seguridad+ Y CONFIANZA DIGITAL

Uso seguro de los dispositivos móviles

- ¿Qué se considera dispositivo móvil?
- Capacidades y funcionalidades
- Amenazas y vulnerabilidades de seguridad en dispositivos móviles
- Servicios de tarificación especial
- Para saber más...

El mejor sistema de seguridad eres tú

JUNTA DE ANDALUCIA

Introducción

El uso de teléfonos inteligentes, tabletas y dispositivos está cada vez más extendido, tanto en el entorno personal como en el profesional, dadas sus numerosas ventajas para comunicarnos, acceder a la información, interactuar, etc. Sin embargo, estas ventajas no están exentas de riesgos, ya que estos dispositivos pueden perderse o ser robados y, además, son vulnerables a amenazas derivadas de virus o ataques informáticos. En la presente guía ofrecemos una serie de **pautas y normas** que nos ayudarán a realizar un uso seguro de los dispositivos móviles protegiendo así nuestra información y archivos.

En el ámbito de la administración pública, la regulación del uso correcto de los recursos tecnológicos corporativos se establece como **uno de los controles fundamentales** definidos en 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 en su posterior modificación mediante Real Decreto 951/2015, de 23 de octubre. Asimismo, en el ámbito de la Administración de la Junta de Andalucía, los usuarios de dispositivos móviles están sometidos al **manual de comportamiento de los empleados públicos** en el uso de los sistemas informáticos y redes de comunicaciones de la administración de la Junta de Andalucía.

¿Son conscientes los usuarios finales de la amenaza real de seguridad existente con los dispositivos móviles?

A pesar de que los dispositivos móviles almacenan información sensible y se utilizan para comunicaciones personales relevantes, privadas y profesionales, el nivel de percepción de la amenaza de seguridad real existente no ha tenido la trascendencia necesaria en los usuarios y las organizaciones, y ello conlleva una mayor exposición a riesgos y, en consecuencia, a posibles incidentes de seguridad.

*La **Dirección y los Servicios de Informática o Departamentos** equivalentes promoverán la efectiva aplicación de unas **mínimas pautas y normas de uso seguro** de los dispositivos móviles, así como concienciar y formar al personal al servicio de la organización para que tome conciencia de los riesgos derivados de un uso incorrecto de estos recursos tecnológicos y adquiera una cultura de buenas prácticas en seguridad. Todo ello, sin perjuicio de la **responsabilidad individual de cada usuario** en el manejo adecuado de los terminales y la atención a las normas de uso establecidas.*

¿Qué se considera dispositivo móvil?

En esta guía, consideramos dispositivo móvil aquel de uso personal o profesional de **reducido tamaño**, que permite la **gestión de información** y el acceso a **redes de telecomunicaciones**, tanto de voz como de datos. Por ejemplo: teléfonos inteligentes, tabletas y libros electrónicos con acceso a Internet.

En principio, quedan fuera de este ámbito los ordenadores portátiles, aunque dada la cada vez más frecuente convergencia de tecnologías e hibridación de dispositivos, algunas de las recomendaciones propuestas, sobre todo las relativas a la conexión a redes de datos, pueden ser aplicables también a los ordenadores portátiles.

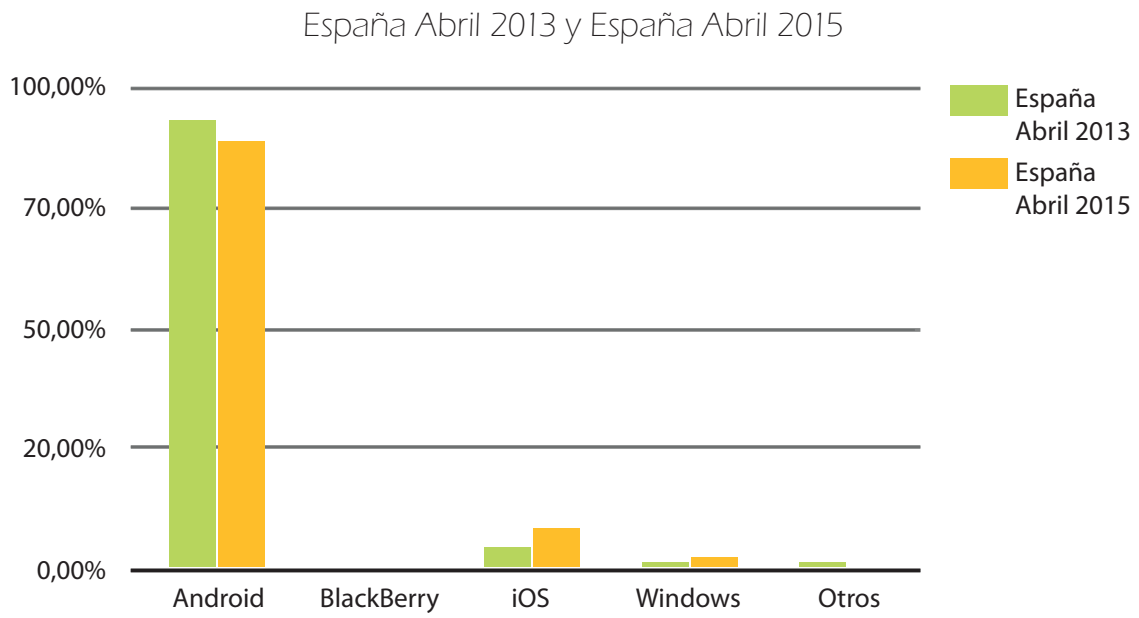
Capacidades y funcionalidades

Los dispositivos móviles, especialmente aquellos más avanzados disponibles en la actualidad, ofrecen capacidades y funcionalidades similares a las de otros dispositivos informáticos más tradicionales, como ordenadores portátiles, de sobremesa o estaciones de trabajo. En algunos casos, incluso superan a éstos al incluir elementos adicionales, como acelerómetros, GPS, cámara de fotos y vídeo, etc.

Las capacidades del dispositivo móvil vienen determinadas por el hardware y el software empleado. En cuanto al software, hay que tener en cuenta:

• El sistema operativo

El sistema operativo: actualmente imperan Andorid e iOS copando entre ambos más del 95% de la cuota de mercado[1]).



[1] Fuente: http://www.movilzona.es/2015/06/03/ios-android-windows-phone-datos-abril-kantar-worldpanel/

• El software y las aplicaciones disponibles para dicho sistema operativo

En función del software y aplicaciones disponibles, es posible lograr, por ejemplo, acceso a los servicios de telefonía (mensajes de texto y multimedia, voz y datos), acceso completo a redes de datos (redes privadas o Internet), incluyendo la gestión del correo electrónico, acceso a redes sociales, navegación web, mensajería instantánea, servicios de localización (mediante el GPS y las redes de datos), servicios de pago electrónico, acceso y edición de documentos, realización de presentaciones, etc.

Amenazas y vulnerabilidades de seguridad en dispositivos móviles

Existen numerosas amenazas y vulnerabilidades que ponen en riesgo la seguridad del dispositivo móvil y la información que gestiona. Existen algunas propias de este tipo de dispositivos y otras son compartidas con otros equipos como ordenadores de sobremesa o portátiles.

¿A qué pueden afectar las amenazas y.vulnerabilidades? Pueden afectar a la:

- **Disponibilidad:** incidentes que impidan acceder a la información y a los archivos, pérdidas y robos.
- **Confidencialidad:** sustracción de información almacenada y enviada o recibida por el dispositivo.
- **Autenticidad:** suplantación del propietario.

En general, las principales amenazas ligadas a estos dispositivos se pueden relacionar con deficiencias o malos usos en alguno de los siguientes aspectos: pantalla de bloqueo, mecanismos de comunicación, software empleado y nivel de mantenimiento.

A continuación, se exponen algunas de las principales amenazas asociadas a los dispositivos móviles:

• Acceso no autorizado al terminal o a la información almacenada

Se trata de una de las principales amenazas de seguridad y se puede producir por disponer de acceso físico al dispositivo (de forma temporal o permanente) o por disponer de acceso remoto al terminal a través de la vulnerabilidad de alguno de sus componentes o mediante una aplicación previamente instalada.

¿A qué datos pueden acceder?:

- Credenciales de acceso a servicios web.
- Cuentas de correo electrónicos.
- Mensajes de correo y del teléfono.
- Información de llamadas de telefonía y VoIP.
- Documentos privados y confidenciales: vídeos, fotografías, grabaciones, etc.
- Agenda de contactos.
- Calendario.

Existe el riesgo de que el dispositivo móvil se pierda o sea robado, lo que puede provocar pérdidas económicas asociadas no sólo al valor terminal, sino a la información que contiene. Pero también es posible acceder a dichos terminales con la instalación de software de espionaje encubierto o malicioso que suele permanecer oculto en el dispositivo, indetectable, realizando la función para la que ha sido diseñado. Existe software comercial de espionaje, orientado fundamentalmente a monitorizar a otras personas, que puede ser utilizado por un atacante. Con este tipo de software se puede acceder a la lista de llamadas y mensajes enviados y recibidos, recibir notificaciones sobre la actividad del dispositivo, interceptar llamadas, etc.

• *Vulnerabilidades propias del sistema operativo del dispositivo*

Los fabricantes de sistemas operativos detectan periódicamente vulnerabilidades de seguridad asociadas a los componentes y librerías básicas del sistema, por lo que es conveniente actualizar de forma frecuente el sistema operativo para incorporar las últimas actualizaciones de seguridad. Este tipo de vulnerabilidades han sido empleadas en el pasado por atacantes y código dañino para disponer de acceso completo al dispositivo mediante la ejecución de código, la realización de ataques de denegación de servicio, o el robo de información.

• *Diversidad de mecanismos de comunicación de los dispositivos móviles.*

El dispositivo móvil dispone de diferentes interfaces de comunicación, tanto físicas (a través de la conexión por cable a un ordenador), como por radiofrecuencia (Wifi, 2G/3G/4G, Bluetooth, GPS) y algunas de éstas posibilitan el acceso a Internet (TCP/IP) y la navegación web. Existen actualmente nuevos vectores de ataque que aprovechan estos mecanismos de comunicación. Además, las posibilidades de comunicación simultánea de los dispositivos con diferentes redes, como por ejemplo Internet y una red de datos privada, hace que los terminales actúen de pasarela entre diferentes infraestructuras, lo que facilita la realización de ataques y la propagación de código dañino entre entornos diferentes.

Las múltiples posibilidades de conexión de este tipo de dispositivos, tanto a redes privadas como públicas, facilita la realización de ataques directos contra los mismos sin necesidad de tener que evitar controles de seguridad corporativos como cortafuegos perimetrales o sistemas de detección de intrusos. Dichos ataques son comunes cuando el usuario se conecta a WiFis abiertas en emplazamientos públicos, donde las cuestiones de seguridad pueden no estar cuidadas.

• Localización física de los usuarios

La disponibilidad de GPS en la mayoría de dispositivos móviles facilita la creación y utilización de nuevos servicios basados en la geolocalización, lo que puede tener implicaciones directas en la privacidad del usuario en caso de que el atacante quiera obtener información detallada de su ubicación en todo momento. Además, existen aplicaciones sociales basadas en la localización que suponen un riesgo de privacidad, ya que los datos son procesados para ofrecer servicios y un atacante podría acceder a ellos.

• Aplicaciones cliente vulnerables y software dañino

Las aplicaciones (apps) facilitan al usuario el acceso a servicios de manera ágil y cómoda, pero tiene asociada una serie de riesgos y amenazas de seguridad: robo de identidad, revelación de información corporativa sensible, localización física del usuario, distribución de malware a través de la red social, etc.

Cabe destacar, la amenaza de ser víctima de fraude con impacto económico en el caso de aquellos servicios que implican transacciones económicas.

¿Cómo se materializan estas amenazas? Normalmente, a través de aplicaciones que presentan alguna vulnerabilidad y son infectadas con software malicioso o mediante ingeniería social, que es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos.

• Amenazas y vulnerabilidades multiplataforma

Habitualmente, conectamos los dispositivos móviles a los ordenadores portátiles y de sobremesa para realizar la sincronización de los datos compartidos entre ambos o para transferir cualquier tipo de información. En estos casos, existe el riesgo de que código dañino residente en el dispositivo sea transferido e infecte al equipo al que se ha conectado. Esto abre nuevas vías para penetrar el perímetro de seguridad de las organizaciones, que es vulnerado cuando el usuario conecta su terminal al ordenador ubicado en redes internas.

Algunos consejos

Es aconsejable que el servicio de informática o departamento responsable de la seguridad establezca instrucciones y recomendaciones de seguridad corporativas en lo referente al uso de dispositivos móviles, garantizando el cumplimiento de la normativa establecida y el uso adecuado de los dispositivos móviles profesionales.

Las normas y recomendaciones de uso deberían tener en cuenta las siguientes cuestiones:

• Grado de sensibilidad y confidencialidad de la información

Es fundamental analizar y evaluar el tipo de información almacenada en el dispositivo móvil, no siendo recomendable almacenar o intercambiar, sin las debidas medidas de seguridad, información confidencial o sensible, como documentos clasificados, datos de cuentas, contraseñas, PINs de acceso a otros servicios, especialmente si están relacionados con la Administración de la Junta de Andalucía.

Conviene recordar que: **‘‘No se pierde ni se puede robar la información que no está’’**. Cuando sea necesario almacenar información en el dispositivo, conviene plantearse la opción de cifrar la información más sensible. Finalmente, se recomienda realizar un borrado seguro de la información contenida en los dispositivos y sus elementos (ej. tarjetas de memoria) una vez finalizado su ciclo de vida con un usuario determinado.

• Centralización de la gestión del parque de dispositivos móviles

Los servicios de informática o departamentos equivalentes pueden realizar un maquetado homogéneo de los terminales de forma previa a la entrega a los usuarios. Las aplicaciones base instaladas por defecto serán las mínimas necesarias para garantizar la funcionalidad del terminal como herramienta de trabajo y la configuración por defecto de los dispositivos deberá ser más segura que la original de fábrica. En este sentido, una herramienta que permita una gestión centralizada del parque de dispositivos móviles puede resultar de gran ayuda.

• Proteger el acceso físico a los dispositivos y a su funcionalidad

Evitar en lo posible dejar el dispositivo móvil desatendido, ya que un potencial atacante sólo necesita unos segundos para instalar un programa malicioso o comprometer la seguridad del terminal o tarjeta SIM.

El objetivo es dificultar el acceso físico al mismo de forma temporal o permanente (pérdida o robo) a un tercero.

También se recomienda restringir al máximo las acciones que pueda realizar un tercero con acceso físico al teléfono, de modo que únicamente el dueño del mismo sea capaz de usarlo. Para ello, se recomienda:

- Utilizar algún tipo de bloqueo para el acceso al dispositivo, ya sea mediante patrón, PIN o contraseña, así como configurar los dispositivos para que se bloqueen automáticamente transcurrido un determinado período de tiempo de inactividad.
- Establecer un PIN en la tarjeta SIM nos ayudará a restringir la posibilidad de hacer uso de llamadas, mensajería SMS y MMS, y de comunicaciones de datos a través de la red móvil.
- Desactivar configuraciones por defecto que permitan, aun estando la pantalla bloqueada, el acceso a funciones de reconocimiento de voz, a funciones de configuración y control del dispositivo, así como la previsualización de notificaciones (esto aplica especialmente en dispositivos con IOS).
- Evaluar los riesgos de la elevación de privilegios. Es necesario recalcar que la elevación de privilegios (rooteo/jailbreak) conlleva riesgos, ya que, aunque este proceso ofrece al usuario la posibilidad de instalar aplicaciones, modificaciones y componentes del sistema no proporcionados a través de repositorios oficiales, los dispositivos así alterados ignoran el modelo de seguridad impuesto por el fabricante del sistema operativo, exponiendo potencialmente a los usuarios a código dañino que podría tomar control completo del terminal.

• Configurar de modo seguro los mecanismos de comunicación del dispositivo

El dispositivo móvil dispone de diferentes interfaces de comunicación, tanto físicas (conexión por cable a un ordenador) como por radiofrecuencia (Wifi, 2G/3G/4G, Bluetooth, GPS). Conviene configurar de manera segura cada una de estas conexiones para que la exposición de nuestra privacidad sea la menor posible.

En este sentido, conviene contemplar varios aspectos:

- **Localización.** Se recomienda activar únicamente la localización mediante GPS, no las que se realizan mediante Wifi o redes de telefonía móvil. Asimismo, no se recomienda hacer uso de los informes de ubicación ni del historial de ubicaciones. Si existe el historial de ubicaciones, debe ser eliminado.
- **Bluetooth y wifi.** Conviene no activar el interfaz inalámbrico Bluetooth o Wifi si no se está haciendo uso de ellos, evitando así la posibilidad de ataques específicos sobre estos canales de comunicación.
- **Conexión mediante USB.** Sólo debemos conectar nuestro dispositivo móvil mediante USB a otros equipos de confianza, nunca a equipos públicos o de terceros. Debemos evitar los riesgos que conlleva: infección por código dañino, filtración de datos, etc.
- **Anclaje a red (tethering).** Cuando un dispositivo móvil, con conexión a Internet, sea usado como pasarela para ofrecer acceso WiFi a otros dispositivos, es aconsejable establecer una cierta configuración de seguridad en el punto de acceso creado en el terminal. En Android suele estar activado por defecto.
- **Conexión a redes de datos móviles.** Es recomendable configurar el APN corporativo de la Junta de Andalucía para la conexión a la red de datos en movilidad, pues permite la conectividad con los sistemas y recursos internos del Organismo, al tiempo que garantiza la protección del tráfico y la consiguiente capacidad para la detección automatizada de incidentes de seguridad por parte de AndalucíaCERT.

• Instalación y actualización de aplicaciones

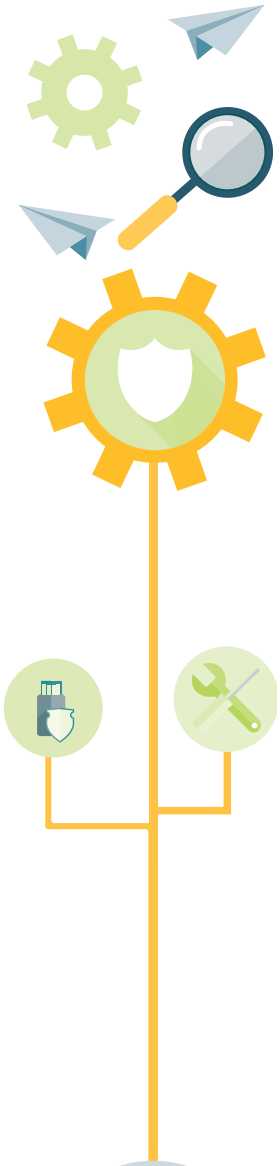
Siempre debemos instalar y utilizar software y aplicaciones seguras. Veamos algunas recomendaciones:

- **Instalación de nuevas aplicaciones.** Cuando instalamos una nueva aplicación, siempre descargadas de las tiendas oficiales (Google Play, Apple Store,...) debemos desconfiar de aquellas que requieren demasiados permisos o permisos sospechosos no relacionados con la funcionalidad de la aplicación. En el caso de los dispositivos con sistema operativo iOS es posible restringir los permisos de las aplicaciones, pero no ocurre así en los que funcionan con sistema operativo Android.
- **Actualización de aplicaciones ya instaladas.** Cuando queremos actualizar aplicaciones a la última versión disponible, algo recomendado porque corrigen posibles fallos de seguridad, las recomendaciones varían según el sistema operativo:
    - **Android.** Se recomienda, a pesar de ser más incómodo para el usuario, no habilitar la opción de actualizaciones automáticas y actualizarlas de forma manual forzando así al usuario a revisar los nuevos permisos solicitados por cada una de las actualizaciones recibidas cada una de las diferentes aplicaciones instaladas en el terminal.
    - **iOS.** Se recomiendan las actualizaciones automáticas.
- **Configuración segura de las aplicaciones.** Revisar qué opciones móviles pueden ser vulnerables. Por ejemplo, en dispositivos Android se debe configurar adecuadamente las aplicaciones Hangout y mensajería para mitigar la vulnerabilidad Stagefright[2] y para preservar la intimidad del usuario.
- **Mantener actualizadas las utilidades de configuración y sincronización con otros dispositivos locales.** Los propios fabricantes de los dispositivos suelen proporcionar herramientas para realizar la sincronización y las copias de seguridad entre el dispositivo y un ordenador/portátil local. Para evitar problemas de seguridad, es necesario que este software esté actualizado a su última versión disponible.
- **Servicios avanzados.** En líneas generales, debemos sopesar las ventajas de ciertos servicios avanzados frente a la renuncia a nuestra privacidad y seguridad. Cada vez surgen más aplicaciones móviles que funcionan en segundo plano y hacen uso de los servicios de ubicación, los datos del calendario del usuario, de sus búsquedas web (incluyendo el historial web) y de otros datos del usuario. Desde el punto de vista de seguridad y privacidad, salvo que existan motivaciones específicas que lo justifiquen, se recomienda no activar este tipo de funcionalidades o servicios. Un ejemplo de esto, entre otros, sería el de Google Now.

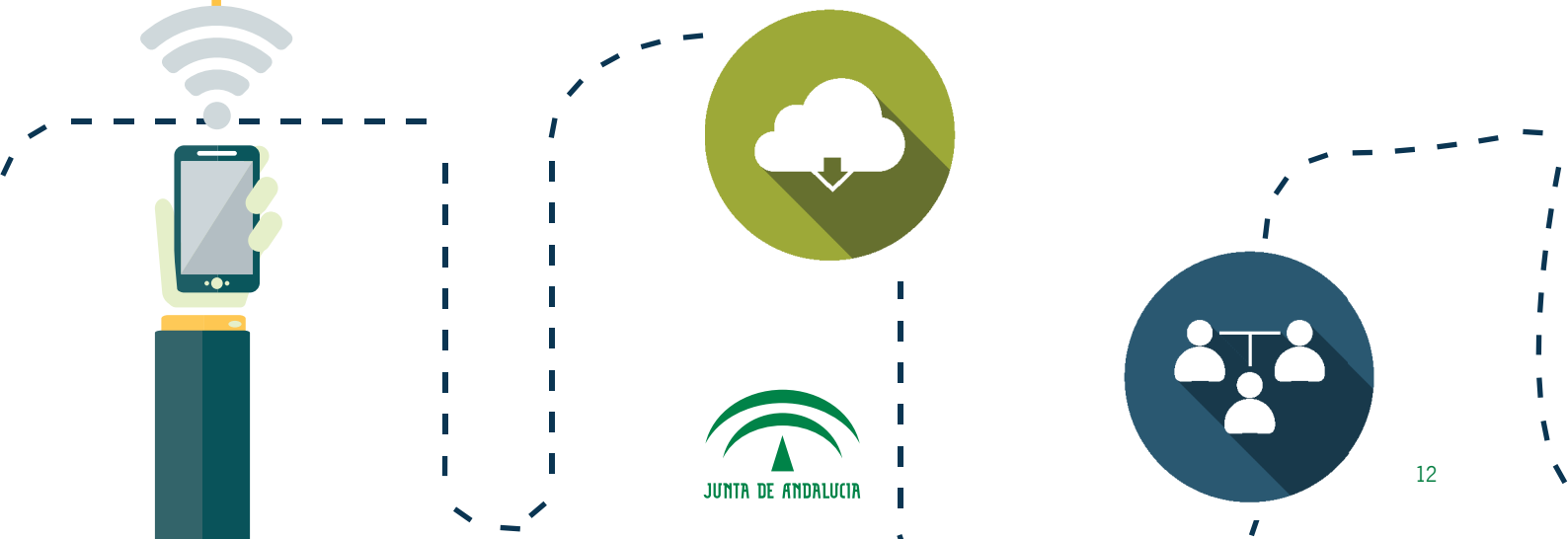
[2] Fuente: http://globbsecurity.com/consejos-stagefright-android-35421/

• Mantenimiento adecuado del dispositivo

Junto con todas las medidas y recomendaciones de seguridad descritas anteriormente, es importante realizar un correcto mantenimiento del dispositivo, ya que condiciona fuertemente su nivel de seguridad. Aspectos a tener en cuenta:



- **Firmware.** Es crítico actualizar el firmware del dispositivo a la última versión de sistema operativo disponible y soportada por el fabricante, con el objetivo de solucionar todas las vulnerabilidades de seguridad públicamente conocidas. Para facilitar esto, los fabricantes lanzan periódicamente actualizaciones del software del dispositivo con el fin de introducir nuevas características y parchear los fallos de seguridad que hayan sido identificados hasta esa fecha.
- **Copias de seguridad de información y configuración.** Para prevenir cualquier tipo de pérdida de información en nuestros dispositivos es muy recomendable realizar copias de respaldo. Los propios fabricantes de los dispositivos suelen proporcionar herramientas para realizar una copia de seguridad. En unos casos, se trata de un software que puede ser instalado en un ordenador de sobremesa o portátil (copias de seguridad locales) para la sincronización y realización de copias de seguridad entre el dispositivo y el ordenador (ej. iTunes para dispositivos con iOS). Asimismo, existen servicios que permiten la realización de copias de seguridad "en la nube" y la sincronización de los datos de los dispositivos móviles (ej. iCloud para dispositivos con iOS, Google Sync Services para dispositivos con Android). Por cuestiones de privacidad se recomienda no utilizar las alternativas basadas en copias de seguridad "en la nube" y, en su lugar, realizar copias de seguridad locales, preferentemente con la opción cifrado de la copia activada y una contraseña robusta.
- **Software antivirus.** Dado que el número y la peligrosidad del código dañino especialmente diseñado para dispositivos móviles es cada vez mayor, es necesaria la instalación de software antivirus en los dispositivos.



Servicios de tarificación especial

Uno de los principales negocios en el sector de las telecomunicaciones es el de los servicios de tarificación adicional, donde a las ya históricas líneas 800 se han sumado en los últimos años los 905 y los mensajes cortos (SMS) y mensajes multimedia (MMS). Debemos tener en cuenta que en los servicios de tarificación especial intervienen dos empresas: por un lado, la empresa con la que los consumidores tienen contratado el servicio de telecomunicaciones y, por otro lado, la empresa prestadora del servicio de tarificación adicional, que cobra una cantidad independiente por la supuesta prestación de un servicio adicional.

• *Las líneas 800*

Las líneas 800 se clasifican en función del tipo de contenidos proporcionados por la empresa prestadora del servicio. Así, existen los siguientes prefijos:

- **803** para servicios exclusivos de adultos.
- **806** para servicios de ocio y entretenimiento.
- **807** para servicios profesionales.

En relación a dichos servicios existe un ***código de conducta*** que se encarga de proteger los derechos de los consumidores. Algunas de las regulaciones fijadas por este código de conducta son:

- Deber del prestador de servicios de informar al usuario el precio máximo por minuto de la llamada, tanto desde la red fija, como desde la red móvil. Dicha información deberá presentarse exhibiendo el precio por minuto, impuestos incluidos, de manera que no requiera mayor indagación por parte de los usuarios.
- Inmediatamente después de descolgar la llamada, deber de informar al usuario del precio máximo por minuto (fijo y móvil), de la información genérica sobre el servicio que se ofrece y de si éste se dirige a mayores de 18 años.
- Obligación de que las bases de los concursos o sorteos, así como la resolución de los mismos, deberán estar depositadas ante un notario u organismo público competente.
- Prohibición de que los servicios prestados tengan una duración superior a treinta minutos.
- Prohibición de que los servicios destinados a solicitar u ofrecer empleo o trabajo, directa o indirectamente, ya sea remunerado o sin remunerar, se puedan ofrecer a través de números de tarificación adicional.

Asimismo, se establece la creación de una ***Comisión de Supervisión de los Servicios Telefónicos de Tarificación Adicional***, integrada en el Ministerio de Industria, Turismo y Comercio, que se encarga de velar por el cumplimiento de dicho código de conducta.

• Números 905

Los números con prefijo 905 corresponden a líneas utilizadas especialmente para la celebración de ***concursos televisivos,*** a los que el usuario puede llamar, bien para votar al participante en un determinado programa, bien para intentar concursar en un juego de pregunta/respuesta.

El número que sigue al 905 determina cuál es la modalidad del servicio, así como el precio del mismo, diferenciándose principalmente entre las modalidades de voz (***"entretenimiento y usos profesionales"***) por un lado y "televoto", por otro.

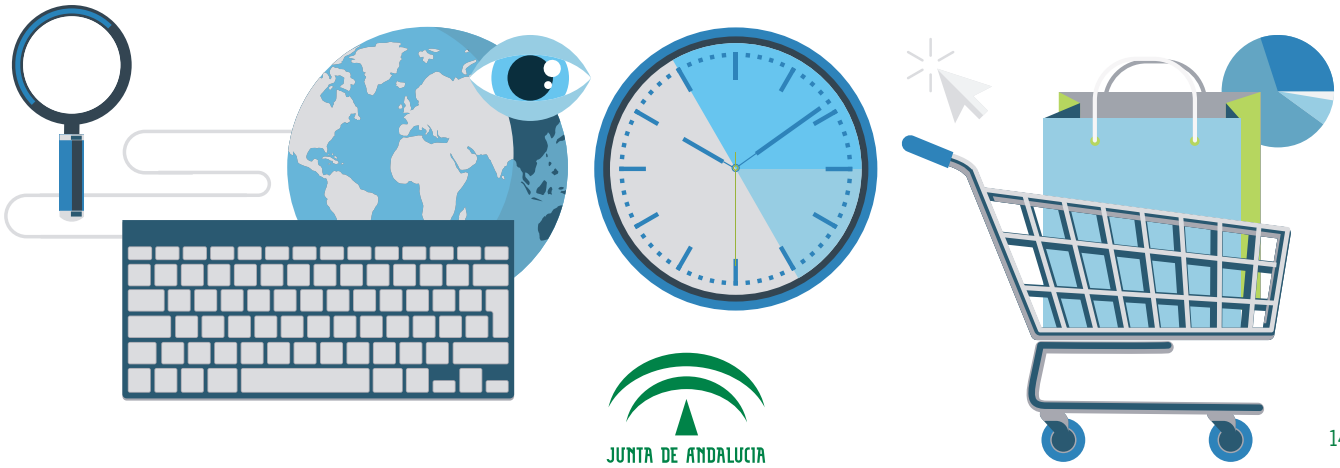
- Para las modalidades de servicios de voz ("entretenimiento y usos profesionales"), el operador de servicio de tarificación adicional deberá garantizar que se informa al usuario, al inicio de la comunicación, mediante una locución, del precio de la llamada del servicio a recibir.
- Para la modalidad de "**televoto**", el operador del servicio de tarificación adicional garantizará que se proporcione al usuario una locución informativa con el nombre o denominación social del prestador del servicio de "televoto", la confirmación de que el voto ha sido contabilizado y el precio del servicio recibido.

• Números 905

Al igual que ocurre con las llamadas, también existen mensajes de tarificación adicional, los cuales son definidos por la legislación como aquellos servicios de telecomunicaciones que supongan el pago por los consumidores, de forma inmediata o diferida, de una retribución añadida al precio de envío de mensajes, en concepto de remuneración por la prestación de algún servicio de información, entretenimiento u otros.

Dentro de este tipo de mensajes cabe prestar especial atención a los denominados **servicios desuscripción** y a las **descargas de melodías**.

- Los **servicios de suscripción** son aquellos que consisten en el envío de determinados mensajes por parte del operador al usuario abonado, bien de forma periódica, bien cuando se produzcan determinados sucesos. Cada mensaje recibido supone un coste, por lo que la factura mensual puede oscilar entre 15 y 25 euros (43·65 SMS mensuales). A lo que hay que sumar el importe de cada una de las conexiones a Internet necesarias para descargar los archivos recibidos.
- Del mismo modo, **descargar melodías** también implica gastos adicionales. El usuario tiene que enviar un SMS y, posteriormente, efectuar una conexión a Internet desde el móvil para acceder al enlace y poder recibir el archivo en su terminal.



seguridad+ Y CONFIANZA DIGITAL

Uso seguro de los dispositivos móviles

Para saber más...

- Guías del Centro Criptológico Nacional: https://www.ccn-cert.cni.es
- Servicio de Gestión de Dispositivos Móviles de la Red Corporativa de Telecomunicaciones https://ovctic.i-administracion.junta-andalucia.es/node/3307
- http://www.minetur.gob.es/telecomunicaciones/es-ES/SecretariaDeEstado/Consejos/Paginas/ComisionSupervision.aspx
- CCN-STIC 450 Seguridad en dispositivos móviles.
- CCN-STIC 453A Seguridad en Android 2.x.
- CCN-STIC 453B Seguridad en Android 4.x.
- CCN-STIC 454 Seguridad en iPad.
- CCN-STIC 455 Seguridad en iPhone.
- CCN-CERT IA-28/15.

El mejor sistema de seguridad eres tú

JUNTA DE ANDALUCIA

Más info en: www.andaluciacert.es