CN-pytec
centro criptológico nacional

CCN-TEC 011

Comunicaciones Móviles Seguras en 5G

CCN
centro criptológico nacional

Febrero 2023

Edita:

CCN-PYTEC

Fecha de Edición: enero de 2023

ÍNDICE

0. RESUMEN EJECUTIVO

El empleo de la **tecnología 5G para uso gubernamental** se está discutiendo ampliamente en diferentes foros y será un elemento clave en el desarrollo de nuevas aplicaciones. Una de las principales cuestiones que está siendo analizada es el proceso de certificación de estas soluciones para que puedan ser empleadas en la protección de información clasificada nacional (o, en general, de información sensible) y que además resulten resistentes a las distintas amenazas que puedan afectar a la seguridad de la información procesada o al propio sistema, como pueden ser los ataques de software espía (p.ej., como puede ser el caso de *Pegasus*).

El Centro Criptológico Nacional (CCN) considera que las **principales cuestiones a tener en cuenta para tratar de garantizar la seguridad en este tipo de redes móviles,** son las siguientes:

1) Con independencia de la tecnología móvil empleada (4G, 5G…), **la base de la seguridad de un sistema de comunicaciones móviles corporativo lo determina la arquitectura del sistema y el contar con terminales móviles verificados y aprobados**, tal como se recoge en la **CCN-STIC-496**. Un terminal aprobado (entre otras cosas) tendrá un sistema operativo distinto a los comerciales que limite sus interfaces de entrada y salida, implementará el "enforcement" de la VPN y forzará que todas las comunicaciones lleguen de forma tunelizada hasta la organización para acceder a los diferentes servicios, **impidiendo** de esta forma **cualquier acceso directo a internet desde el terminal, y viceversa**. Las conexiones a internet, en su caso, se harán a través de una zona de interconexión segura controlada por la organización, donde resulta mucho más sencillo monitorizar a través de una sonda la posible exfiltración de datos, la detección de patrones anómalos, etc.

2) **Las aplicaciones para comunicaciones móviles seguras** (para cifrado de la información en tránsito) sobre terminales no aprobados, **no proporcionan por sí mismas ninguna protección ante programas de software espía** puesto que la exfiltración directa de datos a internet desde el terminal sigue siendo posible. Además, este tipo de aplicación tampoco permite por si misma proteger al terminal frente a otro tipo de ataques, como podría ser la manipulación de los interfaces o la modificación maliciosa de otras aplicaciones que incluya el terminal.

3) Al margen de las cuestiones anteriores, que son agnósticas de la tecnología móvil empelada, **es cierto que las redes 5G ofrecen nuevas posibilidades para llegar a tener cierto nivel de control y de confianza** sobre las mismas. Por ejemplo, existe el mecanismo de "*Network Slicing*" para crear una red virtual dedicada sobre la red de un operador público; también es factible contar con un "*core*" de red propietario y hacer uso del acceso radio de un operador público, etc**. No obstante, la evaluación de seguridad y la correspondiente certificación de todos esos mecanismos es muy compleja** y depende de múltiples factores (p.ej. procedencia del equipamiento de red empleado). Por este motivo, **en el corto plazo, la base para contar con comunicaciones seguras sobre redes 5G sigue siendo la arquitectura del sistema** (alineada con la CCN-STIC-496) **y el empleo de terminales móviles aprobados**.

4) A medida que se vayan evaluando nacionalmente ciertos componentes de algunas soluciones de red 5G en el mercado, será posible **combinar las medidas clásicas** ya expuestas **con las nuevas posibilidades que ofrece el 5G para contar con una red "propia"** sobre los recursos de red y/o radio del operador. Con ello se espera que soluciones actualmente aprobadas para proteger información clasificada nacional de grado DIFUSIÓN LMITADA sobre redes 3G/4G, se puedan emplear para proteger información de mayor grado de clasificación sobre determinadas redes 5G (aquellas con componentes evaluados nacionalmente).

Este documento pretende plantear la visión del CCN en la protección de las comunicaciones en la nueva generación de redes 5G, especialmente a corto plazo con la convivencia de distintas generaciones, y tratar de contribuir a la mejora de la seguridad de la información en este tipo de redes móviles.

1. INTRODUCCIÓN

1. En la actualidad, las organizaciones entienden el valor que los dispositivos móviles pueden añadir a la productividad de sus empleados al proporcionar conectividad, en cualquier momento y desde cualquier lugar, a los recursos corporativos. Esta realidad, no solo ha cambiado la forma en que se llevan a cabo las tareas tradicionales en la oficina, sino que las organizaciones están ideando formas de trabajar completamente innovadoras. Sin embargo, un dispositivo móvil comprometido puede permitir el acceso a datos confidenciales de la organización o a cualquier otro dato que el usuario haya almacenado en dicho dispositivo.
2. Adicionalmente, las organizaciones se enfrentan al reto de llevar a cabo la transición de 4G a 5G, por lo que deben focalizarse en la necesidad de salvaguardar las tecnologías corporativas que utilicen 5G al mismo tiempo que evoluciona el desarrollo, despliegue y uso de esta nueva tecnología, con la dificultad añadida de que hay muchos aspectos sobre la protección de los componentes y el uso de 5G, que aún carecen de estándares.
3. Con esto en mente, **esta píldora CCN-TEC tiene como objetivo plantear las bases para tratar de garantizan a las organizaciones la seguridad en sus comunicaciones móviles 5G.**

2. EL RETO

4. A medida que los empleados usan dispositivos móviles para realizar tareas, las organizaciones se enfrentan el desafío de garantizar que estos dispositivos procesen, modifiquen y almacenen datos sensibles de forma segura.
5. Este reto es especialmente relevante a la hora de cubrir los casos de uso en el entorno de Seguridad y Defensa Nacionales y otros organismos que manejen información sensible: la solución debe ser capaz de proteger información clasificada nacional y debe ser resistente a las amenazas actuales a las que estos dispositivos están expuestos como, por ejemplo, los ataques de software espía, así como a las futuras o que están surgiendo en estos momentos, como es el caso de la amenaza de la computación cuántica a la criptología empleada actualmente.

3. PRINCIPALES AMENAZAS

6. Las amenazas a las comunicaciones móviles de una organización son extensas y muy variadas, y afectan a todos los elementos que componen dicho ecosistema, desde el propio usuario a los servicios de que hace uso, pasando por el terminal y por la red de acceso.

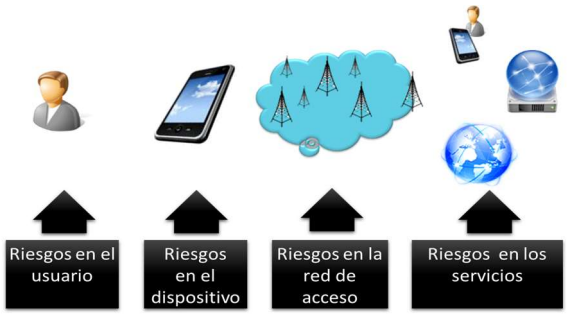

Ilustración 1. Amenazas a un sistema de comunicaciones móviles

7. A continuación, se recogen las amenazas más genéricas.

   a) Escuchas en la red (“*Network Eavesdropping*”). Un atacante se posiciona en el canal de comunicación inalámbrico, o en cualquier otro lugar de la infraestructura del sistema de comunicaciones móviles, pudiendo monitorizar y obtener acceso a los datos intercambiados entre el dispositivo móvil y el punto final.

   b) Ataque a la red (“*Network Attack*”). Un atacante se posiciona en el canal de comunicación inalámbrico o en cualquier otro lugar de la infraestructura del sistema de comunicaciones móviles, pudiendo iniciar comunicaciones con el dispositivo móvil o alterar las comunicaciones entre este y el punto final. Estos ataques incluyen la introducción de software malicioso (malware) en las actualizaciones de cualquier aplicación o del sistema operativo del dispositivo. También incluyen páginas web maliciosas o archivos adjuntos de correo electrónico, que generalmente se envían a los dispositivos a través de la red.

   c) Acceso Físico al dispositivo. Un atacante con acceso físico al dispositivo puede intentar acceder a los datos almacenados en él, incluidas las credenciales. Estas amenazas de acceso físico pueden implicar ataques que intentan acceder al dispositivo a través de puertos de hardware externos o hacerse pasar por el usuario frente a los mecanismos de autenticación.

   d) Aplicaciones maliciosas o defectuosas. Las aplicaciones cargadas en el dispositivo móvil pueden incluir código malicioso o explotable. Este código puede haber sido incluido de forma intencionada o no por el desarrollador, tal vez como parte de una biblioteca de software. Estas aplicaciones maliciosas pueden intentar exfiltrar los datos a los que tienen acceso, atacar el sistema operativo del dispositivo para obtener privilegios adicionales y la capacidad de realizar más actividades maliciosas o controlar los sensores del dispositivo (GPS, cámara, micrófono) para recopilar información sobre el entorno del usuario.

   e) Presencia persistente. La presencia persistente en un dispositivo móvil por parte de un atacante, implica que el dispositivo ha perdido su integridad y que no va a poder recuperarla de forma sencilla. Es probable que esto haya ocurrido debido a algún otro vector de ataque, pero está claro que el acceso continuo por parte de un atacante constituye una amenaza muy grave en sí misma.

4. LA SOLUCIÓN

8. La mitigación de las amenazas existentes en un sistema de comunicaciones móviles debe ser afrontada de manera global y se debe actuar sobre cada uno de los elementos que conforman este ecosistema para garantizar la seguridad de las comunicaciones en este complejo escenario.

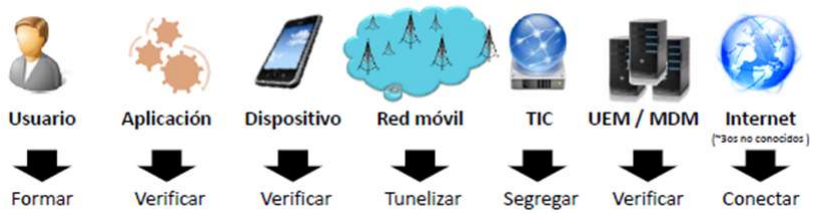

Ilustración 2. Mitigación amenazas en un sistema de comunicaciones móviles

9. Aunque todos los elementos que conforman el ecosistema móvil tienen su importancia, a día de hoy, y con independencia de la tecnología celular empleada (4G, 5G..), **las comunicaciones móviles seguras se sustentan fundamentalmente sobre la base de un dispositivo móvil seguro (confiable) y de una arquitectura segura del sistema de comunicaciones móviles, así como de su correcto uso**.

Ilustración 3. Puntos clave para garantizar la seguridad de las comunicaciones móviles

10. Hay que señalar que la evaluación y la certificación de los distintos elementos que componen el sistema de comunicaciones móviles son la única manera de poder garantizar su seguridad y poder tener confianza en la eficacia y correcta implementación de los distintos mecanismos de seguridad.

11. Como resultado de este proceso de evaluación y certificación, los productos que lo superan son cualificados o aprobados para su uso en la Administración y son incluidos en el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC).

4.1 EL DISPOSITIVO MÓVIL SEGURO: UN TERMINAL APROBADO

12. El dispositivo móvil es probablemente el componente más crítico al ser el más expuesto a las amenazas derivadas de, por un lado, la pérdida, sustracción o manipulación del dispositivo, y por otro lado a la exposición procedente de la conexión directa a redes inseguras (como puede ser en aeropuertos, cafeterías, hoteles, etc.).

13. Un dispositivo móvil seguro es aquel que implementa de forma fehaciente, los mecanismos adecuados para cubrir los siguientes objetivos mínimos y esenciales de seguridad, y que son los que harán frente a las amenazas anteriormente mencionadas.

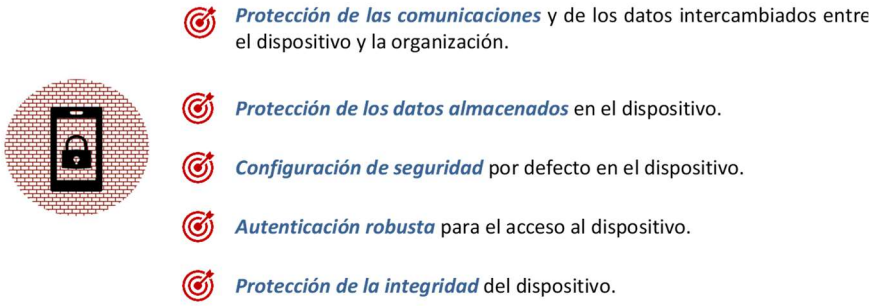

Ilustración 4. Mecanismos presentes en un dispositivo móvil seguro

14. Para tener garantía de que el dispositivo cumple estos objetivos de seguridad de forma fehaciente, éste debe haberse sometido a un proceso de evaluación y certificación del

dispositivo móvil. Los dispositivos móviles **Aprobados** serán los únicos que han superado de forma fehaciente, este proceso de evaluación y certificación.

15. Un dispositivo móvil Aprobado es un dispositivo incluido en el Catálogo CPSTIC (CCN-STIC-105), en la sección de productos "Aprobados", dentro de la familia de "Dispositivos Móviles".

16. El catálogo de Productos y Servicios STIC (CPSTIC) ofrece un listado de productos y servicios de Seguridad TIC que disponen de unas garantías de seguridad verificadas y contrastadas. El CPSTIC está destinado a organismos del Sector Público o entidades privadas que den servicio a éstos y que se encuentren bajo el alcance del Esquema Nacional de Seguridad (ENS), o que manejen Información Clasificada.

17. El catálogo CPSTIC dispone de una lista de productos Cualificados y una lista de productos Aprobados. Ambos tipos de productos han sido certificados, es decir, han superado con éxito un proceso de evaluación realizado por un laboratorio independiente y acreditado, y que ha sido auditado satisfactoriamente por el CCN, como Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de las Tecnologías de la Información (ENECSTI), quien habrá emitido la correspondiente certificación.

18. La siguiente figura ilustra qué son los productos: Certificados, Cualificados y Aprobados.

Ilustración 5. Productos certificados, cualificados y aprobados

19. Además de usar dispositivos móviles Aprobados, estos deben configurarse y utilizarse siguiendo las directrices especificadas en el correspondiente Procedimiento de Empleo Seguro que se indica en la ficha del producto dentro del catálogo CPSTIC.

4.2 EL SISTEMA DE COMUNICACIONES MÓVILES SEGURO: UNA ARQUITECTURA ACORDE CON LA CCN-STIC-496

20. **Una arquitectura segura en el sistema de comunicaciones móviles**, es el otro pilar básico de la seguridad de las comunicaciones móviles.

21. Para ello es indispensable seguir las instrucciones de la guía **CCN-STIC-496**, que especifica las características de una arquitectura segura e incorpora varios modelos de referencia. La siguiente figura muestra un ejemplo a alto nivel, de una arquitectura segura.

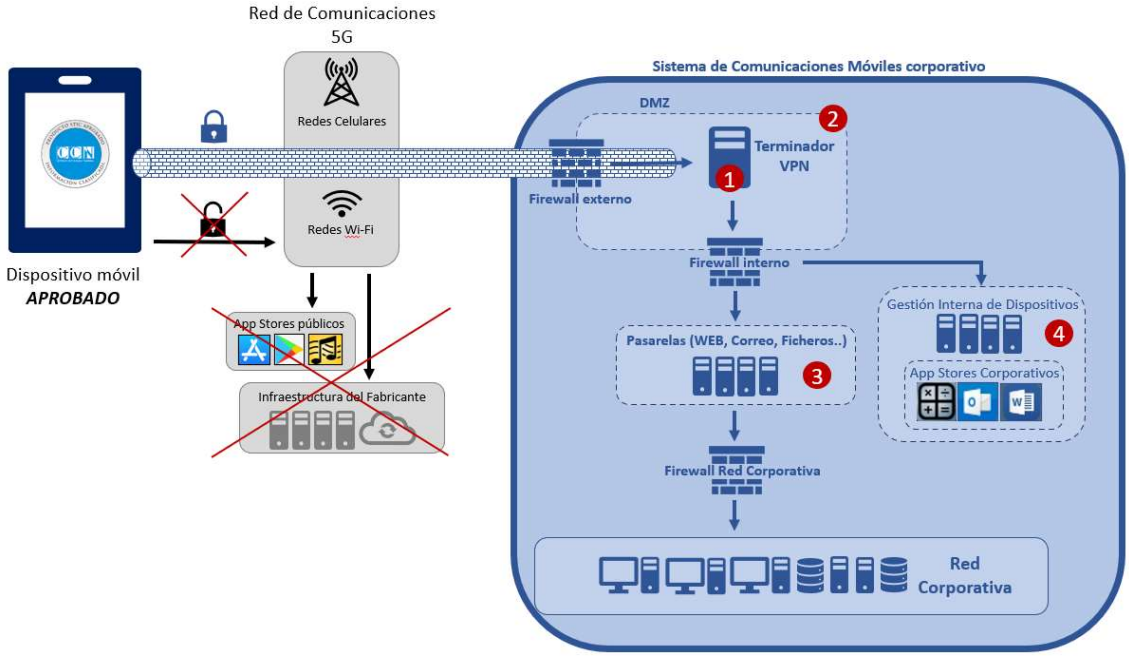

Ilustración 6. Arquitectura segura para un sistema de comunicaciones móviles

22. En la parte izquierda del diagrama está la red celular de acceso 5G, que será una red ajena no controlada por la organización más allá de aspectos de calidad del servicio (ancho de banda, cobertura, etc), y que debe ser considerada no confiable.

23. Generalmente los dispositivos móviles realizan conexiones a la infraestructura en la nube del fabricante para diversos temas: envío de actualizaciones del sistema operativo, notificaciones del fabricante, envío de datos de auditoría, etc. **Esta gestión externa no debe autorizarse**, ni tampoco la conexión para la descarga de aplicaciones de los App stores, por el elevado riesgo que ambas conexiones conllevan. El dispositivo debe ser gestionado por la organización.

24. En la parte derecha del diagrama está el sistema de comunicaciones móviles corporativo. Algunos de los componentes esenciales que este sistema debe incorporar como parte de una arquitectura segura acorde a la CCN-STIC-496, son los siguientes:

    a) **Gateway o Terminador VPN**. La única comunicación que el dispositivo móvil aprobado debe poder establecer, es una comunicación tunelizada con la red de la organización. Es decir, una comunicación cuyo extremo final sea el Gateway o Terminador VPN.

    b) **DMZ (“*Demilitarized Zone*”)**. Es necesario establecer una zona protegida para minimizar los riesgos derivados del hecho de que el Gateway o Terminador VPN es un componente con conexión a internet y que, por lo tanto, podría comprometer la seguridad de la organización. El Cortafuegos o Firewall externo de la DMZ, además, deberá configurarse para no dejar pasar ninguna comunicación móvil que no tenga como destino el Gateway o Terminador VPN.

    c) **Pasarelas de acceso a internet**. El terminal aprobado solo podrá contactarse a internet a través de la red de la organización y filtrado por la pasarela correspondiente (*Proxy*, *email*, etc.).

    d) **Zona de gestión interna de los dispositivos**. En esta zona es donde se despliegan todas las herramientas para la gestión de los dispositivos móviles: usuarios, parámetros del sistema operativo, actualizaciones y el almacén de aplicaciones móviles corporativas (apps), como el cliente VPN. Estas aplicaciones serán las únicas que los dispositivos

móviles podrán descargar y podrán ser aplicaciones desarrolladas de forma privada, o aplicaciones disponibles públicamente que han sido específicamente aprobadas para su uso en la organización.

25. Los componentes del sistema de comunicaciones móviles que forman parte de su arquitectura de seguridad (Firewalls, VPN, pasarelas, etc.) deben ser igualmente productos Aprobados del catálogo CPSTIC, y deben configurarse y utilizarse según las directrices especificadas en los correspondientes Procedimientos de Empleo Seguro que se indican en la ficha del producto dentro del catálogo CPSTIC.

5. CONCLUSIONES

26. Con independencia de la tecnología móvil empleada (4G, 5G…), la base de la seguridad de un sistema de comunicaciones móviles seguras lo determina contar con dispositivos móviles Aprobados y correctamente configurados, junto con una arquitectura del sistema segura tal como se recoge en la CCN-STIC-496.

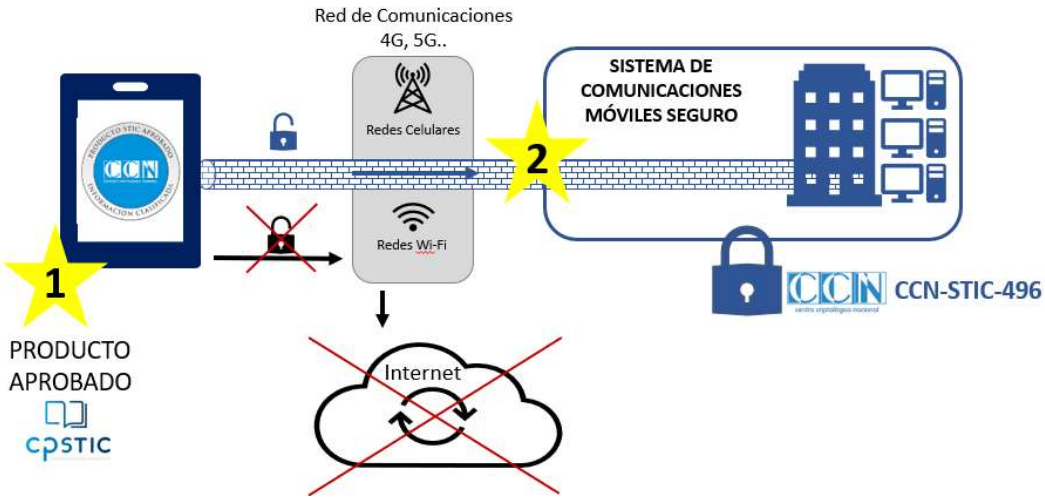

Ilustración 7. Base para la seguridad en sistemas de comunicaciones móviles

27. Un dispositivo móvil Aprobado será aquel que se encuentre en el catálogo CPSTIC y cuyas funciones de seguridad habrán sido evaluadas y certificadas de forma fehaciente y veraz. Una vez que el dispositivo se configure y se use tal y como indica su Procedimiento de Empleo Seguro, será un dispositivo móvil seguro con características de seguridad esenciales, tales como interfaces de entrada y salida limitadas y un "*enforcement*" de la VPN, es decir, sus comunicaciones estarán restringidas y solo serán posibles aquéllas que tengan por destino el Terminador VPN, forzando a que todas las comunicaciones lleguen de forma tunelizada hasta la organización, e impidiendo de esta forma cualquier acceso directo a internet desde el dispositivo. Las conexiones a internet, en su caso, se harán a través de un "firewall" de la organización.

28. Una arquitectura segura en un sistema de comunicaciones móviles, es una arquitectura que cumpla con las especificaciones de la CCN-STIC-496, y cuyos componentes STIC sean productos Aprobados, y se configuren y usen según sus correspondientes Procedimientos de Empleo Seguro. Una arquitectura segura permitirá que los recursos internos de la organización estén protegidos, siendo menos susceptibles a ciberataques y brindando una mejor visibilidad, detección y control de los ataques, lo que reducirá el riesgo.

29. **La tecnología 5G ofrece nuevas posibilidades en lo que respecta a la seguridad y protección de las comunicaciones**. No obstante, la **evaluación de seguridad y la**

certificación de estos mecanismos de seguridad, es **muy compleja**, no está madura y no se espera que lo esté a corto plazo.

30. En un futuro, a medida que se consigan avances en la certificación de seguridad de la tecnología 5G, sí que es esperable que soluciones actualmente aprobadas para proteger información clasificada nacional de grado DIFUSIÓN LMITADA sobre redes 3G/4G, se puedan emplear para proteger información de mayor grado de clasificación sobre determinadas redes 5G.

31. Sin embargo, aunque en un futuro podrán aprovecharse estos nuevos mecanismos de seguridad para combinarlos con las medidas clásicas que se han expuesto en este documento, no es previsible ni a corto ni a medio plazo contar con pleno control sobre las redes 5G de operadores públicos, por lo que **son las medidas expuestas en este documento y sólo estas, las únicas que garantizan la seguridad de un sistema de comunicaciones móviles y no se puede prescindir de ellas pese a la llegada de 5G**.

6. FAQ – PREGUNTAS FRECUENTES

32. ¿No es suficiente con emplear una aplicación que cifre las comunicaciones de mi dispositivo? El uso de aplicaciones para comunicaciones móviles seguras, que generalmente llevan a cabo el cifrado de la información en tránsito, sobre dispositivos no aprobados no proporciona por sí mismo ninguna protección ante las amenazas, puesto que la exfiltración directa de datos a internet desde el dispositivo es posible. Una arquitectura del sistema adecuada y el empleo de dispositivos móviles aprobados, son los dos únicos mecanismos que realmente pueden hacer un sistema de comunicaciones móviles resistente al software espía.

33. ¿Y las nuevas funciones de seguridad de 5G? Es cierto que las redes 5G ofrecen nuevas posibilidades para llegar a tener cierto nivel de control y de confianza sobre la red celular. Por ejemplo, existe el mecanismo de "*Network Slicing*" para crear una red virtual dedicada sobre la red de un operador público. No obstante, la evaluación de seguridad y la correspondiente certificación de todos esos mecanismos es muy compleja y depende de múltiples factores. Por este motivo, la base para contar con comunicaciones seguras sobre redes 5G sigue siendo la arquitectura del sistema (alineada con la CCN-STIC-496) y el empleo de dispositivos móviles aprobados.

34. ¿Puedo usar el dispositivo móvil corporativo para cuestiones personales? Eso dependerá del modelo de propiedad de los dispositivos, que establezca la organización. Existen principalmente 3 modelos: BYOD, COPE y COBO.

    a) En el modelo BYOD ("*Bring Your Own Device*") el dispositivo es adquirido y es propiedad del usuario final, que lo pone a disposición de la organización con fines profesionales. La organización puede gestionar parte del dispositivo, pero no existe trazabilidad ni cadena de custodia del dispositivo.

    b) En el modelo COPE ("*Corporate Owned, Personally Enabled*") el dispositivo es propiedad de la organización. Es puesto a disposición del usuario para el desempeño de sus funciones profesionales, habilitándose desde la organización un espacio separado para albergar y manejar datos de carácter personal del usuario final. La organización gestiona parte o la totalidad del dispositivo.

    c) En el modelo COBO ("*Corporate Owned, Business Only*") el dispositivo es propiedad de la organización y es puesto a disposición del usuario, únicamente para el desempeño de sus funciones profesionales. La organización gestiona la totalidad del dispositivo.

35. El modelo de despliegue recomendado en líneas generales en la guía CCN-STIC-496 es el modelo COBO, en el que todo el dispositivo es gestionado por la organización y está orientado en exclusiva a la realización de tareas profesionales. Por lo tanto, la respuesta a la pregunta planteada es NO, se recomienda que la organización use el modelo de propiedad COBO con lo que el usuario no podrá usar el dispositivo móvil corporativo para fines personales, y únicamente deberá usarse para fines profesionales.

36. ¿Puedo conectarme a través de Wi-fi en zonas sin cobertura de red celular, con el dispositivo móvil Aprobado? Sí, es posible. No obstante, no se recomienda el empleo de redes Wi-Fi públicas o abiertas y sí la utilización de redes de confianza en las que se hayan seguido las recomendaciones del CCN en su implementación.

CCN-PYTEC
centro criptológico nacional

*El Departamento de Productos y Tecnologías de Seguridad TIC del Centro Criptológico Nacional (CCN-PyTec) promueve el desarrollo, la evaluación, la certificación y el uso de productos **verificados** y **confiables**, garantizar la seguridad de los sistemas de tecnologías de la información y la comunicación y, de esta manera, **contribuir a la defensa del ciberespacio.***

CPSTIC
CATÁLOGO DE PRODUCTOS Y SERVICIOS STIC

CATÁLOGO DE PRODUCTOS Y SERVICIOS DE SEGURIDAD TIC

PDF

ONLINE

ccn-pytec@cni.es

@CCNPYTEC

CCN-PYTEC

www.ccn.cni.es **https://oc.ccn.cni.es** **www.ccn-cert.cni.es**