejorar continuamente un sistema eficaz de gestión de activos remitiéndose a las normas ISO/IEC 19770-1 para gestionar los activos de manera integral. Abarca todas las etapas, desde la planificación, la adquisición, el despliegue, el uso y el mantenimiento hasta el desmantelamiento final.
- Proceso de desarrollo de la línea base de la configuración de seguridad: incluye las fases de desarrollo de la línea base, aprobación de la línea base, publicación de la línea base y gestión de los cambios de la línea base.
- Proceso de implantación de cambios en la configuración de seguridad: abarca todas las fases de despliegue de la red, supervisión continua, control de cambios en la configuración, rectificación de desviaciones de la configuración y auditoría.

Una vez establecido el proceso, el responsable del proceso lo ejecuta, evalúa y mejora de acuerdo con sus responsabilidades.

5.3.3 Establecer una plataforma de apoyo a la gestión de la configuración de seguridad

Para apoyar la implementación de las actividades de gestión de la configuración de seguridad, las empresas deben establecer las siguientes plataformas de apoyo para implementar mejor las medidas de gestión, incluyendo:

- Sistema de gestión de activos: Mantener información precisa, completa y oportuna sobre los activos. Los datos clave incluyen: identificador único del activo, tipo (hardware, software, servicio, etc.), fabricante/proveedor, modelo/versión, clave SN/licencia, ubicación, propietario/usuario, estado, fecha/coste de adquisición, información de garantía, registros de mantenimiento, fecha de retirada del servicio, servicios asociados y elementos de configuración, etc.
- Repositorio de componentes comunes: almacena los componentes comunes como el sistema operativo, la base de datos, la web, big data y middleware distribuido.
- Repositorio de línea base de configuración de seguridad: contiene las líneas base de configuración de seguridad aprobadas para productos y sistemas.
- Plataforma de herramientas de supervisión de la configuración de seguridad: Gestiona la herramienta de supervisión automática utilizada para identificar desviaciones de la línea base establecida.

5.4 Identificación de activos y análisis de requisitos de seguridad

El sistema de gestión de activos se utiliza para analizar los activos implicados en las redes privadas 5G, determinar el alcance de los activos implicados en la gestión de la configuración de seguridad y formar una lista de activos, incluida la lista de hardware, la lista de sistemas de servicios y la lista de componentes comunes.

A partir de este inventario de activos, se realiza un análisis de requisitos teniendo en cuenta las leyes y regulaciones aplicables, las prácticas de seguridad del sector y los objetivos de gestión de riesgos de seguridad de la propia organización; todo ello con el fin de identificar los requisitos de seguridad específicos para redes privadas 5G. Los pasos recomendados incluyen:

- Análisis de requisitos de cumplimiento: Identificar las obligaciones legales y regulatorias aplicables, como el Reglamento General de Protección de Datos (GDPR) el Esquema Nacional de Seguridad (ENS, RD 311/2022) y el Esquema Nacional de Seguridad específico de 5G (RD 443/2024) en el caso de España.
- Análisis de buenas prácticas del sector: Evaluar los riesgos asociados a las redes 5G privadas en función de especificaciones como GSMA FS.30, entre otras, para identificar riesgos relevantes.
- Análisis de amenazas: Utilizar metodologías de análisis de amenazas como STRIDE (modelo de amenazas de Microsoft) y árboles de ataque (attack tree) para identificar tanto requisitos de seguridad funcionales como no funcionales.

Una vez completado el análisis de requisitos, se generan especificaciones documentadas de requisitos, que proporcionan una base sólida para la posterior definición de la línea base de configuración de seguridad.

5.5 Gestión de la línea de base de la configuración de seguridad

Las líneas base de configuración de seguridad son el núcleo de la gestión de la configuración de seguridad, ya que constituyen la referencia fundamental para la implementación de configuraciones seguras. Por ello, deben estar sujetas a un control estricto, conforme al proceso de gestión de líneas base de configuración de seguridad. La gestión de las líneas base incluye la formulación de la línea base de la configuración de seguridad, el control de cambios de la línea base, y la aprobación de la línea base.

5.5.1 Desarrollo de la línea base de la configuración de seguridad

Al establecer una línea base de configuración de seguridad, primero se debe verificar si existen estándares de facto reconocidos en la industria que puedan aplicarse, basándose en el documento de especificación de requisitos de seguridad. Por ejemplo, se puede establecer la línea base de configuración de seguridad requerida para el sistema de red privada 5G utilizando

referencias como los CIS Benchmarks[17] y el OWASP Top Ten de Seguridad[18] para sistemas operativos, bases de datos y componentes web.

En segundo lugar, en el caso de los sistemas 5G, dado que no existen líneas base de configuración de seguridad maduras en la industria, esta línea base puede establecerse siguiendo el siguiente enfoque. El proceso, tal como se muestra en la figura 5.2, consta de tres partes: identificación de los elementos configurables, establecimiento del conjunto completo de líneas base de configuración de seguridad y definición de líneas base jerarquizadas en función de diferentes niveles de requisitos. A continuación, se describe en profundidad cada uno de ellos.

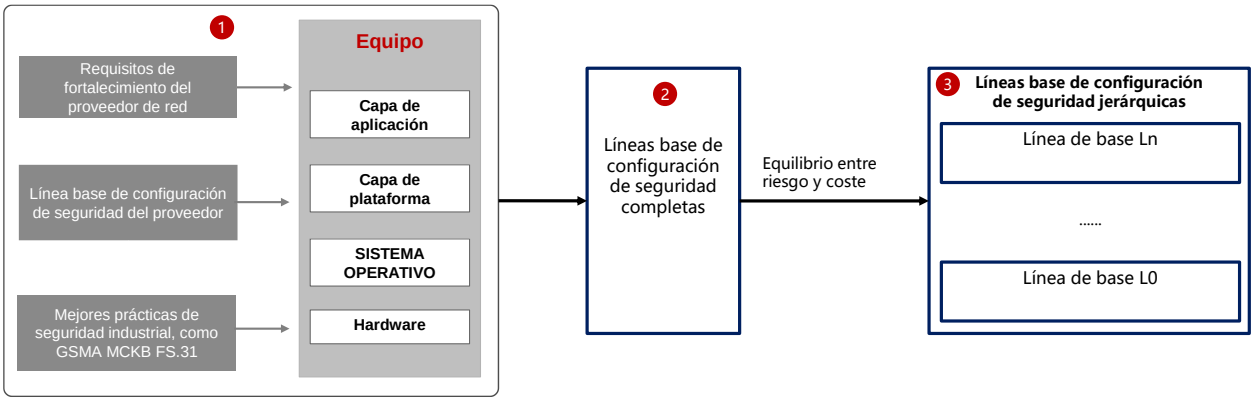


Figura 5.2 Desarrollo de la línea base de configuración de seguridad

Identificar los elementos configurables

Analizar la correspondencia entre los requisitos de seguridad específicos y las capacidades de seguridad específicas del dispositivo, en función de la identificación de activos y el análisis de requisitos de seguridad. Si las funciones del dispositivo exigidas por los requisitos de seguridad son obligatoriamente válidas (es decir, no configurables), no es necesario incluirlas en la línea base de configuración de seguridad para su gestión. Por ejemplo, de acuerdo con el primer requisito de la medida de control BC-013 del estándar GSMA MCKB FS.31:

> *"Los fabricantes deben admitir tecnologías de verificación de integridad en sus productos/soluciones, incluidas firmas digitales en paquetes de software/firmware y mecanismos seguros de entrega para hardware y software"*

Por tanto, no es necesario incluir este aspecto dentro del alcance de la gestión de configuración de seguridad si la verificación de integridad del software que ofrece el dispositivo es obligatoria. En cambio, si la capacidad es configurable, entonces debe considerarse dentro de la gestión de configuración de seguridad.

Identificar los ítems de configuración de seguridad para establecer un conjunto completo de líneas base

Los elementos de configuración de seguridad deben identificarse según los siguientes principios:

[17] https://www.cisecurity.org/cis-benchmarks
[18] https://owasp.org/www-project-top-ten/

1) Ítems de configuración que puedan generar vulnerabilidades de seguridad

   Descripción:
   Si el valor de un ítem de configuración puede colocar al producto en un estado reconocido como inseguro por la industria, dicho ítem debe considerarse como un ítem de configuración de seguridad.

   Ejemplos:

   - Si el valor de configuración incluye un algoritmo inseguro, una versión obsoleta de protocolo o una opción de autenticación deshabilitada, ese ítem debe clasificarse como configuración de seguridad.
   - Si el valor del ítem en la línea base es seguro, pero se considera potencialmente inseguro en futuras evoluciones, también debe incluirse como configuración de seguridad.

2) Ítems de configuración que puedan ampliar la superficie de ataque del producto

   Descripción:
   Cuando un ítem de configuración controla el acceso externo, se debe clasificar como un ítem de configuración de seguridad.

   Ejemplos:

   - Si el ítem “habilita/deshabilita puertos externos”, como un interruptor de punto de acceso Wi-Fi o el puerto de mantenimiento local, este debe gestionarse como ítem de configuración de seguridad.

3) Ítems de configuración que puedan fortalecer las capacidades de seguridad del producto

   Descripción:
   Cuando el ítem habilita funciones de protección de seguridad, debe considerarse como configuración de seguridad.

   Ejemplos:

   - Para mejorar la capacidad de defensa frente a ataques, se deben incluir ítems como la activación de funciones anti-flood y anti-DDoS.

4) Ítems de configuración relacionados con leyes y regulaciones

   Descripción:
   Cuando un ítem de configuración está vinculado a un requisito normativo o regulatorio, debe tratarse como ítem de configuración de seguridad.

   Ejemplos:

   - Si una norma nacional exige explícitamente que se incluya un parámetro de activación para llamadas de emergencia, dicho parámetro debe considerarse un ítem de configuración de seguridad.

Establecer líneas base jerarquizadas en función de diferentes requisitos

Dado que los distintos sectores verticales tienen requisitos de seguridad distintos para redes

privadas 5G y ponen el foco en diferentes tipos de riesgos, es necesario estratificar el conjunto completo de líneas base para aplicar las medidas de seguridad de manera más efectiva y equilibrar la seguridad con el impacto que su implementación puede tener en el negocio.

Se recomienda aplicar los siguientes criterios de evaluación integral para la clasificación de líneas base, tal como se muestra en la Tabla 5.1.

Tabla 5.1 Evaluación de la clasificación de la línea base

Evaluación cualitativa	
Criterios = Riesgo para la seguridad x Impacto para la empresa x Viabilidad de la implantación	
Dimensión	**Descripción**
Riesgo para la seguridad	Determinar el nivel de riesgo correspondiente al elemento de configuración de seguridad en función de los requisitos empresariales del sector. Cuanto mayor sea el riesgo, mayor será la posibilidad de que se incluya en el nivel de referencia empresarial correspondiente. Los niveles de riesgo son los siguientes: Alto, Medio, Bajo y Advertencia.
Impacto en los servicios	Determinar el impacto de los cambios en los elementos de configuración de seguridad en función de los servicios del sector. Cuanto menor sea el impacto, mayor será la probabilidad de que se incluya la línea base de nivel de servicio. El impacto incluye el impacto sobre las funciones y el rendimiento del servicio. Niveles de impacto: Alto, Medio y Bajo
Viabilidad de la implantación	Determinar la viabilidad de implantar cambios en los elementos de configuración de seguridad en función del sector. Cuanto mayor sea la viabilidad, mayor será la probabilidad de incorporar los cambios en la línea de base del nivel correspondiente del negocio. Los niveles de viabilidad se dividen en: Alto, Medio y Bajo.

Comprobar la línea base

La línea base de configuración de seguridad debe ser verificada en un entorno de pruebas con el fin de evaluar su viabilidad de implementación. Los problemas identificados durante la fase de pruebas deben ser registrados detalladamente y se deben proponer soluciones adecuadas. Una vez finalizado el proceso de prueba, se debe elaborar un informe de pruebas y remitirlo al Comité de Revisión de Cambios (Change Review Board) para su evaluación integral y toma de decisiones, utilizándolo como documentación justificativa para el proceso de revisión del cambio.

5.5.2 Gestión de cambios en la línea base de la configuración de seguridad

Para garantizar la exactitud y fiabilidad de la línea base de configuración, los cambios en dicha línea base deben ser gestionados conforme al proceso de gestión de cambios. La gestión de cambios de la línea base incluye los siguientes pasos clave:

1. Presentación y registro de la solicitud de cambio

- Solicitud de cambio: El responsable designado según el proceso de gestión de la línea base de configuración de seguridad debe presentar la solicitud de cambio, la cual debe incluir el motivo del cambio, el objetivo esperado y el impacto potencial que pueda generar sobre la línea base.
- Registro de la solicitud: La solicitud de cambio debe ser registrada en el sistema de control de cambios o en el documento correspondiente, con el fin de garantizar la transparencia y la trazabilidad del proceso.

2. Revisión del cambio

- Comité de Revisión de Cambios (Change Control Board, CCB): Se debe constituir un comité específico de revisión de cambios, que incluya representantes del equipo de seguridad, del equipo de servicios de red privada 5G, del equipo de red y del equipo de operación y mantenimiento (O&M).
- Evaluación del cambio: El comité debe valorar la racionalidad del cambio, el alcance del impacto, los problemas potenciales y el plan de recuperación ante posibles fallos.
- Evaluación de riesgos: Se deben analizar los riesgos de seguridad asociados al cambio propuesto, así como realizar una verificación de cumplimiento normativo, asegurando que los cambios se alinean con las políticas de seguridad y con la legislación aplicable (como el RGPD, ENS 5G, la ISO/IEC 27001/27002 mencionados por el propio ENS 5G, etc).

3. Toma de decisión sobre el cambio

A partir del resultado de la revisión, el Comité de Revisión de Cambios (CCB) decidirá si el cambio es aprobado o rechazado.

- Para los cambios aprobados, se deben definir:
  - La fecha de implementación
  - El responsable de ejecución
  - Los recursos necesarios
- Para los cambios rechazados, se debe documentar de forma detallada la justificación del rechazo.

La documentación necesaria para este proceso incluye, entre otros:

- Informes de evaluación de riesgos
- Listas de verificación de cumplimiento
- Registros de aprobación o rechazo del cambio

5.5.3 Publicación de la línea de base de configuración de seguridad

La línea base de configuración de seguridad aprobada debe publicarse en el repositorio usado por la empresa para gestionar las líneas base de configuración de seguridad, de acuerdo con el proceso de publicación y gestión de versiones establecido para este tipo de configuraciones.

- El repositorio de líneas base de configuración de seguridad incluye la línea base de componentes comunes y la línea base por dominios de servicio. La línea base de componentes comunes abarca las configuraciones de seguridad del sistema operativo, base de datos y componentes web. Las líneas base por dominios de servicio se definen en función de la composición del sistema de la red privada 5G, e incluyen configuraciones específicas de seguridad para servicios como estaciones base y núcleo de red.
- Deben aplicarse medidas estrictas de control de seguridad para prevenir la manipulación

de la línea base de configuración de seguridad.

- Se debe auditar periódicamente la línea base publicada para garantizar su vigencia y eficacia.

5.6 Implementación de la línea base de configuración de seguridad

La línea base de configuración de seguridad puede aplicarse en dos fases del ciclo de vida de una red privada 5G: despliegue de la red y operación de la red. En la fase de despliegue, se aplica la línea base de configuración de seguridad a la configuración inicial del sistema de red, siguiendo el principio de seguridad por defecto, para reforzar la protección de la red privada 5G. En la fase de operación, conforme evoluciona el sistema, las medidas de seguridad iniciales pueden quedar obsoletas (por ejemplo, por vulnerabilidades en versiones antiguas de protocolos). Por ello, es necesario monitorizar de forma continua la red contra la última línea base de configuración de seguridad, identificando cualquier desviación.

5.6.1 Fase de despliegue de la red

El objetivo principal en esta fase es garantizar la seguridad por defecto. La implementación de la línea base de configuración de seguridad se basa en los siguientes principios:

1. **Principio de privilegios mínimos**
    - **Descripción:**
      Al desplegar dispositivos de red, el sistema sólo debe poder acceder a los recursos estrictamente necesarios para sus funciones y ofrecer el mínimo de servicios expuestos.
    - **Ejemplo:**
      Controlar de forma estricta las autorizaciones, especialmente las de cuentas administrativas. Por ejemplo, emplear control de acceso basado en roles (RBAC) para gestionar permisos; deshabilitar interfaces inseguras y mecanismos de arranque automático innecesarios; cerrar puertos no usados; eliminar módulos o servicios prescindibles.
2. **Segmentación y aislamiento**
    - **Descripción:**
      Evita la propagación lateral separando la red en subredes y VLANs.
    - **Ejemplo:**
      Aislar la información sensible, las aplicaciones críticas y los sistemas internos de las redes o usuarios externos. Garantizar que el acceso entre dominios esté estrictamente controlado y auditado.
3. **Control de acceso a la red (NAC)**
    - **Descripción:**
      Asegura que solo dispositivos y usuarios que cumplan los estándares de seguridad puedan acceder a la red.

- **Ejemplo:**
  Utilizar NAC para autenticar equipos y verificar que cumplan criterios como parches de sistema operativo y protección antivirus antes de otorgarles acceso. Por ejemplo, emplear IEEE 802.1X para control de acceso a nivel de puerto, validando el cumplimiento de políticas de seguridad.

4. **Encriptación y comunicaciones seguras**
   - **Descripción:**
     Garantizar que toda la información transmitida esté cifrada, evitando su exposición en claro o manipulación.
   - **Ejemplo:**
     Habilitar protocolos de cifrado para todas las comunicaciones de red: SSL/TLS en tráfico web, IPsec para VPNs y SSH para gestión remota. Al configurar acceso remoto, usar túneles VPN cifrados para proteger los datos en tránsito.
5. **Políticas de contraseñas robustas**
   - **Descripción:**
     Todas las cuentas de acceso a dispositivos de red y aplicaciones deben usar contraseñas fuertes para prevenir ataques de fuerza bruta o adivinación.
   - **Ejemplo:**
     Definir requisitos de complejidad (longitud mínima, combinación de mayúsculas, minúsculas, dígitos y caracteres especiales) y forzar cambios periódicos. No emplear contraseñas por defecto ni débiles. Por ejemplo, exigir que las contraseñas administrativas tengan al menos 12 caracteres con mezcla de letras, números y símbolos.
6. **Escaneo de vulnerabilidades y gestión de parches**
   - **Descripción:**
     Analizar dispositivos y sistemas en busca de vulnerabilidades y aplicar parches de seguridad de forma oportuna.
   - **Ejemplo:**
     Realizar un escaneo exhaustivo de vulnerabilidades durante la fase de despliegue para asegurar que todos los sistemas arranquen en estado plenamente parcheado.

5.6.2 Fase de operación de la red

Durante la operación, el foco está en emplear herramientas de automatización para detectar desviaciones de la línea base de seguridad y asegurar que la configuración de dispositivos y servicios cumpla continuamente con los requisitos establecidos.

Monitorización e identificación de desviaciones de la línea base

Para supervisar de modo eficiente la implementación de la línea base en la red en producción, es imprescindible emplear herramientas automáticas de auditoría de configuración.

- **Trasladar la línea base a controles de auditoría:** Convertir la línea base en reglas de configuración (nombre de regla, nivel de riesgo, descripción, valores recomendados, sugerencias de corrección e impacto de la corrección) facilita su aplicación automatizada.
- **Monitorización basada en herramienta:** Usar herramientas, tanto de código abierto como comerciales, para escanear componentes comunes. Se recomienda desarrollar o integrar un sistema evaluador específico para sistemas de red privada 5G, cuya función sea comparar valores de configuración en la red con la línea base y detectar cualquier desviación (ver Figura 5.3).

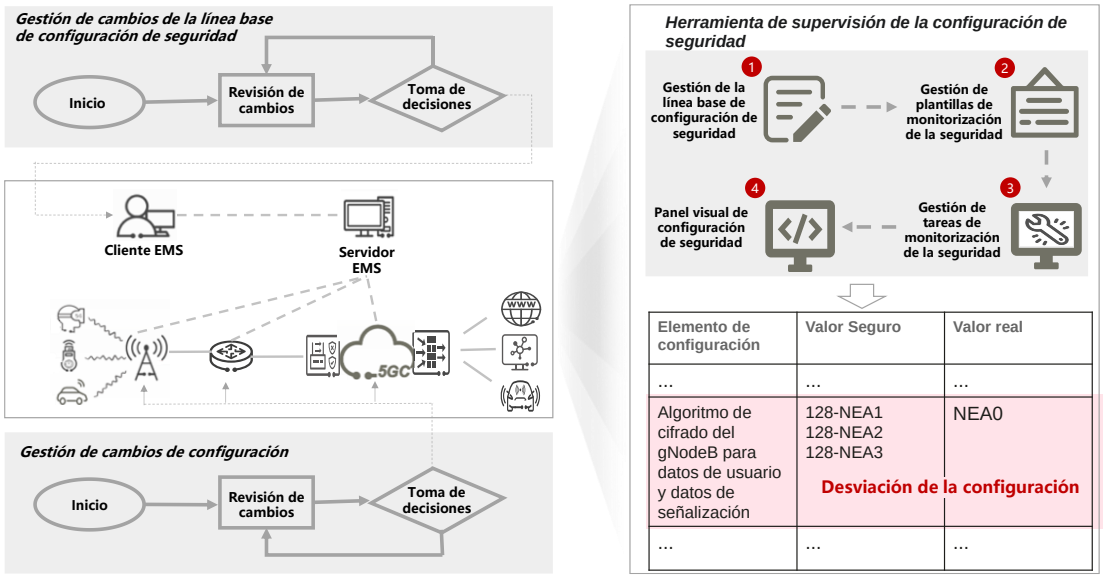


Figura 5.3 Herramienta de monitorización de la configuración de seguridad

Para cumplir con los requisitos de monitorización de las líneas base de configuración de seguridad en distintos escenarios de servicio, la herramienta de monitorización debe ser flexible. Se recomienda que ofrezca las siguientes capacidades:

- **Gestión de líneas base de configuración de seguridad.** Permite personalizar las líneas base de configuración de seguridad. Por ejemplo, si un ítem de configuración de seguridad admite varios valores de distinto nivel, se pueden seleccionar los valores de seguridad necesarios según los requisitos del servicio. Especialmente, una vez que el comité de control de cambios aprueba una modificación de la línea base y la publica oficialmente en el repositorio, la herramienta de monitorización debe actualizarse a la última versión de la línea base de configuración de seguridad.
- **Gestión de plantillas de monitorización de seguridad.** Diferentes tipos de dispositivos y dominios de seguridad tienen diversos requisitos de línea base. La herramienta de monitorización proporciona plantillas para adaptarse a los requisitos de seguridad en distintos escenarios. Cada plantilla puede incluir una línea base de configuración de seguridad distinta.
- **Gestión de tareas de monitorización de seguridad.** Permite asignar distintas plantillas de monitorización a diferentes tareas, para supervisar de forma continua los

dispositivos.

- **Cuadro de mandos con indicadores del nivel de cumplimiento con la línea base deconfiguración de seguridad.** Ofrece los resultados de las tareas de monitorización en distintas dimensiones, mostrando gráficamente los riesgos de configuración de seguridad y mejorando la eficiencia en el cierre de incidencias.

Gestión de cambios en la configuración de seguridad

El proceso de gestión de cambios en la configuración de seguridad es un paso clave para garantizar que la red privada 5G permanezca segura, estable y eficiente durante las modificaciones. Este proceso ayuda a las empresas a gestionar eficazmente los cambios de configuración y a reducir los riesgos y errores asociados. Es similar a la gestión de cambios de las líneas base, con las siguientes diferencias:

- **Solicitud de cambio de configuración.** La presenta el responsable designado por el proceso de operación y mantenimiento de la red privada 5G. Debe incluir el contenido exacto de la configuración a modificar, los sistemas o dispositivos afectados, el efecto esperado tras el cambio, posibles impactos y medidas de reversión (o marcha atrás) en caso de que haya algún problema durante la ejecución que impida que se complete con éxito.
- **Revisión del cambio.** El comité de revisión de cambios de configuración de seguridad, integrado por personal de gestión de recursos y de calidad, evalúa de forma integral el impacto en la red en producción, considerando riesgos de seguridad, costes, calidad y recursos.

Implementación del cambio de configuración de seguridad

- **Elaboración del plan de implementación.** Una vez aprobado el cambio, se redacta el plan de implementación, que incluye el plan de respaldo y recuperación. Se notifica con antelación a los equipos y departamentos implicados para asegurar la coordinación, indicando hora, procedimiento, recursos necesarios y responsables.
- **Ejecución del cambio.** Se llevan a cabo los cambios de configuración en el plazo y condiciones establecidos, asegurando que se sigan todos los pasos conforme al plan. Antes de iniciar, se hace copia de seguridad de la configuración de los sistemas y dispositivos de red. Si durante la ejecución el cambio genera algún impacto negativo, se inicia de inmediato el proceso de reversión (o marcha atrás) para restaurar la configuración original.
- **Verificación y pruebas del cambio.** Tras la implementación, se realizan verificaciones y pruebas exhaustivas para asegurar que la configuración cumple las expectativas y no afecta a otros servicios. Se comprueba que tablas de enrutamiento, listas de control de acceso (ACL), reglas de firewall, etc., estén correctas. Se efectúan pruebas de regresión para garantizar que las modificaciones no interrumpan la configuración existente y que el sistema y las aplicaciones sigan funcionando con estabilidad.
- **Documentación y registro del cambio.** Se documenta cada paso del proceso,

incluyendo información detallada del cambio, resultados de evaluación, procedimientos de implementación y el informe de pruebas. Una vez completados los cambios, los documentos y registros asociados (formulario de registro, informe de resumen de cambio, registros de auditoría, etc.) se archivan para futuras referencias, auditorías y mejora continua.

- **Monitorización y evaluación post-cambio.** Tras la implementación, la herramienta de monitorización automática supervisa de forma continua la estabilidad y seguridad de la red, asegurándose de que no se produzcan desviaciones respecto a la línea base de configuración de seguridad.
- **Resumen y mejora de los cambios de configuración de seguridad.** Al finalizar el proceso, se revisa el desarrollo del cambio, especialmente si se activó la reversión (o marcha atrás), y se evalúa si la línea base de seguridad es adecuada. Si fuera necesario modificarla, se inicia una solicitud de cambio mediante el proceso de gestión de cambios de línea base de configuración de seguridad.

Apéndice

Se adjunta a esta guía el informe de prácticas de configuración de seguridad para el entorno de laboratorio de la red privada 5G. Este documento no se hará público.

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

universidad de león