

Estudio sobre la seguridad de las comunicaciones móviles e inalámbricas en los hogares españoles

Informe anual 2009



Edición: Junio 2010

El “Estudio sobre la seguridad de las comunicaciones móviles e inalámbricas en los hogares españoles (Informe anual 2009)” ha sido elaborado por el siguiente equipo de trabajo del Observatorio de la Seguridad de la Información de INTECO:

Pablo Pérez San-José (Coordinador)

Susana de la Fuente Rodríguez

Laura García Pérez

Cristina Gutiérrez Borge

Javier Rey Perille

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

SIGMADOS



La presente publicación pertenece al **Instituto Nacional de Tecnologías de la Comunicación (INTECO)** y está bajo una licencia Reconocimiento-No comercial 2.5 España de Creative Commons, y por ello esta permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:

- **Reconocimiento:** El contenido de este informe se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa tanto a INTECO como a su sitio web: www.inteco.es. Dicho reconocimiento no podrá en ningún caso sugerir que INTECO presta apoyo a dicho tercero o apoya el uso que hace de su obra.
- **Uso No Comercial:** El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de INTECO como titular de los derechos de autor. Nada en esta licencia menoscaba o restringe los derechos morales de INTECO. <http://creativecommons.org/licenses/by-nc/2.5/es/>

El presente documento cumple con las condiciones de accesibilidad del formato PDF (Portable Document Format). Así, se trata de un documento estructurado y etiquetado, provisto de alternativas a todo elemento no textual, marcado de idioma y orden de lectura adecuado.

Para ampliar información sobre la construcción de documentos PDF accesibles puede consultar la guía disponible en la sección Accesibilidad > Formación > Manuales y Guías de la página <http://www.inteco.es>

ÍNDICE

PUNTOS CLAVE	4
I Seguridad de las comunicaciones móviles e inalámbricas de los hogares	4
1 INTRODUCCIÓN Y OBJETIVOS	6
1.1 Presentación	6
1.2 Estudio sobre la seguridad de las comunicaciones móviles e inalámbricas en los hogares españoles.....	8
2 DISEÑO METODOLÓGICO	9
2.1 Universo	9
2.2 Tamaño y distribución muestral	9
2.3 Trabajo de campo y error muestral	10
3 SEGURIDAD DE LAS COMUNICACIONES DE TELEFONÍA MÓVIL.....	11
3.1 Extensión del teléfono móvil y prestaciones que incorpora	11
3.2 Hábitos de uso del teléfono móvil	13
3.3 Medidas de seguridad utilizadas en el teléfono móvil.....	15
3.4 Incidencias de seguridad	16
4 SEGURIDAD DE LAS CONEXIONES INALÁMBRICAS A LA RED	18
4.1 Extensión de las redes inalámbricas Wi-Fi	18
4.2 Hábitos de uso de las redes inalámbricas Wi-Fi.....	19
4.3 Medidas de seguridad utilizadas en las redes inalámbricas Wi-Fi.....	20
5 CONCLUSIONES Y RECOMENDACIONES	22
5.1 Conclusiones del análisis.....	22
5.2 Recomendaciones	23
ÍNDICE DE GRÁFICOS.....	25

PUNTOS CLAVE

El Observatorio de la Seguridad de la Información publica el *Estudio sobre la seguridad de las comunicaciones móviles e inalámbricas en los hogares españoles (Informe anual 2009)*. Para elaborar el análisis se han realizado encuestas periódicas a usuarios de Internet y telefonía móvil.

El informe permite realizar, con una perspectiva evolutiva, un diagnóstico de los hábitos de uso de las comunicaciones móviles e inalámbricas, las medidas de seguridad utilizadas y, en el caso de la telefonía móvil, las incidencias de seguridad sufridas.

El período analizado en este documento abarca todo el año 2009. Durante este tiempo se han realizado 14.264 encuestas en 4 tomas de datos. Se ofrece, por tanto, un análisis evolutivo a lo largo de los 4 trimestres de 2009.

Se exponen a continuación los puntos clave del estudio.

I Seguridad de las comunicaciones móviles e inalámbricas de los hogares

Telefonía móvil

El 97,6% de los encuestados disponen de un teléfono móvil en el 4º trimestre de 2009. La incorporación del bluetooth en el teléfono móvil es masiva (90,2%), con tendencia creciente a lo largo del año. También frecuente es la disponibilidad de conexión a Internet a través del teléfono móvil (73,1%).

Respecto a las medidas de seguridad adoptadas por los usuarios de móviles, la utilización de PIN o código de seguridad de 4 dígitos es la más extendida a lo largo de todo 2009 (89,7% en el último trimestre del año). Por detrás de esta práctica, la realización de copias de seguridad de los datos del teléfono móvil es practicada por un nada desdeñable 30,2% de usuarios a finales de año. El 17% de usuarios bloquea con contraseña el terminal tras un periodo de inactividad, medida que ha evolucionado lentamente. Y por último, sólo el 2,4% instala un programa antivirus en su terminal (dato que se mantiene estable durante todo 2009).

El 65,6% de los encuestados afirma, en el 4º trimestre de 2009, no haber sufrido ninguna incidencia de seguridad en su teléfono móvil en los últimos tres meses. El robo del terminal (17,3%) y el extravío (19,2%) se mantienen como los problemas de seguridad con más impacto sobre el usuario de telefonía móvil, aunque presentan una tendencia ligeramente a la baja. También en el último trimestre, sólo el 3,8% afirma haber alojado código malicioso en el móvil.

Conexiones inalámbricas

El uso de las redes inalámbricas Wi-Fi sigue en crecimiento, y aumenta el número de usuarios que las utiliza como punto de conexión principal. Así, la mayoría de usuarios (un 62,8%) se conecta a Internet a través de su propia conexión Wi-Fi, con una tendencia ascendente a lo largo de 2009.

Los usuarios que acceden a través de alguna red pública también aumentan ligeramente en el 4º trimestre de 2009 (12,5%, frente a 10,9% en el primer trimestre). En paralelo, en el último trimestre del año, se alcanza el mínimo de usuarios que no se conectan a un punto de red inalámbrico (31,4%).

El 53% de los encuestados reconoce que se conectan a redes Wi-Fi abiertas siempre que lo necesitan, en cualquier circunstancia. Más cautos se muestra el 34,4% que declara acceder a redes Wi-Fi ajenas sólo para realizar ciertas operaciones y el 12,6% que se conectan sólo en el caso de que dicha red esté protegida mediante contraseña pública.

A lo largo de 2009 el protocolo WEP (con un 30,5% de uso en el 4º trimestre) es el sistema de protección más utilizado. El protocolo WPA es adoptado por un 24,5% de los encuestados, presentando un lento crecimiento desde los primeros meses del año. Un 28% de usuarios protege su red pero desconoce el sistema. Un 9,6% desconoce si su red está protegida y un 7,4% que afirma no protegerla.

.

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Presentación

1.1.1 Instituto Nacional de Tecnologías de la Comunicación.

El Instituto Nacional de Tecnologías de la Comunicación, S.A. (INTECO), es una sociedad estatal adscrita al Ministerio de Industria, Turismo y Comercio 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 Centro Demostrador de Tecnologías de Seguridad, y la Oficina de Seguridad del Internauta, 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. Asimismo desarrolla proyectos en el ámbito de la accesibilidad orientados a garantizar el derecho de ciudadanos y empresas a relacionarse electrónicamente con las AA.PP.

- **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.
- **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.

1.1.2 Observatorio de la Seguridad de la Información

El Observatorio de la Seguridad de la Información se inserta dentro de la línea estratégica de actuación de INTECO en materia de Seguridad Tecnológica. Nace con el objetivo de describir de manera detallada y sistemática el nivel de seguridad 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 y la e-confianza.

El Observatorio ha diseñado un Plan de Actividades y Estudios con el objeto de producir conocimiento especializado y útil en materia de seguridad por parte de INTECO, 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 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 la seguridad de las comunicaciones móviles e inalámbricas en los hogares españoles

El *Estudio sobre la seguridad de las comunicaciones móviles e inalámbricas en los hogares españoles* persigue como objetivo general realizar un diagnóstico de la situación actual respecto a la utilización que los usuarios españoles realizan de las tecnologías móviles e inalámbricas, así como las medidas de seguridad utilizadas y las incidencias sufridas.

Este informe sigue la línea iniciada con otras publicaciones del Observatorio de la Seguridad de la Información, [Estudio sobre seguridad y privacidad en el uso de los servicios móviles por los menores españoles](#) y [Estudio sobre la situación de seguridad y buenas prácticas en dispositivos móviles y redes inalámbricas](#). En esta ocasión no se trata de un análisis tan exhaustivo como los estudios anteriores, si no de una actualización de los datos de usuarios basados en encuestas.

Este informe ofrece la evolución trimestral a lo largo de 2009 de los resultados sobre seguridad en las comunicaciones móviles e inalámbricas. Y a su vez constituye el primero de una serie de informes periódicos.

2 DISEÑO METODOLÓGICO

El *Estudio sobre la seguridad de las comunicaciones móviles e inalámbricas en los hogares españoles (Informe anual 2009)* 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.

El panel posibilita la realización de encuestas periódicas acerca de la seguridad de las comunicaciones móviles e inalámbricas en los hogares españoles y ofrecer, por tanto, una perspectiva evolutiva de la situación. Se realizan encuestas online a usuarios españoles de Internet mayores de 15 años con acceso frecuente desde el hogar, llevadas a cabo con una periodicidad trimestral. Los datos extraídos de las encuestas permiten obtener la percepción sobre la situación de las comunicaciones móviles e inalámbricas en los hogares españoles.

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 hábitat¹.

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

Tabla 1: Tamaños muestrales para las encuestas

Período	Tamaño muestral
1 ^{er} trimestre 2009	3.563
2 ^o trimestre 2009	3.521
3 ^{er} trimestre 2009	3.540
4 ^o trimestre 2009	3.640

Fuente: INTECO

¹ Estas cuotas se han obtenido de datos representativos a nivel nacional de usuarios de Internet mayores de 15 años que se conectan más de una vez al mes desde el hogar facilitados por Red.es, entidad pública empresarial del Ministerio de Industria, Turismo y Comercio. ("Las TIC en los hogares españoles: 25^a oleada julio-septiembre 2009")

2.3 Trabajo de campo y error muestral

El trabajo de campo ha sido realizado entre enero y diciembre de 2009 mediante entrevistas online.

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 a $\pm 1,7\%$ en cada uno de los períodos analizados, tal y como se recoge en la siguiente tabla.

Tabla 2: Errores muestrales de las encuestas (%)

Período	Tamaño muestral	Error muestral
1 ^{er} trimestre 2009	3.563	$\pm 1,68\%$
2 ^o trimestre 2009	3.521	$\pm 1,68\%$
3 ^{er} trimestre 2009	3.540	$\pm 1,68\%$
4 ^o trimestre 2009	3.640	$\pm 1,66\%$

Fuente: INTECO

3 SEGURIDAD DE LAS COMUNICACIONES DE TELEFONÍA MÓVIL

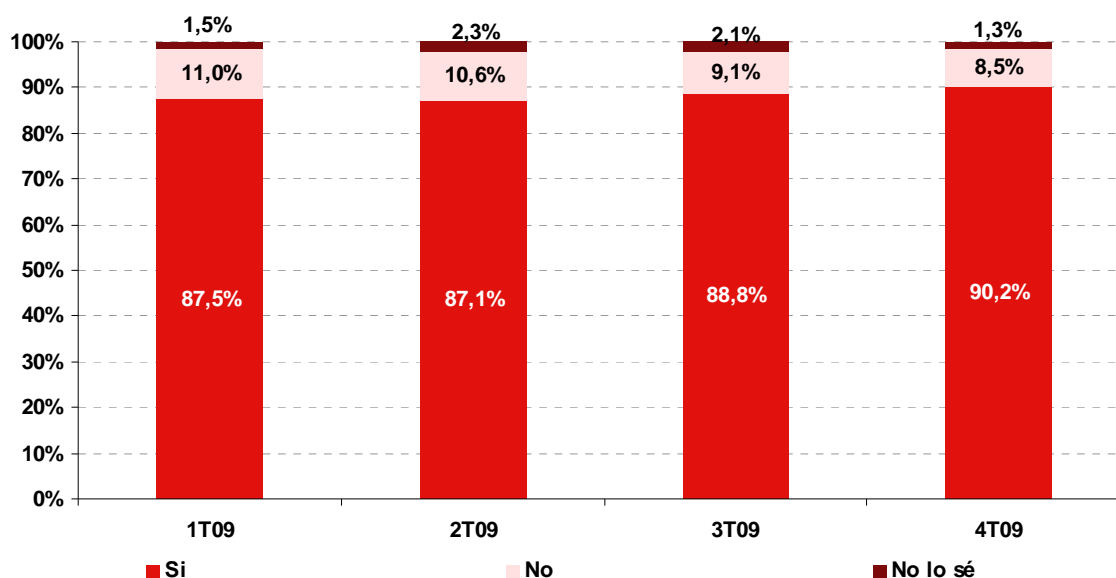
Los móviles no están exentos de sufrir problemas de seguridad. Son cada vez más potentes y con mayores capacidades. Llegando a veces a disponer de los mismos datos que un ordenador personal debido a la gran capacidad de almacenamiento que hoy en día disponen estos dispositivos. Además, su presencia entre la población es prácticamente totalitaria. Es por estos motivos por los que llegará un momento en el que los atacantes encuentren en ellos un objetivo rentable.

3.1 Extensión del teléfono móvil y prestaciones que incorpora

En el 4º trimestre de 2009 el 97,6% de los encuestados disponen de un teléfono móvil. Sólo un 2,4% se resiste a tener un dispositivo de este tipo, aunque la cifra de usuarios sin móvil desciende ligeramente desde comienzos de 2009.

Se trata, de teléfonos que incorporan bluetooth en un 90,2%, tal y como muestra el Gráfico 1. Además experimenta una tendencia creciente a lo largo del año.

Gráfico 1: Evolución de la disponibilidad de teléfono móvil con bluetooth (%)

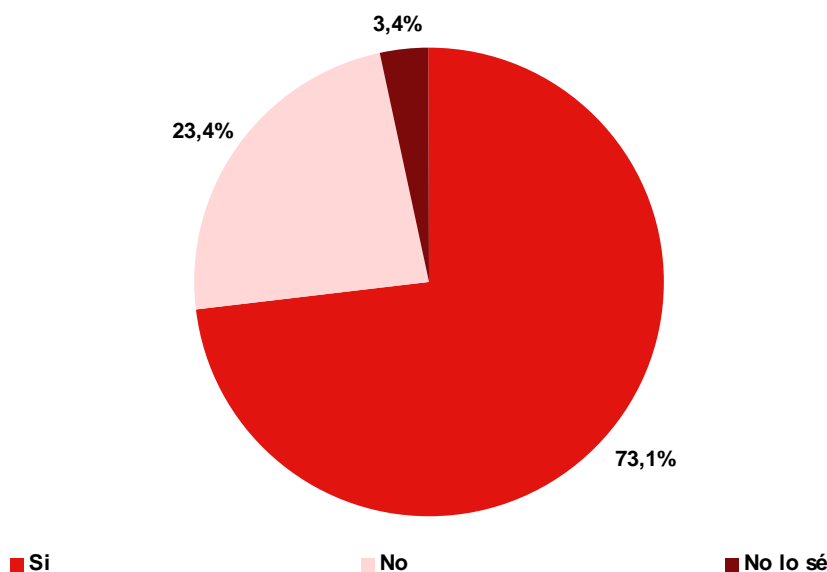


Base: Usuarios con teléfono móvil (n= 3.563 en 4T09)

Fuente: INTECO

También frecuente, aunque no al nivel del bluetooth, es la disponibilidad de conexión a Internet a través del teléfono móvil. El 73,1% de los participantes en el estudio con teléfono móvil, en el 4º trimestre de 2009, afirman que su dispositivo incorpora esta prestación.

Gráfico 2: Disponibilidad de teléfono móvil con conexión a Internet (4T 2009) (%)

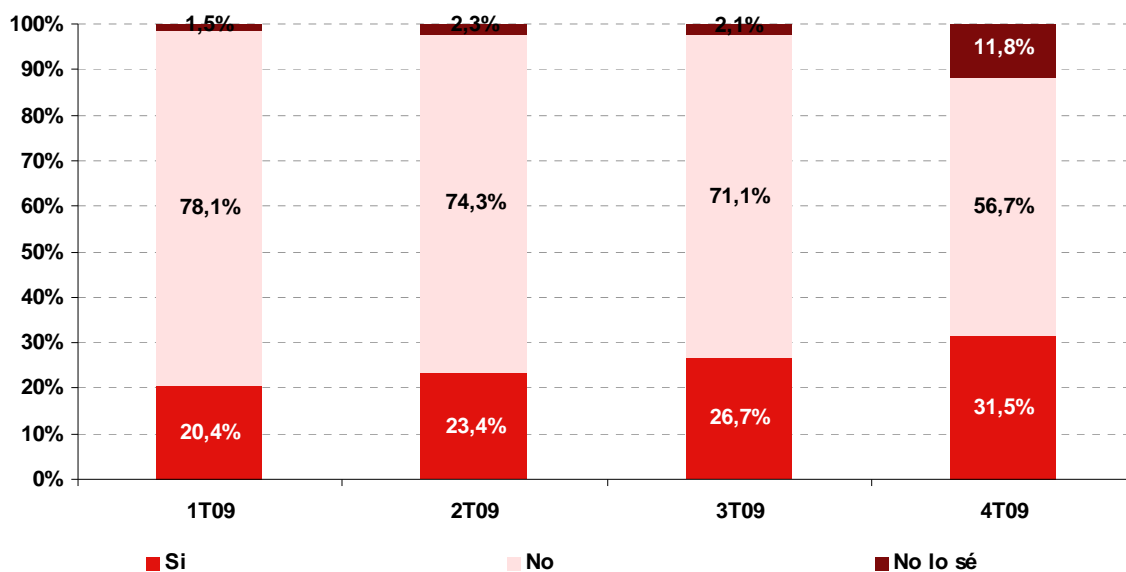


Base: Usuarios con teléfono móvil (n=3.563)

Fuente: INTECO

Algo menor es la incorporación de Wi-Fi en el teléfono móvil. En el 4º trimestre de 2009, un 31,5% de los usuarios españoles afirman que su teléfono dispone de Wi-Fi. La tendencia ha sido creciente durante el año, tal y como se aprecia en el Gráfico 3. El no disponer de tecnología Wi-Fi en el teléfono ha descendido desde el 1º trimestre de 2009 en un 21,4%.

Gráfico 3: Evolución de la disponibilidad de teléfono móvil con Wi-Fi (%)



Base: Usuarios con teléfono móvil (n= 3.563 en 4T09)

Fuente: INTECO

3.2 Hábitos de uso del teléfono móvil

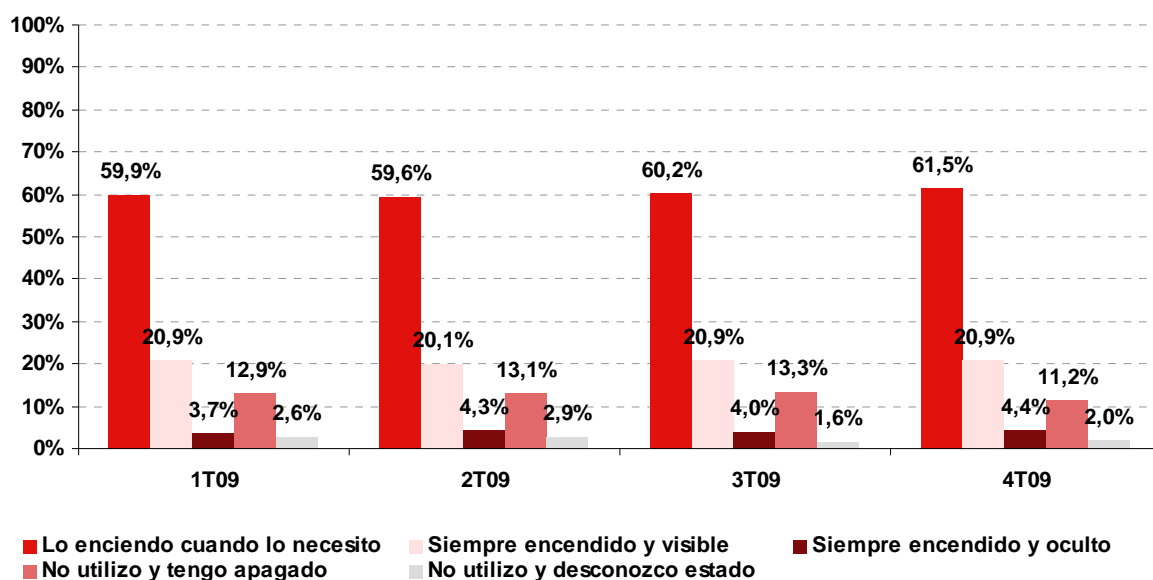
Como se ha visto anteriormente la tecnología inalámbrica bluetooth está incluida en numerosos teléfonos móviles, el 61,4% de los propietarios de móviles con esta tecnología adoptan el hábito seguro de encenderlo únicamente cuando lo van a utilizar (transfiriendo archivos o conectándolo al coche). Este porcentaje ha ido en leve aumento a lo largo de 2009.

Se debe señalar que cada vez que el usuario transmite información en línea mediante bluetooth se pone en situación de riesgo de sufrir ataques. Además del hábito seguro que esto implica, constituye un ahorro de batería en el terminal, pues la señal bluetooth consume recursos que acortan su duración.

Si un atacante detecta la señal de bluetooth activo, puede intentar conectarse con el dispositivo y robar su número de identificación personal (NIP). El usuario puede no notar la intromisión mientras el atacante, que ha averiguado el NIP, puede:

- Robar la información almacenada en el dispositivo.
- Enviar mensajes de texto o imágenes no solicitados.
- Acceder a los comandos del teléfono móvil.

Gráfico 4: Hábitos de uso del bluetooth del teléfono móvil (%)



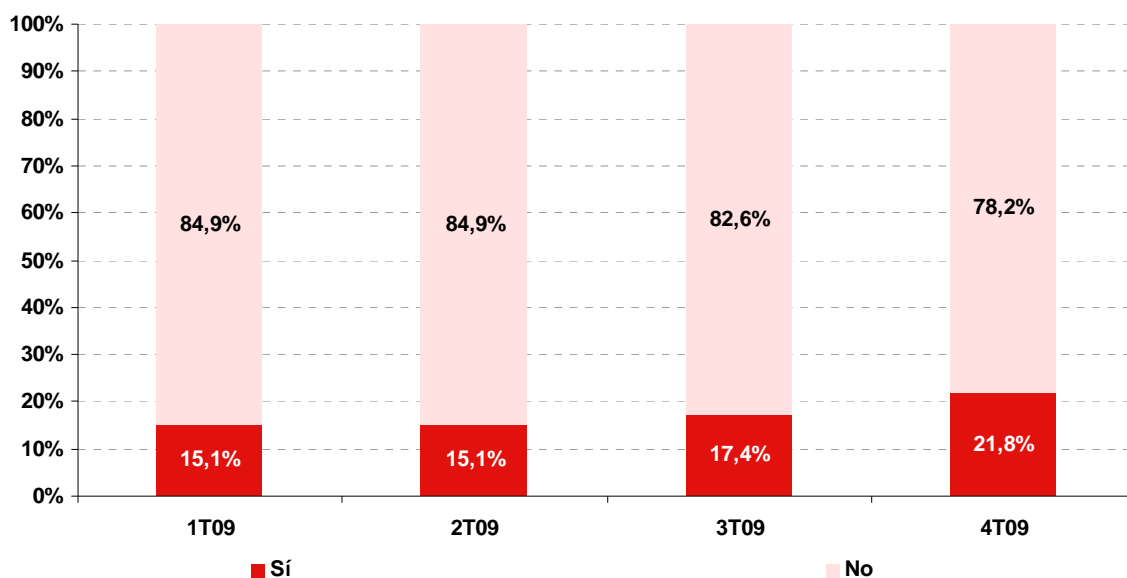
Base: Usuarios con bluetooth (n= 3.192 en 4T09)

Fuente: INTECO

El abaratamiento del acceso a redes de datos a través del móvil (tecnología 3G, que en la actualidad es ofrecida por la mayoría de operadoras con tarifa plana) contribuye al uso del móvil como gestor de correo. El Gráfico 5 es claro en este sentido: aunque en el 4º

trimestre de 2009 todavía son minoritarios (21,8%) los que utilizan el teléfono móvil para acceder al correo electrónico, la cifra va en aumento de forma progresiva desde comienzos de 2009.

Gráfico 5: Evolución de la utilización del teléfono móvil para acceder al correo electrónico (%)



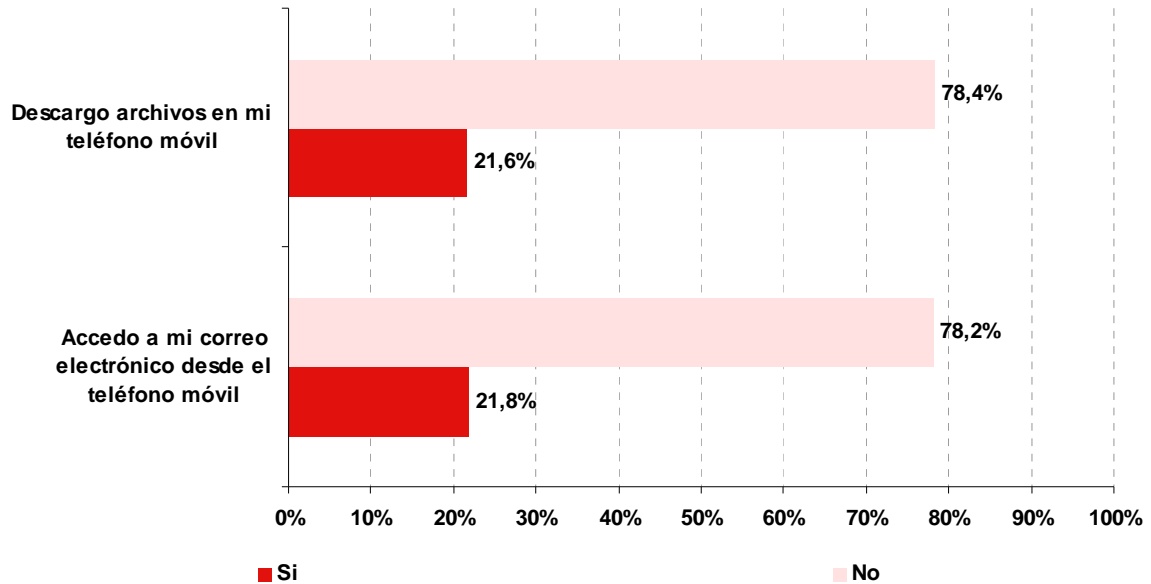
Base: Usuarios con teléfono móvil (n= 3.563 en 4T09)

Fuente: INTECO

También minoritaria es la descarga de archivos en el teléfono móvil: 21,6% de los usuarios en el 4º trimestre de 2009 (en este caso, no se disponen de datos anteriores por lo que habrá que esperar a futuras lecturas para identificar el signo de la tendencia, aunque es de esperar que su evolución sea paralela al acceso al correo electrónico a través del móvil; por ese motivo, el Gráfico 6 presenta ambos datos de manera conjunta).

Esta reducida tasa de adopción puede responder al hecho de que, en la actualidad, la mayoría de los terminales no soportan todos los formatos que se envían a través del correo electrónico, por tanto no pueden interpretar su contenido. También influye en la escasa adopción la existencia de terminales de pequeñas dimensiones, ya que esta característica limita la descarga de archivos en el teléfono o el acceso al correo electrónico.

Gráfico 6: Utilización del teléfono móvil para acceder al correo electrónico y la descarga de archivos 4T 2009 (%)



Base: Usuarios con teléfono móvil (n= 3.563)

Fuente: INTECO

3.3 Medidas de seguridad utilizadas en el teléfono móvil

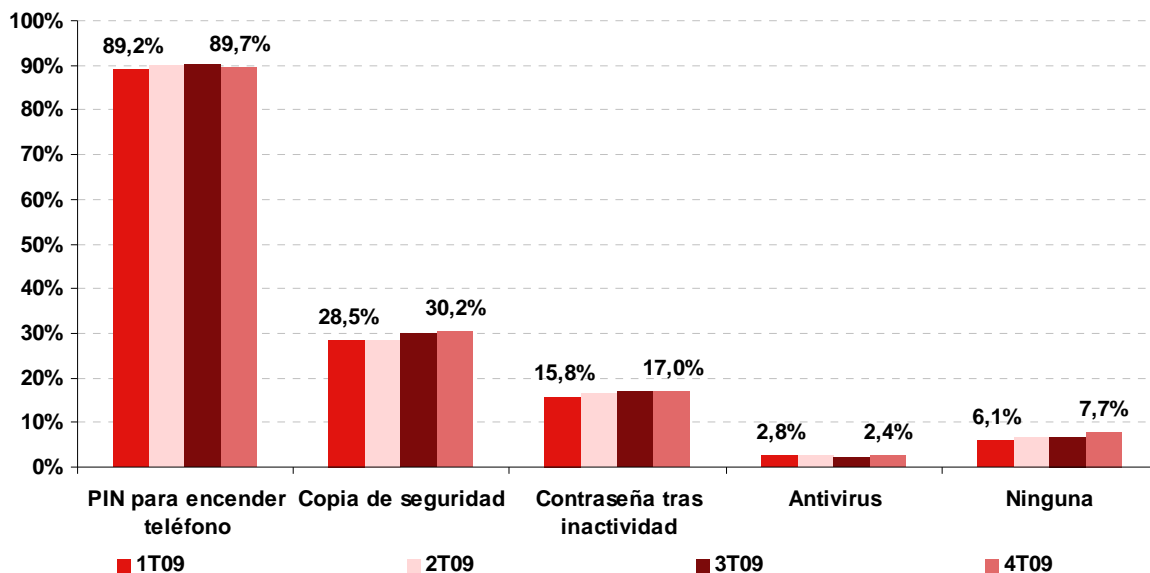
Se han evaluado en el Gráfico 7 las medidas de seguridad adoptadas por los usuarios de móviles. La utilización de PIN o código de seguridad de 4 dígitos sigue siendo la más extendida a lo largo de todo el 2009, alcanzando un 89,7% en el 4º trimestre, con una diferencia más que notable con respecto al resto de medidas adoptadas.

La realización de copias de seguridad de los datos del teléfono móvil es practicada por un nada desdeñable 30,2% en el último trimestre del año. Puede contribuir a ello el hecho de que los terminales suelen venir acompañados con software apropiado para realizar copias de seguridad de los contactos, archivos, imágenes, etc.

El 17% de usuarios (subiendo desde un 15,8% a principios de 2009) bloquea con contraseña el terminal tras un periodo de inactividad. Se trata de un parámetro que no suele estar establecido por defecto en la mayoría de terminales.

Por último, un porcentaje muy poco elevado (2,4% en el último trimestre) instala un programa antivirus en su terminal.

Gráfico 7: Medidas de seguridad utilizadas / instaladas en el teléfono móvil (%)



Base: Usuarios con teléfono móvil (n= 3.563 en 4T09)

Fuente: INTECO

3.4 Incidencias de seguridad

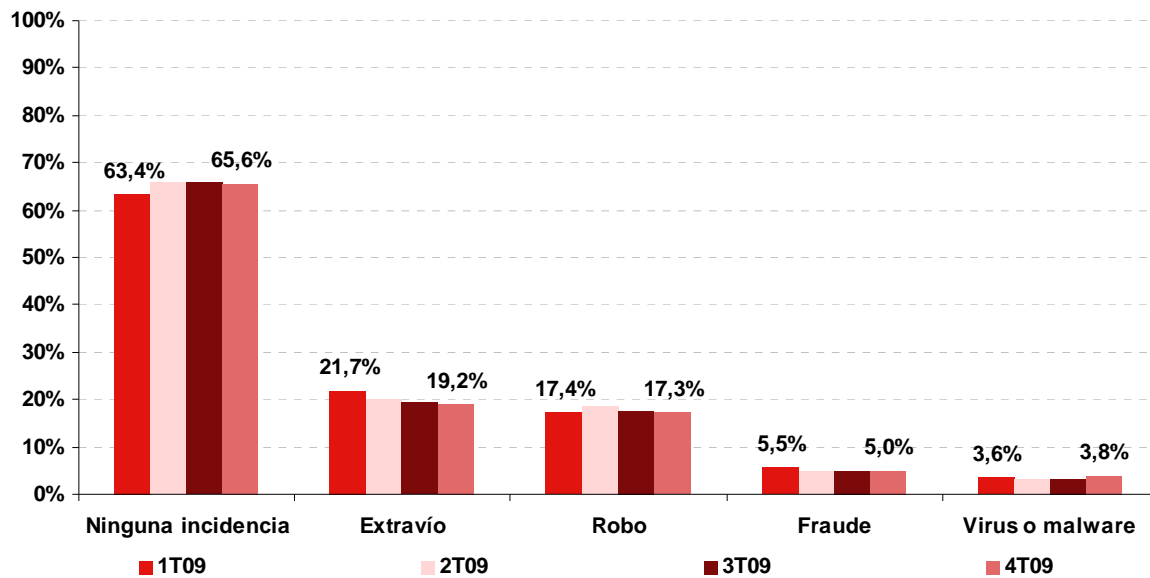
A finales de 2009 el 65,6% de los encuestados afirma no haber sufrido ninguna incidencia de seguridad con su teléfono móvil en los últimos tres meses.

El robo del terminal (17,3%) y el extravío (19,2%) se mantienen como los problemas de seguridad con más impacto sobre el usuario de telefonía móvil, aunque presentan una tendencia ligeramente a la baja.

Sólo el 3,8% afirma haber alojado código malicioso en el móvil (lo que explicaría el también reducido nivel de instalación de antivirus, tal y como se analizaba en el gráfico anterior). Este porcentaje se ha mantenido constante a lo largo del año. Afortunadamente, el código malicioso a través del móvil, se mantiene todavía en lo anecdótico, excepto singularidades con mucha difusión como:

- Virus para móvil denominado *Comwarior*. Este virus se difunde por mensajería multimedia (MMS) y tras infectar a un terminal utiliza la agenda de contactos para auto reenviarse a todos los contactos.
- Aplicaciones maliciosas para el sistema operativo *Windows Mobile* con código malicioso oculto que realiza llamadas internacionales de forma automática y sin que el usuario sea consciente de ello.

Gráfico 8: Incidencias de seguridad ocurridas en el uso del teléfono móvil (%)



Base: Usuarios con teléfono móvil (n= 3.563 en 4T09)

Fuente: INTECO

4 SEGURIDAD DE LAS CONEXIONES INALÁMBRICAS A LA RED

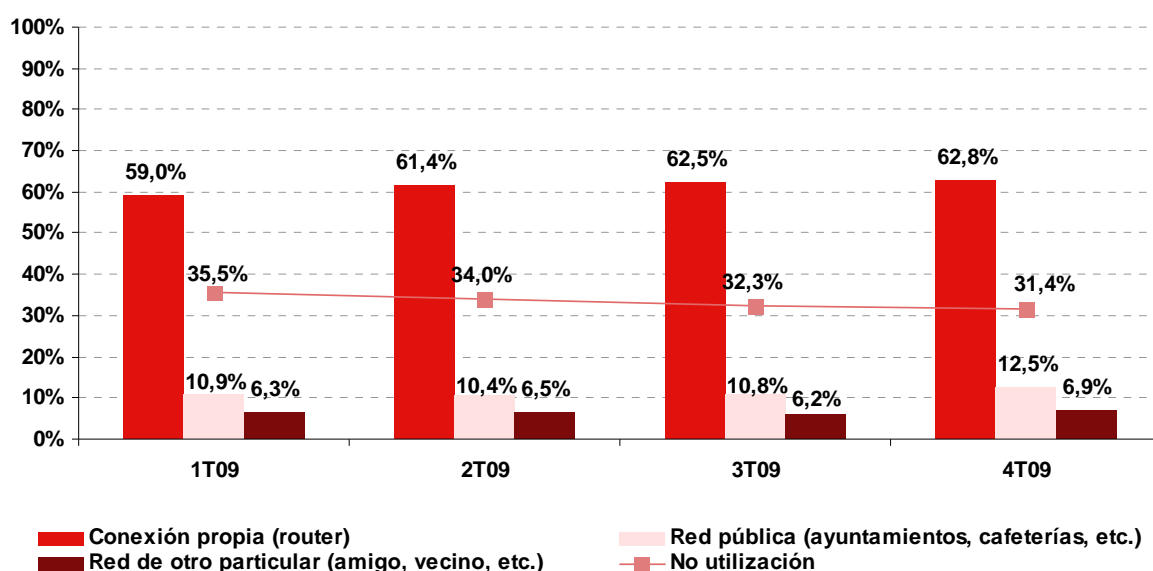
4.1 Extensión de las redes inalámbricas Wi-Fi

El uso de las redes inalámbricas Wi-Fi (cuyo nombre técnico es el estándar IEEE 802.11) sigue en crecimiento, a la vez que desciende el número de los usuarios que no utilizan este tipo de redes como punto de conexión principal (Gráfico 9).

Los proveedores de acceso a Internet hace tiempo que ofrecen la posibilidad de ofrecer un router Wi-Fi por cada servicio de acceso contratado a precio muy reducido, lo que explica que la inmensa mayoría (un 62,8% en el 4º trimestre de 2009) utilizan la Red a través de su propia conexión Wi-Fi, continuando su tendencia ascendente a lo largo de 2009. En paralelo, en el 4º trimestre se alcanza el mínimo anual de usuarios que no se conectan a un punto de red inalámbrico (31,4%).

Los usuarios que acceden a través de alguna red pública también aumentan ligeramente a finales de año (12,5%, frente a 10,9% en el 1º trimestre). La proliferación de la disponibilidad de redes en lugares de utilización comunitaria (instituciones públicas, centros de estudio, bibliotecas, aeropuertos, estaciones de tren, etc.) puede explicar el crecimiento.

Gráfico 9: Evolución del nivel de utilización de redes inalámbricas Wi-Fi (%)



Base: Total usuarios (n=3.640 en 4T09)

Fuente: INTECO

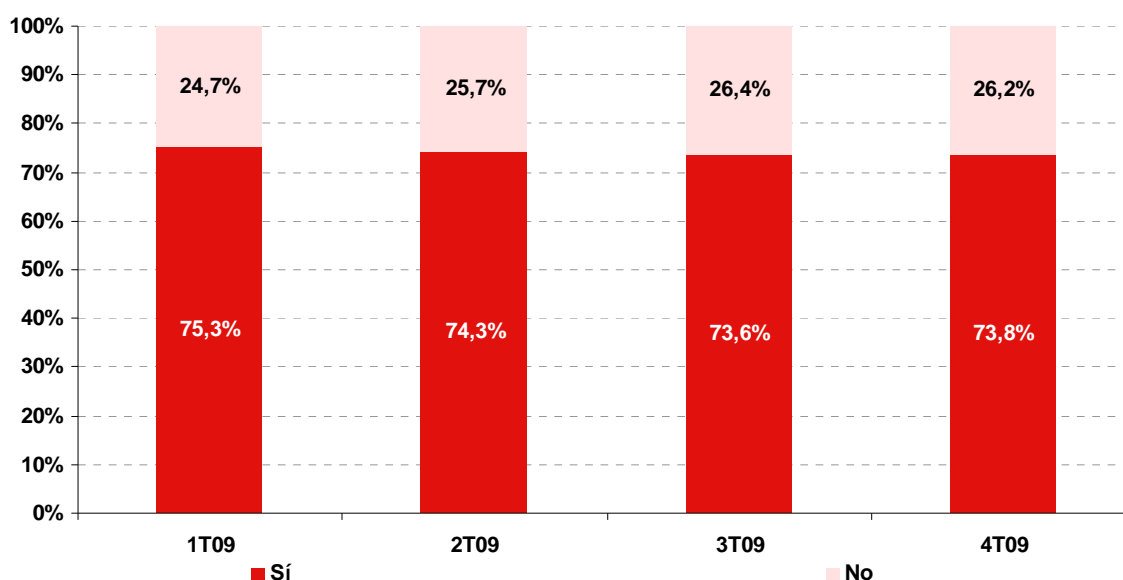
4.2 Hábitos de uso de las redes inalámbricas Wi-Fi

Se analizan a continuación una serie de hábitos de uso de las redes inalámbricas Wi-Fi, que pueden influir en cierto modo en el nivel de seguridad asumida por el usuario.

El 73,8% de los usuarios Wi-Fi con conexión propia tiene el hábito de dejar el punto de acceso encendido en todo momento (aunque no se esté utilizando). Desde una perspectiva evolutiva, se aprecia una ligera tendencia al retroceso de esta práctica, tal y como muestra el Gráfico 10.

Esta no puede considerarse una conducta de riesgo si la red está cifrada y posee una clave robusta.

Gráfico 10: Evolución de los hábitos de uso de las redes inalámbricas Wi-Fi: dejar el router encendido aunque no se esté utilizando (%)



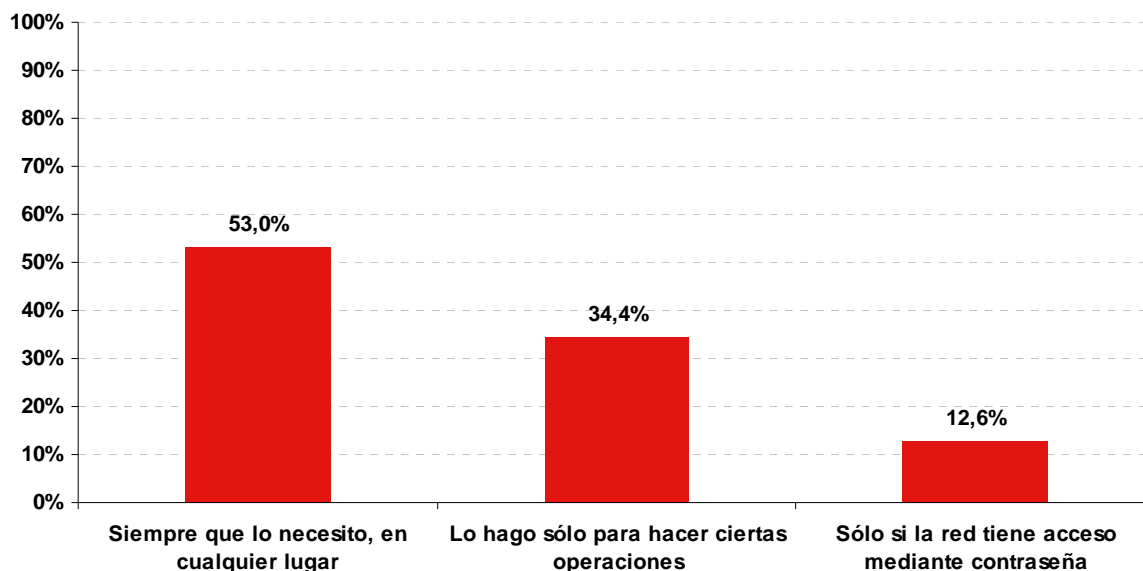
Base: Usuarios Wi-Fi con conexión propia (n= 2.312 en 4T09)

Fuente: INTECO

Acceder a redes inalámbricas ajenas (bien sean de carácter público, bien pertenezcan a otro particular) es un hábito que podría suponer un riesgo si el equipo no está correctamente asegurado. Por ello, se ha preguntado a los usuarios que reconocen conectarse a otras redes en qué condiciones lo hacen (Gráfico 11).

Los datos obtenidos para el 4º trimestre de 2009 muestran que el 53% de los encuestados se conecta a redes Wi-Fi de carácter público y/o de otro particular siempre que lo necesita, en cualquier circunstancia. Más cautos se muestra el 34,4% que declara acceder a redes Wi-Fi ajenas sólo para realizar ciertas operaciones y el 12,6% que se conectan sólo en el caso de que la red esté protegida mediante contraseña.

Gráfico 11: Hábitos de uso de las redes inalámbricas Wi-Fi: conexión en lugares públicos (%)



Base: Usuarios Wi-Fi que se conectan a red pública y/o de otro particular (n=525)

Fuente: INTECO

4.3 Medidas de seguridad utilizadas en las redes inalámbricas Wi-Fi

Con el uso generalizado de redes inalámbricas, se ha conseguido una mayor movilidad y accesibilidad, tanto en lugares públicos como en los hogares de los internautas. Sin embargo, también se ha abierto la posibilidad de nuevos ataques. Los datos ya no quedan ocultos en un cable, sino que viajan en ondas de radio por el aire. Ya no es necesario que un atacante enchufe físicamente un cable en una toma de red de un edificio, sino que puede obtener la señal desde un lugar próximo a la red sin ser visto.

A veces, según la potencia de la red, incluso podría tener acceso a kilómetros de distancia. Una vez obtenido el acceso a una red inalámbrica, un atacante podría lanzar ataques o cometer fraude electrónico a terceros desde dicha conexión, inculcando al dueño legítimo de la red.

Normalmente, este tipo de intrusión se realiza con un simple portátil equipado con una tarjeta WNIC (*Wireless Network Interface Cards*) del tipo PCMCIA y un software que busque automáticamente puertas de enlace o nodos de acceso válidos.

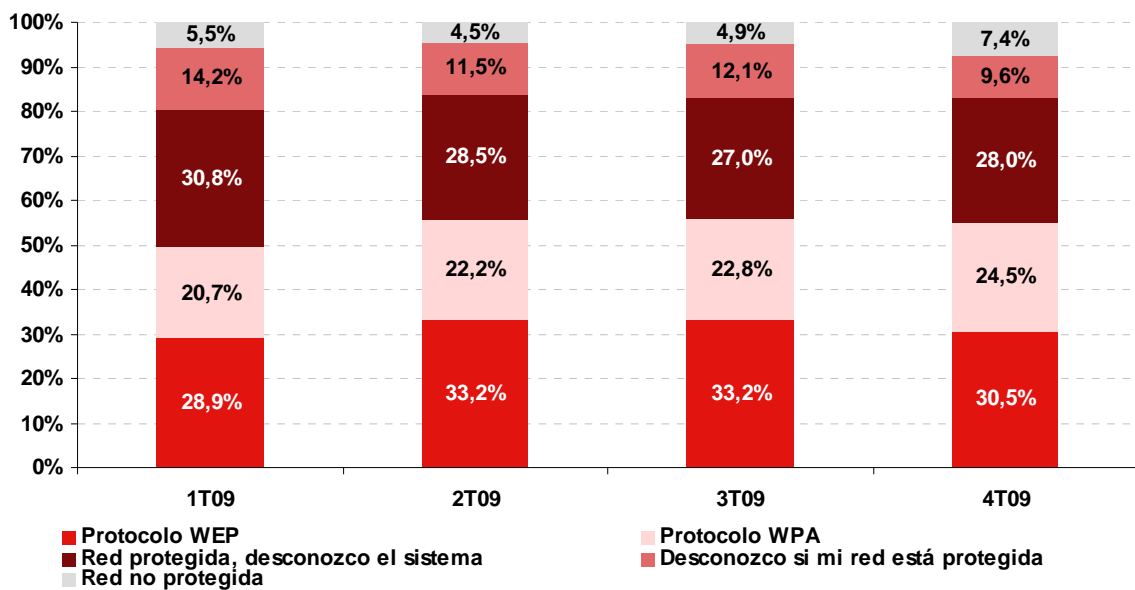
Hoy en día resulta tan fácil como ejecutar un programa y esperar mientras el atacante se mueve por una zona determinada. A esta técnica de búsqueda de nodos de acceso *wireless* se la conoce por varios nombres: *warchalking*, *wardriving* o *stumbling*. Los cibercriminales que practican el *wardriving* suelen publicar en diversas páginas web aquellos puntos de acceso que encuentran sin protección para que otros atacantes puedan aprovecharlos.

Como se aprecia en el Gráfico 12, a lo largo de 2009 el protocolo WEP (con un 30,5% de uso en el 4º trimestre) sigue siendo el sistema de protección más utilizado. Teniendo en cuenta que se trata de un protocolo de cifrado obsoleto, debería sustituirse por el protocolo WPA. El protocolo WPA es adoptado por un 24,5% de los encuestados, presentando un lento crecimiento desde los primeros meses del año.

Cabe destacar que el protocolo WPA emplea el cifrado de clave dinámica (a diferencia del WEP que lo emplea de manera estática), es decir, la clave está cambiando constantemente. De esta manera, las incursiones en la red inalámbrica son más difíciles que con un protocolo WEP.

Un 28% de usuarios protege su red pero desconoce el protocolo. Un 9,6% desconoce si su red está protegida y un 7,4% que afirma no protegerla.

Gráfico 12: Evolución de los sistemas de seguridad de las redes inalámbricas Wi-Fi (%)



Base: Usuarios Wi-Fi con conexión propia (n= 2.312 en 4T09)

Fuente: INTECO

5 CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones del análisis

Como se apuntaba al comienzo del informe, los dispositivos de telefonía móvil no están exentos de sufrir incidentes de seguridad (del mismo modo que sucede con los equipos informáticos). Con mayor razón hoy en día, ya que los terminales incorporan prestaciones muy similares a los ordenadores (navegación web, correo electrónico, almacenamiento de archivos, etc.), pueden utilizar servicios online (consultas y pagos electrónicos, redes sociales, geolocalización, etc.) y que estando extendidos entre casi la totalidad de la población suponen un objetivo potencialmente atractivo para los ciberdelincuentes.

El análisis de las prestaciones que incorporan los terminales muestra que, en el caso del bluetooth, la inmensa mayoría de los terminales móviles domésticos (no corporativos) lo incorporan. También frecuente – aunque no tanto como el bluetooth – es que el dispositivo permita la conexión a Internet. En cambio, la posibilidad de conectarse a redes Wi-Fi a través del teléfono móvil, aunque con tendencia creciente a lo largo de 2009, es menor.

En otro orden de cosas, los hábitos seguros a la hora de utilizar el teléfono móvil han experimentado un ligero crecimiento a lo largo del año. Así, por ejemplo, la buena práctica de encender el bluetooth sólo cuando se va a realizar dicha conexión (no tener dicha función activa permanentemente) cada vez es más común entre los usuarios.

En cuanto a las medidas de seguridad adoptadas por los usuarios de móviles, el uso del código de seguridad PIN sigue siendo la más extendida, seguida de la realización de copias de seguridad de los datos del teléfono y la activación de contraseñas tras un periodo de inactividad.

La instalación de antivirus en el terminal móvil tiene una escasa penetración, sin variaciones a lo largo de todo 2009, aunque cabe esperar que este porcentaje vaya aumentando progresivamente. Cabe recordar que son más los usuarios que se conectan a Internet desde su terminal móvil, exponiéndose a riesgos de seguridad análogos a los que se expone cuando se navega por Internet mediante un ordenador. Uno de los motivos por los que el uso de programas antivirus en los terminales es tan poco elevado puede ser el hecho de que muchos usuarios desconocen desde su propia existencia hasta cómo instalarlo en el teléfono móvil.

Es positivo que del análisis de incidencias de seguridad sufridas en los teléfonos móviles resulte un porcentaje muy bajo de usuarios que declaran que su terminal ha sufrido un ataque mediante malware.

En el caso de las redes inalámbricas Wi-Fi su uso sigue en crecimiento. En paralelo, desciende el número de los usuarios que no utilizan este tipo de conexión como punto de conexión principal, frente a la tradicional conexión por par de cobre o cable coaxial.

El protocolo WEP, sigue siendo el sistema de protección del router Wi-Fi más utilizado, si bien el protocolo WPA presenta un lento repunte desde los primeros meses del año.

5.2 Recomendaciones

Es imposible garantizar que una persona no vaya a perder o le sea robado su **teléfono móvil**. Sin embargo, sí que puede al menos, proteger y/o conservar la información que guarda en el dispositivo, así como bloquear el acceso al mismo.

Es conveniente que el usuario conozca el número IMEI (*International Mobile Equipment Identity*) del teléfono, ya que gracias a este, en caso de pérdida o robo, la operadora de telefonía móvil podrá desactivar el teléfono, incluso en el caso de que se le inserte una tarjeta SIM diferente. Este código se puede visualizar en la pantalla del teléfono marcando *#06#.

Una segunda medida es la activación de la clave de acceso (en este caso, el número PIN) cada vez que se enciende el teléfono. De la misma manera, es conveniente activar el bloqueo automático del teléfono móvil para evitar que personas no autorizadas puedan acceder a los datos, siendo necesaria una contraseña de acceso para desbloquearlo. Para saber cómo aplicar estas medidas, y si el dispositivo lo permite, el usuario debe consultar la guía del fabricante.

Si el usuario almacena información sensible en la memoria del teléfono debe encriptarla para que, en el caso de que otra persona acceda indebidamente a ella, no le sea posible conocer el contenido.

Por otro lado, recordar que si se toma la precaución de desactivar la conexión bluetooth cuando no se esté usando esta, se evitará la posibilidad de que terceros accedan inalámbricamente al terminal y a la información que contiene.

Para evitar infecciones por código malicioso o malware en el dispositivo móvil, es conveniente evitar descargar aplicaciones o archivos desde Internet con origen poco confiable, así como asegurarse que si se realiza una conexión entre dispositivos (de móvil a móvil, o de móvil a ordenador) aquel no se encuentre comprometido debido a que aloje archivos infectados, ya que podrían ser transmitidos a nuestro terminal. En cualquier caso, instalar una herramienta antivirus en el terminal es una buena práctica.

De igual modo, otra de recomendación es 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.

Respecto a las **conexiones inalámbricas a la Red**, con el crecimiento de uso de las redes Wi-Fi se ha abierto la posibilidad de ataques mediante estas tecnologías. Por ello, una medida de prevención es aplicar un buen protocolo de cifrado como sistema de seguridad. En este sentido, el protocolo WPA es sin duda el más seguro ya que fue creado con el objetivo de encontrar un sustituto al protocolo WEP, más vulnerable ante ataques pasivos.

También se recomienda que a la hora de configurar en el router el SSID² (*Service Set Identifier*) o identificador de la red utilizada, se haga de forma que no se difunda su nombre. Así, sólo podrán conectarse a la red aquellos usuarios autorizados que conozcan el nombre de la misma.

Por último la contraseña elegida para proteger la red Wi-Fi debe ser robusta. Para ello algunos consejos son:

- Se deben utilizar al menos 8 caracteres para crear la clave.
- Se recomienda utilizar en una misma contraseña dígitos, letras y caracteres especiales.
- Es recomendable que las letras alternen aleatoriamente mayúsculas y minúsculas.
- Elegir una contraseña que pueda recordarse fácilmente y escribirse rápidamente, preferiblemente, sin que sea necesario mirar el teclado.
- Cambiarla con cierta regularidad.
- No utilizar datos relacionados con el usuario que sean fácilmente deducibles, o derivados de estos.

² Es el nombre de la red. Todos los paquetes de información que se envían o reciben llevan este nombre.

ÍNDICE DE GRÁFICOS

Gráfico 1: Evolución de la disponibilidad de teléfono móvil con bluetooth (%).....	11
Gráfico 2: Disponibilidad de teléfono móvil con conexión a Internet (4T 2009) (%)	12
Gráfico 3: Evolución de la disponibilidad de teléfono móvil con Wi-Fi (%)	12
Gráfico 4: Hábitos de uso del bluetooth del teléfono móvil (%)	13
Gráfico 5: Evolución de la utilización del teléfono móvil para acceder al correo electrónico (%)	14
Gráfico 6: Utilización del teléfono móvil para acceder al correo electrónico y la descarga de archivos 4T 2009 (%).....	15
Gráfico 7: Medidas de seguridad utilizadas / instaladas en el teléfono móvil (%)	16
Gráfico 8: Incidencias de seguridad ocurridas en el uso del teléfono móvil (%)	17
Gráfico 9: Evolución del nivel de utilización de redes inalámbricas Wi-Fi (%)	18
Gráfico 10: Evolución de los hábitos de uso de las redes inalámbricas Wi-Fi: dejar el router encendido aunque no se esté utilizando (%)	19
Gráfico 11: Hábitos de uso de las redes inalámbricas Wi-Fi: conexión en lugares públicos (%)	20
Gráfico 12: Evolución de los sistemas de seguridad de las redes inalámbricas Wi-Fi (%).....	21



Instituto Nacional
de Tecnologías
de la Comunicación

<http://www.inteco.es>

<http://observatorio.inteco.es>