De: Torsten Ericsson
Enviados: viernes, 20 de diciembre de 2024 13:02:36 (UTC-04:00) Asunción
Para: Licitación 3500 MHz 5G CONATEL
Cc: Ulrika Grufman; Ambassaden Buenos Aires; GARCIADEVIEDMA Javier (EEAS-ASUNCION); STERNER Fredrik (EEAS-ASUNCION); Emil Lidén; Andrés Jato; Wictoria Amandustin; Lidia Garcia Guijarro
Asunto: Comentarios sobre el Borrador del Pliego de Bases y las Condiciones Generales con referencia a la Licitacion futura de espectro para 5G en Paraguay

Estimados Señores / Estimadas Señoras,

La Embajada de Suecia ante Argentina, Paraguay y Uruguay agradece la posibilidad de comentar sobre el documento referido y presenta sus observaciones abajo. Debido a ciertas inseguridades sobre algunos términos técnicos los presentamos en inglés, contando con que no les resulte un problema.

….

The Embassy of Sweden is aware of the comments made by the United States with reference to this process, and shares their general concerns regarding the lack of specific criteria's in the 5G tender to protect Paraguays national security.

More specifically, we lack more precise criteria as to how a bidding company's cybersecurity measures will be considered. Without additional specificity, this provision could be interpreted arbitrarily, leading to uncertainty for companies bidding on the projects and opening Paraguay's critical telecommunications infrastructure up to additional cyber vulnerabilities.

Also, we notice a lack of supply chain security standards for the ICT-sector. We suggest that Paraguay consider incorporating SCS 9001 into the 5G spectrum tender. SCS 9001 is a comprehensive, measurable, and independently certifiable supply chain security standard for the information and communications technology (ICT) industry. Importantly, SCS 9001 puts the onus on the operator to obtain certification and assess supply chain security, rather than the government doing the assessment.

As you may be aware, the European Union has agreed a comprehensive framework for 5G cybersecurity, the "the 5G toolbox", which includes both technical and non-technical strategic measures, such as in respect to high-risk vendors. For you reference, attaching an overview of the 5G toolbox.

…

La Embajada de Suecia queda a disposición para cualquier consulta o aclaración con respecto a nuestros comentarios. Se agradece nuevamente la oportunidad dado por CONATEL y el Gobierno de Paraguay para comentar sobre este proceso, que tiene el potencial de interesar a empresas suecas y en consecuencia de fortalecer las relaciones comerciales entre nuestros países.

Atentamente,

Torsten Ericsson
Ambassadör / Embajador
Sveriges ambassad i Buenos Aires / Embajada de Suecia en Buenos Aires
Olga Cossettini 731 – 2do. piso
C1107CDA Buenos Aires, Argentina
Tel. +54 11 4319 5100
torsten.ericsson@gov.se
www.swedenabroad.se

Embajada de Suecia
Buenos Aires

Comisión Europea

CAJA DE HERRAMIENTAS DE LA UNIÓN EUROPEA PARA LA SEGURIDAD DE LAS REDES 5G

UN CONJUNTO DE MEDIDAS SÓLIDAS Y GLOBALES PARA UN PLANTEAMIENTO COORDINADO DE LA UNIÓN EUROPEA EN MATERIA DE SEGURIDAD DE LAS REDES 5G

Marzo de 2021
#Cybersecurity

Redes 5G: una nueva tecnología

Si las redes 3G hicieron posible la internet móvil y las 4G permitieron la banda ancha móvil, se prevé que las 5G se conviertan en una infraestructura de conectividad que allane el camino para nuevos productos y servicios e influya en todos los sectores de la sociedad. Los beneficios serán, entre otros, los siguientes:

SANIDAD ELECTRÓNICA

- Seguimiento sanitario a distancia, historiales de pacientes y diagnóstico inteligente
- Uso de robots para ayudar a los cirujanos y mejorar los resultados médicos

REDES ENERGÉTICAS INTELIGENTES

- Líneas eléctricas de alta eficiencia, interrupciones de suministro menores en número y alcance
- Despliegue más fácil con menos repercusiones en el medio ambiente

FÁBRICAS DEL FUTURO

- Mejor control de los procesos internos sensibles al tiempo
- Acceso de control remoto a la maquinaria de almacenamiento

MEDIOS Y ENTRETENIMIENTO

- Una experiencia amplificada de visionado (por ejemplo, realidad virtual)
- Aplicaciones de banda ancha ultrarrápidas (por ejemplo, *streaming* de vídeo)

MOVILIDAD

- Movilidad conectada y automatizada para llegar a cero accidentes
- Conectividad en todos los modos de transporte

Europa es la región más avanzada en el despliegue de ensayos de 5G a gran escala en industrias verticales (en las que a finales de 2020 se habían invertido cerca de 1 000 millones de euros), incluida la 5G para los corredores de transporte. A finales de 2020 estaban disponibles servicios 5G en 500 ciudades europeas.

Ciberseguridad de las redes 5G: una condición previa obligatoria

Las redes 5G son la columna vertebral del futuro de nuestras economías y sociedades cada vez más digitalizadas. Esto afecta a miles de millones de objetos y sistemas conectados, incluidos los utilizados en sectores críticos como la energía, el transporte, la banca y la sanidad, así como los empleados en sistemas de control industrial que contienen información sensible y que sostienen los sistemas de seguridad. Por lo tanto, es esencial garantizar la ciberseguridad y la resiliencia de las redes 5G.

Al mismo tiempo, debido a una arquitectura menos centralizada, a una potencia de computación inteligente puntera, a la necesidad de más antenas y a una mayor dependencia de los programas informáticos, las redes 5G ofrecen más puntos de acceso a los atacantes.

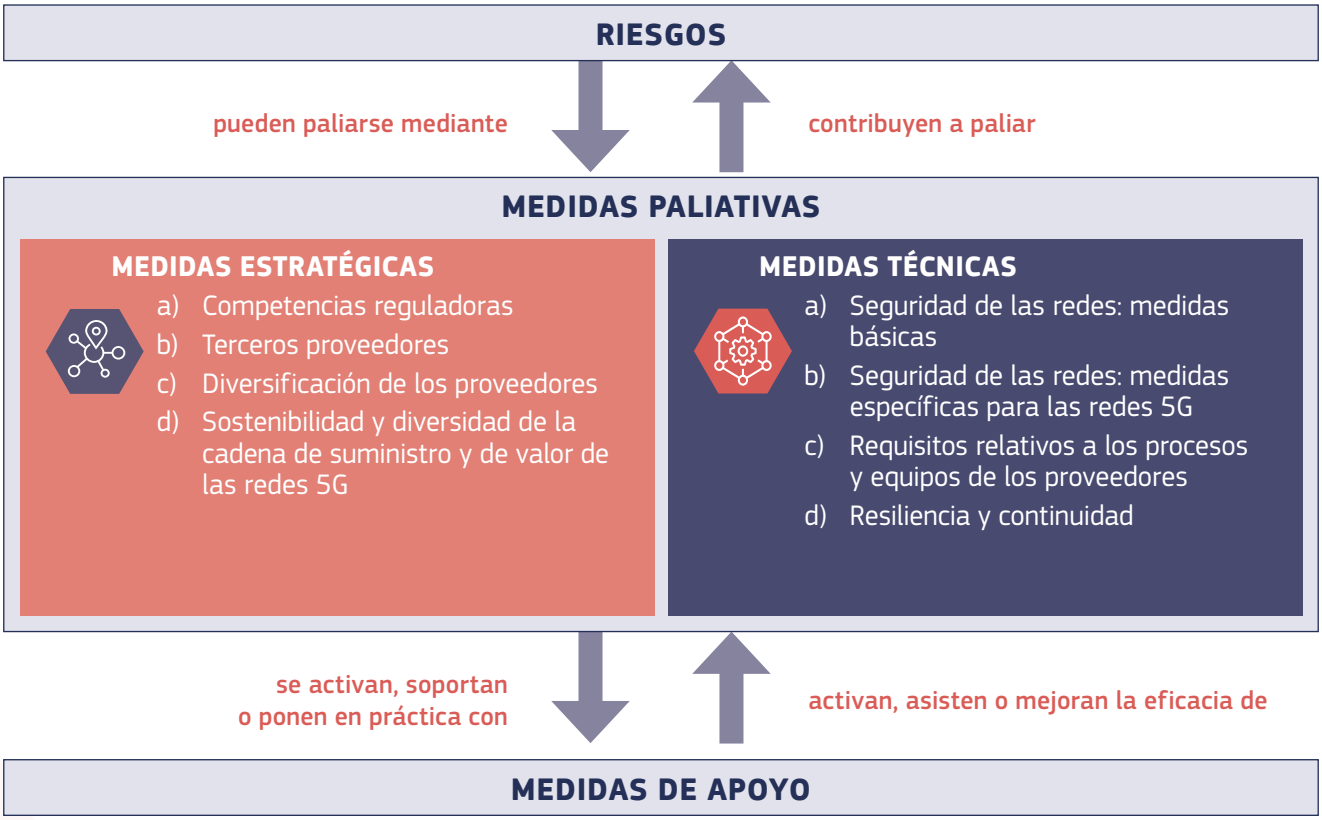
Evaluación de riesgos de la UE: escenarios de riesgo

La evaluación coordinada de riesgos de la Unión Europea (UE) para la seguridad de la red 5G en la Unión determina nueve grandes riesgos, agrupados en cinco escenarios.

I Escenarios de riesgo relacionados con medidas de seguridad insuficientes	R1: Fallos de configuración de las redes R2: Controles de acceso insuficientes
II Escenarios de riesgo relacionados con la cadena de suministro de la 5G	R3: Productos de baja calidad R4: Dependencia de un único proveedor en determinadas redes o falta de diversidad a nivel nacional
III Escenarios de riesgo relacionados con el *modus operandi* de los principales agentes de riesgo	R5: Intromisiones por parte de Estados a través de la cadena de suministro de la 5G R6: Aprovechamiento de las redes 5G por parte de grupos de delincuentes organizados para atacar a usuarios finales
IV Escenarios de riesgo relacionados con interdependencias entre las redes 5G y otros sistemas críticos	R7: Daños significativos a infraestructuras o servicios críticos R8: Caída general de las redes debido a la interrupción del suministro eléctrico u otros sistemas de soporte
V Escenarios de riesgo relacionados con dispositivos de los usuarios finales	R9: Utilización abusiva del internet de las cosas, microteléfonos o dispositivos inteligentes

Caja de herramientas de la UE para la seguridad de las redes 5G

Sobre la base de la evaluación coordinada de la UE de los riesgos de seguridad de las redes 5G, la caja de herramientas consta de una serie de medidas de seguridad para reducir el riesgo de manera eficaz y garantizar el despliegue de redes 5G seguras en toda Europa. También establece **planes de reducción del riesgo** detallados para cada uno de los riesgos detectados y recomienda una serie de **medidas estratégicas y técnicas clave** que deben adoptar todos los Estados miembros o la Comisión.



Conclusiones de la caja de herramientas de la UE: medidas clave

Los **Estados miembros** deben contar con medidas y competencias para reducir el riesgo. En concreto, deberán:

- reforzar los **requisitos de seguridad** aplicables a los **operadores de redes móviles**;
- evaluar el perfil de riesgo de los proveedores; aplicar las **restricciones pertinentes a los proveedores que se consideren de alto riesgo**, incluidas las exclusiones necesarias para activos clave;
- velar por que cada operador tenga una **estrategia adecuada en materia de proveedores múltiples** para **evitar** o **limitar** cualquier **dependencia importante** de un único proveedor y prevenir la dependencia de proveedores considerados de alto riesgo.

La **Comisión Europea**, junto con los Estados miembros, debe tomar medidas para:

- mantener una **cadena de suministro de redes 5G diversa y sostenible** a fin de evitar la dependencia a largo plazo, entre otras cosas:
  - aprovechar plenamente las herramientas e instrumentos de la UE existentes (control de las inversiones extranjeras directas, instrumentos de defensa comercial, competencia);
  - reforzar en mayor medida las capacidades de la UE en materia de tecnologías de las redes 5G y posteriores a estas mediante el recurso a los programas y la financiación de la UE pertinentes;
- facilitar la coordinación entre los Estados miembros en lo que respecta a la **normalización** para alcanzar objetivos de seguridad específicos y crear **regímenes de certificación** pertinentes a escala de la UE.

Además, la **línea de trabajo del Grupo de Cooperación sobre Redes y Sistemas de Información** deberá ampliarse al apoyo, control y evaluación de la aplicación de la caja de herramientas.

Planes de reducción del riesgo: ejemplos de medidas de la caja de herramientas

Para cada una de las nueve áreas de riesgo determinadas en el informe de la UE de evaluación coordinada de riesgos, la caja de herramientas define planes de reducción del riesgo, consistentes en una posible combinación de medidas según su eficacia.

La caja de herramientas ofrece orientaciones sobre criterios objetivos —incluidos factores de riesgo técnicos y no técnicos— para evaluar el perfil de riesgo de los proveedores, esto es, el riesgo de interferencia por parte de un país no miembro de la UE, capacidad de suministro y prácticas de ciberseguridad.

ME03	**Evaluar el perfil de riesgo de los proveedores y aplicar restricciones a los considerados de alto riesgo, incluidas las exclusiones necesarias para mitigar los riesgos de forma eficaz para los activos clave**	Establecer un marco con criterios claros, teniendo en cuenta los factores de riesgo identificados en el apartado 2.37 de la evaluación coordinada de riesgos en la UE y añadiendo información específica por país (por ejemplo, evaluación de las amenazas de los servicios nacionales de seguridad, etc.), para las autoridades nacionales competentes y los operadores de redes de comunicaciones móviles a fin de: — llevar a cabo evaluaciones del perfil de riesgo rigurosas de todos los proveedores pertinentes a nivel nacional o de la UE (por ejemplo, junto con otros Estados miembros u otros operadores de redes de comunicaciones móviles); — sobre la base de la evaluación del perfil de riesgo, aplicar restricciones, incluidas las exclusiones necesarias para mitigar eficazmente los riesgos, en el caso de los activos clave definidos como críticos o sensibles en el informe de evaluación coordinada de riesgos en la UE (por ejemplo, funciones de la red básica, funciones de gestión y organización de la red y funciones de acceso a la red); — tomar medidas para garantizar que los operadores de redes de comunicaciones móviles dispongan de controles y procesos adecuados para gestionar los posibles riesgos residuales, como realizar auditorías regulares de la cadena de suministro y evaluaciones de riesgos, una sólida gestión del riesgo, o requisitos específicos para los proveedores en función de su perfil de riesgo.

La caja de herramientas ofrece orientaciones sobre la sensibilidad de los elementos y funciones de red.

MT03	**Garantizar unos controles de acceso estrictos**	Garantizar que los operadores de redes de comunicaciones móviles apliquen medidas técnicas adecuadas, flexibles y verificables para garantizar que: — se aplican controles estrictos de acceso a la red; — se aplica el principio de mínimo privilegio, garantizando que se minimicen los distintos derechos en la red (por ejemplo, los derechos de acceso entre las funciones de la red, los derechos de los administradores de la red y la configuración de la virtualización); — se aplica el principio de separación de funciones; — se dispone de procedimientos para garantizar que estas normas están en vigor en todo momento y evolucionan con la red. Al establecer las políticas de control de acceso, debe prestarse especial atención a garantizar que el acceso a distancia por parte de terceros, especialmente los proveedores considerados de alto riesgo, se reduzca al mínimo o se evite siempre que sea posible. Cuando sea necesario acceder a distancia, por ejemplo para abordar las interrupciones de servicio, el operador de redes de comunicaciones móviles deberá aplicar la autenticación, la autorización, el registro y la auditoría adecuados para tener una visibilidad clara del acceso a los datos y los cambios de configuración o las alteraciones de la red.

Cronología de la política de la UE en materia de ciberseguridad de la 5G

22 de marzo de 2019
Conclusiones del Consejo Europeo.

26 de marzo de 2019
La **Comisión Europea** publicó una **Recomendación** para que los Estados miembros tomaran medidas concretas para evaluar los riesgos de ciberseguridad de las redes 5G y reforzaran las medidas de reducción del riesgo.

9 de octubre de 2019
Los Estados miembros finalizaron la **evaluación coordinada de la UE de los riesgos de seguridad** de las redes 5G.

21 de noviembre de 2019
La Agencia de la Unión Europea para la Ciberseguridad publicó un amplio **informe sobre las amenazas** relacionadas con las redes 5G.

29 de enero de 2020
Publicación de la **caja de herramientas en forma de medidas de reducción del riesgo** por parte de los Estados miembros. Comunicación de la Comisión sobre la aplicación de la caja de herramientas de la UE [COM (2020) 50 final, de 29 de enero de 2020].

Julio de 2020
Informe de situación sobre la aplicación de la caja de herramientas

Octubre de 2020
El **Consejo Europeo** pide a la UE y a los Estados miembros que «aprovechen al máximo el conjunto de instrumentos para la ciberseguridad de las redes 5G» y «apliquen las restricciones pertinentes a los proveedores que se consideren de alto riesgo para recursos clave».

Diciembre de 2020
Nueva estrategia de ciberseguridad de la UE e **informe** sobre las repercusiones de la Recomendación de la Comisión sobre ciberseguridad en la 5G.

A más tardar en junio de 2021
La Comisión insta a los Estados miembros a **completar la aplicación de las principales medidas de la caja de herramientas.**

Próximos pasos (en el marco de la estrategia de ciberseguridad de la UE para la década digital)

- Completar la aplicación de las principales medidas de la caja de herramientas a más tardar el segundo trimestre de 2021.
- Garantizar que los riesgos detectados se hayan paliado de forma adecuada y coordinada, en particular en lo que respecta al objetivo de minimizar la exposición a proveedores de alto riesgo y evitar la dependencia de estos proveedores a escala nacional y de la Unión Europea.
- Continuar e intensificar la coordinación en la Unión centrándose en los objetivos clave:

1. Garantizar la convergencia de los enfoques nacionales para una reducción eficaz de los riesgos en toda la UE

2. Apoyo al intercambio continuo de conocimientos y el desarrollo de capacidades

3. Fomentar la resiliencia de la cadena de suministro y otros objetivos estratégicos de seguridad de la UE

Luxemburgo: Oficina de Publicaciones de la Unión Europea, 2021

Oficina de Publicaciones de la Unión Europea

Print	ISBN 978-92-76-37738-2	doi:10.2759/558383	KK-02-21-626-ES-C
PDF	ISBN 978-92-76-37720-7	doi:10.2759/41176	KK-02-21-626-ES-N

2021-05-25