

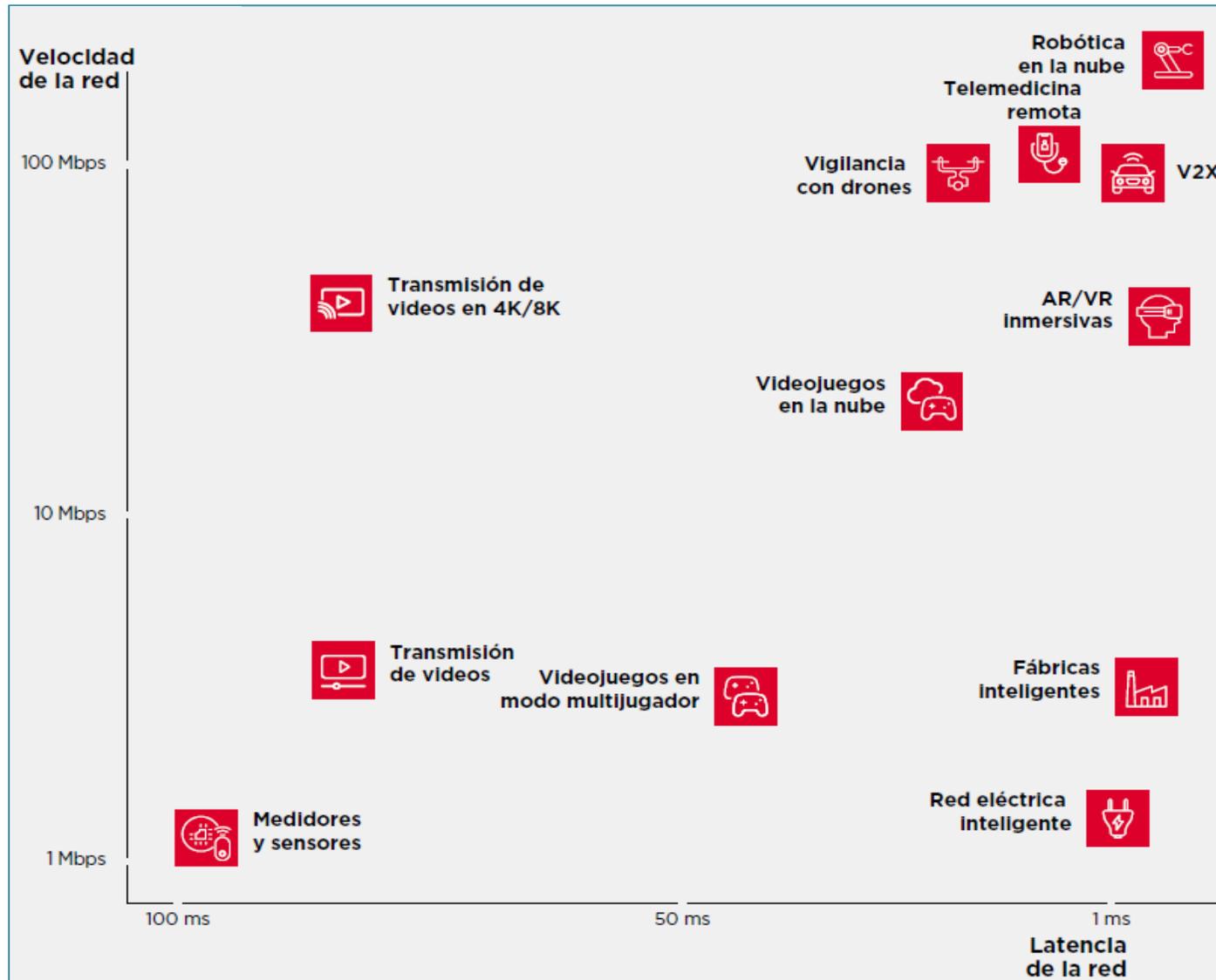
San José, Costa Rica, 25-26 September /septiembre 2023

Implementación de la ciberseguridad en tecnologías 5G y su impacto regulatorio

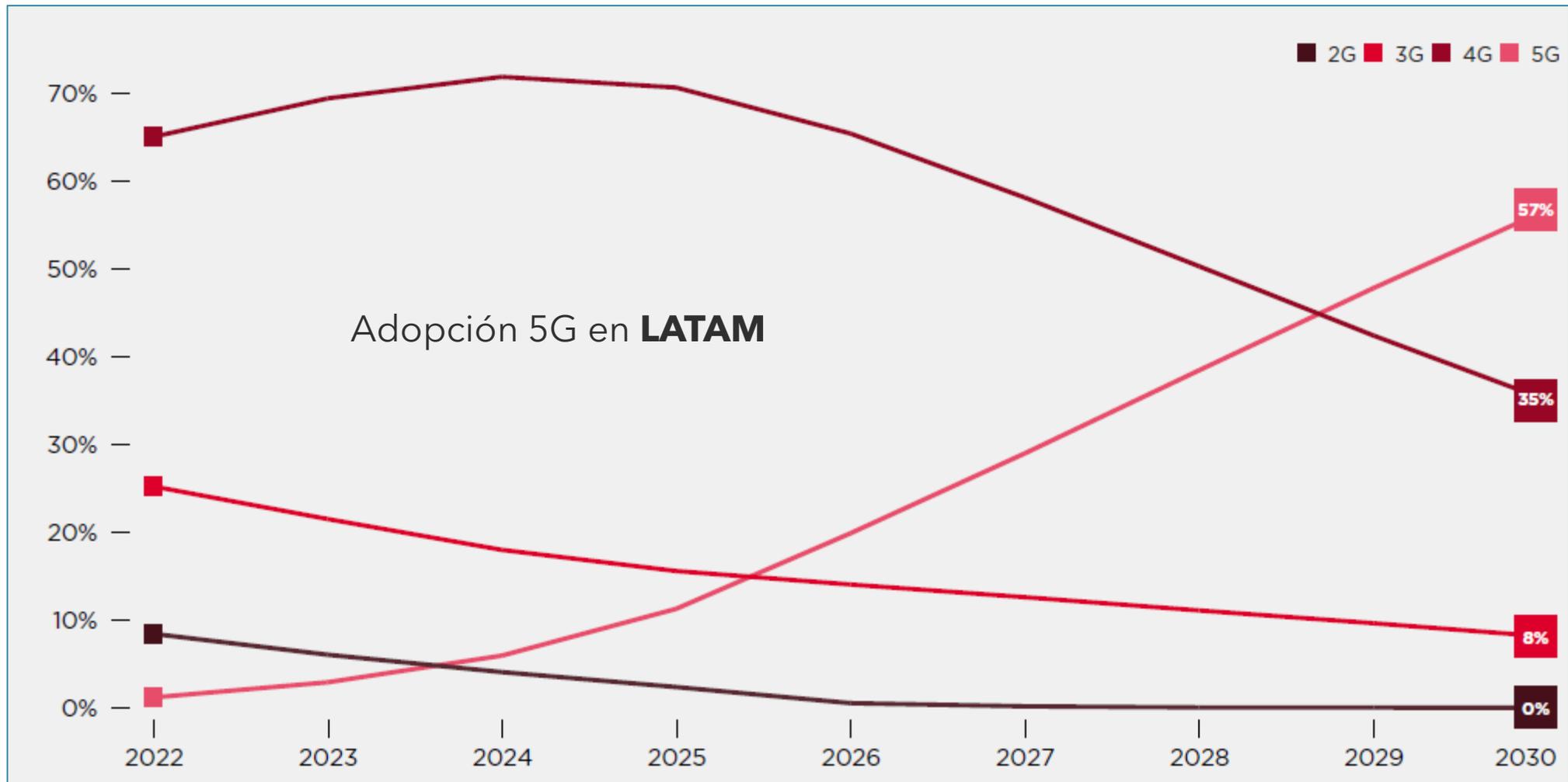
Randall Barnett Villalobos, MSc.
Instituto Costarricense de Electricidad



Casos de uso nuevos y existentes en 5G

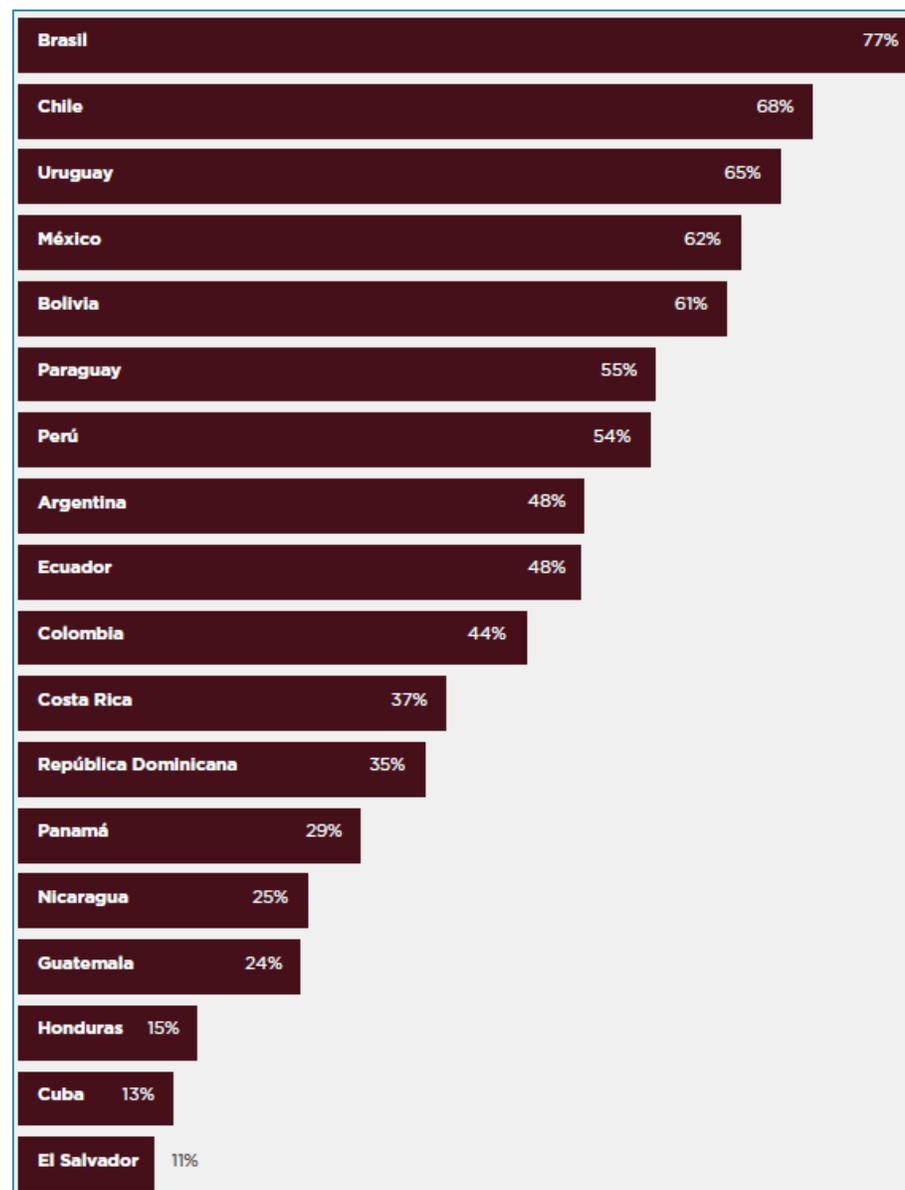


Porcentaje de conexiones totales proyectada 2030

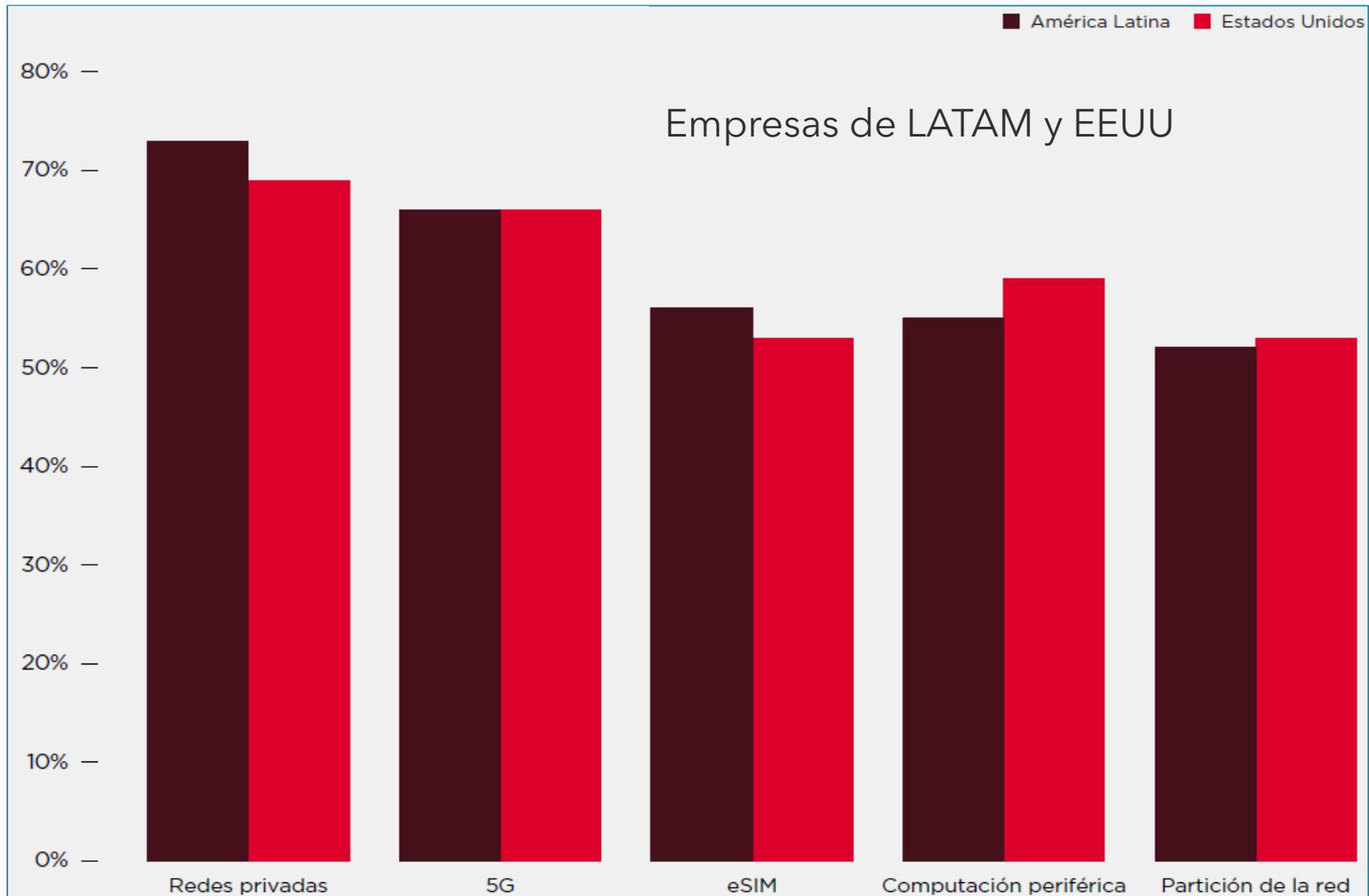


5G en porcentaje del total de conexiones en 2030

Para **2030**, la tecnología 5G representará **más del 50%** del total de conexiones en siete países de **América Latina**



Características más importantes para el despliegue de IoT



Fuente: Encuesta "Enterprise in Focus" de GSMA Intelligence, 2020



El rol clave de las decisiones políticas

Políticas

Políticas públicas pertinentes para 5G se desarrolle en las condiciones adecuadas.

Inversión

Promover las inversiones en 5G, el crecimiento económico y la estabilidad fiscal.

Despliegue

Incentivar la implementación de 5G, en torno a aprobaciones de derecho de vía, despliegues de celdas pequeñas (small cells) y normas de campos electromagnéticos.



Regulación

Regulación más inteligente que cumpla objetivos de manera eficiente, eliminando asimetrías regulatorias, de modo que servicios similares estén sujetos a normas similares.

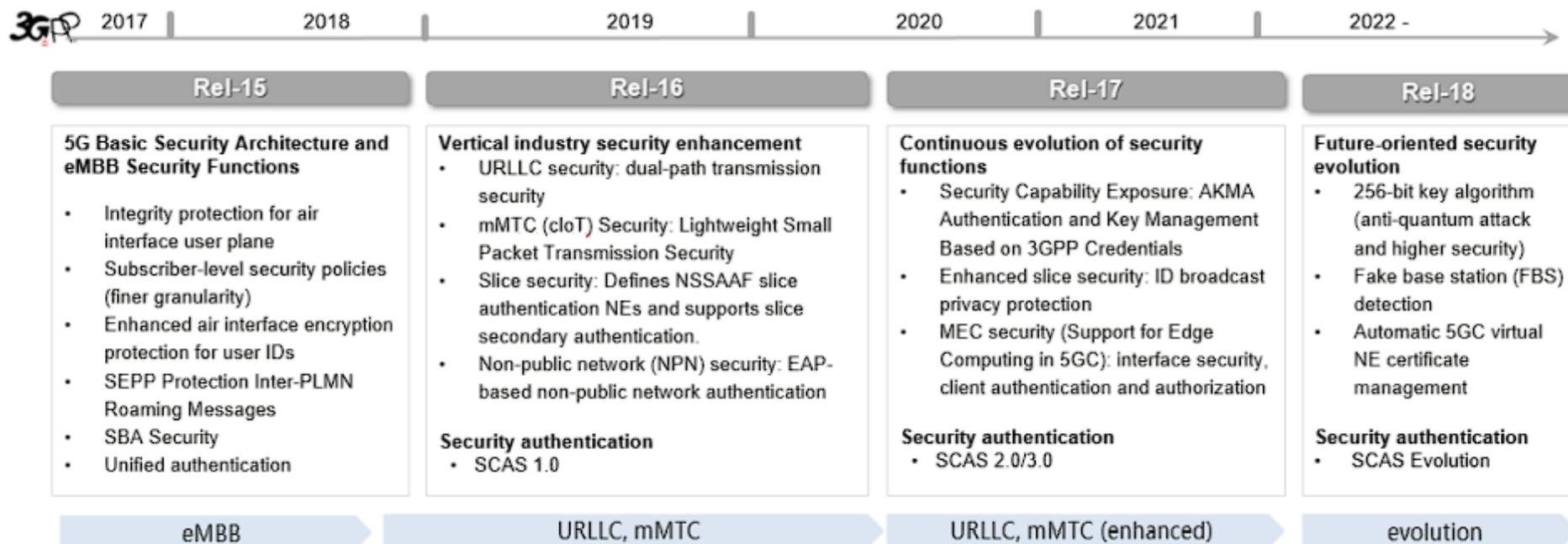
Diálogo

Promover el diálogo entre el sector público y el sector privado.

Seguridad

Impulsar esquemas de seguridad en beneficio del fortalecimiento de las soluciones 5G.

Progreso de las guías de seguridad para 5G según 3GPP



Retos de seguridad en 5G

IoT & M2M

Seguridad incorporada débil en dispositivos IoT, ataques en canales cifrados, casos de uso de: M2M V2X.

Virtualización

Mayor complejidad para mitigar los ataques de canales laterales y proteger arquitecturas cloud-native.

Tecnologías nuevas y legadas

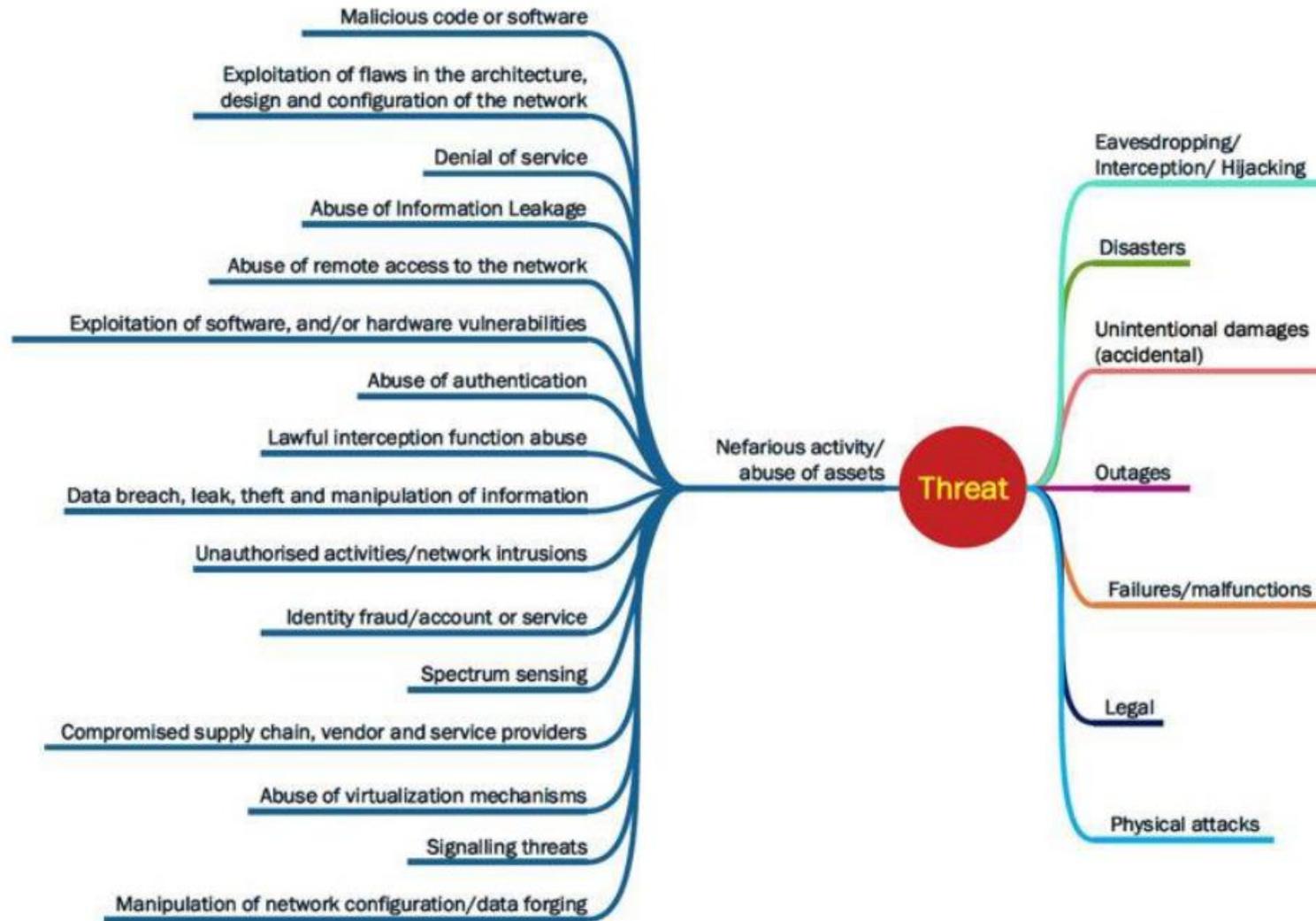
Aumento de los vectores de amenazas en edge computing, network slicing, URLLC (Ultra Reliable Low Latency Communication)

Arquitecturas distribuidas

Convergencia de múltiples tecnologías, migración de amenazas entre tecnologías, incluida la convergencia 5G



Panorama de amenazas 5G



Document title:
GSMA PRD FS.13
Network Equipment Security Assurance Scheme – Overview

This document **Description:** High level explanation of NESAS **Owner:** 

Document title:
GSMA PRD FS.14
Network Equipment Security Assurance Scheme – Security Test Laboratory Accreditation

Description:
Test laboratory accreditation process and requirements

Owner: 

Document title:
GSMA PRD FS.15
Network Equipment Security Assurance Scheme – Development and Lifecycle Assessment Methodology

Description:
Methodology of vendor development and lifecycle processes assessment

Owner: 

Document title:
GSMA PRD FS.16
Network Equipment Security Assurance Scheme – Development and Lifecycle Security Requirements

Description:
Requirements for vendor development and lifecycle processes assessment

Owner: 

Document title: **informative**
GSMA PRD FS.46
Network Equipment Security Assurance Scheme – Audit Guidelines

Description:
Guidelines to Auditors and Equipment Vendors on how to conduct the vendor assessment

Owner: 

Document title:
GSMA PRD FS.47
Network Equipment Security Assurance Scheme – Product and Evidence Evaluation Methodology

Description:
Methodology of product and evidence evaluation

Owner: 

Document title: **informative**
3GPP TR 33.916
Assurance Methodology for 3GPP network products

Description:
Network Equipment Evaluation Process and Creation of SCAS

Owner: 

Document title:
3GPP TS 33.117
Catalogue of General Security Assurance Requirements

Description:
Generic SCAS for all Network Functions

Owner: 

SCAS specific to 3GPP-defined Network Functions are published by 3GPP

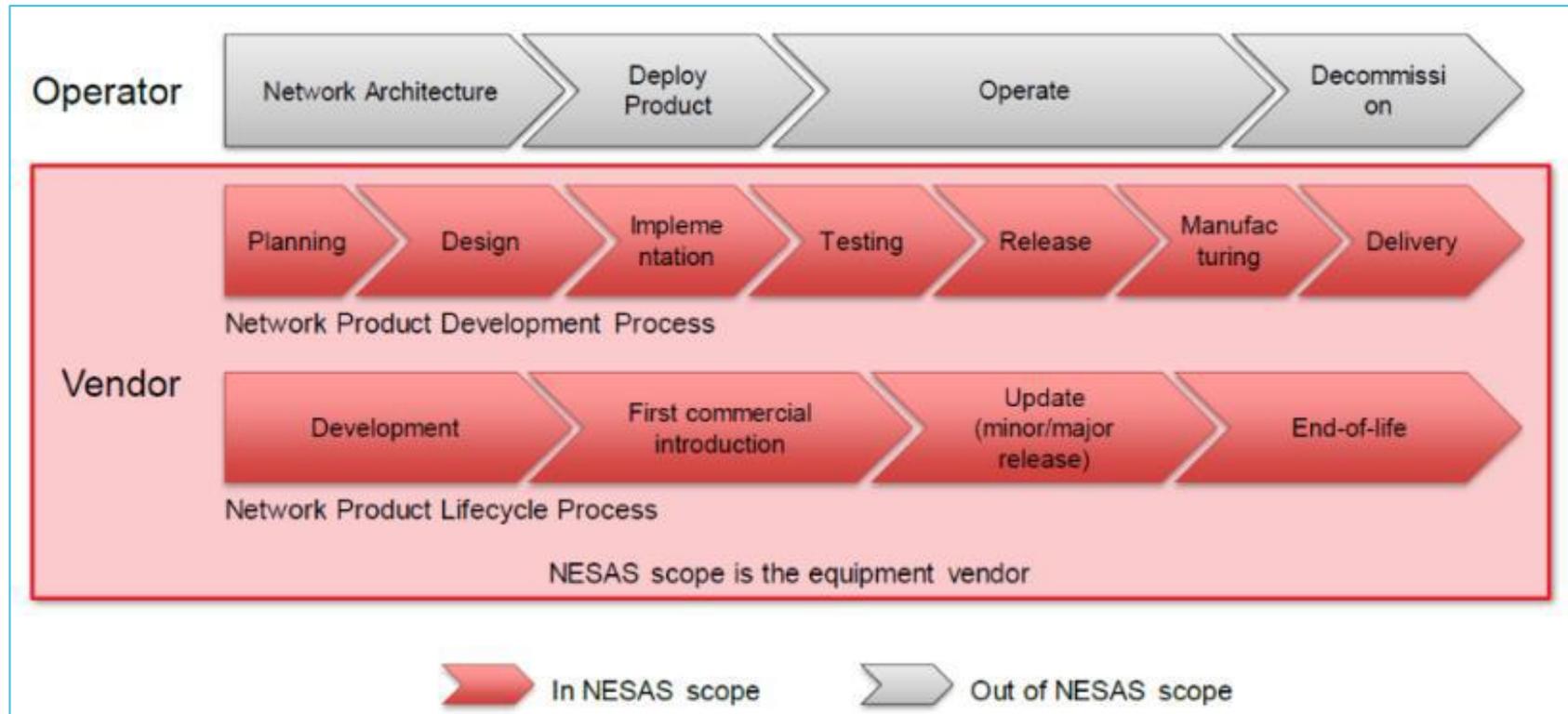
Reference:
<https://www.3gpp.org/DynaReport/33-series.htm>

Owner: 

NESAS 2.2.0



Especificaciones de aseguramiento de la seguridad (SCAS)



Mitigación de amenazas

Device Threats	Air Interface Threats	RAN Threats	Backhaul / Remote DC Threats	5G Packet Core & OAM Threats	SGi / N6 & External Roaming Threats
		Enhanced Visibility & Threat detection Layer			
		DNS Protection Layer			
		Application Protection & Policy enforcement			
		NGFW & DDoS protection Layer			
		Segmentation & Isolation Layer			
		Advanced Malware Protection Layer			

TAKK SKAL DU HA
tānan
BEDANKT
SHUKRAN
KHAWP KHUN
ARIGATOU
DIOLCH
köszönöm
MULTUMESC
DĀKUJEM
mahalo
SPASIBA
GRACIAS
XIE XIE
GRAZIE
toda
YOU
TAKK
TERIMA KASIH RAHMAT
SHUKRAN
Kiitos
PALDIES
OBRIGADO
DHUN YUH VAAD
dzięki
TEŞEKKÜRLER
S' EFHARISTÓ
DANKE
SALAMAT
děkuji vám
GAHM SA HAB NI DA

