

Guía para proteger y usar de forma segura su móvil





El Instituto Nacional de Tecnologías de la Comunicación (INTECO), sociedad estatal promovida por el Ministerio de Industria, Turismo y Comercio, es una plataforma para el desarrollo de la Sociedad del Conocimiento a través de proyectos del ámbito de la innovación y la tecnología.

Datos de contacto:

Instituto Nacional de Tecnologías de la Comunicación (INTECO)
Avda. José Aguado, 41. Edificio INTECO. 24005 León
Teléfono: +(34) 987 877 189 / Email: contacto@cert.inteco.es
www.inteco.es

Depósito Legal: LE - 366 - 2009

Imprime: gráficas CELARAYN, s.a.

Índice

1. Tipos de dispositivos móviles	5
2. Consejos para evitar que personas ajenas puedan acceder a su dispositivo	6
3. Consideraciones a tener en cuenta respecto a las llamadas y envío de mensajes	9
4. Cómo puede proteger la información y el terminal	10
5. Qué hacer en caso de robo	13
6. Medidas a adoptar en dispositivos que incorporan <i>bluetooth</i>	15
7. Consejos para proteger su dispositivo si tiene incorporado Wi-Fi	17
8. Cómo gestionar la instalación de nuevas aplicaciones	18



1 ■ Tipos de dispositivos móviles

Para poder hacer un uso seguro de los dispositivos móviles es necesario conocer las funcionalidades que nos ofrecen los terminales, ya que en función de ellas se deben adoptar unas medidas de seguridad u otras.

Dentro del abanico de dispositivos móviles que tenemos hoy día, los de más amplia difusión son:

□ DISPOSITIVOS BÁSICOS

Son teléfonos móviles que permiten realizar llamadas de voz, enviar mensajes SMS, MMS y en algunos modelos transmitir datos mediante *bluetooth*.

□ DISPOSITIVOS MÓVILES AVANZADOS

Principalmente *SmartPhones* y PDA (Asistente digital personal)

Son ordenadores de mano con unas funcionalidades muy específicas orientadas a las labores de agenda personal, gestión de contactos y gestión básica de documentos. También incluyen capacidad para descargar/enviar correo electrónico, navegación por Internet mediante conexión GRPS, Wi-Fi, etc. Tienen un sistema operativo propio, que permite instalar nuevas aplicaciones o actualizar el sistema. Estos sistemas operativos son, entre otros: *Linux*, *Symbian*, *Palm OS*, *Windows Mobile* y *BlackBerry*. Hoy día son comunes, y cada vez más, las PDA que incorporan comunicación telefónica, de hecho a lo largo de la guía se utiliza el concepto de PDA con capacidad de comunicación móvil.



2. Consejos para evitar que personas ajenas puedan acceder a su dispositivo

- ❑ **NUNCA PIERDA DE VISTA EL DISPOSITIVO, YA QUE ÉSTE RESULTA ATRACTIVO PARA SU SUSTRACCIÓN O ROBO**
- ❑ **ACTIVE EL CÓDIGO PIN Y GUARDE EN LUGAR SEGURO EL PUK**

Los dispositivos móviles están provistos de varios códigos de seguridad para protegerlos contra el uso no autorizado. Estos códigos son conocidos como PIN y PUK.

¿Qué es el código PIN?



PIN o número de Identificación Personal es un código personal de 4 cifras que permite acceder o bloquear el uso de la tarjeta SIM, que es la que permite realizar llamadas con el dispositivo móvil. El PIN original se puede consultar en la documentación que entrega el operador con la tarjeta SIM y puede ser modificado por el usuario de manera sencilla.

Es recomendable que active y modifique el código PIN de su teléfono con una clave de su elección. Así, además de evitar que personas ajenas puedan realizar llamadas a su cargo o acceder a sus contactos evitará olvidar el código de acceso.

¿Qué es el código PUK



Es un código de 8 cifras que sirve para desbloquear la tarjeta SIM cuando ésta se ha bloqueado por introducir erróneamente en 3 ocasiones el código PIN. Este código también se puede consultar en la documentación original de la tarjeta SIM, pero a diferencia del PIN, el PUK no se puede modificar.

En caso de que por error bloquee su tarjeta SIM por haber marcado erróneamente -más de tres veces- el código PIN, deberá desbloquearla marcando el código PUK. Le recomendamos mantenerlo en un lugar seguro y que solamente Ud. conozca.

Para cualquier consulta respecto a la configuración del número PIN y PUK consulte el manual de usuario. En la mayor parte de los casos, su operador o proveedor de servicio es la mejor fuente de ayuda con los problemas relativos a los códigos PIN y PUK. Para ello basta con que se ponga en contacto con su operadora de telefonía móvil a través del número de atención al cliente.

EN DISPOSITIVOS AVANZADOS, ACTIVE LA OPCIÓN DE BLOQUEO DE TERMINAL CADA CIERTO TIEMPO (EJ. 10 MINUTOS), Y LA SOLICITUD DE UNA CONTRASEÑA PARA DESBLOQUEAR EL TERMINAL

Los dispositivos móviles inteligentes permiten poner un código al teléfono distinto del código PIN de la tarjeta SIM. Esto es así dado que pueden utilizarse sin la tarjeta SIM que les habilita a realizar llamadas telefónicas.

3. Consideraciones a tener en cuenta respecto a las llamadas y envío de mensajes

□ VIGILE EL CONSUMO E INFÓRMESE DE CUALQUIER ANOMALÍA EN SU FACTURA

Vigile el consumo y, en caso de notar incrementos bruscos en la factura, verifíquelo con la compañía. Puede estar siendo víctima de un fraude y tener su tarjeta clonada (cuando la tarjeta SIM ha sido copiada de manera no autorizada con el fin de hacer un uso fraudulento de la misma).

□ ESTÉ PREVENIDO ANTE FRAUDES MEDIANTE MECANISMOS DE “INGENIERÍA SOCIAL”, QUE INTENTAN EMBAUCARLE PARA LLAMAR Y/O ENVIAR MENSAJES A DETERMINADOS NÚMEROS

Este tipo de fraudes consisten en engañar a los usuarios para que utilicen el desvío de llamadas mediante la pulsación de una combinación de teclas (*#9...), envíen mensajes de texto o realicen llamadas a números de tarificación adicional (77xx, 80x, 90x). Están normalmente relacionados con trabajos (que no existen), premios (sin haber jugado) o paquetes recibidos (sin haberlos pedido).



4. Cómo puede proteger la información y el terminal

En general las siguientes recomendaciones sólo afectan a dispositivos avanzados, ya que son capaces de almacenar información de todo tipo en su memoria interna y/o externa.

□ NO LIBERE NI MANIPULE LOS COMPONENTES DEL TERMINAL EN LUGARES QUE NO LE OFREZCAN LAS GARANTÍAS SUFICIENTES

No libere el terminal si no es de la manera autorizada por su operadora de telefonía. Liberar el teléfono en un establecimiento no autorizado, puede tener un resultado no adecuado. Además de perder la garantía se puede averiar el terminal, sufrir un robo de datos, o perder la información almacenada.

□ MANTENGA UN SISTEMA PERIÓDICO DE COPIAS DE SEGURIDAD (BACKUP)

Se recomienda consultar el manual de usuario de dispositivo para saber cómo realizar una copia de seguridad de la información – en inglés, *backup*.

Para estar seguro, se recomienda encarecidamente seguir una política de copias de seguridad, en la que haga copias diarias, semanales, mensuales, semestrales y/o anuales, dependiendo de la importancia de la información que tiene almacenada en su dispositivo. Deberá, además, guardar estas copias en un lugar distinto al de los datos originales.



¿Qué pasaría si pierde toda su información y no la tiene respaldada?
Nunca deje de hacer copias de seguridad de su información.

❑ NO ABRA CORREOS ELECTRÓNICOS NI ACEPTE ARCHIVOS DE LOS CUÁLES DESCONOZCA EL REMITENTE

Una de las principales fuentes de acceso de virus o programas maliciosos son los correos electrónicos o la instalación de programas de origen desconocido. Por este motivo, se recomienda como buena práctica no abrir correos con remitente desconocido, y tampoco ejecutar los archivos adjuntos.



No confíe en correos de los que desconoce el remitente, porque al abrirlos puede quedar infectado por algún código malicioso que afecte a su dispositivo y su información.

❑ UTILICE PROGRAMAS DE CIFRADO PARA PROTEGER LA INFORMACIÓN DE LOS DISPOSITIVOS

Para evitar que la información que hay en el dispositivo pueda ser leída por una persona ajena, existen programas que permiten cifrar la información de forma que sólo pueda ser leída por el propietario mediante la introducción de un número secreto conocido por éste.

Algunos dispositivos ya traen instalados estos programas. Para el resto, sería necesario adquirirlos a través de algún proveedor de productos informáticos.



□ INSTALE SOFTWARE ORIGINAL PARA PODER SOLICITAR SOPORTE AL FABRICANTE

La mayor parte de los fabricantes de software y hardware facilitan servicios de atención al cliente de forma que puedan asesorar al usuario sobre aquellas dudas referentes a la configuración de su dispositivo. Para poder disfrutar de estos servicios, se debe disponer del software o hardware original.



Si no tiene el software o hardware original, no podrá solicitar soporte técnico ni asesoramiento al fabricante.

□ NO DEJE LAS TARJETAS DE MEMORIA DENTRO DEL DISPOSITIVO SI NO LO LLEVA ENCIMA, EN CASO DE ROBO O EXTRAVÍO LIMITARÁ EN GRAN MEDIDA LAS PÉRDIDAS

5. Qué hacer en caso de robo

□ HAGA UNA DENUNCIA Y LLAME AL OPERADOR PARA BLOQUEAR LA TARJETA SIM Y EL DISPOSITIVO

Si extravía o le roban su teléfono móvil y quiere evitar que éste pueda ser utilizado por otras personas, los operadores ofrecen el servicio de bloqueo del terminal y de la tarjeta SIM.

El bloqueo de la tarjeta SIM impide que otros usuarios realicen llamadas con cargo a la cuenta del usuario.

El bloqueo del terminal inutiliza éste de manera remota para que no pueda ser utilizado por ninguna persona.

Para realizar esta operación, debe realizar una denuncia y con ella ponerse en contacto con su operador y comunicarle la incidencia.



Si pierde o le roban su teléfono móvil, deberá denunciar este hecho.

Con la denuncia podrá ponerse en contacto con su operador y solicitar el bloqueo de su teléfono.

El operador, para proceder al bloqueo del terminal, le solicitará el código IMEI, que identifica de forma unívoca un dispositivo a nivel mundial. Los operadores suelen disponer de esta información, pero existen algunos casos en los que no disponen de él y lo pedirán al solicitante del bloqueo; si es así, deberá tenerlo disponible. Habitualmente está impreso en la parte posterior del equipo, bajo la batería y también en la caja del teléfono.

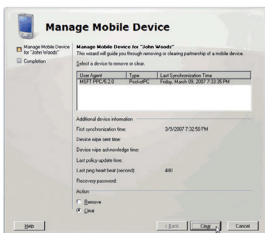
También puede conocer también su IMEI marcando en la pantalla del teléfono: *#06#. Guárdelo en un lugar seguro pero accesible, para cuando tenga que localizarlo.



Cuando solicite desbloquear su teléfono al operador, éste le solicitará el código IMEI. Este código está disponible en la documentación del teléfono o en el propio dispositivo bajo la batería. También puede obtenerlo marcando en su teléfono el código: ***#06#**. Siempre es recomendable que tenga su IMEI en un lugar seguro.

□ SOLICITE EL BORRADO REMOTO DE LA INFORMACIÓN SI DISPONE DE ESTE SERVICIO

Existen en el mercado empresas que ofrecen los servicios y/o productos para la gestión de todos los teléfonos móviles de una empresa. Si dispone de este servicio, consulte a su operador o al responsable de informática de su empresa, puede comunicarle la pérdida de su dispositivo y podrá proceder al borrado remoto de la información existente en él, de forma que nadie ajeno a Ud. pueda consultarla.



Si la información que tiene guardada en su dispositivo móvil es valiosa para Ud. y/o su empresa, le recomendamos contar con el servicio de borrado remoto de la información para evitar que personas no autorizadas puedan acceder a ella.

6. Medidas a adoptar en dispositivos que incorporan *bluetooth*

Seguir las siguientes recomendaciones puede evitarle serios daños en su dispositivo, como por ejemplo: pérdida de información, acceso a ella, etc.

❑ NO DEJE EL *BLUETOOTH* ENCENDIDO SI NO LO ESTÁ USANDO

El *bluetooth* es una tecnología bastante potente y útil para la transmisión de datos y voz (manos libres del coche), pero su nivel de seguridad no lo es tanto, y depende en cierta medida del uso adecuado que haga el usuario de ella.

Muchos dispositivos que utilizan *bluetooth* se pueden configurar para que sólo permanezcan encendidos durante un periodo determinado de tiempo, pasado el cual preguntan al usuario si quiere que permanezca encendido o si prefiere que se apague. Esta opción debería configurarse en todos los dispositivos cuando se vaya a usar *bluetooth*. En caso de duda, consulte la guía de usuario del fabricante.

En cambio, hay casos, como la conexión por *bluetooth* al manos libres del coche, en las que hay que dejar el *bluetooth* encendido mientras dure el trayecto y una vez que éste haya finalizado, se deberá apagar.

❑ SOLICITE AUTORIZACIÓN CADA VEZ QUE UN DISPOSITIVO INTENTE ESTABLECER UNA CONEXIÓN

Para que sea posible una conexión *bluetooth*, los integrantes de la comunicación deben asociarse primero. Esta asociación puede ser directa o mediante el requerimiento de una clave.

Es muy recomendable tener activada la opción de solicitar esta clave cada vez que desee conectarse a otros dispositivos.



❑ CONFIGURE LA CONEXIÓN *BLUETOOTH* PARA QUE NO PUBLIQUE SU IDENTIDAD AL ENTORNO (MODO INVISIBLE)

Los sistemas de *bluetooth* permiten ocultarse para que no sean detectados por otros dispositivos. Esto consiste en que, para realizar la comunicación con el otro dispositivo, se tiene que conocer e indicar previamente su identidad. Sin conocerla es prácticamente imposible que sea localizado. Esto nos permite utilizarlo de forma segura.

❑ NO ADMITA NI SE CONECTE A UN DISPOSITIVO *BLUETOOTH* DE ORIGEN DESCONOCIDO

Muchos de los virus para móviles se propagan por Bluetooth de manera automática, por lo que es posible que alguien infectado que Ud. no conozca le intente instalar un virus en su dispositivo, aunque sea de forma no intencionada. Por este motivo se recomienda aceptar únicamente conexiones de dispositivos que se sepa a priori de dónde provienen.

Aceptar estas conexiones no previstas a veces conlleva que se autorice a un tercer dispositivo la conexión al suyo.

❑ EVITE REALIZAR EMPAREJAMIENTOS EN LUGARES PÚBLICOS

Al realizar el proceso de emparejamiento de dispositivos con *bluetooth*, es cuando se realiza el envío de las claves de conexión. En este momento alguien con malas intenciones y con el equipo adecuado, podría interceptar estas claves y usarlas posteriormente para infectar su dispositivo. Para evitar estos riesgos, se recomienda no realizar estos emparejamientos en lugares públicos o muy concurridos, ya que estas personas aprovechan el anonimato para poder realizar estas actuaciones.

7. Consejos para proteger su dispositivo si tiene incorporado Wi-Fi

□ NO SE CONECTE A PUNTOS DE ACCESO NO CONOCIDOS

Hoy en día existen multitud de puntos de acceso Wi-Fi todavía sin securizar, por lo que se puede acceder a ellos fácilmente. El peligro aparece cuando el punto de acceso está abierto intencionadamente con un propósito malicioso. De esta manera un usuario pensará que está usando “Internet gratis”, pero lo que realmente sucede es que al conectarse a esa red se está permitiendo el acceso a toda la información del dispositivo a una persona no autorizada.



No crea que siempre que existen conexiones a Internet Wi-Fi gratis puede acceder “seguro” a ellas. Muchas veces es un engaño para que un desconocido pueda acceder a la información de su dispositivo.

□ TENGA UN ANTIVIRUS ACTUALIZADO: CON CORTAFUEGOS, ANTI-SPAM, ANTI-ESPÍAS, ETC.

Muchos usuarios piensan que no se deben proteger porque nadie querría atacarles. Esto podría ser cierto, pero el problema de hoy en día es que el código malicioso se transmite de forma automática (por ejemplo con las direcciones de los correos electrónicos de los dispositivos infectados), por lo que no discriminan si Ud. es una “víctima propicia” o no. Por esta razón debe tener instalado un programa antivirus y actualizarlo periódicamente. Además, también es muy recomendable que compruebe periódicamente las posibles actualizaciones del sistema operativo de su dispositivo.



SIEMPRE mantenga su antivirus actualizado.

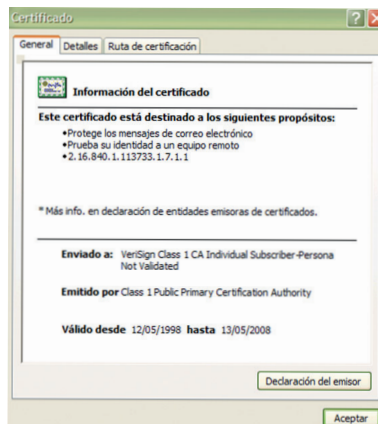
8. Cómo gestionar la instalación de nuevas aplicaciones

NO INSTALE APLICACIONES DE PROCEDENCIA DESCONOCIDA O NO FIABLE

Muchos de los virus o programas dañinos están ocultos bajo programas con nombres llamativos. Por este motivo se recomienda no instalar ningún programa cuya procedencia desconozcamos, pues existe un riesgo elevado de que realice acciones diferentes a las anunciadas.

CONFIGURE EL DISPOSITIVO PARA QUE NO SE PUEDAN INSTALAR PROGRAMAS QUE NO ESTÉN CERTIFICADOS Y/O DE FUENTE DESCONOCIDA

Algunos dispositivos, dentro de sus opciones de seguridad, permiten configurar la opción de no permitir instalar programas que no estén firmados por un remitente de confianza. Tener habilitada esta opción es una garantía para evitar la instalación de programas maliciosos en nuestro dispositivo.







Instituto Nacional
de Tecnologías
de la Comunicación

5
2
7
3
5
2
1