GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Estudio sobre seguridad en dispositivos móviles y smartphones

1er Cuatrimestre 2012 (9ª oleada)

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN

Edición: Diciembre 2012

El "Estudio sobre seguridad en dispositivos móviles y smartphones" (1er Cuatrimestre 2012) ha sido elaborado por el siguiente equipo de trabajo del Instituto Nacional de Tecnologías de la Comunicación:

Pablo Pérez San-José (dirección)

Eduardo Álvarez Alonso (coordinación)

Susana de la Fuente Rodríguez

Cristina Gutiérrez Borge

INTECO quiere señalar la participación en la realización del trabajo de campo e investigación de este estudio de:

ÍNDICE

PUNTOS CLAVE

El Instituto Nacional de Tecnologías de la Comunicación presenta el *Estudio sobre seguridad en dispositivos móviles y smartphones (1er cuatrimestre 2012)*. Para elaborar el análisis se han realizado 3.607 entrevistas online entre los meses de febrero y abril de 2012.

El estudio ofrece un diagnóstico de la utilización de dispositivos móviles y smartphones por parte de los internautas españoles. En concreto, se estudian los hábitos de uso, las herramientas y buenas prácticas de seguridad adoptadas y las incidencias de seguridad declaradas por los usuarios en las comunicaciones móviles. A continuación se exponen los puntos clave del estudio.

I. SEGURIDAD DE LAS COMUNICACIONES DE LA TELEFONÍA MÓVIL

A principios de 2012 casi la totalidad de usuarios disponen de un teléfono móvil y aquellos que posen un smartphone superan ya el 60%.

- En este primer cuatrimestre, un 60,8% de los usuarios con teléfono móvil encuestados dispone de un smartphone, confirmando la tendencia ascendente de este tipo de terminales (aumento de más de 4 puntos porcentuales).

II. HÁBITOS DE USO DEL TELÉFONO MÓVIL

Casi el 70% de quienes disponen de bluetooth toma las medidas necesarias y lo enciende sólo cuando lo necesita o lo mantiene oculto. Además, los panelistas aprovechan al máximo las prestaciones que incorporan los terminales accediendo al correo electrónico a través del teléfono y descargando aplicaciones, utilizando más estas opciones quienes tienen un smartphone. Todos estos usos se incrementan de manera global en este cuatrimestre.

- Desciende más de 3 puntos porcentuales con respecto al cuatrimestre anterior (13,2%) el número de panelistas que mantiene el bluetooth siempre encendido y visible, probándose la tendencia a la baja y la concienciación de los usuarios.

- El acceso al correo aumenta ostensiblemente, más de 5 puntos porcentuales (55,9%), e igualmente sucede con la descarga de aplicaciones, cerca de 6 puntos porcentuales (56,4%) con respecto al anterior estudio. En ambos casos estos porcentajes son mucho mayores entre quienes tienen un smartphone (71.0% frente al 11% y 72,5% frente al 8,3% respectivamente).

- Las descargas de aplicaciones siguen realizándose principalmente desde sitios oficiales, 95,5% de los casos, y se mantiene el alto número de usuarios que utilizan geolocalización en sus aplicaciones, un 64,2%.

III. MEDIDAS DE SEGURIDAD UTILIZADAS EN EL TELÉFONO MÓVIL

Se incrementa sustancialmente el uso de antivirus en los móviles así como el uso de contraseña tras la inactividad. Los usuarios de smartphones ponen en práctica más medidas de seguridad

- Se mantiene estable el alto grado de utilización del PIN (84,4%) como principal medida de seguridad en el móvil. Aumenta el uso de contraseñas o patrones de bloqueo tras la actividad, superando el 21%, así como el uso de antivirus (10,7%), que aumenta sustancialmente con respecto al cuatrimestre anterior.

- Todas las medidas son más utilizadas por quienes tienen un smartphone frente a quien usa un teléfono convencional, especialmente en el caso de los antivirus (16,3% frente a 1,3%).

IV. INCIDENTES DE SEGURIDAD

El incidente de seguridad más declarado por los usuarios españoles es el extravío del terminal, seguido del robo del mismo y de la infección por virus o malware. El fraude se reduce hasta tan solo un 2% de los casos.

- Descenso de cerca 3 puntos porcentuales (15,5%) del intento de fraude telefónico. Se mantiene bajo el número de incidentes, tanto extravío (12,4%) como robo (11,0%) descendiendo ligeramente con respecto a anteriores encuestas.

- La recepción de mensajes cortos de texto que ofrecen servicios que el usuario no ha requerido, desciende más de 2 puntos porcentuales (9,3%), al igual que SMS pidiendo que se visite una página web sospechosa de ser fraudulenta (7,2%). Desciende también la solicitud de claves de usuario o información personal, ya sea mediante mensaje (2,5%) o llamada telefónica (3,2%).

- A inicio de 2012, sólo un 2% de los usuarios declara haber sufrido un perjuicio económico.

- La cantidad media defraudada en ese 2% de casos en que existe un perjuicio económico se sitúa en los 129,89 €. Esta cantidad oscila ampliamente según el tipo de terminal que utilice el usuario (164,28 € entre quienes utilizan smartphones y 80,64 € entre quienes utilizan terminales convencionales). A pesar de estas cifras solamente 1 de cada 4 casos supone pérdidas superiores a los 50 euros.

1 INTRODUCCIÓN Y OBJETIVOS

1.1 PRESENTACIÓN

El Instituto Nacional de Tecnologías de la Comunicación, S.A. (INTECO), es una sociedad estatal adscrita al Ministerio de Industria, Energía y Turismo a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.

La misión de INTECO es reforzar la ciberseguridad, la privacidad y la confianza en los servicios de la Sociedad de la Información, aportando valor a los ciudadanos, empresas, AA.PP. y al sector TIC, y coordinando esfuerzos con los organismos nacionales e internacionales que trabajan en esta materia.

Es uno de los objetivos del Instituto describir de manera detallada y sistemática el nivel de seguridad, privacidad y confianza en la Sociedad de la Información y de generar conocimiento especializado en la materia. De este modo, se encuentra al servicio de los ciudadanos, las empresas y las administraciones públicas españolas para describir, analizar, asesorar y difundir la cultura de la seguridad de la información, la privacidad y la e-confianza.

INTECO, a través de su Observatorio de la Seguridad de la Información, ha diseñado un Plan de Actividades y Estudios con el objeto de producir conocimiento especializado y útil en materia de seguridad y privacidad, así como de elaborar recomendaciones y propuestas que definan tendencias válidas para la toma de decisiones futuras por parte de los poderes públicos.

Dentro de este plan de acción se realizan labores de investigación, análisis, estudio, asesoramiento y divulgación que atenderán, entre otras, a las siguientes estrategias:

- Elaboración de estudios e informes propios en materia de seguridad de la información, privacidad y e-confianza.
- Seguimiento de los principales indicadores y políticas públicas relacionadas con la seguridad de la información y la confianza en el ámbito nacional e internacional.
- Generación de una base de datos que permita el análisis y evaluación de la seguridad, la privacidad y la e-confianza con una perspectiva temporal.
- Difusión de estudios e informes publicados por otras entidades y organismos nacionales e internacionales, así como de información sobre la actualidad nacional y europea en materia de la seguridad y privacidad

- Asesoramiento a las Administraciones Públicas en materia de seguridad de la información, privacidad y confianza, así como el apoyo a la elaboración, seguimiento y evaluación de políticas públicas en este ámbito.

1.2 ESTUDIO SOBRE SEGURIDAD EN DISPOSITIVOS MÓVILES Y SMARTPHONES

El *Estudio sobre seguridad en dispositivos móviles y smartphones* tiene como objetivo general realizar un diagnóstico evolutivo del uso que los internautas españoles realizan de los dispositivos móviles y smartphones, así como las medidas de seguridad utilizadas y los incidentes sufridos. El presente informe constituye la 9ª entrega de una serie de informes periódicos.

Se sigue así la línea iniciada con otras publicaciones como:

- *Estudio sobre la situación de seguridad y buenas prácticas en dispositivos móviles y redes inalámbricas*.
- *Estudio sobre seguridad y privacidad en el uso de los servicios móviles por los menores españoles*.
- *Estudio sobre hábitos seguros en el uso de smartphones por los niños y adolescentes españoles*.
- *Guía para proteger y usar de forma su móvil*.

En esta ocasión, se presenta el informe referente al 1er cuatrimestre de 2012, basado en las encuestas realizadas en dicho periodo de tiempo a través de un panel online.

2 DISEÑO METODOLÓGICO

El *Estudio sobre seguridad de los dispositivos móviles y smartphones (1er cuatrimestre de 2012)* se realiza a partir de una metodología cuantitativa, aplicando un cuestionario online auto-administrado a un panel dedicado compuesto por hogares con conexión a Internet repartidos por todo el territorio nacional.

En la definición de la metodología del estudio, se ha considerado una fórmula que permita obtener información con una perspectiva evolutiva. La necesidad de unos datos robustos sobre los mismos hogares y usuarios en diferentes momentos del tiempo hace que el panel online dedicado resulte la metodología idónea para satisfacer los objetivos del proyecto.

El panel posibilita la realización de entrevistas periódicas acerca de la seguridad de la información en los dispositivos móviles y smartphones de los usuarios españoles y ofrece, por tanto, una perspectiva evolutiva de la situación. Se realizan entrevistas online a mayores de 15 años con acceso frecuente a Internet desde el hogar, estas entrevistas se llevan a cabo con una periodicidad cuatrimestral. Los datos extraídos de la encuesta permiten obtener la percepción sobre la situación de la seguridad de la información en los dispositivos móviles y smartphones de los usuarios españoles.

El presente informe constituye la novena entrega del estudio.

2.1 UNIVERSO

Usuarios de Internet mayores de 15 años, residentes en España y que acceden a Internet desde el hogar y tienen teléfono móvil. Para delimitar con mayor precisión el concepto de usuario, se exige una conexión a Internet desde el hogar de, al menos, una vez al mes.

2.2 TAMAÑO Y DISTRIBUCIÓN MUESTRAL

El tamaño muestral engloba a todos los miembros del panel online que han respondido a la encuesta realizada entre los meses de febrero y abril de 2012.

Para corregir las posibles diferencias en la distribución muestral obtenida y la distribución real del universo se ha aplicado una ponderación que otorga un peso específico a cada caso. Este peso es definido en función de diferentes variables socio-demográficas. De este modo, la muestra obtenida se asimila a la muestra que, en un caso ideal, representaría fielmente a la población internauta en España. Los datos de referencia para esta ponderación son los publicados por el Instituto Nacional de Estadística (INE)[1].

[1] Datos obtenidos de la Encuesta sobre Equipamiento y Uso de Tecnologías de la Información y Comunicación en los hogares 2011, INE.

Para esta ponderación se han tenido en cuenta 8 variables: sexo, edad, Comunidad Autónoma de residencia, tamaño del hábitat/municipio de residencia, tamaño del hogar según número de miembros, nacionalidad, nivel de estudios y situación laboral.

El amplio tamaño muestral permite que las diferencias respecto a la distribución real se reduzcan considerablemente. La Tabla 1 presenta el tamaño de la muestra correspondiente a la encuesta.

2.3 TRABAJO DE CAMPO Y ERROR MUESTRAL

El trabajo de campo ha sido realizado entre enero y abril de 2012 mediante entrevistas online a partir de un panel de usuarios de Internet.

De acuerdo con los criterios del muestreo aleatorio simple para variables dicotómicas en las que p=q=0,5 y para un nivel de confianza del 95,5%, se establece un error muestral inferior o igual a ±1,67% para el periodo analizado, no habiéndose superado el 2,05% en los anteriores períodos analizados, tal y como se recoge en la siguiente tabla.

Tabla 1: Tamaños y errores muestrales de las encuestas[2]

Período	Tamaño muestral	Error muestral
4º trimestre 2009	3.563	±1,68%
1er trimestre 2010	3.524	±1,68%
2º trimestre 2010	3.446	±1,70%
3er trimestre 2010	3.461	±1,70%
4º trimestre 2010	3.486	±1,69%
2º cuatrimestre 2011	2.376	±2,05%
3er cuatrimestre 2011	3.597	±1,67%
1er cuatrimestre 2012	3.607	±1,67%

Fuente: INTECO

Es necesario remarcar que la muestra utilizada no consiste en usuarios de telefonía móvil, sino que se limita a usuarios de Internet desde el hogar que a su vez tienen teléfono móvil. Este matiz puede contar con determinadas implicaciones, ya que se trata de una muestra que se encuentra habituada al uso de Internet frente al conjunto de usuarios de telefonía online que no necesariamente estarían habituados a este medio ni tan siquiera implicaría que lo utilizasen.

[2] Se señala el tamaño muestral considerando los usuarios de teléfono móvil, si bien el panel online cuenta con un tamaño ligeramente superior, y por tanto un error muestral ligeramente inferior, al estar incluidos en él algunos usuarios de Internet que no cuentan con teléfono móvil. Estas diferencias son mínimas debido al escaso número de panelistas que no cuentan con teléfono móvil, por ejemplo en el 1er cuatrimestre de 2012 solamente 39 usuarios no contaban con este tipo de dispositivos.

3 SEGURIDAD EN DISPOSITIVOS MÓVILES Y SMARTPHONES

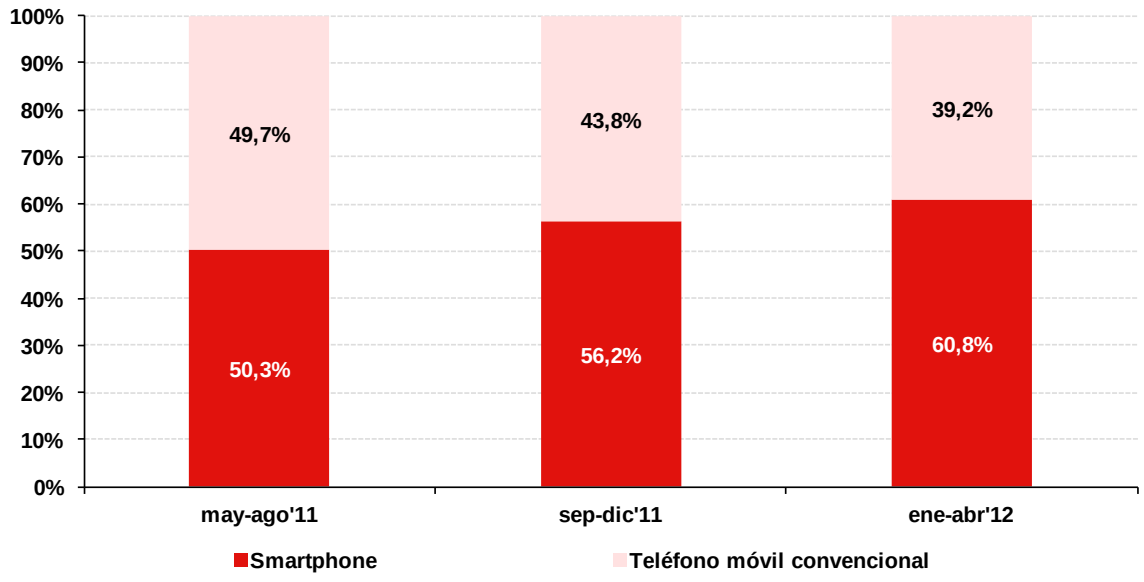
No hace muchos años los terminales móviles se encontraban aislados de muchos riesgos de seguridad al no estar interconectados con la Red. Pero actualmente, la inmensa mayoría incluye mecanismos para que puedan conectarse y descargar contenido de Internet, leer el correo electrónico, etc., encontrándose, por tanto, expuestos a las mismas amenazas de seguridad que los equipos informáticos. Incluso en aquellos casos en que los terminales no se conecten a Internet, existe la posibilidad de conexión con otros dispositivos.

Por ello, se hace necesario un análisis de las prestaciones que incorporan actualmente los terminales móviles y cómo las aprovechan los usuarios. También es de interés analizar cómo afectan estas prestaciones en los hábitos de estos usuarios en cuestión de seguridad.

3.1 TIPOS DE DISPOSITIVOS Y PRESTACIONES QUE INCORPORAN

La principal característica que supone la diferencia más significativa entre un teléfono convencional y un smartphone, es que este último dispone de sistema operativo móvil avanzado. En el presente estudio se ha analizado el porcentaje de panelistas que disponen de teléfonos móviles convencionales frente a quienes disponen de smartphone.

Gráfico 1: Usuarios que disponen de teléfono móvil smartphone



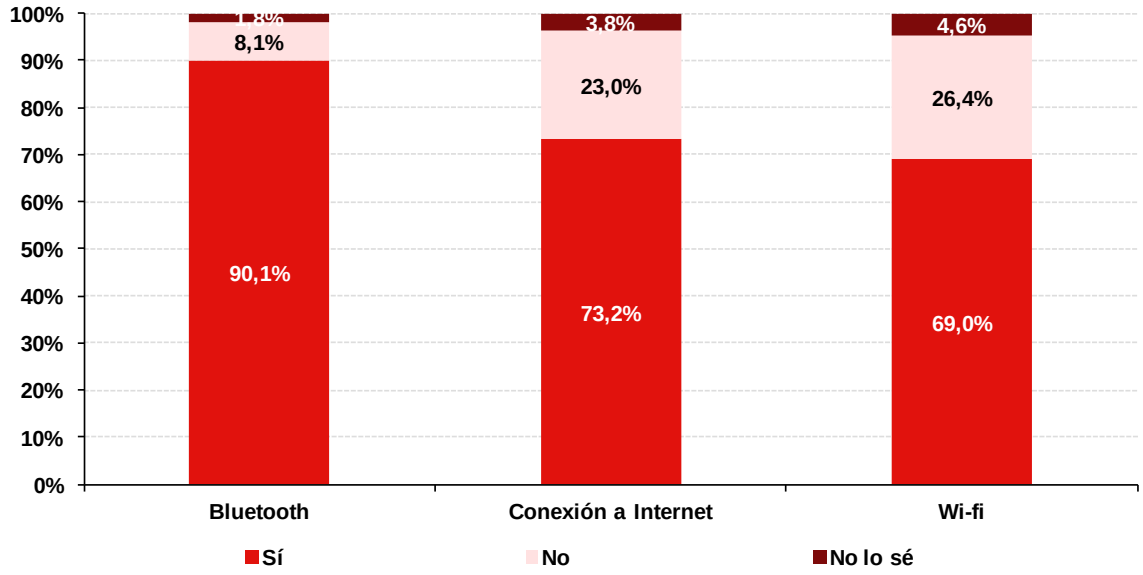
Base: Usuarios que disponen de teléfono móvil (n=3.607 en 1er cuatrimestre 2012) *Fuente: INTECO*

Desde aproximadamente el año 2007, la popularización de los smartphone ha crecido sustancialmente, desplazando a los teléfonos tradicionales. En el primer cuatrimestre de 2012, dos tercios de los encuestados que tienen teléfono móvil disponen ya de este tipo de terminal de última generación. Esto supone un incremento de más de 4 puntos porcentuales con respecto al último cuatrimestre del año 2011, confirmándose la tendencia ascendente.

Esta evolución muestra una mayor conectividad en los dispositivos, aunque la conectividad se puede manifestar en diversos grados, ya que con anterioridad a los smartphones ya se habían desarrollado elementos de conexión entre dispositivos como el sistema Bluetooth. También antes de la llegada de los smartphones, los teléfonos móviles podían conectarse a Internet, si bien su aprovechamiento de la web no era tan extenso como en la actualidad.

Las tres posibilidades de conexión que se estudian a continuación (bluetooth, conexión a Internet y utilización de redes wifi) presentan un alto grado de penetración.

Gráfico 2: Posibilidades de conexión de los terminales



Base: Usuarios que disponen de teléfono móvil (n=3.607 en 1er cuatrimestre 2012) *Fuente: INTECO*

La posibilidad de conexión a través de redes wifi también se mantiene en un nivel alto, incrementándose ligeramente hasta el 69% de los encuestados, más de 3 puntos porcentuales de aumento respecto al cuatrimestre anterior.

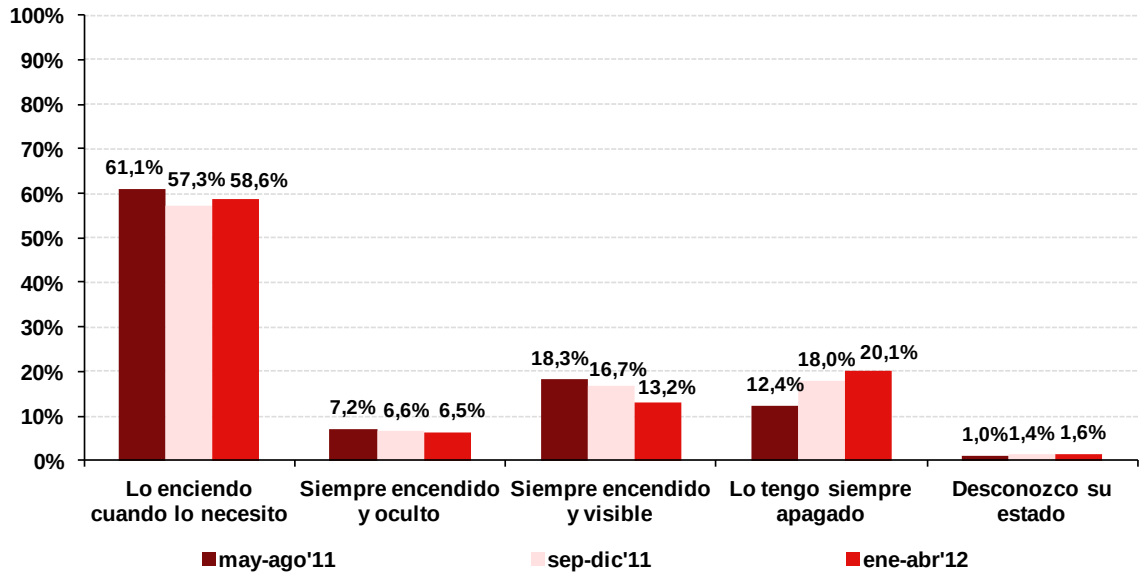
Con respecto al sistema de comunicación bluetooth, se constata la estandarización e implementación en un alto número de terminales disponibles, con 9 de cada 10 encuestados que afirma disponer de esta tecnología.

Estas capacidades de conexión dependen claramente del tipo de dispositivo. Obviamente, estas capacidades de conexión están generalizadas entre los usuarios que poseen un smartphone.

3.2 HÁBITOS DE USO DEL TELÉFONO MÓVIL

Tras conocer las posibilidades de conectividad existentes actualmente en los dispositivos, resulta de interés conocer el modo en que los usuarios las utilizan. Así, el sistema bluetooth mantiene un alto porcentaje de usuarios, 6 de cada 10, que únicamente lo encienden cuando lo necesitan, manteniéndolo desactivado el resto del tiempo.

Gráfico 3: Evolución de hábitos de uso del bluetooth



Base: Usuarios que disponen de bluetooth (n=3.264 en 1er cuatrimestre 2012) *Fuente: INTECO*

Si bien el porcentaje de usuarios que solamente activan este sistema cuando van a utilizarlo se mantiene estable, en los últimos meses se ha apreciado un importante descenso entre los usuarios que mantenían este sistema activo y visible permanentemente. Este descenso se ha acompañado de un mayor porcentaje de usuarios que afirman mantenerlo siempre desactivado.

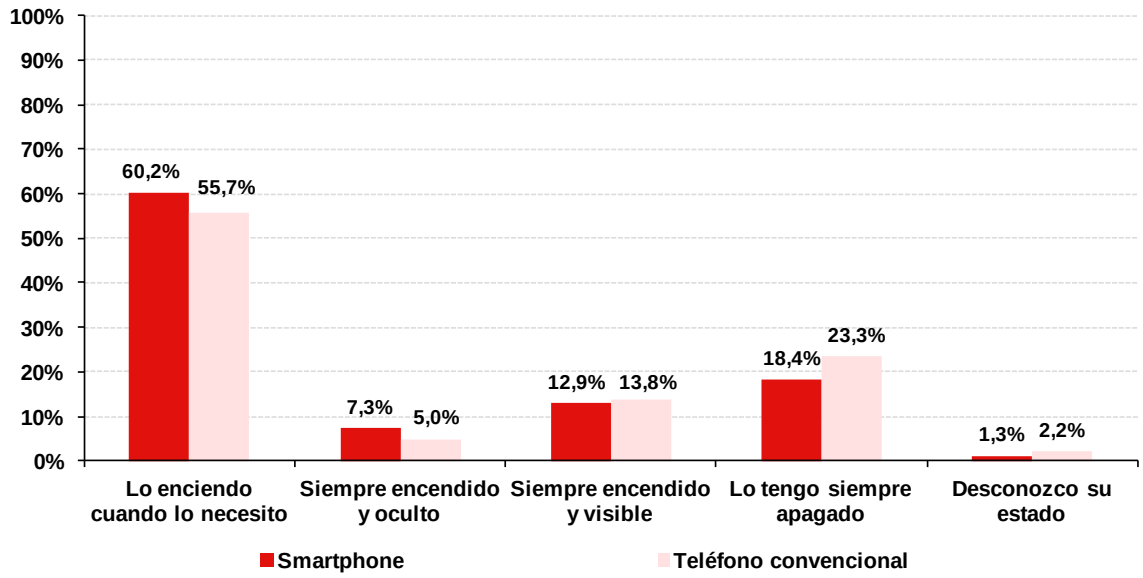
Por su parte, el porcentaje de usuarios que mantienen el sistema activo pero de manera que los demás usuarios no puedan verlo se mantiene estable presentando un ligero descenso en las últimas oleadas hasta el actual 6,5%.

En cuanto a la diferenciación entre usuarios de teléfonos móviles convencionales y los de smartphones, cabe destacar que estos últimos manifiestan utilizar más la tecnología bluetooth (18,3% no lo utiliza frente al 23,3% del resto de usuarios). A su vez, los usuarios de smartphones declaran un uso más seguro, al apuntar en mayor medida que

activan el sistema solamente cuando lo van a utilizar (60,2% frente a 55,7%), o que lo mantienen activado pero en modo oculto (7,3% frente a 5%).

El desconocimiento también parece ser menor entre los usuarios de smartphones, ya que un 1,3% de ellos afirma no conocer el estado de su sistema bluetooth, frente al 2,2% de los usuarios de teléfonos móviles convencionales.

Gráfico 4: Hábitos de uso del bluetooth, según tipo de teléfono móvil



Base: Usuarios que disponen de bluetooth (Smartphone n=2.046, Teléfono convencional n=1.218) *Fuente: INTECO*

Mantener el sistema bluetooth permanentemente activo permite que el dispositivo pueda conectarse con otros equipos en cualquier momento, facilitando por tanto la posibilidad de que se produzca un ataque como por ejemplo el envío de malware a través de este sistema.

Si además de mantener esta posibilidad de conexión activa, la configuración permite que otros conozcan esta situación se ahonda en la posibilidad de ataque. Por ello es recomendable mantener este sistema desactivado y ponerlo en funcionamiento únicamente de manera puntual cuando se vaya a utilizar.

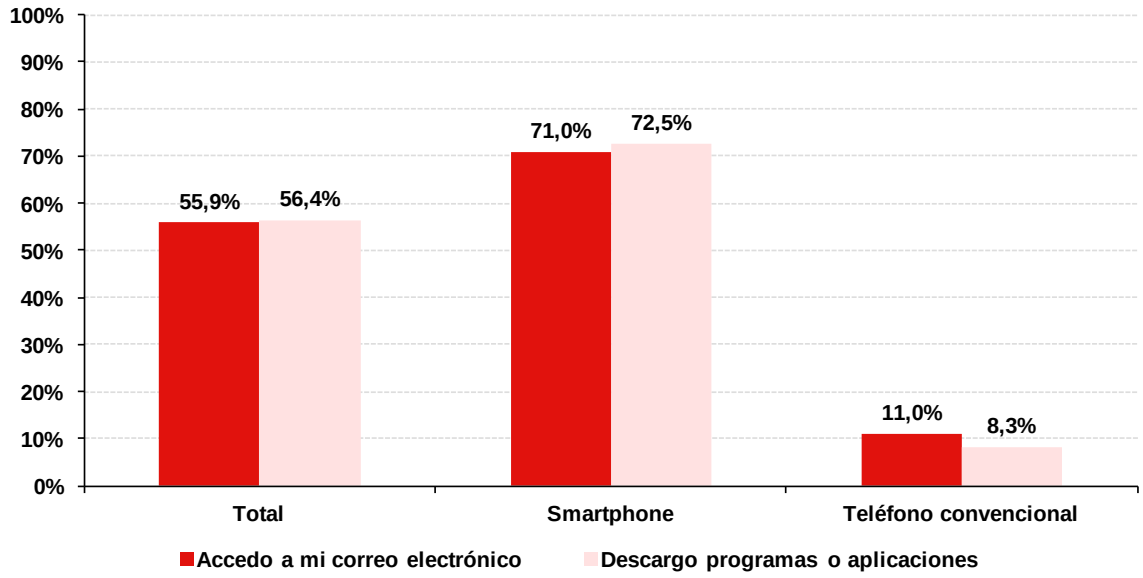
En caso de necesitar que el sistema bluetooth se mantenga activo constantemente, por ejemplo quienes para trabajar necesiten conducir constantemente y utilicen sistemas de manos libres para atender el teléfono al volante, es recomendable ocultar esta posibilidad de conexión para evitar que otras personas conozcan que el sistema está activo y evitar ataques.

En cuanto a los usos de los teléfonos móviles, actualmente estos dispositivos pueden incorporar nuevas funcionalidades a través de la instalación de aplicaciones o programas

específicos. Esta incorporación de nuevas funcionalidades no es una capacidad exclusiva de los smartphones, ya que anteriormente los usuarios de teléfonos móviles ya podían descargar diferentes aplicaciones, especialmente juegos.

Si bien esto es cierto, las capacidades que presentan los smartphones son muy superiores a las del resto de teléfonos, fomentando así la utilización de los dispositivos de modos que van más allá de la mera telefonía. Esto se evidencia en el Gráfico 5, en el que se muestra el acceso al correo electrónico desde los teléfonos y la descarga de nuevas aplicaciones. En ambos casos, el uso general es superior al manifestado en el anterior cuatrimestre, pasando el acceso al correo electrónico de un 50,4% a un 55,9%, mientras que la descarga de programas y aplicaciones aumenta de un 50,6% a un 56,4%.

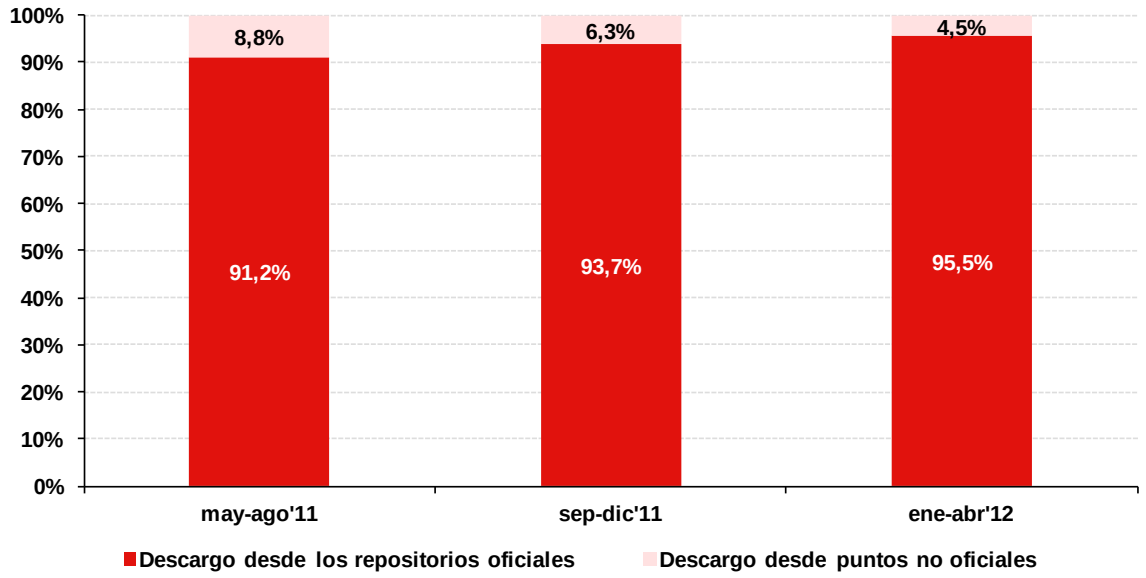
Gráfico 5: Uso del e-mail y descarga de aplicaciones desde el teléfono móvil



Base: Usuarios que disponen conexión a Internet o wifi
(Total n=2.883, Smartphone n=2.096, Teléfono convencional n=787)
Fuente: INTECO

Al descargar aplicaciones para los dispositivos móviles, es de gran importancia realizar estas descargas desde fuentes de confianza, ya que un atacante podría poner a disposición aplicaciones maliciosas o que contuviesen algún tipo de malware. El siguiente gráfico muestra qué hábitos siguen los usuarios respecto a las fuentes desde las que descargan nuevas aplicaciones, en función de si estas fuentes son repositorios oficiales o no.

Gráfico 6: Fuente de descarga de programas o aplicaciones



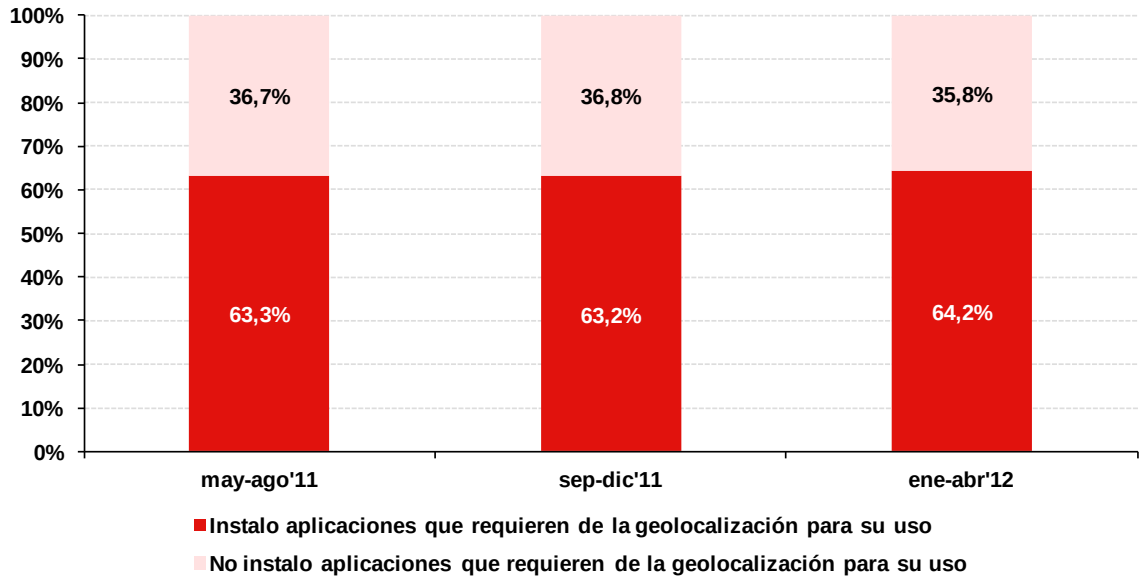
Base: Usuarios que descargan programas o aplicaciones en el teléfono móvil (n=1.537 en 1er cuatrimestre 2012) *Fuente: INTECO*

Como viene siendo habitual, sigue aumentando el uso de repositorios oficiales (*AppStore* de Apple, *Google Play* de Android o *App World* para Blackberry) para la descarga de aplicaciones por parte de los usuarios, siendo la subida en cerca de 2 puntos porcentuales (95,5%) respecto al cuatrimestre anterior y de 4 puntos en un año. Esto refleja los buenos hábitos de seguridad establecidos en este tipo de usuarios y la desconfianza que ofrecen otros sitios no oficiales, que pudieran propiciar la instalación de todo tipo de malware en el terminal.

De entre los diferentes tipos de aplicaciones que pueden incorporarse a los teléfonos móviles, se ha cuestionado específicamente sobre aquellas que requieren el uso de la geolocalización. Estas aplicaciones obtienen los datos de posicionamiento del usuario a través de su conexión a Internet o a través de un sistema GPS, para así poder ofrecer determinados servicios al usuario, desde indicar qué contactos se encuentran cerca hasta establecer una ruta para llegar a un destino concreto. Estas aplicaciones si bien ofrecen una serie de ventajas a sus usuarios, también implican un riesgo al poder desvelar a terceros su posición geográfica.

Los resultados muestran una estabilidad constante en el uso de este tipo de aplicaciones. Casi 2 tercios de los usuarios encuestados hacen uso de este tipo de programas ya sea ya sea a través de conexión a Internet o GPS.

Gráfico 7: Uso de programas con geolocalización



Base: Usuarios que descargan programas o aplicaciones en el teléfono móvil (n=1.537 en 1er cuatrimestre 2012) *Fuente: INTECO*

3.3 MEDIDAS DE SEGURIDAD UTILIZADAS EN EL TELÉFONO MÓVIL

Si bien las posibilidades de uso de los dispositivos móviles han aumentado considerablemente de la mano de sus capacidades de conexión, también lo han hecho los riesgos a los que se pueden exponer. Así, actualmente los teléfonos móviles pueden verse afectados por el malware de mismo modo que los ordenadores personales y también pueden ser utilizarlos para disfrutar de servicios como el comercio electrónico o la banca online, por lo que se exige aplicar medidas de seguridad del mismo modo que en un ordenador.

Por ello, a continuación se analiza en qué medida los panelistas llevan a cabo buenas prácticas en sus teléfonos móviles para estar protegidos ante posibles incidentes de seguridad.

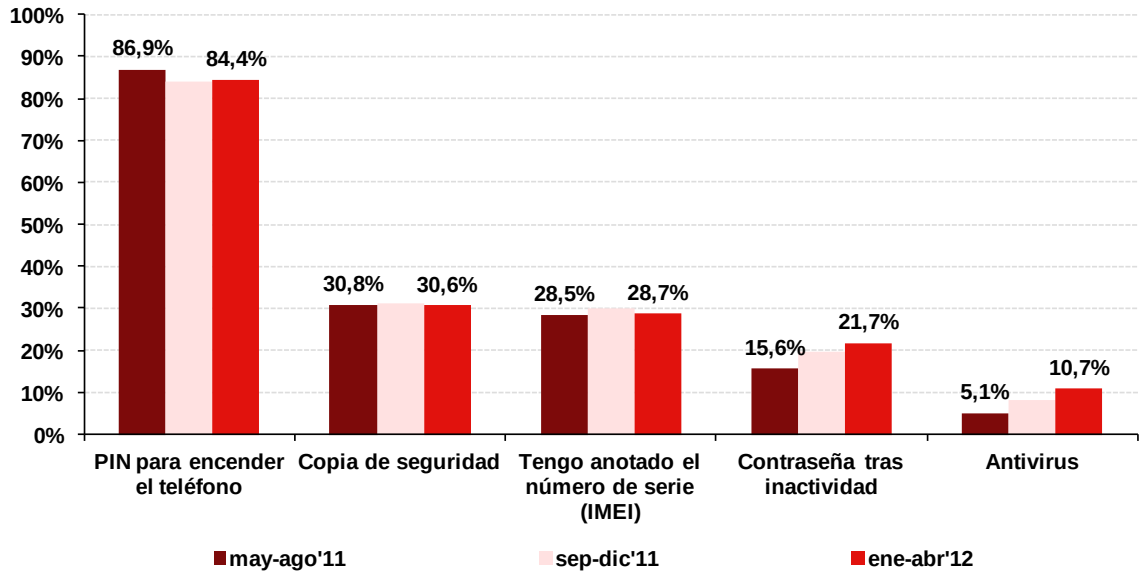
La medida de protección más puesta en práctica sigue siendo, con gran diferencia, el empleo de un PIN, que continúa presentando porcentajes estables en torno al 85%.

También mostrando una tendencia estable se encuentran la realización de copias de seguridad de los contactos y anotar el número de serie o IMEI del teléfono, ambos casos situados en torno a un 30% de adopción. Anotar el IMEI del terminal, el cual permite identificarlo de manera única, y mantenerlo en un lugar seguro, podría permitir su desactivación remota o identificación en caso de robo o pérdida.

Por su parte, el establecimiento de una contraseña para desbloquear el teléfono tras periodos de inactividad y el uso de antivirus son medidas cada vez más adoptadas por

parte de los usuarios (21,7% y 10,7% respectivamente), mostrando un aumento en la concienciación de los usuarios en materia de seguridad. En este conocimiento y concienciación es de especial relevancia, al tiempo que las diferentes campañas de sensibilización, la difusión en los medios de los diferentes incidentes acaecidos de forma masiva o puntualmente a personajes famosos A pesar de estos datos, un 9,6% de los encuestados declara no utilizar ninguna de estas herramientas y medidas.

Gráfico 8: Medidas de seguridad utilizadas / instaladas



Base: Usuarios que disponen de teléfono móvil (n=3.607 en 1er cuatrimestre 2012) *Fuente: INTECO*

Sistemas de localización en caso de robo

Las tres grandes compañías y sus sistemas operativos (Google/Android, Apple/iOS y RIM/Blackberry) disponen de sistemas de localización y antirrobo que aumentan la seguridad y posibilitan la búsqueda del terminal en caso de que, por desgracia, se cometa el robo del mismo.

Android dispone de un sistema de tracking o localización integrado en el SO, aunque también existen aplicaciones desarrollados por terceros (por ejemplo Cerberus[3]).

Apple posibilita las mismas medidas gracias a "Buscar mi iPhone[4]" en conjunción al servicio iCloud También existen alternativas también de pago más completas.

BlackBerry provee de idénticos servicios: BlackBerry Protect[5], igualmente gratuita.

[3] Fuente: Google Play – Cerberus: https://play.google.com/store/apps/details?id=com.lsdroid.cerberus

[4] Fuente: Apple – Buscar mi iPhone: http://itunes.apple.com/es/app/buscar-mi-iphone/id376101648?mt=8

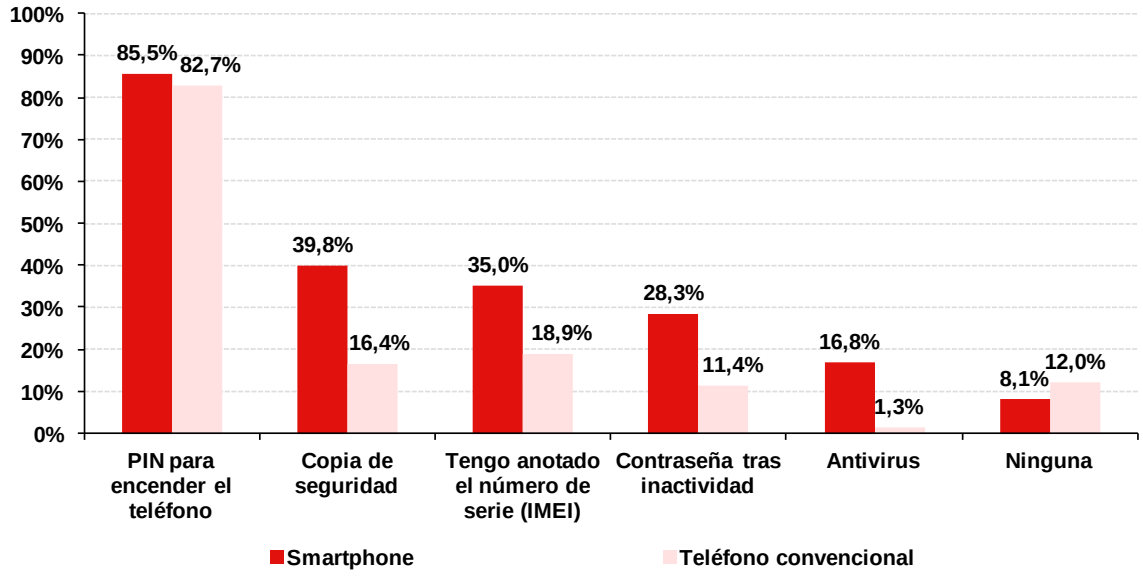
[5] Fuente: Blackberry Protect: http://es.blackberry.com/services/protect/

En cuanto a la diferencia existente entre los teléfonos convencionales y los smartphone, se puede señalar que los usuarios de estos últimos aplican más medidas de seguridad, ya sea por contar con más posibilidades o por conocer mejor los riesgos.

En buena medida, esta diferencia también puede deberse a las mayores facilidades existentes en lo referente a la protección en el caso de los nuevos terminales, así por ejemplo, los smartphones cuentan con la capacidad de ser conectados a un ordenador y para ello, generalmente, existe una serie de programas puestos a disposición del usuario por el propio fabricante. Entre las diferentes funciones de estos programas se encuentra la posibilidad de generar copias de seguridad. En algunos casos estas copias se generan mediante la conexión a Internet desde el propio terminal, sin necesidad de ser conectados a ningún ordenador personal.

Estas evidencias, unidas al constante aumento del porcentaje de smartphones entre los teléfonos móviles utilizados por los españoles, anticipa un aumento del uso de medidas de seguridad en futuras lecturas.

Gráfico 9: Medidas de seguridad aplicadas, según tipo de teléfono móvil



Base: Usuarios que disponen de teléfono móvil (Smartphone n=2.119, Teléfono convencional n=1.488)

Fuente: INTECO

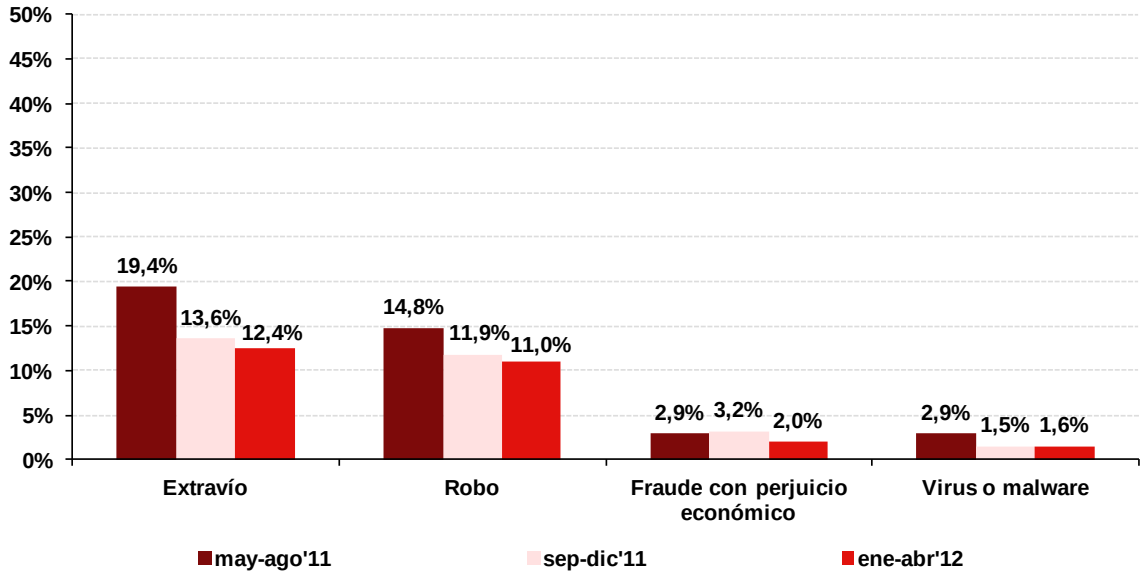
3.4 INCIDENTES DE SEGURIDAD

En este apartado se analizan los incidentes de seguridad que los usuarios han sufrido en sus teléfonos móviles. Para ello se ha consultado a los panelistas sobre algunos de los incidentes más habituales, así como de la posibilidad de haber sufrido fraudes a través de su terminal.

3.4.1 Incidentes de seguridad

De forma general, los incidentes más habituales son declarados en menor medida, en comparación con anteriores lecturas. Los incidentes relacionados con virus o malware en estos dispositivos siguen siendo minoritarios, con un 1,6% de usuarios que declara haber sufrido alguna infección en los últimos 3 meses. Por su parte, la incidencia del perjuicio económico a causa de un fraude a través del teléfono móvil es la menor de las registradas en el último año, situándose en un 2%.

Gráfico 10: Incidencias de seguridad ocurridas en el uso del teléfono móvil



Base: Usuarios que disponen de teléfono móvil (n=3.607 en 1er cuatrimestre 2012) *Fuente: INTECO*

El análisis de estos incidentes según el tipo de terminal utilizado, muestra ligeras diferencias en cuanto al robo de los dispositivos, siendo superior el manifestado por los usuarios de smartphones (12,1% frente a un 9,4%), y también en cuanto a las infecciones por malware (1,9% frente a 1,1%). En los demás casos no existen diferencias reseñables.

3.4.2 Fraude

De entre los posibles incidentes, se realiza un análisis específico de las situaciones que pudieran desembocar en fraudes económicos. Por ello, se ha consultado a los encuestados sobre diferentes situaciones que podrían concluir en un fraude económico y por ello se pueden considerar como intentos de fraude.

Tal y como se muestra en el Gráfico 11, los incidentes considerados cuentan con un escaso nivel de incidencia, ya que un 84,5% de los panelistas usuarios de teléfono móvil asegura no haber sufrido ninguna de estas situaciones, 3 puntos porcentuales más que lo declarado en el último cuatrimestre. De este modo, el porcentaje de usuarios que

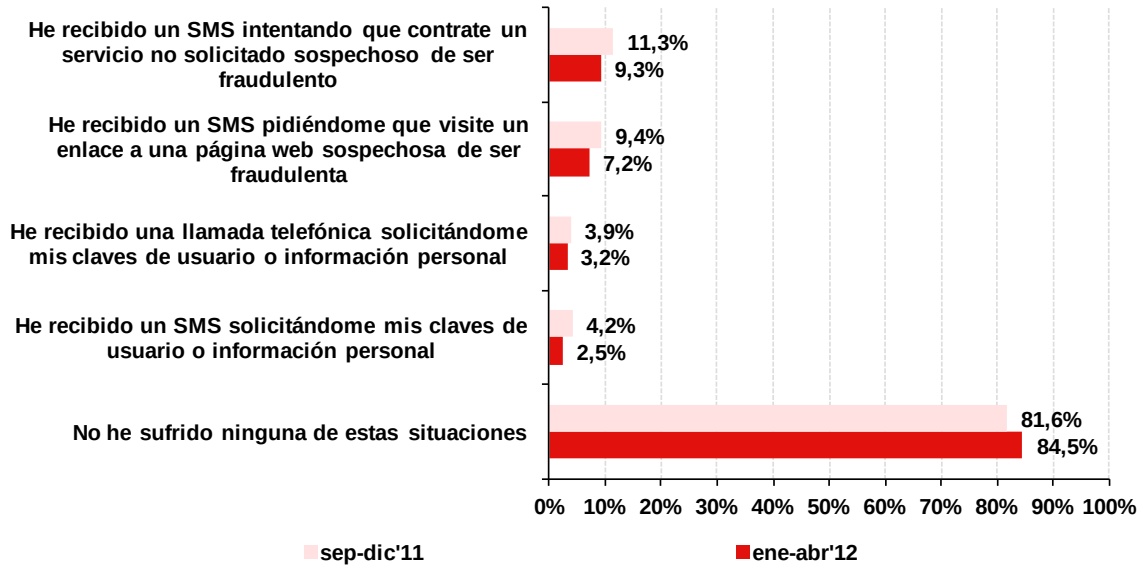
declaran algún incidente se reduce desde un 18,4% a un 15,5%. Esto se refleja en una reducción en la incidencia de todas las situaciones analizadas.

Los incidentes referentes a mensajes que incitan a contratar servicios no solicitados son los más habituales, afirmándolo así el 9,3% de los encuestados, mientras que la invitación a visitar páginas web que el usuario puede considerar fraudulentas se limita al 7,2% de los panelistas.

Por su parte, las comunicaciones cuyo objetivo es conseguir las claves que el usuario emplea en algún servicio o información personal cuentan con menor incidencia aún, situándose en el 3,2% en el caso de llamadas telefónicas y del 2,,5% si la comunicación consiste en un mensaje o SMS.

Las diferencias presentadas entre los usuarios de smartphones y quienes utilizan teléfonos móviles convencionales son mínimas y no siguen un patrón claro.

Gráfico 11: Situaciones relacionadas con el fraude sufridas a través del teléfono móvil

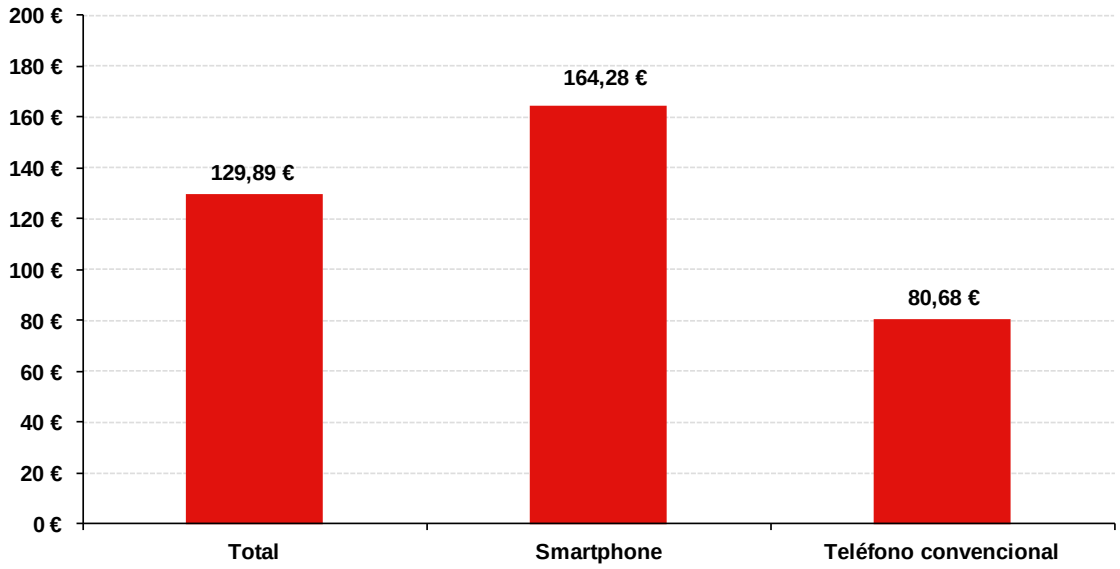


Base: Usuarios que disponen de teléfono móvil (n=3.607 en 1er cuatrimestre 2012) *Fuente: INTECO*

Al igual que la incidencia de los intentos de fraude, la consumación de éstos también se ha visto reducida hasta representar tan solo un 2% de los encuestados, tal y como se ha mostrado en el Gráfico 10.

Si bien la incidencia del perjuicio económico es similar entre los de smartphones y aquellos que utilizan teléfonos móviles convencionales, no ocurre lo mismo en cuanto a las cuantías medias de las personas que han sufrido dicho perjuicio.

Gráfico 12: Cuantía defraudada según tipo de teléfono móvil



Base: Usuarios que han sufrido perjuicio económico fraudulento a través del teléfono móvil (Total n=65, Smartphone n=42, Teléfono convencional n=23) *Fuente: INTECO*

Como se puede observar, en caso de sufrir un perjuicio económico la cuantía media defraudada es mucho mayor entre los usuarios de smartphones, llegando a suponer el doble que en el caso de quienes utilizan teléfonos móviles convencionales. Esta diferencia se debe especialmente a que los casos registrados en los que las cuantías defraudadas han sido mayores, el dispositivo utilizado es un smartphone.

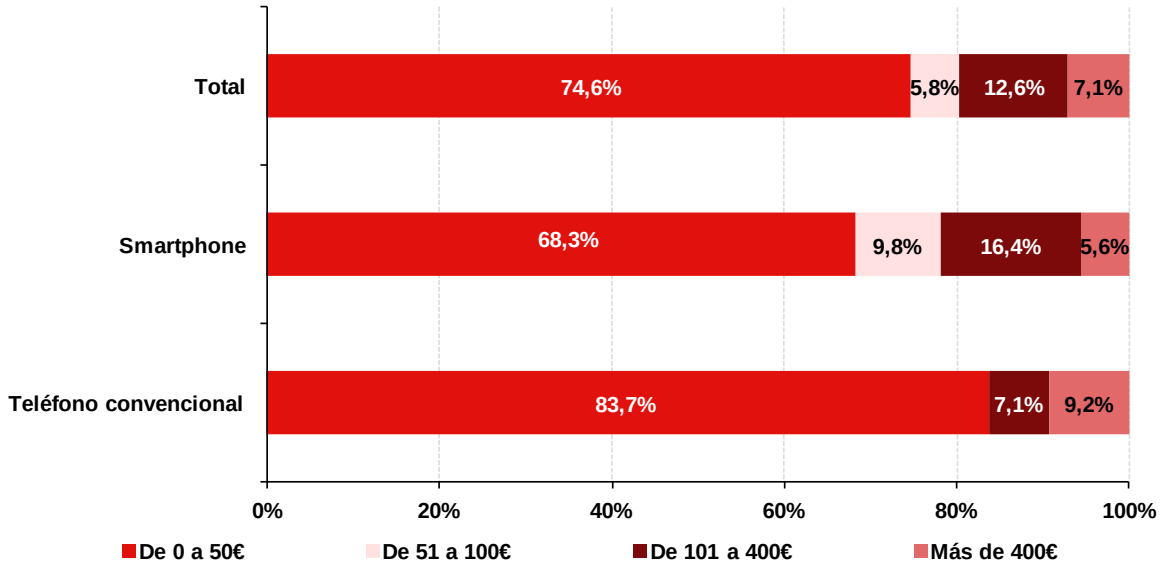
A pesar de lo llamativo de esta diferencia, es necesario recordar que el número de casos en que se basa este análisis es muy reducido debido a la escasa incidencia del fraude a través del teléfono móvil, por lo que estos datos se deben considerar como meramente indicativos al contar un margen de error mucho mayor al mostrado en el resto de indicadores.

Finalmente, se presentan los datos referentes al porcentaje de casos que serían considerados delito frente a los casos que no llegaría a ser considerados como tal. La diferencia entre estos dos conceptos es, al margen de las posibles consecuencias legales para el atacante, la cantidad defraudada, siendo el punto de inflexión la cantidad de 400€.

Como se muestra en el siguiente gráfico, la mayor parte de los casos registrados no llegarían a ser considerados como delitos al no superar la cuantía defraudada la barrera de los 400€. Esta tendencia en la que los atacantes concentran sus esfuerzos en

cantidades menores es similar a la observada al analizar la incidencia del fraude a través de Internet al margen del dispositivo de acceso utilizado[6].

Gráfico 13: Distribución de las cuantías defraudadas, según tipo de teléfono móvil



Base: Usuarios que han sufrido perjuicio económico fraudulento a través del teléfono móvil (Total n=65, Smartphone n=42, Teléfono convencional n=23) *Fuente: INTECO*

A su vez, las diferencias entre lo manifestado por los usuarios de smartphones y quienes utilizan teléfonos convencionales se centra en la polarización en este último caso, ya que si bien muestran un mayor porcentaje de fraudes en la franja de hasta 50€ (15 puntos porcentuales de diferencia), también muestran un mayor porcentaje de casos que superan los 400 euros, acercándose al 10%.

Por otro lado, esto se contrapone con las cantidades medias observadas en ambos casos de fraude, ya que los casos en que usuarios de smartphones han sufrido perjuicios económicos superiores a los 400 euros como consecuencia de un fraude, siendo menos en comparación con los usuarios de teléfonos convencionales, registran cantidades mucho más elevadas en sus casos más extremos.

De nuevo es necesario recordar que debido la escasa incidencia del fraude a través del teléfono móvil los datos presentados, especialmente en la clasificación según tipo de terminal, deben analizarse con cautela ya que las bases muestrales son reducidas y por tanto cuentan con un mayor margen de error.

[6] Para conocer más datos sobre el fraude online se pueden consultan las diferentes oleadas del *Estudio sobre el fraude a través de Internet* realizado por INTECO y disponible en su sección de Estudios e Informes, https://www.inteco.es/Seguridad/Observatorio/Estudios/

4 CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES DEL ANÁLISIS

Los smartphones se han convertido en un tipo de dispositivo en el que se continúa la actividad llevada a cabo en los terminales de sobremesa. En la actualidad, tres de cada cinco usuarios dispone de smartphone y, para aprovechar sus capacidades y continuar su actividad en la red, en los móviles se sigue consultando el correo (55,9%), descargando aplicaciones (56,4%), etc. En consecuencia, con un mayor uso, comienzan a preocuparse por su seguridad:

- Se incrementa incesantemente el porcentaje de usuarios que acude a repositorios oficiales para descargar aplicaciones (hasta un 95,5% este cuatrimestre).
- Igualmente, asciende hasta un 10,7% el porcentaje de usuarios que declara utilizar antivirus en su teléfono.
- También se incrementa el porcentaje de usuarios que bloquea el terminal tras un periodo de inactividad hasta situarse un 21,7%.

Todas son excelentes medidas que, aunque en varios casos todavía se mantienen en niveles bajos, aumentan cada cuatrimestre.

Además, el análisis comparado entre lo declarado por los usuarios de smartphones y quienes utilizan teléfonos móviles convencionales pone de manifiesto que el contar con un dispositivo más avanzado también se acompaña de un mayor uso de las herramientas de seguridad. Esto se debe tanto a un mayor conocimiento de los riesgos por parte de los usuarios más avanzados como a la gran disponibilidad de herramientas de seguridad en los nuevos dispositivos, en muchos casos ya instaladas y en otros sugeridas en diferentes momentos como la primera configuración.

Esta comprobación pone de manifiesto que la actual tendencia de incremento en el uso de medidas de seguridad en terminales móviles, especialmente las hasta ahora minoritarias, se mantendrá en las próximas lecturas debido al incremento del porcentaje de smartphones en el conjunto de los teléfonos móviles utilizados por los usuarios.

A pesar de estas facilidades y estos datos positivos, las noticias y tendencias sobre la seguridad en el mundo móvil no invitan a bajar la guardia. El fraude está sufriendo un trasvase o incluso está encontrando complementariedad en el mundo móvil. Por ejemplo, ya existe malware que infecta tanto el equipo de sobremesa como el terminal móvil[7],

[7] Fuente: S21sec Blog. "*Zeus Mitmo: Man-in-the-mobile*", disponible en http://blog.s21sec.com/2010/09/zeus-mitmo-man-in-mobile.html

buscando atacar a los servicios bancarios que utilizan los SMS como factor de autenticación para realizar una transacción.

Por otro lado, de nuevo, un estudio de Trend Micro afirma que durante el segundo trimestre de 2012, el número de aplicaciones maliciosas para Android se duplicó de 10.000 a 20.000[8], en un crecimiento mayor que meses anteriores, donde a su vez también se incrementó el malware para este sistema operativo. Son varios los factores que pueden achacarse a este interés de los atacantes por los móviles con sistema operativo Android, especialmente su popularidad y sus bajas restricciones a la hora de controlar las aplicaciones descargadas y ejecutadas.

En ese mismo estudio se afirma que casi un tercio del malware se disfraza de aplicaciones legítimas. Google Play (el antiguo Android Market) se ha visto obligado a vigilar más de cerca las aplicaciones que se suben a su repositorio. Así, a principios de año puso en marcha Bouncer[9], un dispositivo especial para analizar las aplicaciones en busca de malware antes de ser puestas a disposición del público. Teniendo esto en cuenta, pero anticipándose a que los atacantes encuentren alguna forma de vulnerar las medidas de seguridad existentes, los usuarios deben reforzar su comportamiento en ciertos aspectos:

- No solo descargar de repositorios legítimos, sino evitar los programas o juegos que exijan demasiados permisos en el terminal.
- Es importante descargar programas exclusivamente de marcas o fabricantes reconocidos.

En cualquier caso, parece que los usuarios cuidan de su terminal tanto a nivel lógico (aumenta el número de usuarios que protege con contraseña tras inactividad y los que instalan antivirus) como a nivel físico (desciende el porcentaje de usuarios a los que han robado o han extraviado el teléfono), de lo que se desprende el valor que le otorgan a estos dispositivos como extensión natural de su actividad en la Red.

4.2 RECOMENDACIONES

Las recomendaciones que se muestran a continuación pretenden servir de ayuda para que los usuarios puedan proteger y/o conservar la información almacenada en sus terminales móviles, así como bloquear el acceso a los mismos:

[8] Fuente: Report: Android malware doubled in just one month, disponible en http://www.h-online.com/open/news/item/Report-Android-malware-doubled-in-just-one-month-1632587.html

[9] Fuente: "Bouncer, la lucha contra el malware en el Market de Android", disponible desde http://unaaldia.hispasec.com/2012/02/bouncer-la-lucha-contra-el-malware-en.html

1. **Que nadie use tu móvil sin tu autorización y protégelo contra la pérdida o robo**

   - Ten localizado el terminal en todo momento para evitar el robo y el acceso indebido por terceros.
   - Activa el bloqueo automático del teléfono móvil para evitar que personas no autorizadas puedan acceder a los datos.
   - Ten activado el número PIN para que cada vez que se encienda el teléfono el acceso no sea automático.
   - Conoce el número de IMEI (International Mobile Equipment Identity) que permite al usuario, a través de la operadora de telefonía móvil, desactivar el terminal en caso de pérdida o robo. Para conocer este número se puede marcar *#06# en el teléfono y se mostrará en la pantalla.

2. **Protege tu terminal frente al malware y el fraude**

   - Instala una herramienta antimalware.
   - Descarga las actualizaciones del sistema operativo móvil y de las aplicaciones que tengas instaladas, y procura hacerlo desde repositorios oficiales o de confianza.
   - Evita descargar aplicaciones o archivos con origen poco confiable. Si se realiza una conexión entre dispositivos (de móvil a móvil, o de móvil a ordenador), comprueba que ninguno de ellos se encuentre comprometido o aloje archivos infectados.
   - Vigilar el consumo y, en caso de notar incrementos bruscos en la factura, verificarlo con la compañía, ya que puede ser un indicio de un fraude o de un uso indebido.

3. **Protege las comunicaciones móviles e inalámbricas**

   - Desactiva la conexión bluetooth, wifi y 3G (siempre que sea posible esta opción) cuando no se esté utilizando.
   - Evita conectarte a redes públicas, especialmente si vas a realizar una transacción económica o de datos sensibles.

4. Cuida la información que guardas en tu dispositivo móvil

- Cifra la información sensible en la memoria del teléfono.
- En entornos corporativos en los que se maneja información altamente sensible, se recomienda conectarse a servidores seguros para acceder a la información, en vez de alojarla en el dispositivo.
- Realiza copias de seguridad de los contenidos que tengas en el terminal, para poder recuperarlos en el caso de los pierdas accidentalmente.
- Realiza un borrado seguro y definitivo de la información almacenada en el dispositivo cuando vayas a deshacerte de él, venderlo o arreglarlo.

5. Protege tu privacidad

- Comprueba las solicitudes de permisos que otorgas a las aplicaciones que instalas y revísalas periódicamente.
- Presta especial atención a las solicitudes de acceso a la tarjeta de memoria, conexión a Internet, intercambio de datos y vinculación con perfiles en redes sociales y otros servicios en los que alojes información y contactos personales.

ÍNDICE DE GRÁFICOS Y TABLAS

Síguenos a través de:

Web

Envíanos tus consultas y comentarios a:

observatorio@inteco.es

Instituto Nacional
de Tecnologías
de la Comunicación