CCN-CERT

BP/03

Dispositivos móviles

INFORME DE BUENAS PRÁCTICAS

MAYO **2021**

ccn-cert centro criptológico nacional
CCN centro criptológico nacional

Edita:

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Índice

1. Sobre CCN-CERT

El **CCN-CERT** es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es **contribuir a la mejora de la ciberseguridad española**, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de **conseguir un ciberespacio más seguro y confiable**, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN.

2. Introducción

La proliferación de dispositivos móviles hace necesario plantearse cuál es la seguridad ofrecida respecto a la información que gestionan, tanto dentro de los entornos corporativos como en el ámbito particular.

En los últimos años, el desarrollo de los dispositivos y comunicaciones móviles junto con las tecnologías inalámbricas ha revolucionado la forma de trabajar y comunicarse. El uso creciente de estas tecnologías sitúa a los dispositivos móviles como uno de los objetivos principales para los atacantes.

La proliferación de dispositivos móviles, unido al desarrollo de capacidades, prestaciones y posibilidades de utilización de los mismos, hace necesario plantearse cuál es la seguridad ofrecida por este tipo de dispositivos respecto a la información que gestionan, tanto dentro de los entornos corporativos como en el ámbito particular.

Se considera como dispositivo móvil aquel dispositivo electrónico de uso personal o profesional de reducido tamaño que permite la gestión (almacenamiento, intercambio y procesamiento) de información y el acceso a redes de comunicaciones y servicios remotos, tanto de voz como de datos, y que habitualmente dispone de capacidades de telefonía, como por ejemplo teléfonos móviles, *smartphones* (teléfonos móviles avanzados o inteligentes), *tablets* (tabletas) y agendas electrónicas (*Personal Digital Assistant*) independientemente de si disponen de teclado físico o pantalla táctil.

2. Introducción

El nivel de percepción de la amenaza real existente no ha tenido la suficiente trascendencia en los usuarios finales y las organizaciones, pese a que los dispositivos móviles se utilizan para establecer comunicaciones personales y profesionales, privadas y relevantes, y para el almacenamiento e intercambio de información sensible. No solo las organizaciones suelen ser objeto de numerosos ataques, sino también la información no corporativa de los usuarios (datos personales).

Últimamente, se ha identificado un incremento notable no solo en el número de especímenes de código dañino para dispositivos móviles (mobile malware), sino que también en su complejidad y sofisticación, encontrándose España entre los países más afectados a nivel mundial en base al número de infecciones.

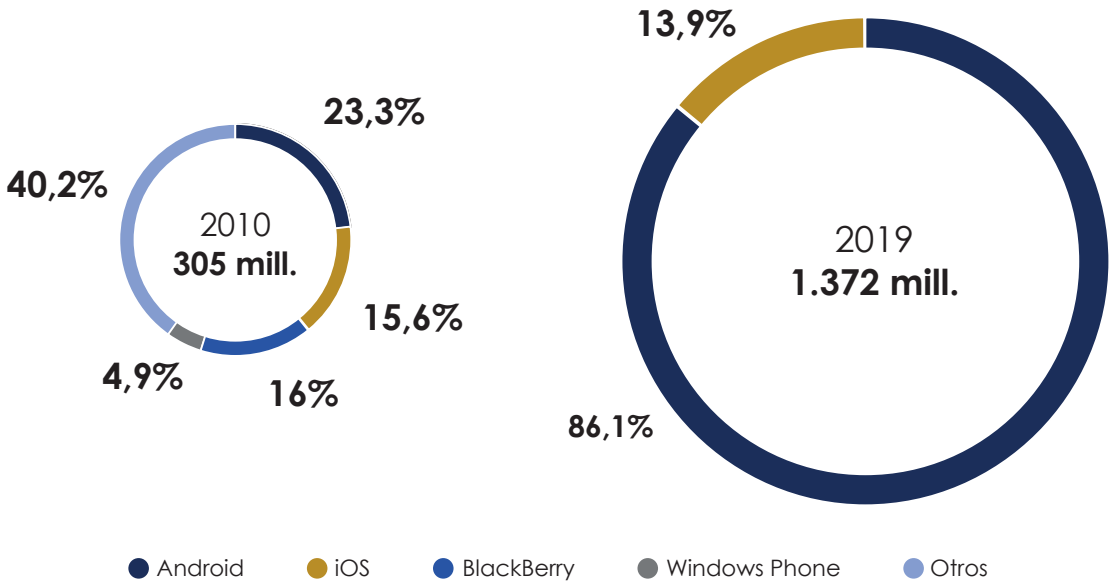


Figura 2-1 Cuota de mercado mundial de dispositivos móviles. Fuente: IDC[1]

La concienciación, el sentido común y las buenas prácticas en la configuración y el uso de los dispositivos móviles constituyen la mejor defensa para prevenir y detectar este tipo de incidentes y amenazas.

1. "Worldwide Smartphone OS Market Share". IDC. Informe. Q2 2015. http://www.idc.com/prodserv/smartphone-os-market-share.jsp

2. Introducción

Debido a que existe una adopción generalizada en la industria, tanto a nivel empresarial como personal, de dos de las plataformas móviles por encima del resto, Android (Google) e iOS (Apple), la mayoría de ejemplos empleados en la presente guía hacen referencia a estas dos plataformas móviles[2].

El presente documento tiene como objetivo describir estas prácticas con el fin de **ayudar a los usuarios** finales a **proteger y hacer un uso lo más seguro posible de los dispositivos móviles**, profundizando en la configuración y utilización de los mecanismos de protección existentes en la actualidad.

Para ello, se ofrecerán un **conjunto de pautas y recomendaciones de seguridad** para mitigar posibles acciones dañinas dándose a conocer las técnicas más habituales de ataque, así como los recursos utilizados por los atacantes para conseguir infectar un dispositivo móvil u obtener información personal de un usuario víctima.

2. Debe tenerse en cuenta que existen diferencias significativas en la configuración y utilización de los dispositivos móviles en función de la versión concreta de Android o iOS disponible.

3. Buenas prácticas en la configuración y uso de los dispositivos móviles

A continuación, se indica que el conjunto de recomendaciones mostrado se encuentra dividido en múltiples grupos, cada uno de ellos relacionado con las diferentes capacidades y funcionalidades ofrecidas por los dispositivos móviles, como por ejemplo: **mejorar la protección frente a un acceso físico no autorizado al propio dispositivo**, **reducir el impacto frente a la pérdida o robo del mismo**, o **mejorar la confidencialidad y seguridad** del **almacenamiento de la información** y de las **comunicaciones con otros equipos y servicios remotos**.

El objetivo de estas recomendaciones es que el usuario pueda aumentar el nivel de protección y de seguridad de sus dispositivos móviles, tanto desde el punto de vista de su configuración como de su uso diario, evitando así ser víctima de alguno de los ataques mencionados.

Debe tenerse en cuenta que algunas de las características descritas y, por tanto, de las recomendaciones de seguridad planteadas, son dependientes del tipo de sistema operativo empleado por el dispositivo móvil (Android, iOS, Windows Phone, etc.), de la versión de este y del fabricante y modelo concreto asociados al mismo.

Por tanto, no necesariamente todas las recomendaciones ofrecidas serán de aplicación en todos los dispositivos móviles existentes. En cualquier caso, se recomienda aplicar el mayor número de recomendaciones posible.

El objetivo de estas recomendaciones es que el usuario pueda aumentar el nivel de protección y de seguridad de sus dispositivos móviles, evitando así ser víctima de alguno de los ataques mencionados.

3.1 Pantalla de bloqueo

La pantalla de bloqueo es el principal mecanismo de defensa frente al acceso físico no autorizado al dispositivo móvil por parte de un potencial atacante.

Los dispositivos móviles modernos resultan muy atractivos para su sustracción o robo debido tanto a su valor económico (del propio hardware), como al valor asociado a la información sensible y personal que almacenan.

Por este motivo, la pantalla debe estar protegida por un código de acceso y permanecer bloqueada el mayor tiempo posible. Asimismo, se recomienda limitar la funcionalidad disponible en la pantalla de bloqueo para un tercero que no conoce el código de acceso.

3.1.1 Código de acceso o huella dactilar digital

Para poder acceder al dispositivo móvil y disponer de toda la funcionalidad ofrecida por el mismo, **se recomienda proteger el dispositivo móvil mediante un código de acceso asociado a la pantalla de bloqueo**.

Aunque este código será solicitado al usuario en múltiples ocasiones a lo largo del día, **es necesario seleccionar un código de acceso robusto**, de al menos seis (6) u ocho (8) dígitos, y preferiblemente combinando letras y números. En ningún caso se recomienda hacer uso de un PIN o código de acceso de cuatro (4) dígitos, que por contra es empleado de manera habitual y generalizada.

Adicionalmente, y con el objetivo de que el dispositivo móvil esté expuesto el menor tiempo posible frente a accesos no autorizados, incluso temporales, **se recomienda configurar el mismo para que el código de acceso sea solicitado inmediatamente tras apagarse la pantalla, que debería de bloquearse automáticamente lo antes posible si no hay actividad por parte del usuario** (por ejemplo, tras un minuto).

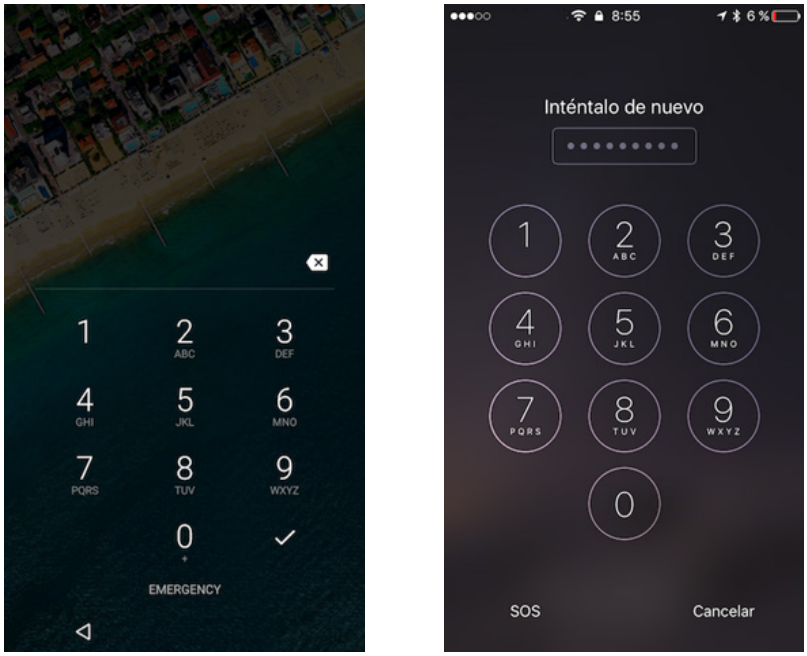


Figura 3-1 Pantalla de bloqueo con código de acceso en Android e iOS.

Con el objetivo de encontrar el equilibrio adecuado entre seguridad y funcionalidad, teniendo en cuenta que el usuario tiene que desbloquear su dispositivo móvil decenas de veces al día para hacer uso del mismo, se recomienda configurar la funcionalidad de desbloqueo mediante una huella dactilar digital (en aquellos dispositivos que disponen de estas capacidades y cuentan con un sensor de huella) complementado por un código de acceso robusto.

Esta funcionalidad permite al dispositivo móvil disponer de un mecanismo de protección y que su utilización sea lo más confortable para el usuario.

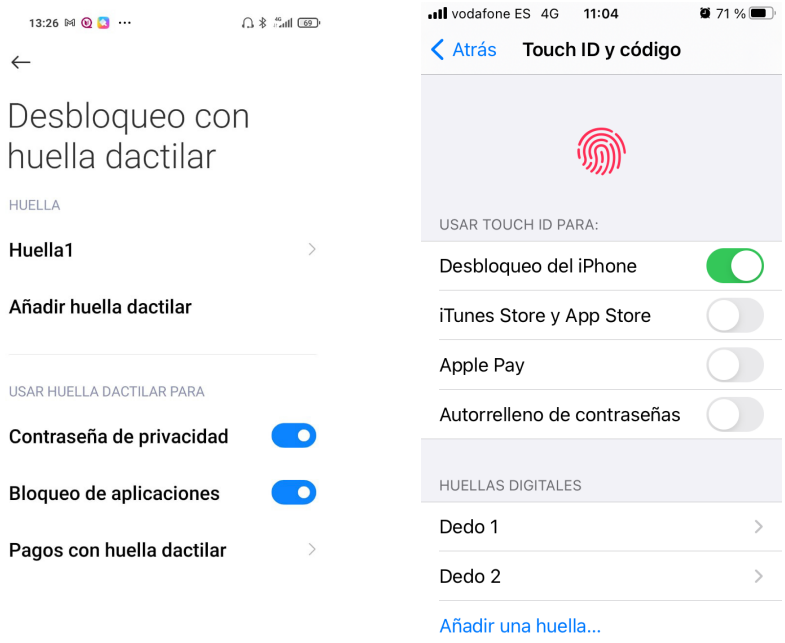


Figura 3-2 Pantalla de bloqueo con huella dactilar digital en Android e iOS.

3.1.2 Funcionalidad en la pantalla de bloqueo

La pantalla de bloqueo del dispositivo móvil permite acceder a numerosas capacidades y funcionalidades de manera rápida y sencilla por parte del usuario sin necesidad de desbloquear el mismo, como por ejemplo recibir y responder mensajes o llamadas de teléfono, recibir notificaciones de eventos y recordatorios, acceder a la cámara, modificar algunos ajustes como las capacidades de comunicación inalámbrica (Bluetooth, Wi-Fi, 2/3/4G, etc.) y gestionar el estado del modo avión, tener acceso a información de aplicaciones (app) concretas, como por ejemplo la información meteorológica o de inversiones, o interactuar con los asistentes personales digitales, como Siri en iOS, Google Assistant (o Google Now) en Android o Cortana en Windows (Phone).

La posibilidad de interactuar con algunas de estas capacidades por parte de un tercero sin conocer el código de acceso tiene implicaciones muy relevantes desde el punto de vista de seguridad.

Por ejemplo, un potencial atacante que obtenga acceso no autorizado al dispositivo móvil (tras ser extraviado o robado), podría activar el modo avión del mismo, interrumpiendo todas las comunicaciones del dispositivo móvil con otras redes y servicios remotos, e imposibilitando las capacidades de gestión a distancia que permiten al usuario localizar la ubicación actual de su dispositivo móvil, o eliminar remotamente los datos almacenados en el mismo (ver apartado "3.7. Gestión remota del dispositivo móvil").

Adicionalmente, a lo largo del tiempo se han identificado múltiples vulnerabilidades basadas en la interacción con estas capacidades, que permiten evitar la pantalla de bloqueo y el código de acceso del dispositivo móvil[3].

3. "Bypassing iOS Lock Screens: A Comprehensive Arsenal of Vulns". DinoSec. Blog Post. October 2016. http://blog.dinosec.com/2014/09/bypassing-ios-lock-screens.html

Se recomienda, por tanto, limitar y minimizar lo máximo posible la funcionalidad disponible en la pantalla de bloqueo si no se introduce el código de acceso. Para ello, se recomienda deshabilitar Google Assistant (o Now) y eliminar los iconos más críticos del panel de control de acceso a los Ajustes Rápidos disponible en la parte superior de Android (funcionalidad disponible en Android 7.0 o versiones superiores), mientras que para iOS se recomienda deshabilitar Siri, el Centro de Control disponible en la parte inferior o el Centro de Notificaciones, así como cualquier otra funcionalidad relevante.

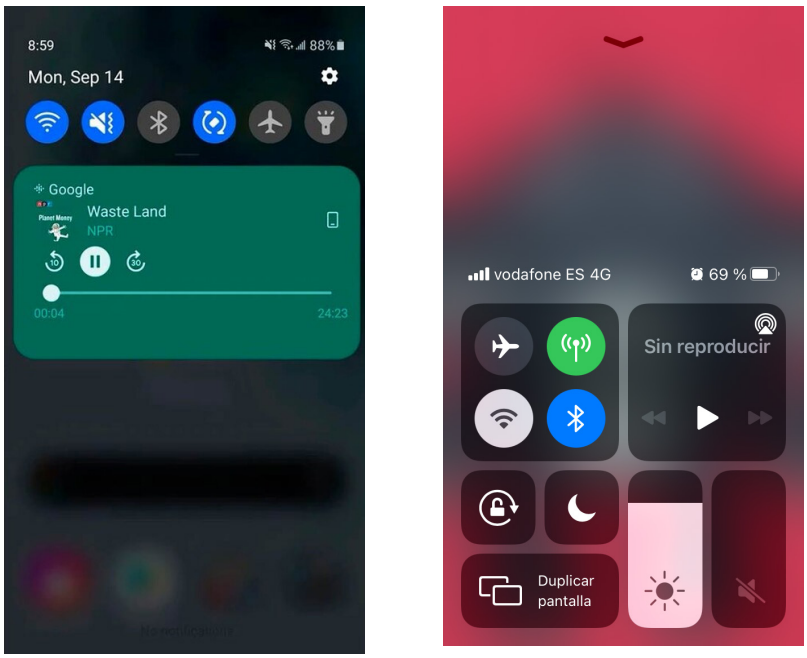


Figura 3-3 Funcionalidad sensible disponible en la pantalla de bloqueo en Android e iOS.

3.2 Comunicaciones a través de USB

Los puertos de carga y sincronización de los dispositivos móviles, situados normalmente en su parte inferior, permiten la conexión por cable mediante un puerto USB a un ordenador o enchufe. La conexión a través de USB proporciona dos (2) funcionalidades: por un lado, permite la transmisión de energía eléctrica para llevar a cabo la carga de la batería del dispositivo móvil, y por otro, permite establecer comunicaciones de datos.

Debido a que una de las limitaciones actuales de los dispositivos móviles es la capacidad y duración de la batería, debiendo los usuarios cargar en ocasiones sus dispositivos móviles a mitad del día y con cierta urgencia, los atacantes han empleado esta funcionalidad dual de las conexiones o comunicaciones USB para comprometer los dispositivos móviles a través de la conexión de datos, haciéndose pasar por una estación de carga en lugares públicos, ataque conocido como *juice jacking*.

Mediante este ataque es potencialmente posible extraer datos personales almacenados en el dispositivo móvil, así como llevar a cabo acciones más dañinas, como la instalación de *apps* dañinas:

Se conoce como *juice jacking* al ataque consistente en robar datos de los usuarios o instalar apps dañinas en sus dispositivos cuando estos los conectan en falsas estaciones de carga.

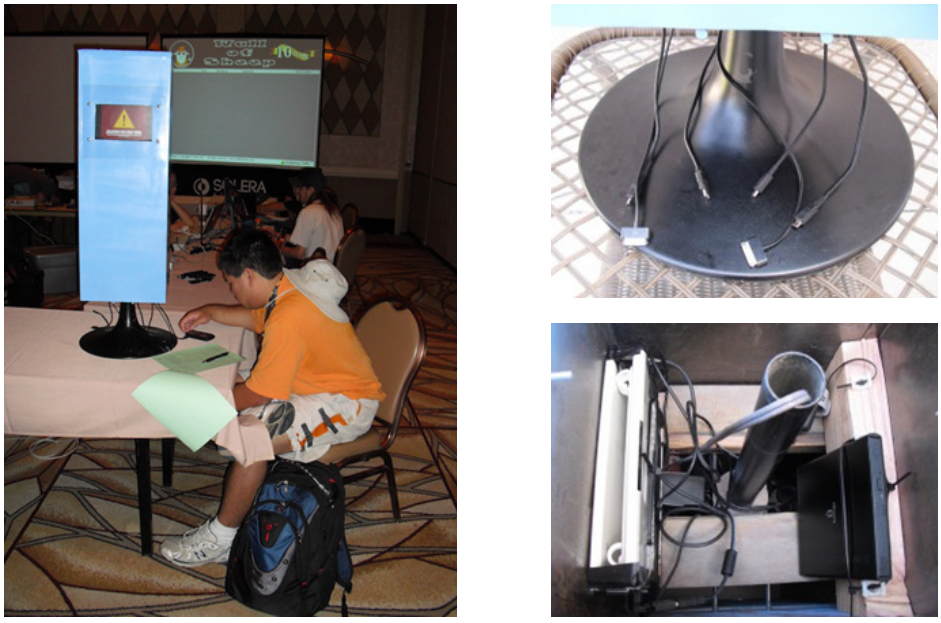


Figura 3-4 Ataques de juice jacking. Fuente: KrebsonSecurity[4]

4. "Beware of Juice-Jacking". KrebsonSecurity. Blog Post. Agosto 2011. https://krebsonsecurity.com/2011/08/beware-of-juice-jacking/

Los sistemas operativos modernos han implementado medidas de protección frente a estos ataques, debiendo establecerse una relación de confianza la primera vez que se conecta el dispositivo móvil a un ordenador a través de USB.

El dispositivo móvil solicitará al usuario si desea establecer esa relación de confianza, siendo necesario desbloquear previamente el dispositivo móvil para confirmar dicha solicitud.

Se recomienda por tanto no conectar el dispositivo móvil a puertos USB desconocidos y no aceptar ninguna relación de confianza a través de USB si no se tiene constancia de estar conectando el dispositivo móvil a un ordenador de confianza.

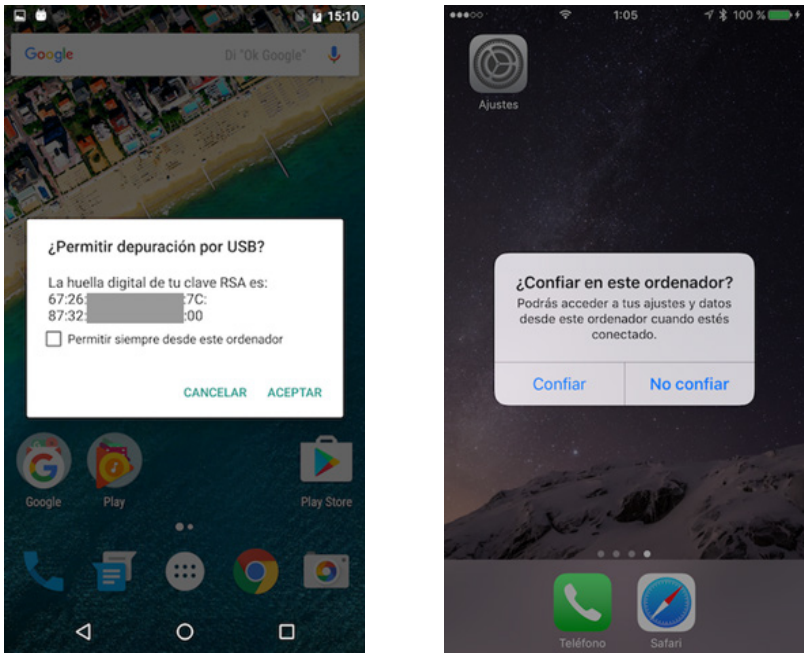


Figura 3-5 Establecimiento de relaciones de confianza vía USB en Android e iOS.

3. Buenas prácticas en la configuración y uso de los dispositivos móviles

Las capacidades de comunicación a través de USB por parte de los dispositivos móviles también permiten la instalación de *apps* en los mismos (ver apartado 3.9). Para que un potencial atacante pueda tener éxito en la instalación de una app, es necesario que el dispositivo móvil presente una configuración insegura que facilite este tipo de comunicación (en el caso de Android) y/o que el dispositivo móvil no esté bloqueado (en el caso de Android e iOS).

Para evitar la instalación de apps a través de USB, **se recomienda (en función de la plataforma móvil) no habilitar las capacidades de depuración mediante USB del dispositivo móvil**, disponibles específicamente para los desarrolladores de *apps*, y **no dejar el dispositivo móvil desatendido sin bloquear**.

3.3 Actualización del sistema operativo y de las aplicaciones

Los dispositivos móviles disponen de un sistema operativo móvil (Android, iOS, Windows Phone, etc.), también denominado *firmware*, que proporciona toda la funcionalidad existente por defecto, y que también incluye un conjunto de aplicaciones móviles que han sido instaladas por defecto por el fabricante del sistema operativo, del dispositivo o del operador de telecomunicaciones.

Adicionalmente, el usuario puede llevar a cabo la instalación de otras *apps* de terceros desde los mercados oficiales de aplicaciones o desde otros repositorios (ver apartado 3.9 "Aplicaciones móviles (apps)").

Se recomienda disponer de un sistema operativo siempre actualizado en el dispositivo móvil. Asimismo, **se recomienda disponer siempre de la última actualización de todas las *apps* instaladas en el dispositivo móvil**.

La última versión tanto del sistema operativo como de las apps soluciona vulnerabilidades públicamente conocidas y, por tanto, reduce significativamente la exposición del dispositivo frente a ataques.

Existen herramientas ofensivas para la explotación de vulnerabilidades en los dispositivos móviles que tienen capacidad para comprometer el dispositivo con tan solo abrir un mensaje de texto (SMS) o multimedia (MMS), o visitar un enlace web (sin necesidad de descargar o ejecutar ningún fichero) al aprovecharse de las debilidades en el navegador web o en el sistema operativo.

Ya que en ocasiones las herramientas ofensivas disponen de *0-days* (*exploits* para vulnerabilidades desconocidas que no han sido parcheadas), **es aconsejable que el usuario sea muy prudente a la hora de abrir mensajes o enlaces web no solicitados, desconocidos o extraños**.

La última versión tanto del sistema operativo como de las apps soluciona vulnerabilidades públicamente conocidas y, por tanto, reduce significativamente la exposición del dispositivo frente a ataques.

3.4 Cifrado del dispositivo móvil

Una característica crítica en la protección de los datos y la información almacenada localmente por el dispositivo móvil es el cifrado de su memoria interna, empleada como unidad de almacenamiento principal, así como de cualquier otra unidad de almacenamiento externa, como por ejemplo una tarjeta SD (*Secure Digital*).

Las capacidades que permiten cifrar la memoria del dispositivo móvil son imprescindibles frente al acceso físico no autorizado al mismo por parte de un tercero, ya que, en caso contrario, sería posible extraer el contenido del chip de memoria del dispositivo móvil y tener acceso a toda la información almacenada.

Independientemente de que algunas *apps* existentes en el dispositivo móvil cifren sus datos antes de almacenarlos, se recomienda hacer uso de las capacidades nativas de cifrado del dispositivo móvil, con el objetivo de proteger todos los datos e información asociadas al usuario u organización almacenados en el mismo.

Para hacer uso de estas capacidades es imprescindible establecer un código de acceso en el dispositivo móvil, que adicionalmente se recomienda que sea robusto (ver apartado 3.1.1 "Código de acceso o huella dactilar digital"), ya que este será utilizado durante el proceso de cifrado.

Se recomienda hacer uso de las capacidades nativas de cifrado del dispositivo móvil, con el objetivo de proteger todos los datos e información asociadas al usuario u organización almacenados en el mismo.

Algunos dispositivos móviles como iOS activan de manera automática las capacidades de cifrado una vez se establece un código de acceso, escenario indicado por el texto *"La protección de datos está activada."*, mientras que otros como Android requieren activar los mecanismos de cifrado intencionadamente.

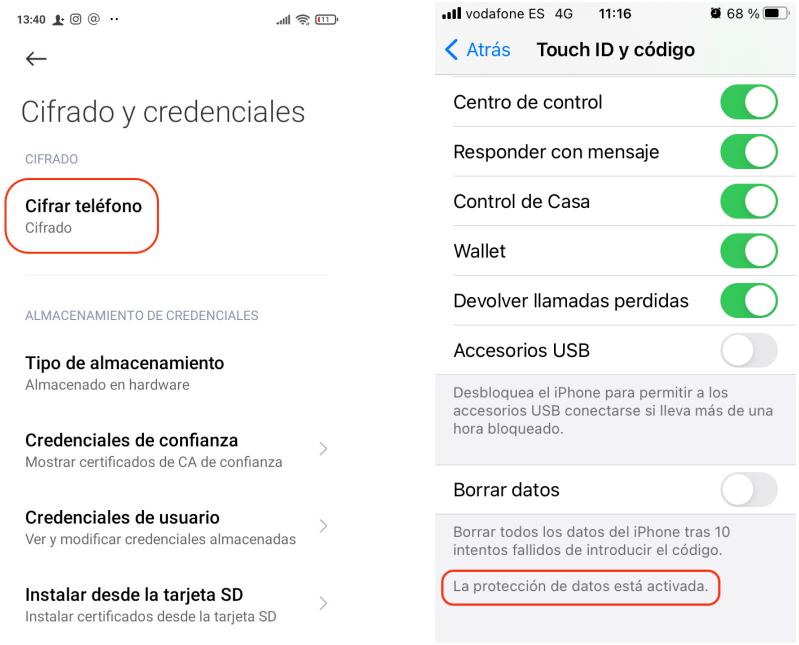


Figura 3-6 Activación de las capacidades nativas de cifrado en Android e iOS. Fuente: EFF[5]

En caso de que el dispositivo móvil disponga de una ranura para una unidad de almacenamiento externa, normalmente basada en la utilización de tarjetas de memoria SD, **se recomienda hacer uso de capacidades de cifrado que permitan proteger también los contenidos de dicha unidad externa de almacenamiento**.

En muchas ocasiones no es posible cifrar dichos contenidos, por lo que se recomienda no almacenar ningún dato o información sensible en la tarjeta SD, como por ejemplo documentos corporativos.

5. https://ssd.eff.org/en/module/how-encrypt-your-iphone

3.5 Configuración por defecto

Los dispositivos móviles, tras su activación inicial, disponen de una configuración por defecto que, por un lado, puede ser insegura y habilitar funcionalidades que podrían ser empleadas por un potencial atacante para comprometer los mismos y, por otro, contribuyen a desvelar información innecesaria acerca del propio dispositivo y/o de su propietario.

Por ejemplo, es habitual que al activar el dispositivo móvil la mayoría de sus servicios y capacidades permanezcan activos, con el objetivo de que el usuario pueda hacer un uso inmediato de los mismos, como por ejemplo el interfaz inalámbrico Bluetooth o Wi-Fi, el asistente personal digital o los servicios de sincronización en la nube.

En los dispositivos móviles más modernos, otros servicios, considerados más críticos desde el punto de vista de la privacidad del usuario, como por ejemplo los servicios de localización, deben de ser activados manualmente por el usuario durante el proceso de configuración inicial del dispositivo móvil.

Se recomienda deshabilitar todos los servicios y funcionalidades del dispositivo móvil que no vayan a ser utilizados de forma permanente por parte del usuario.

En su lugar, se recomienda habilitarlos únicamente cuando vayan a ser utilizados y volver a deshabilitarlos cuando finalice su uso.

Asimismo, se puede desvelar información acerca del propio dispositivo y/o de su propietario, como por ejemplo el fabricante y modelo del mismo o el nombre de su propietario a través del nombre del dispositivo móvil, que es difundido a través de las redes de comunicaciones de datos o mediante otras comunicaciones inalámbricas, como Bluetooth, o al llevar a cabo la configuración de un *hotspot* (punto de acceso) Wi-Fi para compartir la conexión de datos móviles 2/3/4G.

Se recomienda modificar la configuración existente por defecto en el dispositivo móvil, eliminando cualquier referencia a las características técnicas del propio dispositivo y/o de su propietario.

3.6 Copias de seguridad

La protección de la información y los datos almacenados y gestionados por el dispositivo móvil debe de extenderse frente a escenarios de pérdida o robo del mismo, así como frente a daños en el hardware que no permitan acceder a los contenidos existentes en su unidad de almacenamiento principal (o en las unidades externas).

Para evitar la pérdida de los datos, **el usuario debe realizar copias de seguridad (*backups*) periódicas, y preferiblemente automáticas, de todos los contenidos del dispositivo móvil que se desea proteger y conservar**, preferiblemente de forma local a través de USB o de una comunicación inalámbrica Wi-Fi con el ordenador del usuario.

Alternativamente, se puede hacer uso de las capacidades de realización de copias de seguridad en la nube asociadas a las principales plataformas móviles, mediante una comunicación inalámbrica.

Sin embargo, el usuario debe de ser consciente de que la facilidad y comodidad asociadas a estos mecanismos de copias de seguridad remotas conlleva implicaciones en la privacidad y seguridad de sus datos, ya que serán transferidos y almacenados en un servidor gestionado por un tercero (en la nube).

3.7 Gestión remota del dispositivo móvil

Los dispositivos móviles modernos y las capacidades de gestión remotas proporcionadas por los fabricantes de los mismos a través de sus plataformas móviles y servicios en la nube, como iCloud[6] en el caso de iOS o el Administrador de Dispositivos[7] en el caso de Android, permiten a cualquier usuario potencialmente localizar la ubicación actual de su dispositivo móvil, bloquearlo en caso de encontrarse actualmente desbloqueado, hacer que suene para identificar su ubicación cercana, mostrar un mensaje con el objetivo de que alguien que lo encuentre pueda contactar con su propietario o eliminar remotamente los datos almacenados en el mismo.

Se recomienda al usuario familiarizarse con las capacidades de gestión remota del dispositivo móvil y su plataforma móvil asociada, y comprobar el correcto funcionamiento de este servicio y de toda su funcionalidad antes de que sea necesario hacer uso de las mismas en un escenario real tras la pérdida o robo del dispositivo móvil.

Para poder hacer uso de estos servicios, el usuario debe disponer de una cuenta en la plataforma del fabricante, como por ejemplo un ID (identificador de usuario) de Apple para iCloud (iOS) o una cuenta de usuario en Google para el Administrador de Dispositivos (Android). Asimismo, el dispositivo móvil debe de estar asociado a la cuenta del usuario en la plataforma del fabricante.

6. iCloud. Apple. Web. https://www.icloud.com
7. Android Device Manager (o Administrador de Dispositivos Android). Google. Web. https://www.google.com/android/devicemanager

Complementariamente, la funcionalidad "Buscar mi iPhone" (o iPad, en iOS) y "Device Manager" (en Android) deben estar habilitadas y correctamente configuradas en el dispositivo móvil:

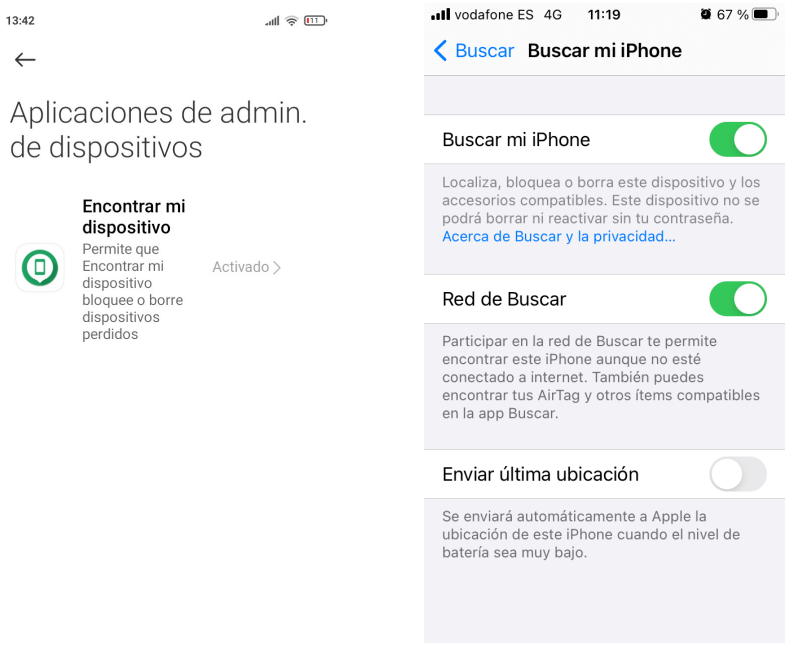


Figura 3-7 Activación de las capacidades de gestión remota en Android e iOS.

Debe tenerse en cuenta que muchas de estas capacidades remotas no estarán realmente operativas si la plataforma de gestión no puede contactar con el dispositivo móvil (o viceversa) o si el dispositivo no tiene la capacidad de obtener su ubicación.

Existen numerosos motivos y escenarios en los que la comunicación entre la plataforma de gestión y el dispositivo móvil no puede establecerse, o por los que no podría obtenerse la ubicación actual como, por ejemplo, estar el dispositivo móvil apagado, agotarse su batería, no disponer de cobertura de las redes de datos móviles 2/3/4G o no tener ninguna red Wi-Fi conocida cercana, estar activado el modo avión, encontrarse en el sótano o garaje de un edificio, etc.

3.8 Capacidades de comunicación inalámbricas

A continuación, se describen otros aspectos de seguridad de gran importancia relacionados con la confidencialidad e integridad de los datos intercambiados a través de las redes de comunicaciones.

Muchas de las funcionalidades existentes en los dispositivos móviles implican el uso de comunicaciones de datos con plataformas remotas, en las cuales se ven involucradas diversas tecnologías y servicios. Entender los escenarios de uso y el funcionamiento, al menos de forma genérica, de estas tecnologías permitirá conocer en mayor profundidad, primero, cuáles son las carencias de seguridad que presentan y, segundo, por qué es necesario tomar algunas medidas de protección para suplir y mejorar dichas carencias.

De manera genérica, **se recomienda deshabilitar todos los interfaces de comunicaciones inalámbricas del dispositivo móvil que no vayan a ser utilizados de forma permanente por parte del usuario**. En su lugar, se recomienda habilitarlos únicamente cuando vayan a ser utilizados y volver a deshabilitarlos cuando finalice su uso.

3.8.1 NFC (*Near Field Communications*)

Las capacidades NFC de los dispositivos móviles permiten establecer comunicaciones inalámbricas de corto alcance y son utilizadas actualmente en los controles de acceso y para la realización de pagos desde el dispositivo móvil, al estar integradas con las *apps* y las tarjetas bancarias.

Disponer del interfaz NFC activo en todo momento podría permitir a un potencial atacante, suficientemente próximo al dispositivo móvil, forzar la realización de transacciones y pagos fraudulentos[8].

Disponer del interfaz NFC activo en todo momento podría permitir a un potencial atacante forzar la realización de transacciones y pagos fraudulentos.

3.8.2 Bluetooth y Bluetooth Low Energy (BLE)

Las tecnologías Bluetooth y BLE son ampliamente utilizadas a día de hoy para la integración, monitorización y control de múltiples dispositivos electrónicos, como por ejemplo dispositivos personales o *wearables* (como los relojes inteligentes o *smartwatches*), vehículos (manos libres) o dispositivos asociados al Internet de las Cosas (IoT, *Internet of Things*), desde el propio dispositivo móvil, actuando este como el cerebro o controlador central del mundo digital que le rodea.

Como consecuencia, disponer del interfaz Bluetooth activo en todo momento podría permitir a un potencial atacante manipular las comunicaciones y acciones asociadas al resto de dispositivos o la información intercambiada entre estos[9].

---

8. "New Android NFC Attack Could Steal Money From Credit Cards Anytime Your Phone Is Near". Blog Post. May 2015. https://www.player.one/new-android-nfc-attack-could-steal-money-credit-cards-anytime-your-phone-near-445497#:~:text=Gadgets-,New%20Android%20NFC%20Attack%20Could%20Steal%20Money%20From,Anytime%20Your%20Phone%20Is%20Near&text=This%20attack%2C%20delivered%20through%20poisoned,are%20near%20the%20victims'%20phone

9. "Bluetooth Hack Leaves Many Smart Locks, IoT Devices Vulnerable". Blog Post. August 2016. https://threatpost.com/bluetooth-hack-leaves-many-smart-locks-iot-devices-vulnerable/119825/

3.8.3 Wi-Fi

El interfaz Wi-Fi es probablemente el mecanismo de comunicación más utilizado en la actualidad en los dispositivos móviles a la hora de intercambiar datos y acceder a servicios y aplicaciones remotas.

Disponer del interfaz Wi-Fi activo en todo momento puede permitir a un potencial atacante suplantar alguna de las diferentes redes Wi-Fi conocidas por el dispositivo móvil y a las que se conecta habitualmente (como por ejemplo la red Wi-Fi de la oficina, de casa, de la biblioteca, de la cafetería, etc.), forzando a que este se conecte automáticamente a la misma, estando en condiciones para capturar todo el tráfico generado/recibido por el dispositivo móvil y realizar ataques directamente sobre el mismo[10].

Adicionalmente, **se recomienda no conectar el dispositivo móvil a redes Wi-Fi públicas abiertas (o *hotspots* Wi-Fi) que no implementan ningún tipo de seguridad**. Aunque su utilización no tenga ningún coste asociado, se está poniendo en riesgo la información personal del usuario. La utilización de esas redes permite a un potencial atacante interceptar y manipular todo el tráfico intercambiado por el dispositivo móvil[11].

En su lugar, debe hacerse uso de redes Wi-Fi de confianza y que tienen configurados mecanismos de seguridad (como WPA2-PSK). En el caso excepcional en el que se deba hacer uso de una red Wi-Fi pública, debe emplearse un servicio de VPN (*Virtual Private Network*, o red privada virtual) para cifrar todo el tráfico transmitido a través de la red Wi-Fi.

10. "Why Do Wi-Fi Clients Disclose their PNL for Free Still Today?". DinoSec. Blog Post. February 2015. http://blog.dinosec.com/2015/02/why-do-wi-fi-clients-disclose-their-pnl.html

11. "Avast free Wi-Fi experiment fools Mobile World Congress attendees". Avast. Blog Post. February 2016. https://blog.avast.com/2016/02/24/avast-free-wi-fi-experiment-fools-mobile-world-congress-attendees/

3.8.4 Redes de telefonía: mensajería/voz y datos móviles (2/3/4G)

Una de las capacidades fundamentales ofrecidas por la mayoría de dispositivos móviles modernos es la posibilidad de conectarse a las redes de telefonía móvil para hacer uso tanto de sus servicios de voz, como de mensajería y datos (2/3/4G).

Se asume que estas capacidades estarán activas en los dispositivos móviles la mayoría del tiempo, para poder realizar y recibir llamadas, mensajes y comunicar con servicios y aplicaciones remotas cuando no se dispone de una red Wi-Fi de confianza próxima. Es necesario, por tanto, ser consciente de las debilidades de estas tecnologías que se comenzaron a extender a finales de los años 80[12] en Europa (GSM).

Las redes de telefonía 2G, todavía existentes hoy en día, no hacen uso de mecanismos de seguridad que permitan al dispositivo móvil estar seguro de que se está conectando a la red legítima del operador de telecomunicaciones (conocidos como autentificación mutua).

En consecuencia, un atacante podría suplantar dicha red legítima (de manera similar a como ocurre con las redes Wi-Fi), forzando a que el dispositivo móvil se conecte automáticamente a la misma e interceptar de nuevo sus comunicaciones con dispositivos conocidos como IMSI-Catchers o Stingrays[13].

Se recomienda que en ningún caso el usuario otorgue prioridad a las redes 2G en su dispositivo móvil frente a las redes 3G o 4G, aunque el consumo de batería sea mayor en estas últimas debido, entre otras, a sus altas capacidades de transferencia de datos. De ser posible, se debería deshabilitar el uso de redes 2G.

12. http://www.gsmhistory.com/who_created-gsm/
13. "Surprise! Scans Suggest Hackers Put IMSI-Catchers All Over Defcon". Blog Post. August 2016. http://motherboard.vice.com/read/surprise-scans-suggest-hackers-put-imsi-catchers-all-over-defcon

3.8.5 Capacidades y servicios de localización

Por último, la disponibilidad de las capacidades y los servicios de localización en los dispositivos móviles modernos, que les permiten conocer su ubicación por todo el planeta mediante el sistema de satélites GPS o a través de las redes Wi-Fi y torres de telefonía móvil, ha abierto un amplio abanico de servicios y posibilidades.

Sin embargo, la obtención y compartición de la ubicación del dispositivo móvil de manera constante, incluso en tiempo real, y por tanto de su propietario, tiene implicaciones muy relevantes desde el punto de vista de la privacidad y seguridad de los usuarios.

Por un lado, los servicios que hacen uso de estas capacidades pueden monitorizar y controlar donde se encuentra el usuario en todo momento. Por otro lado, el usuario, a propósito o de manera inadvertida, puede difundir su localización actual o pasada a través de los metadatos de las fotografías tomadas con el dispositivo móvil y publicadas posteriormente, a través de mensajes en las redes sociales o a través del uso de otras *apps*[14].

Se recomienda que el usuario deshabilite los servicios de localización si no está haciendo uso de ellos, y en caso de estar siendo utilizados, que restrinja lo máximo posible tanto la utilización intencionada de los mismos, como el acceso a estos servicios por parte de las *apps* instaladas en el dispositivo móvil, desactivando el permiso asociado para la mayoría de *apps*.

14. "How mobile apps leak user data that's supposedly off-limits". Sophos. Blog Post. February 2016. https://nakedsecurity.sophos.com/2016/02/29/how-mobile-apps-leak-user-data-thats-supposedly-off-limits/

3.9 Aplicaciones móviles (*apps*)

Los dispositivos móviles como los *smartphones* son considerados inteligentes (*smart*) porque, entre otros motivos, disponen de la capacidad de extender la funcionalidad existente por defecto mediante la instalación de nuevas aplicaciones móviles (*apps*).

3.9.1 Instalación de *apps*

El usuario puede llevar a cabo la instalación de nuevas apps desde las tiendas o mercados oficiales, como Google Play (Android), App Store (iOS) o Microsoft Store (Windows Phone), o desde otros repositorios o mercados no oficiales de terceros (en función de la plataforma móvil). Algunas plataformas móviles como iOS solo permiten por defecto la instalación de apps desde el mercado oficial, por lo que, aunque puede producirse una infección por código dañino, este debe ser introducido y propagado previamente en el mercado oficial.

Aunque se han dado varios casos de código dañino en la App Store de Apple, los controles existentes hacen que la probabilidad de infección sea menor que en otras plataformas móviles, y una vez detectado, es eliminado del mercado lo antes posible (aunque los dispositivos móviles ya infectados permanecerán infectados).

3. Buenas prácticas en la configuración y uso de los dispositivos móviles

Otras plataformas móviles como Android son más flexibles y permiten, si el usuario así lo desea, la instalación de *apps* tanto desde el mercado oficial de *apps* como desde otros mercados no oficiales, así como directamente desde servidores web o mediante mensajes de correo electrónico incluyendo la app como un fichero adjunto[15]. Esta flexibilidad es utilizada por los atacantes para distribuir código dañino e infectar los dispositivos móviles de los usuarios víctima.

Recientemente, en versiones más modernas de iOS (9 o superior) existe también la posibilidad de llevar a cabo la instalación de *apps* a través de USB (ver apartado 3.2 "Comunicaciones a través de USB"), técnica conocida como sideloading, al igual que ocurría ya en versiones previas de Android, si el dispositivo presenta una configuración insegura o no está bloqueado (en función de la plataforma móvil).

Teniendo en cuenta estas capacidades, es importante que el usuario no instale ninguna app que no provenga de una fuente de confianza, como por ejemplo los mercados oficiales de *apps*.

En las plataformas móviles que disponen de esta flexibilidad, se recomienda no habilitar la funcionalidad que permite la instalación de apps desde repositorios de terceros que no son de confianza (fuentes desconocidas) y en ningún caso instalar *apps* desde fuentes de dudosa reputación, aunque estas sean gratuitas.

Es preferible pagar el precio de una *app* (entre 0,99 € y 2,99 € para la mayoría de ellas), que exponer toda nuestra información personal por tan solo ahorrar unos pocos euros.

Es importante que el usuario no instale ninguna *app* que no provenga de una fuente de confianza, como por ejemplo los mercados oficiales de *apps*.

15. "Alternative (Open) Distribution Options". Android Developers. Documentation. https://developer.android.com/distribute/tools/open-distribution.html

3.9.2 Permisos de las apps

Los dispositivos móviles disponen de un entorno de ejecución restringido, donde una *app* no dispone por defecto de acceso a los ficheros y datos de otras apps o del sistema operativo. Para obtener acceso a esos datos y/o funcionalidad adicional, la *app* debe solicitar permisos al usuario, por ejemplo, para acceder a sus contactos, a su calendario, a componentes hardware del dispositivo móvil, como la cámara o el micrófono, o a las fotos.

En función de la plataforma móvil y de la versión de sistema operativo, los permisos serán solicitados al usuario en el momento de la instalación de la *app*, o durante su ejecución, en el momento de hacer uso de cierta funcionalidad para la que un permiso concreto sea necesario, como, por ejemplo, una aplicación que permite escanear códigos de barras y solicita permiso para acceder a la cámara del dispositivo móvil.

Se recomienda no otorgar permisos innecesarios o excesivos a las *apps*, limitando así los datos y la funcionalidad a la que estas tendrán acceso . Para ello, es necesario que previamente el usuario entienda por qué una *app* solicita un permiso determinado y para qué es necesario dicho permiso dentro de la funcionalidad proporcionada por la *app*.

Las apps correctamente desarrolladas deberían informar al usuario de los motivos concretos por los que solicitan un permiso.

Se recomienda no otorgar permisos innecesarios o excesivos a las *apps*, limitando así los datos y la funcionalidad a la que estas tendrán acceso.

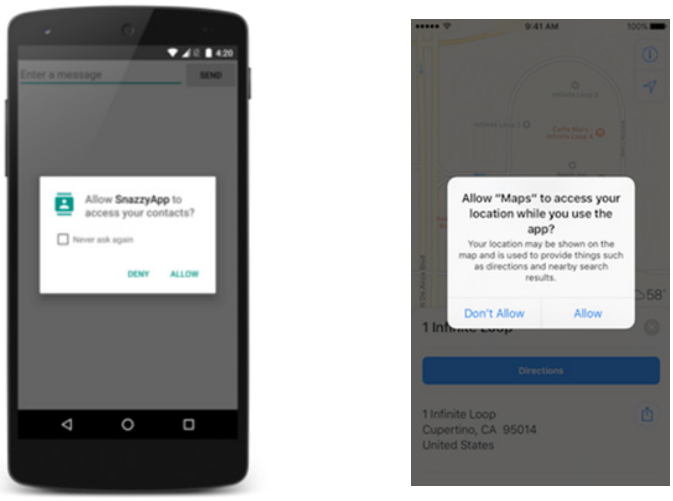


Figura 3-8 Solicitud de permisos por parte de las apps en Android e iOS. Fuente: Android Developers[16] y Apple Developers[17]

16. Requesting Permission. Apple Developers. https://developer.apple.com/ios/human-interface-guidelines/interaction/requesting-permission/
17. Requesting Permissions at Run Time. Android Developers. https://developer.android.com/training/permissions/requesting.html

3.9.3 Correo electrónico

Una de las tareas más habituales para las que son empleados los dispositivos móviles es para el acceso al correo electrónico, disponiendo de una *app* por defecto para la utilización de este servicio.

Se recomienda consultar la guía de buenas prácticas de correo electrónico del CCN-CERT[18], ya que muchas de las recomendaciones allí expuestas son de aplicación no solo para los equipos tradicionales (como los ordenadores personales), sino también para los dispositivos móviles.

3.9.4 Aplicaciones de mensajería

Adicionalmente, los dispositivos móviles son frecuentemente utilizados para establecer comunicaciones personales y profesionales con familiares, amigos, conocidos, compañeros y otros contactos de trabajo a través de las aplicaciones de mensajería, ya sea mediante el envío y recepción de mensajes de texto (SMS) o multimedia (MMS), o mediante el uso de otros servicios de mensajería como WhatsApp, Telegram, Line, etc.

A través de estos servicios es posible recibir mensajes con enlaces web que albergan código dañino, con el objetivo de infectar y comprometer el dispositivo móvil del usuario víctima. El uso de enlaces dañinos es una de las técnicas más utilizadas para conseguir ejecutar código en el dispositivo móvil de la víctima o bien para obtener información de la misma. El tipo de enlace (dónde apunta, qué tipo de acciones ejecutará, etc.) dependerá de los objetivos de los atacantes.

18. "Buenas Prácticas. CCN-CERT BP-02/16. Correo electrónico". CCN-CERT. Informe. Julio 2016. https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/1598-ccn-cert-bp-02-correo-electronico/file.html

Los usos más habituales de enlaces dañinos están descritos en la guía de buenas prácticas de correo electrónico del CCN-CERT[19], y son de aplicación a las comunicaciones de mensajería: phishing, descarga de ficheros dañinos o kits de explotación web (*Web Exploit Kits*).

Los ataques basados en enlaces maliciosos distribuidos a través de las apps de mensajería se suelen referenciar como SMiShing , en lugar de phishing (término empleado en la distribución mediante correo electrónico), y también incluyen mensajes atractivos, sugerentes o sobre los que el usuario debería llevar a cabo una acción urgente:

Los ataques basados en enlaces maliciosos distribuidos a través de las apps de mensajería se suelen referenciar como SMiShing.

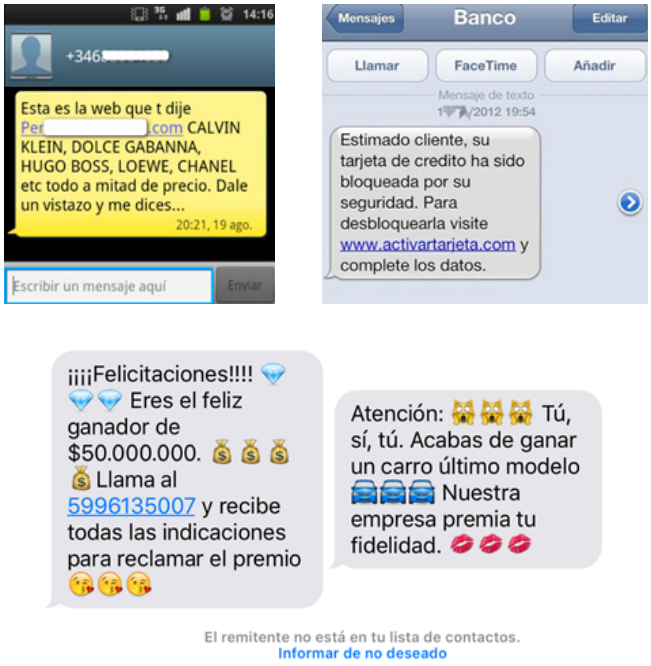


Figura 3-9 Ejemplos de mensajes de SMiShing. Fuentes: OSI[20], Hora Jaén[21], MDE[22].

19. "Buenas Prácticas. CCN-CERT BP-02/16. Correo electrónico". CCN-CERT. Informe. Julio 2016. https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/1598-ccn-cert-bp-02-correo-electronico/file.html
20. https://www.osi.es/es/actualidad/blog/2013/09/09/fraudes-online-vii-smishing-estafa-que-llega-traves-de-un-sms
21. http://horajaen.com/detienen-a-siete-jiennenses-por-una-estafa-de-pishing/
22. http://descubre.mdeinteligente.co/smishing-5-consejos-para-cuidarte-de-las-estafas-via-mensaje-de-texto/

El ataque apodado como Pegasus[23] que tuvo lugar en agosto de 2016 contra Ahmed Mansoor, un defensor de los derechos humanos de reconocido prestigio a nivel internacional y residente en los Emiratos Árabes Unidos, utilizó este tipo de técnicas basadas en el envío de un mensaje SMS dañino para intentar infectar el iPhone de la víctima y tomar el control completo del mismo mediante un software de espionaje (*spyware*) sofisticado, empleando tres nuevas vulnerabilidades desconocidas públicamente con anterioridad (*0-days*):

Figura 3-10 Mensajes SMS dañinos recibidos por Mansoor con el remitente falseado (Pegasus). Fuente: Citizenlab

Sin duda alguna, el consejo más eficaz para identificar mensajes dañinos es el sentido común, al igual que para el correo electrónico. Esto significa **que cualquier síntoma o patrón fuera de lo considerado normal o habitual debe despertar la sospecha del usuario**.

Un patrón o síntoma irregular puede significar: recibir un mensaje de un remitente no conocido, recibir un mensaje que solicite información personal, que el contenido del mensaje sea demasiado atractivo como para ser cierto, etc.

23. "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender". Citizenlab. Blog Post. Agosto 2016. https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

Por ejemplo, un mensaje remitido por una compañía de confianza que presente un asunto o solicitud poco habitual y en el que se incluya algún enlace, debe generar cierta desconfianza por parte del usuario. Ante este escenario, lo más recomendable antes de pulsar en el enlace es contactar con el supuesto remitente utilizando otra vía de contacto diferente como, por ejemplo, teléfono, correo electrónico, etc. De este modo se podrá corroborar si el mensaje recibido es legítimo o no.

Debe tenerse en cuenta que, al igual que sucede con los correos electrónicos, un atacante podrá en ocasiones suplantar el remitente del mensaje, intentando hacerse pasar por él, por lo que no se debe confiar ciegamente en esta información.

3.9.5 Redes sociales

Otro de los usos muy habituales de los dispositivos móviles por parte de los usuarios es la interacción con redes sociales, como por ejemplo Facebook, Twitter, Instagram, etc.

A la hora de publicar cualquier tipo de información personal o imágenes en las redes sociales, **se recomienda evaluar la sensibilidad y privacidad de los datos a publicar y tener en cuenta que esos contenidos pasarán a estar disponibles potencialmente para numerosas personas**, no únicamente para el círculo cerrado de amistades del usuario.

Esa información es frecuentemente utilizada tanto para coaccionar o chantajear al usuario con su difusión, como para obtener datos decisivos o establecer relaciones y comunicaciones que determinen el éxito o fracaso de una campaña de phishing dirigido (*spear phishing*) contra el usuario o la organización en la que trabaja.

3.9.6 Navegación web

Igualmente, es muy habitual que los dispositivos móviles sean utilizados para tareas de navegación web, con el objetivo de consultar contenidos web o de interactuar con multitud de servicios disponibles en Internet, disponiendo del navegador web estándar o de una app específica para su utilización.

El protocolo involucrado en el proceso de navegación web para el acceso a contenidos y servicios web es HTTP. Este protocolo ha sido utilizado desde 1991[24] y cuando fue implementando no se tuvieron en cuenta medidas de seguridad, tales como el cifrado o la autenticación robusta de las comunicaciones.

Esto quiere decir que todo el proceso de petición y respuesta de contenidos entre el dispositivo móvil y un servidor o aplicación web se realiza en texto plano, es decir, que en cualquier punto de la trasmisión un atacante podría ver y manipular el contenido de las páginas web.

Debido a estas carencias en HTTP, se han ido desarrollado diversas tecnologías y extensiones que permiten incorporar medidas de seguridad a las comunicaciones web para, por ejemplo, garantizar el cifrado de los datos transmitidos. Por este motivo surgió el protocolo HTTPS, basado en TLS, indicando mediante la letra "S" sus características de seguridad adicionales.

Utilizar HTTPS permite, por ejemplo, inicializar un intercambio TLS con el servidor web previo al envío de cualquier dato sensible, como las credenciales del usuario necesarias al acceder a un servicio web como el correo electrónico, redes sociales o un banco o tienda online. De esta forma, un atacante que monitorice las comunicaciones no podría acceder a dicha información sensible.

24. http://info.cern.ch/hypertext/WWW/History.html

En el caso de la navegación web a través de un dispositivo móvil, como por ejemplo Safari, Chrome, Firefox, etc., el usuario dispone de la posibilidad de indicar que desea hacer uso del protocolo HTTPS, a diferencia de las comunicaciones empleadas por las aplicaciones móviles, donde la conexión se lleva a cabo automáticamente por parte de la app, sin que el usuario deba o pueda indicar el servidor al que se quiere conectar o cómo desea conectarse.

Los proveedores, organizaciones y compañías más conocidas que disponen de una página web permiten el acceso a sus servidores web mediante HTTPS, aunque todavía muchas organizaciones hoy en día siguen haciendo uso exclusivo de HTTP.

Por tanto, **se recomienda, siempre que sea posible, hacer uso del protocolo HTTPS mediante la inserción del texto "https://" antes de introducir la dirección web del servidor con el que se desea conectar**.

Debe tenerse en cuenta que estas medidas de seguridad son susceptibles de ser atacadas. Por ejemplo, HTTPS es vulnerable frente a ataques *Man-in-the-Middle* (MitM), donde un atacante se sitúa en medio de la comunicación entre el dispositivo móvil y el servidor o aplicación web remoto, con el objetivo de manipular la comunicación. Por un lado, el atacante puede intentar suplantar al servidor o aplicación web legítimo, ofreciendo al usuario víctima un certificado digital que puede ser similar al legítimo, pero que no será aceptado como válido o de confianza por su navegador web.

Como resultado, el navegador web generará un mensaje de error del certificado que, en caso de ser aceptado por el usuario, hará que se establezca una conexión cifrada con el atacante, permitiéndole interceptar todos los datos intercambiados, incluyendo credenciales de acceso y otra información confidencial y crítica.

Por otro lado, el atacante puede intentar eliminar el uso de HTTPS en toda comunicación entre el usuario y el servidor o aplicación web legítimo, empleando un ataque conocido como sslstrip, con consecuencias similares para el usuario.

El usuario nunca debería aceptar un mensaje de error del navegador web asociado a un certificado digital inválido, recomendándose cancelar la conexión. En su lugar, se debe verificar si realmente se está conectando al servidor web que pretende conectarse a través de la dirección web e intentar obtener más detalles del motivo por el que se ha generado el error de certificado.

En caso de ser necesario establecer la conexión, se recomienda hacer uso de otra red, por ejemplo, la red de datos móviles 2/3/4G, si se estaba empleando una red Wi-Fi, o incluso un ordenador conectado a otra red diferente, como la red de la oficina o de casa.

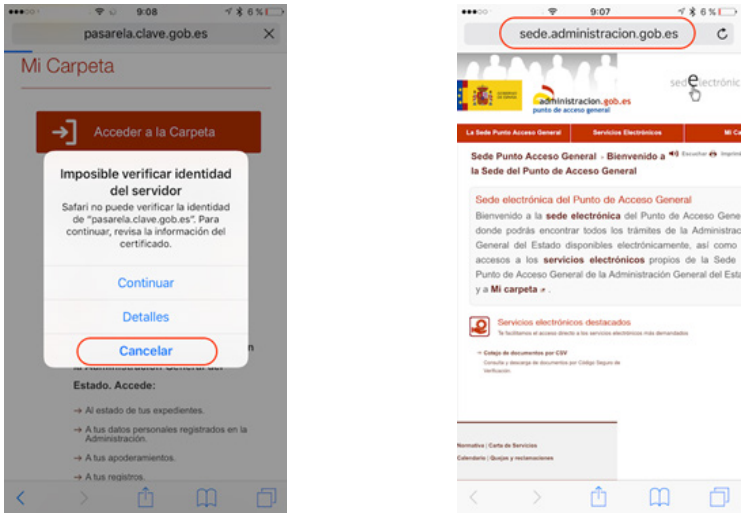


Figura 3-11 Ataques MitM y sslstrip: Error de certificado o ausencia de HTTPS.

Para verificar si la conexión con un servidor o aplicación web es cifrada, debe verificarse que la barra de dirección del navegador web hace uso de HTTPS, indicado por el texto "https://" al comienzo de la dirección web.

Desafortunadamente, por defecto, la barra de dirección de los navegadores web de los dispositivos móviles modernos tiende a minimizar la información mostrada al usuario, destacando únicamente el dominio con el que se ha establecido la conexión.

Para poder obtener todos los detalles del servidor web y del recurso accedido, así como verificar si el método de conexión empleado es HTTPS (verificar que aparece un candado no siempre es suficiente), puede ser necesario seleccionar la barra de dirección y desplazarse hacia la izquierda para visualizar todos los detalles:

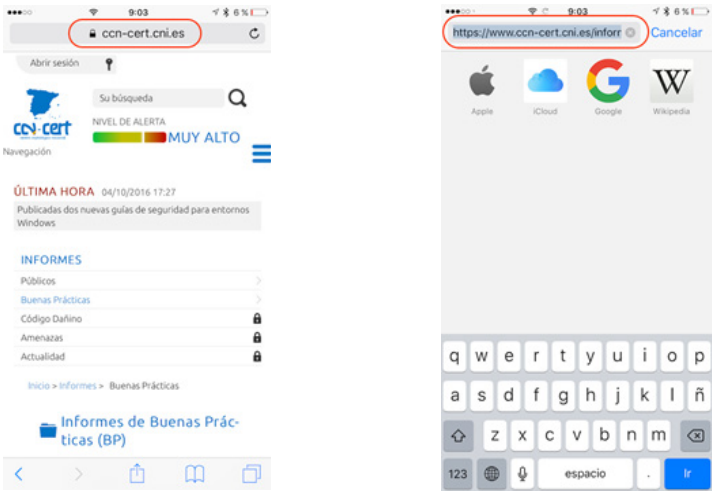


Figura 3-12 Ataques MitM y ssltrip: Verificación manual del uso de HTTPS.

4. Otras recomendaciones de carácter genérico

Desde el punto de vista corporativo, se recomienda hacer uso de soluciones de gestión empresarial de dispositivos móviles (MDM, *Mobile Device Management*), con el objetivo de disponer de capacidades para definir, establecer y monitorizar las diferentes recomendaciones de seguridad sobre todos los dispositivos móviles de la organización de manera homogénea.

Estas soluciones permiten aplicar configuraciones de seguridad en los dispositivos móviles en función de las políticas de seguridad definidas previamente por la organización.

El proceso de *jailbreak* (iOS) o *rooting* (Android) consiste en llevar a cabo ciertas acciones (mediante la explotación intencionada de vulnerabilidades) en el dispositivo móvil para tomar control completo del mismo y disponer de los máximos privilegios.

Aunque algunos usuarios realizan este proceso para disponer de capacidades y funcionalidades no existentes por defecto, debido a limitaciones impuestas por el fabricante, no se recomienda su utilización.

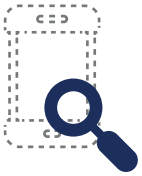
Como resultado, se deshabilitan muchos de los mecanismos de seguridad existentes en las plataformas móviles. Si no se dispone de los suficientes conocimientos técnicos, tras realizar el proceso de *jailbreak* o *rooting*, el usuario dispondrá de un dispositivo móvil más inseguro y que podría ser más fácilmente comprometido o infectado.

4. Otras recomendaciones de carácter genérico

Se recomienda hacer uso de contraseñas robustas[25] para todos y cada uno de los servicios y aplicaciones que son accedidos desde el dispositivo móvil. Dichas contraseñas no deben ser reutilizadas entre distintos servicios o aplicaciones.

Adicionalmente, para los servicios o aplicaciones que dispongan de esta funcionalidad, y especialmente para los de mayor criticidad, se recomienda hacer uso de un segundo factor de autenticación.

En el caso de ser posible, se recomienda no almacenar las credenciales de los diferentes servicios y aplicaciones utilizados en el propio dispositivo móvil, ya que estas podrían ser recuperadas en caso de que el dispositivo se viera infectado.



Debe informarse inmediatamente al responsable de seguridad de la organización en el caso de perder o extraviar el dispositivo móvil, al igual que si se identifica cualquier comportamiento anómalo o sospechoso al hacer uso del mismo.

Adicionalmente al código de acceso, se recomienda establecer el PIN asociado a la tarjeta SIM para evitar un uso indebido y no autorizado de las capacidades de comunicación de telefonía, como la realización de llamadas telefónicas. El código de acceso y el PIN de la tarjeta SIM deben ser diferentes.

Con el objetivo de identificar posibles infecciones en el dispositivo móvil o cualquier otro tipo de fraude relacionado, el usuario debería verificar mensualmente el consumo asociado a su contrato a través de la factura del operador de telefonía móvil e identificar lo antes posible anomalías, como por ejemplo el envío de mensajes de texto (SMS) o multimedia (MMS), o la realización de llamadas de voz que no son reconocidas.

25. Schneier on Security. Blog Post. March 2014. https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html

5. Decálogo de recomendaciones

Con este decálogo de buenas prácticas se pretende mejorar el nivel de protección y seguridad de los dispositivos móviles.

Decálogo de seguridad de los dispositivos móviles

1. **El dispositivo móvil debe estar protegido mediante un código de acceso robusto** asociado a la pantalla de bloqueo (o, en su defecto, una huella dactilar digital).

   El código de acceso debe ser solicitado inmediatamente tras apagarse la pantalla, que debería de bloquearse automáticamente lo antes posible si no hay actividad por parte del usuario. No se debe dejar el dispositivo móvil desatendido sin bloquear.

2. **Se debe hacer uso de las capacidades nativas de cifrado del dispositivo móvil** con el objetivo de proteger todos los datos e información almacenados en el mismo.

3. **El sistema operativo del dispositivo móvil debe estar siempre actualizado**, al igual que todas las aplicaciones móviles (*apps*).

4. **No conectar el dispositivo móvil a puertos USB desconocidos y no aceptar ninguna relación de confianza a través de USB** si no se tiene constancia de estar conectando el dispositivo móvil a un ordenador de confianza.

5. **Deshabilitar todos los interfaces de comunicaciones inalámbricas del dispositivo móvil** (NFC, Bluetooth y BLE, Wi-Fi, servicios de localización, etc.) que no vayan a ser utilizados de forma permanente por parte del usuario. Deberían habilitarse únicamente cuando vayan a ser utilizados y volver a deshabilitarse al finalizar su uso.

6. **No conectar el dispositivo móvil a redes Wi-Fi públicas abiertas** (o *hotspots* Wi-Fi) que no implementan ningún tipo de seguridad.

7. **No instalar ninguna aplicación móvil (app) que no provenga de una fuente de confianza**, como los mercados oficiales de apps (Google Play, App Store, etc.).

8. **Se recomienda no otorgar permisos innecesarios o excesivos a las apps**, limitando así los datos y la funcionalidad a la que estas tendrán acceso.

9. **Siempre que sea posible se debe hacer uso del protocolo HTTPS** (mediante la inserción del texto "https://" antes de la dirección web del servidor a contactar).

   Nunca se debería aceptar un mensaje de error de certificado digital inválido.

10. **Se deben realizar copias de seguridad (backups) periódicas**, y preferiblemente automáticas, de todos los contenidos del dispositivo móvil que se desea proteger y conservar.

CCN centro criptológico nacional

CCN-CERT centro criptológico nacional

Figura 5-1. Decálogo de seguridad

centro criptológico nacional

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es