



**GUÍA DE SEGURIDAD  
(CCN-STIC 827)**

**ESQUEMA NACIONAL DE SEGURIDAD  
GESTIÓN Y USO DE DISPOSITIVOS  
MÓVILES**



MARZO 2014

Edita:



© Editor y Centro Criptológico Nacional, 2014  
NIPO: 002-14-026-0

Fecha de Edición: marzo de 2014

El Ministerio de Hacienda y Administraciones Públicas ha financiado el desarrollo del presente documento y sus anexos.

#### **LIMITACIÓN DE RESPONSABILIDAD**

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

#### **AVISO LEGAL**

Quedan rigurosamente prohibidas, sin la autorización escrita del **Centro Criptológico Nacional**, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

## PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su 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, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

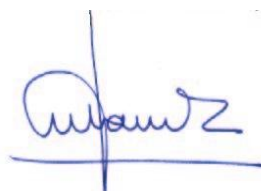
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además, uno de los principios que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el Esquema Nacional de Seguridad (ENS).

Precisamente el Real Decreto 3/2010 de 8 de Enero de desarrollo del Esquema Nacional de Seguridad fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, 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 su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Marzo de 2014



Félix Sanz Roldán  
Secretario de Estado  
Director del Centro Criptológico Nacional

**ÍNDICE**

<b>1. OBJETO DEL DOCUMENTO .....</b>	<b>5</b>
<b>2. ÁMBITO DE APLICACIÓN .....</b>	<b>6</b>
<b>3. LOS DISPOSITIVOS MÓVILES: ASPECTOS DE SEGURIDAD .....</b>	<b>7</b>
3.1. CARACTERÍSTICAS GENERALES DE LOS DISPOSITIVOS MÓVILES.....	7
3.2. LOS DISPOSITIVOS MÓVILES CONSIDERADOS EN ESTA GUÍA.....	7
3.3. PENETRACIÓN DE LOS DISPOSITIVOS MÓVILES Y OBJETIVOS DE SEGURIDAD .....	8
3.4. LOS RIESGOS DERIVADOS DE LA MOVILIDAD .....	9
3.5. EL USO DE DISPOSITIVOS MÓVILES NO-CONFIABLES .....	10
3.6. USO DE REDES INSEGURAS .....	11
3.7. USO DE APLICACIONES NO-CONFIABLES .....	12
3.8. INTERCONEXIÓN CON OTROS SISTEMAS.....	13
3.9. USO DE CONTENIDOS NO-CONFIABLES .....	14
3.10. EL USO DE SERVICIOS DE LOCALIZACIÓN .....	15
<b>4. LA GESTIÓN DE LOS DISPOSITIVOS MÓVILES .....</b>	<b>16</b>
4.1. TIPOS DE GESTIÓN .....	16
4.2. GRUPOS DE MEDIDAS DE SEGURIDAD .....	18
<b>5. EL DESPLIEGUE DE LA SEGURIDAD DE LOS DISPOSITIVOS MÓVILES EN LOS ORGANISMOS.....</b>	<b>22</b>
5.1. INICIACIÓN.....	23
5.2. DESARROLLO.....	30
5.3. IMPLANTACIÓN .....	31
5.4. OPERACIÓN Y MANTENIMIENTO.....	33
5.5. RETIRADA.....	34
<b>6. EL USO DE LOS DISPOSITIVOS MÓVILES EN LOS ORGANISMOS PÚBLICOS EN FUNCIÓN DE LOS NIVELES DE SEGURIDAD DEL ENS .....</b>	<b>35</b>
<b>ANEXO A: LA APLICACIÓN DE LAS MEDIDAS DE SEGURIDAD DEL ENS.....</b>	<b>39</b>
<b>ANEXO B: ASPECTOS DE DECISIÓN SOBRE BYOD.....</b>	<b>55</b>
<b>ANEXO C: MODELO DE NORMATIVA DE SEGURIDAD EN EL USO DE DISPOSITIVOS MÓVILES EN EL &lt;&lt;ORGANISMO&gt;&gt; .....</b>	<b>57</b>
<b>ANEXO D: REFERENCIAS .....</b>	<b>64</b>

## 1. OBJETO DEL DOCUMENTO

1. El propósito esta Guía es establecer unas pautas de carácter general que puedan resultar de aplicación a entidades de distinta naturaleza, dimensión y sensibilidad, sin entrar en casuísticas específicas. Por ello, es de esperar que cada organización las particularice para adaptarlas a su entorno singular.
2. Esta Guía, además de analizar la problemática derivada del uso de los dispositivos móviles, propone a los organismos de las Administraciones públicas españolas un modelo de comportamiento –gestión y uso- de tales dispositivos, en relación con la adopción y mantenimiento de las medidas de seguridad que el uso de tales dispositivos exige, dentro del marco definido por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica (ENS, en adelante).
3. La publicación de esta Guía y los modelos que en ella se contienen contribuirá a:
  - Facilitar el máximo aprovechamiento de los recursos y sistemas de información en la actuación de las Administraciones públicas.
  - Asegurar la protección de los derechos de los ciudadanos en sus relaciones con las Administraciones públicas y el desenvolvimiento profesional de los empleados públicos y usuarios que tienen acceso a los recursos y sistemas de información de las Administraciones públicas.
  - Mejorar los servicios que las Administraciones públicas prestan a los ciudadanos, propiciando una gestión eficiente y segura de los procesos incluidos en los sistemas de información con los que opera.
  - Proteger a los sistemas de información de las Administraciones públicas y a los datos que tratan de los riesgos que puedan deberse a la acción humana, especialmente en lo referente a conductas incorrectas, inadecuadas o ilegales, y todo ello de conformidad con lo dispuesto en el ENS.

**En resumen, el objetivo de esta Guía es ayudar a los organismos en la gestión segura de los dispositivos móviles desplegados en la organización o que puedan ser usados para acceder a recursos, informaciones o servicios de la organización. Incluye, por tanto, a los dispositivos móviles propiedad de la organización, como aquellos otros, propiedad de los usuarios (comportamiento conocido como BYOD<sup>1</sup>), y en ambos casos para el desempeño total o parcial de las labores de los usuarios en relación con sus competencias profesionales en el seno del organismo de que se trate.**

---

<sup>1</sup> **BYOD** (*Bring Your Own Device*) es un concepto que permite a los empleados de una organización usar la tecnología de la que son propietarios para desarrollar sus funciones profesionales dentro de tal organización. Como mínimo, los modelos BYOD permiten a los usuarios acceder a servicios, recursos o datos corporativos desde sus smartphones, tablets, e-readers personales y otros dispositivos. Esto podría incluir también a los ordenadores portátiles y de sobremesa. Sin embargo, a la vista de la madurez alcanzada por las soluciones de seguridad para estos últimos dispositivos, la presente Guía centra su atención en el emergente caso de uso de los dispositivos móviles señalados.

## 2. ÁMBITO DE APLICACIÓN

4. La información y los modelos contenidos en la presente Guía resultan de aplicación a cualquier entidad del sector público del ámbito de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos (LAECSP, en adelante): Administración General del Estado, Administración de las Comunidades Autónomas y Administración de las Entidades Locales.
5. Resultando conveniente la lectura de esta Guía por parte de los Responsables de la Información y los Responsables de los Servicios<sup>2</sup> del organismo de que se trate, el presente documento resultará de especial interés para Responsables de Sistemas de Información, Responsables de Seguridad de Sistemas de Información, Administradores de Seguridad de Sistemas de Información y, en general, a todos aquellos empleados públicos responsables de la planificación, implementación y mantenimiento de los dispositivos móviles en la organización y su seguridad.
6. Por otro lado, la calificación del nivel de seguridad de la información y de los servicios a los que pudieran afectar los modelos comprendidos en la presente Guía, se ha dispuesto atendiendo a las denominaciones establecidas en el ENS: BAJO, MEDIO o ALTO<sup>3</sup>. La calificación de información clasificada (SECRETO, RESERVADO, CONFIDENCIAL y DIFUSIÓN LIMITADA) se hará atendiendo a las regulaciones que le son específicamente de aplicación<sup>4</sup>.
7. Finalmente, todas las recomendaciones que se señalan en la presente Guía se contemplan sin perjuicio de la adicional adopción de las previsiones que dimanen de otras regulaciones, tales como la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, etc.

---

<sup>2</sup> En el sentido que el ENS da a ambos términos.

<sup>3</sup> Estas denominaciones son independientes de las establecidas para las medidas de seguridad contempladas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BÁSICO, MEDIO o ALTO), que asimismo resultarán de aplicación cuando se traten datos de carácter personal.

<sup>4</sup> Denominaciones definidas en la Ley 9/1968, de 5 de abril, reguladora de los Secretos Oficiales (LSO, en adelante) y en la Norma NS/04 de la Autoridad Nacional, así como en Políticas de Seguridad de Organizaciones Internacionales y Acuerdos para Protección de la Información Clasificada, y en determinados Departamentos Ministeriales (MINISDEF), como desarrollo de la precitada LSO.

### 3. LOS DISPOSITIVOS MÓVILES: ASPECTOS DE SEGURIDAD

8. En este epígrafe se detallan aquellas características de los dispositivos móviles que, en materia de seguridad y atendiendo a los previsibles impactos derivados de la materialización de riesgos, exigen un tratamiento diferenciado de otro tipo de equipos, tales como los ordenadores de sobremesa o portátiles.

#### 3.1. CARACTERÍSTICAS GENERALES DE LOS DISPOSITIVOS MÓVILES

9. Los dispositivos móviles comprendidos en el ámbito de aplicación de esta Guía poseen, en general, las siguientes características comunes:
- Tamaño reducido.
  - Un interfaz inalámbrico para acceso remoto y comunicación de datos<sup>5</sup>.
  - Memoria interna, no removible.
  - Sistema operativo, en general distinto de los usados en ordenadores de sobremesa y portátiles<sup>6</sup>.
  - Múltiples aplicaciones disponibles<sup>7</sup>.
10. En algunos casos, los dispositivos móviles también disponen de otras características, de naturaleza opcional, entre las que cabe destacar:
- Interfaces inalámbricas para la construcción de redes personales<sup>8</sup>.
  - Interfaces inalámbricas para la comunicación de voz<sup>9</sup>.
  - Sistema de posicionamiento vía satélite (GPS)<sup>10</sup>.
  - Una (o más) cámara(s) digital(es)<sup>11</sup>.
  - Micrófono.
  - Interfaces para la conexión de memorias externas.
  - Mecanismos para sincronizar la información local dispositivo con otros equipamientos<sup>12</sup>.

#### 3.2. LOS DISPOSITIVOS MÓVILES CONSIDERADOS EN ESTA GUÍA.

11. Para el propósito de esta Guía, los dispositivos móviles que se consideran serán todos aquellos que, atendiendo a las características generales enunciadas con anterioridad, poseen uno de los siguientes sistemas operativos: Android (Google), AOSP- BlackBerry (RIM), iOS (Apple) y Windows Phone (Microsoft), es decir, aquellos que, en la actualidad, están comprendidos dentro de los llamados smartphones y las tabletas (tablets).

<sup>5</sup> Este interfaz estará generalmente sustentado en tecnología wi-fi, telefonía móvil u otras tecnologías que posibiliten la conexión del dispositivo con infraestructuras de red y su acceso a internet.

<sup>6</sup> No obstante, recientemente estamos observando una tendencia en determinadas firmas comerciales, haciendo converger los sistemas operativos usados por los equipos tradicionales con los dispositivos móviles.

<sup>7</sup> Incorporadas de fábrica a los dispositivos móviles o disponibles a través de diferentes métodos tales como el acceso a páginas web o tiendas oficiales y no-oficiales de suministro de software.

<sup>8</sup> Tales como Bluetooth o Near-Field-Communications.

<sup>9</sup> Tales como los habitualmente usados en la telefonía móvil habitual.

<sup>10</sup> Lo que permite el acceso a servicios de localización.

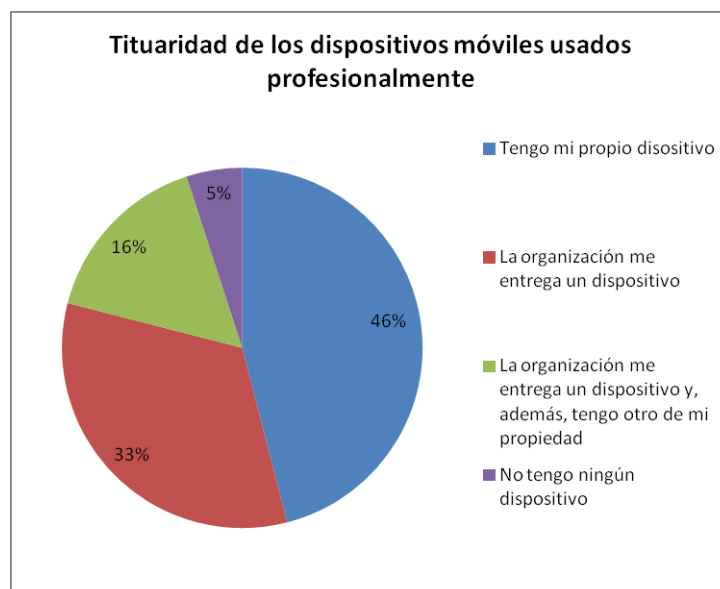
<sup>11</sup> Para la captación de imágenes (fotografías) o vídeos.

<sup>12</sup> Generalmente, ordenadores de sobremesa o portátiles, servidores, ISPs, terceras entidades, etc.

12. No están comprendidos, por tanto, los ordenadores portátiles (laptops o notebooks) entendiéndose que las medidas y controles de seguridad que resultan aplicables a estos equipos son sustancialmente diferentes de las que requiere una gestión segura de los ante dichos dispositivos móviles. Asimismo, están excluidos del ámbito de aplicación de esta Guía aquellos teléfonos móviles que no disponen de una mínima capacidad de computación y que, en general, se utilizan exclusivamente para el intercambio de comunicaciones de voz y mensajes cortos (SMSs).
13. Como se ha dicho, el ámbito de aplicación de esta Guía incluye tanto los dispositivos proporcionados por los organismos a sus usuarios (empleados públicos, generalmente, pero también colaboradores, subcontratistas, etc.), como aquellos otros dispositivos propiedad de las antedichas personas, y que pretenden utilizar en la infraestructura informática y de comunicaciones del organismo en cuestión.

### 3.3. PENETRACIÓN DE LOS DISPOSITIVOS MÓVILES Y OBJETIVOS DE SEGURIDAD

14. De acuerdo con datos de Gartner, en 2014, presumiblemente, el 90% de las organizaciones desplegarán sus aplicaciones corporativas en los dispositivos móviles y el 80% de los profesionales utilizará al menos dos dispositivos móviles personales para acceder a datos corporativos<sup>13</sup>. Además, Gartner señala que en 2016 se adquirirán a nivel mundial más de 1600 millones de dispositivos móviles inteligentes. Dos tercios de los empleados (de organizaciones públicas o privadas) de todo el mundo poseerán su propio smartphone y/o tablet, siendo así que el 40% de tales empleados desarrollarán su trabajo habitualmente con tales dispositivos<sup>14</sup>.



*iPass Mobile Workforce Report*<sup>15</sup>

15. En comparación con otro tipo de equipamientos -como los ordenadores de sobremesa o los ordenadores portátiles-, los dispositivos móviles requieren, en general, medidas de seguridad adicionales, debido a que suelen estar expuestos a un mayor número de riesgos, especialmente los derivados de su uso fuera de las instalaciones de la organización.

<sup>13</sup> <http://www.industryweek.com/workforce/byod-powerful-enabler-or-impending-catastrophe>

<sup>14</sup> <http://www.gartner.com/newsroom/id/2207915>

<sup>15</sup> Nov., 2012



16. Más aún, como se ha recogido en diferentes documentos<sup>16</sup>, los dispositivos móviles constituyen una importante fuente de riesgos a la seguridad IT de las organizaciones que resulta indispensable limitar atendiendo a dos mecanismos complementarios:
- Activación de las características de seguridad incorporadas al propio dispositivo y
  - Aplicación de controles de seguridad adicionales, a través de los procedimientos de gestión de seguridad IT de la organización de que se trate.
17. Como la mayoría de los equipamientos usados para el tratamiento de información, los objetivos de seguridad para dispositivos móviles responden a la satisfacción de las siguientes dimensiones de seguridad:
- 1 *Confidencialidad*: garantizando que la información enviada, recibida o almacenada por el dispositivo no puede ser leída por terceros no autorizados.
  - 2 *Integridad*: garantizando que la información enviada, recibida o almacenada en el dispositivo no es alterada por terceros no autorizados.
  - 3 *Disponibilidad*: garantizando que los recursos que necesitan los usuarios (del propio dispositivo o externos a él) están disponibles siempre que se necesitan.
  - 4 *Autenticación*: garantizando que el dispositivo móvil no está siendo suplantado por otro.
  - 5 *Trazabilidad*: garantizando el seguimiento y la determinación de los tratamientos efectuados en el dispositivo.
18. Para alcanzar los antedichos objetivos de seguridad, el ENS, en su Anexo II, explícita los controles o medidas de seguridad que, en cada caso, y dependiendo del nivel o categoría del sistema, resultan de aplicación.
19. En el Anexo A de esta Guía se incluye un Catálogo de Medidas de Seguridad del ENS que pueden usarse para la gestión de la seguridad de los dispositivos móviles.
20. No obstante, antes de desplegar las oportunas medidas de seguridad que resulten de aplicación a los dispositivos móviles, los organismos públicos deberán analizar los riesgos derivados del uso de tales dispositivos, especialmente cuando dichos equipos pretendan acceder a recursos o informaciones corporativas. Tal análisis de riesgos, por tanto, deberá identificar los recursos (activos) que resulten de interés, sus vulnerabilidades y amenazas y la probabilidad de su materialización, determinándose seguidamente las medidas de seguridad que resulten de aplicación, implantándose de manera proporcional al presumible éxito de los ataques y sus correspondientes impactos.

### 3.4. LOS RIESGOS DERIVADOS DE LA MOVILIDAD

21. Uno de los mayores problemas que plantea la securización de los dispositivos móviles deriva, precisamente, de la posibilidad de que puedan usarse en ubicaciones muy diversas, tanto dentro de las instalaciones del organismo en cuestión (bajo cuyo perímetro de seguridad puede estar desplazándose permanentemente), como en localizaciones externas (domicilio de los usuarios, lugares públicos, hoteles, etc.), obligando a considerar incidentes tales como el extravío o el hurto, lo que eleva sus riesgos, si los comparamos con otro tipo de equipamientos.

---

<sup>16</sup> Véase, por ejemplo, los recientes Informes de Amenazas y Tendencias publicados por el CCN (<https://www.ccn-cert.cni.es/>)

22. Conviene recordar que el acceso a los dispositivos móviles por parte de actores maliciosos posee persigue habitualmente un doble objetivo: acceder a los datos contenidos en el propio dispositivo y/o, a su través, acceder a la información corporativa. Los organismos públicos, en base a esta realidad, deberán adoptar las medidas de seguridad pertinentes.
23. Algunas de las amenazas más frecuentes son:
- Acceso físico no autorizado al dispositivo móvil.
  - Acceso no autorizado a la información almacenada.
  - Acceso no autorizado y manipulación de la información transmitida.
  - Presencia de código dañino en las aplicaciones móviles.
  - Uso de aplicaciones o servicios no aceptados por el organismo.
  - Uso inadecuado cuando el dispositivo se comparte para uso personal y profesional.
  - Reutilización o reciclado de dispositivos móviles.
  - Utilización de BYOD en el seno de la organización.
24. Para mitigar el impacto de ataques de este tipo, las medidas de seguridad que pueden adoptarse pueden ser de muy diversa índole, entre ellas:
- Exigiendo autenticación antes de lograr el acceso al dispositivo móvil y/o a los recursos corporativos accesibles a través de dicho dispositivo.
  - Tales mecanismos de autenticación suelen estar basados en contraseñas simples (PIN) y, salvo excepciones, asumiendo que el dispositivo móvil en cuestión tiene un único usuario.
  - Si el mecanismo anterior resultará débil –por razón de la importancia concedida al dispositivo en cuestión o a la información accedida a su través-, pueden usarse, además, otros métodos de autenticación más robusta, tales como los basados en dispositivos externos (tokens), autenticación de dispositivos basada en red y autenticación de dominios.
  - No permitiendo el almacenamiento de información sensible en el dispositivo móvil. Si esto no es posible, será necesario proteger la información sensible almacenada – cifrándola, por ejemplo-, haciendo al tiempo imposible su extracción del dispositivo por personas no autorizadas.
  - Proporcionando a los usuarios de dispositivos móviles la formación y la concienciación necesarias para reducir los comportamientos poco seguros y su frecuencia.
25. Como se ha dicho, el Anexo A de esta Guía incluye un Catálogo de Medidas de Seguridad del ENS que pueden usarse para la gestión de la seguridad de los dispositivos móviles.

### **3.5. EL USO DE DISPOSITIVOS MÓVILES NO-CONFIABLES**

26. Que un dispositivo móvil se use en el seno de una organización no significa que sea confiable. En muchos casos, especialmente cuando se trata de dispositivos propiedad de los propios usuarios (BYOD), tales equipos pueden presentar importantes inconvenientes en materia de seguridad, derivadas tanto de su configuración como de un uso inseguro. Tal es

el caso, por ejemplo, de los procedimientos de jailbreaking<sup>17</sup> o rooting<sup>18</sup> que algunos usuarios llevan a cabo, introduciendo importantes elementos de riesgo. Por tanto, en ausencia de medidas concretas, los organismos públicos asumirán que tales dispositivos son, por definición, inseguros, debiendo en su consecuencia adoptar las correspondientes medidas de seguridad en tanto tales equipos tengan acceso a aplicaciones o datos corporativos.

27. Algunas de las estrategias que pueden usarse para mitigar estos riesgos son:
  1. Prohibir totalmente el uso de dispositivos móviles propiedad de los usuarios.
  2. Permitir su uso, pero limitando algunas de aquellas características que puedan representar mayores riesgos.
  3. Proporcionar a los usuarios dispositivos móviles de titularidad de la organización.
  4. Adoptar para cada uno de los dispositivos móviles de la organización que pudieran tener acceso a sus recursos las medidas de seguridad que permitan un constante control de los mismos, detectando incumplimientos o desviaciones<sup>19</sup>.

### 3.6. USO DE REDES INSEGURAS

28. El acceso de los dispositivos móviles a los servicios o a los datos corporativos puede llevarse a cabo usando redes públicas (por definición, no confiables) o redes privadas del organismo o infraestructuras de comunicación comunes<sup>20</sup>.
29. En el caso de redes públicas, los organismos no suelen disponer de mecanismos para controlar la seguridad del acceso de dispositivos móviles a tales redes públicas; acceso que puede tener lugar, generalmente, a través de mecanismos wi-fi o tecnologías de telefonía móvil. Por tanto, el uso de este tipo de redes posibilita ciberataques de tipo man-in-the-middle<sup>21</sup>, que podrían interceptar e incluso modificar los datos en tránsito.
30. Por consiguiente, en tanto el acceso a los recursos corporativos no se realice mediante redes seguras, los organismos deberán adoptar las medidas oportunas para impedir que los riesgos derivados del uso de redes inseguras tengan impacto en la organización. Algunas de tales medidas son las siguientes:

---

<sup>17</sup> El **jailbreak** es el proceso de eliminación de las restricciones impuestas por [Apple](#) en dispositivos que utilicen el sistema operativo [iOS](#), mediante el uso de [kernels](#) modificados. Tales dispositivos incluyen los [iPhone](#), [iPod Touch](#), [iPad](#) y la [Apple TV](#) de segunda generación. El jailbreak permite a los usuarios acceder sin limitaciones al [sistema operativo](#), permitiendo descargar aplicaciones y otros elementos que no estén disponibles a través de la [App Store](#) oficial.

<sup>18</sup> El **rooting** es un proceso que permite a los usuarios de smartphones, tabletas y otros dispositivos que ejecutan el sistema operativo móvil Android de elevar el control de privilegios del sistema operativo. El rooting se realiza a menudo con el objetivo de superar las limitaciones que los operadores de comunicaciones o de hardware introducen en algunos dispositivos, lo que hace posible modificar o reemplazar las aplicaciones y ajustes del sistema, ejecutar aplicaciones especializadas que requieren permisos de administrador, o realizar otras operaciones de otro modo inaccesibles para un usuario de Android normal.

<sup>19</sup> Esto puede lograrse, por ejemplo, ejecutando las aplicaciones del organismo en un contenedor seguro (sandbox) dentro del propio dispositivo.

<sup>20</sup> Tal como la Red SARA (Red Interadministrativa de las Administraciones Públicas españolas), por ejemplo.

<sup>21</sup> En [criptografía](#), un **ataque man-in-the-middle o JANUS (MitM o intermediario)**, en español) es un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado. El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas.

- Usar mecanismos de cifrado fuerte (tales como el uso de redes privadas virtuales VPNs)<sup>22</sup>.
- Usar mecanismos de autenticación mutua que permitan a las partes intervinientes en la comunicación identificarse mutuamente antes de intercambiar ningún tipo de información.
- Prohibir el uso de redes wi-fi inseguras, especialmente aquellas para las que se han publicado vulnerabilidades.
- Desactivar aquellos interfaces de red del dispositivo que no vayan a usarse.

### 3.7. USO DE APLICACIONES NO-CONFIABLES

31. En la actualidad, la mayoría de las aplicaciones que se ejecutan en smartphones y tabletas se descargan de tiendas (oficiales y no oficiales) de aplicaciones<sup>23</sup>. Aunque, en algunos casos, estas tiendas realizan controles (limitados) respecto de las aplicaciones de terceros que albergan, no puede obviarse el riesgo adicional para los usuarios finales. Por tanto, asumiendo que no todas las aplicaciones habrán pasado por los adecuados controles de seguridad, los organismos públicos deberán tratar tales aplicaciones como no-confiables por defecto, adoptando para ellas las medidas de seguridad que se estimen convenientes.
32. Algunas de las medidas que pueden usarse para limitar los antedichos riesgos son:
  - Prohibir totalmente la instalación de aplicaciones de terceras partes.
  - Permitir, únicamente, la instalación de determinadas aplicaciones provenientes del “listas blancas” (whitelisting<sup>24</sup>).
  - Verificar que las aplicaciones sólo obtienen del dispositivo móvil los permisos estrictamente necesarios para su adecuado funcionamiento.
  - Posibilitar la ejecución de las aplicaciones en contenedores seguros (sandbox<sup>25</sup>) dentro del dispositivo, que aislen las aplicaciones y datos corporativos de otras aplicaciones y datos que puedan residir en el dispositivo.
  - Ejecutar un análisis de riesgos de cada una de las aplicaciones de tercera parte antes de permitir su uso de los dispositivos móviles de la organización.
33. Como así se ha señalado, conviene advertir que, incluso cuando tales estrategias de mitigación de riesgos se adopten para todas las aplicaciones que puedan descargarse a través de tiendas de aplicaciones, los usuarios de dispositivos móviles siempre tienen la posibilidad de descargar aplicaciones no confiables accediendo a las páginas web de sus distribuidores, mediante el uso del software de navegación del que disponen tales dispositivos.
34. Ante esta problemática, caben las siguientes medidas de seguridad:

---

<sup>22</sup> Sobre este particular, consúltese la Guía CCN-STIC 807 Criptología de empleo en el Esquema Nacional de Seguridad.

<sup>23</sup> Apple Store, para sistemas iOS y Google Play, para sistemas Android, entre otras.

<sup>24</sup> Una **lista blanca**, **lista de aprobación** ó **whitelist** es una lista o registro de entidades que, por una razón u otra, pueden obtener algún privilegio particular, servicio, movilidad, acceso o reconocimiento.

<sup>25</sup> En [seguridad informática](#), el **aislamiento de procesos** (del inglés *sandbox*) es un mecanismo para ejecutar programas de manera segura y separada. A menudo se utiliza para ejecutar código nuevo, o software de dudosa confiabilidad proveniente de terceros. Ese aislamiento permite controlar los recursos proporcionados a los programas "cliente" a ejecutar, tales como espacio temporal en memoria y disco. Habitualmente, se limitan las capacidades de acceso a redes, la posibilidad de inspeccionar la máquina anfitrión y los dispositivos de entrada, entre otros.

- Prohibir totalmente el navegador del dispositivo móvil, o restringir su uso a determinadas páginas.
- Forzar el tráfico de datos a través de pasarelas web seguras.
- Utilizar servidores proxy HTTP, u otros dispositivos intermedios para verificar las URL de destino antes de que sean accedidas.
- Usar un navegador aislado en un contenedor seguro para todos aquellos accesos web requeridos por la organización, dejando el navegador de serie del dispositivo para otros usos no corporativos.

### 3.8. INTERCONEXIÓN CON OTROS SISTEMAS

35. Es muy frecuente que los dispositivos móviles se interconecten con otros sistemas, a efectos de intercambio y almacenamiento de datos. Las interconexiones más usuales son aquellas que tienen lugar, a través de mecanismos inalámbricos o por cable, entre el dispositivo móvil y un ordenador de sobremesa o portátil, al objeto de sincronizar el contenido de ambos equipos.
36. Además de lo dicho, existe un riesgo añadido cuando un dispositivo móvil facilita el acceso de un tercer equipo a Internet<sup>26</sup>. Esta posibilidad debe ser contemplada por el organismo en cuestión y convenientemente recogida en su Normativa de Seguridad en el Uso de Dispositivos Móviles<sup>27</sup>.
37. Un caso frecuente de interconexión de sistemas se produce cuando un dispositivo móvil realiza salvaguardas de seguridad usando proveedores en la nube. Cuando esta provisión de servicios en la nube está controlada por el organismo en cuestión –por ejemplo, cuando se está utilizando una nube privada controlada, gestionada y auditada por el propio organismo- puede decirse que, en la mayoría de los casos, el riesgo es aceptable; cosa que no sucede cuando alguno de los elementos descritos no se encuentra bajo el control de la organización. Los siguientes son algunos ejemplos de riesgo:
  - Conexión de un dispositivo móvil de titularidad del usuario a un ordenador de titularidad de la organización.
  - Conexión de un dispositivo móvil de titularidad de la organización a un ordenador de titularidad privada del usuario.
  - Conexión de un dispositivo móvil de titularidad de la organización a un servicio de backup remoto, prestado por un tercero.
  - Conexión de cualquier dispositivo móvil a una estación de re-carga (de baterías) no confiable.
38. En los escenarios descritos existen los siguientes riesgos:
  - Almacenamiento de datos en ubicaciones no confiables y fuera del control de la organización.
  - Intercambio no autorizado de datos entre dispositivos.
  - Transmisión de infecciones con malware, de un dispositivo a otro.

<sup>26</sup> Este es el caso del *tethering*, que posibilita que un tercer equipo (un ordenador portátil o una tableta, generalmente) se conecte vía wi-fi al dispositivo móvil para, a su través, ganar acceso a Internet.

<sup>27</sup> Hemos denominado **Normativa de Seguridad en el Uso de Dispositivos Móviles** a aquella sección de la Política de Seguridad de la Información del organismo que contiene las precisiones oportunas en materia de uso y gestión de los dispositivos móviles en la organización.

39. Para mitigar los riesgos anteriores caben las siguientes medidas de seguridad:
1. Necesidad de adoptar los controles de seguridad adecuados en el dispositivo móvil suministrado por la organización, que determinen cuáles otros dispositivos concretos (ordenadores privados de titularidad del usuario, por ejemplo) pueden sincronizarse con él.
  2. Necesidad de adoptar los controles de seguridad adecuados en el dispositivo móvil propiedad del usuario, que determinen cuáles otros dispositivos concretos (ordenadores proporcionados por la organización, por ejemplo) pueden sincronizarse con él.
  3. Prevenir que los usuarios puedan acceder a servicios de backup remoto bloqueando tales servicios; impidiendo, por ejemplo, el acceso al dominio correspondiente.
  4. Configurar los dispositivos móviles para que no puedan usar servicios de backup remoto.
  5. Proporcionar formación a los usuarios de dispositivos móviles en el sentido de que eviten re-cargar sus dispositivos en fuentes de carga desconocidas.
  6. Habilitar mecanismos lógicos o físicos que impidan el intercambio de datos con otros dispositivos (bloqueando lógicamente, e incluso físicamente, el dispositivo en cuestión o sus interfaces).

### 3.9. USO DE CONTENIDOS NO-CONFIABLES

40. En algunos casos, los dispositivos móviles pueden tener acceso a contenidos potencialmente peligrosos, que no son accesibles mediante otro tipo de equipamientos. Tal es el caso, por ejemplo, de los códigos QR (Quick Response Codes). Los códigos bidireccionales QR suelen contener direcciones URL a las que los dispositivos móviles acceden a través de sus cámaras. Como se ha dicho<sup>28</sup>, es imposible detectar si la URL de destino da acceso a una página web maliciosa, por lo que este tipo de contenidos deben ser tratados como potencialmente peligrosos, adoptando las medidas de seguridad oportunas.
41. Entre tales medidas pueden mencionarse las siguientes:
1. Formar y concienciar a los usuarios de los riesgos inherentes al uso de contenidos no confiables, desalentando el acceso a tales contenidos cuando se estén desarrollando trabajos relacionados con el organismo en cuestión.
  2. Disponer de aplicaciones software específicas para la lectura de códigos QR, que permitan visualizar el contenido de destino (la URL, singularmente), dejando en manos del usuario proseguir con el acceso o cancelarlo.
  3. Utilizar pasarelas web seguras.
  4. Utilizar servidores proxy HTTP u otro dispositivo intermedio que permita validar las URL de destino antes de posibilitar el acceso.
  5. Si la categoría de seguridad del sistema de información así lo aconseja, siempre es posible restringir o deshabilitar el uso de elementos periféricos de los dispositivos, desconectando, por ejemplo, las cámaras, para evitar el procesamiento de códigos QR.

---

<sup>28</sup> Véase Informe de Ciberamenazas 2012 y Tendencias 2013, publicado por el Centro Criptológico Nacional.



### 3.10. EL USO DE SERVICIOS DE LOCALIZACIÓN

42. Los modernos dispositivos móviles, tales como los smartphones o las tabletas, disponen de capacidades de geo-localización (a través de sistemas GPS<sup>29</sup>), lo que da lugar a la existencia de los llamados “servicios de localización”. Estos servicios se han hecho muy populares y se usan con frecuencia en coordinación con otros, tales como: redes sociales, navegación, web browsers, etc.
43. Sin embargo, aquellos dispositivos móviles que mantienen activos los servicios de localización suponen un riesgo adicional, toda vez que posibilitan a los atacantes determinar la posición del usuario en función de la localización de su dispositivo móvil, lo que puede afectar gravemente no sólo a la seguridad de la organización sino también a las garantías de privacidad del propio usuario, facilitando la creación de mapas geográficos de los movimientos de los usuarios y, en algunos casos, el tipo de actividad que desarrollan<sup>30</sup>.
44. Entre las medidas de seguridad que cabe adoptar en estos casos están:
  1. Deshabilitar los servicios de localización de los dispositivos móviles.
  2. Prohibir el uso de servicios de localización en relación con determinadas aplicaciones (redes sociales, fotografías, etc.)
  3. Formar y concienciar a los usuarios para que deshabiliten los servicios de localización cuando se encuentren dentro de áreas sensibles<sup>31</sup>.
45. Por todo lo anterior, es muy recomendable que, de no ser necesario, se mantengan desactivados los servicios de localización de los dispositivos móviles. Esta exigencia, que en todo caso habrá de recogerse en la Normativa de Seguridad en el Uso de Dispositivos Móviles de la institución, podrá mantenerse siempre en los dispositivos móviles suministrados por el organismo. En aquellos otros en los que los titulares sean los propios usuarios, esta cautela sólo podrá exigirse dentro de las instalaciones del organismo.

---

<sup>29</sup> El **GPS** (*Global Positioning System*) es un [sistema global de navegación por satélite](#) que permite determinar en todo el mundo la [posición](#) de un objeto, una persona o un vehículo con una precisión hasta de centímetros (si se utiliza GPS diferencial), aunque lo habitual son unos pocos metros.

<sup>30</sup> Se han referenciado casos de atacantes que han logrado activar los servicios de localización de dispositivos móviles de sus víctimas, de tal forma que cuando el usuario tomaba una fotografía con su dispositivo se incluía a la imagen la referencia GPS de la localización, remitiéndose todo ello al atacante, y de manera absolutamente inadvertida para el usuario. Este tipo de comportamientos han podido facilitar la comisión de graves delitos, tales como secuestros de personas.

<sup>31</sup> En algún caso, sin embargo, esta cautela puede no evitar la localización del dispositivo, cuando se usa, por ejemplo, su conexión a internet, el rango de direcciones ip en el que se encuentra o la triangulación de antenas de telefonía móvil.

## 4. LA GESTIÓN DE LOS DISPOSITIVOS MÓVILES

46. A la vista de los riesgos derivados del uso de dispositivos móviles, los organismos están considerando la implantación de soluciones para gestionar centralizadamente tal equipamiento, tanto si se trata de dispositivos propiedad de los propios usuarios como si se trata de dispositivos cuyo titular es la propia organización. Mediante estas soluciones las instituciones pueden estar en mejores condiciones para gestionar tales equipamientos y propiciar un acceso más seguro a los recursos corporativos.

### 4.1. TIPOS DE GESTIÓN

47. En la actualidad, caben dos aproximaciones a la gestión de dispositivos móviles:
1. Gestionar los dispositivos móviles mediante el envío de mensajes SMS, que reconoce el software propietario de la marca instalado en el dispositivo o el sistema operativo de que se trate, o
  2. Usar un producto de terceros, capaz de gestionar centralizadamente más de una marca o sistema operativo<sup>32</sup>. Esta solución es la conocida habitualmente como Mobile Device Management (MDM)<sup>33</sup>.
48. Decantarse por una opción o por otra depende de la solución concreta de que se disponga en un instante dado. En general, las soluciones ofrecidas por una marca concreta suelen ser más robustas que las aportadas por terceras partes, aunque carecen de la versatilidad que estas últimas soluciones aportan<sup>34</sup>.

#### Mobile Device Management (MDM)<sup>35</sup>

Se trata de un software centralizado que permite la gestión, monitorización y securización de los dispositivos móviles desplegados en la organización que, en general, deberán tener instalado el correspondiente software-cliente. Mediante este sistema, las organizaciones pueden distribuir de forma remota aplicaciones a los dispositivos móviles y determinar las opciones de configuración y datos de cada uno de ellos. La posibilidad de gestionar diferentes tipos de dispositivos y marcas, facilita el uso de dispositivos propiedad de los usuarios (BYOD) como instrumentos de acceso a recursos corporativos.

La posibilidad de gestionar los controles de configuración de cada uno de los dispositivos sujetos al ámbito de aplicación de la solución MDM de que se trate, facilita igualmente la adopción de medidas de seguridad, reduciendo el riesgo inherente al uso de tales dispositivos.

Las soluciones MDM contemplan cuatro componentes: un servidor centralizado (que envía las órdenes de gestión a los dispositivos móviles), un software-cliente instalado en cada dispositivo móvil (que recibe y ejecuta tales órdenes), una base de datos centralizada (que contiene el estado de situación de cada uno de los dispositivos móviles del ámbito de la solución MDM)<sup>36</sup> y un modelo de comunicación entre el servidor centralizado y cada uno de los dispositivos móviles, denominado OTA (*Over-the-air programming*), capaz de configurar remotamente un dispositivo concreto, un conjunto determinado de

<sup>32</sup> Alguna de estas soluciones es capaz, asimismo, de gestionar ordenadores portátiles.

<sup>33</sup> Véase Guía CCN-STIC 455

<sup>34</sup> Se alienta a los organismos a realizar un estudio previo de los beneficios que pueden obtenerse optando por una u otra solución antes de implantar ninguna de ellas.

<sup>35</sup> Una solución completa de gestión de dispositivos móviles, que incluya todas las funciones posibles, abarca mucho más que la mera administración de dispositivos, a pesar de que éste sigue siendo el punto de partida para una solución extremo-a-extremo. Las otras capas que es preciso abordar son las aplicaciones que se ejecutan en los dispositivos, la gestión de las comunicaciones y redes usadas y los datos a los que se acceden, comparten o generan. El término que, recientemente, está siendo usado para denotar esta funcionalidad expandida es Enterprise Mobility Management (EMM).

<sup>36</sup> La Open Mobile Alliance (OMA) ha desarrollado un protocolo de gestión independiente de la plataforma denominado OMA Device Management, de libre acceso, con el propósito de constituir un estándar abierto (<http://technical.openmobilealliance.org/Technical/DM.aspx>)



ellos, o la totalidad del parque de dispositivos móviles de su ámbito de gestión, incluyendo actualizaciones de software y sistemas operativos, bloqueo y borrado remoto de los dispositivos, análisis remoto, etc.

En la actualidad, las soluciones MDM se ofrecen en base a la adquisición de licencias o mediante servicios cloud (*SaaS, Software as a Service*).

#### **Mobile Application Management (MAM)<sup>37</sup>**

Se trata de una solución similar a MDM, salvo que en este caso se dirige a gestionar una o varias aplicaciones específicas dentro de cada dispositivo móvil, en vez de gestionar la totalidad del dispositivo. El propósito de este mecanismo es permitir únicamente la gestión, actualización o borrado de las aplicaciones o los datos residentes en el dispositivo móvil de naturaleza corporativa, manteniendo inalterado el resto de las aplicaciones que pudiera contener el dispositivo.

Por ejemplo, una organización podría utilizar MAM para ofrecer servicios de correo electrónico seguro y calendario a un determinado dispositivo (o grupo de dispositivos), exigiendo una autenticación específica para el acceso a tales aplicaciones, y liberando al usuario de tales requisitos cuando accediera a la parte privada de su dispositivo móvil.

Esta solución es especialmente útil para la gestión de políticas de seguridad, cifrado selectivo de datos, borrado y bloqueo remotos, etc. Además, desde el punto de vista de la privacidad del usuario, esta solución posibilita que la organización no tenga visibilidad sobre el comportamiento del usuario más allá de las aplicaciones corporativas.

49. Desde el punto de vista técnico ambas soluciones son similares, estando soportadas en arquitectura cliente/servidor.
50. Así, el organismo dispondrá de uno o más servidores que proporcionen la capacidad de gestión centralizada, y una o más aplicaciones-cliente instaladas en cada dispositivo móvil y configuradas de tal forma que puedan estar permanentemente en ejecución. Puede solicitarse del vendedor que las aplicaciones-cliente se encuentren pre-instaladas en los dispositivos. En otros casos, el sistema operativo proporcionará las APIs precisas para recabar la información necesaria y la gestión de las políticas.
51. Si el equipo móvil es propiedad del organismo, la aplicación-cliente se encargará de gestionar la configuración y la seguridad del dispositivo en su conjunto. En otro caso, si el dispositivo móvil es propiedad del usuario (BYOD), la aplicación cliente gestionará únicamente la configuración y la seguridad de los datos corporativos, no del dispositivo entero. Por este motivo, la aplicación-cliente y los datos que maneja deberán ser aislados del resto de las aplicaciones del dispositivo y alojados en un contenedor seguro, con un doble propósito: proteger a la organización en caso de que el dispositivo se hubiere visto comprometido y proteger la privacidad del usuario del dispositivo.
52. En caso de que el organismo no use una solución de gestión centralizada de dispositivos o algunos de ellos no puedan beneficiarse de este tipo de soluciones, tal gestión deberá realizarse de manera manual y particularizada para cada uno de los dispositivos. Esta alternativa comporta los siguientes problemas:
  - Los controles de seguridad proporcionados individualmente a un dispositivo carecen generalmente de la robustez de aquellos otros proporcionados por la aplicación-cliente de un sistema de gestión centralizada de dispositivos. Este es el caso, por ejemplo, de dispositivos móviles que sólo manejan contraseñas cortas para autenticación de usuario

<sup>37</sup> Existe numerosa terminología en la industria para referenciar las diferentes necesidades y funcionalidades asociadas a la gestión de los dispositivos móviles y sus capacidades, adoptándose diferentes acrónimos. Consúltese Guía CCN-STIC 455.

y que no permiten el almacenamiento de datos con cifrado fuerte<sup>38</sup>, por lo que será necesario adquirir, instalar, configurar y mantener una multiplicidad de soluciones de terceros que sean capaces de proporcionar dichas funcionalidades.

- Puede no ser posible gestionar la seguridad de ciertos dispositivos cuando no se encuentran físicamente presentes dentro del organismo. Aunque es posible la instalación de software de gestión de los dispositivos de manera remota, esta solución requerirá un esfuerzo mayor aplicar manualmente las actualizaciones y ejecutar otras tareas de mantenimiento con dispositivos que no estén en las instalaciones del organismo.

53. Por todo ello, para evitar esta problemática, los organismos pueden decidir prohibir el uso de cualquier dispositivo móvil que no esté gestionado de manera centralizada, distinguiéndose entre dispositivos gestionados y dispositivos no-gestionados.

## 4.2. GRUPOS DE MEDIDAS DE SEGURIDAD

54. Se describen seguidamente los cuatro grupos de medidas de seguridad que deben tenerse en cuenta para la gestión de la seguridad de los dispositivos móviles, a saber:

- Grupo 1: Normas Generales de Seguridad para dispositivos móviles.
- Grupo 2: Almacenamiento y Comunicación de Datos.
- Grupo 3: Autenticación de Usuarios y Dispositivos.
- Grupo 4: Aplicaciones.
- Grupo 5: Protección de los servidores corporativos.

55. Las medidas comprendidas en cada uno de los grupos anteriores pueden ser proporcionadas por:

- El sistema operativo del dispositivo móvil.
- El software de gestión centralizada de dispositivos móviles (MDM) del organismo.
- Otros controles de seguridad.

56. Obviamente, según los casos, tales medidas resultarán de aplicación al dispositivo móvil en su conjunto o sólo al contenedor seguro que contenga las aplicaciones y datos corporativos.

57. Muchos de los organismos públicos no precisarán de la totalidad de las medidas descritas seguidamente. Su adopción dependerá del nivel de seguridad de la información tratada y los servicios prestados y, en su consecuencia, de la categoría del sistema de información de que se trate, conforme a lo dispuesto en los Anexos I y II del ENS. Como se ha dicho, el Anexo A de esta Guía incluye un Catálogo de Medidas de Seguridad del ENS que pueden usarse para la gestión de la seguridad de los dispositivos móviles.

### Grupo 1: Normas Generales de Seguridad para dispositivos móviles

58. La utilización de tecnología para la gestión centralizada de dispositivos móviles (MDM) puede facilitar al organismo la implantación de políticas y normas de seguridad aplicables a tales dispositivos<sup>39</sup>.

59. Algunas de tales normas pueden ser las siguientes:

<sup>38</sup> Sobre este particular, consúltese la Guía CCN-STIC 807 Criptología de empleo en el Esquema Nacional de Seguridad.

<sup>39</sup> Sin perjuicio de la aplicación de la Normativa General del organismo en cuestión. La Guía CCN-STIC 821 Normas de Seguridad en el ENS contiene un conjunto de modelos de normas que pueden ser usadas por los organismos como referencia.

- Limitar a los usuarios de dispositivos móviles y a las aplicaciones contenidas en ellos el acceso a determinado hardware, tal como las cámaras digitales, el GPS, el interfaz inalámbrico Bluetooth, los interfaces USB y las memorias removibles.
  - Limitar a los usuarios de dispositivos móviles y a las aplicaciones contenidas en ellos el acceso a servicios nativos del sistema operativo, tales como el navegador pre-instalado en el sistema operativo, el software-cliente de correo electrónico, el calendario, la lista de contactos, servicios de instalación de aplicaciones, etc.
  - Gestionar adecuadamente los interfaces inalámbricos de red (Wi-Fi, Bluetooth, etc.)
  - Monitorizar, detectar e informar automáticamente cuando una norma o política de seguridad haya sido violada, tal como los cambios en la configuración de seguridad aprobada previamente. La aplicación de esta política debería desencadenar acciones automáticas, siempre que ello fuera posible.
  - Limitar o prevenir el acceso a los servicios corporativos en base a la versión del sistema operativo del dispositivo móvil (incluyendo la posibilidad de detectar si tal dispositivo ha sido rooteado), en base a marca/modelo de dispositivo o a la versión software-cliente de gestión centralizada de dispositivos móviles.
60. El Anexo C de esta Guía contiene un Modelo de Normativa de Seguridad en el Uso de Dispositivos Móviles, que los organismos pueden usar como referencia.

## Grupo 2: Almacenamiento y Comunicación de Datos

- Cifrar de manera robusta las comunicaciones de datos entre el dispositivo móvil y el organismo. Aunque esto es frecuente cuando se usan redes privadas virtuales (VPN), pueden establecerse asimismo protocolos de cifrado específicos.
- Cifrar de manera robusta los datos almacenados tanto en la memoria interna del dispositivo móvil como en la memoria removible. Además de ello, los soportes removibles también pueden ser vinculados lógicamente a dispositivos concretos, de forma que la información cifrada y almacenada en ellos sólo pueda ser descifrada cuando el soporte esté conectado al dispositivo. Esta posibilidad limita el riesgo de ataques dirigidos ex profeso contra los soportes removibles.
- Borrar de manera segura, fiable y absoluta el contenido del dispositivo antes de permitir su reutilización por otro usuario o su retirada.
- Borrar de forma remota, segura, fiable y absoluta, el contenido del dispositivo si se ha perdido, ha sido sustraído o se sospecha que ha sido puesto en compromiso, incrementándose por tanto el riesgo de que terceras partes pudieran tener acceso a su contenido<sup>40</sup>.
- Configurar los dispositivos móviles para que procedan a su auto-borrado tras un cierto número de intentos fallidos de autenticación por parte del usuario.

---

<sup>40</sup> No obstante, conviene advertir que el borrado remoto no constituye un mecanismo de seguridad infalible, toda vez que un atacante siempre podría acceder al contenido del dispositivo antes de que éste fuera borrado o, incluso, podría desconectar el dispositivo para evitar recibir una señal externa de borrado. Por tanto, los organismos no deben adoptar el borrador remoto como la única medida de seguridad posible para proteger datos sensibles, sino que deben acomodar medidas adicionales, tales como las que se examinan en esta Guía.

**Grupo 3: Autenticación de Usuarios y Dispositivos.**

- Exigir una contraseña/pin del dispositivo y/u otro tipo de autenticación (por ejemplo, autenticación basada en tokens, autenticación basada en dispositivos de red, autenticación de dominios) antes de acceder a los recursos del organismo. Esta política incluiría decisiones sobre la fortaleza de la contraseña/pin y el número de intentos permitidos antes de que se deriven consecuencias negativas (tales como: bloqueo de la cuenta, borrado del dispositivo, etc.)
- En aquellos casos en que se produzca bloqueo de la cuenta debido al olvido de la contraseña/pin por parte del usuario, un administrador de seguridad debería poder re-activar la cuenta de forma remota y posibilitar el acceso al dispositivo (previo protocolo de identificación fidedigna del usuario).
- Los dispositivos deben bloquearse automáticamente después de un determinado periodo de inactividad (por ejemplo: dos minutos).
- Bajo la potestad del administrador de seguridad, podrá bloquearse de forma remota el dispositivo si se sospecha que ha podido ser dejado en un estado no seguro o en una ubicación no segura.

**Grupo 4: Aplicaciones**

- Limitar las aplicaciones que pueden usarse en el dispositivo móvil.
- Limitar las aplicaciones que pueden instalarse a través de listas blancas (opción deseable) o listas negras.
- Limitar los permisos (de acceso a las cámaras digitales o a los servicios de localización, por ejemplo) asignados a cada aplicación.
- Garantizar la seguridad de los mecanismos usados para la instalación, actualización y borrado de aplicaciones.
- Mantener de un inventario actualizado de todas las aplicaciones instaladas en cada dispositivo.
- Limitar el uso del sistema operativo y de los servicios de sincronización de aplicaciones (por ejemplo, sincronización con dispositivos locales o acceso a websites o servicios para sincronización remota).
- Verificar la firma electrónica de cada aplicación para asegurar que sólo aquellas aplicaciones provenientes de entidades de confianza pueden instalarse en el dispositivo.
- Distribuir las aplicaciones del organismo desde un lugar (ubicación propietaria) de aplicaciones específicamente dedicado a este propósito.

**Grupo 5: Protección de los servidores corporativos<sup>41</sup>**

- Puesto que el método de conexión principal de los dispositivos móviles a las redes corporativas se basa en tecnología Wi-Fi, es fundamental revisar y mejorar la infraestructura Wi-Fi de la organización para proporcionar comunicaciones seguras, disponer de mecanismos avanzados de control de acceso a la red (NAC, Network Access Control), de sistemas de detección/protección de intrusos inalámbricos (WIPS, Wireless Intrusion Protection System) y soluciones de filtrado de contenidos web (proxies).

---

<sup>41</sup> Guía CCN.STIC 455.

- Los mecanismos de control de la organización deben comenzar por el control de acceso a la red (mediante una combinación de soluciones NAC y MDM), definiendo quién tiene acceso a la misma (pudiendo hacer uso de mecanismos de gestión de identidad), monitorizando quién hace uso de ella, y bloqueando o permitiendo el acceso según la política de seguridad, en base a las credenciales del usuario y/o del dispositivo móvil, y del nivel de seguridad actual de este último.

## 5. EL DESPLIEGUE DE LA SEGURIDAD DE LOS DISPOSITIVOS MÓVILES EN LOS ORGANISMOS

61. La implantación de las medidas de seguridad para dispositivos móviles en el organismo debe desarrollarse en torno a una estrategia previamente definida, que ayude a las organizaciones a determinar cuando el despliegue de una determinada medida de seguridad puede ser importante para preservar los activos de información o los servicios del organismo. En los siguientes párrafos desarrollaremos una estrategia basada en la utilización de un modelo tradicional de implantación en cinco fases.
62. Las fases consideradas son las siguientes:

FASE	DENOMINACIÓN	CONTENIDO
1	<b>Iniciación</b>	<p>Esta fase comprende las tareas que el organismo debe acometer en el diseño una solución de seguridad para su parque de dispositivos móviles.</p> <p>Contempla la identificación de necesidades del organismo en relación con el uso de los dispositivos móviles (panorámica general sobre cómo la tecnología móvil puede colaborar en el cumplimiento o de las misiones encomendadas al organismo).</p> <p>Esta fase comprende también el desarrollo de una estrategia de alto nivel para implementar soluciones móviles, el desarrollo de una Normativa de Seguridad en el Uso de Dispositivos Móviles y especificar los requisitos funcionales y competenciales que requerirán las soluciones móviles que finalmente se implanten.</p>
2	<b>Desarrollo</b>	<p>Durante esta fase se especificarán las características técnicas de las soluciones móviles que se requieren, incluyendo los métodos de autenticación exigibles y, en su caso, los mecanismos criptográficos usados para proteger las comunicaciones y los datos almacenados en los dispositivos.</p> <p>Además, esta fase debe determinar el tipo de dispositivos móviles (marcas, modelos, sistemas operativos, etc.) que podrán autorizarse.</p> <p>La elección entre diferentes opciones determinará la implantación práctica de las oportunas medidas de seguridad, por lo que este análisis debe realizarse con sumo cuidado.</p> <p>Al final de esta fase deberían iniciarse las gestiones contractuales pertinentes para la adquisición de los productos.</p>
3	<b>Implantación</b>	<p>En esta fase, los sistemas de información del organismo involucrados en el despliegue de la tecnología móvil (servidores y equipos móviles) se configurarán para alcanzar los objetivos y los requisitos de seguridad fijados con anterioridad.</p> <p>Llegado ese punto, parece recomendable iniciar el despliegue usando un proyecto piloto antes de elevar la solución a definitiva.</p>

		La fase de implantación incluye la integración de los sistemas afectados con otros controles de seguridad y otras tecnologías, tales como la gestión de incidencias y los servidores de autenticación.
4	<b>Operación y Mantenimiento</b>	Esta fase comprende todas aquellas tareas que el organismo debe desarrollar de forma continuada, para garantizar que la solución se mantiene operativa en todo momento y conforme con los niveles de seguridad exigidos. Entre ellas se encuentra el parcheo de los sistemas operativos y aplicaciones, la revisión de logs y la detección de ataques.
5	<b>Retirada</b>	Esta fase comprende todas aquellas tareas que deben acometerse cuando una solución de tecnología móvil o cualquiera de sus componentes se retira del organismo, incluyendo los requisitos legales de conservación de datos, limpieza de soportes y medios y retirada efectiva de equipamientos.

63. Seguidamente, se desarrollan los aspectos esenciales de cada una de las fases enunciadas.

## 5.1. INICIACIÓN

64. Esta fase comprende distintas acciones preparatorias entre las que cabe destacar:

- Identificar las necesidades presentes y futuras del organismo, en relación con el uso de dispositivos móviles.
- Especificar los requisitos funcionales y de seguridad que se prevén.
- Desarrollo de la Normativa de Seguridad en el Uso de Dispositivos Móviles, conteniendo:
  - o Determinación de los recursos del organismo que podrán ser accedidos a través de dispositivos móviles.
  - o Tipos de dispositivos móviles permitidos para acceder a tales recursos.
  - o Nivel de acceso que poseerán por defecto las diferentes clases de dispositivos móviles (por ejemplo, los dispositivos móviles propiedad de los usuarios frente a los dispositivos móviles de titularidad del organismo).
  - o Modelo de distribución de los equipos.
  - o Modelo de gestión y administración centralizada de los dispositivos móviles.
  - o Mecanismos de actualización de políticas y tecnologías de seguridad aplicables.

65. Es muy importante que la Normativa de Seguridad en el Uso de Dispositivos Móviles del organismo esté documentada y permanentemente actualizada, formando parte coherente del conjunto de normas de seguridad que desarrollan la Política General de Seguridad de los Sistemas de Información del organismo (medida [org.2] del ENS).

### Cuestiones específicas relativas al modelo BYOD

66. En caso de que se plantee en el organismo la utilización del modelo BYOD, su implantación puede realizarse bajo tres perspectivas:



- **Virtualización:** Proporcionando acceso remoto a los sistemas de información corporativos, por lo que no habrá datos o ejecución de aplicaciones en el dispositivo personal<sup>42</sup>;
  - **Aislamiento:** Haciendo que los datos o las aplicaciones corporativas se encuentren dentro de un contenedor seguro (sandbox), aislado de los datos y aplicaciones personales de su propietario;
  - **Coexistencia controlada:** Permitiendo en el dispositivo la convivencia de datos y aplicaciones corporativas con datos personales, contemplando las políticas de seguridad adecuadas que garanticen que los controles de seguridad se mantienen en todo momento.
67. Las especiales circunstancias –y los importantes riesgos- que rodean el uso de dispositivos móviles cuando el organismo ha aceptado el modelo BYOD para el desempeño de sus funciones, requiere tener en cuenta las siguientes cuestiones adicionales:
1. **Normativa de Seguridad BYOD:** Antes de investigar sobre la idoneidad o no de adoptar una determinada solución MDM, es necesario redactar, aprobar, solicitar y obtener de los propietarios de los dispositivos móviles el consentimiento informado en relación con la **Normativa de Seguridad BYOD** del organismo (incluida en la Normativa de Seguridad en el Uso de Dispositivos Móviles del organismo) y, en su caso, las **Normas y Procedimientos de Seguridad** derivados.
  2. **Seguridad Jurídica:** Tal vez el mayor riesgo de BYOD es el peligro de revelación de información confidencial si el dispositivo se pierde o es robado. Por este motivo, la mayoría de las Políticas de Seguridad requieren el uso de contraseñas para el acceso, el bloqueo del dispositivo o el cifrado de información, así como el **derecho institucional a borrar remotamente los datos del dispositivo**, cuando se dan ciertas condiciones, incluyendo la finalización de la relación de trabajo del empleado público (o del colaborador, proveedor, subcontratista, etc.). Como se ha explicado, ciertas tecnologías permiten aislar los datos y aplicaciones corporativas del resto de contenidos del dispositivo, lo que posibilita eliminar de forma selectiva sólo lo que es necesario para el mantenimiento de las condiciones de seguridad institucionales. Si no se utilizan tales tecnologías, se eliminarían todos los datos del dispositivo móvil, incluyendo datos e informaciones personales del usuario, lo que podría provocar litigios, si no existiera una política de seguridad previa y claramente definida y formalmente aceptada.
  3. **Responsabilidades de los usuarios:** Los usuarios tienen que entender sus responsabilidades, entre ellas el mantenimiento permanente de las medidas de seguridad hardware y software exigibles en cada caso (por ejemplo, mantener los parches de seguridad permanentemente actualizados). La Normativa de Seguridad BYOD del Organismo podría advertir de la desactivación automática de aquellos dispositivos que no cumplan tales medidas.

---

<sup>42</sup> La aplicación-cliente ligera de escritorio virtual utiliza generalmente un pequeño *plugin* para el navegador, de libre acceso para casi todos los sistemas operativos, que transforma el dispositivo del usuario en un mero visor y controlador del escritorio virtual, siendo así que la ejecución de las aplicaciones se realiza en los sistemas centrales. Por tanto, como el dispositivo del usuario no contiene en ningún momento datos corporativos, esta modalidad de trabajo no presenta ninguno de los problemas legales y de política de seguridad de aquellas otras alternativas que sí permiten que los dispositivos personales almacenen información corporativa.



4. **Actividades permitidas:** La Normativa de Seguridad en el Uso de Dispositivos Móviles del organismo determinará lo que está permitido y lo que no lo está, en relación con el uso de dispositivos móviles. Las limitaciones más frecuentes contendrán normas contra la descarga de datos o documentos corporativos, el acceso a determinadas redes o aplicaciones, o el uso de determinadas características del dispositivo, tales como cámaras o puertos USB, la prohibición del *jailbreak* o *rootado* del dispositivo, y la determinación de listas blancas y listas negras de aplicaciones y sitios web<sup>43</sup>. Algunas herramientas MDM alertan a los usuarios de posibles no conformidades con la política de seguridad y son capaces de bloquear el acceso hasta que se tomen medidas adecuadas<sup>44</sup>.
5. **Dispositivos permitidos:** En determinados casos, puede ser conveniente que la Normativa de Seguridad BYOD limite los dispositivos móviles permitidos por el organismo, en aras a la reducción de gastos de soporte y a la eficiencia en la aplicación de controles de seguridad<sup>45</sup>.
6. **Servicios de soporte (Help/Desk):** La decisión más rigurosa pasaría por hacer responsables a los usuarios cuando el dispositivo no funcione adecuadamente. Sin embargo, esto podría ir contra el principio de productividad en el que se asienta BYOD. Por tanto, será necesario encontrar soluciones de compromiso en las que el organismo asuma el soporte respecto del uso institucional del dispositivo, dejando al usuario la gestión de la problemática particular. Esta solución, matizable en niveles, puede complementarse con la creación de foros de discusión y ayuda a los usuarios en las intranets corporativas.
7. **Asunción de costes:** Cuando el organismo en cuestión acepta el modelo BYOD, surge la pregunta de quién corre con los costes, tanto del propio dispositivo como los cargos por su uso. Parece lógico pensar que si la mayoría del tráfico de datos está relacionado con la actividad profesional, los usuarios confiarán que sea el organismo quién asuma los gastos corrientes. No obstante, para evitar situaciones no deseables, los organismos podrán establecer límites. En cualquier caso, los detalles del pago deberán explicitarse en la Normativa de Seguridad BYOD<sup>46</sup> del organismo.

---

<sup>43</sup> Algunos sitios web muy comunes, y cuyo acceso suele estar restringido, son los relativos a servicios de backup remoto (tales como Dropbox y iCloud). Además, los organismos podrán –atendiendo al preceptivo análisis de riesgos derivado de su casuística particular- restringir el acceso a las redes sociales. Naturalmente, limitar estas funcionalidades puede conducir a desanimar a los usuarios a usar su propio dispositivo para funciones profesionales fuera del horario profesional.

<sup>44</sup> Sin embargo, las soluciones MDM no siempre están en condiciones de hacer cumplir todas las restricciones señaladas en la política de seguridad (tales como el uso de la cámara del dispositivo o el acceso a la red), lo que hace que algunos de tales controles descansen en los suministradores de accesos wireless, capaces de controlar niveles de acceso basados en la identidad de los dispositivos.

<sup>45</sup> Los organismos podrían aplicar la política de seguridad por niveles, según el tipo de dispositivo. Por ejemplo, con equipos BlackBerry podrían accederse a las aplicaciones A, B y C; con iPhone y iPad a las aplicaciones C y D; y con Android a las aplicaciones C.

<sup>46</sup> Suelen manejarse tres opciones: 1. No reembolsar nada a los usuarios; 2. Reembolso de una parte de los gastos mensuales presentados por el operador de comunicaciones al usuario y 3. Asignación de complementos específicos por uso de dispositivo propio.

**Criterios para adoptar (o no) el modelo BYOD**

68. Se suele afirmar que permitir que los empleados públicos (y, en su caso, colaboradores, proveedores y subcontratistas) usen sus propios smartphones y tablets podría incrementar la satisfacción de los usuarios, mejorar la productividad y rebajar los costes del organismo, pero este modelo también tiene posibles inconvenientes. Seguidamente se incluyen diez cuestiones que conviene analizar con cuidado para determinar si el modelo BYOD es adecuado o no para una determinada organización.

1. **Resistencia de los usuarios a asumir costes:** Por regla general, los usuarios se resisten a correr con los gastos corrientes de sus propios smartphones o tablets cuando se usan para propósitos profesionales. La resistencia al pago se extiende tanto a la adquisición del dispositivo como a los posibles gastos mensuales relativos a su uso en redes de telecomunicaciones públicas o a los gastos de mantenimiento, reparación, etc. Esta circunstancia exigiría al organismo disponer de políticas de compensaciones que, en muchos casos, no será fácil acometer.
2. **Problemática reducción de costes:** Muchos Responsables de Sistemas están entendiendo que la adopción del modelo BYOD puede introducir a la organización en una espiral de costes. Sostienen esta afirmación alegando que: 1. Las organizaciones pierden la capacidad de reducir costes mediante la compra masiva de dispositivos móviles y 2. Pueden terminar pagando más de lo debido si se asumen determinados costes como reembolsables.
3. **Complejidad añadida para el Departamento de Sistemas de Información:** Permitir que los usuarios utilicen sus propios equipos añade complejidad a la gestión de los Departamentos de Sistemas de los organismos. Aunque la Normativa de Seguridad BYOD del organismo que se trate asigne a los usuarios la responsabilidad del soporte a sus propios equipos, esta situación puede no ser más que un espejismo, toda vez que los Help-Desk corporativos seguirán constituyendo el primer punto de contacto cuando algo no funcione adecuadamente. Además, la necesidad de adoptar nuevas medidas de seguridad para hacer frente al incremento de dispositivos móviles personales constituye un coste nada despreciable en el corto plazo. A este coste hay que añadir el derivado de la adquisición del nuevo software que será preciso implantar, tal como el requerido para: la protección de datos en los dispositivos móviles, el control de acceso a la red y la propia gestión de dispositivos móviles (soluciones del tipo MDM y/o MAM), y su instalación, implantación y mantenimiento.
4. **Discriminación profesional:** Permitir el modelo BYOD puede crear, involuntariamente, un entorno de trabajo desigual<sup>47</sup>. Si el personal tiene que incrementar su gasto para mantenerse al día con respecto a sus compañeros, esta situación puede afectar negativamente a la moral y, por ende, a la productividad<sup>48</sup>.

---

<sup>47</sup> Si, por ejemplo, un empleado público invirtiera una importante cantidad de dinero en adquirir un dispositivo de gama alta con el que pudiera desarrollar su trabajo más rápidamente, es más que probable que esta circunstancia conduzca a una situación incómoda con su propio entorno.

<sup>48</sup> Por el contrario, el uso de dispositivos propiedad del organismo evita el problema. Se trata del paradigma clásico del “uniforme escolar”.

5. **La asunción de responsabilidades:** Como se ha dicho antes, la seguridad es uno de los mayores problemas con el que debe enfrentarse el modelo BYOD toda vez que permitir el uso de dispositivos de titularidad privada en las redes corporativas conlleva riesgos significativos, si tal despliegue no se gestiona correctamente. Estos riesgos son tan elevados que su uso suele estar terminantemente prohibido cuando se trata de posibilitar el acceso o tratamiento de información sensible, tanto de naturaleza personal como comercial. Puesto que los Departamentos de Sistemas de los organismos tendrán sobre los dispositivos BYOD menos control que si se tratara de dispositivos proporcionados por la propia organización, gran parte de la responsabilidad de la adopción de las medidas de seguridad recaerá en los propios usuarios. Para el usuario individual esto puede suponer un grave inconveniente, que será visto como una carga profesional añadida.
6. **Pérdida de datos:** De manera análoga a lo que sucede con los sistemas de información corporativos, también existe el riesgo de que se destruyan datos sensibles que previamente se han cargado en los dispositivos móviles propiedad de los usuarios. Aunque las modernas soluciones MDM-MAM pueden reducir este riesgo, los usuarios pueden ser reacios a permitir el acceso a sus dispositivos de tal tipo de software. Como hemos visto, el Responsable de Seguridad y el Responsable del Sistema tienen la responsabilidad de la protección de los datos corporativos (haciendo una limpieza remota cuando alguien cesa en sus funciones), sin correr el riesgo de poner en peligro los datos personales del individuo.
7. **Novedad vs. eficacia:** Una de las características más atractivas de BYOD es la posibilidad que tiene el usuario de utilizar dentro de la organización la tecnología más novedosa (o más espectacular) en cada momento, ventaja que es aún mayor si la política BYOD corporativa comporta subvenciones económicas para la compra de dispositivos. No obstante, pasados los primeros momentos de euforia, la realidad del día a día puede ser diferente, sobre todo si los equipos no funcionan como era de esperar y los usuarios han de asumir las consecuencias de una inapropiada elección.
8. **El problema de las licencias:** El modelo BYOD exige mantener una permanente vigilancia sobre las licencias del software que se instale en cada uno de los dispositivos, lo que puede acarrear importantes costes. Además, atendiendo a las condiciones impuestas en determinadas licencias, el software en cuestión sólo podrá instalarse en dispositivos propiedad del organismo, lo que constituye una complicación añadida<sup>49</sup>. Pueden presentarse, asimismo, otras cuestiones de naturaleza jurídica que es necesario contemplar y tratar adecuadamente<sup>50</sup>.
9. **La productividad, en tela de juicio:** Conviene valorar el riesgo que existe para la productividad si se anima a los empleados públicos a utilizar sus propios dispositivos,

---

<sup>49</sup> No obstante, la virtualización de escritorios puede ayudar a paliar esta problemática.

<sup>50</sup> Por ejemplo: ¿Quién asumirá la responsabilidad de una descarga ilegal realizada en un dispositivo que se utiliza tanto para funciones profesionales como de ocio?

en general, más adecuados para el ocio (visionado de videos, juegos, acceso a redes sociales, etc.) que para el trabajo.

10. **No todo el mundo es un apasionado de la tecnología:** Se tiende a olvidar que no todas las personas (todos los usuarios, en nuestro caso) son apasionadas de la tecnología. Estos usuarios no se mostrarán nunca especialmente proclives al BYOD.
69. El Anexo B contiene una relación de aquellos elementos más significativos que deben considerarse para determinar si un programa BYOD es o no adecuado para un organismo público concreto, independientemente de las medidas de seguridad específicas que se mencionan en el apartado 6 de la presente Guía.

### Limitaciones al uso de dispositivos móviles en función de los niveles de acceso

70. Como regla general, la Normativa de Seguridad en el Uso de Dispositivos Móviles del organismo, atendiendo a razones de seguridad, limitará los tipos de dispositivos que pueden ser usados para acceder a los recursos del organismo.
71. Tales limitaciones pueden establecerse en base a Niveles de Acceso, de la forma:

<b>Nivel de Acceso Máximo:</b>	Posible política: Sólo los dispositivos móviles proporcionados y gestionados por el organismo podrán tener acceso a los recursos corporativos.
<b>Nivel de Acceso Intermedio:</b>	Posible política: Los dispositivos móviles propiedad de los usuarios (BYOD) que se encuentren comprendidos dentro del ámbito de gestión centralizada de dispositivos móviles del organismo (y que, en su consecuencia, estén ejecutando el software-cliente correspondiente), podrán acceder a un conjunto pre-definido de recursos corporativos.
<b>Nivel de Acceso Mínimo:</b>	Posible política: Los dispositivos móviles propiedad de los usuarios (BYOD) que no se encuentren comprendidos dentro del ámbito de gestión centralizada de dispositivos móviles del organismo sólo podrán acceder a unos pocos recursos corporativos, tales como el correo electrónico, por ejemplo; o no podrán usarse en el organismo.

72. Esta estratificación en niveles permite a los organismos limitar el riesgo, toda vez que los dispositivos no gestionados por la organización dispondrán únicamente de los privilegios mínimos<sup>51</sup>.
73. Los Niveles de Acceso que cada organismo decida adoptar vendrán determinados por el correspondiente análisis de riesgos<sup>52</sup>. En tal sentido, y a título de ejemplo, el cuadro siguiente enumera aquellos factores que los organismos podrían considerar a la hora de desarrollar su Normativa de Seguridad en el Uso de Dispositivos Móviles.

<b>Sensibilidad de la información manejada</b>	En ocasiones, determinadas actividades comportan el acceso a información sensible. En su consecuencia, deberán elevarse los
--	---

<sup>51</sup> El apartado 6 de la presente Guía contiene una formulación de permisos en función de los niveles de seguridad del ENS.

<sup>52</sup> El desarrollo de tal análisis de riesgos, facilitado por metodologías y herramientas tales como MEGERIT y PILAR, respectivamente, debería poder realizarse de forma individual para cada tipo de dispositivo móvil considerado, si ello es posible y está justificado.

	requisitos de seguridad exigidos para el tratamiento de este tipo de información. Un ejemplo de ello sería la exigencia de que los usuarios solamente pudieran usar dispositivos suministrados por el organismo y/o limitar su uso remoto fuera del perímetro de seguridad de la organización.
<b>Cumplimiento de la Normativa de Seguridad en el Uso de Dispositivos Móviles</b>	La mayor parte de los requisitos de seguridad del organismo sólo podrán alcanzarse cuando la organización tenga acceso a los controles de configuración de cada uno de los dispositivos. Por tanto, cuando un dispositivo no se encuentre dentro del ámbito de gestión centralizada de seguridad, será necesario que el servidor de la organización desarrolle algunas acciones preventivas cuando tal dispositivo pretenda acceder a recursos corporativos. Para evitar esta problemática, los organismos pueden decidir incorporar a su Normativa de Seguridad en el Uso de Dispositivos Móviles la exigencia de que todos los dispositivos móviles ejecuten el software-cliente de gestión de seguridad proporcionado por la organización.
<b>Coste</b>	Obviamente, los costes asociados al mantenimiento de la seguridad de los dispositivos móviles dependerán de las decisiones adoptadas en la Normativa de Seguridad en el Uso de Dispositivos Móviles del organismo, distinguiendo entre costes directos (los correspondientes a cada uno de los dispositivos y al software-cliente instalado en ellos) y costes indirectos (los derivados del mantenimiento de la seguridad en los dispositivos móviles y la provisión del adecuado soporte técnico de seguridad para los usuarios.)
<b>Ubicación de trabajo</b>	En general, los riesgos de seguridad serán menores en aquellos dispositivos que se usen exclusivamente dentro del perímetro de seguridad del organismo, frente a aquellos otros que también puedan usarse en el exterior.
<b>Limitaciones técnicas</b>	Cuando es preciso ejecutar una concreta aplicación puede ser necesario usar determinado tipo de dispositivo móvil o sistema operativo. Este sería el caso, por ejemplo, que obligaría a usar un determinado tipo de dispositivo móvil o, más frecuentemente, un sistema operativo concreto (o una versión de tal sistema operativo), capaz de ejecutar el software cliente de gestión de seguridad de dispositivos móviles del organismo.
<b>Conformidad con la normativa vigente y otras regulaciones de seguridad</b>	Además de todo lo anterior, los organismos deberán asegurar que el uso de los dispositivos móviles en el seno de las competencias estatutarias que les corresponden se desarrolla en todo momento de conformidad con la legislación vigente: Esquema Nacional de Seguridad, pero también la legislación sobre Protección de Datos de Carácter Personal, Administración Electrónica, Firma Electrónica y cualquier otra que resulte de aplicación.

74. La aplicabilidad de cada uno de los factores anteriores vendrá determinada por la categoría de seguridad del sistema de información de que se trate. Así, aquellos organismos que, tras el pertinente análisis de riesgos, entiendan que el tratamiento de determinados datos comporta un riesgo singular, es probable que sólo admitan que el trabajo se desarrolle a través de dispositivos móviles debidamente securizados y suministrados por la propia organización, exigiendo una autenticación robusta antes de permitir que el dispositivo acceda a los recursos corporativos sensibles.
75. Como las medidas de seguridad también pueden implantarse en los servidores, otro posible control de seguridad sería migrar los recursos de alto riesgo a servidores específicos,

- expresamente securizados, que deberán asumir la responsabilidad de la adecuada protección de los datos tratados<sup>53</sup>.
76. Finalmente, en los casos más sensibles o de mayor riesgo, los organismos podrán decidir prohibir de manera absoluta de acceso a determinados tipos de información a través de dispositivos móviles de cualquier tipo<sup>54</sup>.
77. En todo caso, a la vista de la evolución tecnológica, del incremento de las capacidades de los dispositivos móviles, de la efectividad de los controles de seguridad adoptados y de los diferentes tipos de amenazas para cada dispositivo o sistema operativo, los organismos deberán, periódicamente, acomodar su Normativa de Seguridad en el Uso de Dispositivos Móviles a estas nuevas realidades, re-considerando la tipología de dispositivos aceptados por la organización, los niveles de acceso requeridos en cada caso y, en su consecuencia, la disposición de las adecuadas medidas de seguridad.
78. Obviamente, la evolución tecnológica afectará también a los sistemas centralizados de gestión de dispositivos móviles (MDM), que los organismos deberán re-evaluar permanentemente.

### Formación y concienciación de los usuarios

79. De forma análoga a lo que sucede con el equipamiento tradicional, los organismos deberán concienciar y formar a los usuarios respecto de la importancia de las medidas de seguridad adicionales deben adoptarse, así como de las responsabilidades de los usuarios respecto de la adopción de tales medidas y su mantenimiento.
80. El Anexo C de esta Guía contiene un Modelo de Normativa de Seguridad en el Uso de Dispositivos Móviles que los organismos pueden usar como referencia.
81. Una de tales medidas sería limitar (o prohibir, en los casos más rigurosos) la constitución de redes inalámbricas personales (WPAN), tales como aquéllas que pueden construirse usando teclados o ratones inalámbricos, conectando los dispositivos o las impresoras de forma inalámbrica, sincronizando dispositivos de forma inalámbrica, o usando auriculares con micrófonos inalámbricos. Las tecnologías de base que suelen usarse para la construcción de estas redes incluyen Wi-Fi, Bluetooth y Near-Field Communications (NFC).

## 5.2. DESARROLLO

82. Cuando el organismo ha redactado y aprobado su Normativa de Seguridad en el Uso de Dispositivos Móviles, ha identificado las necesidades operativas de tales dispositivos y ha completado las actividades señaladas en el punto anterior, el siguiente paso es determinar qué tipo de tecnologías de gestión de dispositivos móviles pueden usarse en el contexto de la organización, diseñando una solución para su despliegue.
83. Se trata, por tanto, de adoptar decisiones sobre consideraciones de seguridad de naturaleza eminentemente técnica. Entre las más importantes pueden citarse las señaladas en el cuadro siguiente.

<b>Consideraciones de Seguridad de naturaleza Técnica</b>
---

<sup>53</sup> Esto es así, por ejemplo, cuando la información sensible solamente está alojada en los servidores corporativos, no permitiéndose su almacenamiento en los dispositivos móviles.

<sup>54</sup> Como hemos dicho, sea cual fuere la decisión adoptada, deberá figurar en el documento de Política de Seguridad Móvil del organismo.



<b>Arquitectura:</b>	Que debe incluir: <ul style="list-style-type: none"> <li>- Diseño de la arquitectura del servidor de gestión de dispositivos móviles, especialmente a la hora de establecer conexiones con los usuarios remotos (DMZ, DLP, registro de auditoría, etc.), primando aquellas arquitecturas que otorguen control completo al organismo.</li> <li>- Diseño de la arquitectura del software-cliente a instalar en tales dispositivos.</li> <li>- Determinación de la ubicación del servidor de gestión de dispositivos móviles y del resto de los elementos centralizados.</li> <li>- Diseño de la arquitectura de las soluciones de red privada virtual (VPN) que se precisen.</li> </ul>
<b>Autenticación:</b>	Selección de los métodos de autenticación de los usuarios y/o dispositivos, incluyendo los procedimientos de asignación y eliminación de autenticaciones, que, en su caso, deberá contemplar su integración con los sistemas de autenticación corporativos. Presencia de un servidor de autenticación en el lado servidor, en el que la suspensión y revocación de derechos y privilegios sea instantánea.
<b>Criptografía:</b>	Selección de los algoritmos de cifrado y protección de la integridad de las comunicaciones de los dispositivos móviles, así como determinación de la fortaleza y longitud de las claves criptográficas <sup>55</sup> .
<b>Requerimientos de configuración:</b>	Determinación de los estándares de seguridad mínimos para los dispositivos móviles.
<b>Aprovisionamiento de dispositivos:</b>	Determinación de los métodos que se emplearán para cargar en los dispositivos móviles desplegados (tanto nuevos como viejos) el software-cliente, los autenticadores, opciones de configuración etc.
<b>Requerimientos de certificación de aplicaciones:</b>	Determinación de los requisitos de seguridad y funcionalidad que las aplicaciones deben poseer, señalando los indicadores de cumplimiento que se usarán.

84. Los aspectos de seguridad del diseño de la solución para dispositivos móviles deberán estar documentados en la planificación de la Seguridad Móvil del organismo.
85. Análogamente, el organismo deberá determinar cómo deberán tratarse de los incidentes de seguridad que involucren a dispositivos móviles, su gestión y documentación.

### 5.3. IMPLANTACIÓN

86. Como hemos dicho, antes de desplegar definitivamente una solución en el organismo, conviene implantar previamente un proyecto piloto, contemplando la problemática más significativa analizada en la fase de Iniciación.
87. La evaluación del proyecto piloto comprenderá el análisis de, entre otros, los siguientes extremos:

Elementos a analizar en la implantación del Proyecto-Piloto	
<b>Conectividad</b>	Establecimiento y mantenimiento por parte de los usuarios de conexiones al organismo desde aquellas ubicaciones que se espera

<sup>55</sup> Véase Guía CCN-STIC 807 Criptología de empleo en el Esquema Nacional de Seguridad.

	<p>sean usados.</p> <p>Dependiendo de los privilegios de acceso, los usuarios podrán acceder a la totalidad de los recursos corporativos o solamente a cierto número de ellos.</p>
<b>Protección</b>	Garantía de que la información almacenada en el dispositivo móvil y las comunicaciones entre tal dispositivo y el organismo están protegidas debidamente, de acuerdo con lo señalado en la Normativa de Seguridad en el Uso de Dispositivos Móviles del organismo.
<b>Autenticación</b>	Garantía de que no es posible circunvalar la autenticación de usuario/dispositivo, cuando se trata de una exigencia determinada por el nivel de acceso que se posea. Este aspecto requerirá la evaluación de las políticas de autenticación de dispositivos, usuarios y dominios.
<b>Aplicaciones</b>	Garantía de que las aplicaciones que habrán de ser ejecutadas en los dispositivos móviles funcionan adecuadamente. Este aspecto requerirá la evaluación de las restricciones o limitaciones para la instalación de aplicaciones, de manera especial las limitaciones para desinstalar el software-cliente de gestión de dispositivos móviles del organismo.
<b>Gestión</b>	Garantía de que los administradores del sistema (y los administradores de seguridad) pueden configurar y gestionar todos los componentes de la solución de manera efectiva y segura. Habrá de tenerse especialmente en cuenta la facilidad para el despliegue y la configuración de la solución, así como la imposibilidad o dificultad de los usuarios para modificar la configuración del software-cliente o del dispositivo.
<b>Logging</b>	Garantía de que la solución que finalmente se adopte mantiene un log de eventos de seguridad, de acuerdo con la Normativa de Seguridad en el Uso de Dispositivos Móviles del organismo.
<b>Rendimiento</b>	Garantía de que todos los componentes de la solución que finalmente se adopte mantienen un rendimiento adecuado durante un uso normal.
<b>Seguridad de la implantación</b>	Como quiera que la solución adoptada pueda contener vulnerabilidades que podrían ser explotadas por eventuales atacantes, aquellos organismos que posean sistemas de información categorizados con los niveles Medio y Alto deberán realizar una valoración amplia de las vulnerabilidades de la solución que se pretende adoptar. En todo caso, como requerimiento mínimo, todos los componentes de la solución deberán estar actualizados con los últimos parches disponibles, y configurados siguiendo lo dispuesto en la Normativa de Seguridad en el Uso de Dispositivos Móviles del organismo. El organismo, además, deberá adoptar las medidas necesarias para prevenir que un usuario pueda circunvalar las características de seguridad de los dispositivos móviles, incluyendo la detección automática de incumplimientos, cuando ello sea posible, y la prohibición del uso de dispositivos <i>rooteados</i> .
<b>Configuración predeterminada</b>	Garantía de que los valores de configuración por defecto de los dispositivos móviles y/o su modificación son necesarios para soportar los requisitos de seguridad definidos en la Normativa de Seguridad en el Uso de Dispositivos Móviles del organismo.

88. Como es lógico, el organismo debe securizar cada dispositivo móvil que entregue a los usuarios antes de permitir el acceso a los recursos corporativos. Esta cautela debe aplicarse igualmente para aquellos dispositivos móviles que ya hubieren sido desplegados por la organización. Además, dependiendo de los riesgos, podrán incorporarse al dispositivo



determinados controles de seguridad adicionales, tales como software antivirus y tecnologías de prevención de pérdida de datos (Data Loss Prevention, DLP).

#### 5.4. OPERACIÓN Y MANTENIMIENTO

89. El cuadro siguiente enumera los procedimientos operativos más usuales que, de forma periódica, deben ser llevados a cabo por el organismo de que se trate, al objeto de mantener la seguridad de la infraestructura móvil desplegada en la organización.

Procedimientos Operativos y de Mantenimiento más usuales	
<b>P1</b>	Verificación del estado de actualización y parcheado de los componentes de la solución para dispositivos móviles desplegada en el organismo, (contemplando mecanismos de adquisición, pruebas y despliegue de las actualizaciones), incluyendo los componentes de la infraestructura, los sistemas operativos de los dispositivos móviles y las aplicaciones contenidas en ellos.
<b>P2</b>	Verificación de que cada componente de la infraestructura de dispositivos móviles desplegada en el organismo (servidores de gestión de dispositivos móviles, servidores de autenticación, etc.) está adecuadamente sincronizada usando una fuente de tiempo común confiable, que posibilite detectar sellos de tiempo generados por otros sistemas.
<b>P3</b>	Configurar las características de control de accesos en función de las necesidades competenciales del usuario/dispositivo y sustentadas en factores tales como cambios en la política de seguridad, cambios tecnológicos, resultados de auditorías y nuevas necesidades de seguridad.
<b>P4</b>	Monitorizar de manera constante la infraestructura de dispositivos móviles del organismo, de manera que permita detectar y documentar incidentes y anomalías, incluyendo cambios de configuración no autorizados en los dispositivos móviles <sup>56</sup> . Los incidentes de seguridad deben reportarse al sistema de Gestión de Incidentes de seguridad de los sistemas de información del organismo.
<b>P5</b>	Mantener un inventario actualizado de los dispositivos móviles desplegados en el organismo, incluyendo: su(s) usuario(s), las aplicaciones que contienen y los recursos corporativos a los que les está permitido acceder.
<b>P6</b>	Proporcionar formación a los usuarios de dispositivos móviles del organismo en relación con las amenazas de seguridad, incluyendo actividades de concienciación y la adopción de buenas prácticas.
<b>P7</b>	Revocar el acceso (o proceder al borrado) de aquellas aplicaciones, que habiendo sido ya instaladas en los dispositivos móviles, fueran evaluadas como de alto riesgo.
<b>P8</b>	Borrado seguro de todos los datos contenidos en los dispositivos móviles antes de permitir su reutilización por otros usuarios.
<b>P9</b>	Verificación periódica de cara a confirmar que las políticas de seguridad de dispositivos móviles del organismo, su normativa de desarrollo y sus procedimientos asociados están siendo seguidas adecuadamente por todos los usuarios. Tal verificación puede desarrollarse usando medios pasivos (revisión de logs, por ejemplo) o medios activos (tales como pruebas de penetración –IPS- y de explotación de vulnerabilidades, etc.)

<sup>56</sup> Frecuentemente, tales anomalías pueden indicar actividad maliciosa o desviaciones de la política de seguridad, su normativa de desarrollo o los procedimientos asociados.

## 5.5. RETIRADA

90. Como se ha insistido, antes de que un componente de la infraestructura móvil desplegada en el organismo sea retirado permanentemente o reasignado a otro usuario<sup>57</sup>, la organización debe eliminar de manera segura y permanente cualquier dato o información sensible que todavía pudiera residir en los dispositivos móviles o, en general, en cualquier componente de la infraestructura desplegada.
91. Estas acciones de borrado seguro (como las que se realizan con los discos de estado sólido o las tarjetas de memoria, por ejemplo) comportan, en ocasiones, cierta dificultad, debido especialmente a la persistencia de datos de las memorias flash, lo que exige la utilización de procedimientos de borrado específicos para tal tipo de dispositivos.

---

<sup>57</sup> Esto afecta tanto a los propios dispositivos móviles de los usuarios como a los servidores en los que se encuentre alojado el software de gestión centralizada de dispositivos móviles.

## 6. EL USO DE LOS DISPOSITIVOS MÓVILES EN LOS ORGANISMOS PÚBLICOS EN FUNCIÓN DE LOS NIVELES DE SEGURIDAD DEL ENS

92. Como se ha dicho, una de las primeras cuestiones que debe determinar el organismo público que ha decidido incorporar a su infraestructura tecnológica el uso de dispositivos móviles, es la modalidad con la que va a desarrollarse tal actividad, esencialmente: si se trata de facilitar el uso de dispositivos móviles propiedad de la propia organización, o va a permitirse el uso de dispositivos propiedad de los usuarios (BYOD).
93. La selección de la modalidad vendrá condicionada por la categorización de la información gestionada por el Sistema, en los diferentes parámetros que resulten de aplicación (confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad), siendo los requisitos mínimos los dispuestos en la siguiente tabla:

Modelos de uso de los dispositivos móviles	BAJO	MEDIO	ALTO
Se permite el uso de dispositivos móviles propiedad del organismo.	X		
Se permite el uso de dispositivos móviles propiedad del organismo sólo si están gestionados a través de soluciones MDM.	X	X	X
Se permite el uso de dispositivos móviles propiedad del usuario (BYOD)	Totalmente prohibido		
Se permite el uso de dispositivos móviles propiedad del usuario (BYOD) cuando se correspondan con modelos previamente “homologados” o “aceptados” por el organismo.	X		
Se permite el uso de dispositivos móviles propiedad del usuario (BYOD) cuando se correspondan con modelos previamente “homologados” por el organismo, sólo si están gestionados a través de soluciones MDM.	X	X	X
<b>Servicios de terceros en la nube (salvaguardas, soluciones MDM, etc.)</b>			
Se estará a lo dispuesto en la Guía CCN-STIC 823 Seguridad en Entornos Cloud			

94. En virtud de lo contenido en la presente Guía, lo señalado en la tabla anterior, y en base a lo dispuesto en el Anexo II del ENS, se incluye seguidamente una tabla de medidas de seguridad de aplicación a los dispositivos móviles desplegados en los organismos de las AA.PP. españolas y que puedan contener información corporativa o acceder a recursos corporativos o de otros organismos públicos.

Medida	BAJO	MEDIO	ALTO
Configuración del dispositivo			
Se permite el uso de dispositivos móviles <i>rooteados</i> o con <i>jailbreak</i>	En ningún caso		
Software de protección contra código dañino en el dispositivo móvil.	X	X	X
Auto-bloqueo del dispositivo tras cierto tiempo de inactividad.	N/A	X	X
Auto-borrado en caso de vario intentos fallidos de autenticación del usuario.	N/A	X	X
Autenticación del dispositivo/usuario			
Sólo los usuarios (o perfiles de usuarios) autorizados por el organismo podrán usar dispositivos móviles	X	X	X
Utilización de PIN/contraseña para acceder al dispositivo	X	X	X
Utilización de contraseña para acceder a los recursos corporativos	X		
Autenticación basada en certificados digitales instalados en el dispositivo	X	X	
Autenticación basada en tokens externos (certificados digitales externos, por ejemplo)	X	X	X
Almacenamiento			
Se permite el almacenamiento en el dispositivo de información corporativa sin cifrar	X		
Se permite el almacenamiento en el dispositivo de información corporativa, sólo si está cifrada (de acuerdo a los algoritmos y niveles de seguridad definidos en la Guía CCN-STIC 807)	X	X	X
Borrado de la información			
Borrado simple, en caso de reutilización del dispositivo.	X		
Borrado seguro, en caso de reutilización del dispositivo.	X	X	X
Posibilidad de borrado remoto del dispositivo en caso de pérdida, compromiso, etc.	N/A	X	X
Aplicaciones			
Se permite la descarga o el uso de cualquier aplicación, sin ninguna restricción.	Totalmente prohibido		
Se permite la descarga sólo de aquellas aplicaciones	X		

previamente aceptadas por el organismo (de fuentes aceptadas).			
Se permite el uso de determinadas aplicaciones del usuario en el dispositivo móvil, previamente aceptadas u “homologadas” por el organismo y/o con las limitaciones dictadas por el organismo.	X	X	X
<b>Comunicaciones</b>			
Se permiten las comunicaciones del dispositivo móvil con los sistemas corporativos, sin ninguna restricción.	X		
Las comunicaciones del dispositivo móvil con los sistemas corporativos deberá realizarse de manera cifrada (con los algoritmos y niveles de seguridad definidos en la Guía CCN-STIC 807)	X	X	X
<b>Interfaces</b>			
Se permite el uso del interfaz inalámbrico WiFi en el dispositivo, sin restricciones.	X		
Se permite el uso del interfaz inalámbrico WiFi en el dispositivo, con las restricciones impuestas por el organismo.	X	X	X
Se permite el uso del interfaz inalámbrico Bluetooth en el dispositivo, sin restricciones.	X		
Se permite el uso del interfaz inalámbrico Bluetooth en el dispositivo, con las restricciones impuestas por el organismo.	X	X	X
Se permite el uso del interfaz USB del dispositivo, sin restricciones.	X		
Se permite el uso del interfaz USB del dispositivo, con las restricciones impuestas por el organismo.	X	X	X
Se permite el uso de la cámara del dispositivo, sin restricciones.	X		
Se permite el uso de la cámara del dispositivo, con las restricciones impuestas por el organismo.	X	X	X
Se permite el uso de los servicios de localización del dispositivo, sin ninguna restricción.	X		
Se permite el uso de los servicios de localización del dispositivo, con las restricciones impuestas por el organismo.	X	X	X
<b>Formación y concienciación</b>			
Formación y concienciación a los usuarios de dispositivos móviles	X	X	X



## ANEXO A: LA APLICACIÓN DE LAS MEDIDAS DE SEGURIDAD DEL ENS.

El cuadro siguiente muestra aquellas medidas de seguridad del Anexo II del ENS especialmente relevantes en el despliegue de dispositivos móviles en los organismos públicos<sup>58</sup>.

Medida	Denominación	Aplicación a la gestión de Dispositivos Móviles
<b>org</b>	<b>Marco organizativo</b>	
org.1	Política de seguridad	Necesidad de disponer de la Normativa de Seguridad en el Uso de Dispositivos Móviles del organismo, que se incluirá en la Normativa de Seguridad derivada de la Política de Seguridad de los Sistemas de Información del organismo <sup>59</sup> .
org.2	Normativa de seguridad	Necesidad de disponer de la Normativa de Seguridad <sup>60</sup> que resulte de aplicación al uso de dispositivos móviles, contemplando: <ul style="list-style-type: none"> <li>a) El uso correcto de equipos, aplicaciones, servicios e instalaciones.</li> <li>b) Lo que se considerará uso indebido.</li> <li>c) La responsabilidad del personal con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas disciplinarias, de acuerdo con la legislación vigente.</li> </ul>
org.3	Procedimientos de seguridad	Necesidad de disponer de Procedimientos de Seguridad que resulten de aplicación al uso de dispositivos móviles, contemplando: <ul style="list-style-type: none"> <li>a) Cómo llevar a cabo las tareas habituales.</li> <li>b) Quién debe hacer cada tarea.</li> <li>c) Cómo identificar y reportar comportamientos anómalos.</li> </ul>
org.4	Proceso de autorización	Existencia de procesos formales, especialmente para: <ul style="list-style-type: none"> <li>a) Utilización de instalaciones habituales y alternativas (para los sistemas de gestión centralizados de dispositivos móviles, por ejemplo).</li> <li>b) Utilización de dispositivos móviles en el organismo (ya sean de titularidad del organismo, como del</li> </ul>

<sup>58</sup> Se trata, como decimos, de una lista que no pretende ser exhaustiva, toda vez que algunos de los controles que no se mencionan podrían, en algún caso, resultar también de aplicación, a la vista de la especial tipología de los activos a proteger, la naturaleza de las amenazas, la valoración de los impactos posibles o la categoría de los sistemas de información afectados. En todo caso, las medidas de seguridad que hubieren de aplicarse para cada nivel/categoría serán, como mínimo, las señaladas en el Anexo II del ENS.

<sup>59</sup> Véase Guía CCN-STIC 821 Normas de Seguridad en el ENS.

<sup>60</sup> Véase Anexo C de la presente Guía.

		<p>usuario).</p> <p>c) Entrada de aplicaciones (tanto las que se ejecuten en los dispositivos móviles como aquellas otras centralizadas de gestión de dispositivos móviles) en producción.</p> <p>d) Establecimiento de enlaces de comunicaciones con otros sistemas.</p> <p>e) Utilización de medios de comunicación, habituales y alternativos.</p> <p>f) Utilización de soportes de información.</p> <p>g) Utilización de equipos móviles.</p>
<b>op</b>	<b>Marco operacional</b>	
op.pl	Planificación	
op.pl.1	Análisis de riesgos	En función de la categoría del sistema.
op.pl.3	Adquisición de nuevos componentes	En especial, en lo relativo a: <ul style="list-style-type: none"> <li>a) Marcas y modelos de dispositivos móviles.</li> <li>b) Sistemas operativos.</li> <li>c) Software de aplicación a instalar en los dispositivos.</li> <li>d) Software para la gestión centralizada de dispositivos móviles.</li> </ul>
op.pl.5	Componentes certificados	En especial, en lo relativo a aquellos módulos de naturaleza criptográfica. (Por ejemplo, tarjetas SIM criptográficas).
op.acc	Control de acceso	
op.acc.1	Identificación	Necesidad de disponer de mecanismos de identificación de: <ul style="list-style-type: none"> <li>a) Usuarios de dispositivos móviles.</li> <li>b) Los propios dispositivos.</li> </ul>
op.acc.2	Requisitos de acceso	Determinación de los Niveles de Acceso fijados por el organismo, en relación con los recursos corporativos a los que puede accederse a través de dispositivos móviles.
op.acc.4	Proceso de gestión de derechos de acceso	Atendiendo a: mínimo privilegio, necesidad de conocer y capacidad de autorizar.
op.acc.5	Mecanismo de autenticación	Atendiendo al nivel del sistema.
op.acc.6	Acceso local	Se considera acceso local el realizado desde los dispositivos móviles a los recursos corporativos desde dentro de las propias instalaciones de la organización y utilizando redes controladas por el organismo.
op.acc.7	Acceso remoto	Se considera acceso remoto el realizado desde los dispositivos móviles ubicados fuera de las propias instalaciones de la organización, a través de redes de terceros (en general, a través de internet público o redes de telefonía móvil).
op.exp	Explotación	
op.exp.1	Inventario de activos	Se mantendrá un inventario actualizado de todos los elementos de la infraestructura móvil del organismo, detallando su naturaleza e identificando a su responsable.



op.exp.2	Configuración de seguridad	<p>Previamente a su entrada en explotación, los dispositivos móviles se configurarán de forma que:</p> <ul style="list-style-type: none"> <li>a) Se retiren cuentas y contraseñas estándar.</li> <li>b) Se aplicará la regla de «mínima funcionalidad»<sup>61</sup>: <ul style="list-style-type: none"> <li>1.º El dispositivo debe proporcionar la funcionalidad requerida para que la organización alcance sus objetivos y ninguna otra funcionalidad,</li> <li>2.º No proporcionará funciones gratuitas, ni de operación, ni de administración, ni de auditoría, reduciendo de esta forma su perímetro al mínimo imprescindible.</li> <li>3.º Se eliminará o desactivará mediante el control de la configuración, aquellas funciones que no sean de interés, no sean necesarias, e incluso, aquellas que sean inadecuadas al fin que se persigue<sup>62</sup>.</li> </ul> </li> <li>c) Se aplicará la regla de «seguridad por defecto»: <ul style="list-style-type: none"> <li>1.º Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo.</li> <li>2.º Para reducir la seguridad, el usuario tiene que realizar acciones conscientes.</li> <li>3.º El uso natural, en los casos que el usuario no ha consultado el manual, será un uso seguro.</li> </ul> </li> </ul>
op.exp.3	Gestión de la configuración	<p>Se gestionará de forma continua la configuración de los componentes de los dispositivos móviles de forma que:</p> <ul style="list-style-type: none"> <li>a) Se mantenga en todo momento la regla de «funcionalidad mínima» ([op.exp.2]).</li> <li>b) Se mantenga en todo momento la regla de «seguridad por defecto» ([op.exp.2]).</li> <li>c) El sistema que sustenta la infraestructura móvil del organismo se adapte a las nuevas necesidades, previamente autorizadas ([op.acc.4]).</li> <li>d) El sistema que sustenta la infraestructura móvil del organismo reaccione a vulnerabilidades reportadas ([op.exp.4]).</li> <li>e) El sistema que sustenta la infraestructura móvil del organismo reaccione a incidencias (ver [op.exp.7]).</li> </ul>
op.exp.4	Mantenimiento	<p>Para mantener el equipamiento físico y lógico que constituye el sistema que sustenta la infraestructura móvil del organismo, se aplicará lo siguiente:</p> <ul style="list-style-type: none"> <li>a) Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas implicados (software centralizado de gestión de dispositivos móviles y los propios dispositivos).</li> <li>b) Se efectuará un seguimiento continuo de los anuncios de defectos.</li> <li>c) Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad (tanto en el software centralizado de gestión de dispositivos móviles,</li> </ul>

<sup>61</sup> Esto es especialmente aconsejable en dispositivos suministrados por la organización, planteando dificultades que deben evaluarse en el caso de dispositivos propiedad de los usuarios.

<sup>62</sup> Idem.

		como en los sistemas operativos y las aplicaciones instaladas en los dispositivos), parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la aplicación o no de la actualización.
op.exp.5	Gestión de cambios	<p>Cuando por el nivel/categoría del sistema así esté establecido, se mantendrá un control continuo de cambios realizados en el sistema, de forma que:</p> <ol style="list-style-type: none"> <li>a) Todos los cambios anunciados por el fabricante o proveedor (tanto del software centralizado de gestión de dispositivos móviles, como de los sistemas operativos y las aplicaciones instaladas en los dispositivos) serán analizados para determinar su conveniencia para ser incorporados, o no.</li> <li>b) Antes de poner en producción una nueva versión o una versión parcheada, se comprobará en un equipo que no esté en producción, que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario. El equipo de pruebas será equivalente al de producción en los aspectos que se comprueban.</li> <li>c) Los cambios se planificarán para reducir el impacto sobre la prestación de los servicios afectados.</li> <li>d) Mediante análisis de riesgos se determinará si los cambios son relevantes para la seguridad del sistema que sustenta la infraestructura móvil del organismo. Aquellos cambios que impliquen una situación de riesgo de nivel alto serán aprobados explícitamente de forma previa a su implantación.</li> </ol>
op.exp.6	Protección frente a código dañino	En los dispositivos móviles se dispondrá de mecanismos de prevención y reacción frente a código dañino (virus, gusanos, troyanos, programas espía, conocidos en terminología inglesa como «spyware», y en general, todo lo conocido como «malware») con mantenimiento de acuerdo a las recomendaciones del fabricante.
op.exp.7	Gestión de incidencias	<p>Cuando por el nivel/categoría del sistema así esté establecido, se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema que sustenta la infraestructura móvil del organismo, incluyendo:</p> <ol style="list-style-type: none"> <li>a) Procedimiento de reporte de incidentes reales o sospechosos, detallando el escalado de la notificación.</li> <li>b) Procedimiento de toma de medidas urgentes, incluyendo la detención de servicios, el aislamiento del dispositivo(s) afectado(s), la recogida de evidencias y protección de los registros, según convenga al caso.</li> <li>c) Procedimiento de asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.</li> <li>d) Procedimientos para informar a las partes interesadas, internas y externas.</li> <li>e) Procedimientos para: <ol style="list-style-type: none"> <li>1.º Prevenir que se repita el incidente.</li> <li>2.º Incluir en los procedimientos de usuario la identificación y forma de tratar el incidente.</li> <li>3.º Actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidencias.</li> </ol> </li> </ol> <p>La gestión de incidentes que afecten a datos de carácter personal tendrá en cuenta lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normas de desarrollo, sin perjuicio de cumplir, además, las medidas</p>

		establecidas en el ENS.
op.exp.8	Registro de la actividad de los usuarios	<p>Cuando por el nivel/categoría del sistema así esté establecido, se registrarán todas las actividades de los usuarios en el sistema, de forma que:</p> <ul style="list-style-type: none"> <li>a) El registro indicará quién realiza la actividad, cuando la realiza y sobre qué información.</li> <li>b) Se incluirá la actividad de los usuarios y, especialmente, la de los operadores y administradores del sistema de gestión centralizada de dispositivos móviles del organismo en cuanto pueden acceder a la configuración y actuar en el mantenimiento del mismo.</li> <li>c) Deben registrarse las actividades realizadas con éxito y los intentos fracasados.</li> <li>d) La determinación de qué actividades debe en registrarse y con qué niveles de detalle se determinará a la vista del análisis de riesgos realizado sobre el sistema ([op.pl.1]).</li> </ul>
op.exp.9	Registro de la gestión de incidencias	<p>Cuando por el nivel/categoría del sistema así esté establecido, se registrarán todas las actuaciones relacionadas con la gestión de incidencias del sistema que sustente la infraestructura móvil del organismo, de forma que:</p> <ul style="list-style-type: none"> <li>a) Se registrará el reporte inicial, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.</li> <li>b) Se registrará aquella evidencia que pueda, posteriormente, sustentar una demanda judicial, o hacer frente a ella, cuando el incidente pueda llevar a actuaciones disciplinarias sobre el personal interno, sobre proveedores externos o a la persecución de delitos. En la determinación de la composición y detalle de estas evidencias, se recurrirá a asesoramiento legal especializado.</li> <li>a) Como consecuencia del análisis de las incidencias, se revisará la determinación de los eventos auditables.</li> </ul>
op.exp.10	Protección de los registros de actividad	<p>Cuando por el nivel/categoría del sistema así esté establecido, se protegerán los registros del sistema que sustenta la infraestructura móvil del organismo, de forma que:</p> <ul style="list-style-type: none"> <li>a) Se determinará el periodo de retención de los registros.</li> <li>b) Se asegurará la fecha y hora. Ver [mp.info.5].</li> <li>c) Los registros no podrán ser modificados ni eliminados por personal no autorizado.</li> <li>d) Las copias de seguridad, si existen, se ajustarán a los mismos requisitos.</li> </ul>
op.exp.11	Protección de claves criptográficas	<p>Las claves criptográficas se protegerán durante todo su ciclo de vida: (1) generación, (2) transporte al punto de explotación, (3) custodia durante la explotación, (4) archivo posterior a su retirada de explotación activa y (5) destrucción final.</p> <p><b>Categoría BÁSICA</b></p> <ul style="list-style-type: none"> <li>a) Los medios de generación estarán aislados de los medios de explotación.</li> <li>b) Las claves retiradas de operación que deban ser archivadas, lo serán en medios aislados de los de explotación.</li> </ul> <p><b>Categoría MEDIA</b></p> <ul style="list-style-type: none"> <li>a) Se usarán programas evaluados o dispositivos criptográficos certificados.</li> </ul>

		b) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.
op.ext	Servicios externos	
op.ext.1	Contratación y acuerdos de nivel de servicio	Cuando por el nivel/categoría del sistema así esté establecido, previa a la utilización de recursos externos se establecerán contractualmente las características del servicio prestado y las responsabilidades de las partes. Se detallará lo que se considera calidad mínima del servicio prestado y las consecuencias de su incumplimiento. Esto es especialmente importante en la contratación de servicios de gestión centralizada de dispositivos móviles, alojados en la nube.
op.ext.2	Gestión diaria	Cuando por el nivel/categoría del sistema así esté establecido, para la gestión diaria del sistema de información que sustenta la infraestructura móvil del organismo, se establecerán los siguientes puntos: <ul style="list-style-type: none"> <li>a) Un sistema rutinario para medir el cumplimiento de las obligaciones de servicio y el procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordado ([op.ext.1]).</li> <li>b) El mecanismo y los procedimientos de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas afectados por el acuerdo.</li> <li>c) El mecanismo y los procedimientos de coordinación en caso de incidencias y desastres (ver [op.exp.7]).</li> </ul>
op.cont	Continuidad del servicio	
op.cont.1	Análisis de impacto	Cuando por el nivel/categoría del sistema así esté establecido, se realizará un análisis de impacto que permita determinar: <ul style="list-style-type: none"> <li>a) Los requisitos de disponibilidad de cada servicio afectado por el uso de dispositivos móviles medidos como el impacto de una interrupción durante un cierto periodo de tiempo.</li> <li>b) Los elementos que son críticos para la prestación de cada servicio.</li> </ul>
op.cont.2	Plan de continuidad	Cuando por el nivel/categoría del sistema así esté establecido, se desarrollará un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los sistemas de información habituales que sustentan la infraestructura móvil del organismo. Este plan contemplará los siguientes aspectos: <ul style="list-style-type: none"> <li>a) Se identificarán funciones, responsabilidades y actividades a realizar.</li> <li>b) Existirá una previsión de los medios alternativos que se va a conjugar para poder seguir prestando los servicios.</li> <li>c) Todos los medios alternativos estarán planificados y materializados en acuerdos o contratos con los proveedores correspondientes.</li> <li>d) Las personas afectadas por el plan recibirán formación específica relativa a su papel en dicho plan.</li> <li>e) El plan de continuidad será parte integral y armónica de los planes de continuidad de la organización en otras materias ajenas a la seguridad.</li> </ul>
op.cont.3	Pruebas periódicas	Cuando por el nivel/categoría del sistema así esté establecido, se realizarán pruebas periódicas para localizar y, corregir en su caso, los errores o deficiencias que puedan existir en el plan de continuidad.

op.mon	Monitorización del sistema	
op.mon.1	Detección de intrusión	Se dispondrán de herramientas de detección o de prevención de intrusión. Por ejemplo: intentos de acceso a los recursos corporativos con dispositivos móviles, sistemas operativos o aplicaciones no autorizadas.
op.mon.2	Sistema de métricas	Se establecerá un conjunto de indicadores que mida el desempeño real del sistema en materia de seguridad, en los siguientes aspectos: a) Grado de implantación de las medidas de seguridad. b) Eficacia y eficiencia de las medidas de seguridad. c) Impacto de los incidentes de seguridad.
<b>mp</b>	<b>Medidas de protección</b>	
mp.if	Protección de las instalaciones e infraestructuras	
mp.if.1	Áreas separadas y con control de acceso	El equipamiento del sistema centralizado de gestión de dispositivos móviles del organismo se instalará en áreas separadas específicas para su función. Se controlarán los accesos a las áreas indicadas de forma que sólo se pueda acceder por las entradas previstas y vigiladas.
mp.if.2	Identificación de las personas	El mecanismo de control de acceso se atenderá a lo que se dispone a continuación: a) Se identificará a todas las personas que accedan a los locales donde hay equipamiento que forme parte del sistema de información que sustenta la infraestructura móvil del organismo. b) Se registrarán las entradas y salidas de personas.
mp.if.3	Acondicionamiento de los locales	Los locales donde se ubique el sistema de información que sustenta la infraestructura móvil del organismo y sus componentes, dispondrán de elementos adecuados para el eficaz funcionamiento del equipamiento allí instalado. Y, en especial: a) Condiciones de temperatura y humedad. b) Protección frente a las amenazas identificadas en el análisis de riesgos. c) Protección del cableado frente a incidentes fortuitos o deliberados.
mp.if.4	Energía eléctrica	Los locales donde se ubique el sistema de información que sustenta la infraestructura móvil del organismo y sus componentes dispondrán de la energía eléctrica, y sus tomas correspondientes, necesaria para su funcionamiento, de forma que en los mismos: a) Se garantizará el suministro de potencia eléctrica. b) Se garantizará el correcto funcionamiento de las luces de emergencia. Además, cuando por el nivel/categoría del sistema así esté establecido, se garantizará el suministro eléctrico a los sistemas en caso de fallo del suministro general, garantizando el tiempo suficiente para una terminación ordenada de los procesos, salvaguardando la información.
mp.if.5	Protección frente a incendios	Los locales donde se ubique el sistema de información que sustenta la infraestructura móvil del organismo y sus componentes se protegerán frente a incendios fortuitos o deliberados, aplicando al menos la normativa industrial pertinente.

mp.if.6	Protección frente a inundaciones	Cuando por el nivel/categoría del sistema así esté establecido, los locales donde se ubique el sistema de información que sustenta la infraestructura móvil del organismo y sus componentes se protegerán frente a incidentes fortuitos o deliberados causados por el agua.
mp.if.7	Registro de entrada y salida de equipamiento [dispositivos móviles y soportes]	Se llevará un registro pormenorizado de toda entrada y salida de equipamiento (dispositivos móviles y soportes, incluyendo soportes para software de gestión de dispositivos móviles, sistemas operativos o aplicaciones), incluyendo la identificación de la persona que autoriza de movimiento.
mp.if.9	Instalaciones alternativas	Cuando por el nivel/categoría del sistema así esté establecido, se garantizará la existencia y disponibilidad de instalaciones alternativas del sistema de información que sustenta la infraestructura móvil del organismo para poder trabajar en caso de que las instalaciones habituales no estén disponibles. Las instalaciones alternativas disfrutarán de las mismas garantías de seguridad que las instalaciones habituales.
mp.per	Gestión del personal	
mp.per.1	Caracterización del puesto de trabajo	Cuando por el nivel/categoría del sistema así esté establecido, cada dispositivo/usuario se caracterizará de la siguiente forma: <ul style="list-style-type: none"> <li>a) Se definirán las responsabilidades relacionadas con cada dispositivo/usuario en materia de seguridad móvil (en general, recursos corporativos a los que puede acceder). La definición se basará en el análisis de riesgos.</li> <li>b) Se definirán los requisitos que deben satisfacer los dispositivos/usuarios que vayan a usar determinados privilegios/niveles de acceso, en particular, en términos de confidencialidad.</li> <li>c) Dichos requisitos se tendrán en cuenta en la selección de los usuarios, incluyendo la verificación de sus antecedentes laborales, formación y otras referencias.</li> </ul>
mp.per.2	Deberes y obligaciones <sup>63</sup>	Se informará a cada usuario de dispositivos móviles de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad. <ul style="list-style-type: none"> <li>a) Se especificarán las medidas disciplinarias a que haya lugar.</li> <li>b) Se cubrirá tanto el periodo durante el cual se desempeña el puesto, como las obligaciones en caso de término de la asignación, o traslado a otro puesto de trabajo.</li> <li>c) Se contemplará el deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que estén adscritos al puesto de trabajo, como posteriormente a su terminación.</li> </ul> En caso de personal contratado a través de un tercero: <ul style="list-style-type: none"> <li>a) Se establecerán los deberes y obligaciones del personal.</li> <li>b) Se establecerán los deberes y obligaciones de cada parte.</li> <li>c) Se establecerá el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones.</li> </ul>

<sup>63</sup> Véase Guía CCN-STIC 821: Normas de Seguridad en el ENS y Anexo C de esta Guía.

mp.per.3	Concienciación	<p>Se realizarán las acciones necesarias para concienciar regularmente a los usuarios de dispositivos móviles acerca de su papel y responsabilidad para que la seguridad de la infraestructura móvil del organismo alcance los niveles exigidos.</p> <p>En particular, se recordará regularmente:</p> <ol style="list-style-type: none"> <li>a) La normativa de seguridad relativa al buen uso de los sistemas<sup>64</sup>.</li> <li>b) La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.</li> <li>c) El procedimiento de reporte de incidencias de seguridad, sean reales o falsas alarmas.</li> </ol>
mp.per.4	Formación	<p>Se formará regularmente a los usuarios de dispositivos móviles en aquellas materias que requieran para el desempeño de sus funciones, en particular en lo relativo a:</p> <ol style="list-style-type: none"> <li>a) Configuración de dispositivos móviles, sistemas operativos y aplicaciones.</li> <li>b) Detección y reacción a incidentes.</li> <li>c) Gestión de la información en cualquier soporte en el que se encuentre. Se cubrirán al menos las siguientes actividades: almacenamiento, transferencia, copias, distribución y destrucción.</li> </ol>
mp.eq	Protección de los equipos	
mp.eq.2	Bloqueo de puesto de trabajo [dispositivo móvil]	<p>Cuando por el nivel/categoría del sistema así esté establecido, el dispositivo móvil se bloqueará al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso.</p> <p>En los niveles superiores de seguridad, además, pasado un cierto tiempo, superior al anterior, se cancelarán las sesiones abiertas desde dicho dispositivo móvil.</p>
mp.eq.3	Protección de portátiles [dispositivos móviles]	<p>Los dispositivos móviles que abandonen las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente, con un riesgo manifiesto de pérdida o robo, serán protegidos adecuadamente.</p> <p>Sin perjuicio de las medidas generales que les afecten, se adoptarán las siguientes:</p> <ol style="list-style-type: none"> <li>a) Se llevará un inventario de dispositivos móviles junto con una identificación de la persona responsable del mismo y un control regular de que está positivamente bajo su control.</li> <li>b) Se establecerá un canal de comunicación para informar, al servicio de gestión de incidencias, de pérdidas o sustracciones.</li> <li>c) Se establecerá un sistema de protección perimetral que minimice la visibilidad exterior y controle las opciones de acceso al interior cuando el dispositivo móvil se conecte a redes, en particular si el equipo se conecta a redes públicas.</li> <li>d) Se evitará, en la medida de lo posible, que el dispositivo contenga claves de acceso remoto a la organización. Se considerarán claves de acceso remoto aquellas que sean capaces de habilitar un</li> </ol>

<sup>64</sup> Idem.



		<p>acceso a otros equipos de la organización, u otras de naturaleza análoga.</p> <p>Además, en la categoría alta de seguridad:</p> <ul style="list-style-type: none"> <li>a) Se dotará al dispositivo de detectores de violación que permitan saber el equipo ha sido manipulado y activen los procedimientos previstos de gestión del incidente.</li> <li>b) La información de nivel alto almacenada en el dispositivo se protegerá mediante cifrado.</li> </ul>
mp.com	Protección de las comunicaciones	
mp.com.1	Perímetro seguro	<p>Se dispondrá un sistema cortafuegos que separe la red interna del exterior. Todo el tráfico generado por dispositivos móviles deberá atravesar dicho cortafuegos que sólo dejara transitar los flujos previamente autorizados.</p> <p>En la categoría alta de seguridad:</p> <ul style="list-style-type: none"> <li>a) El sistema de cortafuegos constará de dos o más equipos de diferente fabricante dispuestos en cascada.</li> <li>b) Se dispondrán sistemas redundantes.</li> </ul>
mp.com.2	Protección de la confidencialidad	<p>Cuando por el nivel/categoría del sistema así esté establecido:</p> <ul style="list-style-type: none"> <li>a) Se emplearán, redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad.</li> <li>b) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.</li> </ul> <p>En el nivel alto de seguridad, además:</p> <ul style="list-style-type: none"> <li>a) Se emplearán, preferentemente, dispositivos hardware en el establecimiento y utilización de la red privada virtual.</li> <li>b) Se emplearán, preferentemente, productos certificados [op.pl.5].</li> </ul>
mp.com.3	Protección de la autenticidad y de la integridad	<ul style="list-style-type: none"> <li>a) Se asegurará la autenticidad del otro extremo de un canal de comunicación antes de intercambiar información alguna (ver [op.acc.5]).</li> <li>b) Se prevendrán ataques activos, garantizando que al menos serán detectados. y se activarán los procedimientos previstos de tratamiento del incidente Se considerarán ataques activos: <ul style="list-style-type: none"> <li>1.º La alteración de la información en transito</li> <li>2.º La inyección de información espuria</li> <li>3.º El secuestro de la sesión por una tercera parte</li> </ul> </li> </ul> <p>Además, para el nivel MEDIO:</p> <ul style="list-style-type: none"> <li>a) Se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad:</li> <li>b) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.</li> </ul> <p>Además, para el nivel ALTO:</p> <ul style="list-style-type: none"> <li>a) Se valorará positivamente en empleo de dispositivos hardware en el establecimiento y utilización de la red privada virtual.</li> </ul>

		b) Se emplearán, preferentemente, productos certificados [op.pl.5].
mp.si	Protección de los soportes de información	
mp.si.1	Etiquetado [de dispositivos móviles y soportes]	Los soportes de información de los dispositivos móviles (singularmente, las memorias removibles) se etiquetarán de forma que, sin revelar su contenido, se indique el nivel de seguridad de la información contenida de mayor calificación. Los usuarios han de estar capacitados para entender el significado de las etiquetas, bien mediante simple inspección, bien mediante el recurso a un repositorio que lo explique.
mp.si.2	Criptografía	Esta medida se aplica, en particular, a todos los soportes removibles usados por los dispositivos móviles (o por los equipos en los que se ejecute el software centralizado de gestión de dispositivos móviles). Por tanto, se entenderán por dispositivos removibles, en este caso, las memorias flash, pen drives o las tarjetas SIM de los dispositivos móviles, y los CD, DVD, discos USB, u otros de naturaleza análoga. Para el nivel MEDIO, además, se aplicarán mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida. Para el nivel ALTO, además: a) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional. b) Se emplearán, preferentemente, productos certificados [op.pl.5].
mp.si.3	Custodia [de dispositivos móviles y soportes]	Se aplicará la debida diligencia y control a los dispositivos móviles y soportes de información que permanecen bajo la responsabilidad de la organización <sup>65</sup> , mediante las siguientes actuaciones: a) Garantizando el control de acceso con medidas físicas ([mp.if.1] y [mp.if.7]) ó lógicas ([mp.si.2]), o ambas. b) Garantizando que se respetan las exigencias de mantenimiento del fabricante, en especial, en lo referente a temperatura, humedad y otros agresores medioambientales.
mp.si.4	Transporte [de dispositivos móviles y soportes]	El responsable de sistemas garantizará que los dispositivos permanecen bajo control y que satisfacen sus requisitos de seguridad mientras están siendo desplazados de un lugar a otro. Para ello: a) Se dispondrá de un registro de salida que identifique al transportista que recibe el dispositivo/soporte para su traslado. b) Se dispondrá de un registro de entrada que identifique al transportista que lo entrega. c) Se dispondrá de un procedimiento rutinario que coteje las salidas con las llegadas y levante las alarmas pertinentes cuando se detecte algún incidente. d) Se utilizarán los medios de protección criptográfica ([mp.si.2]) correspondientes al nivel de calificación de la información contenida de mayor nivel. e) Se gestionarán las claves según [op.exp.11].

<sup>65</sup> Algunas de tales medidas son igualmente predicables de los usuarios de los dispositivos móviles.

mp.si.5	Borrado y destrucción [de los contenidos de los dispositivos móviles y sus memorias fijas o removibles]	<p>Cuando por el nivel/categoría del sistema así esté establecido, la medida de borrado y destrucción de soportes de información se aplicará a todo tipo de dispositivos móviles (y sus componentes, fijos o removibles) susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos.</p> <ol style="list-style-type: none"> <li>a) Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto de un borrado seguro de su anterior contenido.</li> <li>b) Se destruirán de forma segura los soportes, en los siguientes casos: <ol style="list-style-type: none"> <li>1.º Cuando la naturaleza del soporte no permita un borrado seguro.</li> <li>2.º Cuando así lo requiera el procedimiento asociado al tipo de la información contenida,</li> </ol> </li> <li>c) Se emplearán, preferentemente, productos certificados [op.pl.5].</li> </ol>
mp.sw	Protección de las aplicaciones informáticas	
mp.sw.2	Aceptación y puesta en servicio [de las aplicaciones que se ejecutarán en los dispositivos móviles]	<p>Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación.</p> <ol style="list-style-type: none"> <li>a) Se comprobará que: <ol style="list-style-type: none"> <li>1.º Se cumplen los criterios de aceptación en materia de seguridad.</li> <li>2.º No se deteriora la seguridad de otros componentes del servicio.</li> </ol> </li> <li>b) Las pruebas se realizarán en un entorno aislado (pre-producción).</li> <li>c) Las pruebas de aceptación no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.</li> </ol> <p>Para sistemas de categoría MEDIA, además, se realizarán las siguientes inspecciones previas a la entrada en servicio:</p> <ol style="list-style-type: none"> <li>a) Análisis de vulnerabilidades.</li> <li>b) Pruebas de penetración.</li> </ol> <p>Para sistemas de categoría ALTA, además, se realizarán las siguientes inspecciones previas a la entrada en servicio:</p> <ol style="list-style-type: none"> <li>a) Análisis de coherencia en la integración en los procesos.</li> <li>b) Se considerará la oportunidad de realizar una auditoría de código fuente.</li> </ol>
mp.info	Protección de la información	
mp.info.1	Datos de carácter personal	<p>Cuando el dispositivo móvil trate datos de carácter personal, se estará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y sus normas de desarrollo, sin perjuicio de cumplir, además, las medidas establecidas por el ENS.</p> <p>Lo indicado en el párrafo anterior también se aplicará, cuando una disposición con rango de ley se remita a las normas sobre datos de carácter personal en la protección de información.</p>
mp.info.2	Calificación de la información [tratada por los dispositivos móviles]	<p>Para sistemas de nivel BAJO:</p> <ol style="list-style-type: none"> <li>1. Para calificar la información se estará a lo establecido legalmente sobre la naturaleza de la misma.</li> <li>2. La política de seguridad de gestión de dispositivos móviles del organismo establecerá quién es el responsable de cada información manejada por el sistema.</li> </ol>

		<p>3. La política de seguridad de gestión de dispositivos móviles del organismo recogerá, directa o indirectamente, los criterios que, en cada organización, determinarán el nivel de seguridad requerido, dentro del marco establecido en el artículo 43 y los criterios generales prescritos en el Anexo I del ENS.</p> <p>4. El responsable de cada información seguirá los criterios determinados en el apartado anterior para asignar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal.</p> <p>5. El responsable de cada información en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido, de acuerdo a los apartados anteriores.</p> <p>Para sistemas de nivel MEDIO, además:  Se redactarán los procedimientos necesarios que describan, en detalle, la forma en que se ha de etiquetar y tratar la información en consideración al nivel de seguridad que requiere; y precisando cómo se ha de realizar:</p> <ol style="list-style-type: none"> <li>a) Su control de acceso.</li> <li>b) Su almacenamiento.</li> <li>c) La realización de copias.</li> <li>d) El etiquetado de soportes.</li> <li>e) Su transmisión telemática.</li> <li>f) Y cualquier otra actividad relacionada con dicha información.</li> </ol>
mp.info.3	Cifrado de la información	<p>Para sistemas con nivel ALTO, para el cifrado de información se estará a lo que se indica a continuación:</p> <ol style="list-style-type: none"> <li>a) La información con un nivel alto en confidencialidad se cifrará tanto durante su almacenamiento dentro del dispositivo móvil como durante su transmisión. Sólo estará en claro mientras se está haciendo uso de ella.</li> <li>b) Para el uso de criptografía en las comunicaciones, se estará a lo dispuesto en [mp.com.2].</li> <li>c) Para el uso de criptografía en los soportes de información (por ejemplo, en las memorias removibles de los dispositivos móviles, se estará a lo dispuesto en [mp.si.2].</li> </ol>
mp.info.4	Firma electrónica	<p>La firma electrónica es un mecanismo de prevención del repudio; es decir, previene frente a la posibilidad de que en el futuro el signatario pudiera desdecirse de la información firmada.</p> <p>La firma electrónica garantiza la autenticidad del signatario y la integridad del contenido.</p> <p>Cuando se emplee firma electrónica en los dispositivos móviles:</p> <ol style="list-style-type: none"> <li>a) El signatario será la parte que se hace responsable de la información, en la medida de sus atribuciones.</li> <li>b) Se dispondrá de una Política de Firma Electrónica para Dispositivos Móviles (Integrada en la Política General de Firma Electrónica del organismo), aprobada por el órgano superior competente que corresponda.</li> </ol>

		<p>Para sistemas de nivel BAJO se empleará cualquier medio de firma electrónica de los previstos en la legislación vigente.</p> <p>Para sistemas de nivel MEDIO:</p> <ol style="list-style-type: none"> <li>1. Los medios utilizados en la firma electrónica serán proporcionados a la calificación de la información tratada. En todo caso: <ol style="list-style-type: none"> <li>a) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.</li> <li>b) Se emplearán, preferentemente, certificados reconocidos.</li> <li>c) Se emplearán, preferentemente, dispositivos seguros de firma.</li> </ol> </li> <li>2. Se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquella soporte, sin perjuicio de que se pueda ampliar este período de acuerdo con lo que establezca la Política de Firma Electrónica y de Certificados que sea de aplicación. Para tal fin: <ol style="list-style-type: none"> <li>a) Se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación: <ol style="list-style-type: none"> <li>1.º Certificados.</li> <li>2.º Datos de verificación y validación.</li> </ol> </li> <li>b) Se protegerán la firma y la información mencionada en el apartado anterior con un sello de tiempo.</li> <li>c) El organismo que recabe documentos firmados por el administrado verificará y validará la firma recibida en el momento de la recepción, anexando o referenciando sin ambigüedad la información descrita en los epígrafes a) y b).</li> <li>d) La firma electrónica de documentos por parte de la Administración anexará o referenciará sin ambigüedad la información descrita en los epígrafes a) y b).</li> </ol> </li> </ol> <p>Para sistemas de nivel ALTO se aplicarán las medidas de seguridad referentes a firma electrónica exigibles en la nivel Medio, además de las siguientes:</p> <ol style="list-style-type: none"> <li>a) Se usarán certificados reconocidos.</li> <li>b) Se usarán dispositivos seguros de creación de firma.</li> <li>c) Se emplearán, preferentemente, productos certificados [op.pl.5].</li> </ol>
mp.info.9	Copias de seguridad (backup) [de los datos contenidos en los dispositivos móviles]	<p>Para sistemas de nivel MEDIO se realizarán copias de respaldo del contenido de los dispositivos móviles que permitan recuperar datos perdidos accidental o intencionadamente con una antigüedad determinada. Las copias de respaldo disfrutarán de la misma seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. En particular, se considerará la conveniencia o necesidad de que las copias de seguridad estén cifradas para garantizar la confidencialidad. Las copias de respaldo deberán abarcar:</p>

		<ul style="list-style-type: none"> <li>a) Información de trabajo de la organización.</li> <li>b) Aplicaciones en explotación, incluyendo los sistemas operativos.</li> <li>c) Datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga.</li> <li>d) Claves utilizadas para preservar la confidencialidad de la información.</li> </ul>
mp.s	Protección de los servicios	
mp.s.1	Protección del correo electrónico (e-mail)	<p>El correo electrónico se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:</p> <ul style="list-style-type: none"> <li>a) La información distribuida por medio de correo electrónico, se protegerá, tanto en el cuerpo de los mensajes, como en los anexos.</li> <li>b) Se protegerá la información de encaminamiento de mensajes y establecimiento de conexiones.</li> <li>c) Se protegerá a la organización frente a problemas que se materializan por medio del correo electrónico, en concreto: <ul style="list-style-type: none"> <li>1.º Correo no solicitado, en su expresión inglesa «spam».</li> <li>2.º Programas dañinos, constituidos por virus, gusanos, troyanos, espías, u otros de naturaleza análoga.</li> <li>3.º Código móvil de tipo «applet».</li> </ul> </li> <li>d) Se establecerán normas de uso del correo electrónico por parte del personal determinado<sup>66</sup>. Estas normas de uso contendrán: <ul style="list-style-type: none"> <li>1.º Limitaciones al uso como soporte de comunicaciones privadas.</li> <li>2.º Actividades de concienciación y formación relativas al uso del correo electrónico.</li> </ul> </li> </ul>
mp.s.2	Protección de servicios y aplicaciones web [accesibles a través de dispositivos móviles]	<p>Los subsistemas dedicados a la publicación de información deberán ser protegidos frente a las amenazas que les son propias.</p> <ul style="list-style-type: none"> <li>a) Cuando la información tenga algún tipo de control de acceso, se garantizará la imposibilidad de acceder a la información obviando la autenticación (de dispositivo móvil y/o de usuario), en particular tomando medidas en los siguientes aspectos: <ul style="list-style-type: none"> <li>1.º Se evitará que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado.</li> <li>2.º Se prevendrán ataques de manipulación de URL.</li> <li>3.º Se prevendrán ataques de manipulación de fragmentos de información que se almacena en el dispositivo móvil del visitante de una página web a través de su navegador, a petición del servidor de la página, conocido en terminología inglesa como «cookies».</li> <li>4.º Se prevendrán ataques de inyección de código.</li> </ul> </li> </ul>

<sup>66</sup> Ver Guía CCN-STIC 821. Normas de Seguridad en el ENS.

		<ul style="list-style-type: none"><li>b) Se prevendrán intentos de escalado de privilegios.</li><li>c) Se prevendrán ataques de «cross site scripting».</li><li>d) Se prevendrán ataques de manipulación de programas o dispositivos que realizan una acción en representación de otros, conocidos en terminología inglesa como «proxies» y, sistemas especiales de almacenamiento de alta velocidad, conocidos en terminología inglesa como «cachés».</li></ul>
--	--	--



## ANEXO B: ASPECTOS DE DECISIÓN SOBRE BYOD

Por su importancia y los riesgos derivados de su implantación, se muestra seguidamente una relación de aquellos elementos más significativos que deben considerarse para determinar si un programa BYOD es o no adecuado para un organismo público concreto.

Esta relación, que no pretende ser exhaustiva, incluye consideraciones sobre políticas, normas y procedimientos dirigidos a Responsables de Seguridad, Responsables de Sistemas, Responsables de Recursos Humanos, Responsables Económico-Financieros y Responsables de Compras Públicas, entre otros.

- Implementación técnica:
  - Virtualización.
  - Aislamiento.
  - Coexistencia controlada.
- Roles y responsabilidades:
  - Organismo.
  - Usuarios.
  - Help Desk.
  - Asistencia técnica del operador (móvil).
- Incentivos para el organismo y los usuarios:
  - Opinión de los usuarios sobre beneficios/retos de su adopción.
  - Análisis de la participación voluntaria en el programa y su impacto en términos de servicio.
- Formación, uso y operación:
  - Determinación de la formación, entrenamiento y acuerdos con los potenciales usuarios.
  - Determinación de las políticas correspondientes, en colaboración con los representantes de los trabajadores.
  - Garantizar el cumplimiento de los acuerdos y normas laborales que resulten de aplicación.
  - Determinación del impacto en el tráfico de datos (sus costes y sus posibles reembolsos), de cara a escoger la solución técnica más adecuada.
  - Determinar los Acuerdos de Teletrabajo admisibles.
- Seguridad:
  - Evaluar y documentar los riesgos, en relación con:
    - La seguridad de la información.
    - La seguridad de las operaciones.
    - La seguridad de la transmisión.
  - Garantizar la coherencia con las normas y estándares nacionales que resulten de aplicación.
  - Evaluar la seguridad alcanzada con el modelo BYOD frente a la seguridad de los dispositivos a los que está sustituyendo.
  - Garantizar los requisitos de interoperabilidad impuestos por el Esquema Nacional de Interoperabilidad, cuando resulten de aplicación.

- Privacidad:
  - Identificar el adecuado equilibrio entre la privacidad de los usuarios y la seguridad de la organización.
  - Documentar los procesos de usuario para proteger los datos personales en caso de que se proceda a un borrado del dispositivo.
- Cuestiones legales y éticas:
  - Definir "uso aceptable" desde las perspectivas del organismo y del usuario.
  - Determinar el tipo de monitorización que puede llevarse a cabo (incluida la retirada del dispositivo) y las cuestiones sobre responsabilidad de los usuarios (por ejemplo, a través de adhesiones voluntarias a códigos de comportamiento).
  - Considerar las implicaciones de igualdad en el desempeño de las funciones profesionales (por ejemplo, las derivadas de la disparidad en la calidad de los dispositivos personales).
- Proveedores de servicios:
  - Identificar a las empresas que puedan ofrecer descuentos para empleados públicos.
  - Analizar la conveniencia o no de impulsar programas corporativos para la adquisición de quipos y dispositivos.
  - Evaluar las implicaciones fiscales en relación con los reembolsos, si las hubiere.
- Dispositivos y aplicaciones:
  - Identificar los dispositivos permitidos para evitar la introducción de hardware o firmware dañino.
  - Definir las aplicaciones que se precisan, las permitidas y las prohibidas, incluyendo el uso de soluciones para la Gestión Centralizada de Dispositivos Móviles (MDM) y/o la Gestión de Aplicaciones Móviles (MAM).
  - Adoptar las mejores prácticas de desarrollo de aplicaciones para asegurar la portabilidad de los datos a través de distintas plataformas.
  - Analizar los problemas de compatibilidad entre aplicaciones.
  - Analizar la oportunidad de usar enfoques orientados al almacenamiento en cloud frente al almacenamiento en el dispositivo.
  - Establecer mecanismos de clarificación respecto de la titularidad de las aplicaciones y datos contenidos en el dispositivo.
- Gestión de activos:
  - Acciones derivadas de la retirada del dispositivo (debido a sustitución, pérdida, robo, etc., o cancelación de la actividad profesional del usuario).
  - Acciones para la comunicación y seguimiento de incidencias en caso de dispositivos personales perdidos o robados.
  - Acciones para reemplazar los dispositivos perdidos si el usuario decide no reemplazarlo con fondos personales.
  - Aprovisionamiento de fondos para servicio técnico y mantenimiento de los dispositivos.

## ANEXO C: MODELO DE NORMATIVA DE SEGURIDAD EN EL USO DE DISPOSITIVOS MÓVILES EN EL <<ORGANISMO>>

Las Administraciones públicas, en el desarrollo de sus funciones de servicio, policía o fomento, están sometidas a diferentes normativas, de carácter estatal, autonómico o local. La particularidad de la actuación administrativa realizada por medios electrónicos viene requiriendo, en los mismos tres niveles, la existencia de normas asimismo específicas, al objeto de acomodar aquellas funciones originarias a los condicionantes y medios electrónicos.

En este sentido, la LAECSP ha supuesto el punto de partida de un extenso compendio de regulaciones que vienen completando nuestro moderno ordenamiento jurídico administrativo-electrónico, entre las que cabe destacar: el Real Decreto 1671/2009, de 6 de septiembre, de desarrollo parcial de la LAECSP, el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica y el Real Decreto 4/2010, de de enero, por el que se regula el Esquema Nacional de Interoperabilidad, entre otras.

Con el objetivo de profundizar en las medidas de seguridad requeridas por los sistemas de información del ámbito de la LAECSP, el ENS insta a los organismos de las AA.PP. a desarrollar, publicar y hacer valer normas de carácter interno a los propios organismos, tendentes a mejorar el nivel de seguridad de las informaciones que manejan y los servicios que prestan.

La necesidad de completar el marco normativo aparece explícitamente en muchos de los preceptos del ENS. Por ejemplo, en los artículos 14 (Gestión del personal), 18 (Adquisición de productos de seguridad), 21 (Protección de información almacenada y en tránsito), 23 (Registro de actividad), 34 (Auditoría de la seguridad), 37 (Prestación de servicios de respuesta a incidentes de seguridad en las Administraciones públicas), Disposición adicional tercera (Comité de Seguridad de la Información de las Administraciones Públicas), etc.

En concreto, en el Anexo II del ENS (Medidas de Seguridad), se encuentra la medida [org.2], que señala:

### 1.2 Normativa de seguridad [org.2].

Se dispondrá de una serie de documentos que describan:

- a) El uso correcto de equipos, servicios e instalaciones.
- b) Lo que se considerará uso indebido.
- c) La responsabilidad del personal con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

Esta habilitación a los organismos de las AA.PP. para que promuevan su propia normativa interna y de relación con terceros se alienta en varias medidas de seguridad del ENS: Requisitos de acceso [op.acc.2], Deberes y obligaciones [mp.per.2], Concienciación [mp.per.3], Formación [mp.per.4], Protección del correo electrónico (e-mail) [mp.s.1], etc.

1. De acuerdo con lo previsto en el artículo 37 del ENS, el CCN-CERT investigará y divulgará las mejores prácticas sobre seguridad de la información entre todos los miembros de las Administraciones públicas. Con esta finalidad, las series de

Documentos CCN-STIC, elaboradas por el Centro Criptológico Nacional, ofrecerán **normas, instrucciones, guías y recomendaciones** para aplicar el Esquema Nacional de Seguridad y para garantizar la seguridad de los sistemas de información en la Administración.

2. Es en base a este mandato por el que se incluyen en la presente Guía un **Modelo de Normas de Seguridad** que puede ser usado por los organismos de las Administraciones públicas españolas, en cumplimiento de lo preceptuado en la anteriormente citada medida del ENS: **Normativa de Seguridad [org.2]**.
3. El modelo presentado seguidamente deben ser tomado como referencia. Cada organismo deberá adaptar las normas a su casuística particular.

En el Modelo siguiente se han seguido las siguientes convenciones:

Término	Significado
<<ORGANISMO>>	<p>Cualquier <b>organismo</b> de las Administraciones públicas del ámbito de aplicación del ENS.</p> <p>Puede ser también aplicado a unidades administrativas inferiores, si disponen de la autonomía correspondiente para decidir sobre su propia normativa.</p>
<<U/OC>>	<p><b>Unidad / Organismo Colegiado</b> competente para desarrollar la acción que se menciona.</p> <p>En ocasiones, un mismo párrafo puede contener varias de estas expresiones, que podrán referirse a la misma unidad o a unidades distintas, según corresponda.</p>
<<texto>>	<p>Se incluirá el contenido que se considere adecuado.</p> <p>Por ejemplo &lt;&lt;señalar periodicidad&gt;&gt; podría dar lugar a &lt;&lt;mensualmente&gt;&gt;.</p>
[contenido opcional]	<p>Inclusión de contenido (textos, gráficos, etc.), de naturaleza opcional.</p>

**NORMATIVA DE SEGURIDAD EN EL USO DE LOS DISPOSITIVOS MÓVILES EN EL <<ORGANISMO>>****Versión <<x>>, <<fecha>>****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 del <<ORGANISMO>> de lo que debe ser considerado un “uso correcto”, señalando aquellas características o funcionalidades que se consideran “aceptables” para propósitos profesionales y “permitidas” cuando se use para propósitos privados.

Estas normas se establecen para proteger la información del <<ORGANISMO>> contenida o tratada en los antedichos dispositivos móviles, o accesible a través de ellos.

**2. Ámbito de aplicación y responsabilidades.**

Para la presente Normativa, se entenderá por “dispositivo móvil” cualquier elemento electrónico no fijo con capacidad de registrar, almacenar y/o transmitir datos, voz, video o imágenes, incluyendo entre ellos a los asistentes digitales personales (PDA), teléfonos móviles (especialmente, los smartphones), y tabletas (tablets), que operen bajo uno de los siguientes sistemas operativos: Android (Google), AOSP- BlackBerry (RIM), iOS (Apple) y Windows Phone (Microsoft).

La normativa contenida en este documento afecta tanto a los dispositivos móviles suministrados a los usuarios por el propio <<ORGANISMO>> como aquellos otros, propiedad de los usuarios, que estén autorizados a usar en el tratamiento o acceso a recursos, servicios o datos corporativos, debiendo ser observada por todos los usuarios del <<ORGANISMO>>. La unidad <<U/OC>> del <<ORGANISMO>> es la competente para dirigir y supervisar el adecuado cumplimiento de lo contenido en el presente documento.

Este documento, además, determina, de manera clara, la responsabilidad que asumen los usuarios de dispositivos móviles propiedad del <<ORGANISMO>> de tratar tales equipos de acuerdo con las normas señaladas en este documento. El cuidado del dispositivo móvil es responsabilidad de cada usuario. El incumplimiento de las directrices que figuran seguidamente 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>>.**

El Comité de Seguridad de la Información del <<ORGANISMO>> (entre cuyos miembros se contará con el Responsable de Seguridad y el Responsable del Sistema) tiene la responsabilidad general de establecer las medidas de seguridad para los dispositivos móviles.

**Responsable del Sistema**

El Responsable del Sistema del <<ORGANISMO>> tiene la responsabilidad de implementar las medidas de seguridad anteriores.

**Unidad <<U/OC>> competente**

La unidad <<U/OC>> competente del <<ORGANISMO>> deberá:

- a) Adquirir los dispositivos móviles propiedad del <<ORGANISMO>> para aquellos usuarios que lo precisen.
- b) Aprobar los tipos de dispositivos móviles propiedad de los usuarios, que se acepten para su uso profesional.
- c) Garantizar que la entrega de los dispositivos propiedad del <<ORGANISMO>> a determinados usuarios está fundamentada en razones profesionales y goza de las aprobaciones pertinentes.
- d) Adoptar las acciones oportunas para la distribución, operación y soporte de los dispositivos móviles propiedad del <<ORGANISMO>> que se entregan a los usuarios.
- e) Mantener un inventario de los dispositivos móviles propiedad del <<ORGANISMO>>, incluyendo marca, modelo, número de serie, departamento del usuario, nombre del usuario y las fechas de entrega, inicio y fin del servicio.
- f) Mantener un inventario de las licencias del software instalado en los dispositivos móviles, tanto cuando sean propiedad del <<ORGANISMO>> como cuando sean de titularidad privada (software corporativo).
- g) Establecer y mantener las configuraciones de seguridad para todos los dispositivos móviles propiedad del <<ORGANISMO>> distribuidos, incluidos parches y actualizaciones de software o firmware.
- h) Registro y seguimiento de la actividad de todos los dispositivos propiedad del <<ORGANISMO>> entregados, en relación con el cumplimiento de las normas de comportamiento que resulten de aplicación.
- i) Desarrollar la **Guía de Usuario para el Acceso Remoto con Tecnología Móvil** del <<ORGANISMO>>.

**Responsable de Seguridad / Responsables de Seguridad Delegados / Administradores de Seguridad (Supervisores)**

Se encargarán de la supervisión de aquellos usuarios que han solicitado o se les ha hecho entrega de dispositivos móviles propiedad del <<ORGANISMO>>, o desean utilizar sus dispositivos móviles personales para desarrollar actividades profesionales.

Estas acciones comprenden, entre otras, la supervisión de que el usuario:

- a) Cumple los requisitos de gestión, tal y como se describen en la Guía de Usuario para el Acceso Remoto con Tecnología Móvil del <<ORGANISMO>>.
- b) Suscribe, en su caso, el Acuerdo de Usuario de Tecnología Móvil del <<ORGANISMO>>
- c) Informa a la <<U/OC>> competente sobre la pérdida, robo, daño, destrucción, puesta en compromiso o mal funcionamiento de cualquier dispositivo móvil propiedad del <<ORGANISMO>> entregado.

[

**4. Plan de Tarifas**

El actual Plan de Tarifas que el <<ORGANISMO>> ha suscrito con <<operador de comunicaciones móviles>> incluyen:

- <<precisiones en cuanto a tráfico de voz local, nacional e internacional>>
- <<precisiones en cuanto a tráfico de datos>>
- <<precisiones en cuanto a fechas/días/horarios de tarificación especial>>
- <<precisiones en cuanto a tarifa plana o llamadas ilimitadas de voz>>

- <<precisiones en cuanto a tarifa plana o mensajes de texto ilimitados>>
  - <<otras cuestiones>>
- ]

## 5. Usuarios

Aquellos usuarios que desarrollen actividades profesionales con dispositivos móviles deberán:

- a) Suscribir, en su caso, el Acuerdo de Usuario de Tecnología Móvil del <<ORGANISMO>><sup>67</sup>.
- 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>> cuando utilice el dispositivo<sup>68</sup>.
- 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 del Plan de Tarifas señalado anteriormente. Si sus necesidades profesionales son significativamente diferentes a lo señalado en tal Plan de Tarifas, deberá ponerse en contacto con la <<U/OC>> competente del <<ORGANISMO>> para examinar las opciones disponibles.]
- e) Abstenerse de usar el dispositivo móvil para tratar o acceder a Información Clasificada.
- f) Utilizar sólo aquellos dispositivos aprobados o autorizados por el <<ORGANISMO>> para su conexión física con sistemas del <<ORGANISMO>>.
- g) El usuario deberá adquirir, a sus expensas, cualquier otro accesorio que no le fuere suministrado por el <<ORGANISMO>> y que, sin estar expresamente prohibido y con las cautelas precisas, pretendiera usar para propósitos no profesionales (por ejemplo: fundas, estuches, cargadores de coche, protectores de pantalla, auriculares Bluetooth, etc.)
- h) En caso de necesidad, almacenar en el dispositivo móvil aquella información de carácter personal estrictamente indispensable para el desarrollo de las funciones profesionales, procediendo a su borrado cuando ya no sea necesario su tratamiento. Los usuarios deberán recibir la aprobación por escrito de su supervisor antes de acceder, procesar, transmitir o almacenar información sensible tratada por el <<ORGANISMO>>, tal como datos de carácter personal.
- i) Disponer las medidas oportunas para evitar la puesta en compromiso, pérdida o robo del dispositivo móvil, especialmente durante los viajes o fuera de las dependencias del <<ORGANISMO>>.
- j) Contactar inmediatamente con la <<U/OC>> competente (Help-Desk) y el supervisor si el dispositivo no funciona adecuadamente, sufre daños, se pierde o es robado. En caso de robo o pérdida, el <<ORGANISMO>>, tras la notificación, procederá a bloquear y desactivar el dispositivo. Un dispositivo perdido o robado se reemplazará un máximo de <<x>> veces, dependiendo de la disponibilidad de los dispositivos.
- k) Cumplir con la legislación que resulte de aplicación en materia de uso de dispositivos móviles durante la conducción de vehículos a motor.
- l) El uso de los dispositivos móviles propiedad del <<ORGANISMO>> no otorga a sus usuarios el derecho a tener una expectativa de privacidad en todo momento, incluyendo el acceso a Internet, el correo electrónico o las comunicaciones de voz. En la medida en que los usuarios deseen mantener una absoluta privacidad, deberán evitar usar el dispositivo suministrado por el <<ORGANISMO>> más allá de un uso exclusivamente profesional. Al aceptar el dispositivo proporcionado por el <<ORGANISMO>>, los

<sup>67</sup> En general, se corresponderá con la tabla de permisos derivada del modelo contenido en el apartado 6 de la presente Guía.

<sup>68</sup> Véase Guía CCN-STIC 821 Normas de Seguridad en el ENS.



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.

Además de lo anterior, aquellos usuarios que hayan recibido un dispositivo móvil propiedad del <<ORGANISMO>>, deberán:

- a) Cumplir con la Normativa de Seguridad en el Uso de Dispositivos Móviles del <<ORGANISMO>>.
- b) No desactivar o alterar las características de seguridad del dispositivo.
- c) Usar el dispositivo propiedad del <<ORGANISMO>> para actividades profesionales o, limitadamente, para aquellas otras actividades privadas que estén autorizadas por el <<ORGANISMO>>.
- d) Asumir los costes de uso del dispositivo cuando se encuentren fuera de los límites establecidos previamente por el <<ORGANISMO>>, siempre que tales costes no hayan sido debidamente justificados y previamente aprobados (por ejemplo, los costes derivados de las llamadas personales en itinerancia).
- e) Asumir los costes del dispositivo móvil cuando sufre daños, se pierde o es robado por negligencia, mal uso o la acción voluntaria del usuario, sin perjuicio de las acciones disciplinarias, administrativas, civiles o penales a las que hubiere lugar.

## 6. Normas adicionales

- La <<U/OC>> del <<ORGANISMO>> es la unidad encargada de la supervisión, gestión del uso y control de gastos asociados al dispositivo.
- 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.
- [A la vista de las limitaciones impuestas por el antedicho Plan de Tarifas,] los usuarios, cuando se encuentren en su puesto de trabajo, deberán optar por usar el teléfono fijo para la realización o recepción de llamadas.
- El <<ORGANISMO>> permite a los usuarios un uso limitado de los recursos tecnológicos del <<ORGANISMO>> para propósito personal, siempre y cuando tal uso no interfiera en asuntos oficiales y no comporte gastos adicionales. [Indicar el tipo de llamadas, horarios, etc., que está permitido que hagan los usuarios usando los dispositivos móviles entregados por el <<ORGANISMO>>, señalando, si ello es necesario, días, horas, etc. Lo mismo cabe decir del uso de Internet con el dispositivo móvil]. En todo caso, el uso personal y limitado del dispositivo entregado por el <<ORGANISMO>> deberá respetar la “Normativa General de Uso de los Sistemas de Información del <<ORGANISMO>>” y la normativa de Seguridad Móvil que resultaran de aplicación.
- La selección de los dispositivos móviles se fundamentará en la disponibilidad señalada en los contratos suscritos con los fabricantes o distribuidores y en la necesidad de contar con los certificados de “productos seguros”, cuando ello sea preciso.
- La asistencia y soporte técnico será realizado por <<U/OC>> [incluyendo dirección, teléfono, etc.] que se constituye en el Help-Desk del <<ORGANISMO>> para incidencias relativas a los dispositivos móviles entregados por el <<ORGANISMO>> a los usuarios.
- Los servicios internacionales en itinerancia podrán estar disponibles de forma temporal sólo para viajes profesionales. El usuario deberá contactar con la <<U/OC>> competente, con 30 días de antelación al viaje, para concretar las características del roaming. De no hacerlo, el roaming internacional podría dar lugar a excesos de costes de los que el <<ORGANISMO>>, en principio, no se hace responsable.

- El <<ORGANISMO>> se reserva el derecho de retirar o desconectar el dispositivo móvil del usuario, cuando existan restricciones presupuestarias, modificaciones en las prioridades de implementación o alteraciones de la presente Normativa.
- Las preguntas relacionadas con la presente Normativa y sus Directrices se dirigirán a la <<U/OC>> del <<ORGANISMO>>.

### MODELO DE ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO

Todos los usuarios de dispositivos móviles del <<ORGANISMO>> deberán tener acceso permanente, durante el tiempo de desempeño de sus funciones, a la presente Normativa, debiendo suscribirla.

Mediante la cumplimentación de la siguiente declaración, el abajo firmante, [*personal del <<ORGANISMO>>/empleado de la <<EMPRESA>>*], 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 20\_\_>>

<b>Organismo:</b>	
<b>Trabajador (Nombre y Apellidos):</b>	
<b>DNI número:</b>	
<b>Número de Registro de Personal:</b>	
<b>Firmado:</b>	

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

DNI número: \_\_\_\_\_

Número de Registro de Personal: \_\_\_\_\_

## ANEXO D: REFERENCIAS

- Guía CCN-STIC 450 Seguridad de dispositivos móviles.
- Guía CCN-STIC 451 Seguridad de dispositivos móviles: Windows Mobile 6.1
- Guía CCN-STIC 452 Seguridad de dispositivos móviles: Windows Mobile 6.5
- Guía CCN-STIC 453 Seguridad de dispositivos móviles: Android 2.x
- Guía CCN-STIC 455 Seguridad de dispositivos móviles: iPhone.
- Guía CCN-STIC 801 Responsables y Funciones en el Esquema Nacional de Seguridad.
- Guía CCN-STIC 804 Medidas de implantación del Esquema Nacional de Seguridad.
- Guía CCN-STIC 805 Política de Seguridad de la Información.
- Guía CCN-STIC 807 Criptología de empleo en el Esquema Nacional de Seguridad.
- Guía CCN-STIC 813 Componentes certificados en el ENS.
- Guía CCN-STIC 817 Criterios comunes para la Gestión de Incidentes de Seguridad.
- Guía CCN-STIC 821 Normas de Seguridad en el ENS.
- Guía CCN-STIC 822 Procedimientos de Seguridad en el ENS.
- Guía CCN-STIC 823 Seguridad en entornos Cloud.
- ENISA: Consumerization of IT: Top Risks and Opportunities.
- ENISA: Consumerization of IT: Risk Mitigation Strategies.
- *NIST SP 800-124 Revision 1, Guidelines for Managing and Securing Mobile Devices in the Enterprise.*
- *NIST SP 800-114 Revision 1, User's Guide to Telework and Bring Your Own Device (BYOD) Security*
- *NIST SP 800-46 Revision 2), Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.*