centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 496

Sistemas de Comunicaciones Móviles Seguras

Abril 2021

MINISTERIO DE DEFENSA

Edita:

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.04.28 18:15:20 +02'00'

NIPO: 785-18-036-1

Fecha de Edición: Abril de 2021.

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Abril de 2021

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

ANEXOS

1. INTRODUCCIÓN

1. La incorporación masiva de dispositivos móviles (smartphones, tablets, phablets, etc.) a todos los ámbitos profesionales, unida a las circunstancias derivadas de la emergencia sanitaria global desencadenada por el SARS-CoV-2 han impulsado a todas las entidades, con independencia de su naturaleza y tamaño, a enfrentar como prioridad insoslayable la gestión y plena implementeción del trabajo remoto, a distancia o distribuido, para garantizar la consecución de sus objetivos y su pervivencia..

2. Existen varios documentos pertenecientes a las serie CCN-STIC que tratan diferentes aspectos relacionados con la implantación de dispositivos móviles en la organización y, en general, en este trabajo se tendrán en cuenta dichas directrices, mereciendo especial atención los documentos CCN-STIC-002, CCN-STIC-101, CCN-STIC-302, CCN-STIC-404, CCN-STIC-407, CCN-STIC 45X, CCN-STIC 811 y CCN-STIC-827. Dichos documentos tienen diferentes ámbitos de aplicación, y cada responsable de sistemas deberá atender a unos u otros en función de la categorización de su sistema TIC y de la clasificación o no de la información que maneja. Igualmente, y de manera progresiva, el lector podrá encontrar un mayor número de Procedimientos de Empleo Seguro (Serie 1000 de CCN-STIC), donde se da un mayor detalle sobre las configuraciones, arquitecturas de despliegue y seguridad ofrecida por diferentes productos que cuenta con diferentes grados de aval por parte del Centro Criptológico Nacional (CCN).

3. Gracias a los sistemas operativos móviles y la accesibilidad de la banda ancha móvil, las organizaciones tienen a su disposición multitud de posibilidades, como la creación de documentos de manera colaborativa, la consulta de mapas en tiempo real, la realización de reuniones virtuales, todo ello a través de un solo dispositivo. Sin embargo, las capacidades de estos dispositivos son directamente proporcionales a los potenciales riesgos de seguridad a los que se enfrentará cualquier organización en su utilización.

4. Es pertinente en este punto incluir un fragmento del documento CCN-STIC-002:

> *6. Para la protección de la información nacional clasificada se deberán emplear equipos de cifra con certificación criptológica nacional. En el caso de que no existiera un equipo con certificación criptológica nacional con las características necesarias, se contactará de forma oficial con el CCN para explicarle la situación, proponer el equipo que desean emplear, adjuntar toda la información disponible (fabricante, teléfono de contacto, algoritmos utilizados, medidas de seguridad, esquemas de fabricación, código fuente, etc.) y solicitar autorización al ACC para el empleo del equipo propuesto.*
>
> *7. La utilización de productos con certificación criptológica nacional no autoriza a un Sistema a manejar información nacional clasificada, aunque sí*

podrá ser un elemento indispensable para obtener la correspondiente autorización. […]

14. Los Sistemas de la Administración que requieran manejar información nacional clasificada DIFUSIÓN LIMITADA o superior deberán protegerla empleando productos de cifra con certificación criptológica nacional de acuerdo al grado de clasificación de la información a proteger.

15. Si un sistema maneja información nacional no clasificada, pero la pérdida de integridad o de disponibilidad de esta información, o de los Sistemas que la manejan, cause un perjuicio equivalente al de la pérdida de confidencialidad de un determinado grado de clasificación de la información, se utilizarán equipos criptográficos nacionales con certificación criptológica del grado adecuado.

5. En aquellas organizaciones en las que la acreditación del sistema TIC para manejar información clasificada no es requisito obligatorio, dicha acreditación puede ser considerada como un objetivo a largo plazo, que sirva de meta para aumentar progresivamente la seguridad del sistema.
6. Para las organizaciones para cuyos sistemas y servicios sea de aplicación lo prescrito en el Esquema Nacional de Seguridad, el Centro Criptológico Nacional articula y actualiza periódicamente el Catálogo de Productos y Servicios STIC, donde se incluyen Productos y Servicios que han sido verificados en diferentes niveles por parte del CCN y que contaran con el correspondiente Procedimientos de Empleo Seguro (Serie 1000 de CCN-STIC).
7. En cualquier caso, los criterios aquí contemplados persiguen aumentar la seguridad de los dispositivos móviles y del sistema de comunicaciones al que dan acceso. Esta tarea de segurización puede afrontarse de manera progresiva, y será necesariamente una tarea continua, de forma similar a como lo es en el entorno TIC "tradicional" o en el entorno de la seguridad física.

2. OBJETO

8. El presente documento tiene como objetivo establecer un conjunto de directrices para el diseño de Sistemas de Comunicaciones Móviles Corporativos, así como para la revisión y adaptación de despliegues ya existentes. El objetivo en ambos casos es dotar a dichos sistemas de mayor seguridad, tanto para las comunicaciones establecidas con los dispositivos como para la información almacenada en los mismos.
9. Dichas directrices deben ser consideradas en conjunto con el resto de documentos de las series CCN-STIC, dado que el sistema de comunicaciones móviles será, con toda probabilidad, parte de una infraestructura TIC de la organización.
10. Más adelante, dichas directrices deberán traducirse en medidas concretas, sin olvidar que la carencia (temporal) de capacidades o la incesante aparición en el mercado de nuevos dispositivos no debe modificar "per se" los criterios de seguridad de la organización.
11. El sistema de comunicaciones móviles aquí planteado utilizará como base modelos de dispositivos móviles y redes de acceso de telefonía móvil fácilmente disponibles en el mercado, en cuyo diseño y fabricación no se ha intervenido, o al menos no en gran medida. Esta hipótesis de diseño impone ciertas limitaciones, y requiere realizar esfuerzos en el modelado de la solución, pero aporta enormes ventajas, sobre todo en lo relativo a usabilidad de los interfaces, coste del despliegue y tiempo necesario hasta la puesta en marcha del sistema.

3. COMUNICACIONES MÓVILES CORPORATIVAS

12. Como paso previo a la "movilización" de los recursos corporativos, cada organización debe establecer una política de sistemas de información en movilidad.
13. La elaboración y aprobación de esta política, y su equiparación con la normativa interna preexistente, ayudará a objetivar las decisiones durante la adopción de dichas tecnologías y capacidades. La organización, a través de los responsables designados al efecto, debe fijar unos objetivos claros para el despliegue de esta nueva tecnología, que justifique la introducción de nuevos sistemas y subsistemas de comunicaciones y que ayude a racionalizar el necesario Análisis de Riesgos que la organización realizará antes y durante la puesta en marcha/reestructuración del Sistema de Comunicaciones Móviles Corporativo. Esta reflexión debe ser propia de cada organización y contar con la aprobación y el respaldo de la alta dirección.

14. Se fijara igualmente una Política de Seguridad de la información para las Comunicaciones Móviles Corporativas, que debe estar alineada y subordinada a la Política de Seguridad de la Información Corporativa preexistente.
15. En el caso más habitual, la organización ya habrá "movilizado" de una u otra manera sus recursos y estará manejando información corporativa desde dispositivos móviles y/o portátiles. En este caso, el presente documento puede ser tomado como una referencia para la reestructuración ordenada de dichos sistemas TIC hacia una mayor seguridad.

3.1 PROCEDIMIENTO DE USO Y NORMATIVA INTERNA

16. Como elemento tangible de la Política de Seguridad de la Información, la organización debe elaborar y facilitar al usuario final unas directrices claras de uso o un Procedimiento de Uso, en función del nivel de seguridad que se quiera alcanzar.
17. Dicho marco de actuación debe fijarse en una Normativa y un Acuerdo de Aceptación de Términos de Usuario Final en los que queden claros los roles y responsabilidades de cada una de las partes, y que sea aceptada de forma explícita por el usuario final del dispositivo.
18. En los Anexos de este documento se pueden encontrar diferentes modelos que cada organización puede tomar como referencia para elaborar dicha Normativa.

4. ARQUITECTURA DE REFERENCIA PARA SISTEMAS DE COMUNICACIONES MÓVILES CORPORATIVOS

19. El sistema móvil considerado utilizará redes de acceso comerciales y dispositivos de propósito generalista. En el caso de la red de acceso, teniendo en cuenta que es propiedad de un tercero y que se tendrá un control limitado, únicamente se considera la posibilidad de influir en determinados parámetros de la calidad de servicio a través de la negociación comercial o del cumplimiento de la normativa vigente relativa a la cadena de suministro.
20. Teniendo en cuenta estas restricciones, el diseñador del sistema dispondrá de los siguientes puntos de actuación:

    a) En el dispositivo: modificando solo las capas superiores de su estructura lógica, sin plantear modificaciones en el hardware ni el hardware/software propio del interfaz de radio frecuencia (banda base). Como parte de la segurización del dispositivo, se incluye la seguridad de los datos que se almacenan en el mismo (información corporativa, datos personales del usuario, claves de entrada a otros sistemas, etc.). En caso de manejar información clasificada, deberá estar certificado en función de la dicha clasificación. Se prestará especial atención en la configuración de estos dispositivos a la habilitación y configuración de los interfaces de entrada/salida del dispositivo (wifi, red móvil, bluetooth, USB, etc.) y al módelo de propiedad del dispositivo y sus implicaciones en la gestión de los datos almacenados (datos personales vs datos de la organización).

    b) En la infraestructura corporativa: donde se ubicaran las herramientas de gestión de los dispositivos móviles y la infraestructura de servicios adicional que de servicio al Sistema de Comunicaciones Móviles. Teniendo en cuenta el dinamismo del sector de la ciberseguridad y de la tecnología móvil, los bloques funcionales que realizan esta función pueden ir cambiando de denominación (MDM, MAM, EMM, UEM, MTD, …). Se prestará especial atención a la seguridad del punto de interconexión entre el dispositivo móvil y el resto de redes, actuando como un puerto seguro para la comunicación entre los equipos finales de los usuarios y las redes o sistemas de terceros. Teniendo en cuenta la alta exposición de los equipos periféricos del sistema de comunicaciones (móviles), dicho punto de interconexión necesita reservar recursos para dar soporte a los dispositivos periféricos en los aspectos de seguridad.

21. Uno de los principios generales del diseño será la creación de un perímetro lógico que incluya a los dispositivos móviles en una nueva subred que se pueda interconectar (si se considera necesario) a la infraestructura TIC corporativa. A

continuación se presenta el esquema genérico para la conexión entre dicha subred móvil y la red corporativa "tradicional".

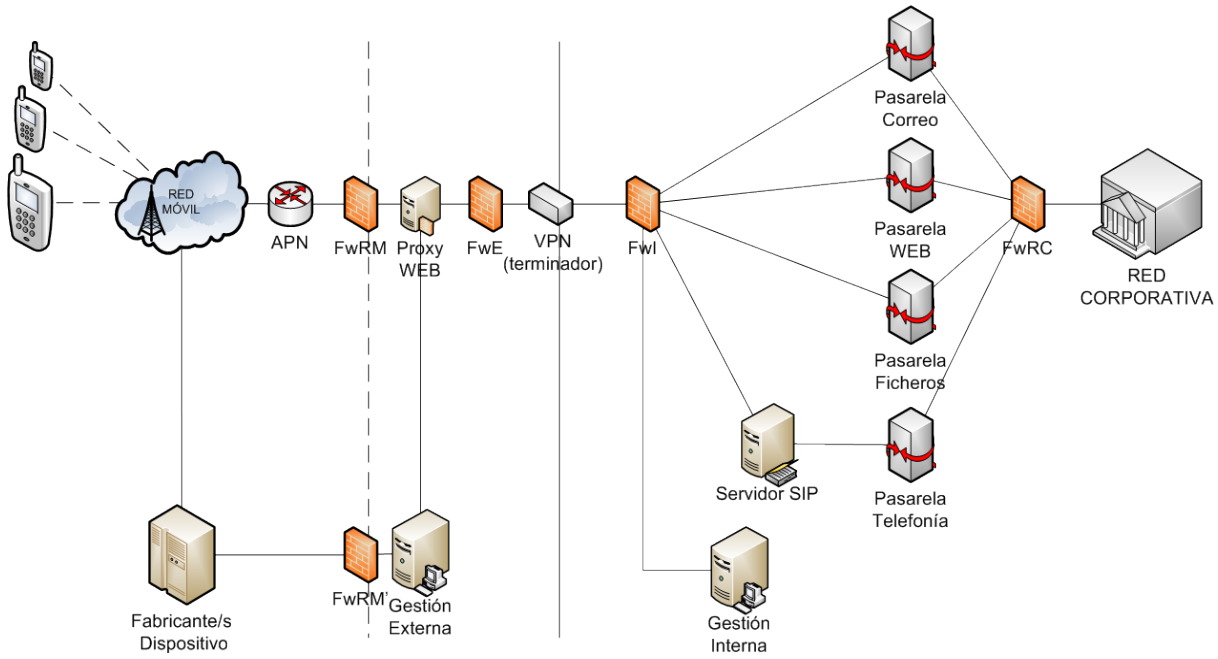

Figura 1. Sistema de comunicaciones móviles corporativas: modelo de referencia.

22. Este diseño (Figura 1) es genérico y puede ajustarse en función de la infraestructura de servicios o interconexión con la que cuente la organización previamente.

23. En caso de que la infraestructura de interconexión de la organización soporte una configuración suficiente para ofrecer acceso a los dispositivos móviles incorporados, la arquitectura móvil podría quedar como se ilustra en la siguiente figura (Figura 2):

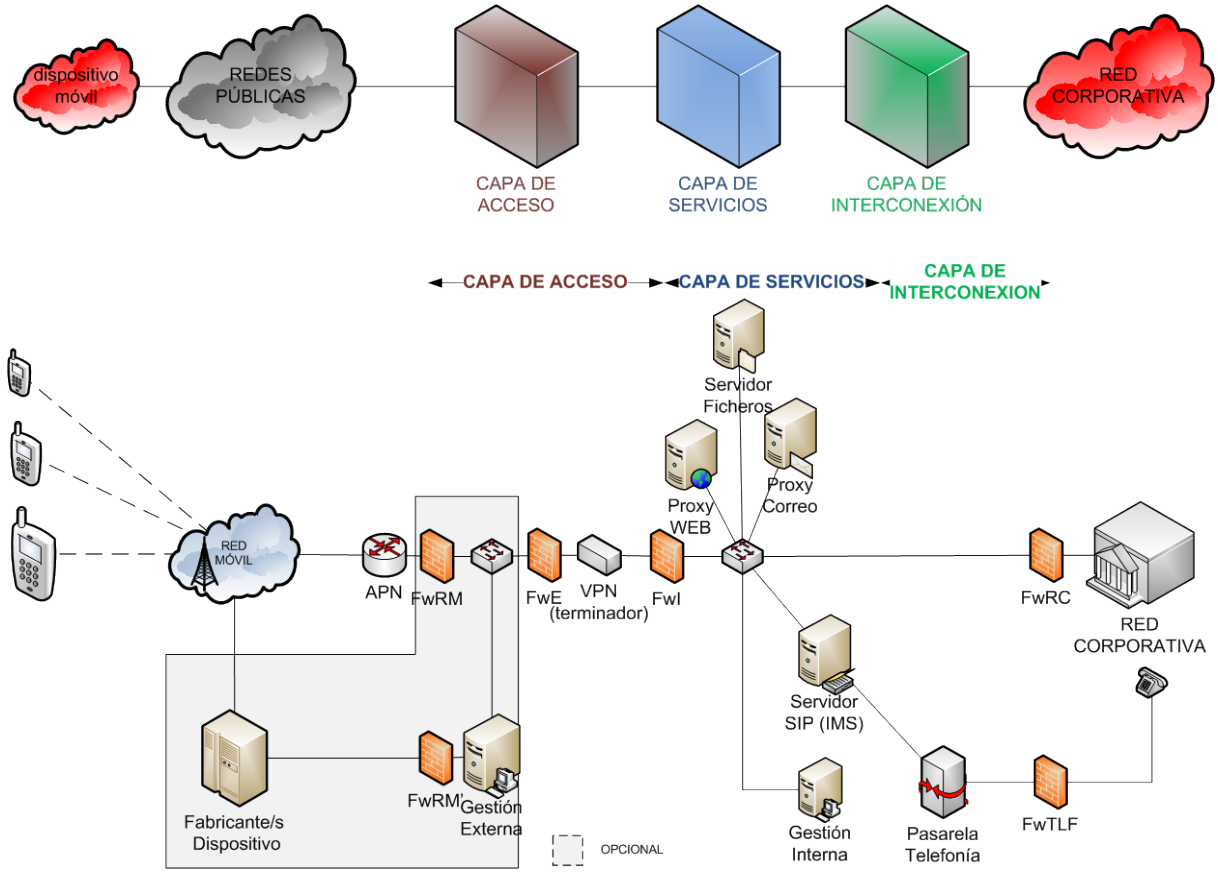

Figura 2. Sistema de comunicaciones móviles corporativas (existen servicios de interconexión).

24. En el caso en que no se disponga ya de pasarelas con capacidades de presentación para los dispositivos móviles, será necesario introducir mayores capacidades en la capa de interconexión, reduciendo al mínimo la capa de servicios de la arquitectura de interconexión con la red móvil.

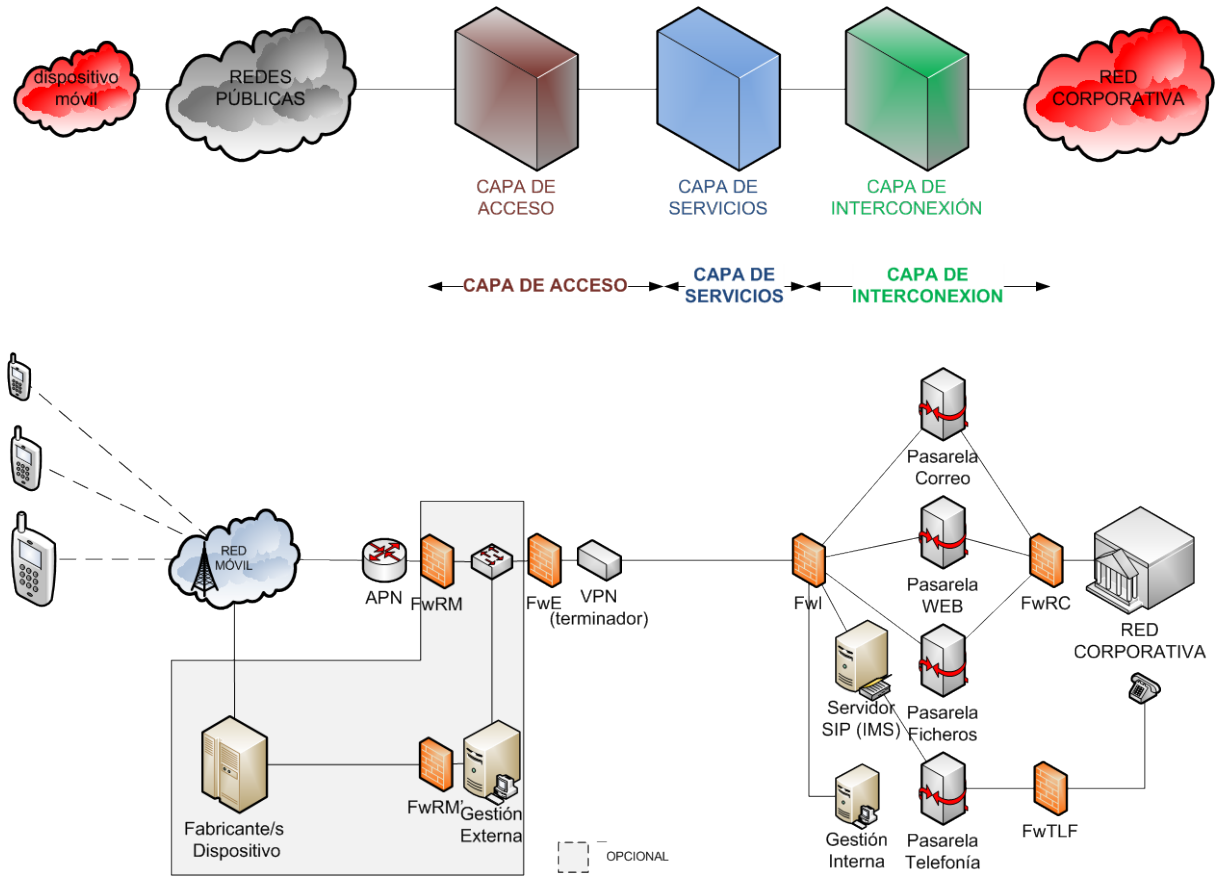

Figura 3. Sistema de comunicaciones móviles corporativas (no existen servicios de interconexión).

25. Esta última configuración (Figura 3) es la recomendada, ya que permite una mayor adaptación a los requisitos de la subred móvil (y a la presentación de servicios TIC), de manera que los cambios o configuraciones propios del despliegue móvil tengan el menor impacto en el resto de la infraestructura TIC corporativa.

4.1 BLOQUES FUNCIONALES Y COMPONENTES DE LA ARQUITECTURA DE REFERENCIA

26. A continuación se revisaran los parámetros a tener en cuenta en cada uno de los bloques funcionales del sistema.

4.1.1. DISPOSITIVO

27. El dispositivo representa el punto más crítico para la seguridad de la red de comunicaciones, debido en gran parte al bajo nivel de protección física que se deriva de los casos de uso más habituales (utilización en domicilios particulares, aeropuertos, periodos con falta de custodia del dispositivo en hoteles o salas de

reunión, etc.), que lo hacen muy vulnerable a perdidas, sustracciones o manipulaciones por parte de potenciales atacantes. Otra gran fuente de riesgo de los dispositivos es la conexión "directa" con servicios y redes de terceros, sin elementos de seguridad intermedios que actúen de cortafuegos (independientes del dispositivo y del usuario final).

28. Se considera el dispositivo dividido en "capas", sobre las que existe una diferente capacidad de influencia en la fase de diseño, fabricación y utilización.

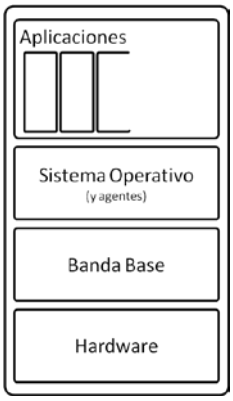

Figura 4. Estructura de capas "lógicas" propia de un dispositivo móvil.

29. En el caso del hardware y la banda base, lo más habitual es que sean de propósito general (y sean adquiridos entre los disponibles comercialmente en cada ocasión).
30. Las capas superiores (sistema operativo y aplicaciones), en cambio, si será posible seleccionarlas teniendo en cuenta la posibilidad de verificación, modificación o configuración por parte de la organización propietaria del sistema.
31. Para conseguir la mayor seguridad en cuanto a la autenticidad del dispositivo (en su conjunto) se pueden considerar varias alternativas:

    a) Disponer de una base hardware de confianza, e incluir desde la organización las herramientas para crear un vínculo lógico con el software de las capas superiores. En este caso, solo una autoridad declarada como "confiable" podría actualizar el sistema operativo o el software del dispositivo.

    b) Habilitar un mecanismo de autenticación fuerte entre el dispositivo (al menos desde sus capas superiores) y la infraestructura corporativa central, e incluir elementos de monitorización específicos dedicados a una monitorización continua de dicho vínculo.

32. La selección de un sistema operativo "comercial"[1] puede hacer necesaria la introducción en la infraestructura corporativa de una zona destinada a las herramientas de gestión de dispositivos, y que dicha zona de gestión requiera para su funcionamiento de una conexión lógica con el fabricante o distribuidor del dispositivo. La introducción de un sistema operativo de estas características y su correspondiente herramienta de gestión es tratada más adelante.
33. En el caso de organizaciones que requieran un nivel de seguridad igual o equivalente al exigido para el manejo de información clasificada, la dependencia de herramientas de gestión externa debe minimizarse para cumplir con las exigencias de la Autoridad de Certificación Criptológica, siendo una mejor opción contar con herramientas de gestión autónomas.
34. Las capacidades a gestionar por ambos tipos de herramientas de gestión serán similares (control de los interfaces de captura de datos del dispositivo, habilitación de sensores/actuadores del dispositivo, gestión de cuentas habilitadas, gestión de software habilitado, etc.)
35. En el caso de organizaciones que manejen información clasificada a través de dispositivos móviles, es necesario acudir siempre a la utilización de plataformas[2] aprobadas por la Autoridad de Certificación Criptológica.

4.1.1.1. MODELOS DE PROPIEDAD DE LOS DISPOSITIVOS

36. En el diseño o revisión del Sistema de Comunicaciones Móviles de una organización, una de las primeras decisiones que debe tomar la organización es el modelo de propiedad de los dispositivos utilizados para acceder a, o manejar datos de la organización.
37. Estos modelos suelen dividirse en cuatro grupos con diferentes posibilidades e implicaciones. Lo más común es denominarlos por sus siglas en inglés[3]):

- 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. Entre otras, este modelo destaca por estas características:
  - La organización puede gestionar parte del dispositivo.
  - No existe trazabilidad ni cadena de custodia del dispositivo[4] por lo que el punto inicial de seguridad se obtiene mediante diagnosis.

[1] Los sistemas operativos más utilizados en los dispositivos comerciales en el momento de redactar el documento (Android, iOS) requieren de dicha infraestructura de gestión externa.
[2] El listado de plataformas (sistema operativo y dispositivo asociado) aprobadas puede consultarse con el Centro Criptológico Nacional a través de su página web o de su dirección de correo (movilsec.ccn@cni.es)
[3] Al igual que en otros ámbitos, el dinamismo de las compañías desarrolladoras suele ir modificando estos nombres (COBO-COSU-WP, etc), por lo que es importante entenderlos para poder interpretar y adaptar dichos conceptos al contexto técnico y marco legislativo que aplique a la organización.

- CYOD (*Choose your own device*): Es una solución intermedia entre los modelos COPE y COBO. Permite a los trabajadores la elección del modelo de dispositivo entre varios de una lista elaborada previamente por la organización que a su vez conserva el control total del dipositivo y establece las condiciones de seguridad y uso, pudiendo permitir o denegar su utilización para fines personales.
- 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.
- 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.

38. El modelo de despliegue recomendado en líneas generales por el Centro Criptológico Nacional 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. Las razones para la recomendación de este modelo de propiedad/despliegue son de carácter técnico, legal y organizativo.

39. Desde el punto de vista técnico, el nivel de riesgo introducido por una zona "personal" en un dispositivo corporativo, así como la no trazabilidad e imposibilidad de gestionar las cuentas personales del usuario, recomienda el modelo COBO. Desde el punto de vista legal, las implicaciones de habilitar una zona para uso personal por parte del usuario final en un dispositivo que es propiedad de un organismo incluido en el ámbito subjetivo del artículo 2 Ley 39/2015 de 1 de octubre quedan supeditadas al interés general y a la prestación del servicio público correspondiente, por cuanto la información gestionada mediante dicho dispositivo obedece a ese fin primordial, haciendo que el control de las medidas de seguridad a implementar en el mismo se torne necesario, y dejando –también desde este punto de vista– el modelo COBO[5] como la opción recomendada.

[4] Cuando una organización ya tiene los dispositivos distribuidos entre sus usuarios finales y después procede a su configuración (enrolado) en el MDM, suele decirse que el despliegue es tipo BYOD. Esta situación no es la ideal, pero puede representar el punto de partida en un plan de segurización.

[5] Solo se considera admisible en algún caso un modelo COPE en sistemas ENS-Cat. Básica, teniendo la organización que analizar y articular internamente la normativa que permita la puesta a disposición de un bien de la organización a un usuario final para su uso privado.

4.1.1.2. APLICACIONES /SOFTWARE AUXILIAR[6]

40. Las plataformas móviles actuales permiten aumentar la funcionalidad y ajustarla a las necesidades de las organizaciones, gracias a la posibilidad de incorporar aplicaciones a los dispositivos con posterioridad. Dichas aplicaciones (y sus infraestructuras de servicio) pueden alcanzar un alto grado de complejidad, siendo necesario tenerlas en cuenta en la definición del sistema.

41. Las aplicaciones, una vez instaladas, pueden requerir de interconexión con infraestructura controlada por terceros, o disponer de acceso a diferentes zonas de memoria del dispositivo, de manera exclusiva o compartida por varias aplicaciones[7]. Esta complejidad aumenta la importancia de que la organización tenga un control proactivo de las aplicaciones utilizadas en los dispositivos desde los que se acceda a sus recursos.

42. La descarga, instalación y ejecución de dichas aplicaciones debe llevarse a cabo solamente a través de listas blancas gestionadas por los responsables TIC de la organización. Este control puede materializarse de diferentes formas, bien a través de la apertura de un repositorio de aplicaciones corporativas controlado por la organización o permitiendo la instalación de estas únicamente por parte del grupo de administración TIC.

43. El responsable TIC de la organización debe articular un procedimiento de incorporación de aplicaciones, así como de las actualizaciones de las mismas[8]. Dado que las necesidades de las diferentes organizaciones son en su mayor parte coincidentes, lo más habitual es que diferentes organizaciones acudan a un sistema de validación de aplicaciones común, y externo a dichas organizaciones.

44. El procedimiento será análogo al necesario en el caso de las actualizaciones propias del sistema operativo.

45. A continuación se expone un esquema genérico de dicho procedimiento[9], en el cual será necesario validar tanto la aplicación como la infraestructura de servicio utilizada o las comunicaciones que realice:

[6] Es frecuente la utilización de la denominación Apps en lugar de Aplicaciones.
[7] Diferentes aplicaciones pueden requerir acceder al mismo calendario o a un directorio de contactos almacenado, permanente o temporalmente, en el dispositivo, como puede ser el listado de teléfonos.
[8] Cada una de las actualizaciones puede introducir vulnerabilidades en el sistema.
[9] Este procedimiento es ilustrativo y puede ser modificado por cada organización, pudiendo utilizarse el documento NIST SP 800-163 como referencia.

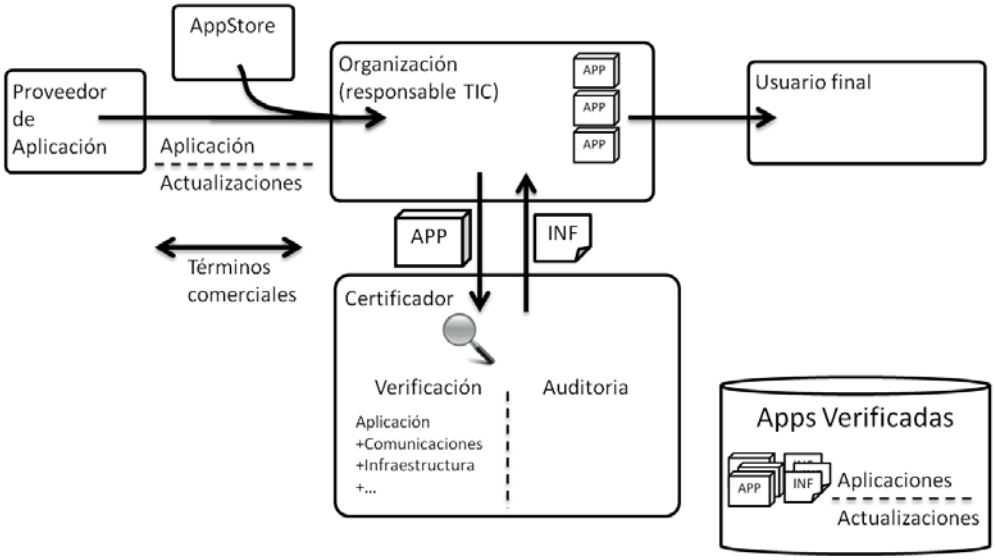

Figura 5. Mecanismos de verificación de aplicaciones.

4.1.2. RED MÓVIL

46. En la mayor parte de los casos, las modificaciones que se pueden imponer a la red móvil se limitaran a la Calidad de Servicio (Ancho de banda mínimo disponible, Cobertura geográfica, Tiempo máximo de no disponibilidad, etc.), y siempre se debe tener en cuenta que se trata de una red ajena y sobre la cual la organización no tendrá un control real.
47. La organización debe ser consciente de la diferencia entre el material propiedad de, y controlado enteramente por, la organización y aquel que es propiedad, o es gestionado por, el proveedor de servicios.
48. La organización debe, al menos, tener la posibilidad de vetar o imponer la utilización de determinados productos en la infraestructura que le da servicio. Esta práctica, común en otros sectores industriales, permite aumentar la seguridad extremo a extremo.
49. El criterio general en cuanto a la red de acceso será considerarla potencialmente comprometida o no confiable, y ser conscientes de los riesgos que implica su utilización:
    a) Dificultad para conseguir Protección por Anonimato.
    b) Fragilidad del medio en cuanto a Disponibilidad (Denegación de servicio).
    c) Posible falta de transparencia del proveedor de servicios en cuanto a sus infraestructuras (subcontratación).
    d) Riesgo de acceso a la información que se transmite a través de esta red por parte de terceros (desconocidos).

4.1.2.1. APN

50. El APN (Access Point Name) es el punto, perteneciente a la red del proveedor de red móvil, donde se conectan los dispositivos móviles cuando acceden a determinados servicios ofrecidos por el operador (MMS, internet, banda ancha móvil,…). Su función es ejercer de pasarela entre la red móvil del operador y otras redes de datos (ISDN, WWW, …)

51. La nomenclatura de un APN sigue la estructura:

    organizacioncliente.mncXXX.mccYYY.gprs

    donde mncXXX (mobile network code) identifica la red del operador y mccYYY (mobile country code) identifica el país donde se ubica el APN. Esta nomenclatura permite que la red de cualquier operador en cualquier país pueda redirigir el tráfico al punto de la red móvil del operador en el país origen del dispositivo.

52. La mayor parte de proveedores de comunicaciones ofrece la posibilidad de contratar un APN Privado para la organización, pudiendo fijar su tipología y configuración.

53. En el caso de comunicaciones corporativas se debe definir un punto de acceso privado (APN privado), al que solamente se puedan conectar los MSISDN[10] definidos por la organización. Esto permitirá establecer una primera capa de protección para la subred móvil de la organización (delegada en el proveedor de comunicaciones).

54. El proveedor de comunicaciones entregará (y recogerá) todo el tráfico de datos generado por (y destinado a) los dispositivos de la organización en este punto, por lo que puede ser considerado la frontera exterior de la infraestructura corporativa dedicada a movilidad.

4.1.3. FIREWALL RED MÓVIL

55. El firewall entre la red del operador móvil y la organización es la primera barrera real de protección bajo control de la organización, lo cual debe ser tenido en cuenta para su dimensionamiento.

56. Debe permitir igualmente el tráfico con origen/ destino el terminador de VPNs presente en la zona más interna de la red, y las conexiones entre dicha zona de gestión externa y hacia los sistemas del fabricante de los dispositivos.

[10] MSISDN: Mobile Station Integrated Service Digital Network, identificador de red del dispositivo móvil

4.1.4. ROUTER

57. Su objetivo es únicamente separar el tráfico de gestión de dispositivos del tráfico con destino la red corporativa. En caso de considerarlo necesario, este será el punto para la inserción de un IPS.

4.1.5. ZONA DE GESTIÓN EXTERNA

58. La zona de gestión externa solo existirá en caso de necesidad justificada, siendo preferible, siempre que sea posible, la gestión privada o autónoma. La gestión externa puede venir impuesta por la selección de dispositivos (sistemas operativos) realizada por la organización, de ahí la importancia de esta selección. . Lo más adecuado es seleccionar ambos componentes (dispositivos y herramientas de gestión) de manera coordinada o condicionada, teniendo en cuenta igualmente el conjunto de políticas de seguridad que se vaya a aplicar (definido de manera agnóstica al dispositivo en primer lugar).
59. Esta zona de gestión externa se focaliza en la gestión del dispositivo desde el punto de vista del hardware y del sistema operativo o algunas aplicaciones especialmente integradas en el sistema. La conexión con el fabricante del dispositivo o con el proveedor del mismo se utilizará para un tráfico de gestión, señalización y auditoria (en general, tráfico de media-baja prioridad y con no muy alto volumen de datos por dispositivo), como puede ser:
    a) Recibir actualizaciones del sistema operativo desde el fabricante/vendedor del dispositivo y de las aplicaciones que estén instaladas en los dispositivos.
    b) Enviar información del dispositivo al fabricante del mismo.
    c) Enviar/recibir notificaciones a/de las herramientas de notificaciones en la nube del fabricante/vendedor del dispositivo.
    d) Enviar/recibir notificaciones a/de las herramientas de gestión de dispositivos.
    e) Enviar/recibir notificaciones a/de las herramientas de gestión del proveedor de comunicaciones.
    f) Enviar/recibir datos destinados a la auditoria de seguridad de los dispositivos, aplicaciones o servicios.
60. El principal bloque funcional de esta zona de gestión externa se puede materializar a través de una herramienta MDM (Mobile Device Management) de propósito general, que normalmente requerirá de la utilización de identificadores de usuario/dispositivo. Los identificadores de usuario/dispositivo en este punto deben ser neutros y no revelar información no necesaria, pues se compartirán tanto con el fabricante del dispositivo como con socios comerciales de este o desarrolladores de aplicaciones que se instalen en los dispositivos.

61. Habitualmente, el MDM se comercializa por separado respecto a los dispositivos, pero la selección de ambos necesita ser coherente. Las medidas de seguridad deben concretarse en función de la familia de dispositivos seleccionados y del perfil de seguridad de la organización. Las políticas de seguridad a aplicar en los dispositivos son un recurso valioso de la organización, por lo que a pesar de necesitar cierta conectividad con el exterior, deben estar convenientemente protegidas para garantizar su integridad.

62. En este documento, por coherencia con los diferentes documentos elaborados por el CCN y con las diferentes referencias internacionales utilizadas se utiliza la denominación MDM (Mobile Device Management). Debido al dinamismo propio del sector de la ciberseguridad y en especial de la tecnología móvil, el lector podrá encontrar diferentes denominaciones para este "bloque funcional, dependiendo de la perspectiva del fabricante. Entre estas denominaciones se puede encontrar MAM (M Application M), MTD (Mobile Threat Defense), EMM (Enterprise Mobility Management), UEM (Unified EndPoint Management), etc.. La función común a estas denominaciones será la gestión y monitorización de los dispositivos finales y de la información manejada a través de los mismos, siendo el bloque responsable de "traducir" la Política de Seguridad TIC Corporativa en configuraciones concretas que se accionen en los dispositivos.

4.1.5.1. POLÍTICAS/CONFIGURACIÓN DE SEGURIDAD

63. A continuación, se incluye un conjunto de políticas de seguridad generales. Se han definido teniendo en cuenta las capacidades habitualmente disponibles en los dispositivos de gama media-alta en el momento de redactar el documento. Por esta razón, deben ser periódicamente revisadas, y concretadas por cada organización en función de los dispositivos seleccionados, siempre de manera razonada[11]:

Aspecto \ Nivel	ENS C. BÁSICA	ENS C. MEDIA	ENS C. ALTA	Información Clasificada
Monitorización del software presente en el dispositivo	Obligatoria	Obligatoria	Obligatoria	Obligatoria
Disponibilidad de vinculo hardware para comprobaciones	Obligatorio	Obligatorio	Obligatorio	Obligatorio
Auto bloqueo del dispositivo tras cierto tiempo de inactividad	No necesario	Recomendable	Si	Si

[11] En caso de duda o necesidad de aclaraciones, puede ponerse en contacto con el Centro Criptológico Nacional.

Aspecto \ Nivel	ENS C. BÁSICA	ENS C. MEDIA	ENS C. ALTA	Información Clasificada
Auto borrado del dispositivo (puesta a fábrica) en caso de intentos fallidos sucesivos de autenticación del usuario	No necesario	No necesario	Si (orientación, 5 intentos)	Si (orientación, 5 intentos)
Longitud mínima de PIN/contraseña de acceso a dispositivo[12]	Si (orient., 6 caracteres)	Si (orient., 6 caracteres)	Si (orient. , 8 caracteres)	Si (orient., 8 caracteres)
Utilización de contraseña para acceder a los recursos corporativos	Si	Si	Si	Si
Autenticación extremo a extremo con certificados digitales	Recomendable	Recomendable	Si	Si
Autenticación del usuario basada en elementos externos[13]	Recomendable	Recomendable	Recomendable	Muy recomendable
Cifrado de la memoria del dispositivo	Si	Si	Si	Si
Borrado remoto (puesta a fábrica) del dispositivo en caso de pérdida, compromiso, etc.	Si	Si	Si	Si
Instalación de actualizaciones del Sistema Operativo[14]	Controlado por la organización	Controlado por la organización	Controlado por la organización	Solo desde la infraestructura de gestión
Instalación de aplicaciones	Utilización de listas blancas/negras controladas por la organización[15]	Únicamente desde repositorio corporativo	Únicamente desde repositorio corporativo	Únicamente desde repositorio corporativo

[12] La utilización de caracteres alfanuméricos puede ser sustituida por la utilización de dígitos numéricos acompañadas de restricciones que dificulten la utilización de combinaciones inseguras por parte del usuario.
[13] Un segundo factor de autenticación solo puede ser considerado externo si utiliza identificadores primarios y canales de comunicación diferentes a los utilizados en el subsistema móvil.
[14] La organización debe tener la posibilidad de bloquear/imponer/arrancar en remoto la actualización del sistema operativo del dispositivo del usuario final
[15] Las organizaciones usuarias de tecnologías de comunicaciones móviles deben articular un proceso internos de auditoria y verificación de aplicaciones, con el objetivo a corto plazo de que en los dispositivos corporativos solamente se instale software explícitamente autorizado por la organización.

Aspecto \ Nivel	ENS C. BÁSICA	ENS C. MEDIA	ENS C. ALTA	Información Clasificada
Instalación de certificados desde la organización	Permitido	Permitido	Permitido	Permitido
Uso de los servicios de comunicación propios del operador (llamadas de voz, sms, mms, wap push, …)	Permitido	Permitido	Permitido	No recomendable
Configuración remota de los parámetros de conectividad (APN, volumen de datos, …)	Si	Controlado por la organización	Controlado por la organización	Controlado por la organización
Uso de interfaces inalámbricos de corto alcance (wifi, bt, nfc, …) fuera de las instalaciones controladas por la organización[16]	Permitido	Permitido	No recomendable	No permitido
Uso del interfaz USB del dispositivo como dispositivo de almacenamiento[17]	No recomendable	No recomendable	Autorización explícita del administrador del sistema	Autorización explícita del administrador del sistema
Uso de soportes de memoria extraíble del dispositivo	Permitido (cifrado)	Cifrado	Cifrado	Cifrado (no recomendable)
Uso de las cámaras del dispositivo	Si	Si	Decidido por la organización	Controlado por la organización
Uso de los servicios de localización	Permitido	Permitido	Decidido por la organización	Controlado por la organización
Uso de navegador web (seleccionado por la organización)	Permitido	Permitido[18]	Permitido[19]	Permitido
Uso de VPN para la información de la organización[20]	Recomendable	Obligatorio	Obligatorio	Obligatorio

[16] La organización debe decidir explícitamente sobre el uso de estos interfaces, para lo cual puede tener en cuenta los diferentes perfiles de usuario final presente en la organización (trabajo de campo, entorno de oficina, nivel de exposición, …)
[17] En los casos en los que no se considera recomendable, la organización puede decidir autorizarlos en base al riesgo/beneficio que presenten los diferentes perfiles de usuario final presente en la organización (trabajo de campo, entorno de oficina, nivel de conocimientos,…)
[18] La conexión con sistemas de terceros (internet) se realizará siempre que sea posible a través de la infraestructura de la organización y siguiendo la normativa de interconexión.
[19] La conexión con sistemas de terceros (internet) se realizará siempre a través de la infraestructura de la organización y siguiendo la normativa de interconexión.

Aspecto \ Nivel	ENS C. BÁSICA	ENS C. MEDIA	ENS C. ALTA	Información Clasificada
Uso de VPN para la comunicación	Recomendable	Muy recomendable	Obligatorio	Obligatorio
Configuración de cuentas personales (correo, mensajería instantánea, almacenamiento externo)	Temporal[21]	Autorización explícita del administrador del sistema	No permitido	No permitido
Habilitación de zona específica para información personal	No recomendable	No permitido	No permitido	No permitido
Mecanismos de borrado en caso de reutilización del dispositivo por otro usuario	Obligatorio	Obligatorio	Obligatorio	Obligatorio
Formación y compromiso explícito de los usuarios con la política de seguridad organizativa	Si	Si	Si	Si

64. A partir de este conjunto de políticas se puede derivar unas configuraciones concretas validas que en el caso de contar con una herramienta de gestión interna (autónoma) actúe directamente sobre los dispositivos desplegados.

4.1.6. FIREWALL EXTERNO DMZ

65. En caso de no existir zona de gestión externa, este equipo será la primera barrera bajo control de la organización, lo cual debe ser tenido en cuenta para su dimensionamiento.

66. Hasta este punto, la red móvil corporativa se considera no segura, lo cual debe ser tenido en cuenta a la hora de fijar criterios de interconexión, tal y como queda reflejado en los documentos CCN-STIC-302 o CCN-STIC-811.

[20] Se considera información de la organización toda aquella relacionada con los objetivos, misión y desempeño laboral del usuario final, tales como acceso a unidades de red, intranet, aplicaciones corporativas, correo electrónico corporativo, mensajería corporativa, …

[21] La configuración de cuentas personales en dispositivos pertenecientes a un despliegue corporativo tiene implicaciones tanto desde el punto de vista de seguridad como legal, por lo que se desaconseja fuertemente su habilitación. La organización puede autorizarlas temporalmente en base a un progresivo aumento de la seguridad.

67. Únicamente permitirá el tráfico con origen o destino (salida o entrada) en el terminador de VPN y con los protocolos utilizados por este, denegándose el acceso al resto del tráfico.

68. Se realizará un seguimiento del servicio basado en las herramientas de mejora de la interconexión, con el objetivo de mantener actualizadas las posibles reglas de filtrado de tráfico.

4.1.7. VPN (TERMINADOR)

69. Este dispositivo actúa como extremo de la VPN[22] en la sede de la organización. A partir de este punto, el tráfico de datos de cada dispositivo cuenta con una única capa de protección criptográfica (en caso de existir), lo cual debe ser tenido en cuenta a la hora de monitorizar el tráfico de la red interna.

70. La necesidad de ser compatible con la implementación presente en los dispositivos móviles puede imponer restricciones en la selección del proveedor de VPN. En cualquier caso, debe contar con el aval de la autoridad competente en materia de cifra.

4.1.8. FIREWALL INTERNO DMZ

71. Este dispositivo representa el final de la DMZ externa, su objetivo es proteger al terminador de VPN de posibles envíos no legítimos desde la red corporativa y a la vez, encaminar el tráfico hacia cada uno de los servicios corporativos.

72. Es importante que se conozca el tipo de tráfico que recibirá/ enviará cada servicio, de manera que se respeten las diferentes características del mismo, permitiendo alcanzar un compromiso entre Calidad de Servicio y Coste. A continuación se incluye una tabla ilustrativa con las principales características de algunos tipos de tráfico, pudiendo variar en función de la casuística de cada organización.

Servicio	Tolerancia a la latencia	Ancho de banda necesario
Voz	Baja	Medio-Bajo
Videoconferencia	Baja	Alto
Correo electrónico	Alta	Alto

[22] En este documento se considera la opción de utilizar una VPN como único medio de transporte de datos entre el dispositivo móvil y la infraestructura corporativa, sin analizar las diferentes opciones existentes para la implementación de una red privada.

Servicio	Tolerancia a la latencia	Ancho de banda necesario
Intercambio de ficheros	Alta	Alto
Gestión de dispositivos	Alta	Bajo (si aplica)

4.1.9. PROXY/ PASARELAS DE SERVICIOS CORPORATIVOS

73. En función de la capacidad instalada en materia de interconexión, será necesaria la introducción de pasarelas específicas orientadas a movilidad, o bien se podrán configurar los proxy y pasarelas ya existentes.

74. En este documento se ha considerado que la red corporativa ofrece como servicios hacia el exterior la funcionalidad de correo electrónico, el intercambio de ficheros y la más generalista capacidad de navegación web (sobre la que podrían implementarse otros servicios). Para cada una de las diferentes pasarelas habrá que tener en cuenta:

    a) **Pasarela de correo**: dada la presencia de diferentes sistemas operativos, es necesario tener un especial cuidado en cuanto a la infección de correos por virus u otro tipo de software malicioso, para lo cual se deberán definir políticas de seguridad relativas a la descarga de adjuntos, tamaño máximo de los mismos, extensión, etc. La casuística relativa al spam también será concreta, sobre todo si las políticas de la compañía permiten la utilización de cuentas de correo personales en los dispositivos de la organización (pese a que la recomendación en este sentido es que no se permita el uso de cuentas de correo personales en dispositivos corporativos).

    b) **Pasarela de acceso a ficheros**: al igual que en la pasarela de correo, será necesario prestar especial atención al software malicioso. Se recomienda la implementación de políticas adicionales de control, como puede ser la creación de unidades (sandbox) especialmente dedicadas al intercambio de información con los dispositivos móviles, en las que se puedan aplicar periodos de "cuarentena" y procesos de revisión específicos.

    c) **Pasarela WEB**: el acceso a la web desde dispositivos móviles debe ser siempre realizado en base a listas blancas de dominios, tanto para http como para https. Para permitir otro tipo de tráfico, debe someterse al criterio de los administradores TIC de la red corporativa. El seguimiento estadístico (agregado) del tráfico generado será especialmente útil para detectar posibles fuentes de infección o filtrado de información. Tal y como se recomienda en otros documentos relativos a seguridad de sistemas IT, se prestará especial atención a las conexiones periódicas o repetitivas por parte de un dispositivo o a las conexiones hacia redes

externas que envíen una cantidad significativa de información (atípicas en navegación web). Igualmente, y dada la natural asociación entre usuario y dispositivo, se podrá tener en cuenta para esta monitorización los patrones de uso esperables por cada perfil de usuarios. Para ello se recomienda el empleo de herramientas de seguridad adicionales, cuyas referencias pueden encontrarse en las series de documentos CCN-STIC, en especial en CCN STIC 430.

75. Asimismo, en el sistema se considera la existencia de una Pasarela de Telefonía, especialmente si se utiliza alguna aplicación basada en sistemas de Voz sobre IP (VoIP).

4.1.10. SERVIDOR SIP

76. Para la comunicación entre los dispositivos de la organización se recomienda la utilización de un sistema de comunicaciones basado en VoIP en el caso de las llamadas y de sistemas de mensajería basados en datos IP. Estos servicios harán necesaria la introducción de un servidor SIP (IMS) que realice la gestión de identidades y de permisos para las comunicaciones punto a punto dentro de la red móvil de la organización.

4.1.11. PASARELA DE TELEFONÍA

77. Este equipo servirá de punto de conexión con la red de telefonía corporativa, realizando una conversión de protocolos y conexión de redes de comunicaciones (VoIP-Telefonía).

78. A partir de la red de telefonía corporativa, el usuario de un dispositivo móvil podría obtener conectividad con cualquier teléfono de las redes de telefonía pública (PSTN/ GSM/ LTE/…), siempre que la organización lo apruebe por política. En función de la infraestructura de la organización, podrá habilitarse un Firewall Telefónico antes de su conexión a la red telefónica corporativa.

4.1.12. ZONA DE GESTIÓN INTERNA

79. La zona de gestión interna se orienta a la gestión de los usuarios desde el punto de vista de la organización, siendo responsable de todos los parámetros de la zona segura del dispositivo (sistema operativo/ contenedor/ aplicaciones seguras), así como de la VPN que conecta dicha zona segura con la organización.

4.1.13. FIREWALL RED CORPORATIVA

80. Este equipo representa el inicio de la red corporativa, por lo tanto, puede estar condicionado por los criterios ya fijados en el resto de la organización para la interconexión con redes externas.

4.1.14. RED CORPORATIVA

81. En la situación más habitual, la red corporativa ya estará desplegada, y será necesario modificar las reglas de interconexión y probablemente adaptar parte de su funcionamiento a la nueva red móvil.

5. OTRAS CONSIDERACIONES

5.1 COMUNICACIONES MÓVILES E INFORMACIÓN SENSIBLE/CLASIFICADA.

82. Aquellas organizaciones que, debido a su naturaleza prevean la necesidad de manejar información clasificada, sensible o de importancia equivalente[23], deben tener en cuenta consideraciones adicionales en el diseño o adaptación de un subsistema móvil corporativo.

83. En estos casos, será de utilidad acudir a los documentos:

    a) CCN-STIC-101, Acreditación de sistemas de las TIC que manejan información nacional clasificada en la administración, para conocer los criterios generales y los procedimientos de Acreditación de Sistemas, y

    b) CCN-STIC 302 Interconexión de Sistemas, para la interconexión con otros sistemas, especialmente sistemas responsabilidad de terceros (internet)

    c) NS/03, Seguridad Física, para la consideración de medidas de seguridad física y condiciones de utilización[24].

84. Tanto en estos documentos como en los documentos propios del Esquema Nacional de Seguridad se indica la importancia de acudir a sistemas, productos o equipos cuyas funcionalidades de seguridad y nivel hayan sido evaluados conforme a normas europeas o internacionales y cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información. En este sentido, tendrán la consideración de normas europeas o internacionales, ISO/IEC 15408 u otras de naturaleza y calidad análogas.

85. Cualquier organismo que este en proceso de diseño o adaptación de un subsistema de comunicaciones móviles puede acudir al Centro Criptológico Nacional en busca de información sobre los sistemas, productos o equipos que dispongan de dichos certificados, así como de las Instrucciones Técnicas pertinentes.

[23] En general, todos aquellos sistemas considerados en el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, publicado en el Real Decreto 3/2010, de 8 de enero y posteriormente modificado en el Real Decreto 951/2015, de 23 de octubre.

[24] Si bien estos documentos solo son de obligado cumplimiento en el caso de información clasificada, su lectura y análisis se recomienda igualmente en el caso de sistemas con información considerada sensible por sus responsables.

5.2 GESTIÓN DE PROVEEDORES Y CADENA DE SUMINISTRO

86. Una organización puede no tener capacidad de negociación sobre sus proveedores como para obligarles a implementar una normativa estricta en materia de seguridad de la cadena de suministro, o no querer hacerlo por cualquier razón.

87. Incorporar en la negociación algunos criterios equivalentes a los que se incluyen en las normas ISO 28000 permite incrementar la seguridad sobre los componentes y equipamientos que utiliza.

6. REFERENCIAS

[Ref.- 1] NS-03, Seguridad Física

[Ref.- 2] NS-05, Seguridad en los Sistemas de Información y Comunicaciones

[Ref.- 3] CCN-STIC-002, Coordinación Criptológica en la administración

[Ref.- 4] CCN-STIC-302, Interconexión de sistemas de las tecnologías de la información y las comunicaciones que manejan información nacional clasificada en la Administración

[Ref.- 5] CCN-STIC-404, Control de soportes informáticos

[Ref.- 6] CCN-STIC-407, Seguridad en telefonía móvil

[Ref.- 7] CCN-STIC-430 Herramientas de Seguridad

[Ref.- 8] CCN-STIC 811 Interconexión en el ENS

[Ref.- 9] CCN-STIC-827, Esquema nacional de seguridad gestión y uso de dispositivos móviles

7. ABREVIATURAS

APN	Access Point Name
APP	Aplicaciones
CCN	Centro Criptológico Nacional
DMZ	DeMilitarized Zone – Zona Desmilitarizada
FwRM	Firewall Red Movil (corporativa)
FwE	Firewall Externo
FwI	Firewall Interno
FwRC	Firewall Red Corporativa
FwTLF	Firewall Telefónico
GSM	Global System for Mobile Communications (sistema global de comunicaciones móviles)
IMS	IP Multimedia Subsystem
INF	Informe de auditoria
IP	Internet Protocol – Protocolo de Internet
IPS	Intrusion Prevention System – Sistema de Prevención de Intrusos
ISDN-RDSI	Integrated Services Digital Network-Red Digital de Servicios Integrados
ISO/IEC	International Standard Organization /International Electrotechnical Comission
LTE	Long Term Evolution
mcc	Mobile country code
MDM	Mobile Device Management
MMS	Multimedia Messaging Service
mnc	Mobile network code
MSISDN	Mobile Station Integrated Service Digital Network, identificador de red del dispositivo móvil
NS	Normativa de Seguridad de la Oficina Nacional de Seguridad (ONS)
ONS	Oficina Nacional de Seguridad
PSTN	Public Switched Telephone Network
REF	Referencia
SIP	Session Initiation Protocol
SMS	Short Messaging System
STIC	Seguridad de las Tecnologías de la Información y la Comunicación
TIC	Tecnologías de la Información y la Comunicación
VoIP	Voz sobre IP
VPN	Virtual Private Network - Red Privada Virtual
WWW	World Wide Web

ANEXO A. DOCUMENTOS CCN-STIC ORIENTADOS A LAS COMUNICACIONES MÓVILES CORPORATIVAS

88. El Centro Criptológico Nacional, dentro del cumplimiento de sus funciones, publica diferentes documentos orientados a ayudar a los responsables de sistemas TIC de la Administración Española a aumentar la seguridad de los sistemas TIC en los que se gestionen recursos de la Administración.

89. En las series documentales CCN-STIC se puede encontrar información, recomendaciones o normativa orientada a diferentes tecnologías y niveles de seguridad.

90. En el campo de las comunicaciones móviles o de sistemas basados en productos pensados para comunicaciones móviles, el lector puede encontrar los siguientes documentos:

    CCN-STIC-302 Interconexión de CIS

    CCN-STIC 1(XXX), siendo esta serie documental en el que se encontraran referencias más concretas en función del dispositivo/s y/o productos que se vayan a utilizar en el sistema.

    CCN-STIC 827 Dispositivos móviles en el ENS

    CCN-STIC 811 Interconexión en el ENS

    CCN-STIC-407 Seguridad Telefonía Móvil

    CCN-STIC-416 Seguridad en VPN´s

    CCN-STIC-417 Seguridad en PABX

    CCN-STIC-418 Seguridad en Bluetooth

    CCN-STIC-45(X), debiendo tener en cuenta solo aquellos sistemas operativos y dispositivos que dispongan de soporte y actualizaciones de seguridad en cada momento.

ANEXO B. EJEMPLO (1) DE NORMATIVA INTERNA DE SEGURIDAD PARA DISPOSITIVOS MÓVILES

1. PROPÓSITO.

El objeto de la presente Normativa de Seguridad en el Uso de Dispositivos Móviles es informar a los usuarios de dispositivos móviles propiedad de <<ORGANISMO>> de lo que es considerado un "uso correcto" de los dispositivos móviles propiedad de <<ORGANISMO>> o, sin ser de su propiedad, accedan a recursos, servicios o datos propiedad del <<ORGANISMO>>.

Esta normativa se establece para proteger la información del <<ORGANISMO>> contenida o tratada en dispositivos móviles, o accesible a través de ellos.

2. ÁMBITO DE APLICACIÓN Y RESPONSABILIDADES.

Se entenderá por "dispositivo móvil" cualquier dispositivo de uso personal o profesional de reducido tamaño con capacidad de registrar, almacenar y/o transmitir datos, voz, video o imágenes, incluyendo entre ellos teléfonos móviles (especialmente, los smartphones), o tabletas (tablets), que sean propiedad del <<ORGANISMO>> o accedan a recursos, servicios o datos propiedad del <<ORGANISMO>> con la autorización explícita de <<ORGANISMO>>.

La unidad <<UNIDAD>> de <<ORGANISMO>> es la competente para dirigir y supervisar el adecuado cumplimiento de lo contenido en el presente documento.

El incumplimiento de las directrices que figuran en la presente normativa puede dar lugar a responsabilidad administrativa, civil o, incluso, penal, atendiendo a la legislación vigente en cada momento.

3. ROLES Y RESPONSABILIDADES.

Comité de Seguridad de la Información del <<ORGANISMO>>

Tiene la responsabilidad general de establecer las medidas de seguridad para los dispositivos móviles que accedan a recursos, servicios o datos propiedad del <<ORGANISMO>>.

El Comité de Seguridad de la Información del <<ORGANISMO>> contará entre sus miembros con el Responsable del Sistema, el Responsable de la Unidad <<U/OC>> competente y el Responsable de Seguridad.

Responsable del Sistema

El Responsable del Sistema tiene la responsabilidad de implantar las medidas de seguridad en el <<ORGANISMO>>.

Unidad competente << UNIDAD **>>**

La unidad << UNIDAD >> debe:

a) Coordinar la adquisición de los dispositivos móviles del <<ORGANISMO>> .

b) Gestionar la entrega de los dispositivos propiedad del <<ORGANISMO>> a los usuarios siguiendo los criterios acordados por el Comité de Seguridad de la Información del <<ORGANISMO>>.

c) Adoptar las acciones oportunas para la distribución, operación y soporte de los dispositivos móviles propiedad del <<ORGANISMO>> que se entreguen.

d) Mantener un inventario de los dispositivos propiedad del <<ORGANISMO>> y de aquellos que, sin ser de su propiedad, accedan a recursos, servicios o datos propiedad del <<ORGANISMO>>. Este inventario incluirá, al menos, marca, modelo, número de serie, departamento del usuario, nombre del usuario y las fechas de entrega, inicio y fin del servicio.

e) Mantener un inventario de las licencias del software instalado en los dispositivos móviles propiedad del <<ORGANISMO>>.

f) Establecer las configuraciones de seguridad para los dispositivos móviles propiedad del <<ORGANISMO>> distribuidos, incluidos parches y actualizaciones de software o firmware.

g) Establecer los requisitos técnicos y las configuraciones necesarias para los dispositivos móviles que no siendo propiedad del <<ORGANISMO>> accedan a recursos, servicios o datos propiedad del <<ORGANISMO>>.

h) Registro de la actividad de los dispositivos propiedad del <<ORGANISMO>> en relación con el cumplimiento de las normas que resulten de aplicación.

i) Aprobar y mantener, si se considera necesario, el listado de dispositivos móviles (marca, modelo, versión) que, no siendo propiedad de <<ORGANISMO>> puedan ser potencialmente utilizados para acceder a recursos, servicios o datos propiedad del <<ORGANISMO>>. En cualquier caso, cada uno de estos dispositivos deberá ser aprobado individualmente, junto con su propietario, antes de permitir el acceso de dicho dispositivo-usuario a recursos, servicios o datos propiedad del <<ORGANISMO>>.

j) Desarrollar, en caso de ser necesario, la Guía de Usuario para el Acceso Remoto con Tecnología Móvil del <<ORGANISMO>>.

k) Revisar periódicamente el cumplimiento de la normativa y estado de actualización de las políticas de seguridad en el sistema.

Responsable de Seguridad

El Responsable de Seguridad se encarga de la supervisión de los dispositivos propiedad del <<ORGANISMO>>, o de los dispositivos que, no siendo propiedad del <<ORGANISMO>> accedan a recursos, servicios o datos propiedad del <<ORGANISMO>>. Igualmente, se encarga de la supervisión de su actividad en relación con el acceso o tratamiento a recursos, servicios o datos propiedad del <<ORGANISMO>>.

En especial, será responsable de que el usuario:

a) Suscriba, en su caso, el Acuerdo de Usuario de Tecnología Móvil del <<ORGANISMO>>, en el que se comprometa al cumplimiento de la presente Normativa.

b) Reciba la información necesaria para el correcto cumplimiento de la presente Normativa.

Usuarios

Los Usuarios son aquellas personas que desarrollen actividades profesionales con dispositivos móviles propiedad del <<ORGANISMO>> o que utilizan o acceden a recursos propiedad del Organismo. Dichos Usuarios deberán:

a) Suscribir la presente Normativa de seguridad en el uso de los dispositivos móviles en el <<ORGANISMO>>.

b) Suscribir (si no lo ha hecho con anterioridad) y cumplir, en lo que resulte de aplicación, con la Normativa General de Uso de los Sistemas de Información del <<ORGANISMO>>.

c) Utilizar el dispositivo móvil de acuerdo con la presente Normativa, con la legislación que resulte aplicable y con la Guía de Usuario para el Acceso Remoto con Tecnología Móvil del <<ORGANISMO>>.

d) El usuario debe utilizar el dispositivo dentro de los parámetros comunicados por el <<ORGANISMO>>.

e) Utilizar sólo aquellos dispositivos entregados o autorizados por el <<ORGANISMO>> para su conexión con sistemas del <<ORGANISMO>>.

f) Utilizar sólo aquellos dispositivos y accesorios entregados o autorizados por el <<ORGANISMO>> para el acceso a recursos, servicios o datos propiedad del <<ORGANISMO>>.

g) Cualquier otro accesorio que no le sea suministrado por el <<ORGANISMO>> y que, sin estar expresamente prohibido, pretendiera usar combinado con el dispositivo (por ejemplo: fundas, estuches, cargadores de coche, protectores de pantalla, auriculares Bluetooth, etc.) deberá ser adquirido por el usuario. Estos accesorios deben poder ser retirados del dispositivo en cualquier momento, devolviendo este a su estado original cuando fue entregado al usuario.

h) Almacenar en el dispositivo móvil aquella información de carácter personal estrictamente indispensable para el desarrollo de las funciones profesionales. Este almacenamiento se realizará solo en caso de necesidad y se procederá a su borrado cuando ya no sea necesario su almacenamiento o tratamiento. Al aceptar el dispositivo proporcionado por el <<ORGANISMO>>, los usuarios prestan su consentimiento informado para que el <<ORGANISMO>> pueda monitorizar su uso, incluyendo el contenido de los archivos y la información almacenada, los mensajes recibidos o enviados o el historial de navegación.

i) Disponer las medidas oportunas para evitar la pérdida, robo o compromiso del dispositivo móvil, especialmente fuera de las dependencias del <<ORGANISMO>> o durante viajes.

j) No desactivar o alterar las características de seguridad del dispositivo.

k) Comunicar inmediatamente a la Unidad Competente (Centro de Soporte) y su supervisor si el dispositivo sufre daños, se pierde, es robado o se sospecha de su manipulación por terceras partes.

l) Cumplir con la legislación en materia de uso de dispositivos móviles ajena al <<ORGANISMO>> que le fuera de aplicación.

Aquellas personas que desarrollen actividades profesionales en el <<ORGANISMO>> con dispositivos móviles que no sean propiedad del <<ORGANISMO>> deberán:

a) Suscribir la presente Normativa de seguridad en el uso de los dispositivos móviles en el <<ORGANISMO>>.

b) Suscribir (si no lo ha hecho con anterioridad) y cumplir, en lo que resulte de aplicación, con la Normativa General de Uso de los Sistemas de Información del <<ORGANISMO>>.

c) Utilizar el dispositivo móvil de acuerdo con la presente Normativa, con la legislación que resulte aplicable y con la Guía de Usuario para el Acceso Remoto con Tecnología Móvil del <<ORGANISMO>>.

d) El usuario debe utilizar el dispositivo dentro de los parámetros comunicados por el <<ORGANISMO>>.

e) Almacenar en el dispositivo móvil aquella información de carácter profesional estrictamente indispensable para el desarrollo de las funciones profesionales. Este almacenamiento se realizará solo en caso de necesidad, se procederá a su borrado cuando ya no sea necesario su tratamiento.

f) No desactivar o alterar las características de seguridad del dispositivo por las cuales el dispositivo ha sido autorizado a acceder a recursos del <<ORGANISMO>>.

g) Disponer las medidas oportunas para evitar la pérdida, robo o compromiso del dispositivo móvil, especialmente fuera de las dependencias del <<ORGANISMO>> o durante viajes.

h) Comunicar inmediatamente con la Unidad Competente (Centro de Soporte) y su supervisor si el dispositivo sufre daños, se pierde, es robado o se sospecha de su manipulación por terceras partes.

4. NORMAS ADICIONALES

La << UNIDAD >> del <<ORGANISMO>> es la unidad encargada de la supervisión, gestión del uso y control de gastos asociados a los dispositivos móviles propiedad del <<ORGANISMO>>.

Los dispositivos proporcionados por el <<ORGANISMO>> se entregan como herramientas profesionales de productividad. El <<ORGANISMO>>, a través de la <<U/OC>> competente, se reserva el derecho de suspender los servicios por no uso o uso indebido.

El <<ORGANISMO>> permite a los usuarios un uso limitado de los recursos tecnológicos del <<ORGANISMO>> para propósito personal, siempre que tal uso no interfiera en el uso profesional y no comporte gastos adicionales para el <<ORGANISMO>>. En todo caso, el uso personal y limitado del dispositivo entregado por el <<ORGANISMO>> se regirá mediante la "Normativa General de Uso de los Sistemas de Información del <<ORGANISMO>>".

La selección de los dispositivos móviles es competencia de la << UNIDAD >>. Para la selección tendrá en cuenta la disponibilidad señalada por los fabricantes o distribuidores y en la necesidad de contar con la aprobación o autorización para su uso como dispositivos con las medidas de seguridad necesarias.

La asistencia y soporte técnico será realizado por << UNIDAD >> [incluyendo dirección, teléfono, etc.] que se constituye en Centro de Soporte del <<ORGANISMO>> para incidencias relativas a los dispositivos móviles propiedad del <<ORGANISMO>>.

Las tarifas y modalidades de contratación son competencia exclusiva del Comité de Seguridad de la Información del <<ORGANISMO>> y de la Unidad << UNIDAD >> competente. Estas tarifas serán comunicadas a los usuarios de los dispositivos propiedad del <<ORGANISMO>> bajo criterio de la << UNIDAD >>competente.

El <<ORGANISMO>> se reserva el derecho de retirar o no permitir la utilización de los dispositivos de su propiedad, así como de modificar los permisos asociados a usuarios que accedan a recursos propiedad del <<ORGANISMO>> con dispositivos que no sean propiedad del <<ORGANISMO>>.

Las modificaciones a la presente Normativa son competencia de la << UNIDAD >> y del Comité de Seguridad de la Información del <<ORGANISMO>>, y serán comunicadas a los usuarios de los dispositivos móviles que hayan suscrito el cumplimiento de dicha Normativa.

Las preguntas relacionadas con la presente Normativa y sus Directrices se dirigirán a la << UNIDAD >> del <<ORGANISMO>>.

ACUERDO DE USUARIO DE TECNOLOGÍA MÓVIL

Aceptación y compromiso de cumplimiento

Mediante la cumplimentación de la siguiente declaración, el abajo firmante, [*personal del <<ORGANISMO>>*], como usuario de dispositivos móviles del <<ORGANISMO>>, declara haber leído y comprendido la NORMATIVA DE SEGURIDAD EN EL USO DE DISPOSITIVOS MÓVILES EN EL <<ORGANISMO>> (*versión x*) y se compromete, bajo su responsabilidad, a su cumplimiento.

<<En _____, a ____ de _____ de 2___>>

Organismo:	
Empleado (nombre y apellidos):	
Documento de Identificación/DNI:	
Número de Registro de Personal en <<ORGANISMO>>:	
Firmado:	

Por el <<ORGANISMO>>: <<*Nombre y Apellidos*>>

Documento de Identificación/DNI número: _____

Número de Registro de Personal en <<ORGANISMO>>: _____

ANEXO C. EJEMPLO (2) DE NORMATIVA INTERNA DE SEGURIDAD PARA DISPOSITIVOS MÓVILES

<<ORGANISMO>>, a través de <<UNIDAD>>, facilita/autoriza a los usuarios el equipamiento móvil y portátil necesario para la realización de las tareas relacionadas con su puesto de trabajo. En consecuencia, este equipamiento no está destinado para uso personal, teniendo dicho uso carácter excepcional y limitado, de conformidad con la presente Norma.

No está permitido alterar la configuración física o lógica del equipamiento a iniciativa del usuario, contar con la autorización expresa de <<UNIDAD>>. Dicha autorización debe ser individual para cada usuario final y dispositivo utilizado.

No está permitido instalar aplicaciones o cualquier tipo de software no autorizado expresamente por <<UNIDAD>>, además, previo a la instalación de dicho software, debe contarse con la correspondiente licencia de uso.

Se respetará la normativa en todo lo referente a tratamiento de información en los dispositivos móviles y portátiles proporcionados por <<ORGANISMO>>, así como con los autorizados por <<ORGANISMO>> para acceder a sus recursos.

Los servicios técnicos de <<UNIDAD>> ofrecerán el soporte necesario ante las incidencias y averías en el equipamiento móvil y portátil sujeto a la presenta Normativa. Estos servicios técnicos, en el desempeño de sus tareas, podrán supervisar los dispositivos, así como el software instalado en ellos, o las comunicaciones realizadas.

Es estrictamente necesario cumplir las medidas de seguridad y control establecidas por <<UNIDAD>> en cada momento.

Todos los usuarios del sistema deben estar identificados de manera univoca, pudiendo habilitarse identificadores “de grupo” solo en casos excepcionales y siempre autorizados expresamente por <<UNIDAD>>.

El acceso a Internet desde dispositivos móviles y portátiles gestionados por <<UNIDAD>> de <<ORGANISMO>>, en caso de estar configurado, obedece a fines profesionales. El uso personal ocasional debe limitarse al mínimo imprescindible y debiendo extremarse la precaución en el acceso a páginas web o servicios no controlados por <<ORGANISMO>>.

La utilización de sistemas de comunicaciones (correo electrónico, mensajería instantánea, VozIP, etc.) diferentes a los gestionados por <<ORGANISMO>> y que permitan el intercambio de información con dispositivos ajenos a <<ORGANISMO>> debe limitarse a los autorizados expresamente por <<UNIDAD>>

El abajo firmante, *personal del <<ORGANISMO>>*, como usuario de dispositivos móviles de <<ORGANISMO>>, declara haber leído y comprendido la NORMATIVA INTERNA DE SEGURIDAD PARA DISPOSITIVOS MÓVILES EN <<ORGANISMO>> y se compromete, bajo su responsabilidad, a su cumplimiento.

Organismo:	
Empleado (nombre y apellidos):	
Documento de Identificación/DNI:	
Número de Registro de Personal en <<ORGANISMO>>:	
Firmado:	

Por <<ORGANISMO>>: <<Nombre y Apellidos>>

Documento de Identificación/DNI número: _____

Número de Registro de Personal en <<ORGANISMO>>: _____

<<En _____, a ____ de _____ de 2___>>

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL