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

Informe anual 2011 (8ª oleada)

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN

Edición: Julio 2012

El "*Estudio sobre seguridad en dispositivos móviles y smartphones" (Informe anual 2011)* ha sido elaborado por el Instituto Nacional de Tecnologías de la Comunicación (INTECO):

Pablo Pérez San-José (dirección)

Laura García Pérez (coordinación)

Eduardo Álvarez Alonso

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 publica el *Estudio sobre seguridad en dispositivos móviles y smartphones (Informe anual 2011)*. Para elaborar el análisis se han realizado 3.655 entrevistas online (en PC). El período analizado en este documento abarca los meses de septiembre a diciembre de 2011.

El estudio, correspondiente al 3er cuatrimestre de 2011, 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.

Se exponen a continuación los puntos clave del estudio.

I. EXTENSIÓN Y PRESTACIONES QUE INCORPORAN

A finales de 2011 casi la totalidad de usuarios dispone de un teléfono móvil y más de la mitad posee un smartphone. Se pone de manifiesto la estandarización e implementación del bluetooth en un alto número de terminales y se declara evidente el alto uso de Internet y conexión wifi vía móvil.

- En el 3er cuatrimestre de 2011 un 98,4% disponen de un teléfono móvil, reflejándose la amplia distribución y arraigo del uso de esta tecnología. Además, un 56,2% de los que tiene terminal móvil es propietario de un smartphone o dispositivo de última generación.

- Se ve la estandarización e implementación del bluetooth en un alto número de terminales con un 90,1% de encuestados que declara disponer esta tecnología en el teléfono móvil. También se declara evidente el alto uso de Internet vía móvil con un 71,6 %. Y por último, la disponibilidad de conexión wifi también se sitúa en un alto porcentaje con un 65,5%.

II. HÁBITOS DE USO DEL TELÉFONO MÓVIL

Los usuarios de telefonía móvil aprovechan al máximo las prestaciones que incorporan sus terminales: leyendo el correo electrónico, descargando aplicaciones o usando servicios de geolocalización, entre otras.

- La mitad de los internautas con dispositivo móvil (50,4%) lee el correo electrónico a través de su dispositivo, un 50,6% accede a descargas desde su teléfono y un 63,2% instala aplicaciones que requieren de la geolocalización para su uso.

- En los últimos 3 años se ha más que duplicado el porcentaje de usuarios que accede al correo electrónico desde el teléfono móvil: del 21,8% al 50,4%.

III. MEDIDAS DE SEGURIDAD UTILIZADAS EN EL TELÉFONO MÓVIL

Sigue siendo generalizado el empleo de código PIN en los panelistas como medida principal de protección del dispositivo, aunque desciende ligeramente en comparación con el cuatrimestre anterior, en contrapunto al aumento del uso de contraseña tras la inactividad y el antivirus. Más de la mitad de los usuarios que disponen de bluetooth toma las medidas necesarias y lo enciende sólo cuando lo necesita.

- En el 3er cuatrimestre de 2011 el uso de código PIN se sitúa en un 84%, 2,9 puntos porcentuales menos que el cuatrimestre anterior.

- Aumenta el uso de contraseña tras la inactividad, cerca de 4 puntos porcentuales, situándose a finales de 2011 en un 19,5%. También el uso de antivirus con un 8,1% asciende 3 puntos porcentuales en comparación con el periodo anterior. Otras medidas preventivas como copias de seguridad y tener anotado el número de serie (IMEI) se mantienen relativamente estables a lo largo de 2011.

- En el 3er cuatrimestre de 2011 un 57,3% toma las medidas necesarias y enciende el bluetooth sólo cuando lo necesita. En contraste y como mal hábito, un 16,7% lo mantiene encendido de manera habitual.

IV. INCIDENCIAS DE SEGURIDAD

La incidencia de seguridad más declarada por los usuarios españoles es el extravío del terminal, seguido del robo del mismo y de la infección por virus o malware. Además, menos de la quinta parte de usuarios declara haber sido objeto de algún intento de fraude telefónico y es poco elevado (aunque mayor que el cuatrimestre anterior) el porcentaje de aquellos que declara que este hecho haya derivado en un perjuicio económico.

- En el 3er cuatrimestre de 2011 el extravío del terminal se sitúa en un 13,6%, seguido del robo del mismo (11,9%) y de la infección por virus o malware (1,5%). Estas tres incidencias sufren un ligero descenso si se comparan con los datos del periodo pasado, siendo el descenso más significativo el de la pérdida del teléfono móvil con 5,8 puntos porcentuales menos.

- Un 18,4% de los encuestados declara haber sido objeto de algún intento de fraude telefónico (no consumado), frente a un 81,6% que no han constatado una situación de este tipo.

- Haber sufrido impacto económico provocado por los intentos de fraude telefónico (SMS o llamada telefónica) es declarado por un 3,2% de los usuarios. Este dato supone un ligero aumento comparado con el dato del 2º cuatrimestre del año que se situaba en un 2,9%.

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.

INTECO es un centro de desarrollo de carácter innovador y de interés público de ámbito nacional que se orienta a la aportación de valor, a la industria y a los usuarios, y a la difusión de las nuevas tecnologías de la información y la comunicación (TIC) en España, en clara sintonía con Europa.

Su objetivo fundamental es servir como instrumento para desarrollar la Sociedad de la Información, con actividades propias en el ámbito de la innovación y el desarrollo de proyectos asociados a las TIC, basándose en tres pilares fundamentales: la investigación aplicada, la prestación de servicios y la formación.

La misión de INTECO es aportar valor e innovación a los ciudadanos, a las PYMES, a las Administraciones Públicas y al sector de las tecnologías de la información, a través del desarrollo de proyectos que contribuyan a reforzar la confianza en los servicios de la Sociedad de la Información en nuestro país, promoviendo además una línea de participación internacional.

Para ello, INTECO desarrolla actuaciones en las siguientes líneas:

- **Seguridad tecnológica:** INTECO está comprometido con la promoción de servicios de la Sociedad de la Información cada vez más seguros, que protejan los datos personales de los interesados, su intimidad, la integridad de su información y eviten ataques que pongan en riesgo los servicios prestados. Y, por supuesto, que garanticen un cumplimiento estricto de la normativa legal en materia de TIC. Para ello coordina distintas iniciativas públicas en torno a la seguridad de las TIC, que se materializan en la prestación de servicios por parte del Observatorio de la Seguridad de la Información, el Centro de Respuesta a Incidentes de Seguridad en Tecnologías de la Información (INTECO-CERT), con su Catálogo de Empresas y Soluciones de Seguridad TIC, y la Oficina de Seguridad del Internauta (OSI), de los que se benefician ciudadanos, pymes, Administraciones Públicas y el sector tecnológico.

- **Accesibilidad:** INTECO promueve servicios de la Sociedad de la Información más accesibles, que supriman las barreras de exclusión, cualquiera que sea la dificultad o carencia técnica, formativa, etc., incluso discapacidad, que tengan sus usuarios. Y que faciliten la integración progresiva de todos los colectivos de

usuarios, de modo que todos ellos puedan beneficiarse de las oportunidades que ofrece la Sociedad de la Información. En particular, INTECO dispone de amplia experiencia en el desarrollo de proyectos en el ámbito de la accesibilidad para la televisión digital, así como de aquellos orientados a garantizar los derechos de los ciudadanos a relacionarse con las administraciones públicas por medios electrónicos, reconocidos en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos

- **Calidad TIC**: INTECO promueve unos servicios de la Sociedad de la Información que cada vez sean de mayor calidad, que garanticen unos adecuados niveles de servicio, lo cual se traduce en una mayor robustez de aplicaciones y sistemas, un compromiso en la disponibilidad y los tiempos de respuesta, un adecuado soporte para los usuarios, una información precisa y clara sobre la evolución de las funcionalidades de los servicios, y en resumen, servicios cada vez mejores. En esta línea impulsa la competitividad de la industria del Software a través de la promoción de la mejora de la calidad y la certificación de las empresas y profesionales de la ingeniería del software, a través del Laboratorio Nacional de Calidad del Software.

- **Formación**: la formación es un factor determinante para la atracción de talento y para la mejora de la competitividad de las empresas. Por ello, INTECO impulsa la formación de universitarios y profesionales en las tecnologías más demandadas por la industria.

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 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 las Tecnologías de la Información y la Comunicación, con especial énfasis en la Seguridad y privacidad en Internet.

- 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 y la confianza con una perspectiva temporal.
- Impulso de proyectos de investigación en materia de seguridad TIC.
- 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 confianza en la Sociedad de la Información.
- Asesoramiento a las Administraciones Públicas en materia de seguridad de la información 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* persigue 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 las incidencias sufridas. El presente informe constituye la 8ª 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 la actualización para el 3er cuatrimestre de 2011 de los datos de usuarios basados en entrevistas comparando estos resultados con los obtenidos en el 2º cuatrimestre de 2011 y, de esta manera, poder ofrecer un análisis evolutivo de 2011. Adicionalmente, en los casos en los que la comparabilidad sea posible por la existencia de datos anteriores se realiza un análisis interanual desde 2009 a 2011.

2 DISEÑO METODOLÓGICO

El *Estudio sobre seguridad de los dispositivos móviles y smartphones (Informe anual 2011)* se realiza a partir de una metodología basada en el panel online 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 internautas españoles mayores de 15 años con acceso frecuente a la Red 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 octava entrega del estudio.

2.1 UNIVERSO

Usuarios españoles de Internet mayores de 15 años con acceso frecuente a Internet desde el hogar. 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

La afijación muestral responde a un modelo polietápico:

- Estratificación por Comunidades Autónomas para garantizar un mínimo de sujetos en cada una de ellas.
- Muestreo por cuotas de tamaño del hogar, edad, sexo, actividad laboral y tamaño del hábitat[1].

La Tabla 1 presenta el tamaño de la muestra correspondiente a la encuesta.

[1] Estas cuotas se han obtenido de datos representativos a Nivel Nacional de Usuarios españoles de Internet de 15 a 74 años, con una frecuencia de uso de Internet al menos mensual desde su casa. Datos elaborados a partir de los obtenidos de la Encuesta sobre Equipamiento y Uso de Tecnologías de la Información y Comunicación en los hogares 2010, INE.

Tabla 1: Tamaños muestrales para la encuesta

Período	Tamaño muestral
4º trimestre 2009	3.640
1er trimestre 2010	3.599
2º trimestre 2010	3.519
3er trimestre 2010	3.538
4º trimestre 2010	3.571
2º cuatrimestre 2011	2.405
3er cuatrimestre 2011	3.655

Fuente: INTECO

2.3 TRABAJO DE CAMPO Y ERROR MUESTRAL

El trabajo de campo ha sido realizado entre septiembre y diciembre de 2011 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 igual o inferior a ±2% en cada uno de los períodos analizados, tal y como se recoge en la siguiente tabla.

Tabla 2: Errores muestrales de las encuesta (%)

Período	Tamaño muestral	Error muestral
4º trimestre 2009	3.640	±1,66%
1er trimestre 2010	3.599	±1,66%
2º trimestre 2010	3.519	±1,68%
3er trimestre 2010	3.538	±1,68%
4º trimestre 2010	3.571	±1,68%
2º cuatrimestre 2011	2.405	±2,00%
3er cuatrimestre 2011	3.655	±1,62%

Fuente: INTECO

3 SEGURIDAD EN DISPOSITIVOS MÓVILES Y SMARTPHONES

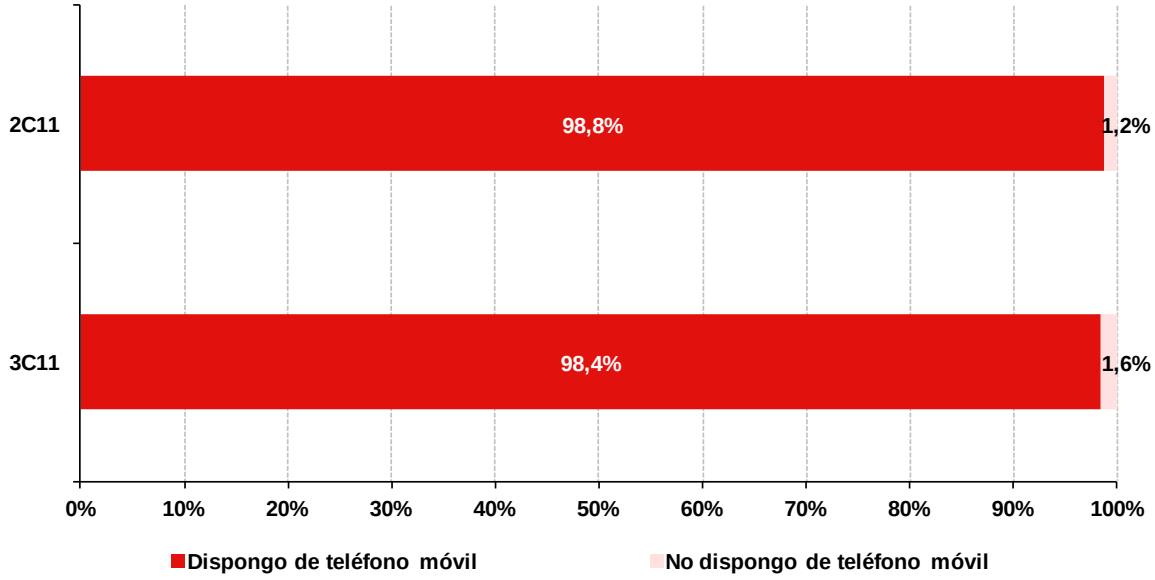
No hace muchos años los terminales móviles se encontraban aislados de muchos riesgos de seguridad al no estar interconectados con la Red. Pero actualmente, la inmensa mayoría incluye mecanismos para que puedan conectarse y descargar contenido de Internet, leer el correo electrónico, etc., y por tanto, enfrentarse a las mismas amenazas de seguridad que los equipos.

Es por esto que, se hace necesario un análisis de las prestaciones que incorporan actualmente los terminales móviles y cómo las aprovechan los internautas. También, cómo afectan estas prestaciones en los hábitos de los usuarios en cuestión de seguridad.

3.1 EXTENSIÓN Y PRESTACIONES QUE INCORPORAN

En el 3er cuatrimestre de 2011 casi la totalidad de los usuarios (98,4%) dispone de un teléfono móvil, reflejándose la amplia distribución y arraigo del uso de esta tecnología. Este dato se mantiene constante respecto al cuatrimestre anterior.

Gráfico 1: Usuarios que disponen de teléfono móvil (%)



Base: Total usuarios (n= 3.655 en 3er cuatrimestre2011) *Fuente: INTECO*

¿Qué características adicionales al teléfono móvil convencional presenta un smartphone? La principal característica adicional que además supone la diferencia más significativa entre ambos es que el smartphone dispone de sistema operativo móvil y el teléfono móvil convencional no.

Los principales fabricantes han desarrollado sistemas operativos móviles que permiten la gestión de los procesos informáticos del dispositivo, así como el funcionamiento de otros programas y aplicaciones que se instalan posteriormente.

¿Qué sistemas operativos utilizan los smartphones?

Según el análisis relacionado con el número de ventas en 2011[2] se encuentran los siguientes sistemas operativos:

Android: diseñado, potenciado y mantenido por Google, supone el sistema operativo con mayor penetración a nivel mundial, copando el 50,9% del volumen de ventas durante el 4º trimestre de 2011. Es de código abierto y totalmente personalizable.

iOS: sistema operativo propietario, creado por Apple para sus iPhones, iPads e iPods. De carácter cerrado, es el segundo sistema operativo por cuota de uso (23,8%) durante 2011.

Symbian: perteneciente a la empresa noruega Nokia, tiene un 11,7% de uso y actualmente es utilizado principalmente en sus terminales de gama media y baja.

Blackberry: propiedad de RIM. Originalmente enfocado al mundo empresarial es el que mayor descenso de uso ha sufrido (ocupa en 2011 el cuarto lugar con un 8,8%).

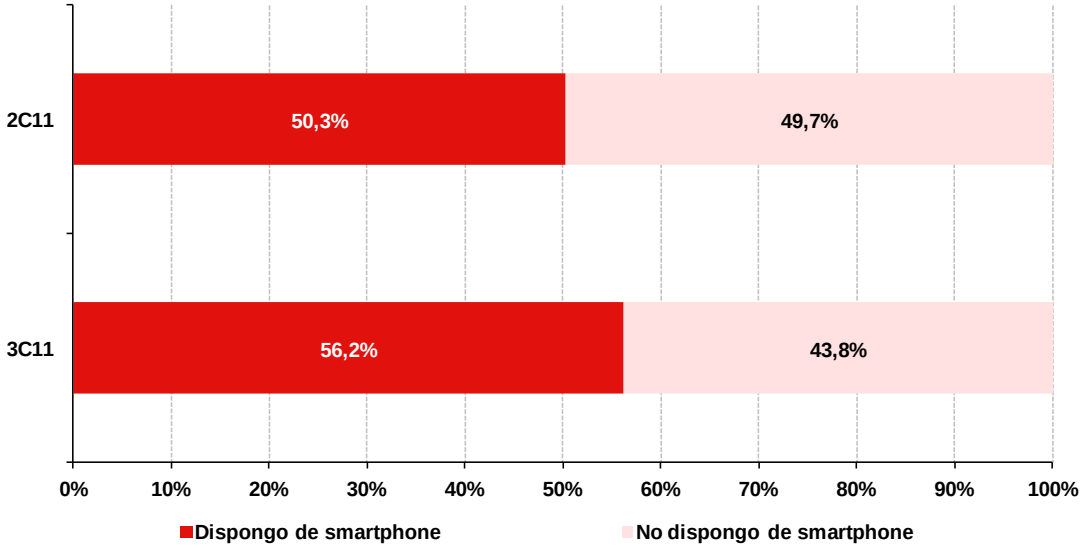
Existen otros sistemas operativos en auge como los de las compañías Microsoft o Samsung, conocidos como Windows Phone 7 y Bada respectivamente.

En el presente estudio se han analizado aquellos panelistas que disponen de móviles smartphone capaces de conectarse a la red (negación, correo, redes sociales, realizar descargas…)

Desde, aproximadamente el año 2007, su popularización ha crecido sustancialmente, desplazando a los teléfonos tradicionales. En este año, un 56,2% de los encuestados con teléfono móvil dispone ya de este tipo de terminal de última generación, lo cual supone un aumento considerable de casi 6 puntos porcentuales con respecto a la anterior oleada (50,3%).

[2]Gartner. *Gartner Says Worldwide Smartphone Sales Soared in Fourth Quarter of 2011 With 47 Percent Growth*. Disponible en: http://www.gartner.com/it/page.jsp?id=1924314

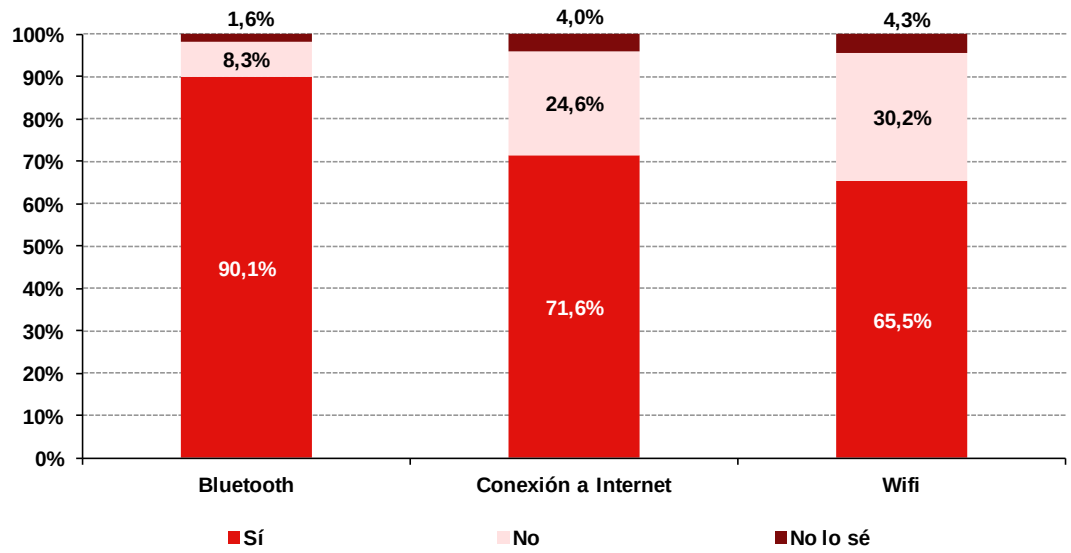
Gráfico 2: Usuarios que disponen de teléfono móvil smartphone (%)



Base: Usuarios que disponen de teléfono móvil (n=3.597 en 3er cuatrimestre2011) *Fuente: INTECO*

¿Qué tecnologías incorporan los teléfonos móviles de los usuarios en la actualidad? Por un lado, se ve la estandarización e implementación del bluetooth en un alto número de terminales, con un 90,1% de encuestados que declara disponer esta tecnología en el teléfono móvil. Por otro, también se declara evidente el alto uso de Internet vía móvil con un 71,6 % gracias a la proliferación de las denominadas "tarifas planas" de cada operador móvil. Por último, la disponibilidad de conexión wifi también se sitúa en un alto porcentaje con un 65,5%.

Gráfico 3: Usuarios que disponen de móvil con bluetooth, conexión a Internet y wifi (%)

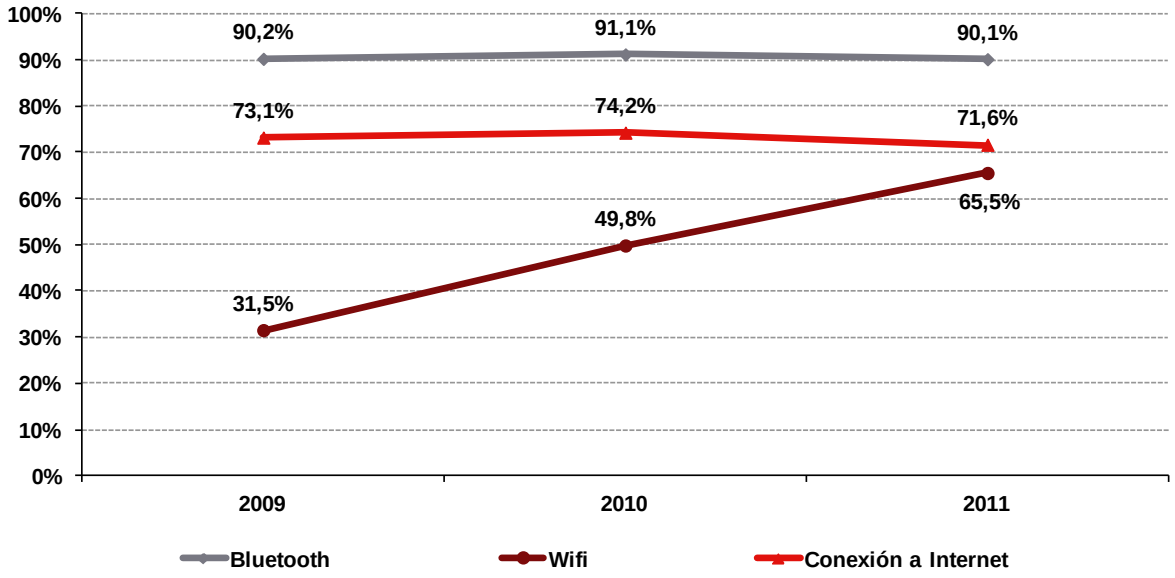


Base: Usuarios que disponen de teléfono móvil (n=3.597 en 3er cuatrimestre2011) *Fuente: INTECO*

El Gráfico 4 muestra la evolución interanual de 2009 a 2011 en lo que respecta a la disponibilidad de teléfono móvil con tecnología bluetooth, conexión a Internet o wifi. Para este análisis, tanto en 2009 como en 2010 se ha tomado el dato del último trimestre del año y en 2011 el del último cuatrimestre[3].

Como reflejo del cambio registrado durante estos últimos años, se puede ver como la presencia de conexiones wifi en los terminales ha crecido hasta implantarse con un 65,5% en el último cuatrimestre de 2011, incrementándose 34 puntos porcentuales desde finales de 2009. Tanto la disponibilidad de teléfono móvil con tecnología bluetooth como con conexión a Internet presentan porcentajes similares a lo largo de estos tres años.

Gráfico 4: Evolución de usuarios que disponen de teléfono móvil con tecnología bluetooth, conexión a Internet o wifi entre 2009 y 2011 (%)



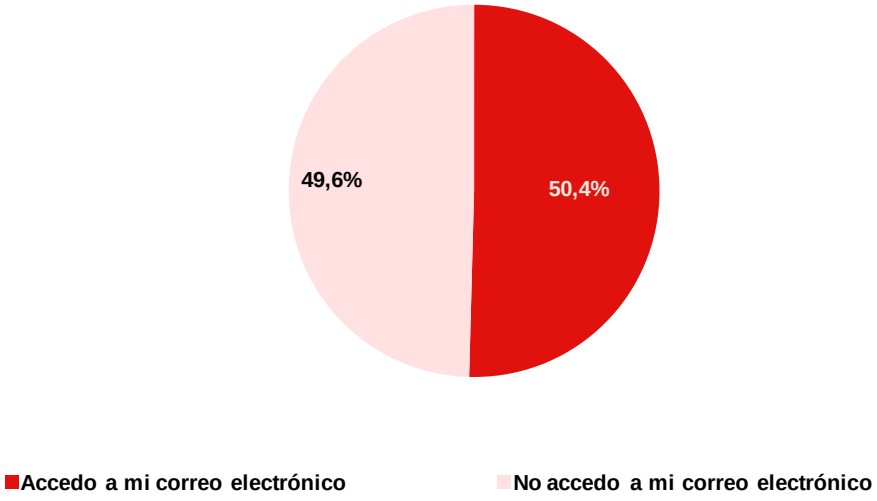
Base: Usuarios que disponen de teléfono móvil (n=3.597 en 3er cuatrimestre2011) *Fuente: INTECO*

3.2 HÁBITOS DE USO DEL TELÉFONO MÓVIL

¿Cómo utilizan los usuarios las aplicaciones y prestaciones incorporadas en sus teléfonos móviles? El siguiente gráfico muestra qué porcentaje de usuarios consultan el email en su terminal. La mitad de los internautas con dispositivo móvil (50,4%) lee su correo electrónico a través de su dispositivo móvil.

[3] Para este gráfico y para todos los que ofrezcan un análisis interanual para 2009 y 2010 se toma el dato del último trimestre del año y en 2011 el del último cuatrimestre, lo mismo para las tablas que puedan existir.

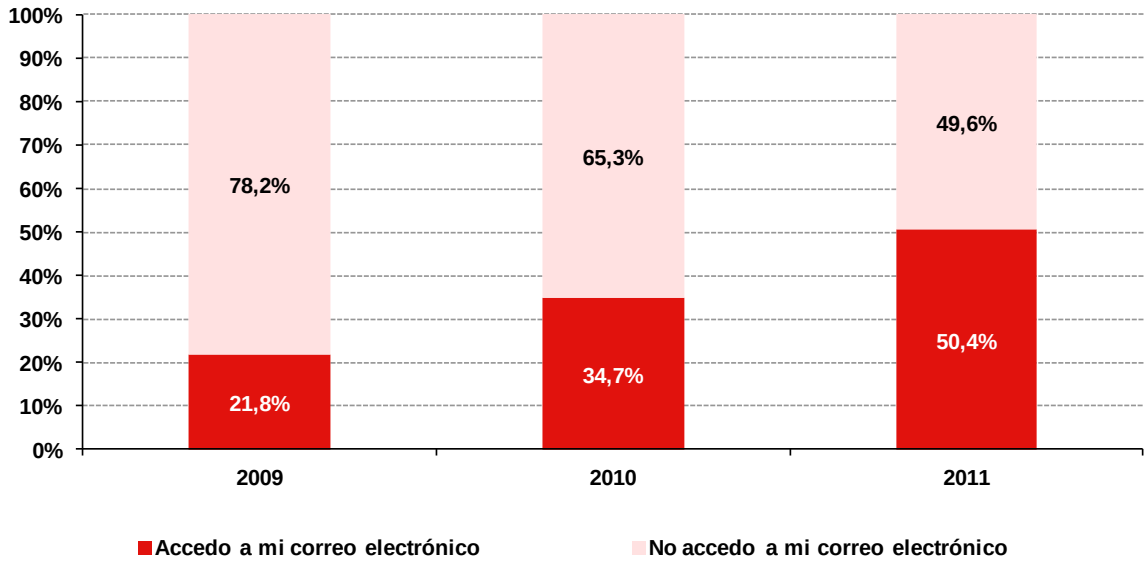
Gráfico 5: Usuarios que acceden al correo electrónico desde el teléfono móvil (%)



Base: Usuarios que disponen conexión a Internet o wifi (n=2.812) *Fuente: INTECO*

Los datos recogidos a finales de 2009, 2010 y 2011 ponen de manifiesto que los usuarios muestran cada vez más preferencia por la utilización de teléfonos móviles para acceder a las cuentas de correo electrónico (valor que ha experimentado una subida de 28,6 puntos porcentuales en el 3er cuatrimestre de 2011 con respecto al valor del mismo período dos años antes).

Gráfico 6: Evolución de usuarios que acceden al correo electrónico desde el teléfono móvil entre 2009 y 2011 (%)

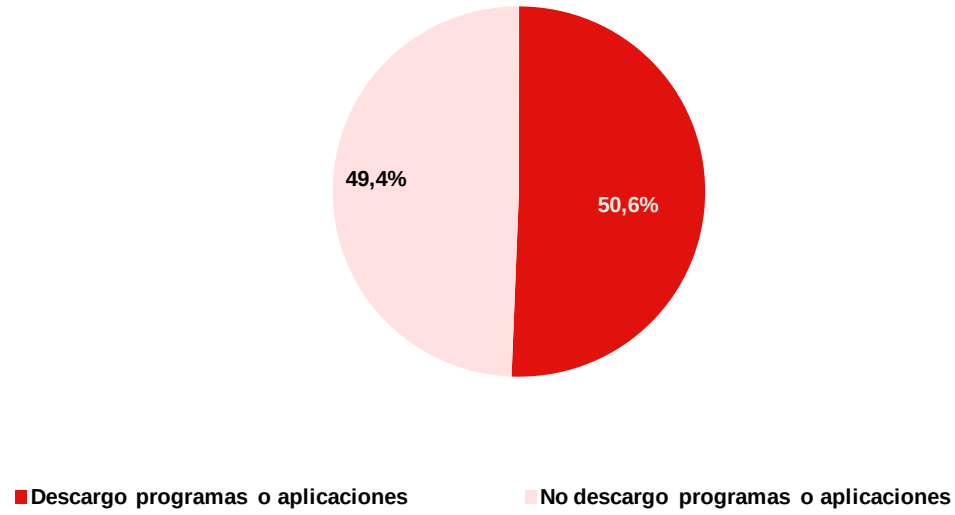


Base: Usuarios que disponen conexión a Internet o wifi (n=2.812 en 3er cuatrimestre de 2011) *Fuente: INTECO*

Una de las características que incorporan la mayoría de móviles de hoy en día, es que son capaces de ejecutar programas y aplicaciones que añaden funcionalidad al aparato, además de permitir la descarga directa de diferentes tipos de ficheros (habitualmente multimedia u ofimáticos). A continuación se muestra que porcentaje de usuarios descarga ficheros o programas en su terminal.

El acceso a descargas desde el móvil (50,6%) es similar al porcentaje de utilización del correo, revelando el uso intensivo de este tipo de terminales por parte de los usuarios, que aprovechan al máximo sus características. La conexión a Internet les permite consultar el correo y la descarga de archivos y, en igual medida, aprovechan estas prestaciones.

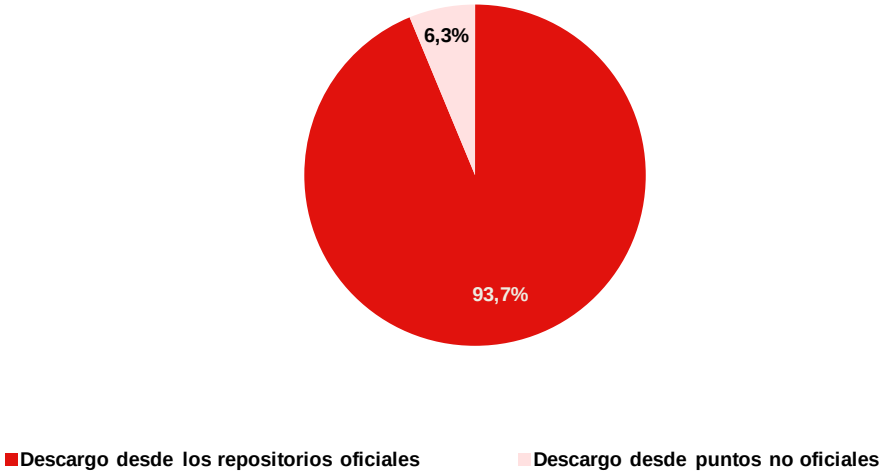
Gráfico 7: Usuarios que descargan programas o aplicaciones en el teléfono móvil (%)



Base: Usuarios que disponen conexión a Internet o wifi (n=2.812 en 3er cuatrimestre de 2011)
Fuente: INTECO

Tan importante es analizar en qué medida se usa el terminal para la descarga de programas o aplicaciones como el lugar de donde provienen esos ficheros. Al igual que ocurre con los equipos de sobremesa, ejecutar o utilizar programas y archivos que provienen de fuentes dudosas puede suponer un problema de seguridad. El Gráfico 8 muestra qué un 93,7% descarga los programas o aplicaciones en su teléfono móvil desde sitios oficiales (como *AppStore* de Apple, *Play Store* de Google o *App World* para Blackberry) reflejando este buen hábito de seguridad establecido entre los usuarios que disponen de teléfono móvil.

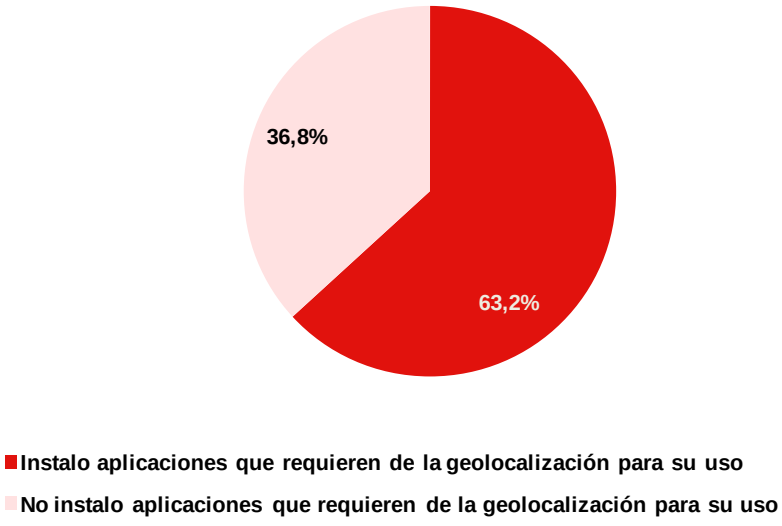
Gráfico 8: Lugar de descarga de programas o aplicaciones (%)



Base: Usuarios que descargan programas o aplicaciones en el teléfono móvil (n=1.388) *Fuente: INTECO*

El porcentaje de usuarios que hace uso de aplicaciones que utilizan geolocalización se sitúa a finales de 2001 en un 63,2%. Algunos ejemplos habituales de programas que hacen uso de esta tecnología son las cámaras fotográficas integradas y sistemas de localización de usuarios, que utilizan los datos de geolocalización para situar al móvil en el mapa o almacenar los datos de dónde se realiza una fotografía. Esto podría derivar en un riesgo para la privacidad del usuario teniendo como ejemplo muy actual los recientes cambios de política de privacidad de Google[4].

Gráfico 9: Usuarios que usan servicios de geolocalización a través del teléfono móvil (%)



Base: Usuarios que descargan programas o aplicaciones en el teléfono móvil (n=1.388) *Fuente: INTECO*

[4] ElPais. *Cambios en la política de* Google. Disponible en: http://tecnologia.elpais.com/tecnologia/2012/01/25/actualidad/1327483852_263916.html

3.3 MEDIDAS DE SEGURIDAD UTILIZADAS EN EL TELÉFONO MÓVIL

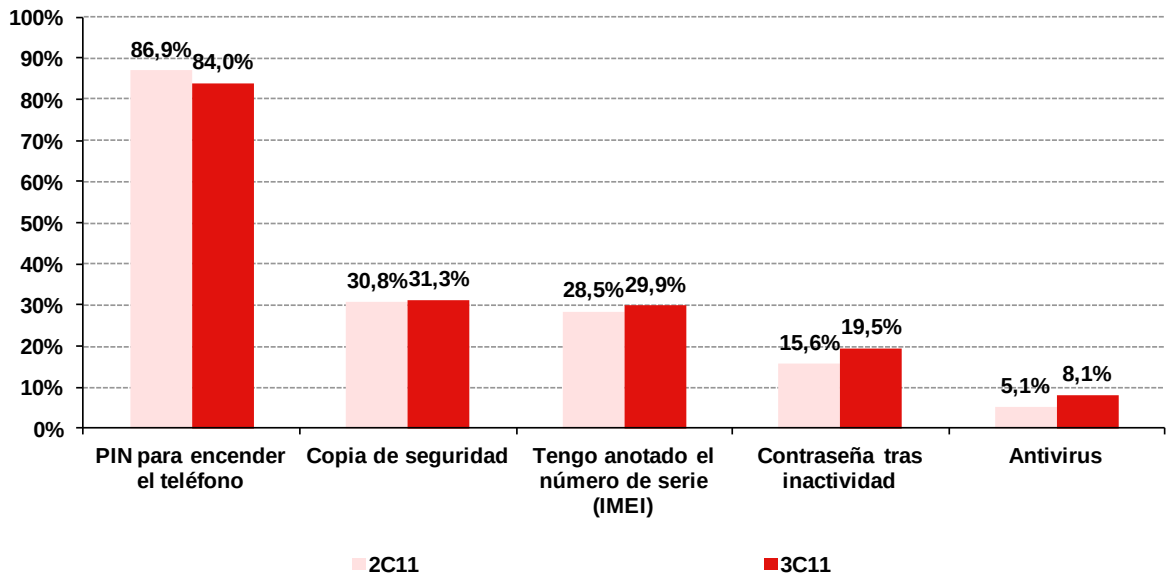
¿Cómo protegen los usuarios sus terminales? ¿Utilizan herramientas y medidas de seguridad? ¿Tienen en cuenta el riesgo potencial que representan las tecnologías y servicios asociadas a estaos nuevos dispositivos? Las buenas prácticas y hábitos seguros en el uso del teléfono móvil reflejan el grado de conciencia sobre la seguridad que el usuario aplica sobre los dispositivos, y se estudian en el presente apartado.

A continuación se analiza en qué medida los panelistas llevan a cabo buenas prácticas en sus teléfonos móviles para estar protegidos ante incidencias de seguridad.

Sigue siendo generalizado el empleo de código PIN en los panelistas (84%) como medida principal de protección del dispositivo, aunque desciende ligeramente en comparación con el cuatrimestre anterior, en contrapunto al aumento del uso de contraseñas tras la inactividad (cerca de 4 puntos porcentuales) situándose a finales de 2011 en un 19,5%. También el uso de antivirus con un 8,1%, aumenta 3 puntos porcentuales. Otras medidas preventivas como copias de seguridad y tener anotado el número de serie (IMEI) se mantienen relativamente estables a lo largo de 2011.

Con respecto a la anterior, la práctica de anotar el IMEI del terminal permanece en valores contantes cercanos al 30%, aumentando ligeramente. Un 29,9% afirma que realiza este buen hábito. Mantener en un lugar seguro el número IMEI del teléfono permite identificarlo y podría permitir su desactivación remota o identificación en caso de robo o pérdida.

Gráfico 10: Medidas de seguridad utilizadas / instaladas en el teléfono móvil (%)

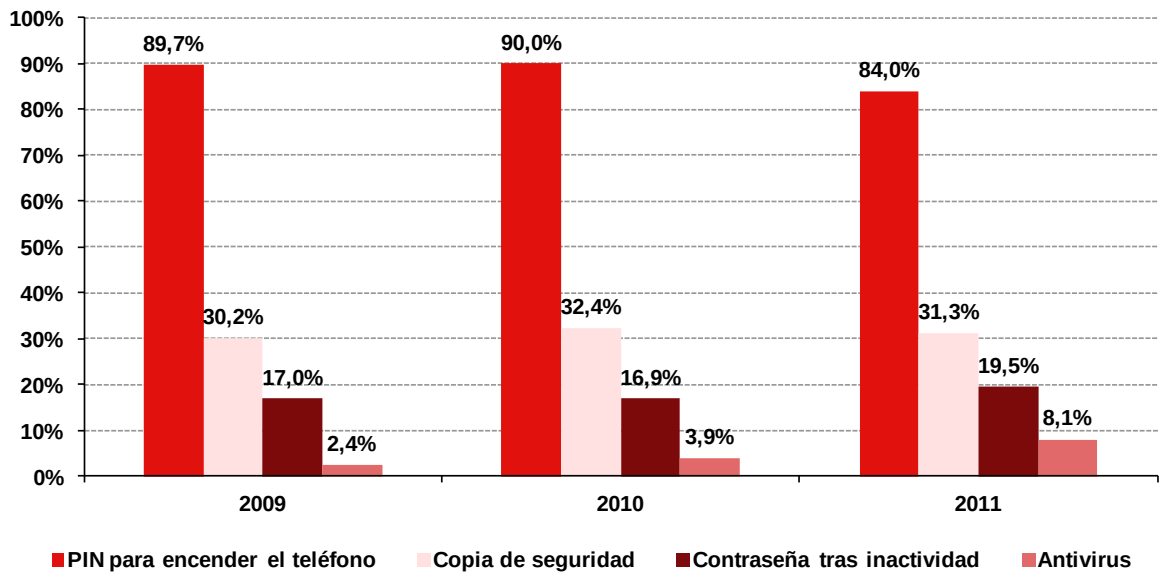


Base: Usuarios que disponen de teléfono móvil (n=3.597 en 3er cuatrimestre2011) *Fuente: INTECO*

De la evolución anual entre 2009 y 2011 de las medidas de seguridad utilizadas / instaladas en el teléfono móvil cabe destacar el aumento paulatino del uso de antivirus en los terminales de los usuarios. Aunque, presentando porcentajes no muy elevados, ha aumentado 5,7 puntos porcentuales durante estos dos años.

Las demás medidas, tanto el uso del PIN para encender el teléfono, como la realización de copias de seguridad de los contactos y/u otro tipo de datos del teléfono móvil (fotografías, documentos, etc.), o la activación de una contraseña para desbloquear el terminal tras un periodo de inactividad, presentan valores constantes a lo largo de 2009 a 2011.

Gráfico 11: Evolución de las medidas de seguridad utilizadas / instaladas en el teléfono móvil entre 2009 y 2011(%)



Base: Usuarios que disponen de teléfono móvil (n=3.597 en 3er cuatrimestre2011) *Fuente: INTECO*

Con respecto a la utilización del bluetooth, se observan los hábitos de uso de esta tecnología en el Gráfico 12. En el 3er cuatrimestre de 2011 un 57,3% toma las medidas necesarias y enciende el bluetooth sólo cuando lo necesita. Es relativamente bajo (16,7%) el número de panelistas que, en contraste y como mal hábito, lo mantiene encendido como norma habitual.

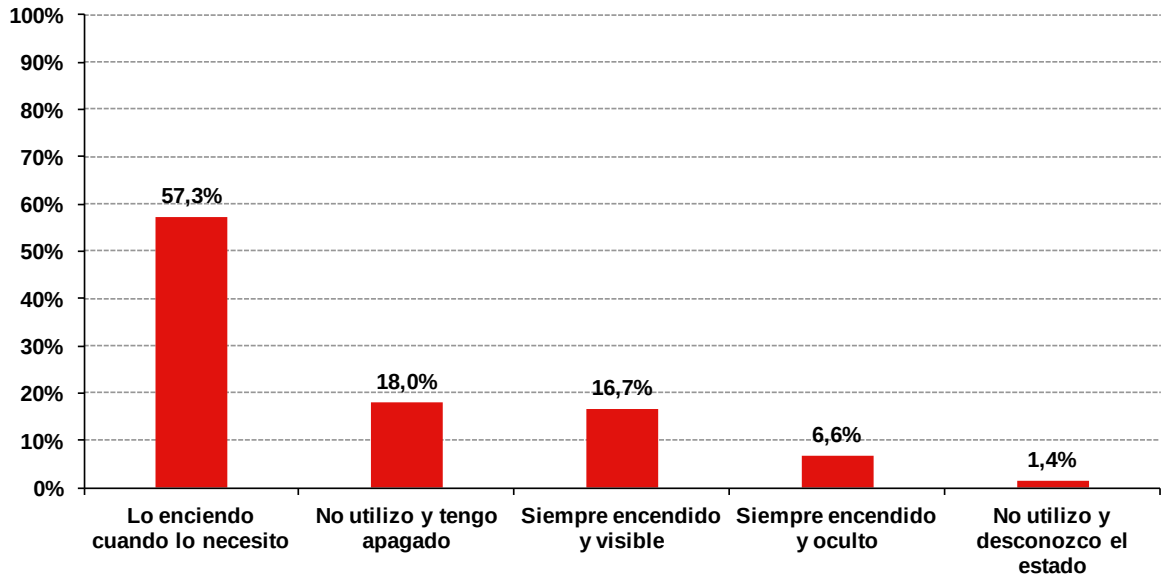
La ocultación de las conexiones bluetooth cuando no se estén utilizando supone un buen hábito de seguridad porque evita posibles intentos de conexión exterior, envíos de mensajes de correo basura o invitaciones fraudulentas. Si, además de ocultar la conexión, se desactiva, se ahorrará batería en el dispositivo.

También existen usuarios que disponiendo de este tecnología no la utilizan, a finales de 2011 un 18% así lo declara. En este sentido, cabe apuntar que actualmente existe una

generalización de otras tecnologías de intercambio directo o comunicación vía wifi, 3G/GRPS o NFC. Muchos usuarios utilizan aplicaciones que ya integran el envío y recepción de imágenes y ficheros (por ejemplo la aplicación *Whatsapp*) facilitando ese intercambio y evitando el posible uso de bluetooth.

> **NFC** son las siglas en inglés de *Near Field Communication*, una tecnología de comunicación inalámbrica de corto alcance y alta frecuencia que permite el intercambio de datos entre dispositivos a menos de 10 centímetros.

Gráfico 12: Hábitos de uso del bluetooth (%)



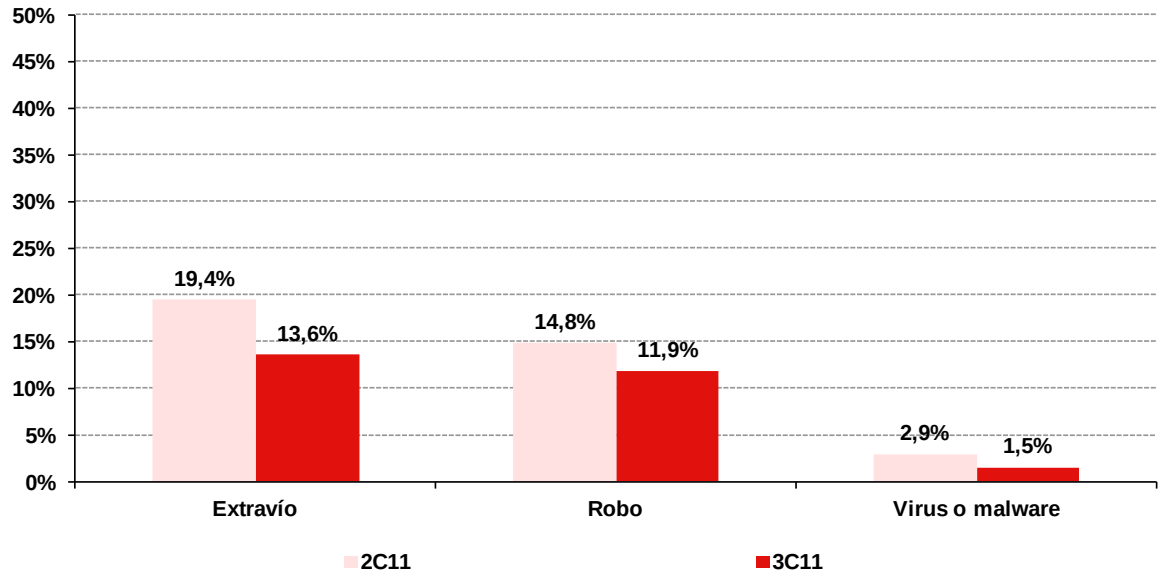
Base: Usuarios que disponen de bluetooth (n=3.241) *Fuente: INTECO*

3.4 INCIDENCIAS DE SEGURIDAD

En este apartado se analiza las incidencias de seguridad que los usuarios han sufrido en sus teléfonos móviles. Se les pregunta a los panelistas tanto si les han robado el terminal, como si lo han extraviado, o si han padecido infección por virus o malware en sus dispositivos. Además, se profundiza en si han sufrido fraude a telefónico especificando que tipo de incidencia han sufrido y si este hecho ha derivado en un perjuicio económico.

En el 3er cuatrimestre de 2011 la incidencia de seguridad más declarada por los usuarios españoles es el extravío del terminal (13,6%), seguido del robo del mismo (11,9%) y de la infección por virus o malware (1,5%). Estas tres incidencias sufren un ligero descenso si se comparan con los datos del cuatrimestre anterior, siendo el descenso más significativo el de la pérdida del teléfono móvil con 5,8 puntos porcentuales menos.

Gráfico 13: Incidencias de seguridad ocurridas en el uso del teléfono móvil (posibilidad de respuesta múltiple) (%)



Base: Usuarios que disponen de teléfono móvil (n=3.597 en 3er cuatrimestre2011) *Fuente: INTECO*

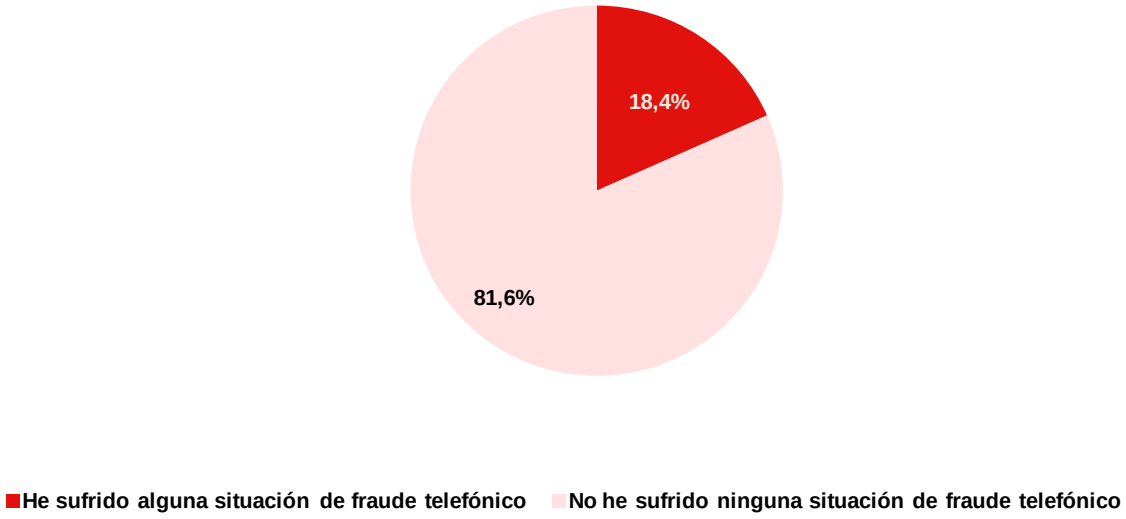
Continuando con el análisis de las incidencias sufridas en los teléfonos móviles de los usuarios, se estudia a continuación la incidencia declarada de situaciones de intento de fraude telefónico en los últimos tres meses. Para la interpretación correcta de los datos, es necesario realizar dos puntualizaciones previas:

- En primer lugar, los datos proporcionados están basados en las respuestas a la encuesta aplicada al panel de usuarios de Internet españoles, ofreciendo por tanto la perspectiva del ciudadano. Esta percepción, según la sofisticación de los ataques, puede haber permitido o no identificar las posibles amenazas.

- En segundo lugar, no debe entenderse que las personas que afirman haber experimentado alguna de las situaciones analizadas son efectivamente víctimas de fraude telefónico. Se habla, por tanto, de intento de fraude y no de fraude consumado.

A finales de 2011, un 18,4% de los encuestados declara haber sido objeto de algún intento de fraude telefónico (no consumado), frente a un 81,6% que no han constatado una situación de este tipo.

Gráfico 14: Incidencia declarada de situaciones de intento (no consumado) de fraude telefónico en los últimos tres meses (%)



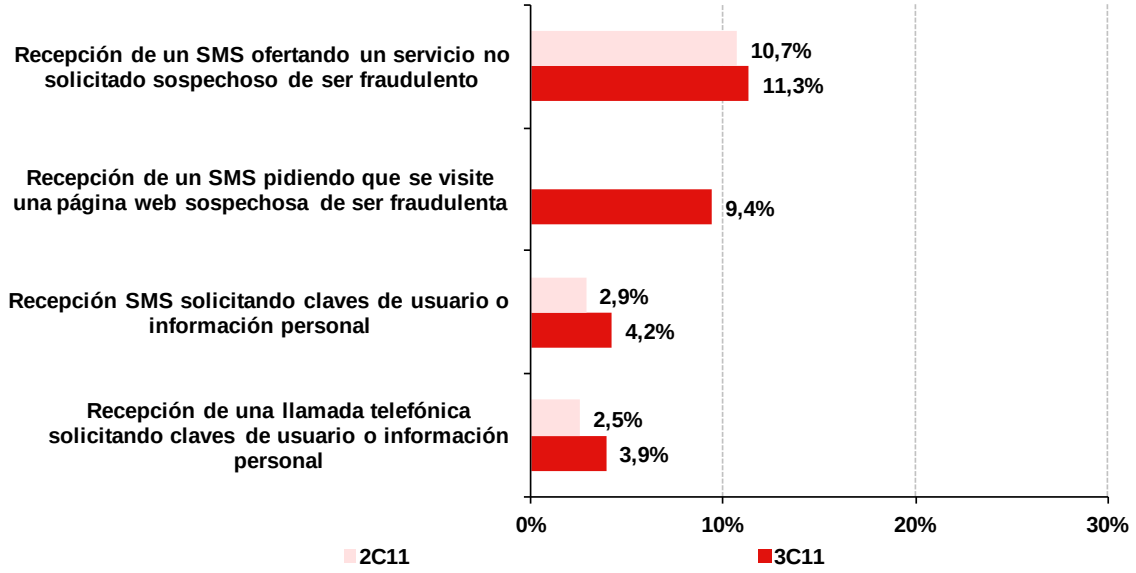
Base: Total usuarios (n= 3.655) *Fuente: INTECO*

El siguiente gráfico ofrece más detalle en cuanto a las incidencias de fraude telefónico qué más perciben los encuestados, con una perspectiva evolutiva al comparar los datos del 3er cuatrimestre de 2011 con los del cuatrimestre anterior.

La circunstancia más común es recibir mensajes cortos de texto que ofrecen servicios que el usuario no ha requerido (11,3%). Muy cercano a este porcentaje, se encuentra el de la recepción de un SMS pidiendo que se visite una página web sospechosa de ser fraudulenta (9,4%). Con valores más inferiores se encuentra la solicitud de claves de usuario o información personal, ya sea mediante mensaje corto de texto (4,2%) o mediante una llamada telefónica (3,9%).

En cuanto a la perspectiva evolutiva que se obtiene al comparar los datos actuales con los del 2º cuatrimestre de 2011 destaca que los valores de todas las situaciones de intento de fraude telefónico aumentan.

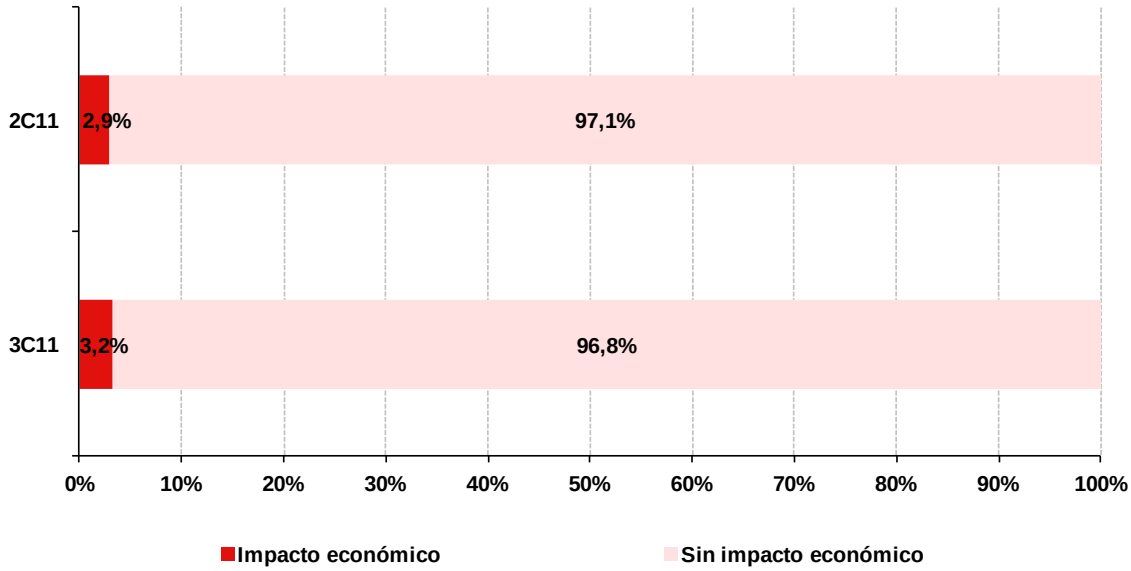
Gráfico 15: Evolución de la incidencia declarada de situaciones de intento (no consumado) de fraude telefónico en los últimos 3 meses (%)



Base: Total usuarios (n= 3.655 en 3er cuatrimestre 2011) *Fuente: INTECO*

Se analiza, para finalizar, el impacto económico provocado por los intentos de fraude telefónico (SMS o llamada telefónica). A finales de 2011, un 3,2% de los usuarios declara haber sufrido un perjuicio económico (frente a un 96,8% que contesta negativamente). Este dato supone un ligero aumento comparado con el dato del 2º cuatrimestre del año que se situaba en un 2,9%.

Gráfico 16: Evolución del fraude con impacto económico para el usuario (%)



Base: Total usuarios (n= 3.655 en 3er cuatrimestre 2011) *Fuente: INTECO*

4 CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES DEL ANÁLISIS

Cada vez son más las prestaciones incorporadas en los teléfonos móviles, así como las medidas de seguridad disponibles. Queda de manifiesto en el aumento del número de usuarios que disponen en su terminal de características de comunicación avanzadas como bluetooth, 3G (o conexión directa a Internet) y tecnología wifi y del uso de medidas de seguridad alternativas (como el bloqueo en espera) o aplicaciones antivirus.

Por otro lado, durante 2011 la tendencia al alza de aparición de malware específico para plataformas móviles ha sido clara y contundente. Así, para una de las plataformas más populares (Android, el sistema operativo para móviles más usado actualmente en España[5]), el malware se ha incrementado un 472% desde julio de 2010 hasta noviembre de 2011[6]. La mayoría de este malware se propaga a través de aplicaciones camufladas (alojadas tanto en repositorios oficiales como extraoficiales).

Los usuarios han atacado este problema desde dos frentes claros:

- Protegiendo su dispositivo con productos antivirus específicos para móviles. Así lo confirma el 8,1% de usuarios que declara hacer uso de este tipo de software. El porcentaje, aunque bajo, está condicionado por la escasa cantidad de productos antivirus en oferta para muchas de las plataformas existentes (por ejemplo, el smartphone iPhone de Apple, carece de productos de este tipo).

- Aumentando el uso de repositorios oficiales para la descarga de aplicaciones, que este último cuatrimestre del año llega al 93,7%. Así evitan los repositorios no oficiales susceptibles de contener malware.

Aun así, es necesario explicar los riesgos inherentes incluso a las propias medidas de seguridad. El usuario debe entender que los productos antivirus no son infalibles, y que deben ser combinados con otras medidas de seguridad proactivas. Un estudio reciente publicado en noviembre de 2011, afirmaba que "*La mayoría de los antivirus gratuitos para Android son inservibles*"[7], donde se sometían a diferentes productos del mercado a una batería de pruebas que pocos superaban con unas mínimas garantías.

[5] StatCounter. Disponible en: http://gs.statcounter.com/#mobile_os-ES-quarterly-200803-201104

[6] CNET News. *Android leads the way in mobile malware*. Disponible en: http://news.cnet.com/8301-1009_3-57325774-83/android-leads-the-way-in-mobile-malware/

[7] DiarioTi. La mayoría de los antivirus gratuitos para Android son inservibles. Disponible en: http://www.diarioti.com/noticia/La_mayoria_de_los_antivirus_gratuitos_para_Android_son_inservibles/30780

Por otro lado, se han dado casos en los que los atacantes han conseguido mantener, al menos durante un tiempo, malware en repositorios oficiales, por lo que no se debe confiar ciegamente en las aplicaciones de mercados autorizados, especialmente los que no controlan de manera robusta la publicación de aplicaciones.

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.

- Tener localizado el terminal en todo momento, para evitar el robo o acceso indebido por terceros.
- Conocer el número de IMEI[8] (marcar en el teléfono *#06# para que lo muestre en la pantalla) que permite al usuario (a través de la operadora de telefonía móvil) desactivar el terminal en caso de pérdida o robo.
- Tener activado el número PIN para que cada vez que se encienda el teléfono el acceso no sea automático.
- Realizar copias de seguridad de los contenidos de los que se disponga en el terminal.
- Activar el bloqueo automático del teléfono móvil para evitar que personas no autorizadas puedan acceder a los datos.
- Cifrar la información sensible en la memoria del teléfono.
- En entornos corporativos en los que se maneja información altamente sensible, resulta más seguro conectarse a servidores seguros para acceder a la información, en vez de alojarla en el dispositivo.
- Desactivar la conexión bluetooth, WIFI y 3G (siempre que sea posible esta opción) cuando no se esté usando.
- Evitar descargar aplicaciones o archivos desde Internet con origen poco confiable. Si se realiza una conexión entre dispositivos (de móvil a móvil, o de móvil a ordenador), comprobar que ninguno de ellos se encuentre comprometido o aloje archivos infectados.

[8] *International Mobile Equipment Identity.*

- Revisar las solicitudes de permisos que aparecen, por ejemplo, al realizar acciones como descargar ficheros y aplicaciones. Antes de aceptar estas solicitudes, es necesario comprender y valorar a qué se está dando permiso (por ejemplo, acceso a la tarjeta de memoria, conexión a Internet, intercambio de datos, etc.).

- Vigilar el consumo y, en caso de notar incrementos bruscos en la factura, verificarlo con la compañía, ya que puede ser un indicio de fraude o de uso indebido.

- Mantener el software del móvil actualizado.

- Configurar el dispositivo para que no se puedan instalar programas que no estén certificados y/o de fuente desconocida.

- A la hora de deshacerse del terminal, realizar un borrado seguro y definitivo de la información almacenada en el mismo.

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

Síguenos a través de:

Web

Envíanos tus consultas y comentarios a:

observatorio@inteco.es

Instituto Nacional
de Tecnologías
de la Comunicación