GUÍA DE SEGURIDAD DE LAS TIC
(CCN-STIC-606)

SEGURIDAD EN OS X:
YOSEMITE (10.10.X)

SEPTIEMBRE 2015

Edita:

NIPO: 002-15-022-3

Fecha de Edición: Septiembre de 2015

Raúl Siles (DinoSec) ha participado en la elaboración y modificación del presente documento y sus anexos.

PRÓLOGO

Entre los elementos más característicos del actual escenario nacional e internacional figura el desarrollo alcanzado por las Tecnologías de la Información y las Comunicaciones (TIC), así como los riesgos emergentes asociados a su utilización. La Administración no es ajena a este escenario, y el desarrollo, adquisición, conservación y utilización segura de las TIC por parte de la Administración es necesario para garantizar su funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales.

Partiendo del conocimiento y la experiencia del Centro sobre amenazas y vulnerabilidades en materia de riesgos emergentes, la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Una de las funciones más destacables que, asigna al mismo, el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración.

La ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 crea del Esquema Nacional de Seguridad (ENS), que establece las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos.

El Real Decreto 3/2010 de 8 de Enero desarrolla el Esquema Nacional de Seguridad y fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración. En su artículo 29 se autoriza que a través de la series CCN-STIC el CCN desarrolle lo establecido en el mismo.

La serie de documentos CCN-STIC se ha elaborado para dar cumplimiento a esta función y a lo reflejado en el ENS, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Agosto de 2015

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN 8
2. OBJETO 9
3. ALCANCE 9
4. ENTORNO DE APLICACIÓN DE ESTA GUÍA 10
5. CONFIGURACIÓN DE SEGURIDAD DE OS X 18
5.1 PROCESO DE INSTALACIÓN Y CONFIGURACIÓN INICIAL 18
5.2 NOMBRE DE EQUIPO 19
5.2.1 ENTRADA DE DATOS DESDE EL TERMINAL 21
5.3 ACTUALIZACIONES 21
5.3.1 ACTUALIZACIONES DE SISTEMA OPERATIVO: OS X 21
5.3.2 ACTUALIZACIONES DE FIRMWARE 28
5.3.3 ACTUALIZACIONES DE APLICACIONES: APP STORE 31
5.3.4 ACTUALIZACIONES DE APLICACIONES DE TERCEROS 32
5.3.4.1 ORACLE JAVA 33
5.3.4.2 ADOBE FLASH 35
5.3.5 CASO PRÁCTICO: VULNERABILIDADES EN OS X 38
5.4 PROTECCIÓN DEL PROCESO DE ARRANQUE DEL EQUIPO 40
5.4.1 MODO SEGURO 41
5.4.2 GESTOR DE ARRANQUE 43
5.4.2.1 ARRANCAR DESDE UN CD/DVD O UNA MEMORIA USB EXTERNA 44
5.4.3 APPLE HARDWARE TEST (AHT) O DIAGNÓSTICOS DE APPLE 45
5.4.4 RECUPERACIÓN DE OS X 47
5.4.4.1 OPCIONES DE ACCESO AL MODO DE RECUPERACIÓN 49
5.4.4.2 TERMINAL DESDE EL MODO DE RECUPERACIÓN 50
5.4.4.3 ASISTENTE DE DISCO DE RECUPERACIÓN 53
5.4.5 MODO DE RESTABLECIMIENTO DE LA NVRAM 55
5.4.6 MODO DE RESTABLECIMIENTO DEL SMC 55
5.4.7 MODO DE UN SOLO USUARIO 56
5.4.8 MODO VERBOSO 58
5.4.9 ESTABLECER UNA CONTRASEÑA EN EL FIRMWARE DEL EQUIPO 58
5.4.9.1 UTILIDAD "FIRMWAREPASSWD" 60
5.4.9.2 FUERZA BRUTA DE LA CONTRASEÑA DEL FIRMWARE 62
5.4.9.3 ELIMINACIÓN DE LA CONTRASEÑA DEL FIRMWARE POR PARTE DE APPLE 63
5.4.9.4 ELIMINACIÓN DE LA CONTRASEÑA DEL FIRMWARE RESTABLECIENDO LA NVRAM 64

5.4.9.5 ELIMINACIÓN Y OBTENCIÓN DE LA CONTRASEÑA DEL FIRMWARE MEDIANTE EFIPW 64

5.4.9.6 ELIMINACIÓN DE LA CONTRASEÑA DEL FIRMWARE REEMPLAZANDO O REPROGRAMANDO EL CHIP ATMEL 65

5.4.9.7 ATAQUES FIRMWARE MEDIANTE EL PUERTO THUNDERBOLT (Y EL EFI) 66

5.5 PROTECCIÓN DEL PROCESO DE ARRANQUE DE OS X 67

5.5.1 PROCESO DE ARRANQUE 67

5.5.2 ACTIVACIÓN DE SERVICIOS Y APLICACIONES DURANTE EL PROCESO DE ARRANQUE DE OS X 68

5.5.3 EJECUCIÓN DE APLICACIONES DURANTE EL INICIO O FINALIZACIÓN DE SESIÓN 70

5.6 EJECUCIÓN DE TAREAS PROGRAMADAS EN OS X 72

5.7 USUARIOS Y GRUPOS 73

5.7.1 CREACIÓN DE UNA CUENTA DE USUARIO ESTÁNDAR 73

5.7.2 OPCIONES DE INICIO DE SESIÓN 77

5.7.2.1 INICIO DE SESIÓN AUTOMÁTICO 77

5.7.2.2 PANTALLA DE INICIO DE SESIÓN O LOGIN 78

5.7.2.3 MENÚ DE CAMBIO RÁPIDO DE USUARIO 82

5.7.2.4 MENSAJE PERSONALIZADO EN LA PANTALLA DE INICIO DE SESIÓN 82

5.7.3 CONTRASEÑA MAESTRA 83

5.7.4 SOLICITUD DE CONTRASEÑA 84

5.7.5 CUENTAS DE USUARIO 87

5.7.6 ALMACENAMIENTO DE LAS CONTRASEÑAS DE USUARIO 89

5.7.7 SOLICITAR CONTRASEÑA DE ADMINISTRADOR PARA MODIFICAR PREFERENCIAS DEL SISTEMA 89

5.8 MECANISMOS DE PROTECCIÓN Y TECNOLOGÍAS DE SEGURIDAD EN OS X 91

5.8.1 TECNOLOGÍAS GENÉRICAS DE SEGURIDAD 91

5.8.2 GATEKEEPER Y CUARENTENA DE ARCHIVOS 92

5.8.3 XPROTECT: SOFTWARE MALICIOSO (*MALWARE*) 100

5.8.4 CIFRADO COMPLETO DEL DISCO: FILEVAULT 102

5.8.4.1 CIFRADO DE UNIDADES O DISCOS EXTERNOS 112

5.8.5 SANDBOX 115

5.8.6 FIRMA Y VERIFICACIÓN DE APLICACIONES Y DEL KERNEL 115

5.8.6.1 FIRMA DE EXTENSIONES DE KERNEL 116

5.8.7 ACCESO A LLAVEROS 117

5.8.8 ACCESO A LLAVEROS EN ICLOUD 123

5.8.9 BORRADO SEGURO DE FICHEROS 124

5.8.10 BASE DE DATOS DE AUTORIZACIONES DE SEGURIDAD 127

5.8.11 PERMISOS DEL SISTEMA DE FICHEROS 127

5.9 PRIVACIDAD 129
5.9.1 DESHABILITAR LAS SUGERENCIAS DE SPOTLIGHT 134
5.10 EVENTOS DE SEGURIDAD 137
5.11 COPIAS DE SEGURIDAD (*BACKUPS*) 138
5.11.1 COPIAS DE SEGURIDAD LOCALES O EN RED 138
5.11.2 COPIAS DE SEGURIDAD EN ICLOUD 138
5.12 ICLOUD: BUSCAR MI MAC 143
5.12.1.1 BLOQUEO REMOTO DE OS X DESDE ICLOUD 145
5.12.1.2 ELIMINACIÓN DEL PIN DE BLOQUEO DE ICLOUD DESDE OS X 148
5.12.1.3 FUERZA BRUTA DEL PIN DE BLOQUEO DE ICLOUD 149
5.12.1.4 BORRADO REMOTO DESDE ICLOUD 149
5.13 COMUNICACIONES 149
5.13.1 INTERFACES DE RED 150
5.13.2 CONFIGURACIÓN DE LOS INTERFACES DE RED 155
5.13.3 PROXIES 157
5.13.4 BONJOUR 158
5.13.5 IPV6 159
5.13.6 SERVICIOS COMPARTIDOS 160
5.13.6.1 COMPARTIR PANTALLA 162
5.13.6.2 COMPARTIR ARCHIVOS 165
5.13.6.3 COMPARTIR IMPRESORA 170
5.13.6.4 SESIÓN REMOTA 171
5.13.6.5 GESTIÓN REMOTA 173
5.13.6.6 EVENTOS APPLE REMOTOS 175
5.13.6.7 COMPARTIR INTERNET 176
5.13.6.8 COMPARTIR BLUETOOTH 177
5.13.7 AIRDROP 179
5.13.8 VOLVER A MI MAC 181
5.13.9 SERVICIOS Y APLICACIONES TCP/IP DISPONIBLES POR DEFECTO 182
5.13.10 CORTAFUEGOS 183
5.13.10.1 APPLICATION LAYER FIREWALL (ALF) 183
5.13.10.2 PACKET FILTER (PF) 191
5.13.11 BLUETOOTH 193
5.13.12 WI-FI 196
5.13.13 VERIFICACIÓN DE CERTIFICADOS DIGITALES 204
5.13.14 NAVEGACIÓN WEB 205
5.13.14.1 MÓDULOS DEL NAVEGADOR WEB 205

5.13.14.2 DESCARGA DE ARCHIVOS 208
5.13.14.3 AUTORELLENO DE FORMULARIOS WEB Y CONTRASEÑAS 209
5.13.14.4 SITIOS WEB FRAUDULENTOS 210
5.13.14.5 SEGURIDAD 210
5.13.14.6 COOKIES 211
5.13.14.7 SERVICIOS DE UBICACIÓN Y SEGUIMIENTO 211
5.13.14.8 AJUSTES DE CONFIGURACIÓN AVANZADOS 211
5.13.15 VPN 213
5.14 ANTIVIRUS 213
5.15 SISTEMA DE DETECCIÓN DE INTRUSOS (IDS) 213
ANEXO A. PROCESO DE INSTALACIÓN Y CONFIGURACIÓN INICIAL DE OS X 214
ANEXO B. PROCESO DE RESTAURACIÓN DE LOS AJUSTES DE FÁBRICA O FORMATEO DE OS X 221
ANEXO C. LISTADO DE EXTENSIONES DE KERNEL POR DEFECTO 223
ANEXO D. REFERENCIAS 228

1. INTRODUCCIÓN

1. La presente guía refleja un conjunto de normas desarrolladas por el Centro Criptológico Nacional (CCN) para entornos y equipos (u ordenadores) basados en el sistema operativo OS X de Apple, sistema operativo también referenciado en el pasado como Mac OS X[1].

2. El sistema operativo OS X de Apple constituye la única opción disponible por defecto para los ordenadores de Apple, tanto portátiles como equipos de sobremesa o servidores, durante el proceso de instalación y configuración inicial.

3. Pese a que el software Boot Camp[2] permite la instalación y ejecución de otros sistemas operativos, como por ejemplo Windows (diferentes versiones) o Linux, en los ordenadores de Apple basados en la arquitectura Intel, la opción más comúnmente utilizada en los equipos de Apple pasa por hacer uso de OS X.

4. Boot Camp permite gestionar las particiones del disco duro (ver siguiente "Nota") del equipo para acomodar la coexistencia de diferentes sistemas operativos en los ordenadores de Apple mediante un sistema de arranque dual, pero su utilización, así como la ejecución de otros sistemas operativos distintos a OS X en estos equipos, queda fuera del alcance de la presente guía.

Nota: a lo largo de la presente guía se hace referencia indistintamente al "sistema de almacenamiento principal" empleado por el ordenador Mac empleando ese término descriptivo, junto al término disco duro (por abreviar), pese a que los modelos de equipos Mac más modernos no hacen uso de discos duros tradicionales (HDD, *Hard Disk Drive*) sino de discos, unidades o memorias SSD (*Solid State Drive*).

5. La presente guía es complementada por algunas de las guías de la serie CCN-STIC-450 correspondientes a la seguridad de dispositivos móviles, y en concreto por aquellas asociadas al sistema operativo iOS de Apple (empleado en los dispositivos móviles iPhone e iPad, entre otros) debido a sus capacidades de integración con OS X:

    - CCN-STIC-454 - Seguridad de dispositivos móviles: iPad (iOS 7.x)
    - CCN-STIC-455 - Seguridad de dispositivos móviles: iPhone (iOS 7.x)

Nota: esta guía está diseñada considerando como requisito la necesidad de encontrar un equilibrio entre seguridad y funcionalidad en relación a las capacidades disponibles en los equipos a proteger, con el objetivo de poder hacer uso de la mayoría de características disponibles en los mismos de forma segura. Por ejemplo, la presente guía asume que el equipo objeto de aplicación de la misma dispondrá de conexión con redes no seguras como puede ser Internet.

[1] http://es.wikipedia.org/wiki/OS_X

[2] https://www.apple.com/es/support/bootcamp/

2. OBJETO

6. El propósito de la presente guía es proporcionar una lista de recomendaciones de seguridad para la configuración de equipos basados en el sistema operativo OS X versión Yosemite (10.10.x), y en concreto sobre ordenadores portátiles de Apple (en adelante referenciados como equipo u ordenador, indistintamente).

7. El objetivo principal de la presente guía es realizar un análisis detallado de los mecanismos y las opciones de configuración de seguridad disponibles en el sistema operativo OS X de Apple[3], y evaluar su aplicación sobre los equipos objeto de aplicación de la misma.

8. Como resultado se pretende tanto proteger el propio equipo, como sus comunicaciones y la información y datos que gestiona y almacena, reduciendo su superficie de exposición frente a accesos no autorizados y potenciales ataques, y minimizando los riesgos, amenazas, y vulnerabilidades de seguridad a las que están expuestos los equipos basados en el sistema operativo OS X de Apple en la actualidad.

9. La presente guía proporciona los detalles específicos de aplicación e implementación de las recomendaciones de seguridad previamente identificadas, comenzando por el proceso de instalación inicial del equipo y continuando con las tareas adicionales y necesarias para su configuración y administración.

10. En el pasado Apple proporcionaba guías de configuración de seguridad de OS X para diferentes versiones de su sistema operativo. Desafortunadamente, la última versión para la que hay disponible una guía oficial en la actualidad es la versión OS X 10.6, Snow Leopard [Ref.- 5].

Nota: los términos equipo y ordenador son empleados indistintamente y de manera general en la presente guía para referenciar a los ordenadores de Apple objeto de aplicación de la misma, siendo posible su implantación tanto sobre ordenadores portátiles como ordenadores de sobremesa, e independientemente de su función principal, cliente o servidor.

Sin embargo, el enfoque principal de la presente guía se centra en ordenadores portátiles MacBook Air, MacBook o MacBook Pro de Apple, empleados como equipos cliente.

3. ALCANCE

11. Las Autoridades responsables de la aplicación de la Política de Seguridad de las TIC (STIC) determinarán su análisis y aplicación a los equipos basados en el sistema operativo OS X de Apple ya existentes o futuros bajo su responsabilidad.

12. En concreto este documento incluye un conjunto de recomendaciones de seguridad a aplicar durante el proceso de instalación y configuración inicial de un equipo Mac nuevo basado en OS X, así como el conjunto de recomendaciones de seguridad que permite modificar la configuración de un equipo Mac ya instalado y operativo en cualquier momento posterior a su instalación.

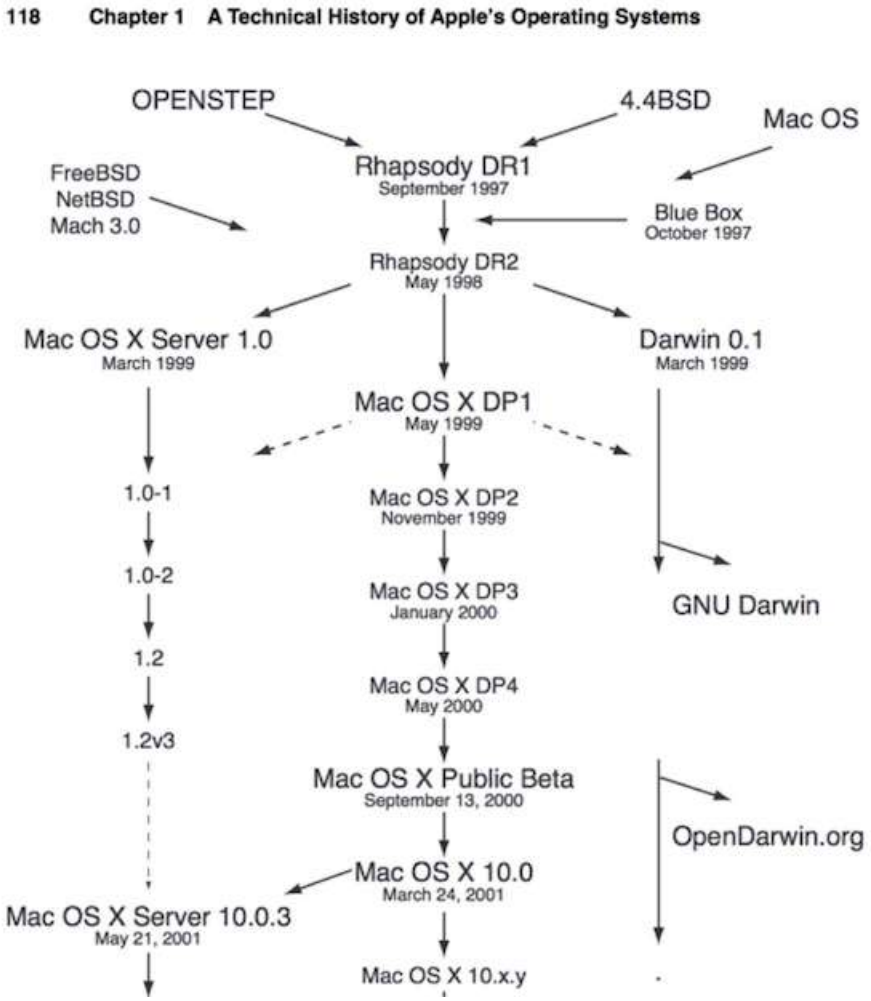
[3] https://www.apple.com/osx/what-is/security/

4. ENTORNO DE APLICACIÓN DE ESTA GUÍA

13. El diseño y evolución del sistema operativo OS X, en sus primeras versiones denominado Mac OS X, tiene sus orígenes en otros sistemas operativos creados anteriormente por Apple. OS X se estableció finalmente como la evolución de Raphsody (un sistema operativo que nunca fue público), y que constituía a su vez una evolución de la última versión de Mac OS Classic, Mac OS 9 (el sistema operativo de los equipos Macintosh), y que también integraba componentes de Openstep y BSD, Berkley Software Distribution (en sus diferentes variantes: FreeBSD, NetBSD, y OpenBSD) [Ref.- 1]..

14. Este apartado proporciona una visión general de OS X, su historia y evolución, y sus principales particularidades y características

15. La siguiente imagen resume la evolución de los últimos sistemas operativos justo antes de la publicación de la primera versión de (Mac) OS X 10.0 en marzo de 2001 [Ref.- 2]:



16. Adicionalmente, OS X tiene una notable influencia del sistema operativo NeXTSTEP, creado por NeXT y del que ha heredado componentes principales como el microkernel Mach, el lenguaje de programación Objetive-C, el conjunto de librerías o APIs (*Application Programming Interface*) Cocoa, el entorno de desarrollo Xcode o el uso de Bundles (descritos posteriormente) [Ref.- 3].

17. OS X es el nombre empleado para referirse al sistema operativo en su conjunto (incluyendo todos sus componentes), mientras que Darwin constituye el núcleo del sistema operativo, de código abierto[4] y basado en Unix. Darwin está compuesto a su vez del kernel XNU (acrónimo de "X is Not Unix"), basado en Mach 3.0 y FreeBSD 5, y del entorno de ejecución [Ref.- 2] [Ref.- 3].

18. En la actualidad, el kernel de OS X es de 64 bits (pudiendo gestionar equipos con hasta 128 GB de RAM [Ref.- 87]) y permite la ejecución de aplicaciones tanto de 32 como de 64 bits.

19. El kernel XNU está formado por el módulo o núcleo principal y por las extensiones del kernel, que pueden ser cargadas dinámicamente bajo demanda por el demonio kextd ("/usr/libexec/kextd"), y que están disponibles bajo "/System/Library/Extensions" (y sus cachés asociadas) y pueden ser visualizadas con el comando "kextstat":

```
$ kextstat

Index Refs Address            Size       Wired      Name (Version) <Linked Against>
    1  100 0xffffff7f80a3e000 0x8c50     0x8c50     com.apple.kpi.bsd (14.0.0)
    2    7 0xffffff7f80e00000 0x28c0     0x28c0     com.apple.kpi.dsep (14.0.0)
    3  119 0xffffff7f80a03000 0x20500    0x20500    com.apple.kpi.iokit (14.0.0)
    4  127 0xffffff7f80a24000 0xbf50     0xbf50     com.apple.kpi.libkern (14.0.0)
    5  113 0xffffff7f80a00000 0x2d50     0x2d50     com.apple.kpi.mach (14.0.0)
…
```

Nota: la versión 10.10.0 de OS X hace uso de la versión 14.0.0 para las extensiones de kernel, mientras que por ejemplo la versión 10.10.5 de OS X refleja la versión 14.5.0 en las extensiones de kernel.

20. La relación entre las versiones de (Mac) OS X y Darwin, desde la versión OS X 10.1 inclusive, se representa mediante la siguiente fórmula. Así, por ejemplo, OS X Mountain Lion (10.8.0) hace uso de Darwin 12.0:

    Versión OS X ==10.x.y → Versión Darwin = (4+x).y

21. La versión de aplicación de la presente guía, OS X 10.10.x (Yosemite) hace por tanto uso de la versión 14.x.0 de Darwin.

22. Adicionalmente, OS X dispone de I/O Kit, un entorno (o framework) modular para el desarrollo de drivers para dispositivos hardware y sus componentes software asociados, que emplea un modelo orientado a objetos y está basado en C++.

23. El registro de I/O Kit puede ser visualizado con el comando "ioreg":

```
$ ioreg

+-o Root  <class IORegistryEntry, id 0x100000100, retain 9>
  +-o MacBookPro11,1  <class IOPlatformExpertDevice, id 0x100000112, ...>
    +-o AppleACPIPlatformExpert  <class AppleACPIPlatformExpert, id 0x100000113, ...>
    | +-o IOPMrootDomain  <class IOPMrootDomain, id 0x100000116, ...>
    | | +-o IORootParent  <class IORootParent, id 0x100000117, ...>
…
```

[4] https://superuser.com/questions/19492/is-mac-os-x-open-source

24. El sistema de ficheros de OS X, basado en HFS+ (Hierarchical File System Plus), dispone de cuatro dominios diferentes [Ref.- 2]:

    - Dominio de usuario: Contiene recursos para cada usuario, y está asociado al directorio principal o *home* de Unix del usuario, disponible bajo "/Users".
    - Dominio local: Contiene recursos del sistema disponibles para todos los usuarios, ubicado bajo "/Applications", y su modificación requiere permisos de administrador.
    - Dominio de red: Contiene recursos de la red local disponibles para todos los usuarios, como por ejemplo documentos o aplicaciones, ubicado bajo "/Network" (vacío por defecto en versiones recientes de OS X).
    - Dominio de sistema: Contiene recursos del sistema propios de OS X, como por ejemplo librerías, scripts, ficheros de configuración, etc, disponible bajo "/System". Gran parte del sistema operativo reside bajo "/System/Library".

25. El formato de los ficheros binarios empleados por OS X es Mach-O, Mach Object File Format. Los ficheros Mach-O disponen de una cabecera al comienzo del archivo que define sus propiedades, características y diferentes segmentos y secciones.

26. Los binarios fat (o binarios en formato Apple Universal Binary) permiten disponer de un único archivo que contiene múltiples copias de un mismo ejecutable Mach-O, por ejemplo, compiladas para diferentes arquitecturas, como PowerPC, Intel, o incluso 32 (x86) y 64 (x86_64) bits.

27. OS X hace uso de Bundles, una colección de recursos relacionados entre sí y empaquetados dentro de una jerarquía de directorios estructurada. Por ejemplo, las aplicaciones se distribuyen en OS X como Bundles (con la extensión ".app"), habitualmente auto contenidos, que incluyen todos los componentes de la aplicación, tales como el ejecutable, las librerías, scripts, plug-ins, imágenes, documentos, ficheros de configuración, etc.

28. Este modelo facilita la instalación, eliminación y gestión de software y aplicaciones, ya que, normalmente, es suficiente con copiar, borrar o mover el directorio ".app".

29. La aplicación encargada de la gestión de ficheros en OS X, Finder, trata los Bundles como objetos atómicos, aunque es posible inspeccionar sus contenidos a través de la opción "Mostrar contenido del paquete" ("Show Package Contents" en inglés) disponible al seleccionar el Bundle con el botón derecho[5] desde Finder.

Nota: por defecto OS X requiere hacer uso de una pulsación firme (presionando) con un dedo en el *trackpad* (en los portátiles de Apple) para indicar la realización de una pulsación del botón izquierdo del ratón, así como hacer uso de una pulsación firme con dos dedos para indicar la realización de una pulsación del botón derecho del ratón.

Se recomienda, por comodidad, modificar el funcionamiento del botón izquierdo y derecho desde "Preferencias del Sistema - Trackpad", activando que la pulsación ligera con un dedo o dos dedos sea equivalente a la pulsación firme, mediante la opción "Señalar y hacer clic: Pulsar para hacer clic (Pulsar con 1 dedo)".

[5] Pulsar el botón derecho es equivalente en OS X a utilizar la tecla de control (Ctrl) al pulsar el botón izquierdo.

30. Los Bundles también son empleados en OS X para distribuir Frameworks (con la extensión ".framework"), es decir, (una o más) librerías dinámicas compartidas (dynamic shared libraries) empaquetadas con todos sus recursos asociados, tales como ficheros de cabeceras, documentación, APIs, ficheros de definición de sus interfaces, strings para diferentes idiomas, imágenes, etc, y que proporcionan la funcionalidad del sistema operativo a nivel de usuario.

31. OS X dispone de numerosos Frameworks que proporcionan funcionalidad asociada al propio sistema operativo (servicios core), a la gestión de aplicaciones, del interfaz gráfico de usuario (GUI) y las capacidades multimedia, del acceso a hardware y otros periféricos, de las tareas de automatización y scripting, y de los mecanismos de seguridad, entre otros.

32. Los Frameworks estándar de OS X pueden estar disponibles bajo los siguientes directorios y son buscados en el siguiente orden[6]: "~/Library/Frameworks" (inexistente por defecto), "/Library/Frameworks", "/Network/Library/Frameworks" (inexistente por defecto) y "/System/Library/Frameworks".

33. Adicionalmente Apple hace uso de otro conjunto de Frameworks privados, cuyas APIs no son publicadas, y que están disponibles bajo "/System/Library/PrivateFrameworks".

34. La información y detalles de un Framework está disponible en el fichero "Info.plist" del subdirectorio "Resources" dentro de su Bundle.

35. OS X hace un uso extensivo de ficheros PLIST, Property Lists. Estos ficheros permiten almacenar datos de manera estructurada, y los tipos de datos que emplean tienen una representación directa en el Framework Core Foundation (CF), como por ejemplo: CFArray, CFBoolean, CFData, CFDate, CFDictionary, CFNumber, o CFString.

36. Un fichero PLIST puede almacenar la información en formato binario, directamente serializado de su representación en memoria, o en formato ASCII, empleando el formato XML.

37. Los ficheros PLIST emplean normalmente la extensión ".plist" y son empleados tanto por el sistema operativo como por las aplicaciones para almacenar detalles de la configuración, preferencias del usuario, datos relacionados con la propia aplicación y su utilización, etc.

38. El directorio "~/Library/Preferences" de cada usuario almacena numerosos ficheros PLIST con la configuración o preferencias del usuario para múltiples aplicaciones, empleando una nomenclatura basada en un formato de resolución de DNS inversa. Por ejemplo, las preferencias del navegador web Safari se almacenan bajo "com.apple.Safari.plist" en dicho directorio.

39. Los ficheros PLIST en formato binario pueden ser manejados mediante la herramienta "plutil" o a través del entorno de desarrollo Xcode. Los ficheros PLIST en formato XML pueden ser gestionados con cualquier editor de texto.

[6] De manera similar, la búsqueda de librerías compartidas se lleva a cabo bajo "~/lib", /usr/local/lib" (ambos inexistentes por defecto) y "/usr/lib".

40. El siguiente listado detalla las versiones del sistema operativo (Mac) OS X, incluyendo su nombre en clave de proyecto y su fecha de publicación (en inglés)[7]:

    - 10.0: Cheetah (March 24, 2001)
    - 10.1: Puma (September 25, 2001)
    - 10.2: Jaguar (August 24, 2002)
    - 10.3: Panther (October 24, 2003) + Safari
    - 10.4: Tiger (April 29, 2005)
    - 10.5: Leopard (October 26, 2007)
    - 10.6: Snow Leopard (August 28, 2009) + soporte de 64-bits
    - 10.7: Lion (July 20, 2011)
    - 10.8: Mountain Lion (July 25, 2012)
    - 10.9: Mavericks (October 22, 2013)
    - 10.10: Yosemite (October 16, 2014)

41. El sistema operativo fue denominado Mac OS X desde la versión 10.0 hasta la versión 10.7, pasando a denominarse OS X (sin emplear el término Mac) desde la versión 10.8 en adelante.

42. Desde la versión 10.0 hasta la versión 10.3, Mac OS X sólo estaba disponible para plataforma PowerPC, pasando por una transición en las versiones 10.4 y 10.5, al estar disponible simultáneamente tanto para PowerPC como para plataforma Intel, y estableciéndose finalmente sólo para la plataforma Intel desde la versión 10.7 en adelante.

43. Por tanto, las últimas versiones de OS X disponen de soporte para los equipos hardware de Apple, y en concreto, para los equipos de sobremesa Mac mini, iMac y Mac Pro, los servidores Mac mini Server y Mac Pro Server, y los equipos portátiles MacBook Air, MacBook y MacBook Pro.

44. OS X está disponible tanto en la versión estándar, objeto de la presente guía, como en la versión servidor, denominada OS X Server[8]. La versión servidor de OS X es similar a la versión estándar, diferenciándose principalmente en los componentes software o servicios proporcionados por defecto (o disponibles oficialmente).

45. OS X destaca por integrar la potencia asociada a la línea de comandos de sistemas Unix junto a un interfaz gráfico de usuario (GUI, Graphical User Interface) que simplifica y mejora su usabilidad.

46. La presente guía ha sido diseñada con la misma filosofía, combinando la aplicación de configuraciones y ajustes de seguridad a través del interfaz gráfico de usuario cuando es posible, con tareas y detalles a más bajo nivel empleando la línea de comandos de OS X a través de un terminal.

[7] http://en.wikipedia.org/wiki/OS_X#Versions

[8] http://www.apple.com/es/osx/server/specs/ y http://www.apple.com/es/osx/server/features/.

47. Los contenidos de esta guía aplican a equipos Apple basados en OS X y configurados con el idioma principal (o Primary) en español: "Español" (o "Spanish"). El idioma puede ser seleccionado desde "Preferencias del Sistema - Idioma y región", a través de la sección "Idiomas preferidos".

Nota: en la versión en inglés de OS X, por si fuera necesario cambiar el idioma desde esa versión, la configuración del idioma está disponible bajo "System Preferences - Language & Region" y, en concreto, a través de la sección "Preferred languages".

48. Si se modifica el idioma de OS X es necesario reiniciar el equipo para que los cambios surtan efecto.

Nota: la información general del equipo está accesible a través del icono de la manzana (□) disponible en la barra principal de menú, bajo la opción "Acerca de este Mac" (o "*About This Mac*"). En concreto, la información de la versión del sistema operativo se encuentra bajo la sección "Visión general" y el texto "Versión", por ejemplo, 10.10.

49. La guía ha sido probada y verificada (inicialmente) con la versión 10.10.0[9] del sistema operativo OS X de Apple en un equipo MacBook Pro, basado en la plataforma y procesador Intel, actualizándose posteriormente a la última versión disponible de OS X Yosemite (ej. 10.10.5[10] [Ref.- 85]) en el momento de elaboración de la presente guía.

50. A la hora de analizar desde el punto de vista de seguridad una nueva versión de OS X es siempre interesante evaluar la nueva funcionalidad existente a través de los nuevos binarios que han sido introducidos a nivel de sistema operativo [Ref.- 16].

51. Los detalles de la versión del sistema operativo, arquitectura y versión de Darwin están disponibles desde un terminal mediante el comando "uname -a" (donde "portatil" es el nombre del equipo):

```
OS X 10.10:
$ uname -a
Darwin portatil.local 14.0.0 Darwin Kernel Version 14.0.0: Fri Sep 19
00:26:44 PDT 2014; root:xnu-2782.1.97~2/RELEASE_X86_64 x86_64

OS X 10.10.5:
$ uname -a
Darwin portatil.local 14.5.0 Darwin Kernel Version 14.5.0: Wed Jul 29
02:26:53 PDT 2015; root:xnu-2782.40.9~1/RELEASE_X86_64 x86_64
```

52. El hardware sobre el que se ha verificado la presente guía tiene las siguientes características:

- Equipo MacBook Pro de 13,3 pulgadas fabricado por Apple [Ref.- 2]:
  - Versión de OS X: 10.10.0 y 10.10.5 (tras actualizaciones)
  - Modelo: MacBookPro11,1 (A1502)

[9] Publicada oficialmente el 16 de octubre de 2014.

[10] Publicada oficialmente el 13 de agosto de 2015 (OS X 10.10.4 fue publicada oficialmente el 30 de junio de 2015).

- Procesador: Intel Core i5 (2,8 GHz)
- Memoria RAM: 8GB
- Disco duro: SSD 500GB
- Versión de la ROM de arranque: MBP111.0138.B11
- Pantalla: 13,3 pulgadas Retina (2560x1600) - Intel Iris 1536 MB
- Interfaz Wi-Fi: Airport Extreme (Broadcom BCM43xx 1.0) 802.11 a/b/g/n/ac
- Interfaz Bluetooth: Broadcom

Nota: Mactracker es una aplicación disponible tanto para OS X como para iOS que proporciona información detallada sobre el hardware de cualquier ordenador Mac y dispositivo fabricado por Apple, incluyendo los detalles de las versiones de sistema operativo soportadas: http://mactracker.ca.

53. La información del hardware del equipo puede obtenerse mediante el icono de la manzana (□) disponible en la barra de menús, bajo la opción "Acerca de este Mac", y en concreto, desde la sección "Visión general" y el botón "Informe del sistema…" y sus diferentes secciones:

Nota: las imágenes incluidas en la presente guía corresponden principalmente a las versiones 10.10.0, 10.10.4 y 10.10.5 de OS X, clarificación necesaria dado que potencialmente algunas imágenes pueden variar entre diferentes versiones o subversiones de OS X futuras.

Nota: las pantallas de Finder disponibles a lo largo de la presente guía pueden mostrar personalizaciones realizadas específicamente respecto a su configuración por defecto, por ejemplo, mostrando por defecto el directorio raíz del usuario ("Finder - Preferencias… - General - Las nuevas ventanas del Finder muestran: <usuario>"), o la carpeta de usuario o el disco duro del equipo en la barra lateral ("Finder - Preferencias… - Barra lateral - Mostrar estos ítems en la barra lateral: Favoritos - <usuario>" y "Dispositivos - <hostname>").

54. El manual con la información esencial del hardware y su utilización asociada a los equipos de Apple está disponible para los últimos modelos en la página oficial de manuales [Ref.- 15], como por ejemplo el manual "MacBook Pro (Retina, 13-inch, Early 2015) - Essentials" asociado a la última versión del modelo MacBook Pro de 13 pulgadas empleado para la elaboración de la presente guía[11].

55. Se recomienda siempre recabar e inventariar la información de versiones, tanto hardware como software, de los equipos a proteger, con el objetivo de disponer de toda la información necesaria a la hora de tomar decisiones relativas a la aplicación de nuevas actualizaciones de seguridad.

56. La presente guía ha sido desarrollada teniendo en cuenta principalmente los aspectos de seguridad y capacidades de protección de OS X. Es posible que alguna o algunas de las funcionalidades esperadas hayan sido desactivadas y, por tanto, sea necesario aplicar acciones adicionales para habilitar los servicios o características deseadas.

[11] https://manuals.info.apple.com/MANUALS/1000/MA1695/en_US/macbook_pro_retina_13_inch_early_2015_essentials.pdf

57. Antes de aplicar esta guía en un entorno de producción debe confirmarse su adecuación a la organización objetivo, siendo probada previamente en un entorno aislado y controlado donde se puedan realizar las pruebas necesarias y aplicar cambios en la configuración para que se ajusten a los criterios específicos de cada organización.

58. El espíritu de esta guía no está dirigido a reemplazar políticas consolidadas y probadas de las organizaciones, sino servir como línea base de seguridad que deberá ser adaptada a las necesidades propias de cada organización.

Nota: el alcance de la presente guía no contempla la realización de un análisis de seguridad detallado y exahustivo de los protocolos de comunicaciones basados en HTTPS (o SSL/TLS) y empleados entre los equipos con OS X y los diferentes servicios de Apple o de terceros.

5. CONFIGURACIÓN DE SEGURIDAD DE OS X

59. Existen numerosos aspectos y funcionalidades generales de OS X que pueden ser configuradas desde el punto de vista de seguridad, restringiendo su uso y protegiendo el equipo o los datos del usuario frente a potenciales ataques.

5.1 PROCESO DE INSTALACIÓN Y CONFIGURACIÓN INICIAL

60. Una vez el equipo ha sido desempaquetado por primera vez, arrancará en su estado original de fábrica, por lo que será necesario completar el proceso de instalación y configuración inicial (detallado en el apartado "ANEXO A. Proceso de instalación y configuración inicial").

61. Este proceso de instalación y configuración inicial será utilizado como referencia para el resto de recomendaciones, referencias de valores por defecto y modificaciones de configuración reflejadas en la presente guía.

62. Una vez completado este proceso de instalación y configuración inicial, se recomienda en primer lugar crear una cuenta de usuario estándar (sin privilegios) (ver apartado "5.7.1. Creación de una cuenta de usuario estándar").

63. Posteriormente, y haciendo uso de esta cuenta de usuario, se sugiere aplicar el resto de recomendaciones de configuración detalladas en la presente guía:

5.2 NOMBRE DE EQUIPO

64. Por defecto, el nombre (o hostname) asignado al equipo por OS X es "MacBook-Pro-de-admin.local", donde "admin" es el nombre de la cuenta de usuario creada inicialmente durante el proceso de instalación y configuración de OS X.

65. Se recomienda modificar el nombre del equipo para que no desvele, ni contenga detalles, ni del tipo de equipo y sistema operativo empleado, ni de su propietario.

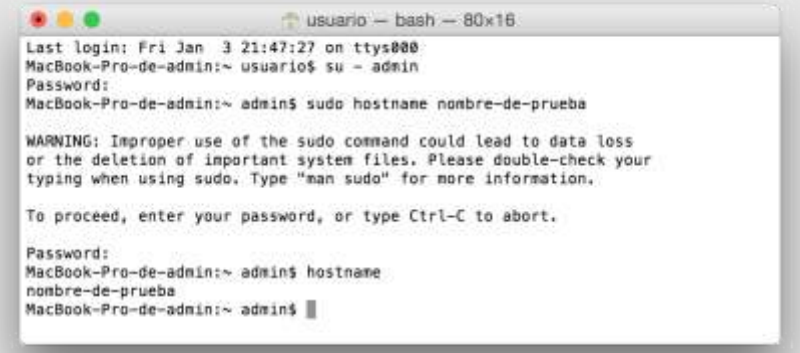
66. Mediante "Preferencias del Sistema - Compartir", y la opción "Nombre del ordenador" es posible modificar el nombre del equipo (por ejemplo, "portatil").

67. El nombre del equipo puede ser visualizado desde un terminal mediante el comando "hostname", y también puede ser modificado permanentemente desde un terminal mediante el siguiente comando (con ciertas implicaciones detalladas posteriormente):

```
$ hostname
MacBook-Pro-de-admin.local

$ scutil --set HostName portatil
$ hostname
portatil
```

Nota: si la invocación del comando "scutil" se realiza sin hacer uso de "sudo", OS X detectará que se está intentando modificar la configuración del sistema y solicitará al usuario a través del interfaz gráfico las credenciales de un usuario administrador (por ejemplo, "admin") a través de una ventana de diálogo. Alternativamente se puede hacer uso de "sudo" desde un terminal asociado a un usuario administrador siguiendo las indicaciones detalladas en la siguiente nota.

Nota: la ejecución de comandos desde un terminal con privilegios mediante "sudo", haciendo uso de un usuario estándar **no administrador**, por ejemplo "usuario", requiere de varios pasos. El usuario estándar no dispone de acceso a "sudo", por lo que en primer lugar es necesario abrir una sesión en el terminal como un usuario administrador, por ejemplo "admin", mediante el comando "su - admin":



Desde esa sesión de terminal asociada al usuario administrador sí es posible llevar a cabo la ejecución de comandos privilegiados mediante "sudo" tras introducir la contraseña del propio usuario "admin".

A lo largo de la presente guía se muestra la ejecución de diferentes comandos privilegiados desde un terminal mediante la utilización de "sudo". Dado que se recomienda siempre hacer uso de un usuario estándar, para su ejecución será necesario llevar a cabo este procedimiento.

Por defecto, el comando "sudo" está disponible sin ser necesario el proceso de autentificación durante 5 minutos tras introducir las credenciales de administrador.

68. El comando "hostname" sólo permite cambiar el nombre del equipo temporalmente desde un terminal, por lo que volverá a emplearse el nombre previo tras reiniciarse el equipo:

```
$ hostname
MacBook-Pro-de-admin.local

$ sudo hostname portatil
$ hostname
portatil
```

69. Al hacer uso del comando "scutil" para cambiar el nombre del equipo (mostrado anteriormente), este cambia internamente, pero no en la sección "Preferencias del Sistema - Compartir", y la opción "Nombre del ordenador".

70. El motivo es que OS X dispone de tres nombres asociados al equipo, tal como detalla la ayuda de "scutil" ("man scutil"):

    - ComputerName: El nombre amigable del equipo.
    - LocalHostName: El nombre local del equipo para Bonjour.
    - HostName: El nombre Unix asociado a "hostname" y "gethostname()".

71. Por tanto, si se desea cambiar el nombre del equipo desde un terminal, es también necesario cambiar el nombre asociado a las otras funcionalidades para disponer del mismo nombre de equipo en los diferentes escenarios descritos. El primer comando modifica el nombre visible desde la sección "Preferencias del Sistema - Compartir", y la opción "Nombre del ordenador":

```
$ scutil --set ComputerName portatil

$ scutil --set LocalHostName portatil
```

Nota: adicionalmente se recomienda limpiar la caché de DNS mediante "dscacheutil -flushcache".

72. La modificación del nombre desde la sección "Preferencias del Sistema - Compartir", y la opción "Nombre del ordenador", modifica directamente el valor de las dos representaciones amigables del nombre del equipo, "ComputerName" y "LocalHostName", pero no la asociada a "hostname", incluso tras reiniciar el equipo.

73. Se recomienda por tanto modificar el nombre del equipo desde el terminal empleando las tres versiones del comando "scutil" descritas.

5.2.1 ENTRADA DE DATOS DESDE EL TERMINAL

74. El terminal de OS X es utilizado habitualmente para tareas de más bajo nivel, y normalmente críticas, con permisos de administrador o root mediante "sudo".

75. Con el objetivo de evitar que otras aplicaciones tengan acceso a la información y comandos tecleados en el terminal, es posible configurar la opción "Entrada de teclado segura", disponible desde el menú "Terminal" de la propia aplicación terminal.

76. Es posible verificar que este parámetro de configuración está activo desde un terminal:

```
$ defaults read -app Terminal SecureKeyboardEntry
```

5.3 ACTUALIZACIONES

5.3.1 ACTUALIZACIONES DE SISTEMA OPERATIVO: OS X

77. Mediante el icono de la manzana (□) disponible en la barra de menús, a través de la opción "Acerca de este Mac", es posible acceder a las capacidades de verificación de actualizaciones de sistema operativo de OS X (botón "Actualización de software…" de la sección "Visión general"):

78. Este acceso ejecuta la aplicación App Store, que desde su pestaña "Actualizaciones", permite verificar tanto la existencia de actualizaciones de sistema operativo como de las aplicaciones instaladas desde la App Store (ver imagen de la App Store a continuación).

79. Inicialmente es posible que OS X Yosemite detecte la disponibilidad de nuevas versiones para algunas de las aplicaciones oficiales de Apple, como GarageBand, iMovie, Keynote, Numbers y Pages, así como nuevas actualizaciones de sistema operativo.

80. Desde los ajustes de configuración de la aplicación App Store, disponibles desde "Preferencias del Sistema - App Store", es posible definir si se realizarán comprobaciones automáticas en busca de actualizaciones periódicamente y si las actualizaciones serán descargadas automáticamente en segundo plano (background) y sin la intervención del usuario. El usuario será notificado de la existencia de actualizaciones cuando estén listas para ser instaladas. Adicionalmente, un símbolo distintivo en el Dock mostrará el número de actualizaciones pendientes. Ambas opciones están habilitadas por defecto:

81. Por otro lado, es posible definir independientemente si las actualizaciones de aplicaciones (o apps), de sistema operativo (OS X), y de archivos de datos del sistema y actualizaciones de seguridad, serán instaladas automáticamente. En el caso de la instalación de aplicaciones y de OS X es necesario haber habilitado las dos opciones previas para realizar las comprobaciones y descargas de manera automática:

82. Por defecto, OS X comprueba la existencia de actualizaciones periódicamente. Aunque la documentación existente es contradictoria, indicando en algunos casos que se comprueba diariamente, los detalles extraídos del fichero de configuración del servicio de actualizaciones de software parecen indicar que se comprueba cada 6 horas (21.600 segundos):

```
$  grep Repeating -A3
/System/Library/LaunchDaemons/com.apple.softwareupdated.plist
    <key>Repeating</key>
    <true/>
    <key>Interval</key>
    <integer>21600</integer>
```

83. Esta frecuencia podría ser verificada junto a otros parámetros asociados y modificada (por ejemplo, para comprobar la disponibilidad de actualizaciones cada 3 días, opción desaconsejada desde el punto de vista de seguridad, mediante los siguientes comandos:

```
$ defaults read /Library/Preferences/com.apple.SoftwareUpdate.plist

$ sudo defaults write /Library/Preferences/com.apple.SoftwareUpdate
ScheduleFrequency 3
```

Nota: la utilización mostrada del comando "defaults" permite de manera estándar en OS X obtener (read) el valor de los parámetros de configuración disponibles en los ficheros PLIST, así como modificar (write, con privilegios de administrador) el valor de dichos parámetros.

84. Adicionalmente, es posible gestionar desde un terminal el catálogo con las actualizaciones disponibles, así como su descarga e instalación, a través de la utilidad "softwareupdate".

85. Por ejemplo, los siguiente comandos desactivan y activan las capacidades de comprobación de actualizaciones automáticas de OS X desde un terminal:

```
$ sudo softwareupdate --schedule off

$ sudo softwareupdate --schedule on
```

86. Por defecto no se instalarán automáticamente actualizaciones de aplicaciones o de OS X, pero sí se instalarán archivos de datos del sistema y actualizaciones de seguridad.

87. Se recomienda, al menos, buscar actualizaciones automáticamente e instalar archivos de datos del sistema y actualizaciones de seguridad. La recomendación sobre la gestión de las descargas correspondientes a las actualizaciones es muy dependiente del entorno y uso de OS X (tipo de red de comunicaciones empleada, ancho de banda, etc).

88. Mediante la herramienta "defaults", desde un terminal, es posible verificar si las capacidades automáticas de comprobación de actualizaciones están activas o no, así como activarlas en caso necesario [Ref.- 86]:

```
$ defaults read /Library/Preferences/com.apple.SoftwareUpdate
AutomaticCheckEnabled

$ sudo defaults write /Library/Preferences/com.apple.SoftwareUpdate
AutomaticCheckEnabled -int 1
```

Nota: este mecanismo de verificación y modificación de propiedades y ajustes de configuración de OS X mediane "defaults" es estándar y puede ser aplicado a numerosos aspectos de la personalización de OS X (aunque no se detalle de manera exhaustiva a lo largo de la presente guía para cada ajuste disponible).

89. Los ficheros correspondientes a las actualizaciones de OS X son almacenados temporalmente bajo "/Library/Updates/" y se eliminan al reiniciar el equipo para completar el proceso de actualización[12].

90. Asimismo, existe la posibilidad de descargar automáticamente aplicaciones obtenidas de la App Store desde otros equipos con OS X (Macs) con la misma cuenta de usuario o Apple ID.

91. En cualquier momento, a través del botón "Buscar ahora" disponible en los ajustes de la App Store, es posible verificar la existencia de nuevas actualizaciones (de nuevo a través de la aplicación App Store). En el caso de existir actualizaciones pendientes de aplicar, el botón mostrará el texto "Mostrar actualizaciones":

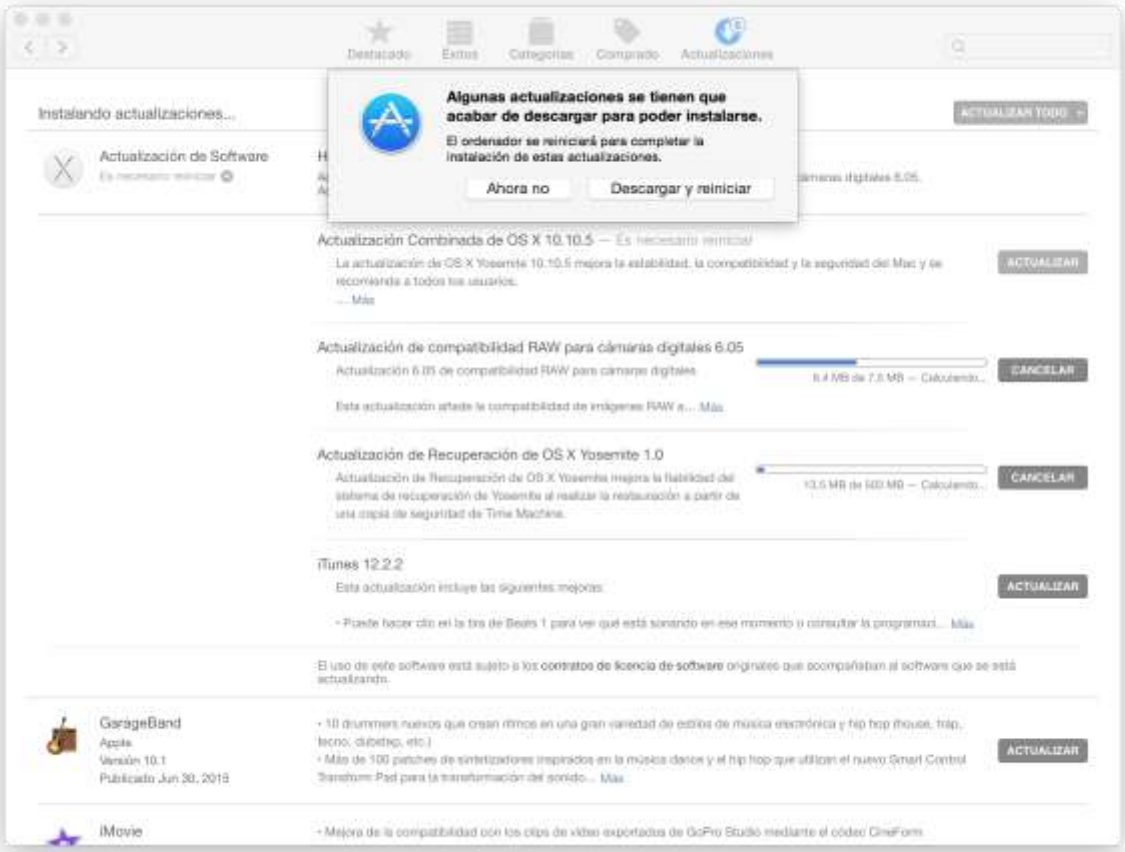
92. Desde la pestaña "Actualizaciones" de App Store es posible identificar las actualizaciones de software disponibles, que indican si es necesario reiniciar el equipo para su aplicación, así como actualizar todas ellas simultáneamente (botón "Actualizar Todo") o individualmente (botones "Actualizar"):

[12] En algunos casos, complementado por el uso de la caché disponible bajo "~/Library/Caches/com.apple.SoftwareUpdate".

Nota: durante la fase final de publicación de la presente guía se liberó la versión 10.10.5 de OS X (13 de agosto de 2015)[13], especialmente relevante desde el punto de vista de seguridad debido a las numerosas vulnerabilidades solucionadas en la misma [Ref.- 85].

93. Para proceder a la instalación de actualizaciones de sistema operativo no es necesario proporcionar un usuario de App Store (o Apple ID) válido, junto a su contraseña, pero en ocasiones es necesario aceptar los términos de licencia del software a instalar, y normalmente es necesario reiniciar el equipo:

[13] https://support.apple.com/kb/DL1832



94. La utilidad "softwareupdate" permite verificar el listado de actualizaciones disponibles desde un terminal:

```
$ sudo softwareupdate --list
```

95. El recurso oficial con las actualizaciones de seguridad de Apple (HT1222) contiene referencias detalladas de todas las actualizaciones de sistema operativo publicadas por Apple para OS X. Se recomienda consultar su versión en inglés (EN), ya que es habitual que las últimas actualizaciones no aparezcan publicadas en la versión en español hasta días o semanas después de estar disponibles [Ref.- 6].

96. Dicho recurso proporciona enlaces a los recursos que describen todos los detalles sobre los contenidos y las actualizaciones de seguridad oficiales para las diferentes versiones de OS X, como por ejemplo, la versión inicial de OS X Yosemite 10.10[14].

97. La comprobación de actualizaciones se realiza mediante HTTPS (desde OS X Mountain Lion, en la actualidad empleando TLS v1.2) hacia el servidor "swscan.apple.com" (que en el momento del análisis es redirigido y gestionado por Akamai). OS X, y en concreto tanto la aplicación App Store como la utilidad "softwareupdate", realizan una verificación

[14] https://support.apple.com/en-gb/HT203112

estricta del certificado digital obtenido en la conexión HTTPS, empleando certificate pinning, y no aceptando cualquier otro certificado.

Nota: es posible restablecer la caché DNS en OS X desde un terminal mediante el siguiente comando[15]: `$ sudo killall -HUP mDNSResponder`

98. Es posible que OS X haga uso de otros servidores durante el proceso de actualización de software [Ref.- 14], como por ejemplo "swcdn.apple.com", "swdownload.apple.com" o "swquery.apple.com".

99. La URL del catálogo empleado por OS X para comprobar las actualizaciones de sistema operativo y aplicaciones es "https://swscan.apple.com/content/catalogs/others/index-10.10-10.9-mountainlion-lion-snowleopard-leopard.merged-1.sucatalog.gz".

100. Las actualizaciones del sistema operativo OS X[16] pueden ser también descargadas manualmente, como actualizaciones individuales (individual update) que se aplican sobre la subversión previa (por ejemplo, desde OS X Yosemite 10.10.3 a 10.10.4[17]) o como actualizaciones combinadas (combo update) que actualizan a una versión determinada desde la subversión original o inicial de esa versión de OS X (por ejemplo, desde OS X Yosemite 10.10 a 10.10.4[18)].

101. En el caso de descargar manualmente las actualizaciones de OS X, individuales o combinadas, es posible verificar también manualmente su autenticidad, al estar firmadas por Apple.

102. Para ello es necesario verificar la huella digital (*hash* o *fingerprint*) SHA1 del certificado digital con el que el paquete de actualización (".pkg") ha sido firmado, debiendo pertenecer a la autoridad certificadora "Apple Software Update Certificate Authority", y coincidir con las huellas digitales de los certificados oficiales de Apple19 (actuales y/o previos).

5.3.2 ACTUALIZACIONES DE FIRMWARE

103. La mayoría de las actualizaciones de firmware se instalan automáticamente cuando se actualiza el sistema operativo OS X (ver apartado previo). Sin embargo, algunas actualizaciones de firmware también están disponibles para su descarga independientemente, pudiendo ser instaladas manualmente.

104. Las actualizaciones de firmware para componentes hardware específicos de los equipos de Apple, como por ejemplo los MacBook, MacBook Air o MacBook Pro[20], están disponibles para su descarga desde la página oficial de descargas de Apple [Ref.- 7].

[15] https://support.apple.com/es-es/HT202516

[16] https://en.wikipedia.org/wiki/OS_X_Yosemite#Releases

[17] https://support.apple.com/kb/DL1819

[18] https://support.apple.com/kb/DL1820

[19] https://support.apple.com/en-us/HT202369

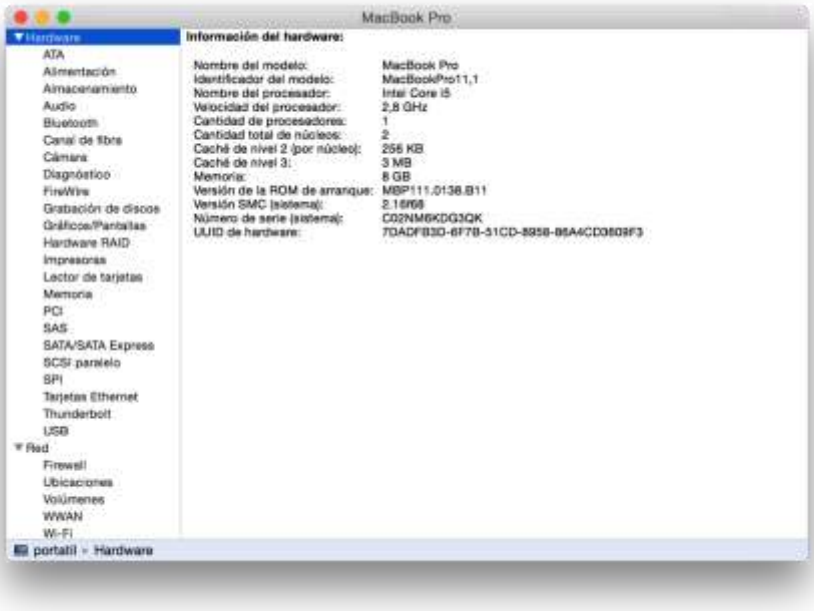
[20] https://support.apple.com/downloads/macnotebooks

105. Por ejemplo, se dispone de una actualización de software para el sistema de almacenamiento Flash (v1.0) de los MacBook Pro Retina de 15 pulgadas comercializados a mediados de 2015[21].

106. Los componentes hardware que son habitualmente actualizados por Apple son el sistema de almacenamiento Flash (*Flash Storage*), el sistema, BIOS o ROM de arranque del equipo (EFI, *Extensible Firmware Interface*, existente en los equipos Mac con procesador o plataforma Intel) y el controlador de gestión del sistema o SMC (*System Management Controller*) [Ref.- 11].

107. Las actualizaciones de firmware para equipos Mac con procesador Intel requieren un esquema o tabla de particiones GUID (GPT, *GUID Partition Table*) en el dispositivo de almacenamiento[22], esquema configurado por defecto de fábrica por Apple.

108. Mediante el icono de la manzana (□) disponible en la barra de menús, a través de la opción "Acerca de este Mac", y el botón "Informe del sistema…" de la sección "Visión general", es posible acceder a la información del identificador de modelo del equipo (por ejemplo, MacBookPro11,1) y a los detalles de la versión del SMC ("Versión SMC (sistema)") y del EFI ("Versión de la ROM de arranque"):



109. Se recomienda comprobar el número de versión del SMC y del EFI para el modelo de equipo empleado y verificar si existe una versión más actualizada en la página oficial de Apple [Ref.- 10]. En caso afirmativo, se recomienda llevar a cabo su descarga e instalación manualmente [Ref.- 13].

110. En realidad, la utilidad de actualización de firmware hace uso de la herramienta "bless" (disponible desde un terminal) y del fichero SCAP (*Secure Capsule*) descargado, que contiene el paquete de actualización de firmware, firmado mediante RSA 2.048 bits y un

[21] https://support.apple.com/kb/DL1830?locale=en_US

[22] https://support.apple.com/es-es/HT201723

hash SHA256[23]. "bless" copia el fichero SCAP a la partición de recuperación de EFI y establece la variable NVRAM "efi-apple-recovery" apuntando al fichero SCAP [Ref.- 32], para que en el siguiente reinicio del sistema se cargue el nuevo firmware.

111. Los siguientes comandos permiten verificar el valor de dicha variable y confirmar la existencia del fichero SCAP referenciado en la partición EFI[24]:

```
$ nvram efi-apple-recovery
efi-apple-recovery
       <array><dict><key>IOMatch</key><dict><key>IOProviderClass</key><string>IOM
edia</string><key>IOPropertyMatch</key><dict><key>UUID</key><string>01…89</string
></dict></dict><key>BLLastBSDName</key><string>disk0s1</string></dict><dict><key>
IOEFIDevicePathType</key><string>MediaFilePath</string><key>Path</key><string>\EF
I\APPLE\FIRMWARE\MBP112_0138_B15_LOCKED.scap</string></dict></array>%00

$ diskutil list
/dev/disk0
   #:       TYPE                    NAME       SIZE       IDENTIFIER
   0:       GUID_partition_scheme              *500.3 GB   disk0
   1:       EFI                     EFI        209.7 MB   disk0s1
...

$ mkdir /tmp/EFI
$ sudo mount -t msdos /dev/disk0s1 /tmp/EFI
$ ls -l /tmp/EFI/EFI/APPLE/FIRMWARE
...
-rwxrwxrwx  1 admin  staff  8520304 Aug 15 02:47 MBP112_0138_B15_LOCKED.scap
```

112. Por ejemplo, la actualización del EFI para los MacBook Pro identificada como "Mac EFI Security Update 2015-001" [Ref.- 12] resolvía una vulnerabilidad de seguridad que permitía a un potencial atacante (desde la zona de usuario y con permisos de root) deshabilitar el bloqueo del gestor de arranque y sobrescribir sin autorización el contenido del EFI (por ejemplo, para instalar un *rootkit* en el firmware, o *bootkit*) al resumir la ejecución desde el estado suspendido[25] [26]. Adicionalmente la actualización solucionaba la vulnerabilidad conocida como Rowhammer.

113. Esta actualización, según la documentación oficial de Apple, sólo aplica a OS X 10.8.5 (Mountain Lion) y 10.9.5 (Mavericks), no así a OS X Yosemite. La vulnerabilidad tampoco parece afectar a los nuevos modelos de MacBook (en sus diferentes variantes) de los años 2014 y 2015. El asistente comprueba antes de comenzar la instalación que la versión de OS X sea la correcta, 10.8.5 o 10.9.5.

114. Sin embargo, los detalles asociados a las vulnerabilidades de Thunderstrike 2 (ver apartado "5.4.9.7. ATAQUES FIRMWARE MEDIANTE EL PUERTO THUNDERBOLT (Y EL EFI)") parecen confirmar que también este tipo de vulnerabilidades afectan a OS X 10.10 Yosemite.

[23] https://www.lostinsecurity.com/blog/2015/08/22/ficheros-scap-de-firmware-de-apple/

[24] https://www.lostinsecurity.com/blog/2015/08/21/actualizaciones-de-firmware-usando-capsulas/

[25] https://reverse.put.as/2015/05/29/the-empire-strikes-back-apple-how-your-mac-firmware-security-is-completely-broken/

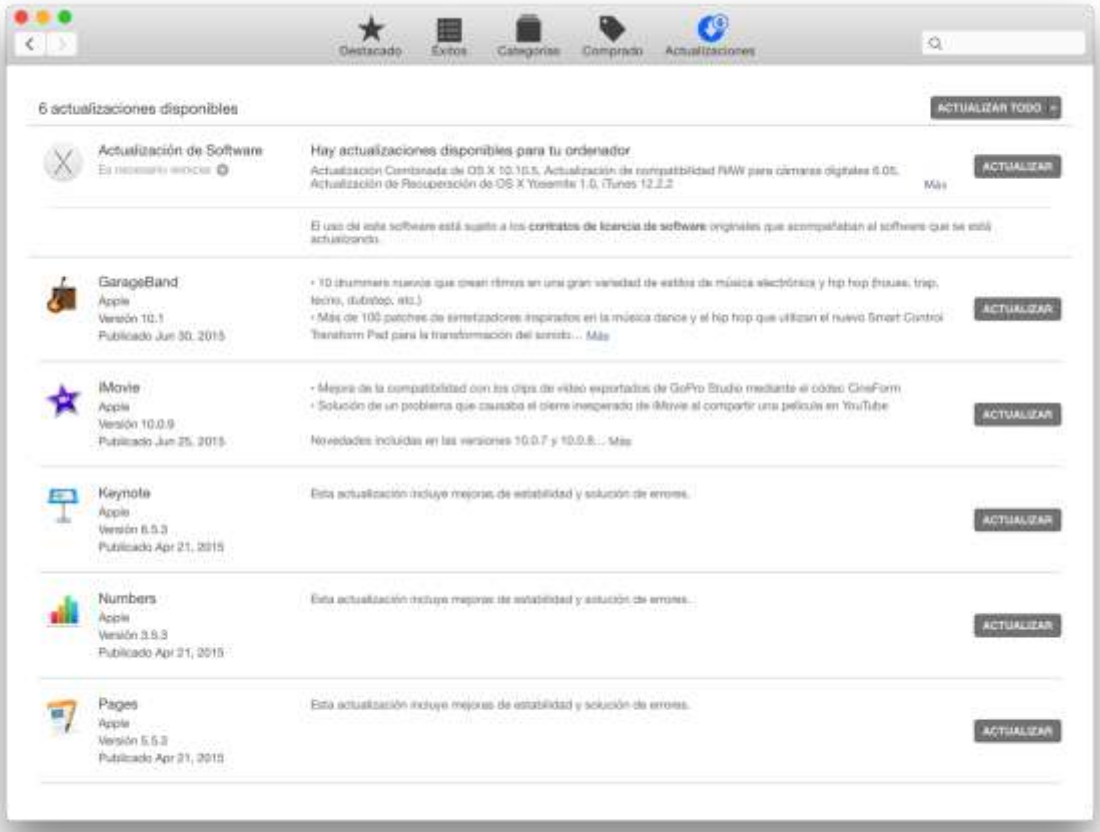
[26] OS X puede ser suspendido desde un terminal mediante el comando: sudo pmset sleepnow.

115. Las actualizaciones de firmware y software para otros periféricos y dispositivos hardware de Apple están disponibles para su descarga desde la página oficial asociada [Ref.- 9].

5.3.3 ACTUALIZACIONES DE APLICACIONES: APP STORE

116. Mediante el icono de la manzana (□) disponible en la barra de menús, a través de la opción "Acerca de este Mac", es posible acceder a las capacidades de verificación de actualizaciones de sistema operativo de OS X (botón "Actualización de software…" de la sección "Visión general"), tal como se ha descrito previamente.

117. Este acceso ejecuta la aplicación App Store, que desde su pestaña "Actualizaciones", permite verificar tanto la existencia de actualizaciones de sistema operativo como de las aplicaciones instaladas desde la App Store:



118. En el caso de las aplicaciones, se dispone de un registro con las actualizaciones instaladas durante los últimos 30 días, así como una lista de las actualizaciones de aplicaciones pendientes de instalar en la parte superior, que pueden ser aplicadas mediante el botón "Actualizar".

119. Para proceder a la instalación de aplicaciones de la App Store es necesario proporcionar un usuario de App Store (o Apple ID) válido, junto a su contraseña:

5.3.4 ACTUALIZACIONES DE APLICACIONES DE TERCEROS

120. Independientemente de las actualizaciones de sistema operativo y de las aplicaciones obtenidas a través de la App Store, es necesario también actualizar otras aplicaciones proporcionadas por terceros.

121. En concreto, se recomienda actualizar de manera automática, o al menos periódicamente, aplicaciones que presentan vulnerabilidades frecuentemente y que son objetivo de ataques dirigidos o masivos, como Oracle Java o Adobe Flash.

122. A través de "Preferencias del Sistema", desde la parte inferior, es posible acceder a las opciones de configuración de aplicaciones y componentes de terceros que han sido instaladas en OS X:

123. Los siguientes apartados detallan las opciones recomendadas para la actualización de algunas aplicaciones comúnmente utilizadas, vulnerables y críticas.

5.3.4.1 ORACLE JAVA

124. En el caso de hacer uso de tecnologías Java, se recomienda llevar a cabo su descarga e instalación en OS X desde el sitio web oficial de Oracle: https://www.java.com.

125. Se recomienda configurar Java para que compruebe automáticamente si hay actualizaciones disponibles.

126. Tras acceder al panel de control de Java desde "Preferencias del Sistema" (disponible desde la versión 7 de Java en adelante), se recomienda habilitar la opción "Comprobar Actualizaciones Automáticamente" de la pestaña "Actualizar":

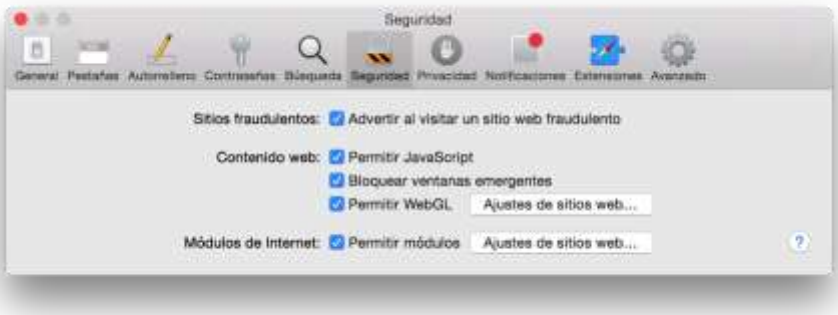
127. Si se pretende hacer uso de tecnologías Java únicamente desde aplicaciones locales, se recomienda desactivar Java en el (los) navegador(es) web.

128. Por un lado, es posible deshabilitar los contenidos Java en los navegadores web de forma genérica desde el panel de control de Java accesible desde "Preferencias del Sistema", mediante la desactivación de la opción "Activar el contenido Java en el explorador" de la pestaña "Seguridad":

129. Como resultado, no será posible cargar contenido Java desde el navegador web (por ejemplo, Safari), aunque debe tenerse en cuenta que el panel de Java especifica que sólo ha sido deshabilitado para el usuario actual.

130. Desde esa misma pestaña, se recomienda mantener el nivel de seguridad para aplicaciones que no están en la lista de excepciones en el valor "Muy Alta" (el valor por defecto es "Alta").

131. Por otro lado, algunos navegadores web[27] como por ejemplo Safari, permiten deshabilitar Java o establecer políticas de uso personalizadas desde el menú "Safari - Preferencias…", y en concreto mediante la opción "Módulos de Internet" (o *plug-ins*) de la pestaña "Seguridad", a través del botón "Ajustes de sitios web…"[28]:

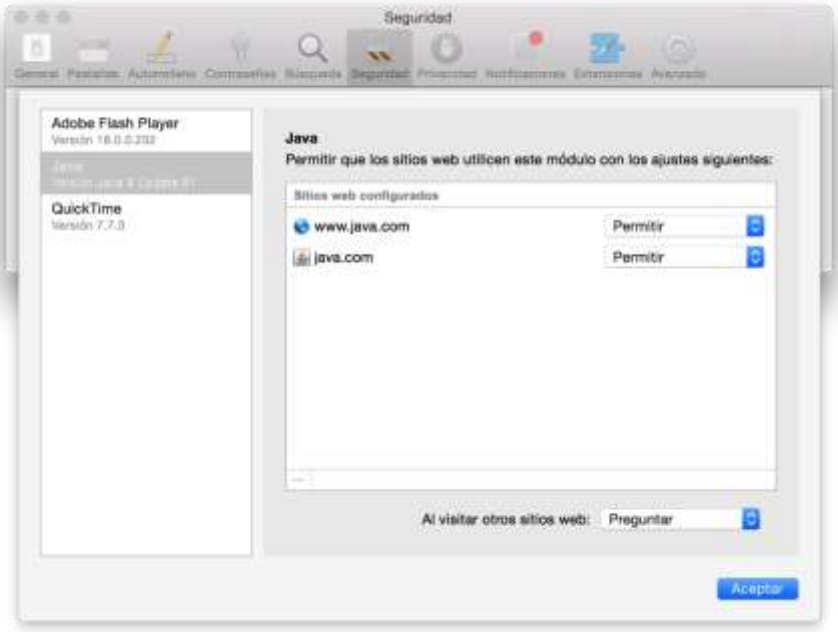


[27] https://support.apple.com/en-us/HT202447

[28] Se puede verificar Java en el navegador desde: https://www.java.com/verify.

Nota: las opciones de configuración de Safari detalladas a lo largo de la presente guía corresponden a la versión de safari detallada en el apartado "5.13.13. Verificación de certificados digitales".

132. La ventana de ajustes de los sitios web permite establecer políticas de ejecución de los diferentes módulos o *plug-ins* para sitios web concretos, y declarar la política por defecto para el resto de sitios web. Por defecto, la política para Java es "Preguntar" al usuario:



133. Otra opción más tediosa pero mas segura, si no se conocen de antemano los sitios web que hacen uso de tecnologías Java pero es necesario emplear esta tecnología, es habilitar el *plug-in* de Java antes de acceder a uno de estos sitios web, acceder a su contenido (mientras está activo el *plug-in* de Java no se recomienda acceder a ningún otro sitio web), y deshabilitar de nuevo el *plug-in* al acabar de usar ese sitio web.

134. Si no se va a hacer uso de tecnologías Java, se recomienda su desinstalación.

5.3.4.2 ADOBE FLASH

135. En el caso de hacer uso de tecnologías Flash, se recomienda llevar a cabo su descarga e instalación en OS X desde el sitio web oficial de Adobe: https://get.adobe.com/flashplayer/.

136. Se recomienda configurar Flash para que compruebe automáticamente si hay actualizaciones disponibles.

137. Durante el proceso de instalación de las últimas versiones de Flash, el usuario puede seleccionar la opción de actualización deseada, disponiéndose de la opción "Permitir que Adobe instale actualizaciones (recomendada)" activa por defecto.

138. Tras acceder al panel de control de Flash Player desde "Preferencias del Sistema", se recomienda habilitar la opción "Notificarme para instalar actualizaciones" de la pestaña "Actualizaciones", si se desea tener mayor control sobre la disponibilidad de actualizaciones y poder decidir el momento de su instalación:

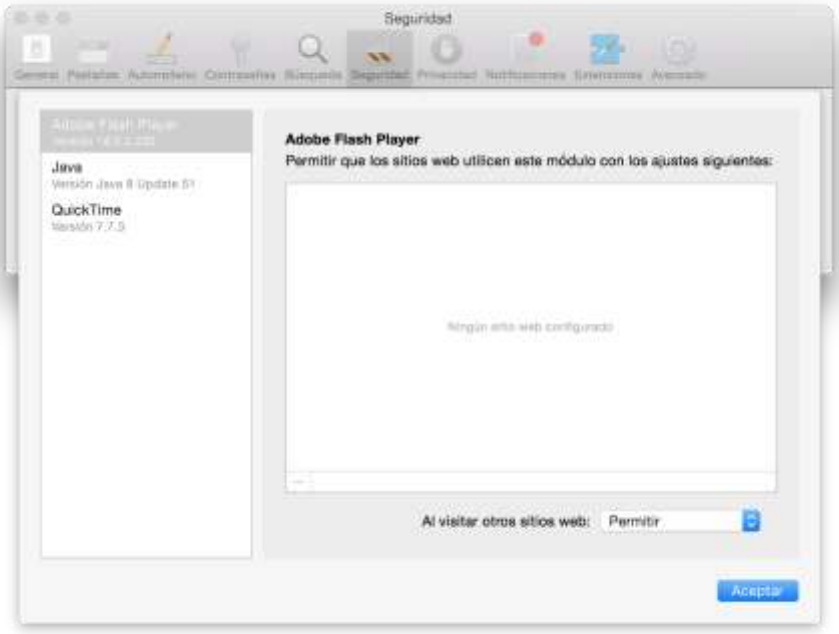
139. Adicionalmente, es posible configurar Flash para que instale automáticamente las actualizaciones disponibles sin la intervención del usuario, a través de la opción "Permitir que Adobe instale actualizaciones (recomendado)".

140. Si no se hace uso de tecnologías Flash en entornos críticos, dónde una nueva actualización que pudiera no ser compatible con dichos entornos bloquearía el acceso a los mismos en caso de ser instalada automáticamente, se recomienda hacer uso de esta opción desde el punto de vista de seguridad para disponer de soluciones frente a las vulnerabilidades de seguridad conocidas lo antes posible.

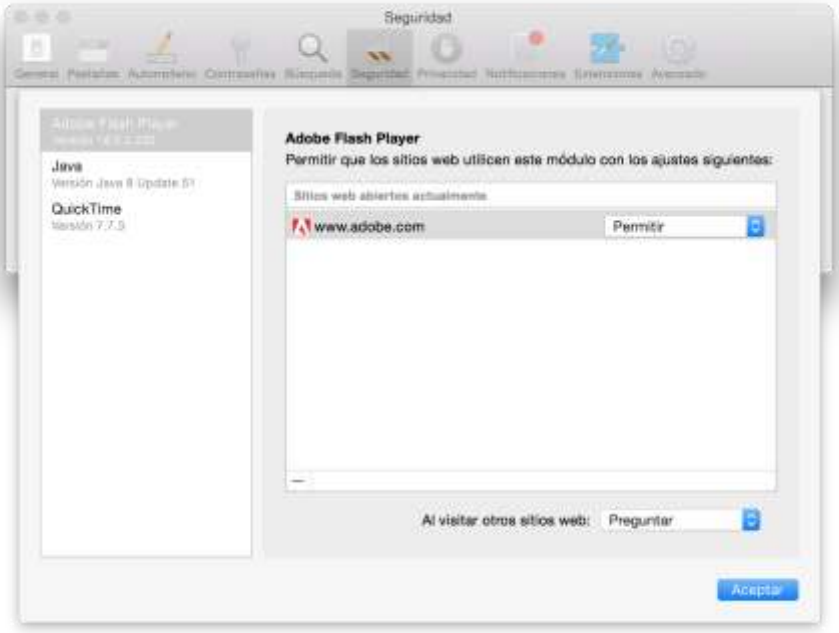
141. Por otro lado, algunos navegadores web como por ejemplo Safari, permiten deshabilitar Flash o establecer políticas de uso personalizadas desde el menú "Safari - Preferencias…", y en concreto mediante la opción "Módulos de Internet" (o *plug-ins*) de la pestaña "Seguridad", a través del botón "Ajustes de sitios web…"[29]:

142. La ventana de ajustes de los sitios web permite establecer políticas de ejecución de los diferentes módulos o *plug-ins* para sitios web concretos, y declarar la política por defecto para el resto de sitios web. Por defecto, la política para Flash es "Permitir" su utilización:

[29] Se puede verificar Flash en el navegador desde: http://www.adobe.com/es/software/flash/about.



143. Se recomienda modificar la política por defecto para Flash en Safari a la opción "Preguntar":



144. Si no se va a hacer uso de tecnologías Flash, se recomienda su desinstalación a través de las instrucciones y el software oficial proporcionado por Adobe [Ref.- 17]. Una vez Flash Player ha sido desinstalado, se debe verificar que realmente no se dispone del *plug-in* accesible desde el navegador web[30].

[30] https://helpx.adobe.com/flash-player.html

5.3.5 CASO PRÁCTICO: VULNERABILIDADES EN OS X

145. Con el objetivo de poder evaluar los riesgos reales de seguridad que afectan a OS X y el ciclo de vida del descubrimiento, publicación y solución de vulnerabilidades de seguridad en OS X, a continuación se detallan un par de casos prácticos, a modo de ejemplo (mediante las vulnerabilidades "OS X 10.10 DYLD_PRINT_TO_FILE Local Privilege Escalation Vulnerability" y "RootPipe"), que deben ser tenidos en cuenta a la hora de stablecer los mecanismos de gestión y protección de los equipos Mac.

146. En OS X 10.10 Yosemite, Apple introdujo modificaciones en el enlazador dinámico o dyld (*dynamic linker*), permitiendo por ejemplo escribir mensajes de error en cualquier fichero a través de la variable de entorno "DYLD_PRINT_TO_FILE".

147. Debido a que es posible hacer uso de esta funcionalidad incluso con binarios SUID pertenecientes a root, se dispone de la capacidad de abrir, modificar y crear ficheros como root en cualquier lugar del sistema de ficheros. Adicionalmente, como el fichero no es cerrado, los procesos derivados del proceso SUID de root ejecutado inicialmente también disponen de acceso al fichero.

148. Como resultado, es posible escalar privilegios en OS X y disponer de acceso como root a nivel del sistema operativo, es decir, control completo del mismo.

149. La vulnerabilidad fue publicada en julio de 2015 [Ref.- 50], afectando a todas las versiones de OS X Yosemite disponibles, 10.10.4 (última versión pública oficial durante el transcurso de la elaboración de la presente guía), pero estando solucionada en la versiones beta iniciales de la siguiente versión de OS X, El Capitan o 10.11.x y en la versión *pre-release* de OS X 10.10.5[31].

150. Esta vulnerabilidad, identificada con el CVE-2015-3760, fue finalmente solucionada por Apple en OS X 10.10.5 [Ref.- 85].

Nota: debido a la ausencia durante varias semanas de actualizaciones por parte de Apple que solucionasen esta vulnerabilidad crítica en las versiones actuales de OS X, el investigador que publicó la misma también publicó adicionalmente una herramienta en formato de extensión de kernel, denominada SUIDGuard, que bloquea el uso de variables de entorno "DYLD_*" en el dyld para binarios SUID root, junto a otras mitigaciones asociadas al flag O_APPEND empleado en la interacción con ficheros.

URL: https://www.suidguard.com
URL: https://github.com/sektioneins/SUIDGuard

151. La ausencia de mecanismos de protección en la gestión de esta variable de entorno en dyld permite mediante el siguiente comando, verificar si el equipo es vulnerable:

```
$ EDITOR=/usr/bin/true DYLD_PRINT_TO_FILE=/vulnerable crontab -e

$ ls -la /vulnerable
-rw-r--r--   1 root  wheel       0 Aug 1 17:17 vulnerable
```

[31] https://developer.apple.com/osx/download/

152. Si como resultado se ha creado el fichero "/vulnerable", perteneciente a root, el equipo es vulnerable y es posible añadir datos e incluso modificar cualquier fichero del sistema de ficheros, incluidos los pertenecientes a root.

153. La publicación original hacía uso del siguiente comando para explotar la vulnerabilidad mediante la modificación del fichero "/etc/sudoers", permitiendo por tanto a un usuario estándar disponer de acceso a "sudo" y poder ejecutar cualquier comando como root a partir de ese momento:

```
$ echo 'echo "$(whoami) ALL=(ALL) NOPASSWD:ALL" >&3' |
    DYLD_PRINT_TO_FILE=/etc/sudoers newgrp

$ sudo tail -1 /etc/sudoers
usuario ALL=(ALL) NOPASSWD:ALL

$ sudo -s
bash-3.2#
```

154. Las técnicas de explotación publicadas han ido cambiando desde la publicación original [Ref.- 50] y actualmente se basan en la creación de un shell local SUID de root ("/usr/bin/boomsh").

155. Esta técnica de explotación ha sido identificada en la distribución e instalación real de Adware para OS X[32] en agosto de 2015.

156. Desde el punto de vista de seguridad, existe la posibilidad de que esta vulnerabilidad, una vez resuelta en las últimas versiones de OS X, no sea resuelta en versiones previas a OS X Yosemite, siendo por tanto obligatorio actualizar a la última versión de OS X para evitar hacer uso de equipos vulnerables.

157. Este fue específicamente el escenario asociado a la vulnerabilidad RootPipe [Ref.- 51], identificada con el CVE-2015-1130, que aprovechaba una funcionalidad oculta en la API del entorno de administración de OS X (*Admin Framework*), asociado a las "Preferencias del Sistema" y a la herramienta "systemsetup".

158. La vulnerabilidad permitía escalar privilegios a cualquier usuario, al comunicarse con dicho entorno a través de los servicios XPC (*Cross Process Communication*, o comunicación entre procesos, también conocido como IPC, *Inter Process Communications*), y disponer de acceso como root a nivel del sistema operativo, es decir, control completo del mismo.

159. Esta vulnerabilidad afectaba a OS X desde el año 2011 (OS X 10.7), fue descubierta en octubre de 2014 y publicada en abril de 2015, tras la actualización de OS X 10.10.3, que resolvía (supuestamente) esta vulnerabilidad, RootPipe. Sin embargo, Apple no publicó actualizaciones para versiones previas de OS X, como por ejemplo 10.9.x, supuestamente por la complejidad y la cantidad sustancial de cambios involucrados en su resolución.

160. OS X 10.10.3 resolvía la vulnerabilidad inicial verificando que sólo las aplicaciones con un *entitlement* concreto podían hacer uso de la funcionalidad disponible en los servicios XPC de *Admin Framework*.

[32] https://blog.malwarebytes.org/mac/2015/08/dyld_print_to_file-exploit-found-in-the-wild/

161. Los *entitlements* de OS X proporcionan capacidades específicas o permisos de seguridad a las aplicaciones, como por ejemplo, habilitar que ejecuten dentro del *sandbox* de OS X.

Nota: el análisis de la funcionalidad y de todas las capacidades de los *entitlements* de OS X, orientadas principalmente a desarrolladores de aplicaciones para OS X, queda fuera del alcance de la presente guía. Se dispone de una visión detallada de estos mecanismos de seguridad en la "Entitlement Key Reference" [Ref.- 45].

Es posible obtener los *entitlements* asociados a una aplicación (en formato PLIST) mediante el siguiente comando:

```
$ codesign -d --entitlements - /usr/sbin/systemsetup
Executable=/usr/sbin/systemsetup
...
<dict>
      <key>com.apple.private.admin.writeconfig</key>
      <true/>
</dict>
</plist>
```

162. Investigaciones posteriores confirman que la vulnerabilidad RootPipe no fue resuelta completamente en OS X 10.10.3 [Ref.- 53], existiendo otros métodos para poder explotarla, como por ejemplo los *plug-ins* (".daplug") de la aplicación "Utilidad de Directorios" (junto a numerosas otras vulnerabilidades relacionadas) [Ref.- 54] [Ref.- 56].

163. Este segundo conjunto de vulnerabilidades, identificadas con los CVE-2015-3671 al 3673, fue resuelto en OS X 10.10.4 [Ref.- 55].

164. En resumen, debe tenerse en cuenta que los equipos basados en OS X pueden estar desprotegidos durante semanas frente a vulnerabilidades de seguridad críticas públicamente conocidas debido a la ausencia de actualizaciones de seguridad oficiales por parte de Apple que las solucionen. Adicionalmente, las actualizaciones oficiales podrían no resolver completamente la vulnerabildiad, por lo que será necesario aplicar una segunda actualización. Por último, las actualizaciones oficiales podrían no estar disponibles para versiones previas de OS X, siendo necesario actualizar siempre a la última versión del sistema operativo.

5.4 PROTECCIÓN DEL PROCESO DE ARRANQUE DEL EQUIPO

165. OS X proporciona diferentes opciones durante el proceso de arranque para los equipos Mac basados en plataforma Intel que permiten acceder a diferentes modos de arranque y a su funcionalidad asociada [Ref.- 19].

166. Para acceder a los distintos modos de arranque es necesario mantener pulsadas ciertas teclas durante el proceso de arranque (ver siguiente tabla [Ref.- 19]), nada más encender el equipo e inmediatamente después de escuchar el sonido o tono de arranque. Normalmente es necesario mantener la tecla pulsada hasta que aparece el logo de Apple en la pantalla, o la siguiente pantalla asociada al modo de arranque seleccionado:

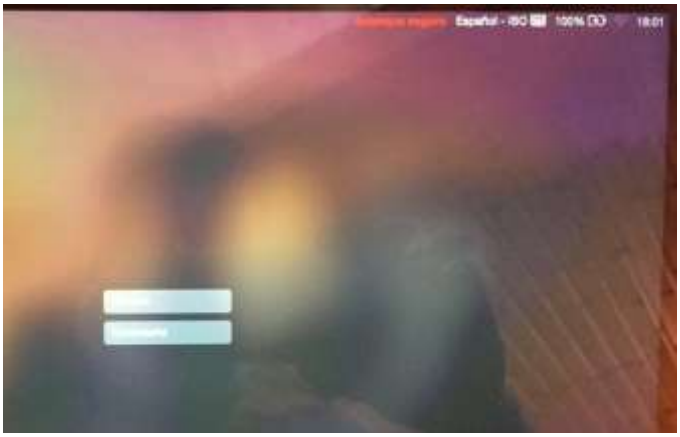
Mantener pulsada/s durante el arranque	Descripción
Mayúsculas ⇧	Arranca en modo seguro.
Opción ⌥	Arranca con el Gestor de arranque.
C	Arranca desde un CD, un DVD o una unidad de memoria en miniatura USB de arranque (como por ejemplo el soporte de instalación de OS X).
D	Arranca con el Apple Hardware Test o con Diagnósticos de Apple, en función del Mac que estés utilizando.
Opción-D	Arranca con el Apple Hardware Test o con Diagnósticos de Apple a través de Internet.
N	Arranca desde un servidor NetBoot compatible.
Opción-N	Arranca desde un servidor NetBoot utilizando la imagen de arranque predeterminada.
Comando (⌘)-R	Arranca desde Recuperación de OS X.
Comando-Opción-R	Arranca desde Recuperación de OS X a través de Internet.
Comando-Opción-P-R	Restablece la NVRAM. Suelta las teclas después de volver a escuchar el sonido de arranque.
Comando-S	Arranca en modo de usuario único.
M	Arranca en modo de disco de destino.
X	Arranca desde un volumen de arranque de OS X cuando el Mac debería arrancar desde un volumen de arranque distinto.
Comando-V	Arranca en modo verboso.
Expulsar (⏏), F12, botón del ratón o botón del trackpad	Se expulsan los soportes extraíbles, como por ejemplo un disco óptico.

Nota: es posible reiniciar el equipo desde cualquier modo especial de arranque, o cualquier estado, manteniendo pulsada la tecla de encendido y apagado durante al menos 5 segundos.

5.4.1 MODO SEGURO

167. El modo seguro [Ref.- 20] (*safe mode* o *safe boot*), tecla Shift, permite que al arrancar el equipo se lleven a cabo ciertas comprobaciones y evita que se ejecute software que puede estar causando problemas durante el proceso de arranque. Por este motivo, el proceso de arranque es habitualmente más lento que en el modo normal.

168. Es posible identificar que se ha arrancado en modo seguro mediante el texto "Arranque seguro" en color rojo en la parte derecha de la barra principal de menú en la pantalla de inicio de sesión (o login, o pantalla de autentificación).



169. Asimismo, una vez iniciada sesión en OS X, el modo de arranque puede obtenerse mediante el icono de la manzana ( ) disponible en la barra de menús, bajo la opción "Acerca de este Mac", y en concreto, desde la sección "Visión general" y el botón "Informe del sistema…". Desde la sección "Software" se dispone de la opción "Modo de arranque", que mostrará el valor "Seguro" en lugar de "Normal".

170. Adicionalmente, es posible arrancar en modo seguro de forma local o remota desde un terminal (asumiendo que se dispone de acceso al equipo, por ejemplo, mediante SSH) a través del siguiente comando y el parámetro "-x" (el parámetro "-v", opcional, permite obtener información detallada o *verbose* durante el arranque - modo verboso):

```
$ sudo nvram boot-args="-x -v"

$ sudo nvram boot-args=""
```

171. Se puede arrancar en modo normal de nuevo sin especificar ningún argumento de arranque, a través del segundo comando, siendo necesaria su utilización, ya que los argumentos de arranque permanecen activos hasta que son modificados de nuevo explícitamente.

172. Arrancar en modo seguro puede ser necesario, por ejemplo, si el equipo ha sido comprometido y contiene software malicioso que es ejecutado durante el proceso de arranque y que está afectando al funcionamiento normal del equipo.

173. Teóricamente es posible arrancar en modo seguro incluso si se hace uso de FileVault (ver apartado "5.8.4. Cifrado completo del disco: FileVault"), sin embargo, la tecla empleada para este modo de arranque (Shift) no es procesada durante el arranque y, en cualquier caso, se arranca en modo normal[33].

174. Alternativamente, para arrancar en modo seguro cuando FileVault está activo es necesario hacer uso de un terminal y del comando "nvram" previamente detallado, especificando el parámetro "-x" en los argumentos de arranque de NVRAM del equipo.

[33] En OS X Yosemite esta opción no parece funcionar ni siquiera haciendo uso de la tecla Shift justo después de introducir la contraseña del usuario en la pantalla de inicio de sesión de FileVault.

175. Tras reiniciar el equipo en modo seguro, si FileVault está activo, será necesario autentificarse dos veces al arrancar en modo seguro[34], la primera para descifrar el disco de arranque desde la pantalla de inicio de sesión de FileVault, y la segunda para iniciar sesión en OS X desde la pantalla de inicio de sesión estándar.

5.4.2 GESTOR DE ARRANQUE

176. El gestor de arranque de OS X [Ref.- 21], tecla Opción (o Alt), permite seleccionar un volumen (en terminología Apple, o partición lógica) desde el que arrancar un sistema operativo cuando el equipo inicia el proceso de arranque, correspondiente a un sistema de almacenamiento local o disponible a través de la red, o asociado a Boot Camp (para arrancar un sistema operativo alternativo, como Windows, en el equipo Mac).

177. Mediante una doble pulsación del botón izquierdo del ratón es posible arrancar el sistema operativo del volumen seleccionado.

178. Por defecto OS X arrancará el sistema operativo del volumen especificado como disco de arranque predeterminado, disponible mediante "Preferencias del sistema - Disco de arranque":

[34] https://support.apple.com/en-us/HT201262

Nota: la funcionalidad "Modalidad de disco de destino" (*target disk mode*)[35], que permite reiniciar el ordenador Mac para usarlo como disco duro desde otro equipo usando un cable Thunderbolt o FireWire, queda fuera del alcance de la presente guía.

5.4.2.1 ARRANCAR DESDE UN CD/DVD O UNA MEMORIA USB EXTERNA

179. Durante el proceso de arranque del equipo, es posible reiniciar el mismo desde un CD o DVD mediante la tecla C.

180. Adicionalmente, desde el gestor de arranque de OS X es también posible arrancar el equipo desde una unidad de memoria USB externa de arranque que disponga de una copia del disco de instalación de OS X [Ref.- 26] ("Instalador de OS X" o "OS X Installer") o de un sistema de recuperación (ver apartado "5.4.4.3. ASISTENTE DE DISCO DE RECUPERACIÓN"):

181. Desde el mismo es posible acceder a la funcionalidad asociada al modo de recuperación integrado en OS X (ver apartado "5.4.4. Recuperación de OS X").

182. Por tanto, en este escenario es también posible llevar a cabo ataques basados en disponer de acceso a un terminal y a la capacidad de modificar la contraseña de cualquier usuario (ver apartado "5.4.4.2. TERMINAL DESDE EL MODO DE RECUPERACIÓN").

183. En el caso del instalador de OS X, "OS X Installer", las herramientas asociadas están también disponibles desde el menú "Utilidades" (ver siguiente imagen).

184. La funcionalidad disponible desde el sistema de recuperación y desde el instalador de OS X es equivalente.

[35] https://support.apple.com/en-us/HT201462

5.4.3 APPLE HARDWARE TEST (AHT) O DIAGNÓSTICOS DE APPLE

185. El Apple Hardware Test (AHT) [Ref.- 22] es un modo de arranque que incluye un conjunto de herramientas de diagnóstico para verificar el hardware del ordenador y ayudar en la detección de problemas de hardware.

186. AHT está disponible para equipos Apple de antes de junio de 2013, por lo que queda fuera del alcance de la presente guía.

187. Para equipos Apple más modernos se dispone de Diagnósticos de Apple [Ref.- 23], con funcionalidad similar a AHT, y un asistente que ofrece una serie de pasos iniciales para intentar ayudar a resolver los problemas hardware detectados:

188. Durante el proceso de diagnóstico, el equipo mostrará el mensaje "Comprobando su Mac…" y el tiempo estimado hasta la finalización del proceso (habitualmente, si no se detectan problemas, entre 2 y 3 minutos):

189. Si se hace uso de Diagnósticos de Apple disponiendo de conectividad hacia Internet, los resultados del diagnóstico se enviarán a Apple (incluyendo el número de serie del equipo y los códigos de referencia[36] de los problemas hardware identificados) y, adicionalmente, se obtendrá información y artículos recomendados desde los recursos de soporte técnico de Apple.

[36] https://support.apple.com/es-es/HT203747

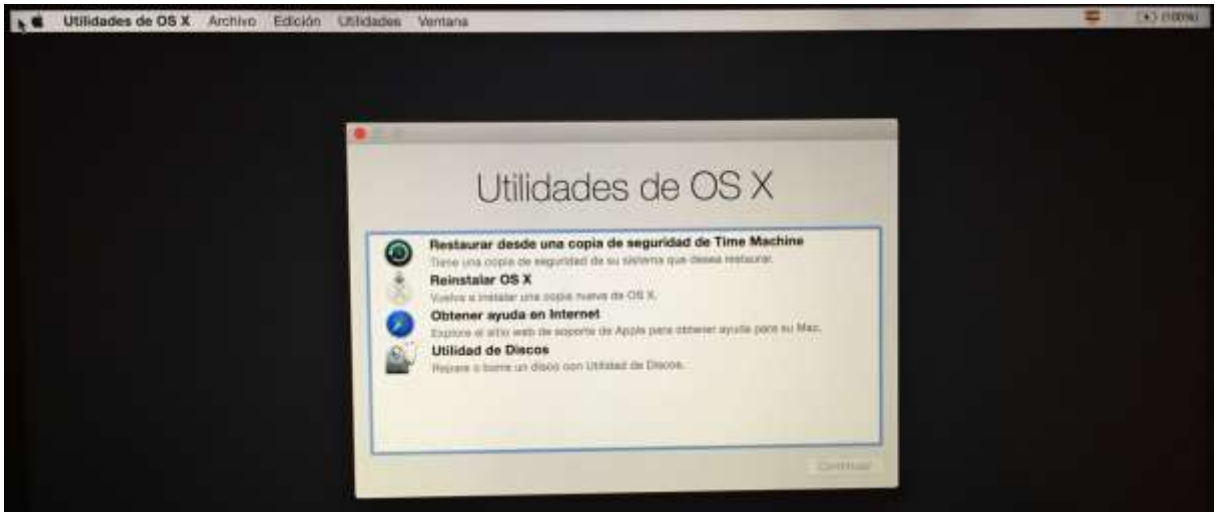
190. Desde el punto de vista de privacidad se recomienda limitar la información que es enviada a Apple durante el proceso de diagnóstico, y por tanto, deshabilitar la conectividad del equipo (aunque esta acción también limitará la información disponible durante el proceso de diagnóstico).

191. El modo AHT o Diagnósticos de Apple no está operativo si se ha establecido una contraseña en el firmware del equipo (ver apartado "5.4.9. Establecer una contraseña en el firmware del equipo").

5.4.4 RECUPERACIÓN DE OS X

192. El modo de recuperación de OS X [Ref.- 24], teclas Cmd+R, incluye un conjunto de utilidades que permiten reinstalar el sistema operativo OS X en el equipo, así como comprobar y reparar el sistema de almacenamiento principal (mediante la "Utilidad de Discos"[37]), verificar la conexión a Internet y obtener ayuda desde Internet (empleando la versión restringida de Safari disponible en la imagen de recuperación de OS X), o restaurar los datos desde una copia de seguridad de Time Machine.

193. Tras iniciar en el modo de recuperación aparecerá un escritorio con una barra de menús que muestra el texto "Utilidades de OS X", junto a su pantalla asociada, y que proporciona un acceso rápido a las funcionalidades previamente mencionadas:



194. El modo de recuperación hace uso de una partición de recuperación creada específicamente para este propósito y que habitualmente no es accesible desde OS X (por ejemplo, desde Finder o desde la "Utilidad de Discos"). Las particiones de recuperación de las unidades de memoria USB externas son visibles, por ejemplo, al arrancar desde el gestor de arranque (ver apartado "5.4.2. Gestor de arranque").

195. Es posible ver los detalles de la partición de recuperación, con un tamaño de 650 MB aproximadamente e identificada con el nombre "Recovery HD", mediante el comando "diskutil" (o alternativamente mediante el comando "sudo gpt show -l /dev/disk0"):

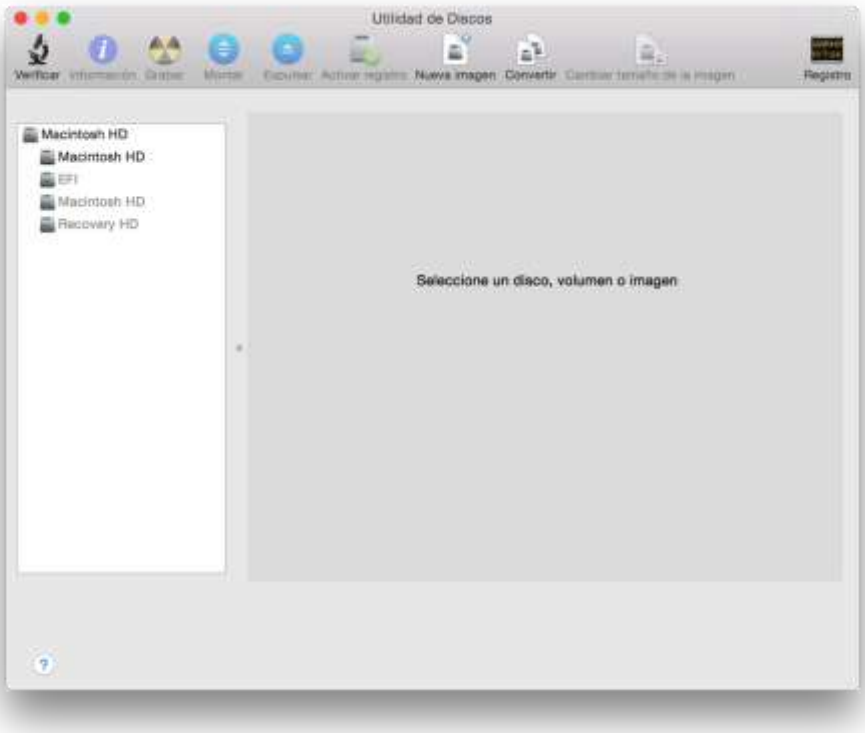
[37] https://support.apple.com/es-es/HT203176

```
$ diskutil list
/dev/disk0
   #:       TYPE        NAME                SIZE       IDENTIFIER
   ...
   3:       Apple_Boot Recovery HD          650.0 MB   disk0s3
   ...

$ diskutil info disk0s3
```

196. Para poder visualizar la partición de recuperación desde la "Utilidad de Discos" es necesario habilitar las capacidades de depuración. Tras cerrar la "Utilidad de Discos", y ejecutar el siguiente comando, al volverla a abrir se dispondrá de un nuevo menú "Depurar" (entre los menús "Ventana" y "Ayuda"):

```
$ defaults write com.apple.DiskUtility DUDebugMenuEnabled 1
```

197. A través de este menú es posible, mediante la opción "Depurar - Mostrar cada partición", visualizar todas las particiones existentes en el sistema de almacenamiento principal de OS X, además de "Macintosh HD" visible por defecto, tales como "EFI" (tipo EFI), "Macintosh HD" (tipo volumen físico Core Storage) y "Recovery HD" (tipo partición de arranque de Apple), así como el tipo de partición:



198. El proceso de reinstalación de OS X requiere disponer de conexión a Internet (siendo necesario disponer de DHCP en la red Wi-Fi o Ethernet empleada), ya que se instalará OS X

empleando una versión del instalador disponible en Internet obtenida desde los servidores de Apple.

199. Es posible reinstalar OS X manteniendo intactos los archivos, datos y ajustes del usuario mediante la opción "Reinstalar OS X" o reinstalar OS X con los ajustes de fábrica (ver apartado "ANEXO B. Proceso de restauración de los ajustes de fábrica o formateo de OS X").

200. En concreto se instalará la versión de OS X con la que venía originalmente el ordenador, por lo que será necesario aplicar posteriormente todas las actualizaciones disponibles para esa versión de sistema oeprativo (ver apartado "5.3.1. Actualizaciones de sistema operativo: OS X").

201. Desde el punto de vista de seguridad, son especialmente relevante las opciones del menú "Utilidades", ya que disponen por un lado de la utilidad para establecer una contraseña en el firmware (o EFI) del equipo (ver apartado "5.4.9. Establecer una contraseña en el firmware del equipo", y por otro, de capacidades para ejecutar un terminal (ver apartado "5.4.4.2. TERMINAL DESDE EL MODO DE RECUPERACIÓN").

202. Para hacer uso del modo de recuperación e interactuar con el disco de arranque de OS X, si el disco duro está cifrado con FileVault (ver apartado "5.8.4. Cifrado completo del disco: FileVault"), es necesario primero desbloquear el disco, y luego descifrarlo para poderlo montar mediante la "Utilidad de Discos" [Ref.- 77]. Alternativamente es posible desbloquear y descifrar el disco desde un terminal [Ref.- 78].

203. Desde el modo de recuperación, mediante la "Utilidad de Discos", y tras seleccionar la partición lógica de arranque de OS X cifrada (segunda entrada), desde el menú "Archivo - Desbloquear 'Macintosh HD'" es posible desbloquear el disco.

204. Para ello es necesario introducir la contraseña de una de las cuentas de usuario que tiene autorización para desbloquear y descifrar FileVault, es decir, una de las cuentas de usuario activas en FileVault.

205. Una vez desbloqueado el disco, tras seleccionarlo y pulsar la tecla Alt (Opción) a la vez que se selecciona el menú "Archivo", aparecerá la opción "Desactivar encriptación…", que permitiría, tras introducir de nuevo la contraseña de un usuario activo en FileVault, deshabilitar el cifrado del disco de arranque.

5.4.4.1 OPCIONES DE ACCESO AL MODO DE RECUPERACIÓN

206. Los equipos Mac actuales, dependiendo del modelo de hardware y de la versión de sistema operativo OS X, disponen de múltiples alternativas para acceder al modo de recuperación.

207. El método más directo es empleando el modo de recuperación integrado en OS X, disponible a través de la partición de recuperación del sistema de almacenamiento principal (ver apartado "5.4.4. Recuperación de OS X").

208. Alternativamente, si el disco duro principal está dañado, es posible acceder al modo de recuperación a través de Internet, mediante la pulsación de las teclas Cmd+Alt+R durante el proceso de arranque (disponiéndose de la posibilidad de seleccionar una red Wi-Fi si no se dispone aún de conectividad desde el equipo):

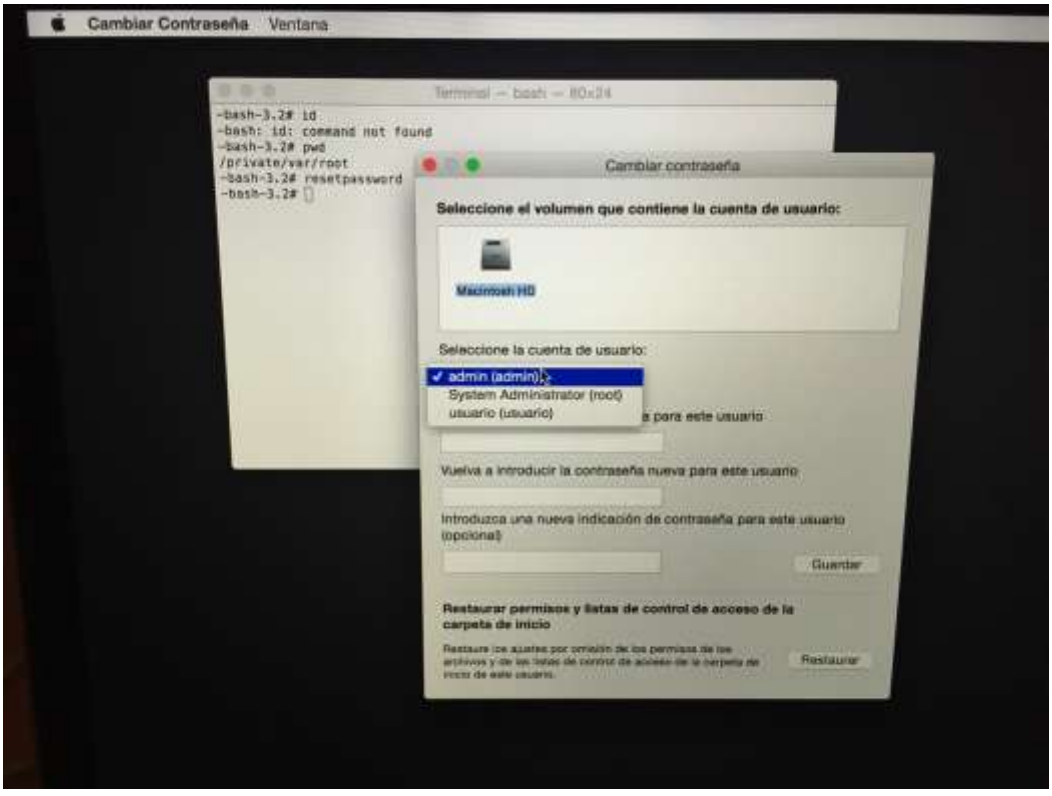
209. Esta funcionalidad de recuperación desde Internet, obtiene la propia imagen de recuperación de OS X desde Internet (en lugar de hacer uso de la partición de recuperación local de OS X), y está disponible en los ordenadores Mac comercializados tras la publicación de OS X Lion (mediados del año 2011).

210. Por último, y en el caso de que el disco duro principal esté dañado y no se disponga de conectividad hacia Internet, también es posible acceder al modo de recuperación a través de una unidad de memoria USB externa (ver apartado "5.4.4.3. ASISTENTE DE DISCO DE RECUPERACIÓN").

5.4.4.2 TERMINAL DESDE EL MODO DE RECUPERACIÓN

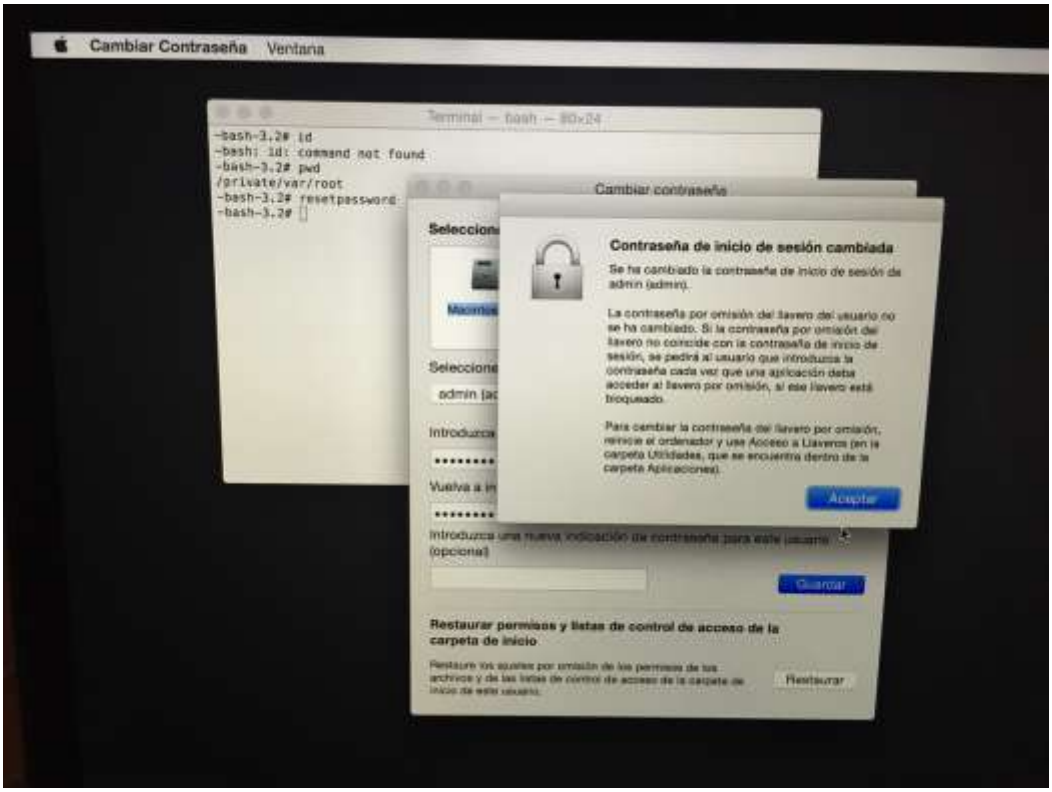
211. La posibilidad de ejecutar un terminal desde el modo de recuperación proporciona acceso como root al entorno asociado a OS X y vinculado al sistema o partición de recuperación.

212. Desde el terminal es posible ejecutar el comando "resetpassword" (en versiones previas de OS X existía incluso la opción "Cambiar contraseña" en el menú de "Utilidades") para cambiar la contraseña de cualquier usuario:



213. Para ello, sólo es necesario seleccionar el volumen del equipo que contiene la instalación de OS X (por ejemplo, "Macintosh HD"). Como resultado se mostrará el listado de cuentas de

usuario disponibles en dicho volumen y, tras seleccionar la cuenta de usuario objetivo (por ejemplo, "admin"), será posible introducir la nueva contraseña que será asignada a dicho usuario:



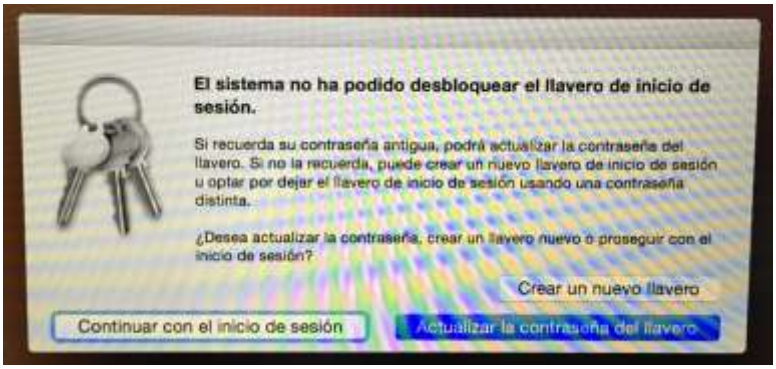
214. Como resultado, un potencial atacante con acceso físico al equipo podría modificar la contraseña de cualquier usuario, incluyendo los usuarios administradores, y reiniciar el equipo en modo normal para disponer de control completo del mismo.

215. Para hacer uso de la utilidad "Cambiar contraseña" desde el modo de recuperación, si el disco duro está cifrado con FileVault (ver apartado "5.8.4. Cifrado completo del disco: FileVault"), se necesita desbloquear y montar el disco mediante la "Utilidad de Discos". Para ello, es necesario conocer la contraseña de una de las cuentas de usuario que tiene autorización para desbloquear FileVault (ver apartado "5.4.4. Recuperación de OS X").

216. En caso de no desbloquear el disco, no es posible hacer uso de la utilidad, ya que al no poder acceder a los contenidos del volumen cifrado, el disco no aparece en la lista de volúmenes con las cuentas de usuario y, como resultado, la lista de usuarios disponible para el cambio de contraseña estará vacía. Tras desbloquear el disco de arranque de OS X cifrado con FileVault mediante la "Utilidad de Discos", es posible hacer uso de la utilidad "resetpassword" normalmente, tal y como se ha descrito previamente.

217. Este ataque puede ser llevado a cabo tanto empleando el modo de recuperación integrado en OS X, como utilizando una unidad de memoria USB externa con el disco de instalación de OS X [Ref.- 26] o con el sistema de recuperación de OS X [Ref.- 25].

218. El cambio de contraseña sólo modifica la contraseña de inicio de sesión del usuario, siendo necesario posteriormente modificar la contraseña por omisión del llavero del usuario (la contraseña asociada a su *keychain*; ver apartado "5.8.7. Acceso a Llaveros"):

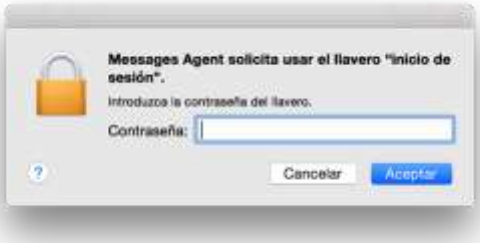


219. Este cambio se puede llevar a cabo tras reiniciar el equipo en modo normal, iniciando una sesión con la cuenta de usuario y empleando la utilidad "Acceso a Llaveros" desde la carpeta "Utilidades" de OS X, dentro de la carpeta "Aplicaciones" (también accesible desde "Finder - Ir - Utilidades").

220. Al iniciar sesión con ese usuario se mostrará una ventana con un mensaje que refleja esta discrepancia entre la contraseña de la cuenta de usuario o contraseña de inicio de sesión (o *login*), y la contraseña del llavero de inicio de sesión (o *login*).

221. El mensaje proporciona diferentes opciones: actualizar la contraseña del llavero si se recuerda la contraseña antigua, crear un nuevo llavero de inicio de sesión, o continuar, dejando el llavero de inicio de sesión con una contraseña distinta a la de inicio de sesión (en concreto, la contraseña antigua).

222. Si se continua con el inicio de sesión (tercera opción), diferentes servicios (como por ejemplo *Messages Agent*, cloudpaird, etc) solicitarán frecuentemente la contraseña del llavero de inicio de sesión para poder hacer uso de sus contenidos:



223. En el escenario de ataque planteado, y al no conocerse la contraseña antigua, la única opción disponible para un potencial atacante pasa por poder iniciar sesión como el usuario, pero no dispondría de capacidades para acceder a los contenidos de su llavero, salvo que sea capaz de obtener la contraseña previa del usuario.

224. Si se conoce la contraseña antigua[38] (primera opción), desde el mensaje mostrado al iniciar sesión o desde "Acceso a Llaveros" y a través del menú "Edición - Cambiar contraseña del llavero "inicio de sesión"…" es posible establecer una nueva contraseña y disponer de acceso a todos los contenidos del llavero.

[38] https://support.apple.com/es-es/HT201609

225. Otra alternativa es crear un nuevo llavero[39] (segunda opción), acción que eliminará los contenidos previos del llavero del usuario. Desde el mensaje mostrado al iniciar sesión o desde "Acceso a Llaveros" y mediante el menú "Preferencias…" y el botón "Restaurar mi llavero por omison" es posible establecer una nueva contraseña y crear un nuevo llavero vacío.

226. El llavero por omisión original, es decir el existente actualmente y asociado a la contraseña antigua, será movido, pero no se eliminará.

227. Por defecto, el fichero asociado al llavero de inicio de sesión del usuario está disponible en "~/Library/Keychains/login.keychain". Al crear un nuevo llavero de inicio de sesión, el llavero anterior se almacena en "~/Library/Keychains/login_renamed_1.keychain".

5.4.4.3 ASISTENTE DE DISCO DE RECUPERACIÓN

228. OS X proporciona un asistente para la creación de un disco, unidad o sistema de recuperación [Ref.- 25] en una unidad de memoria USB externa que puede ser utilizada posteriormente desde el gestor de arranque:

229. La unidad de memoria USB externa (con al menos 1 GB de capacidad) debe ser formateada siguiendo los requisitos necesarios, es decir, con tabla de particiones GUID y formato Mac OS Plus (con registro).

230. Posteriormente, el asistente instalará el sistema de recuperación en la misma, y pese a que la partición no será visible desde Finder o desde la "Utilidad de Discos", será posible reiniciar desde ella empleando el gestor de arranque y acceder a la misma funcionalidad asociada al modo de recuperación integrado en OS X:

[39] https://support.apple.com/es-es/HT203192

231. Si el sistema de recuperación para la unidad de memoria USB externa se crea empleando un sistema OS X con FileVault activo, el asistente intentará copiar a la unidad de memoria USB externa el volumen principal "Macintosh HD", en lugar de la partición de recuperación, por lo que la unidad de memoria USB externa no será creada correctamente. Este escenario puede ser identificado porque el nombre del volumen creado en la unidad USB externa es "Macintosh HD" en lugar de "Recovery HD".

232. En su lugar, es necesario utilizar el asistente en un sistema OS X sin FileVault activo. Sin embargo, tras llevar a cabo el proceso de creación desde OS X Yosemite, la situación es similar, no siendo posible crear la unidad de memoria USB externa correctamente (de nuevo, el nombre del volumen creado es "Macintosh HD"):

233. La documentación del asistente refleja que éste sólo aplica a las versiones Lion y Mountain Lion de OS X, y aunque es también válido para ser usado en equipos con OS X Yosemite, la creación del sistema de recuperación en la unidad de memoria USB externa debe llevarse a cabo en una versión previa de OS X.

5.4.5 MODO DE RESTABLECIMIENTO DE LA NVRAM

234. La NVRAM es una pequeña memoria del ordenador (*Non-Volatile Random Access Memory*, memoria de acceso aleatorio no volátil) que almacena algunos ajustes de configuración a los que OS X puede acceder rápidamente. Los ajustes de configuración almacenados en la NVRAM dependen del modelo de ordenador Mac utilizado y de los dispositivos o periféricos conectados a éste.

235. Por ejemplo, la NVRAM puede almacenar el volumen del altavoz, la resolución de la pantalla, el disco de arranque predeterminado, mensajes de error del kernel, información de zona horaria, etc.

Nota: este tipo de información se almacenaba en los ordenadores Mac más antiguos en la PRAM (*Parameter Random Access Memory*, o RAM de parámetros), en lugar de en la NVRAM.

236. Para llevar a cabo el restablecimiento de la NVRAM en los equipos Mac es necesario abrir el equipo con un destornillador y modificar la configuración hardware de la memoria RAM existente, añadiendo o eliminando módulos de memoria en función del número de módulos y bahías disponibles actualmente.

237. En los equipos Mac más modernos no es necesario modificar la configuración hardware de la memoria RAM, ya que en algunos (como los MacBook Air) no es posible, al estar integrada la memoria directamente en la placa lógica del equipo.

238. Tras realizar la modificación hardware de la memoria RAM (en equipos Mac más antiguos), es necesario reiniciar el equipo en modo restablecimiento de la NVRAM [Ref.- 27], pulsando la combinación de teclas Cmd+Alt+P+R durante el proceso de arranque, inmediatamente después de escuchar el sonido o tono de arranque. Tras escuchar por segunda vez el sonido de arranque de OS X, se debe de dejar de presionar las teclas indicadas. Se volverá a escuchar el sonido de arranque de OS X una tercera vez, e incluso una cuarta vez, y el equipo arrancará a continuación normalmente.

239. Este modo de arranque restablece la configuración de la NVRAM a sus valores por defecto.

240. Mediante el comando "nvram -p" es posible imprimir todas las variables existentes en la NVRAM y sus valores asociados:

```
$ nvram -p
```

241. Tras restablecer la NVRAM, la siguiente vez que se accede al modo de recuperación se mostrará una pantalla para que el usuario especifique el idioma a emplear en ese modo.

5.4.6 MODO DE RESTABLECIMIENTO DEL SMC

242. El controlador de administración del sistema (SMC, *System Management Controller*) es responsable de muchas funciones de bajo nivel de los ordenadores Mac, como la gestión de los ajustes de configuración asociados a la alimentación del equipo (activación, apagado, modo reposo, carga de la batería, etc), ventiladores y gestión de la temperatura, indicadores luminosos y retroalimentación del teclado, detección de la luz ambiental, eventos de apertura y cierre de la pantalla de los ordenadores portátiles, etc.

243. El modo de restablecimiento del SMC [Ref.- 11] es diferente según si el ordenador portátil tiene o no batería extraíble (los equipos Apple más modernos no disponen de batería extraíble, mientras que los más antiguos sí).

244. Para equipos sin batería extraíble es necesario conectar el equipo a la electricidad, y el restablecimiento del SMC se lleva a cabo pulsando la combinación de teclas Shift+Alt+Cmd (de la parte izquierda del teclado) junto al botón de encendido, simultáneamente.

245. Posteriormente, se debe de dejar de presionar las teclas indicadas y el botón de encendido al mismo tiempo. Mediante una nueva pulsación del botón de encendido, se arrancará el equipo habiendo restablecido el SMC.

5.4.7 MODO DE UN SOLO USUARIO

246. En el modo de un solo usuario o usuario único (*single user mode*, o SUM) [Ref.- 34], teclas Cmd+S, el equipo arranca con un terminal de texto con privilegios de root (indicado por el *prompt* "bash-3.2#" en OS X Yosemite), en lugar de mostrar el interfaz gráfico de usuario (GUI, *Graphical User Interface*) con la pantalla de login de OS X.

247. En este modo, OS X y en concreto launchd, no lleva a cabo la ejecución de ninguno de los servicios y subsistemas asociados al proceso de arranque, ni se establece ninguna sesión de usuario gráfica.

248. En el modo de un solo usuario se hace uso del teclado con la configuración de inglés americano (USA). Para salir del modo de un solo usuario es suficiente con rearrancar el equipo mediante el comando "reboot". Mediante el comando "exit" el equipo continuará el proceso de arranque normal.

249. El arranque en modo de un solo usuario lleva implícito el modo verboso (ver apartado "5.4.8. Modo verboso"), mostrando los detalles del proceso de arranque de OS X:

250. Para hacer uso del modo de un solo usuario, si el disco duro está cifrado con FileVault (ver apartado "5.8.4. Cifrado completo del disco: FileVault"), es necesario introducir la

contraseña de una de las cuentas de usuario que tiene autorización para desbloquear FileVault en la pantalla de inicio de sesión de FileVault [Ref.- 79]. Una vez introducida, el proceso de arranque progresará normalmente y se dispondrá de acceso en modo de un solo usuario.

251. Si se ha establecido una contraseña en el firmware del equipo (ver apartado "5.4.9. Establecer una contraseña en el firmware del equipo", e independientemente del estado de FileVault), no será posible arrancar en modo de un solo usuario (aunque se presionen las teclas asociadas), arrancándose en modo normal en su lugar. Es necesario desactivar dicha contraseña, por ejemplo a través del modo de recuperación, para poder arrancar en modo de un solo usuario.

252. Desde el modo de un solo usuario es posible realizar múltiples tareas en OS X, como por ejemplo, modificar la contraseña de cualquier usuario mediante los siguientes comandos:

```
# /sbin/fsck -fy
# /sbin/mount -uw /
# launchctl load
/System/Library/LaunchDaemons/com.apple.opendirectoryd.plist
# ls /Users
.localized    Shared    admin    usuario
# dscl . -passwd /Users/admin nuevacontraseña

o

# passwd admin
```

253. Esta secuencia de comandos monta la partición raíz en modo de lectura y escritura (por defecto está montada sólo en modo de lectura), ejecuta el demonio Open Directory necesario para cambiar la contraseña de inicio de sesión de cualquier usuario y cambia la contraseña, en el ejemplo, del usuario "admin".

254. Este procedimiento es válido para versiones previas de OS X (OS X 10.7 y posteriores[40]) pero, en el caso de OS X Yosemite, se genera el siguiente mensaje de error ("/System/Library/LaunchDaemons/com.apple.DirectoryServicesLocal.plist: No such file or directory") y no se obtiene respuesta del comando "dscl". En el caso del procedimiento basado en el comando "passwd", tampoco se obtiene respuesta tras ejecutarlo.

255. El motivo es que el comando "dscl" no está plenamente operativo en modo de un solo usuario en OS X Yosemite, y cualquier comando asociado[41] (incluso el abrir una sesión interactiva mediante "dscl") da lugar al mismo resultado. El comando "dscl" en una sesión de OS X Yosemite estándar sí funciona correctamente.

256. Este procedimiento de cambio de onctraseña no modifica la contraseña del llavero del usuario (ver apartado "5.4.4.2. TERMINAL DESDE EL MODO DE RECUPERACIÓN").

[40] El comando para OS X <=10.6 es: # launchctl load /System/Library/LaunchDaemons/com.apple.DirectoryServices.plist

[41] # dscl . -read /Users/admin O # dscl /local/Default -read /Users/admin

257. Otro método alternativo válido en OS X Yosemite para crear un nuevo usuario administrador con capacidad para modificar la contraseña de otros usuarios, o realizar cualquier otro cambio en OS X, es eliminar el fichero ("/var/db/.AppleSetupDone") que indica que no se debe llevar a cabo el proceso de instalación inicial de OS X durante el proceso de arranque porque éste ya ha sido completado:

```
# /sbin/fsck -fy
# /sbin/mount -uw /
# rm /var/db/.AppleSetupDone
# reboot
```

258. Como resultado, al arrancar el sistema operativo pensará que debe llevarse a cabo el proceso de instalación inicial de OS X (ver apartado "ANEXO A. Proceso de instalación y configuración inicial"), permitiendo la creación de un nuevo usuario administrador.

5.4.8 MODO VERBOSO

259. El modo verboso (*verbose*) [Ref.- 34], teclas Cmd+V, proporciona detalles sobre los diferentes pasos y acciones llevadas a cabo por OS X durante el proceso de arranque, mostrando los mensajes de los diferentes subsistemas y servicios que están siendo arrancados. Este modo puede ser empleado complementariamente tanto en modo normal, como en modo seguro o en modo de un solo usuario.

5.4.9 ESTABLECER UNA CONTRASEÑA EN EL FIRMWARE DEL EQUIPO

260. Con el objetivo de limitar el tipo de ataques detallados en apartados previos, "5.4.4.2. TERMINAL DESDE EL MODO DE RECUPERACIÓN" o "5.4.7. Modo de un solo usuario", en sus diferentes variantes y modos de arranque de OS X (ver apartados "5.4.2.1. ARRANCAR DESDE UN CD/DVD O UNA MEMORIA USB EXTERNA" o "5.4.4.1. OPCIONES DE ACCESO AL MODO DE RECUPERACIÓN"), es fundamental establecer una contraseña en el firmware (o EFI) del equipo.

261. Adicionalmente, existen herramientas comerciales como Kon-Boot que proporcionan capacidades para manipular el proceso de arranque de OS X y poder acceder al equipo con la cuenta de cualquier otro usuario o crear un nuevo usuario administrador [Ref.- 82]. Es posible también mitigar los ataques de este tipo de herramientas estableciendo una contraseña en el firmware del equipo o habilitando el cifrado de disco mediante FileVault ("5.8.4. Cifrado completo del disco: FileVault").

Nota: el firmware de los ordenadores Mac basados en arquitectura PowerPC estaba basado en Open Firmware, mientras que el firmware de los ordenadores Mac basados en arquitectura Intel está basado en EFI (*Extensible Firmware Interface*). El EFI define un interfaz entre el sistema operativo y el firmware del equipo, y sustituye a las BIOS (*Basic Input Output System*) más antiguas.

262. OS X proporciona la posibilidad de establecer una contraseña en el firmware del equipo que proteja el proceso de arranque y evite la posibilidad de arrancar desde el gestor de arranque para hacer uso de un disco o unidad de memoria USB externa, o en modo de recuperación, modo de usuario único o modo de disco de destino.

263. La contraseña del firmware sólo será solicitada al usuario al arrancar el equipo desde uno de estos modos especiales, y no así al arrancar en modo normal desde el disco de arranque predeterminado.

264. Esta contraseña complementa la contraseña de la cuenta de usuario, que evita que un potencial atacante pueda iniciar sesión en el equipo, y las capacidades de cifrado de FileVault (también basadas en la contraseña de inicio de sesión del usuario y/o en una clave de recuperación), que evitan que un potencial atacante pueda acceder a los datos almacenados en el disco duro sin conocer la contraseña.

265. Para establecer la contraseña en el firmware (o EFI) del equipo [Ref.- 28] es necesario arrancar el equipo en modo de recuperación (ver apartado "5.4.4. Recuperación de OS X").

266. Desde el menú "Utilidades", y mediante la opción "Utilidad Contraseña Firmware", se accede a la utilidad que permite establecer una contraseña en el firmware (o EFI) del equipo mediante el botón "Activar contraseña de firmware…":

267. Tras introducir la contraseña del firmware[42] y pulsar el botón "Definir contraseña", se recomienda salir de la utilidad y reiniciar el equipo para que la contraseña del firmware sea activada:

[42] Una cadena igual o inferior a 255 caracteres teóricamente, aunque podrían sólo aceptarse los primeros 48 [Ref.- 29].

268. Desde este momento, si se reinicia el equipo en algún modo distinto al normal, por ejemplo en modo de recuperación, se mostrará una pantalla solicitando la contraseña de firmware:

Nota: existe un bug conocido desde OS X Yosemite 10.10.3 en el que si se hace uso de FileVault para el cifrado del disco y se establece posteriormente la contraseña del firmware, el equipo no arranca, ya que no es capaz de identificar el disco de arranque, mostrando una carpeta blanca con un símbolo de interrogación parpadeando, sobre un fondo negro.

En ese escenario es necesario arrancar el equipo en modo de recuperación y establecer de nuevo el disco de arranque mediante el icono de la manzana (□) y la opción "Disco de arranque…", desbloqueando previamente el disco con FileVault, para que el proceso de arranque de OS X funcione normalmente con ambos mecanismos de protección activos.

5.4.9.1 UTILIDAD "FIRMWAREPASSWD"

269. La utilidad "setregproptool", disponible antiguamente (hasta OS X Yosemite) dentro del paquete de instalación de OS X[43], es el equivalente desde un terminal a la "Utilidad Contraseña Firmware" del modo de recuperación.

270. En el caso de OS X Yosemite, esta utilidad sólo está disponible desde un terminal en el modo de recuperación, en concreto, bajo "/Applications/Utilities/Firmware\ Password\ Utility.app/Contents/Resources".

271. A nivel de sistema operativo, OS X Yosemite ha sustituido dicha herramienta por "/usr/sbin/firmwarepasswd".

272. La ventaja de la utilidad "firmwarepasswd", frente a su uso desde el modo de recuperación, es que permite comprobar (y gestionar) la configuración de la contraseña del firmware desde

[43] En concreto, en "/Contents/SharedSupport/InstallESD.dmg", dentro de "BaseSystem.dmg", y bajo "/Applications/Utilities/Firmware\ Password\ Utility.app/Contents/Resources" (https://github.com/CLCMacTeam/Install-setregproptool).

el propio sistema operativo, incluyendo si existe o no una contraseña establecida, y el modo de seguridad asociado (por defecto, "command"):

```
$ sudo firmwarepasswd -mode
Mode: none
$ sudo firmwarepasswd -check
Password Enabled: No

$ sudo firmwarepasswd -setpasswd
Setting Firmware Password
Enter new password: ...
Re-enter new password: ...
Password changed
NOTE: Must restart before changes will take effect

$ sudo firmwarepasswd -check
Password Enabled: Yes
$ sudo firmwarepasswd -mode
Mode: command
```

273. Si se desea restringir aún más el proceso de arranque de OS X, se recomienda modificar el modo de seguridad del firmware para que se solicite la contraseña asociada incluso al arrancar el equipo en modo normal (mediante el modo de seguridad "full"):

```
$ sudo firmwarepasswd -setmode full
Enter password: ...
Mode changed
NOTE: Must restart before changes will take effect
```

274. Para cambiar el modo de seguridad es necesario introducir la contraseña del firmware actual, y el cambio surtirá efecto tras reiniciar el equipo.

275. Los modos de seguridad del firmware disponibles en OS X son:

- none: No se ha establecido una contraseña en el firmware.
- command: La contraseña del firmware es solicitada en los modos de arranque especiales (modo de seguridad por defecto).
- full: La contraseña del firmware es solicitada para todos los modos de arranque, incluyendo el modo de arranque normal.

276. Mediante el comando "firmwarepasswd -verify", que permite verificar el valor correcto de la contraseña de firmware actual, se pueden llevar a cabo ataques de fuerza bruta desde OS X sobre la contraseña, empleando un usuario administrador.

277. La opción "unlockseed" permite obtener desde el propio OS X el código de 33 caracteres para la eliminación de la contraseña del firmware (ver apartado "5.4.9.3. ELIMINACIÓN DE LA CONTRASEÑA DEL FIRMWARE POR PARTE DE APPLE"):

```
$ sudo firmwarepasswd -unlockseed
C024...F54D
```

278. Es también posible eliminar la contraseña del firmware existente mediante esta utilidad, tras introducir la contraseña del firmware actual, opción no recomendada desde el punto de vista de seguridad:

```
$ sudo firmwarepasswd -delete
Delete Firmware Password
Enter password: ...
Password removed
NOTE: Must restart before changes will take effect
```

279. Pese a que para hacer uso de la utilidad "firmwarepasswd" es necesario ejecutarla con privilegios de root, existe la posibilidad de que si el equipo es comprometido, cualquier software malicioso que ejecute en OS X con permisos de administrador podría interactuar con el EFI e intentar cambiar el modo de seguridad, obtener el valor de la contraseña del firmware y/o eliminarla, u obtener el valor del código de eliminación de la contraseña.

5.4.9.2 FUERZA BRUTA DE LA CONTRASEÑA DEL FIRMWARE

280. Si no se introduce la contraseña correcta en la pantalla de solicitud de la contraseña del firmware durante el proceso de arranque, no se recibe ninguna confirmación, ni mensaje de error, salvo que el equipo no continua con el proceso de arranque normal.

281. La pantalla de arranque que solicita la contraseña de firmware no dispone de un mecanismo robusto frente ataques de fuerza bruta para la adivinación de la contraseña.

282. Tras realizar varios intentos de acceso fallidos (a partir de 6 intentos), se establece un retardo que impide realizar un nuevo intento de acceso inmediatamente. El retardo va siendo incrementado progresivamente, hasta alcanzar aproximadamente los 10 segundos a partir del intento fallido número 15. Para el resto de intentos de acceso, el retardo permanece constante en ese valor de 10 segundos.

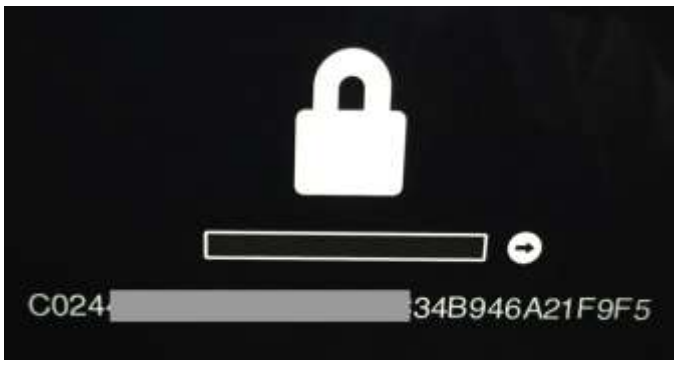
283. Es por tanto posible llevar a cabo ataques de fuerza bruta empleando un dispositivo USB que simule un teclado (como por ejemplo, el Teensy 3), que tenga en cuenta el valor del retardo y que se encargue de introducir automáticamente todas las combinaciones posibles [Ref.- 30].

284. El tiempo máximo estimado para recorrer las 10.000 combinaciones asociadas a un PIN de 4 dígitos es de unas 48 horas, tomando un valor de 17 segundos entre intentos (empleando una aproximación conservadora, al ser significativamente superior ese valor al retardo máximo identificado entre intentos, de 10 segundos).

5.4.9.3 ELIMINACIÓN DE LA CONTRASEÑA DEL FIRMWARE POR PARTE DE APPLE

285. Si no se recuerda la contraseña establecida en el firmware del equipo (o el PIN empleado al hacer uso de la funcionalidad de bloqueo de "Buscar mi Mac", ver apartado "5.12. iCloud: Buscar mi Mac"), existe la posibilidad de llevar el equipo a una tienda Apple[44] (gratuitamente) o a un *Apple Authorized Service Provider* (potencialmente, con coste asociado), junto al comprobante de compra (recibo o factura), y un técnico de soporte de Apple podrá desbloquear el equipo (en unas 24 horas aproximadamente, aunque el proceso requiere menos tiempo para ser completado).

286. Existe, por tanto, un mecanismo que permite eliminar la contraseña de firmware de los equipos Mac sin conocer su valor actual. Este mecanismo requiere pulsar la siguiente combinación de teclas, Ctrl+Alt+Cmd+Shift+S[45], en la pantalla de arranque que solicita la contraseña de firmware, con el objetivo de que se muestre un código (o *hash*, de 33 caracteres alfanuméricos) específico para ese equipo:



287. Los primeros 17 caracteres corresponden a un identificador de la placa lógica y del número de serie del chip Atmel del equipo (*Mac logic board serial number*), y los siguientes 16 caracteres son un *hash* derivado de la contraseña[46].

288. La parte del código correspondiente a la contraseña (16 últimos caracteres) cambia con cada modificación de la contraseña del firmware o modificación del modo de seguridad (tras reiniciar el equipo; ver apartado "5.4.9.1. UTILIDAD "FIRMWAREPASSWD""), aunque la contraseña del firmware no haya sido modificada. Por tanto, el modo de seguridad también en utilizado en la generación del *hash*, no sólo el valor de la contraseña.

289. Tras remitir ese código a Apple, Apple genera un código de respuesta en forma de fichero (*keyfile*), denominado "SCBO" y único para ese equipo y *hash* concretos, y que al ser cargado desde el gestor de arranque mediante una unidad de memoria USB externa, permite eliminar la contraseña de firmware actual en ese equipo.

290. Se recomienda por tanto que el valor de la contraseña de firmware sea diferente a cualquier otra contraseña utilizada en el equipo, como por ejemplo, la de las cuentas de usuario existentes en OS X.

---

[44] https://www.apple.com/retail/geniusbar/

[45] Las teclas pueden pulsarse en cualquier órden, salvo para la tecla S que debe ser pulsada en último lugar, y se deben mantener pulsadas todas ellas simultáneamente.

[46] http://forums.macrumors.com/threads/efi-firmware-password-removal.1710012/ y http://macefibiosunlock.blogspot.com

291. Adicionalmente al proceso oficial ofrecido por Apple, existen servicios de terceros[47] en Internet que proporcionan este servicio empleando el mismo método, potencialmente sin verificar quién es el propietario del ordenador adecuadamente, solicitando acceso al equipo (requieren que se les envíe el equipo físicamente) o a la información necesaria (código de 33 caracteres).

292. Como resultado proporcionan el fichero "SCBO", directamente en un disco o unidad USB externa o únicamente el fichero, para que el propio usuario pueda proceder a la creación de la unidad de memoria USB externa de eliminación de la contraseña de firmware. Como parte del servicio detallan todos los pasos a seguir para crear dicho disco USB (en formato texto y vídeo). Estas instrucciones también están disponibles en foros de Internet relacionados con los ordenadores Mac[48] y específicamente con el EFI[49].

5.4.9.4 ELIMINACIÓN DE LA CONTRASEÑA DEL FIRMWARE RESTABLECIENDO LA NVRAM

293. En el pasado existía una vulnerabilidad en los equipos Mac que permitía a un potencial atacante con acceso físico al equipo eliminar (o resetear) la contraseña de firmware realizando un restablecimiento (o reseteo) de la PRAM o NVRAM (ver apartado "5.4.5. Modo de restablecimiento de la NVRAM").

294. Independientemente de las limitaciones de expansión implícitas al hardware de ciertos ordenadores Apple, como por ejemplo la imposibilidad de extraer los módulos de memoria RAM de los MacBook Air ya que están directamente integrados en la placa lógica, este escenario de ataque no es posible hoy en día[50].

295. En la actualidad, si se ha establecido una contraseña en el firmware del equipo, es necesario introducir dicha contraseña y desactivarla, por ejemplo a través del modo de recuperación, para poder llevar a cabo el proceso de restablecimiento de la NVRAM detallado en el apartado "5.4.5. Modo de restablecimiento de la NVRAM". En caso contrario, el equipo permanecerá en la pantalla que solicita la contraseña del firmware.

296. Por tanto, en el caso de tener activa una contraseña en el firmware, la funcionalidad de restablecimiento de la NVRAM no está disponible con el objetivo de limitar posibles manipulaciones de la NVRAM sin conocer dicha contraseña.

5.4.9.5 ELIMINACIÓN Y OBTENCIÓN DE LA CONTRASEÑA DEL FIRMWARE MEDIANTE EFIPW

297. Por otro lado, debe tenerse en cuenta que existen herramientas como "efipw" [Ref.- 29] que permiten modificar la contraseña del firmware (o EFI) del ordenador Mac, e incluso decodificar la contraseña actual, si se dispone de privilegios de root en OS X.

298. Sin embargo, de nuevo esta utilidad no funciona con los nuevos equipos de Apple, ya que estos no disponen de esa información almacenada en la NVRAM, y en concreto, de las

---

[47] Servicios de terceros: macefiunlock.com, macefibiosunlock.blogspot.com y efihashcrack.blogspot.com (24-48h), macunlocked.com (envío del equipo).

[48] http://www.hackmac.org/forum/topic/1227-anyone-want-to-try-a-macbook-air-efi-hash/page__p__7045#entry7045

[49] http://www.hackmac.org/forum/forum/19-efi-firmware/

[50] En equipos Apple más antiguos (hasta alrededor del año 2010 aproximadamente) sí que era posible eliminar la contraseña de firmware realizando un restablecimiento de la NVRAM (o PRAM).

variables de seguridad de la NVRAM utilizadas por equipos más antiguos de Apple, como "security_password" (valor de la contraseña del firmware) y "security_mode" (modo de seguridad: none, command o full [Ref.- 29]):

```
$ sudo nvram security_password
$ sudo nvram security_mode
```

299. La contraseña del firmware de los nuevos equipos de Apple (desde el año 2011 aproximadamente[51]) se almacena en el chip Atmel[52] del equipo, ubicado en la placa madre o placa lógica[53].

Nota: la placa madre o placa principal de los ordenadores Mac de Apple, según el modelo concreto, se denomina también placa lógica (*logic board*).

5.4.9.6 ELIMINACIÓN DE LA CONTRASEÑA DEL FIRMWARE REEMPLAZANDO O REPROGRAMANDO EL CHIP ATMEL

300. Otra alternativa para eliminar la contraseña del firmware si se dispone de acceso físico al equipo pasa por reemplazar el chip Atmel[54] por uno nuevo ya pre-programado con el firmware de Apple para el modelo de ordenador Mac y tipo de placa lógica concretos.

301. Alternativamente, se podría reemplazar la placa lógica completa, proceso más costoso pero que también reemplazaría el chip Atmel.

302. Para ello sería necesario abrir el equipo, localizar y desoldar el chip Atmel actual, y soldar el nuevo chip Atmel (sin contraseña establecida) en su lugar. En este caso es recomendable instalar un nuevo disco duro y reinstalar el sistema operativo OS X en el mismo.

303. Otro método alternativo similar, disponiendo de acceso físico al chip Atmel, sería emplear un dispositivo (*SPI* o *PIC o EEPROM programmer*[55]) que permite reprogramar dicho chip, para proceder a escribir en el mismo una versión original del firmware de Apple sin contraseña[56] (existen repositorios públicos no oficiales con el firmware original para los diferentes modelos de ordenadores Mac[57]).

304. Adicionalmente, existe otro método empleando el mismo dispositivo, basado en leer el contenido del chip Atmel, identificar dónde está almacenada la contraseña, y reemplazar ese valor con un valor vacío[58] (opción también disponible comercialmente como servicio[59]).

[51] http://www.cnet.com/news/efi-firmware-protection-locks-down-newer-macs/

[52] http://www.atmel.com/Images/2535s.pdf

[53] Algunos chips de Atmel disponen de un *Security Register* para almacenar números de serie o identificadores únicos.

[54] Los chips Atmel para Apple están disponibles en el mercado como "BIOS EFI firmware chip". Por otro lado, se dispone de entornos de desarrollo para los chips de Atmel AVR, como CrossPack: https://www.obdev.at/products/crosspack/index.html.

[55] http://openprog.altervista.org/OP_eng.html

[56] http://ho.ax/posts/2012/06/unbricking-a-macbook/

[57] Apple EFI Repository: https://ghostlyhaks.com/downloads/2014-07-25-06-43-32/efi-firmware (El valor de EMC para cada modelo de ordenador Mac está disponible a través de Mactracker)

[58] https://www.ghostlyhaks.com/blog/blog/hacking/18-how-to-bypass-apple-efi-firmware-lock

[59] http://allservice.ro/forum/viewtopic.php?t=2724

305. Los diferentes métodos de eliminación de la contraseña del firmware descritos previamente ratifican la importancia que tiene la seguridad física del equipo, siendo necesario disponer de control del mismo en todo momento para poder asegurar su protección.

5.4.9.7 ATAQUES FIRMWARE MEDIANTE EL PUERTO THUNDERBOLT (Y EL EFI)

306. Thunderstrike [Ref.- 32] es el nombre de un conjunto de vulnerabilidades de seguridad en el firmware (o EFI) de los ordenadores Mac que permiten a software malicioso, o a dispositivos Thunderbolt maliciosos, sobrescribir el contenido del EFI e incluso propagarse a través de dispositivos Thunderbolt compartidos.

307. Un dispositivo Thunderbolt de uso muy común en equipos Mac es, por ejemplo, el adaptador de red Gigabit Ethernet necesario para conectarse a redes Ethernet en los nuevos ordenadores Mac (como el empleado para la elaboración de la presente guía), al no disponer estos de tarjeta Ethernet integrada debido a su grosor y configuración hardware.

308. Un potencial atacante con acceso físico al equipo puede, por tanto, reprogramar el EFI, a nivel de firmware, utilizando código malicioso con funcionalidades de *rootkit* en el proceso de arranque, conocido como *bootkit*.

309. La versión 10.10.2 de OS X Yosemite [Ref.- 33] solucionó parcialmente esta vulnerabilidad, identificada con el CVE-2014-4498, mitigando la misma durante el proceso de actualización del EFI. Sin embargo, sigue siendo vulnerable a la vulnerabilidad en las Option ROM de Thunderbolt del año 2012[60] durante el proceso normal de arranque [Ref.- 32] (consultar la FAQ).

310. Establecer una contraseña en el firmware del equipo, o habilitar FileVault, no evitan este tipo de ataques, ya que tienen lugar previamente durante el proceso de arranque.

Nota: esta vulnerabilidad en Thunderbolt es independiente de otra vulnerabilidad similar, denominada "Inception"[61], y que permitía acceso directo de lectura y escritura a los primeros 4GB de memoria RAM vía DMA (*Direct Memory Access*) a través de los interfaces FireWire, Thunderbolt, ExpressCard, PC Card o cualquier otro interfaz PCI/PCIe del equipo.

Esta vulnerabilidad fue mitigada en OS X 10.8.2 Mavericks en los ordenadores Mac del año 2012 (aproximadamente) activando VT-D y bloqueando las peticiones DMA.

311. Adicionalmente, un nuevo conjunto de vulnerabilidades en el firmware de los ordenadores Mac, denominado Thunderstrike 2 [Ref.- 44] fue publicado a mitad de 2015 (evolución de las vulnerabilidades Thunderstrike descritas previamente), permitiendo la propagación de código malicioso entre diferentes ordenadores (con comportamiento de gusano o *firmworm*)[62].

312. Estas vulnerabilidades afectan al firmware de los equipos Mac, tanto en su propagación a través de las Option ROM de dispositivos Thunderbolt compartidos, como a través del vector de infección inicial, que puede ser explotado remotamente, comprometiendo el EFI del equipo.

[60] http://ho.ax/downloads/De_Mysteriis_Dom_Jobsivs_Black_Hat_Slides.pdf

[61] http://www.breaknenter.org/projects/inception/

[62] La herramienta "t2e_integrity_check" permite verificar la integridad de las (PCI) Option ROM de los adaptadores Apple de Thunderbolt a Ethernet (t2e): https://github.com/legbacore/t2e_integrity_check.

313. La versión 10.10.4 de OS X Yosemite [Ref.- 12] solucionó parcialmente esta vulnerabilidad, identificada con el CVE-2015-3692.

5.5 PROTECCIÓN DEL PROCESO DE ARRANQUE DE OS X

5.5.1 PROCESO DE ARRANQUE

314. Con el objetivo de gestionar los servicios y aplicaciones que son activados durante el proceso de arranque de OS X, es necesario realizar una muy breve introducción al proceso de arranque de los ordenadores Mac.

315. Al encender un equipo Mac, la BootROM se activa y su firmware realiza las siguientes tareas a través de dos componentes (POST y EFI): inicializa algunos componentes hardware (como la memoria) y verifica su estado a través del POST (*Power-On Self Test*) y el EFI (*Extensible Firmware Interface*) inicializa otros componentes hardware y selecciona el sistema operativo a arrancar del volumen especificado como disco de arranque predeterminado (ver apartado "5.4.2. Gestor de arranque") [Ref.- 38].

316. Una vez el BootROM finaliza sus tareas y selecciona el sistema operativo, pasa el control al *boot loader* (boot.efi), que ejecuta dentro del EFI, y cuyo principal objetivo es cargar el entorno de ejecución del kernel. El *boot loader* se almacena en "/System/Library/CoreServices/boot.efi".

317. El *boot loader* muestra la pantalla de arranque (con el logo de la manzana de Apple), y en el caso de hacer uso de FileVault, muestra la pantalla de arranque o inicio de sesión de FileVault (a través del EFI) qué solicita las credenciales del usuario, necesarias para descifrar el disco y poder arrancar desde él[63].

318. Desde OS X 10.7, para agilizar el arranque, el *boot loader* busca el kernel[64] a través de una caché que ya tiene todas las extensiones de kernel enlazadas con éste, bajo "/System/Library/Caches/com.apple.kext.caches/Startup/kernelcache".

319. Sino se puede usar la caché, el *boot loader* busca en "/System/Library/Extensions/*.kext" las extensiones de kernel a cargar según el tipo de arranque, un proceso más lento que consulta el fichero "./Contents/Info.plist" de cada extensión y ejecuta el *linker* (enlazador).

320. Una vez se han cargado el kernel y todas las extensiones necesarias para el arranque, el *boot loader* ejecuta el procedimiento de inicialización del kernel, dónde se localiza la partición raíz (localmente o a través de la red), y se inicializa el I/O Kit, encargado de enlazar los *drivers* de los diferentes componentes hardware en el kernel.

321. A partir de ese momento, el kernel arranca el sistema operativo OS X (basado en FreeBSD) desde la partición raíz, e invoca launchd, el primer proceso que es ejecutado en el sistema[65].

322. launchd inicializa el sistema, parte del entorno de usuario y se encarga de ejecutar los servicios de sistema[66]. launchd también tiene la capacidad de ejecutar servicios bajo

[63] Si FileVault no está activo, la pantalla de inicio de sesión o *login* estándar es gestionada por "loginwindow".

[64] *Unified prelinked kernel.*

[65] https://developer.apple.com/library/mac/documentation/Darwin/Reference/ManPages/man8/launchd.8.html

[66] https://developer.apple.com/library/mac/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/Lifecycle.html

demanda, desactivarlos en periodos de inactividad, y activarlos de nuevo cuando sea necesario.

323. Finalmente, launchd ejecuta "loginwindow", la aplicación encargada de mostrar la pantalla de inicio de sesión o *login* y llevar a cabo la autentificación de los usuarios. Si el proceso de autentificación tiene éxito, "loginwindow" inicializa el entorno gráfico del usuario, con el escritorio, Finder, Dock, etc.

324. Por tanto, las extensiones de kernel son el primer elemento donde el software malicioso puede establecerse de manera persistente para ejecutar cada vez que arranca el equipo.

325. Las extensiones de kernel están disponibles bajo "/System/Library/Extensions/*.kext" y "/Library/Extensions/*.kext".

326. Se recomienda verificar el contenido de esos directorios y confirmar que no existe ninguna extensión de kernel sospechosa o desconocida, analizando el propósito de cada uno de los elementos no habituales en OS X (como referencia, el apartado "ANEXO C. Listado de extensiones de kernel por defecto" contiene el listado por defecto de extensiones de kernel en la versión OS X 10.10 Yosemite para el modelo de equipo Mac empleado para la elaboración de la presente guía).

5.5.2 ACTIVACIÓN DE SERVICIOS Y APLICACIONES DURANTE EL PROCESO DE ARRANQUE DE OS X

327. En OS X, los *Startup Items*[67] constituían la lista de servicios y aplicaciones que serán arrancados durante el proceso de arranque del sistema operativo, disponibles bajo "/System/Library/StartupItems" y "/Library/StartupItems".

328. Pese a estar obsoletos, se recomienda verificar el contenido de esos directorios y confirmar que no existe ningún *Startup Item* definido, o en caso de existir, únicamente permitir la ejecución de aquellos de los que se quiere hacer uso.

329. Adicionalmente, y también heredado de los sistemas Unix más antiguos, OS X tiene la capacidad de ejecutar tareas durante el arranque del equipo que han sido definidas en el fichero "/etc/rc.common".

330. Se recomienda verificar el contenido de este fichero y confirmar que no incluye la ejecución de ningún script, binario o aplicación no deseado.

331. En el caso de OS X Yosemite (10.10.x), el mecanismo de ejecución de actividades durante el proceso de arranque basado en *Startup Items* se considera obsoleto[68] y ha sido sustituido por el servicio launchd y sus demonios y agentes asociados[69], disponibles genéricamente bajo "/Library/LaunchDaemons" (ejecutados durante el proceso de arranque del sistema) y "~/Library/LaunchAgents" (ejecutados durante el proceso de inicio de sesión de cada usuario), respectivamente.

332. El proceso o servicio launchd gestiona demonios (*daemons*), servicios a nivel de sistema del que hay una única instancia para todos los usuarios, no interactivos y que son ejecutados

[67] https://developer.apple.com/library/mac/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/StartupItems.html

[68] Habiéndose eliminado SystemStarter: /System/Library/LaunchDaemons/com.apple.SystemStarter.plist

[69] https://developer.apple.com/library/mac/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLaunchdJobs.html

incluso antes de que ningún usuario inicie una sesión, y agentes (*agents*), servicios que ejecutan individualmente a nivel de usuario, que son ejecutados tras haber iniciado el usuario una sesión, y que pueden interactuar con el interfaz gráfico de OS X y con la sesión del usuario.

333. En concreto, los directorios relevantes para la configuración de launchd son los siguientes:

- ~/Library/LaunchAgents: Agentes de usuario creados por cada usuario.
- /Library/LaunchAgents: Agentes de usuario creados por el administrador.
- /Library/LaunchDaemons: Demonios de sistema creados por el administrador.
- /System/Library/LaunchAgents: Agentes de usuario proporcionados por OS X.
- /System/Library/LaunchDaemons: Demonios de sistema proporcionados por OS X.

334. Estos directorios incluyen un fichero PLIST de configuración para cada uno de los demonios o agentes existentes, que habrán sido creados por el usuario, por el administrador o por el software y aplicaciones instaladas en OS X (normalmente con permisos de administrador).

Nota: la modificación de múltiples ajustes y parámetros de configuración en OS X puede llevarse a cabo en algunos casos mediante la edición de ficheros PLIST (*Property List*), un formato propietario de Apple. Estos ficheros, con contenido XML, pueden ser almacenados tanto en formato ASCII como en formato binario.

Si los ficheros son almacenados en formato ASCII es posible visualizarlos y modificarlos con cualquier editor de texto. Si son almacenados en formato binario será necesario emplear un editor con soporte para ficheros PLIST para su visualización y modificación, como por ejemplo el entorno de desarrollo de Apple Xcode, disponible en la página de recursos para desarrolladores de Apple [Ref.- 8] o la utilidad plutil (por ejemplo, que mernite ver su contenido mediante el comando: `$ plutil -convert xml1 -o - Info.plist | less`).

A través de la utilidad "file" es posible determinar si el formato empleado es ASCII o binario:

```
$ file /Library/LaunchDaemons/com.oracle.java.JavaUpdateHelper.plist
/Library/LaunchDaemons/com.oracle.java.JavaUpdateHelper.plist: XML  document text

$ file /Library/Preferences/com.apple.SoftwareUpdate.plist
/Library/Preferences/com.apple.SoftwareUpdate.plist: Apple binary property list
```

335. Se recomienda revisar cada uno de los ficheros PLIST existentes en todos los directorios descritos previamente y verificar si se desea que se ejecute cada uno de los demonios y agentes asociados, considerando que cada uno de ellos corresponde a diferentes servicios y aplicaciones instaladas.

Nota: los detalles de cómo diseñar y programar demonios o agentes de launchd en OS X quedan fuera del alcance de la presente guía, pero están disponibles en la "Daemons and Services Programming Guide", guía para desarrolladores de OS X:

https://developer.apple.com/library/mac/documentation/MacOSX/Conceptual/BPSystemStartup/BPSystemStartup.pdf

336. Mediante el comando "launchctl" (*launchd control*) es posible interactuar, controlar y gestionar launchd. Por ejemplo, el parámetro "list" muestra todos los trabajos ejecutados por launchd, incluyendo el PID del proceso asociado, lo que facilita su identificación mediante el comando "ps -ef":

```
$ launchctl list
```

337. Adicionalmente, OS X tiene la capacidad de ejecutar tareas durante el arranque del equipo que han sido definidas en el fichero "/etc/launchd.conf" (que no existe por defecto), por ejemplo, mediante el comando "bsexec" (una directiva de launchctl que permite ejecutar otros comandos) [Ref.- 41].

338. Se recomienda verificar si este fichero ha sido creado y confirmar que su contenido no incluye la ejecución de ningún script, binario o aplicación no deseado.

Nota: la herramienta *KnockKnock (UI)*, evolución de una herramienta en Python con capacidades similares[70], permite descubrir la presencia de software que se ha instalado de manera persistente en OS X, una característica común en el software malicioso (*malware*) para poder ser ejecutado cada vez que se inicia el equipo. La herramienta comprueba diferentes ubicaciones o categorías que permiten disponer de persistencia en OS X.

URL: https://objective-see.com/products/knockknock.html

Por otro lado, la herramienta *BlockBlock (beta)*, monitoriza continuamente las ubicaciones que permiten disponer de persistencia en OS X y genera una alerta cuando se añaden nuevos elementos a las mismas, permitiendo al usuario incluso tomar acciones al respecto.

URL: https://objective-see.com/products/blockblock.html

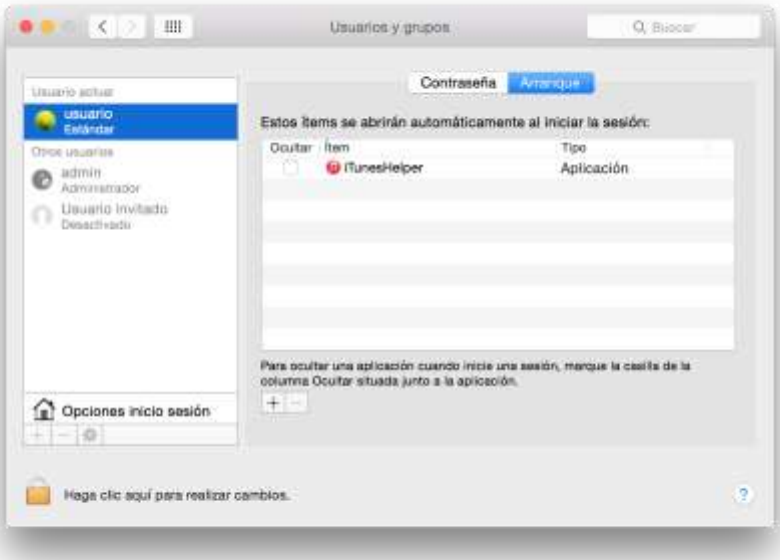
5.5.3 EJECUCIÓN DE APLICACIONES DURANTE EL INICIO O FINALIZACIÓN DE SESIÓN

339. En OS X, los elementos o Ítems de Arranque (*Login Items*) constituyen la lista de aplicaciones que serán ejecutadas durante el proceso de inicio de sesión de un usuario determinado, disponibles bajo "Preferencias del Sistema - Usuarios y grupos", tras seleccionar un usuario, desde la pestaña "Arranque" (ver siguiente imagen).

340. Desde dicha pestaña es posible visualizar las aplicaciones que serán ejecutadas cuando el usuario inicie una sesión en el equipo, y si dichas aplicaciones serán visibles o estarán ocultas, así como añadir o eliminar aplicaciones.

341. Las aplicaciones disponibles en la lista son almacenadas bajo el fichero de configuración "~/Library/Preferences/com.apple.loginitems.plist" del usuario. Los datos contenidos en este fichero (<data>…</data>) están codificados en base64.

[70] https://github.com/synack/knockknock



342. Se recomienda verificar para cada usuario, y especialmente para los usuarios administradores, la lista de Ítems de Arranque definidos y únicamente permitir la ejecución de aquellos de los que se quiere hacer uso.

343. Adicionalmente, OS X permite establecer la ejecución de tareas o *scripts* durante el inicio o la finalización de la sesión de un usuario a través de los *Login & Logout Hooks* [Ref.- 41].

344. El usuario root puede crear tareas asociadas al inicio y finalización de sesión, y éstas se ejecutarán para todos los usuarios del equipo. Mediante el siguiente comando es posible configurar la ejecución de una tarea (asociada a un script) cada vez que un usuario inicie sesión en OS X:

```
$ sudo defaults write com.apple.loginwindow LoginHook
/usr/bin/script.sh
```

345. Estas tareas son almacenadas en el fichero de configuración de la pantalla de login (loginwindow), pero no a nivel de sistema[71], sino el asociado al usuario root, y que puede ser consultado mediante los siguientes dos comandos (que son prácticamente equivalentes):

```
$ sudo defaults read com.apple.loginwindow LoginHook

$ plutil -convert xml1 -o -
/var/root/Library/Preferences/com.apple.loginwindow.plist
```

[71] El LoginHook no es almacenado en el fichero de sistema "/Library/Preferences/com.apple.loginwindow.plist".

346. Si estas tareas son creadas por usuarios estándar en sus ficheros de configuración de la pantalla de login ("~/Library/Preferences/com.apple.loginwindow.plist"), no son ejecutadas por OS X.

347. Se recomienda verificar la lista de *Login & Logout Hooks* definidos por root y únicamente permitir la ejecución de aquellos de los que se quiere hacer uso.

Nota: existen adicionalmente otras ubicaciones que pueden ser empleadas por el software malicioso (*malware*) para lograr persistencia de su código y que éste sea ejecutado en el futuro, como por ejemplo los *plug-ins* (o módulos) de Spotlight, los *plug-ins* de autorización o sistema o los *plug-ins* (o extensiones) de los navegadores web [Ref.- 41]. Estas técnicas quedan fuera del alcance de la presente guía.

5.6 EJECUCIÓN DE TAREAS PROGRAMADAS EN OS X

348. En OS X es posible programar la ejecución de tareas en un momento temporal concreto a través de launchd y de cron, siendo el primero el método oficial actualmente[72].

349. La planificación de tareas mediante launchd se lleva a cabo a través del fichero de configuración de los demonios o agentes (ver apartado "5.5. Protección del proceso de arranque de OS X"), incluyendo en el mismo la directiva "StartCalendarInterval" y cuando debe ser ejecutado.

350. Si el equipo está en estado suspendido cuando debe ejecutar una tarea de launchd, ésta se ejecutará una vez el equipo sea activado y salga de ese estado.

351. Si el equipo está apagado cuando debe ejecutar una tarea de launchd, ésta no se ejecutará hasta el siguiente momento temporal planificado.

352. La planificación de tareas a nivel de sistema mediante cron se lleva a cabo a través del fichero "/etc/crontab". La planificación de tareas a nivel de usuario mediante cron se lleva a cabo a través de la herramienta "crontab".

353. Si el equipo está en estado suspendido o apagado cuando debe ejecutar una tarea de cron, ésta no se ejecutará hasta el siguiente momento temporal planificado.

354. Se recomienda revisar cada uno de los ficheros PLIST existentes en todos los directorios asociados a los demonios y agentes de launchd (ver apartado "5.5. Protección del proceso de arranque de OS X") y verificar cuales de ellos están programados:

```
$ grep -A10 StartCalendarInterval /Library/LaunchAgents/*.plist
```

355. A modo de ejemplo, el comando previo pretende identificar agentes de usuario creados por el administrador que disponen de acciones programadas actualmente.

356. Se recomienda revisar las tareas de cron actualmente programadas por cada uno de los usuarios existentes mediante el comando "crontab -l [-u <usuario>]" (a continuación se muestra el mismo comando en formato visual o en una sóla línea de ejecución):

[72] https://developer.apple.com/library/mac/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/ScheduledJobs.html

```
$ for user in $(dscl . list /Users | grep -v '^_')
> do
> echo "- $user:"
> sudo crontab -l -u $user
> echo
> done
```

```
$ for user in $(dscl . list /Users | grep -v '^_'); do echo "- $user:";
sudo crontab -l -u $user; echo; done
```

357. Los comandos previos permiten listar el conjunto de usuarios existente[73] y verificar su fichero cron con las tareas programadas actualmente.

358. Se recomienda restringir qué usuarios disponen de la capacidad de añadir nuevas tareas programadas a través de cron mediante los ficheros "/usr/lib/cron/cron.allow" y "/usr/lib/cron/cron.deny", que permiten la creación de listas blancas o negras de usuarios autorizados y/o restringidos.

359. Por defecto, en OS X sólo existe el fichero "/usr/lib/cron/cron.deny" y únicamente contiene al usuario invitado (Guest).

5.7 USUARIOS Y GRUPOS

5.7.1 CREACIÓN DE UNA CUENTA DE USUARIO ESTÁNDAR

360. Uno de los primeros pasos que deben llevarse a cabo tras la instalación y configuración inicial de OS X es la creación de una cuenta de usuario estándar o no privilegiada con la que implementar el resto de tareas de configuración.

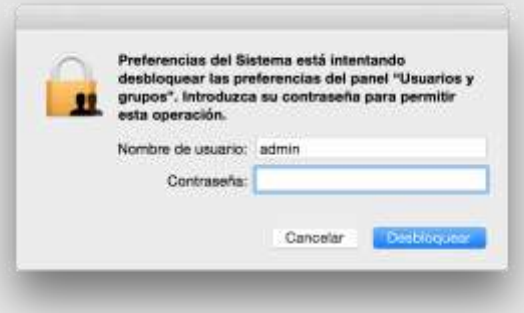
361. En este escenario, será necesario proporcionar las credenciales de la cuenta de administrador creada durante el proceso de instalación y configuración inicial cuando sean solicitadas por OS X, es decir, a la hora de llevar a cabo acciones críticas que requieren disponer de privilegios.

362. Mediante "Preferencias del Sistema - Usuarios y grupos", a través del botón "+" de la parte inferior izquierda, es posible añadir una nueva cuenta de usuario:

[73] Es posible obtener información más detallada sobre los usuarios mediante "dscacheutil -q user".

Nota: para llevar cambios a través de "Preferencias del Sistema", tanto con un usuario estándar como con un usuario administrador, es necesario pulsar en el icono del candado de la parte inferior izquierda. Esta acción desbloqueará la posibilidad de realizar cambios y ajustes en la configuración de OS X:

Tanto en el caso de emplearse un usuario estándar, como de hacer uso del usuario administrador, OS X solicitará por defecto al usuario (mediante un cuadro de diálogo) las credenciales del usuario administrador con privilegios suficientes para poder realizar dichos cambios:



Este funcionamiento por defecto es el recomendado desde el punto de vista de seguridad, por lo que no se recomienda modificarlo a través de la opción "Solicitar una contraseña de administrador para acceder a las preferencias de todo el sistema" (ver apartado "5.7.7. Solicitar contraseña de administrador para modificar preferencias del sistema").

363. Al añadir la nueva cuenta de usuario de tipo "Estándar", se debe introducir el nombre completo del usuario y de la cuenta de usuario, y se recomienda emplear una contraseña[74] local suficientemente robusta.

364. La utilidad "pwpolicy" permite definir los requisitos de la política de las contraseñas de los usuarios.

365. Por ejemplo, el siguiente comando define una política de contraseñas en OS X que establece como requisito que la contraseña tenga al menos un caracter numérico, una letra (alfa) y un símbolo, el número máximo de intentos fallidos tras el cual la cuenta de usuario será bloqueada (definido a diez en el ejemplo), y que la longitud mínima sea de 15 caracteres. El segundo comando permite verificar la política actual:

```
$ sudo pwpolicy -setglobalpolicy "maxFailedLoginAttempts=10 minChars=15
requiresNumeric=1 requiresAlpha=1 requiresSymbol=1"

$ pwpolicy -getglobalpolicy
```

366. Por defecto, OS X sugiere hacer uso de la contraseña de iCloud, tras indicar el ID de iCloud (o ID de Apple) del usuario, para el acceso local al equipo. Se recomienda independizar el acceso a OS X local de los servicios de Apple disponibles en Internet (o "en la nube"), como por ejemplo, iCloud, y no hacer uso de estas capacidades.

367. Tras pulsar el botón "Crear usuario" se añadirá la nueva cuenta a OS X, pudiendo opcionalmente seleccionar la imagen asociada a la cuenta, y empleándose el nombre de la cuenta como nombre del directorio principal o *home* (o carpeta de inicio) asociada al usuario bajo "/Users/" (por ejemplo, "/Users/usuario/"):

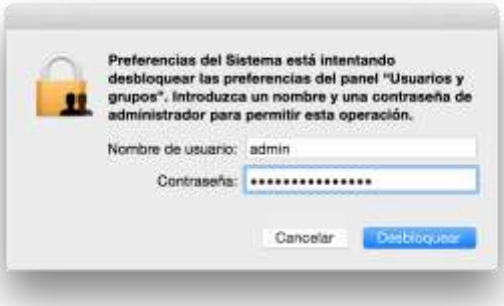
[74] La contraseña del usuario puede ser modificada posteriormente por el propio usuario o por cualquier usuario administrador: https://support.apple.com/en-us/HT202860.

368. No se recomienda añadir ninguna indicación o recordatorio de la contraseña del usuario.

Nota: queda fuera del alcance de la presente guía la capacidad de activar los controles parentales de las cuentas de usuario en OS X, ya que se considera que esta funcionalidad está asociada a un entorno más personal, y no al uso corporativo o empresarial de OS X. Igualmente, no se profundizará en las cuentas de tipo "Gestionada con controles parentales" o "Solo compartir" (ver apartado "5.13.6. Servicios compartidos"). Las nuevas cuentas de "Grupo" permiten definir grupos de usuarios en OS X para asignar controles de acceso sobre el grupo, en lugar de individualmente sobre cada usuario[75].

369. Finalmente, es necesario asegurarse de que el usuario invitado está desactivado (configuración por defecto).

370. Una vez se ha creado una cuenta de usuario estándar, se recomienda cerrar la sesión del usuario administrador, iniciar sesión en el equipo con la nueva cuenta, y llevar a cabo todas las tareas como usuario estándar. Cuando sea necesario, OS X solicitará al usuario (mediante un cuadro de diálogo) las credenciales del usuario administrador para obtener los privilegios requeridos para llevar a cabo los cambios indicados:



[75] https://support.apple.com/kb/PH18891

5.7.2 OPCIONES DE INICIO DE SESIÓN

5.7.2.1 INICIO DE SESIÓN AUTOMÁTICO

371. Desde Preferencias del Sistema - Usuarios y grupos", y en concreto desde el menú "Opciones inicio de sesión", es posible configurar diferentes aspectos de seguridad asociados al inicio de sesión por parte de los usuarios en OS X:

372. Se recomienda asegurarse de que la opción "Inicio de sesión automático" está desactivada (configuración por defecto). En caso contrario, sería posible iniciar sesión en OS X automáticamente con el usuario indicado al arrancar el equipo sin conocer su contraseña.

373. Si se activa el inicio de sesión automático, la contraseña del llavero de inicio de sesión del usuario seleccionado se almacena en el fichero "/etc/kcpassword", cifrada mediante XOR.

La clave empleada para este cifrado XOR no ha cambiado desde la versión 10.4 de OS X hasta la versión 10.10 de OS X, Yosemite.

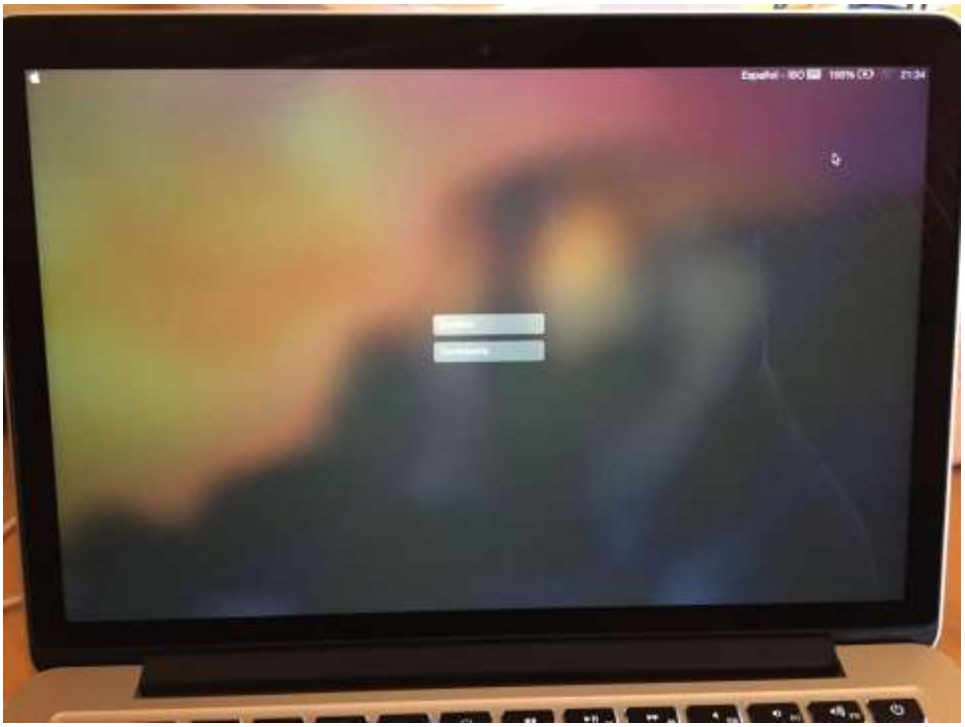
374. Este fichero sólo es accesible por root, por lo que mediante el siguiente comando, cualquier usuario administrador podría extraer la contraseña del llavero de inicio de sesión del usuario seleccionado para el inicio de sesión automático:

```
$ sudo ruby -e
'key=[125,137,82,35,210,188,221,234,163,185,31];IO.read("/etc/kcpassword"
).bytes.each_with_index{|b,i|break if key.include?(b);print
[b^key[i%key.size]].pack("U*")}'
```

375. Al desactivar esta funcionalidad, el fichero es eliminado.

5.7.2.2 PANTALLA DE INICIO DE SESIÓN O LOGIN

376. Se recomienda fijar el valor de la opción "Mostrar ventana de inicio como:" a "Nombre y contraseña". Por defecto se hace uso de la opción "Lista de usuarios", lo que facilita a un potencial atacante obtener la lista de usuarios existentes en el equipo en la pantalla de login de OS X (junto a sus imágenes de usuario asociadas):



377. En el caso de hacer uso de la opción "Lista de usuarios" (no recomendada desde el punto de vista de seguridad), existe la posibilidad de ocultar la existencia de cuentas de usuario individualmente en la pantalla de login de OS X, así como del menú de cambio rápido de usuario.

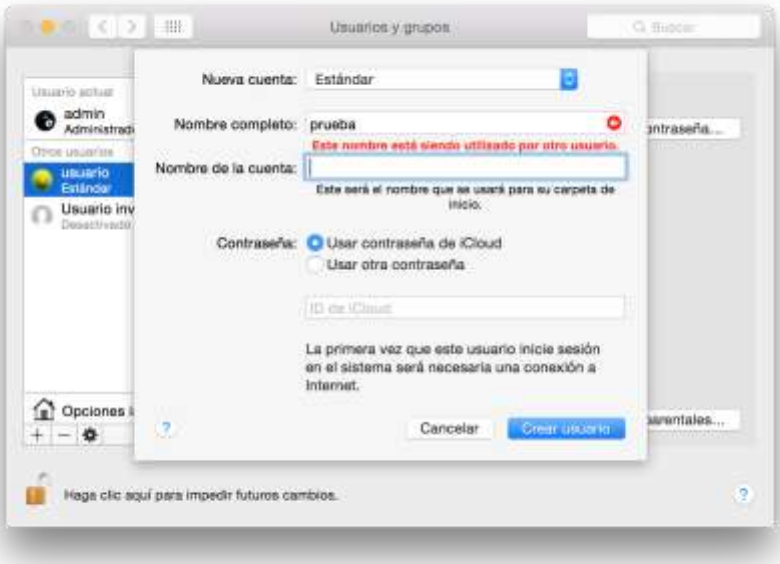
378. En el caso de hacer uso de esta opción, se recomienda ocultar las cuentas de usuario con permisos de administrador, disponiendo aún de la posibilidad de hacer uso de las mismas desde accesos remotos, como por ejemplo SSH o la funcionalidad de compartir pantalla (*Screen Sharing*); ver apartado "5.13.6. Servicios compartidos".

379. Mediante el siguiente comando es posible eliminar la presencia del usuario "admin" de la pantalla de login de OS X [Ref.- 37]:

```
$ sudo dscl . create /Users/admin IsHidden 1
```

380. En su lugar se muestra la presencia de otro usuario con el texto "Otro…", pero que no puede ser seleccionado para iniciar directamente sesión en OS X. El icono asociado solicita introducir el nombre de usuario y la contraseña en su lugar:

381. Adicionalmente, la cuenta de usuario desaparece de "Preferencias del Sistema - Usuarios y grupos", pudiendo confirmarse que existe al intentar crear otra cuenta de usuario con el mismo nombre o a través del siguiente comando:




```
$ dscl . list /Users
```

382. Esta acción puede ser revertida, haciendo que la existencia del usuario "admin" se muestre de nuevo en la pantalla de login de OS X (y en el resto de ubicaciones donde ha sido ocultada) empleando el valor "IsHidden 0"[76].

383. Adicionalmente es posible, mediante los siguientes comandos, ocultar el directorio principal o *home* del usuario en Finder, moviéndolo a un directorio oculto para Finder (como por ejemplo, "/var") y actualizando la referencia a dicho directorio, así como ocultando la carpeta pública compartida de dicho usuario [Ref.- 37]:

```
$ sudo mv /Users/admin /var/admin
$ sudo dscl . -create /Users/admin NFSHomeDirectory /var/admin
$ sudo dscl . -delete "/SharePoints/Administrador Public Folder"
```

Nota: los dos primeros comandos hacen uso del nombre corto de la cuenta del usuario ("admin"), mientras que el tercer comando hace referencia al nombre largo de la cuenta del usuario ("Administrador").

384. Se recomienda desactivar la opción "Mostrar los botones Reposo, Reiniciar y Apagar" (habilitada por defecto), con el objetivo de que un potencial atacante no pueda llevar estas acciones en el equipo desde la pantalla de login sin conocer las credenciales de un usuario válido.

385. Se recomienda activar la opción "Mostrar el menú Teclado en la ventana de inicio de sesión" (deshabilitada por defecto), ya que en algunos escenarios en los que se ha activado el cifrado completo del sistema de almacenamiento del equipo mediante FileVault, y dependiendo del valor de la contraseña seleccionada por el usuario, podría ser necesario cambiar de teclado para introducir caracteres sólo disponibles en ciertos idiomas a la hora de iniciar sesión.

Nota: para poder disponer de teclados asociados a otros idiomas en la pantalla de login de OS X no es necesario tener definidos en la sección "Teclado - Fuentes de entrada" de las "Preferencias del Sistema" varios teclados de distintos países o regiones.

386. No se recomienda activar la opción "Mostrar indicaciones de contraseña" (deshabilitada por defecto) para no proporcionar ninguna información sobre la contraseña del usuario.

387. Salvo indicación expresa, no es necesario activar la opción "Utilizar VoiceOver en la ventana de inicio de sesión" (configuración por defecto):

[76] Al eliminar la cuenta de usuario oculta se recomienda verificar que se ha eliminado su directorio principal bajo "/Users".

5.7.2.3 MENÚ DE CAMBIO RÁPIDO DE USUARIO

388. Se recomienda que la opción "Mostrar menú cambio rápido usuario como" sea desactivada (habilitada por defecto), ya que al permitirse el inicio de sesión de varios usuarios simultáneamente, unos usuarios pueden obtener información de otros (como por ejemplo los procesos en ejecución).

389. Si se desea hacer uso de la funcionalidad de cambio rápido de usuario, se recomienda que el valor de la opción "Mostrar menú cambio rápido usuario como" sea "icono" (por defecto la opción seleccionada es "nombre completo"), con el objetivo de evitar que, si un potencial atacante puede visualizar la pantalla del equipo una vez hay una sesión de usuario establecida, pueda ver en la barra de menús principal el nombre del usuario asociado a la sesión actual. Este nombre podría ser utilizado posteriormente para intentar lograr acceso al equipo.

Nota: la utilización de un servidor Open Directory o un dominio Active Directory para la autentificación de usuarios a través de la opción "Servidor de cuentas de red" y el botón "Acceder…" queda fuera del alcance de la presente guía.

5.7.2.4 MENSAJE PERSONALIZADO EN LA PANTALLA DE INICIO DE SESIÓN

390. Se recomienda mostrar un mensaje personalizado de texto en la pantalla de inicio de sesión de OS X, conteniendo por ejemplo un texto legal o de autorización de acceso al equipo asociado al propietario u organización.

391. Los siguientes comandos permiten confirmar si existe actualmente un mensaje personalizado, y establecer o borrar dicho mensaje:

```
$ defaults read /Library/Preferences/com.apple.loginwindow.plist
LoginwindowText
```

```
$ sudo defaults write /Library/Preferences/com.apple.loginwindow \
LoginwindowText "Mensaje personalizado de acceso no autorizado"

$ sudo defaults delete /Library/Preferences/com.apple.loginwindow \
LoginwindowText
```

392. Si adicionalmente se desea recibir confirmación expresa del usuario respecto a dicho mensaje durante el proceso de autentificación a través de la pantalla de inicio de sesión, se debe establecer el mensaje en el fichero "/Library/Security/PolicyBanner.txt", siendo necesario que el usuario apruebe el mensaje (pulsando en la ventana con el mismo) para poder introducir sus credenciales.

5.7.3 CONTRASEÑA MAESTRA

393. La funcionalidad que permite establecer una contraseña maestra sigue disponible en OS X Yosemite, aunque tiene sus orígenes en la primera versión de FileVault. En el caso de FileVault 2 (ver apartado "5.8.4. Cifrado completo del disco: FileVault") la contraseña maestra se emplea como una clave de recuperación institucional [Ref.- 76].

394. Desde "Preferencias del Sistema - Usuarios y grupos", y en concreto desde el botón o icono con un engranaje (a la derecha de los botones "+" y "-") se puede seleccionar "Definir contraseña maestra…", opción que permite crear una contraseña para las cuentas que hacen uso de cifrado mediante la versión original de FileVault:

395. Al activar el cifrado del equipo (ver apartado "5.8.4. Cifrado completo del disco: FileVault"), por defecto, si un usuario olvida su contraseña no será posible recuperar los datos contenidos en su directorio principal o *home* (o carpeta de inicio), salvo que se disponga de una clave de recuperación.

396. Al establecer una contraseña maestra, en el escenario descrito previamente, un administrador podría usar esta contraseña para cambiar la contraseña de cualquier usuario y poder así recuperar los datos cifrados.

397. No se recomienda añadir ninguna indicación o recordatorio de la contraseña maestra.

398. Una vez seleccionada la contraseña maestra, la opción disponible desde el botón o icono con un engranaje es modificada a "Cambiar contraseña maestra…" y permite, tras especificar la contraseña maestra actual, cambiar la contraseña maestra:

399. Tras establecer la contraseña maestra se crean los siguientes dos ficheros:

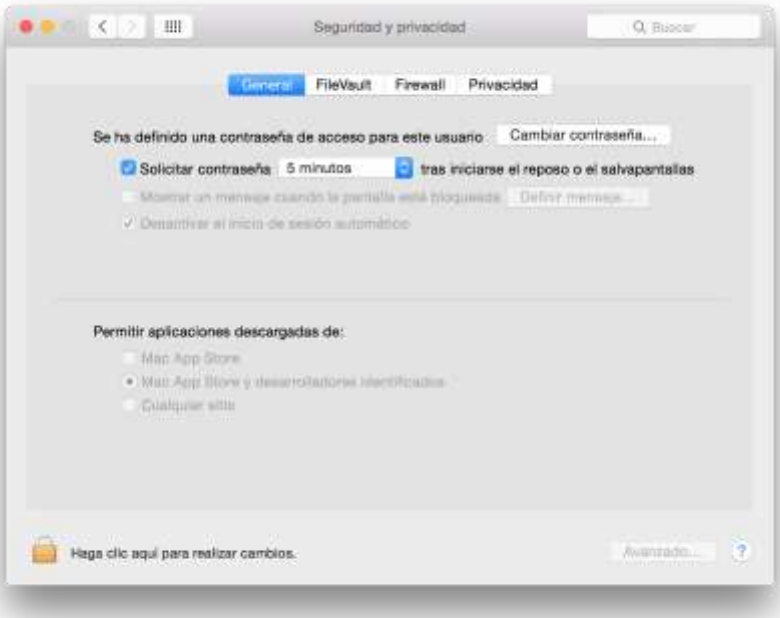
```
/Library/Keychains/FileVaultMaster.cer
/Library/Keychains/FileVaultMaster.keychain
```

400. El fichero "FileVaultMaster.keychain" debe ser copiado y almacenado en un lugar seguro, externo al equipo, ya que contiene la clave privada que permite descifrar y desbloquear el disco protegido por FileVault. Para ello debe seguirse un procedimiento basado en arrancar desde la partición de recuperación y hacer uso de una unidad de almacenamiento externa para poder acceder a una copia de este fichero [Ref.- 75].

401. OS X no proporciona ningún mecanismo en el entorno gráfico para eliminar la contraseña maestra, por lo que la única opción disponible pasa por borrar los dos ficheros indicados previamente.

5.7.4 SOLICITUD DE CONTRASEÑA

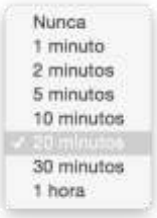
402. Desde "Preferencias del Sistema - Seguridad y privacidad", a través de la pestaña "General", es posible establecer el tiempo tras el que se solicitará la contraseña al usuario tras entrar el equipo en el estado de reposo o suspendido (*sleep*), o tras activarse el salvapantallas por ausencia de actividad (el valor por defecto es de 5 minutos):



403. Se recomienda solicitar la contraseña lo antes posible (opción "inmediatamente") una vez el equipo pasa al estado de reposo o suspendido o se activa el salvapantallas.

404. Por otro lado, debe definirse el tiempo que debe transcurrir sin actividad para que se active el salvapantallas, mediante "Preferencias del Sistema - Escritorio y salvapantallas", a través de la pestaña "Salvapantallas", empleando el parámetro "Iniciar tras:":

405. Se recomienda disminuir el tiempo de activación del salvapantallas (por defecto, 20 minutos) a un valor inferior de entre 1 y 5 minutos (1, 2 ó 5 minutos):



406. Asimismo, es necesario comprobar que la configuración de los ajustes de energía de la pantalla disponen de un temporizador con un valor superior al tiempo de activación del salvapantallas, con el objetivo de que siempre que se apague la pantalla se haya activado previamente el bloqueo del salvapantallas.

407. Desde "Preferencias del Sistema - Economizador", la opción "Apagar la pantalla tras:", tanto de la pestaña "Batería" como de la pestaña "Adaptador de corriente", muestra el tiempo sin actividad tras el cual se apagará la pantalla.

408. Este valor puede ser obtenido mediante el siguiente comando:

```
$ pmset -g | grep displaysleep
```

409. Adicionalmente y por comodidad, se recomienda configurar una de las esquinas del escritorio para poder activar el salvapantallas inmediatamente y poder hacer uso del mismo

de forma rápida y sencilla cada vez que se va a dejar el equipo desatendido, incluso aunque sólo sea temporalmente durante unos segundos[77].

410. Mediante "Preferencias del Sistema - Escritorio y salvapantallas", a través de la pestaña "Salvapantallas", empleando el botón "Esquinas activas…" (*Hot Corners*), se puede establecer (por ejemplo) que la esquina inferior izquierda permita activar el salvapantallas (por defecto ninguna de las esquinas activas tiene una acción asociada):

411. Por otro lado, esa misma pantalla de configuración general de seguridad ("Preferencias del Sistema - Seguridad y privacidad", a través de la pestaña "General") permite cambiar la contraseña del usuario actual, así como desactivar el inicio de sesión automático, aunque ambas opciones pueden llevarse a cabo también desde "Preferencias del Sistema - Usuarios y grupos" (ver apartado "5.7. Usuarios y grupos").

5.7.5 CUENTAS DE USUARIO

412. La cuenta de usuario creada por defecto por OS X durante el proceso de instalación dispone de permisos de administrador.

413. Si esta cuenta de usuario es utilizada para realizar las actividades diarias, puede ser utilizada para comprometer el equipo y acceder a funcionalidad crítica de OS X con mayor facilidad.

414. Se recomienda por tanto crear una cuenta de usuario estándar (sin privilegios) tan pronto se haya completado el proceso de instalación y configuración inicial (ver apartado "5.7.1. Creación de una cuenta de usuario estándar").

415. Esta nueva cuenta de usuario debe ser utilizada para realizar todas las actividades diarias por parte del usuario. En el caso de que esta cuenta sea comprometida, un potencial atacante

[77] https://support.apple.com/kb/PH18796

deberá encontrar alguna vulnerabilidad adicional en OS X que le permita escalar privilegios para disponer de acceso como administrador y poder realizar modificaciones críticas en el equipo.

416. Únicamente debe hacerse uso de la cuenta de usuario administrador para llevar a cabo tareas administrativas que requieren disponer de este acceso más privilegiado, como por ejemplo, la instalación de software.

417. OS X automáticamente solicitará al usuario las credenciales del usuario administrador a través de una ventana (o cuadro) de diálogo cuando sean necesarias a la hora de realizar tareas administrativas.

418. La herramienta "sysadminctl", introducida en OS X Yosemite, permite gestionar las cuentas de usuario desde un terminal, incluyendo su creación, borrado, o modificación o restablecimiento de contraseña[78].

419. Se recomienda limitar el número total de cuentas de usuario existentes en el equipo, especialmente las de tipo administrador, y verificar que la contraseña asociada a todas ellas es suficientemente robusta.

420. Por defecto, OS X permite a cualquier usuario visualiar los contenidos del directorio principal o *home* de otros usuarios. Las restricciones de OS X aplican a los contenidos dentro del directorio principal, pero no al propio directorio:

```
$ ls -l /Users
total 0
drwxr-xr-x+ 11 Guest    _guest   374 15 ene  2015 Guest
drwxrwxrwt   5 root     wheel    170 14 ene  2015 Shared
drwxr-xr-x+ 18 admin    staff    612 11 ago 13:17 admin
drwxr-xr-x+ 40 usuario  staff   1360 12 ago 10:12 usuario

$ id
uid=502(usuario) gid=20(staff) groups=...

$ ls -l /Users/admin
total 0
drwx------+  3 admin  staff   102 11 ene  2015 Desktop
drwx------+  4 admin  staff   136 17 feb  2015 Documents
drwx------+  5 admin  staff   170 31 may 12:29 Downloads
...
drwx---r-x+  4 admin  staff   136 11 ene  2015 Public
$
```

421. Con el objetivo de limitar la identificación de información, ficheros y documentos sensibles pertenecientes a otros usuarios, se recomienda limitar los permisos asociados al directorio principal de cada usuario mediante el siguiente comando, que debe repetirse para todos y cada uno de los usuarios existentes:

[78] Estas capacidades son complementadas por la herramienta "unsetpassword", disponible para cuentas de usuario administrador, también introducida en OS X Yosemite.

```
$ sudo chmod -R og-rwx /Users/admin

$ ls -ld /Users/admin/
drwx------+ 18 admin  staff  612 11 ago 13:17 /Users/admin/
```

422. Tras modificar los permisos, los usuarios no podrán hacer uso de las carpetas públicas ("Public") de otros usuarios, debiendo usar "/Users/Shared" para la compartición de ficheros en su lugar.

5.7.6 ALMACENAMIENTO DE LAS CONTRASEÑAS DE USUARIO

423. OS X almacena las contraseñas de inicio de sesión de las cuentas de usuario bajo el directorio "/var/db/dslocal/nodes/Default/users", en un fichero PLIST para cada usuario, como por ejemplo "usuario.plist", "admin.plist" o "root.plist". Tanto el directorio como los ficheros sólo son accesibles por root.

424. Desde la versión 10.8 de OS X, Mountain Lion, se hace uso de PBKDF2 con numerosas iteraciones para la derivación de las claves, junto al uso de una semilla (o *salt*), y empleando un *hash* SHA512.

425. A través del siguiente comando es posible obtener el *hash* asociado a la contraseña de un usuario concreto, que puede ser empleado para llevar a cabo auditorías de seguridad sobre la fortaleza de las contraseñas seleccionadas por los usuarios, con herramientas como DaveGrohl[79] o John the Ripper[80]:

```
$ sudo defaults read /var/db/dslocal/nodes/Default/users/usuario.plist
ShadowHashData | tr -dc 0-9a-f|xxd -r -p|plutil -convert xml1 - -o -
```

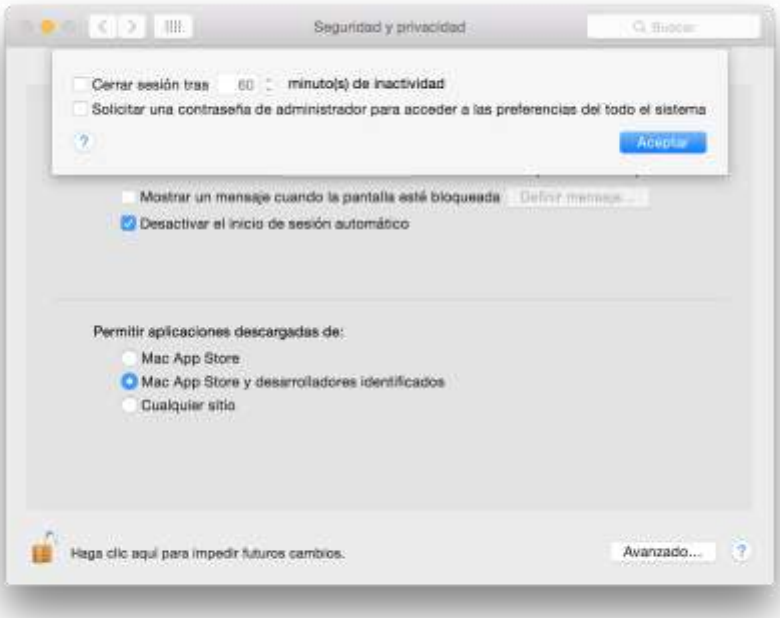
426. Debido a las protecciones asociadas a la capacidad de computo necesaria en el proceso de obtención de las contraseñas (*cracking*) mediante ataques de diccionario o fuerza bruta, al hacer uso de PBKDF2, se recomienda desde el punto de vista de seguridad seleccionar contraseñas robustas y suficientemente largas.

5.7.7 SOLICITAR CONTRASEÑA DE ADMINISTRADOR PARA MODIFICAR PREFERENCIAS DEL SISTEMA

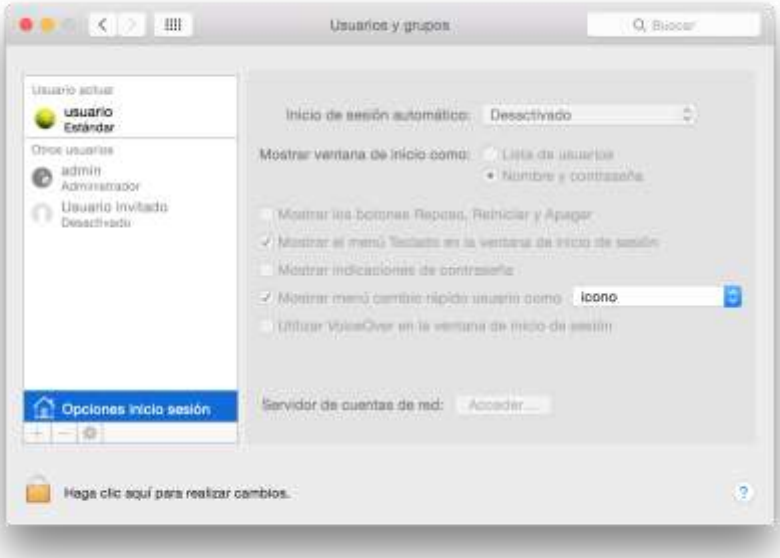
427. Desde "Preferencias del Sistema - Seguridad y privacidad" (en cualquiera de las pestañas), a través del botón "Avanzado…" disponible en la parte inferior derecha, es posible solicitar la contraseña de un usuario administrador para acceder a las preferencias de todo el sistema, a través de la opción asociada:

[79] https://github.com/octomagon/davegrohl (http://davegrohl.org/DaveGrohl-2.1.zip)

[80] La opción "-j" de la herramienta DaveGrohl porporciona los *hashes* en un formato (ml) que puede ser procesado por John the Ripper.



428. Se recomienda activar esta opción (deshabilitada por defecto), con el objetivo de forzar que para poder modificar cualquier sección de preferencias críticas del sistema, individualmente, sea necesario siempre introducir las credenciales de un usuario administrador. Será necesario introducir las credenciales para cada una de las secciones de preferencias críticas:



429. La configuración por defecto (con esa opción deshabilitada) no permite modificar la configuración de ciertas preferencias críticas del sistema, como por ejemplo "Usuarios y grupos", "Seguridad y privacidad", "Fecha y hora" o "Controles parentales". Sin embargo, cuando un usuario administrador introduce sus credenciales para llevar a cabo una modificación en unas de esas secciones, todas las secciones son desbloqueadas globalmente, por lo que el usuario podría modificar ajustes de cualquier otra sección.

430. Este es el comportamiento teórico de OS X, pero se ha verificado que en OS X 10.10 Yosemite el comportamiento por defecto es el mismo tanto si está como si no está activa esa opción de configuración, y en todos los casos es necesario introducir las credenciales de administrador en cada uno de los paneles individualmente (escenario similar a si la opción estuviese activa).

431. Cuando un panel de configuración es desbloqueado, ese panel específico permanece desbloqueado, pero el resto de paneles de configuración siguen bloqueados.

5.8 MECANISMOS DE PROTECCIÓN Y TECNOLOGÍAS DE SEGURIDAD EN OS X

432. OS X dispone de diferentes mecanismos de protección y tecnologías de seguridad que son añadidas progresivamente, o mejoradas, con la incorporación de nuevas versiones o nuevas actualizaciones del sistema operativo [Ref.- 87].

433. Los siguientes apartados detallan las características, funcionamiento y configuración de algunas de estas tecnologías.

5.8.1 TECNOLOGÍAS GENÉRICAS DE SEGURIDAD

434. OS X implementa tecnologías de seguridad ampliamente adoptadas en la industria, como por ejemplo XD (*eXecute Disabled*), que permite establecer qué secciones de memoria almacenan datos y cuales almacenan código, y por tanto, pueden ser ejecutadas, o ASLR (*Address Space Layout Randomization*), qué modifica de forma aleatoria las posiciones de memoria en la que los diferentes componentes o secciones de las aplicaciones estarán ubicados durante su ejecución, con el objetivo de dificultar la explotación de vulnerabilidades.

435. Las capacidades de protección de XD están disponibles en OS X desde la versión 10.4.4, la primera disponible para la plataforma Intel, protegiendo inicialmente únicamente la pila (*stack*). Posteriormente, en OS X 10.5 se añadió también la protección de XD a otros segmentos de memoria, como el *heap*, para los ejecutables de 64 bits inicialmente (y para los de 32 bits posteriormente).

436. Las capacidades de protección de ASLR están disponibles en OS X desde la versión 10.7 (julio de 2011), tanto para ejecutables de 32 como de 64 bits[81], y aplican tanto al kernel y a sus extensiones, como a los entornos o *frameworks* del sistema. Sin embargo, para hacer uso de estas capacidades las aplicaciones deben haber sido compiladas con el flag PIE (*Position Independent Executable*). Es posible verificar si una aplicación dispone del flag PIE mediante el siguiente comando:

```
$ otool -hv /Applications/Safari.app/Contents/MacOS/Safari
/Applications/Safari.app/Contents/MacOS/Safari:
Mach header
magic cputype cpusubtype  caps    filetype ncmds sizeofcmds  flags
MH_MAGIC_64  X86_64        ALL LIB64     EXECUTE    19       1336
    NOUNDEFS DYLDLINK TWOLEVEL PIE
```

[81] https://stackoverflow.com/questions/12824045/what-exactly-is-randomized-with-aslr-in-macos-x-and-ios

437. Estas tecnologías son empleadas tanto para proteger las aplicaciones como el propio kernel del sistema operativo, en diferentes niveles y aplicando a distintos componentes de la arquitectura de OS X, según la versión de sistema operativo [Ref.- 83].

5.8.2 GATEKEEPER Y CUARENTENA DE ARCHIVOS

438. OS X, desde la versión OS X Lion 10.7.5, proporciona capacidades de validación de archivos a través de su firma digital y políticas de cuarentena [Ref.- 39] mediante Gatekeeper, y que afectan a las aplicaciones con capacidades de descargar ficheros desde Internet (por ejemplo, Safari), o desde fuentes externas, como por ejemplo, ficheros adjuntos a un correo electrónico (por ejemplo, Mail).

439. Debe tenerse en cuenta que la funcionalidad original de cuarentena de archivos descargados fue introducida en la versión 10.5 (Leopard) de OS X, encargada de notificar y pedir autorización al usuario a la hora de abrir un fichero descargado desde Internet mediante una aplicación compatible, como Safari o Mail.

440. La tecnología Gatekeeper pretende evitar o mitigar la distribución de software malicioso (*malware*) en OS X, complementando las capacidades de detección de software malicioso de XProtect [Ref.- 36] y las de cuarentena de archivos, y permitiendo al usuario restringir qué aplicaciones podrán ejecutar en el equipo en función de su firma digital.

441. La configuración de Gatekeeper está disponible a través de "Preferencias del Sistema - Seguridad y privacidad", mediante la pestaña "General" y la opción "Permitir aplicaciones descargadas de:":

442. La opción más restrictiva, "Mac App Store"[82], sólo permite la ejecución de aplicaciones legítimas distribuidas a través de la App Store y que por tanto han sido verificadas antes de ser aceptadas y han sido firmadas por Apple. Adicionalmente, si hubiera algún problema posteriormente con una aplicación, Apple puede retirarla rápidamente de la App Store.

443. Sin embargo, si una aplicación ya instalada tiene asociado un certificado (de Gatekeeper) que ha sido revocado, ésta podrá continuar siendo ejecutada.

444. Por otro lado, debe tenerse en cuenta que una aplicación aprobada por Apple en la App Store podría posteriormente descargar contenido externo malicioso y evitar los controles impuestos por Gatekeeper, ya que esta tecnología sólo verifica el Bundle de la aplicación (es decir, todos los contenidos del paquete de software original asociado a la aplicación), pero no componentes externos.

445. Por ejemplo, las aplicaciones que emplean referencias externas relativas a librerías dinámicas (dylib, *dynamic library*) pueden ser manipuladas[83], añadiendo al fichero ".dmg" del paquete de software de la aplicación las librerías que esta intentará cargar, pero pudiendo emplear librerías maliciosas o no firmadas. Este fichero puede ser distribuido en Internet y podrá ser abierto incluso con la opción más restrictiva de Gatekeeper seleccionada [Ref.- 40][84].

446. A partir de la versión 10.10.4 de OS X Yosemite Gatekeeper también verifica las librerías externas cargadas adicionalmente al Bundle de la aplicación [Ref.- 43].

Nota: la herramienta DHS, *Dylib Hijack Scanner*, permite identificar tanto aplicaciones susceptibles de ser vulnerables a inyección de librerías dinámicas (dylib), como escenarios de ataque dónde se está aprovechando esta vulnerabilidad, mediante el escaneo y análisis de todos los procesos en ejecución y del sistema de ficheros completo ("*full system scan*").

URL: https://objective-see.com/products/dhs.html

447. Debido a la existencia de este escenario de ataque, se recomienda descargar todas las aplicaciones y software a través de canales de comunicación seguros, mediante HTTPS y una correcta validación del certificado digital asociado.

448. Se recomienda establecer la opción intermedia (habilitada por defecto), "Mac App Store y desarrolladores identificados", ya que proporciona un equilibrio adecuado entre seguridad y usabilidad.

449. Para ser considerado como desarrollador identificado por Apple, los desarrolladores pueden obtener un identificador (ID) de desarrollador de Apple y emplearlo para firmar sus aplicaciones y distribuirlas fuera de la App Store. Este ID permite a Gatekeeper bloquear aplicaciones de desarrolladores que han distribuido software malicioso y verificar la integridad de las aplicaciones, es decir, que no han sido manipuladas desde que fueron firmadas por el desarrollador.

[82] La tienda oficial de aplicaciones para Mac de Apple se denomina Mac App Store, para diferenciarla de la tienda oficial de aplicaciones para iOS (iPhone, iPad, etc) de Apple, denominada App Store. Por simplificar, en adelante se usará el término App Store.

[83] La herramienta "otool" con la opción "-l" permite identificar aplicaciones potencialmente vulnerables.

[84] Las téncicas de injección de librerías dinámicas (dylib hijacking) pueden ser utilizadas para otros tipos de ataques, como por ejemplo, evitar la política de seguridad del cortafuegos personal aprovechando los permisos asignados a otra aplicación.

450. La opción desaconsejada desde el punto de vista de seguridad, "Cualquier sitio", deshabilita prácticamente por completo la funcionalidad ofrecida por Gatekeeper y permite la ejecución de cualquier aplicación en OS X, creadas por desarrolladores desconocidos (es decir, que no tienen un ID de desarrollador de Apple).

451. Incluso con esta opción seleccionada, las aplicaciones firmadas con un ID de desarrollador que hayan sido modificadas posteriormente no podrán ser abiertas en OS X. El mensaje de error mostrado es "<Nombre de la aplicación> está dañado y no puede abrirse. Debería trasladarlo a la Papelera.".

Nota: la herramienta *Task Explorer*, similar al Monitor de Actividad, permite explorar todos los procesos en ejecución en OS X e identificar su firma (Apple, desarrolladores de terceros o ninguna - muy útil para verificar el estado de Gatekeeper), las librerías dinámicas (dylib) cargadas, los ficheros abiertos, las conexiones de red, tiene integración con VirusTotal, etc.

La herramienta proporciona la posibilidad de ver el árbol jerárquico de procesos o identificar rápidamente el software que no ha sido firmado por Apple (#apple) o por desarrolladores de terceros (#nonapple), mediante la etiqueta "#unsigned".

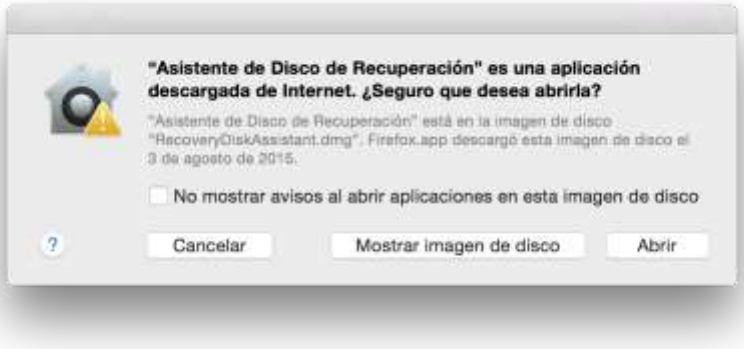
URL: https://objective-see.com/products/taskexplorer.html

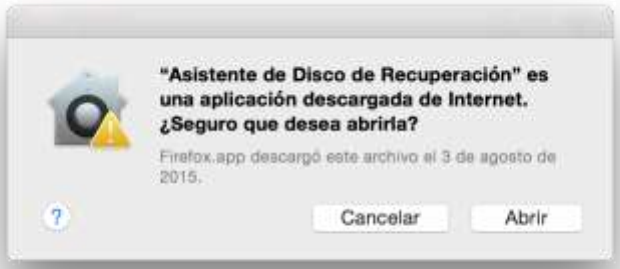
452. La verificación de la firma asociada al ID de desarrollador sólo aplica a las aplicaciones descargadas de Internet. Las aplicaciones obtenidas de otras fuentes como servidores de archivos y unidades externas, salvo que hubieran sido descargadas originalmente de Internet y aún dispongan de los atributos de cuarentena, están excluidas de Gatekeeper.

453. Gatekeeper, por tanto, está integrado con la funcionalidad de cuarentena de archivos, y sus mecanismos de protección solo aplican a ficheros descargados de Internet mediante una aplicación con capacidades de cuarentena de archivos.

454. Las aplicaciones que hacen uso de las capacidades de cuarentena de archivos, como por ejemplo Safari, Mensajes, y Mail, asignan los atributos de cuarentena de archivos a los ficheros descargados: fecha, hora y un registro de la procedencia del archivo.

455. A la hora de abrir por primera vez un fichero con atributos de cuarentena asociados, OS X informa al usuario de su procedencia a través de un cuadro de diálogo (o mensaje de alerta) y le solicita autorización para abrirlo:





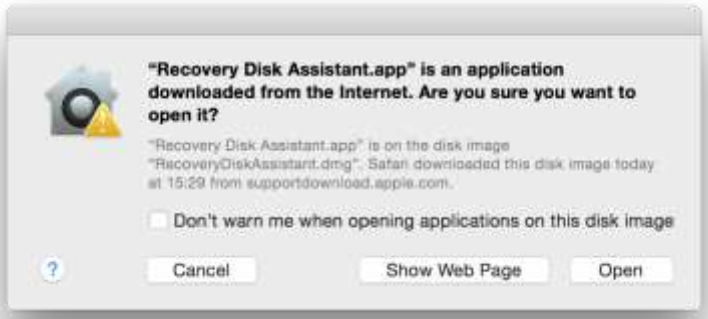
456. Los atributos de cuarentena de archivos pueden ser inspeccionados desde un terminal. Si la salida del comando "ls -l" muestra el símbolo "@" tras los permisos tradicionales de Unix, indica que el fichero dispone de atributos extendidos. Mediante el comando "ls -l@" es posible consultar la información general de dichos atributos:

```
$ ls -l fichero.dmg
-rw-r--r--@ 1 usuario  staff  123456 Apr 1 08:00 fichero.app

$ ls -l@ fichero.dmg
-rw-r--r--@ 1 usuario  staff  123456 Apr 1 08:00 fichero.app
    com.apple.metadata:kMDItemDownloadedDate         53
    com.apple.metadata:kMDItemWhereFroms      214
    com.apple.quarantine     61
```

457. Finalmente, mediante el comando "xattr" (*extended attributes*) es posible consultar todos los contenidos de los atributos extendidos asociados al archivo, tanto en formato hexadecimal como ASCII, como por ejemplo y en el caso de Gatekeeper, los atributos de cuarentena asociados (ejemplo del "RecoveryDiskAssistant.dmg" descargado con Safari):

```
$ xattr -l RecoveryDiskAssistant.dmg
com.apple.metadata:kMDItemDownloadedDate:
00000000  62 70 6C 69 73 74 30 30 A1 01 33 41 BB 78 DE C1  |bplist00..3A.x..|
00000010  53 33 98 08 0A 00 00 00 00 00 00 01 01 00 00 00  |S3..............|
00000020  00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00  |................|
00000030  00 00 00 00 13                                   |.....|
00000035
com.apple.metadata:kMDItemWhereFroms:
00000000  62 70 6C 69 73 74 30 30 A1 01 5F 10 A7 68 74 74  |bplist00.._..htt|
00000010  70 3A 2F 2F 73 75 70 70 6F 72 74 64 6F 77 6E 6C  |p://supportdownl|
00000020  6F 61 64 2E 61 70 70 6C 65 2E 63 6F 6D 2F 64 6F  |oad.apple.com/do|
00000030  77 6E 6C 6F 61 64 2E 69 6E 66 6F 2E 61 70 70 6C  |wnload.info.appl|
00000040  65 2E 63 6F 6D 2F 41 70 70 6C 65 5F 53 75 70 70  |e.com/Apple_Supp|
00000050  6F 72 74 5F 41 72 65 61 2F 41 70 70 6C 65 5F 53  |ort_Area/Apple_S|
00000060  6F 66 74 77 61 72 65 5F 55 70 64 61 74 65 73 2F  |oftware_Updates/|
00000070  4D 61 63 5F 4F 53 5F 58 2F 64 6F 77 6E 6C 6F 61  |Mac_OS_X/downloa|
00000080  64 73 2F 30 34 31 2D 32 30 30 31 2E 32 30 31 31  |ds/041-2001.2011|
00000090  30 38 30 38 2E 51 46 43 31 64 2F 52 65 63 6F 76  |0808.QFC1d/Recov|
000000A0  65 72 79 44 69 73 6B 41 73 73 69 73 74 61 6E 74  |eryDiskAssistant|
000000B0  2E 64 6D 67 08 0A 00 00 00 00 00 00 01 01 00 00  |.dmg............|
000000C0  00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00  |................|
000000D0  00 00 00 00 00 B4                                |......|
000000d6
com.apple.quarantine: 0002;55c8a741;Safari.app;A6EE899D-97A8-4B7D-9013-
    E31674AE4BAA
```

458. Los atributos de cuarentena asociados a un archivo descargado de Internet incluyen cuando fue descargado (fecha), desde qué URL y qué aplicación lo descargó, información empleada en el cuadro de diálogo de Gatekeeper (en su versión en inglés para el ejemplo previo de "xattr"):



459. Es posible ver el valor de los diferentes atributos en formato PLIST, como por ejemplo la fecha, tras convertirlos desde hexadecimal a formato PLIST binario (mediante "xxd") y posteriormente a formato XML (mediante "plutil"):

```
$ xattr -px com.apple.metadata:kMDItemDownloadedDate
    RecoveryDiskAssistant.dmg | xxd -r -p | plutil -convert xml1 - -o -

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://...">
<plist version="1.0">
<array>
    <date>2015-08-10T13:29:37Z</date>
</array>
</plist>
```

460. Sólo el usuario que descargó el archivo, y el usuario administrador, tienen la capacidad de eliminar los atributos de cuarentena de archivos. Por ejemplo, es posible eliminar el atributo que indica desde dónde se descargo el archivo con el primer comando, o eliminar todos los atributos extendidos del archivo con el segundo comando:

```
$ xattr -d com.apple.metadata:kMDItemWhereFroms fichero.dmg

$ xattr -c fichero.dmg
```

461. Una vez el fichero ya ha sido abierto la primera vez, OS X no volverá a solicitar autorización al usuario. El motivo es que los atributos de cuarentena del archivo son modificados tras la aceptación del usuario durante el primer acceso, reflejando esa autorización en futuras interacciones con el fichero:

```
$ xattr -l Recovery\ Disk\ Assistant.app/
com.apple.quarantine: 0001;55bf7af7;Firefox.app;

<Tras aceptar poder abrirlo la primera vez>

$ xattr -l Recovery\ Disk\ Assistant.app/
com.apple.quarantine: 0061;55bf7af7;Firefox.app;
```

462. Gatekeeper almacena una lista blanca de *hashes* (denominados CDHash) en el fichero de base de datos SQLite 3.x "/var/db/gkopaque.bundle/Contents/Resources/gkopaque.db", es decir, el conjunto total de *hashes* asociados a las aplicaciones de confianza identificadas por Apple a lo largo del tiempo.

463. La tabla "whitelist" contiene un total de 36.292 entradas únicas para el campo "current" en la versión 10.10 de OS X Yosemite, mientras que contiene 39.003 entradas en la versión 10.10.5 de OS X Yosemite:

```
$ sqlite3 /var/db/gkopaque.bundle/Contents/Resources/gkopaque.db
"select count(distinct current) from whitelist;"

39003
```

464. El valor del CDHash de una aplicación puede ser obtenido a través de la utilidad "codesign" y como resultado, para cualquier aplicación, es posible determinar si su CDHash está incluido en la lista blanca de Gatekeeper:

```
$ codesign -dvvv Recovery\ Disk\ Assistant.app/ 2>&1 | grep CDHash
CDHash=f94be0ec29b225a466d65da583d38b3252411242

$ sqlite3 /var/db/gkopaque.bundle/Contents/Resources/gkopaque.db "select
quote(current), quote(opaque) from whitelist" | grep -i
f94be0ec29b225a466d65da583d38b3252411242

X'F94BE0EC29B225A466D65DA583D38B3252411242'|X'D88F20EE4494F1A757303971D24
    049FFC3ECEEA9'
```

465. La herramienta "spctl" (*Security Assessment, SecAssesment system policy security*) permite confirmar desde un terminal si una aplicación será aceptada por Gatekeeper, y por tanto ejecutada, o si será potencialmente rechazada por algún motivo concreto[85]:

```
$ spctl -vva aplicacion.app
```

[85] Muchas aplicaciones de OS X pueden aparecer como rechazadas con el motivo "obsolete resource envelope", que habitualmente, pero no siempre, indica que se hace uso de un envoltorio de firma de versión 1, en lugar de versión 2 (disponible desde OS X 10.9), o que se usan reglas de omisión personalizadas ("custom omit rules"). Esta información está disponible mediante "codesign -vv fichero". Pesé a ello, pueden pasar los criterios de validación de Gatekeeper y ser ejecutadas en función de la lista blanca descrita previamente (http://indiestack.com/2014/10/gatekeepers-opaque-whitelist/).

```
aplicacion.app: accepted
source=Apple System
origin=Software Signing

$ spctl -vva otra-aplicacion.app
otra-aplicacion.app: rejected
source=obsolete resource envelope
origin=Developer ID Application: <Third-Party> (ID)
```

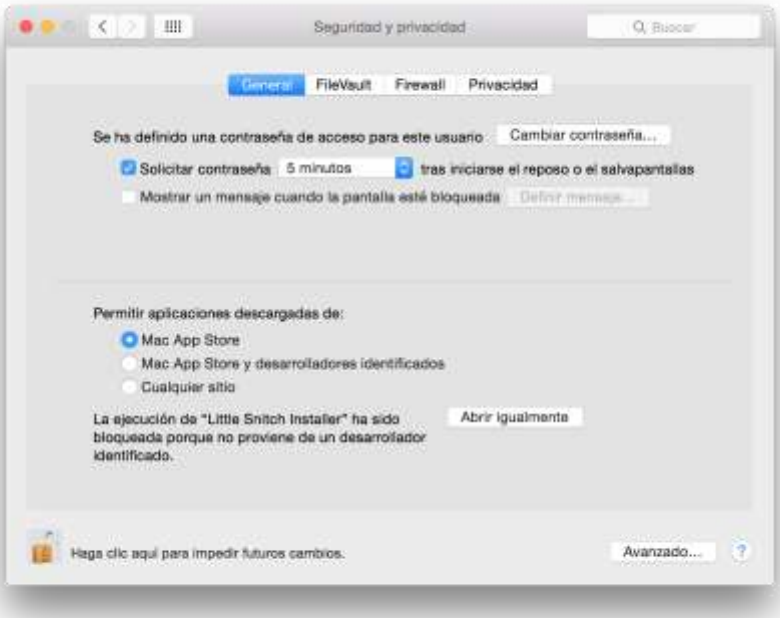
466. La herramienta "spctl" permite gestionar Gatekeeper desde un terminal, y entre otros, conocer su estado, así como habilitarlo (en su opción mas restrictiva) o deshabilitarlo:

```
$ sudo spctl --master-enable
$ spctl --status
assessments enabled
$ sudo spctl --master-disable
```

467. En el caso de que el usuario esté seguro que una aplicación descargada de Internet es de confianza, incluso con Gatekeeper activo con la opción más restrictiva, existe la posibilidad de abrir la aplicación, evitando así las protecciones de Gatekeeper:

468. Por un lado, desde "Preferencias del Sistema - Seguridad y privacidad", en la pestaña "General" aparecerá el texto "La ejecución de '<aplicación>' ha sido bloqueada porque no proviene de un desarrollador identificado." (correspondiente a la última aplicación

bloqueada por Gatekeeper - tras pulsar el botón "Aceptar" del cuadro de diálogo mostrado por Gatekeeper). El botón "Abrir igualmente" permite abrir dicha aplicación:



469. Por otro lado, se puede seleccionar la aplicación con el botón derecho y pulsar en la opción "Abrir". Esta acción mostrará la primera vez el cuadro de diálogo con el mensaje de alerta pero con un nuevo botón "Abrir", que permite abrir aplicaciones no permitidas por defecto. En ocasiones posteriores la aplicación podrá ser abierta normalmente[86]:

470. Mediante "spctl" es también posible gestionar, añadir o eliminar, desde un terminal excepciones a la lista de aplicaciones permitidas por Gatekeeper:

```
$ sudo spctl --add [--label "AppsPermitidas"] aplicacion.app
$ sudo spctl --remove [--label "AppsPermitidas"] aplicacion.app
```

[86] https://support.apple.com/kb/PH18658

```
$ sudo spctl --enable --label "AppsPermitidas"
$ sudo spctl --disable --label "AppsPermitidas"
```

471. Las aplicaciones pueden ser gestionadas individualmente, o por grupos o categorías mediante el uso de etiquetas (o *labels*) [Ref.- 46].

472. Por último, el comando "spctl" permite obtener la lista de aplicaciones permitidas por Gatekeeper, incluyendo su *hash* (o CDHash), y si la autorización es para proceder a su instalación o ejecución. Las aplicaciones que han sido autorizadas explícitamente por el usuario aparecen bajo la categoría "UNLABELED" [Ref.- 46]:

```
$ spctl --list

$ spctl --list --label "AppsPermitidas"

$ spctl --list | grep -i UNLABELED
```

5.8.3 XPROTECT: SOFTWARE MALICIOSO (*MALWARE*)

473. Adicionalmente a Gatekeeper, a la hora de abrir un fichero con atributos de cuarentena asociados, OS X comprueba si contiene software malicioso (*malware*) conocido. En caso afirmativo, se mostrará una alerta al usuario con el texto "(Nombre del archivo) dañará su ordenador." [Ref.- 36]:

474. Esta tecnología se denomina XProtect y está disponible desde la versión OS X Snow Leopard 10.6.7.

475. XProtect, por tanto, está integrado con la funcionalidad de Gatekeeper, por lo que de nuevo, la detección de software malicioso sólo aplica a las aplicaciones descargadas de Internet. Las aplicaciones obtenidas de otras fuentes como servidores de archivos y unidades externas, están excluidas de XProtect.

476. Apple mantiene una lista con definiciones de software malicioso conocido (lista negra) que es empleada durante el proceso de verificación de los ficheros descargados.

477. Esta lista se almacena localmente en OS X en el fichero "XProtect.plist" y se actualiza periódicamente. Es posible verificar la fecha de la última actualización del fichero con las definiciones de software malicioso mediante el siguiente comando:

```
$ ls -l
/System/Library/CoreServices/CoreTypes.bundle/Contents/Resources/XProtect
.plist
```

478. Adicionalmente, para limitar la exposición frente a amenazas, XProtect también define controles respecto a las versiones de los *plug-ins* o módulos asociados a los navegadores web. El siguiente fichero contiene la lista negra de *plug-ins*, incluyendo la versión mínima permitida de cada uno de ellos (por ejemplo, para Java, Flash, etc):

```
$ less
/System/Library/CoreServices/CoreTypes.bundle/Contents/Resources/XProtect
.meta.plist
```

479. Desde OS X 10.9 en adelante, incluyendo Yosemite, Apple ha integrado el proceso de actualización de XProtect en el proceso estándar de actualizaciones de sistema operativo. Como resultado, la utilidad de actualización de XProtect ya no está disponible[87] ("/usr/libexec/XProtectUpdater") y debe utilizarse la utilidad "softwareupdate" en su lugar.

480. El siguiente comando, que hace uso de una opción no documentada[88] [89], permite forzar la verificación y actualización del fichero de definición de software malicioso de XProtect:

```
$ sudo softwareupdate --background-critical
```

481. A la vez que se ejecuta este comando es posible ver las acciones llevadas a cabo por OS X a través del log de actividad: "`$ tail -f /var/log/install.log`"[90].

482. Es posible deshabilitar la actualización de XProtect (opción desaconsejada desde el punto de vista de seguridad) desactivando la opción "Instalar archivos de datos del sistema y actualizaciones de seguridad" (habilitada por defecto) disponible a través de "Preferencias del Sistema - App Store".

483. Debido a que XProtect se basa en la definición y verificación de listas negras de software malicioso, se han identificado vulnerabilidades que permiten recompilar el código de un espécimen de *malware*, y al cambiar el *hash*, evitar XProtect. En algunos casos, incluso cambiando el nombre del *malware* ha sido suficiente para evitar XProtect [Ref.- 41].

484. Adicionalmente a la identificación y bloqueo de software malicioso Apple ha actualizado en diferentes ocasiones XProtect para bloquear la utilización de versiones antiguas y vulnerables de los *plug-ins* de Java y Flash[91].

[87] http://macops.ca/monitoring-apples-XProtect-meta-feed-for-changes/

[88] https://derflounder.wordpress.com/2014/12/17/forcing-xprotect-blacklist-updates-on-mavericks-and-yosemite/

[89] https://managingosx.wordpress.com/2013/04/30/undocumented-options/

[90] http://macops.ca/os-x-admins-your-clients-are-not-getting-background-security-updates/

485. Complementariamente, desde la versión 10.8.3 de OS X, se dispone de la tecnología MRT, *Malware Removal Tool*. MRT (disponible como descarga individual o en las actualizaciones de OS X[92]) ejecuta automáticamente de fondo y verifica, y elimina, software malicioso detectado en el equipo, y que haya podido comprometer el mismo evitando los mecanismos de protección previos, o por otras vías, como por ejemplo explotando vulnerabilidades en los *plug-ins* del navegador web, como Java o Flash.

486. Al igual que XProtect, MRT es efectivo únicamente frente a especímenes de *malware* conocidos. MRT notifica al usuario si detecta *malware*, pero en caso contrario, es transparente, al no disponer de ningún interfaz gráfico de usuario (GUI) asociado.

5.8.4 CIFRADO COMPLETO DEL DISCO: FILEVAULT

487. La tecnología FileVault, y en concreto FileVault 2[93] [Ref.- 71], la segunda versión de esta tecnología disponible actualmente en OS X Yosemite e introducida por Apple en OS X Lion tras un proceso de rediseño significativo, proporciona capacidades de cifrado para la totalidad del sistema de almacenamiento principal o disco duro del equipo.

488. La versión original de FileVault (también denominada *Legacy FileVault*), disponible desde OS X 10.3 Panther, cifraba únicamente el directorio principal o *home* del usuario. Para ello, OS X hacía uso de una imagen de disco cifrada que se empleaba como volumen para el directorio principal del usuario.

489. FileVault 2 cifra el volumen completo empleado por OS X para el arranque del equipo (partición raíz). Para ello, la información necesaria para descifrar el disco es obtenida de una partición de arranque alternativa (de tipo "Apple_Boot"), no cifrada (denominada *helper partition* [Ref.- 87]). En concreto, OS X emplea la partición de recuperación identificada con la etiqueta "Recovery HD" (ver apartado "5.4.4. Recuperación de OS X").

490. FileVault hace uso de cifrado empleando XST-AES-128 con claves de 256 bits.

491. Asimismo, FileVault simplifica el proceso de eliminación de los datos del equipo, ya que la funcionalidad de borrado instantáneo (*instant wipe*[94]) elimina las claves de cifrado del equipo (haciendo de manera efectiva que los datos ya no sean accesibles), y a continuación lleva a cabo un proceso de borrado en profundidad sobre los datos del disco [Ref.- 72].

492. Si un potencial atacante obtiene acceso físico al equipo, por ejemplo porque éste haya sido perdido o robado, podría disponer de acceso a los datos almacenados en el mismo. Los mecanismos de cifrado completo del sistema de almacenamiento disponibles en OS X mediante FileVault permiten proteger el equipo frente a esta amenaza.

493. Debe tenerse en cuenta que los mecanismos de cifrado de FileVault tienen especial relevancia cuando el equipo está apagado. Si el equipo se encuentra en el estado suspendido, aún podría disponerse potencialmente de acceso a la información protegida por FileVault.

---

[91] Se dispone de detalles sobre las versiones mínimas permitidas para los *plug-ins* bloqueados en los ficheros de configuración asociados, como por ejemplo, http://configuration.apple.com/configurations/macosx/xprotect/3/clientConfiguration.plist.

[92] Flashback malware removal tool: https://support.apple.com/en-us/HT202456

[93] La presente guía, por simplificar, usa el término FileVault para referirse a la versión 2 de esta tecnología, o FileVault 2.

[94] http://www.apple.com/osx/what-is/security/

494. FileVault hace uso de la contraseña del usuario (o los usuarios activos en FileVault) empleada para el inicio de sesión para cifrar el disco.

495. FileVault puede ser activado accediendo a "Preferencias del Sistema - Seguridad y privacidad", a la pestaña "FileVault", mediante el botón "Activar FileVault…":

496. Alternativamente se puede activar FileVault mediante el comando "sudo fdesetup enable".

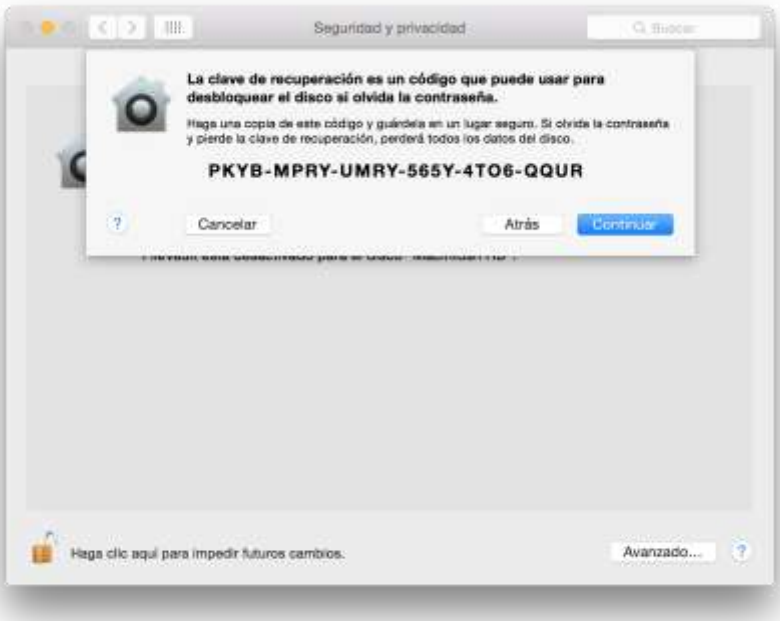
497. Durante el proceso de activación de FileVault, se debe crear una clave de recuperación, que debe ser almacenada en un lugar seguro, externo al equipo. Esta clave de recuperación se puede emplear para desbloquear el disco cifrado si se olvida la contraseña del usuario (o para deshabilitar FileVault).

498. Alternativamente, FileVault sugiere al usuario hacer uso de su cuenta de iCloud, es decir, de los servidores de Apple, para poder restablecer la clave de cifrado de FileVault (ver siguiente imagen).

499. El usuario debe decidir cual de las dos alternativas desea utilizar durante el proceso de activación.

500. Desde el punto de vista de seguridad, se recomienda de manera general encontrar el equilibrio entre seguridad y funcionalidad, evitando el uso de servicios de terceros para tareas críticas asociadas a la seguridad, como por ejemplo, las capacidades de iCloud para restablecer la clave de cifrado de FileVault.

501. Si se selecciona crear una clave de recuperación, el asistente de activación de FileVault mostrará el valor en pantalla, compuesto por 6 grupos de 4 caracteres alfanuméricos (números y letras mayúsculas):



502. El disco es cifrado con la contraseña de inicio de sesión de uno o varios usuarios, que a su vez deben ser empleadas para descifrar o desbloquear el disco durante el proceso de arranque del equipo.

503. Por tanto, durante el proceso de activación de FileVault es necesario activar todos los usuarios que dispondrán de la capacidad de desbloquear el disco, mediante el botón "Activar usuario…" de cada uno de ellos (o hacerlo posteriormente para algunos de ellos):


Seguridad y privacidad
Para desbloquear el disco, cada usuario debe introducir su contraseña.
admin
Administrador
Activar usuario...
usuario
Activar usuario...
Cancelar
Atrás
Continuar
Haga clic aquí para impedir futuros cambios.
Avanzado...


Seguridad y privacidad
usuario
Usuario estándar
La introducción de la contraseña de esta cuenta permitirá a este usuario desencriptar todos los archivos del disco de arranque.
Contraseña:
Cancelar
Aceptar
Cancelar
Atrás
Continuar
Haga clic aquí para impedir futuros cambios.
Avanzado...

504. Se recomienda activar al menos el usuario administrador ("admin"), para poder hacer uso del mismo en situaciones de emergencia, y activar también el usuario estándar principal ("usuario"), encargado de arrancar el equipo y hacer uso del mismo habitualmente:

505. El último paso requiere reiniciar el equipo para comenzar con el proceso de cifrado. Mientras se lleva a cabo el cifrado completo del disco (al estar conectado el ordenador a una toma de corriente o electricidad) es posible hacer uso del equipo. Todo el proceso de activación de FileVault se puede llevar a cabo con un usuario estándar, siendo necesario introducir las credenciales de administrador en este último paso únicamente.

506. Desde "Preferencias del Sistema - Seguridad y privacidad - FileVault" es posible realizar un seguimiento del proceso de cifrado, pudiendo verificarse que está activo para el disco de arranque y que se ha configurado una clave de recuperación, y mostrándose el tiempo estimado restante para completar el proceso de cifrado. Una vez se completa el proceso aparece el mensaje "Encriptación finalizada":

507. Sin la clave de recuperación ni la contraseña del usuario no será (teóricamente) posible descifrar los contenidos del disco.

508. FileVault, a partir de OS X 10.9, permite verificar si la clave de recuperación es válida mediante el siguiente comando, una vez el cifrado del disco se ha completado (FDE hace referencia a *Full Disk Encryption*), que devolverá "true" en caso afirmativo:

```
$ sudo fdesetup validaterecovery
Enter the current recovery key: ...
true
```

509. La utilidad "fdesetup" permite llevar a cabo la gestión de FileVault en OS X desde un terminal, especialmente en entornos empresariales, incluyendo capacidades para su activación o desactivación, conocer su estado (incluyendo el porcentaje completado), añadir o eliminar usuarios de FileVault, gestionar las claves de recuperación (personales e institucionales), etc [Ref.- 74]. La utilidad permite proporcionar las opciones de configuración u obtener las respuestas en formato PLIST, para automatizar el proceso de configuración.

510. Por ejemplo, el siguiente comando permite obtener todos los usuarios activos en FileVault, incluyendo el nombre de usuario y su UUID (*Universally Unique Identifier* o identificador único de usuario, en ocasiones referenciado como GUID, *Generated UID*[95]). Es posible obtener la lista general de usuarios y su UUID en OS X (independiente de FileVault) con el segundo comando mostrado:

```
$ sudo fdesetup list
admin,<admin-UUID>
usuario,<usuario-UUID>

$ dscl /Search -list /Users GeneratedUID | grep -v '^_'
```

511. En versiones previas de FileVault no era posible cambiar la clave de recuperación sin cifrar de nuevo el disco, pero en OS X Yosemite, desde el terminal y mediante el siguiente comando, es posible cambiar la clave de recuperación del usuario. Como resultado se generará una nueva clave de recuperación y la clave previa dejará de ser válida:

```
$ fdesetup changerecovery -personal
```

512. Las cuentas de usuario nuevas que son añadidas después de activar FileVault en OS X se activarán automáticamente como usuarios de FileVault (visibles mediante el comando "fdesetup list" previo). Si no se desea que estas nuevas cuentas de usuario de OS X sean activadas como usuarios de FileVault, es necesario eliminarlas con el siguiente comando:

[95] Los UUID (o GUID) emplean un formato de 8-4-4-4-12 caracteres hexadecimales.

```
$ sudo fdesetup remove -user <otro_usuario>
```

513. La única indicación en el interfaz gráfico de usuario de OS X de que el usuario está activo en FileVault se obtiene en la nueva pantalla de inicio de sesión durante el proceso de arranque.

514. Como resultado de haber activado FileVault, el proceso de arranque normal del equipo mostrará una nueva pantalla de inicio de sesión o *login* (EFI-login), previa al arranque (*pre-boot*), que permite autentificarse a cualquiera de los usuarios activos en FileVault y descifrar el disco de arranque de OS X:

515. La pantalla de inicio de sesión de FileVault automáticamente traslada las credenciales introducidas por el usuario, tras descifrar el disco, a la pantalla de inicio de sesión estándar de OS X (*password-forwarding* [Ref.- 73]), con el objetivo de que el usuario no tenga que introducir en dos ocasiones las mismas durante el proceso de arranque e inicio de sesión en el equipo.

516. La nueva pantalla de inicio de sesión de FileVault, por defecto, muestra las cuentas de usuario activas en FileVault, de manera similar a como lo haría la pantalla de inicio de sesión estándar cuando la opción "Mostrar ventana de inicio como: Lista de usuarios" está habilitada (ver apartado "5.7.2.2. PANTALLA DE INICIO DE SESIÓN"), opción desaconsejada desde el punto de vista de seguridad.

517. La pantalla de inicio de sesión de FileVault es gestionada durante el proceso de arranque por el firmware (o EFI) del equipo (cuyos recursos están disponibles bajo "/usr/standalone/i386/EfiLoginUI")[96]. Se dispone de una versión en caché de los recursos de

[96] https://www.lostinsecurity.com/blog/2015/08/28/recovery-hd-y-ficheros-efire/

la pantalla de inicio de sesión de FileVault o del EFI bajo "/System/Library/Caches/com.apple.corestorage/EFILoginLocalizations/*.efires".

La modificación de las propiedades de "loginwindow" y la restauración de los ficheros de caché permite, entre otros, establecer el idioma de entrada o mostrar un mensaje de texto en la pantalla de inicio de sesión de FileVault[97] (opción recomendada si se desea mostrar un texto legal o de autorización en la pantalla de arranque del equipo al estar FileVault activo; ver apartado "5.7.2.4. MENSAJE PERSONALIZADO EN LA PANTALLA DE INICIO DE SESIÓN").

518. Sin embargo, las imágenes asociadas a cada cuenta de usuario sí cambian en la pantalla de inicio de sesión de FileVault al ser modificadas en OS X, ya que aunque la pantalla fue creada y configurada en el momento de activar FileVault, se sincroniza con los cambios realizados en OS X posteriormente.

519. Este comportamiento asociado a la pantalla de inicio de sesión de FileVault, donde se desvela la lista de usuarios en lugar de los campos de entrada de usuario y contraseña (recomendado desde el punto de vista de seguridad), no puede ser modificado.

520. Si se realizan tres intentos de acceso fallido en la pantalla de inicio de sesión de FileVault, o si se pulsa el icono con una interrogación, aparece un mensaje que indica que se puede hacer uso de la clave de recuperación. Tras pulsar el triángulo asociado a dicho mensaje, se muestra un campo de entrada para introducir la clave de recuperación [Ref.- 73]:

[97] https://derflounder.wordpress.com/2013/06/19/enabling-filevault-2-pre-boot-login-screen-functions-from-the-command-line/

521. Si se desbloquea el disco cifrado mediante la clave de recuperación, la pantalla de inicio de sesión estándar mostrará un asistente que permite seleccionar una nueva contraseña de inicio de sesión para el usuario (asumiendo que no se recuerda la contraseña previa, motivo por el que se empleó la clave de recuperación), y que también requerirá actualizar la contraseña del llavero (en este caso sí es necesario conocer la contraseña previa del usuario para actualizar la contraseña del llavero, y en caso contrario, será necesario crear un nuevo llavero; ver apartado "5.4.4.2. TERMINAL DESDE EL MODO DE RECUPERACIÓN"):

522. Adicionalmente, es posible incrementar la seguridad de FileVault en equipos que gestionan información muy sensible forzando la eliminación de las claves de cifrado de la memoria del equipo cuando este pasa al estado suspendido, así como forzando el proceso de hibernación en lugar del proceso de reposo o suspensión (*sleep* o *standby*):

```
$ sudo pmset -a destroyfvkeyonstandby 1
$ sudo pmset -a hibernatemode 25
```

523. OS X hace uso del EFI para almacenar las claves de cifrado de FileVault y restaurar el estado previo del equipo desde el modo suspendido de manera transparente[98]. Los dos comandos previos permiten minimizar el riesgo de que las claves de cifrado puedan ser obtenidas mientras el equipo se encuentra en el estado suspendido.

[98] https://github.com/drduh/OS-X-Yosemite-Security-and-Privacy-Guide

524. En el caso de ser ejecutados, las claves de FileVault serán eliminadas del firmware del equipo, y al restaurar el equipo desde el modo suspendido será necesario proporcionar la contraseña de FileVault para disponer de acceso al disco y a sus contenidos.

5.8.4.1 CIFRADO DE UNIDADES O DISCOS EXTERNOS

525. Adicionalmente, FileVault y OS X puede también ser empleado para llevar a cabo el cifrado completo de discos duros y unidades de almacenamiento externas, como por ejemplo unidades de memoria USB externas o las copias de seguridad de Time Machine.

526. Desde el Finder, tras selecciona la unidad o disco externo en la columna de la izquierda, mediante el botón derecho es posible utilizar la opción "Encriptar '<nombre de unidad>'…":

527. Como resultado se mostrará un asistente que permite establecer la contraseña de cifrado, que debe ser suficientemente robusta. El campo "Indicación de contraseña" es obligatorio, sin embargo, y dado que no se recomienda añadir ninguna indicación o recordatorio de la contraseña del usuario, se sugiere introducir el carácter de espacio en blanco en el mismo:

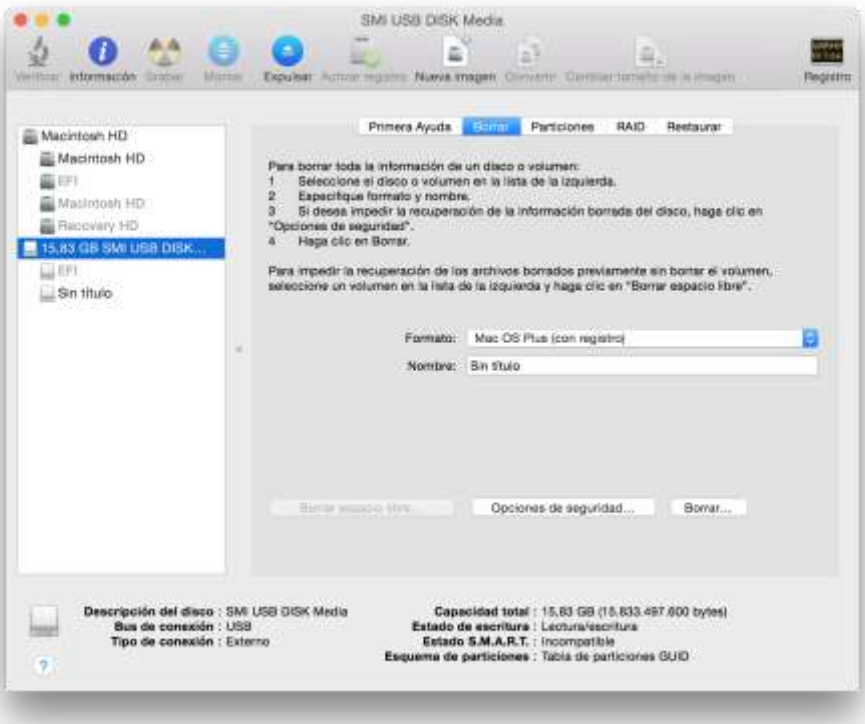
528. Al pulsar el botón "Encriptar disco" se comenzará el proceso de cifrado, sin ninguna indicación adicional. Es posible confirmar que el proceso ha comenzado mediante el indicador (o led) de actividad del propio disco. Desde OS X, únicamente pulsando el botón derecho sobre el disco o unidad externa, se puede ver el texto "Desencriptando '<nombre de unidad>'…" en color gris que (aunque es un mensaje confuso, ya que se está cifrando y no descifrando el disco) indica que el proceso sigue activo:

529. Es posible confirmar que se ha completado el proceso cuando en su lugar aparece el mensaje "Desencriptar '<nombre de unidad>'…" (ver imagen superior derecha).

530. Una vez cifrado, la próxima vez que se conecte el disco o unidad externa, se solicitará al usuario la contraseña para proceder a descifrarlo (desbloquearlo) y poder acceder a sus contenidos:

531. Con el objetivo de proteger el disco o unidad externa, y solicitar la contraseña cada vez que se haga uso del mismo, no se recomienda marcar la casilla "Guardar esta contraseña en mi llavero".

532. Para poder cifrar unidades o discos externos es necesario que hagan uso de un esquema de particiones GPT (tabla de particiones GUID o *GUID Partition Table*[99]), por lo que puede ser necesario formatear la unidad o disco previamente cumpliendo estos requisitos:



533. Alternativamente se pueden cifrar ficheros individualmente en OS X mediante la utilización de una imagen de disco, o contenedor de ficheros, cifrado. Esta imagen puede ser creada

[99] https://www.lostinsecurity.com/blog/2015/08/26/sobre-guids-gpt-y-otros-temas-de-interes/

mediante la "Utilidad de Discos", y deberá ser montada y descifrada para poder acceder a sus contenidos[100].

5.8.5 SANDBOX

534. OS X dispone de tecnologías de *sandbox* (o aislamiento) de las aplicaciones, con el objetivo de asegurarse que las aplicaciones solo llevan a cabo las acciones esperadas, aislándolas de otros componentes críticos del sistema, de los datos de usuario y/o de otras aplicaciones.

535. Si una aplicación es comprometida por software malicioso, el *sandbox* restringe qué componentes se ven afectados.

536. Las capacidades de *sandbox* de OS X están disponibles por defecto en Safari, en concreto en el visor de ficheros PDF integrado y en los *plug-ins*, como Java, Flash, QuickTime, etc, así como en otras aplicaciones, como por ejemplo la Mac App Store, Mensajes, Calendario, Contactos, Diccionario, Photo Booth, vistas rápidas (*Quick Look Previews*), Notas, Recordatorios, Mail y FaceTime.

537. El *sandbox* de OS X proporciona un nivel de seguridad adecuado siempre que no se identifiquen vulnerabilidades a nivel de kernel que permitan evitar sus mecanismos de protección [Ref.- 41], al gestionarse desde el kernel por el subsistema kauth [Ref.- 87].

538. El tipo de acciones permitidas y controles de acceso (acceso al sistema de ficheros, a la red, a iCloud, a ciertos componentes hardware, etc) asociados a una aplicación depende de los *entitlements* solicitados por la misma, declarados en el fichero PLIST del *bundle* de la propia aplicación.

539. Durante los últimos años se han identificado numerosas vulnerabilidades en el kernel de OS X, por ejemplo por parte del Proyecto Cero de Google [Ref.- 42] (reflejadas mediante el texto "OS X"), que han sido resueltas por Apple en las diferentes versiones y actualizaciones del sistema operativo, como por ejemplo el *issue* 92 resuelto en OS X Yosemite 10.10.2[101].

5.8.6 FIRMA Y VERIFICACIÓN DE APLICACIONES Y DEL KERNEL

540. OS X dispone de mecanismos para firmar digitalmente las aplicaciones y verificar en tiempo de ejecución dichas firmas. Si la aplicación ha sido modificada y no es posible comprobar la firma por parte del cargador de OS X, se finalizará la ejecución del proceso asociado.

541. El mecanismo de verificación de código comprueba si existe una firma digital asociada a las aplicaciones antes de ejecutarlas, pero si no se dispone de firma, la aplicación es ejecutada igualmente. Por tanto, es sencillo evitar este mecanismo de protección mediante la manipulación de una aplicación, simplemente eliminando su firma [Ref.- 41].

542. Las capacidades de firma digital de código son empleadas por OS X en diferentes funcionalidades del sistema operativo, desde el *sandbox* de las aplicaciones, pasando por Gatekeeper y los controles de acceso a los llaveros, hasta el cortafuegos de aplicaciones.

[100] http://www.howtogeek.com/183826/how-to-create-an-encrypted-file-container-disk-image-on-a-mac/

[101] https://support.apple.com/en-us/HT204244

Nota: el análisis de la funcionalidad y de todas las capacidades de la firma digital de código en OS X, orientadas principalmente a desarrolladores de aplicaciones para OS X, queda fuera del alcance de la presente guía. Se dispone de una visión detallada de estos mecanismos de seguridad en la "Technical Note TN2206: OS X Code Signing In Depth" [Ref.- 43].

543. Adicionalmente, desde OS X Mavericks, el código del kernel del sistema operativo, así como de las extensiones de kernel, debe estar firmado para poder ser ejecutado, con el objetivo de evitar la ejecución de no autorizado en el nivel de más privilegios del sistema operativo (*ring 0* o kernel).

544. Sin embargo, la verificación de firmas del kernel y sus extensiones se lleva a cabo en OS X desde código que ejecuta a nivel de usuario (*ring 3*) dentro del proceso "kextd" ("/usr/libexec/kextd"). Si un potencial atacante dispone de permisos de root, podría deshabilitar este mecanismo de seguridad y modificar las extensiones de kernel actualmente cargadas, o cargar el código de nuevas extensiones de kernel no firmadas a través del comando "kextload" [Ref.- 41].

545. Adicionalmente, se podría llevar a cabo la carga de extensiones de kernel mediante un cargador de kernel manipulado que no haga uso de "kextd" y que no verifique la firma de las mismas [Ref.- 41].

546. Las vulnerabilidades reflejadas previamente denotan la importancia de limitar quién dispone de privilegios de root (o administrador) en OS X, con el objetivo de evitar su explotación a nivel de kernel.

547. Las vulnerabilidades mencionadas a lo largo de la presente guía que permiten obtener privilegios de root en OS X, como por ejemplo RootPipe o DYLD_PRINT_TO_FILE (ver apartado "5.3.5. Caso práctico: Vulnerabilidades en OS X"), tienen por tanto un mayor impacto debido a las debilidades mencionadas y existentes actualmente en la arquitectura de OS X.

5.8.6.1 FIRMA DE EXTENSIONES DE KERNEL

548. En OS X Yosemite Apple introdujo *kext signing*, un nuevo mecanismo de seguridad que comprueba la firma digital de las extensiones de kernel (kext, *kernel extensions*) y los drivers, con el objetivo de verificar su integridad.

549. Si se modifica uno de estos elementos, la extensión o driver no será cargado por OS X Yosemite.

550. Aunque está completamente desaconsejado desde el punto de vista de seguridad, es posible deshabilitar está verificación de la firma de las extensiones de kernel desde el modo de recuperación (ver apartado "5.4.4. Recuperación de OS X").

551. Para ello es necesario establecer el parámetro "kext-dev-mode=1" en el proceso de arranque desde un terminal:

```
$ sudo nvram boot-args=kext-dev-mode=1
```

552. Igualmente, desde un terminal, mediante el comando "nvram boot-args" es posible confirmar si la verificación de la firma de las extensiones de kernel está o no habilitada.

553. Si se recibe un mensaje de error "Error getting variable…" indica que no hay ningún parámetro (o argumento) fijado para el proceso de arranque, por lo que la protección está habilitada. Si hubiera algún parámetro definido, debe verificarse que es diferente al descrito previamente.

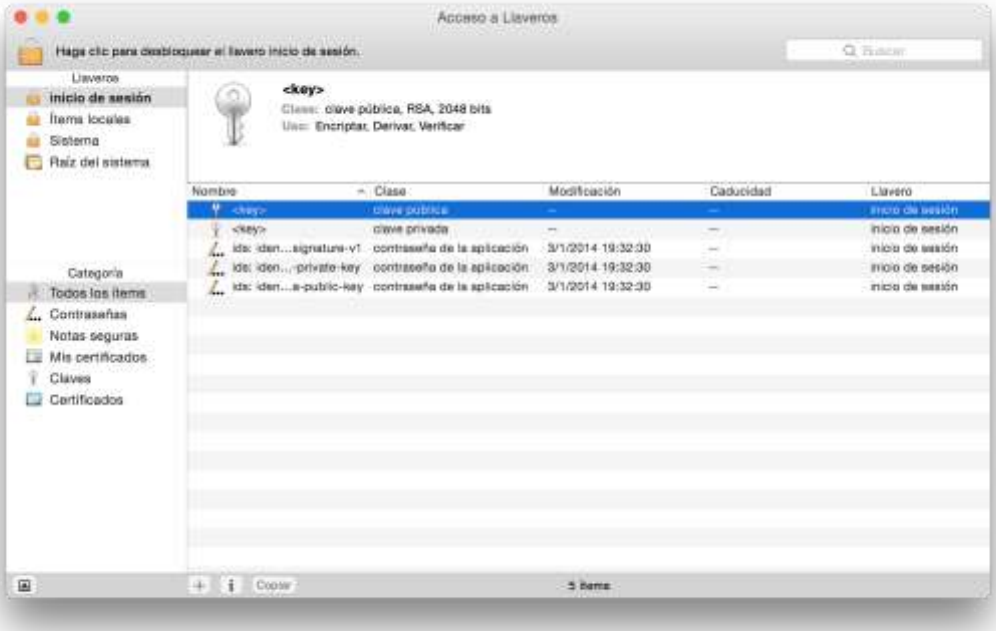
554. Si el parámetro "kext-dev-mode=1" está actualmente definido en la variable "boot-args", puede ser eliminado mediante el siguiente comando, considerando que no hay ningún otro parámetro definido para dicha variable[102]:

```
$ sudo nvram -d boot-args
```

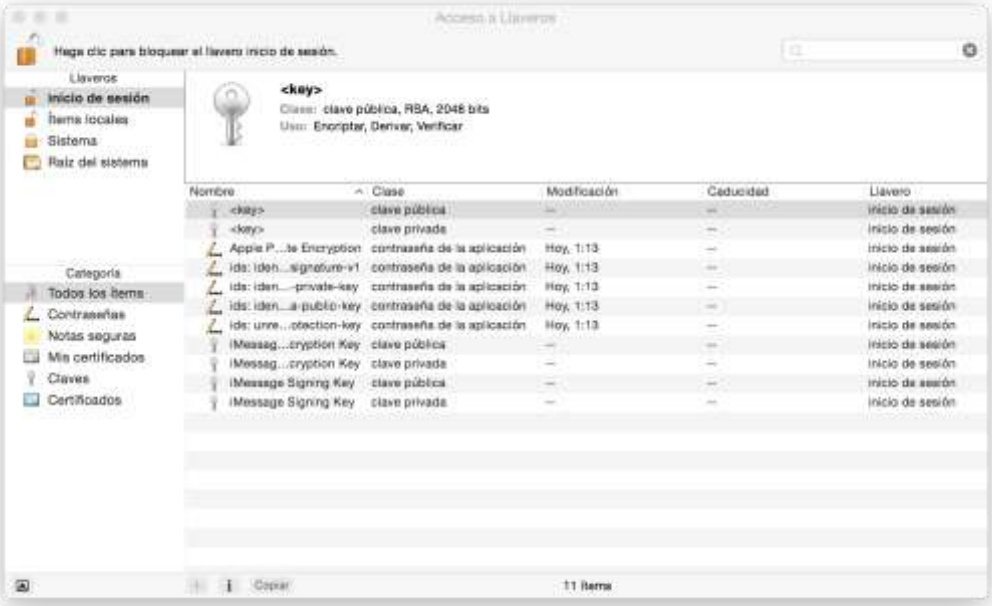
5.8.7 ACCESO A LLAVEROS

555. La funcionalidad de "Acceso a Llaveros" (*Keychain Access*) disponible desde la carpeta "Utilidades" de OS X, dentro de la carpeta "Aplicaciones", proporciona un almacén para guardar credenciales, contraseñas, claves, certificados y otra información sensible.

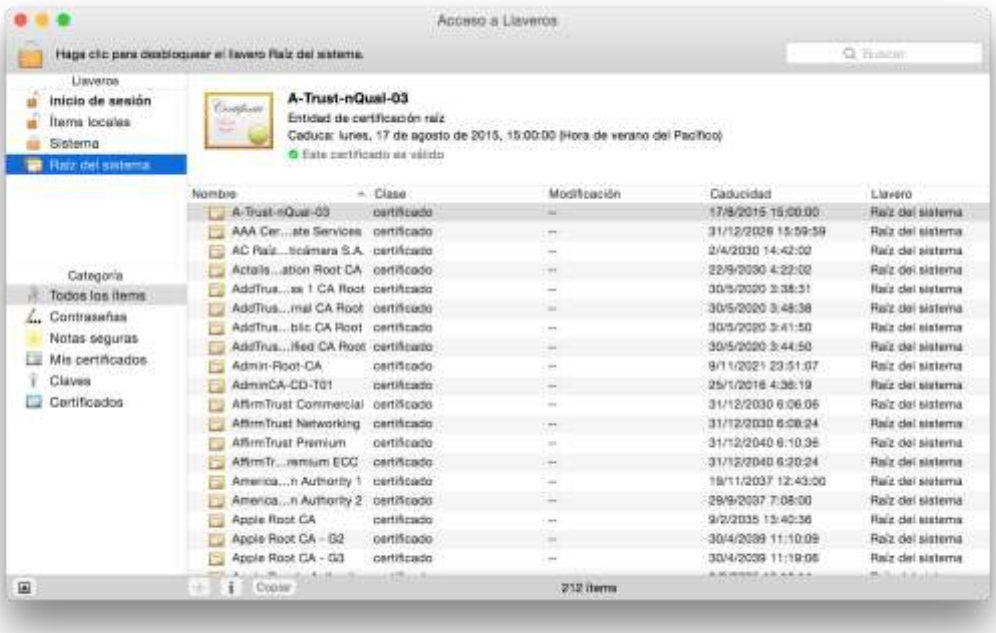
556. Por defecto se dispone de tres llaveros, que en realidad corresponden a ficheros cifrados dónde se almacena la información sensible: inicio de sesión (login), ítems locales, y sistema. Adicionalmente se muestra el repositorio de autoridades certificadoras raíz de confianza ("Raíz del sistema"):



[102] En el caso en el que hubiese otros parámetros de arranque definidos, sería necesario establecer el valor de la variable "boot-args" con estos, pero omitiendo el parámetro "kext-dev-mode=1".



557. La sección "Categoría" de la parte izquierda refleja los tipos de elementos que pueden ser almacenados en los llaveros: contraseñas, notas seguras, certificados, claves, etc:



558. Se recomienda verificar el conjunto total de autoridades certificadoras de confianza existentes por defecto en OS X (por ejemplo, 200 en OS X 10.10.5), y eliminar aquellas en las que no se confíe mediante los siguientes comandos:

```
$ echo "00 11 22 ... FF" | tr -d ' '
001122...FF
```

```
$ sudo security delete-certificate -t -Z 001122...FF
/System/Library/Keychains/SystemRootCertificates.keychain
```

559. Para ello, es necesario previamente obtener el *hash* SHA1 del certificado digital a eliminar a través de la utilidad "Acceso a Llaveros", copiando su valor desde la parte inferior de la ventana con la información detallada del certificado[103].

560. Para cada elemento protegido por el llavero es posible especificar una política de control de acceso, que define qué aplicaciones pueden acceder a ese elemento, si se solicita confirmación por parte del usuario antes de permitir el acceso al elemento, o si incluso se solicita al usuario la contraseña del llavero para permitir el acceso:

561. La tercera opción es la más segura y la recomendada desde el punto de vista de seguridad a la hora de proteger información sensible y crítica a través del llavero, debiendo siempre encontrar el equilibrio adecuado entre seguridad y usabilidad.

562. El fichero asociado al llavero de inicio de sesión del usuario está disponible en su directorio principal o *home*, bajo "~/Library/Keychains/login.keychain".

563. El llavero de ítems locales está disponible bajo "/~Library/Keychains/<GUID>/", donde "GUID" (*Generated UID*) es un identificador único creado por OS X. Dentro de esta carpeta se encuentran, entre otros, los ficheros "keychain-2.db" (base de datos SQLite) y "user.kb".

564. El fichero asociado al llavero de sistema está disponible en "/Library/Keychains/System.keychain".

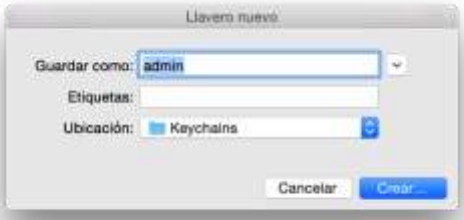
El fichero asociado al llavero de FileVault está disponible en "/Library/Keychains/FileVaultMaster.keychain" (ver apartado "5.7.2.4. MENSAJE PERSONALIZADO EN LA PANTALLA DE INICIO DE SESIÓN").

565. El fichero "/Library/Keychains/apsd.keychain" está asociado al *Apple Push notification Service Daemon*.

[103] https://github.com/drduh/OS-X-Yosemite-Security-and-Privacy-Guide

566. El fichero asociado al llavero con las autoridades certificadoras ráiz del sistema está disponible en "/System/Library/Keychains/SystemRootCertificates.keychain".

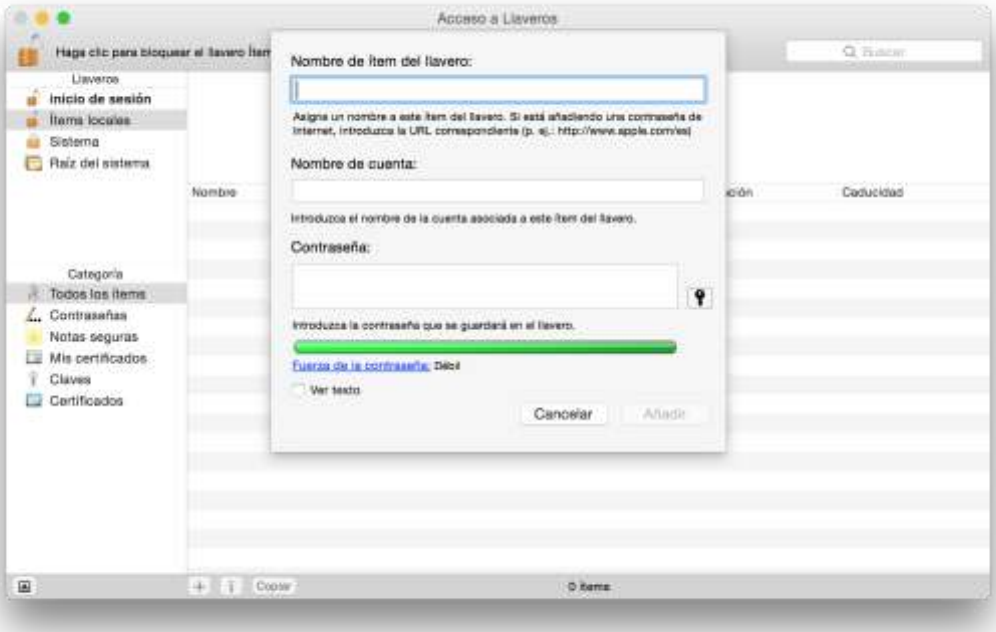
567. Adicionalmente, existe la posibilidad de crear nuevos llaveros, independientes del llavero por omisión de inicio de sesión, a través del menú "Archivo - Nuevo llavero…" de "Acceso a Llaveros":

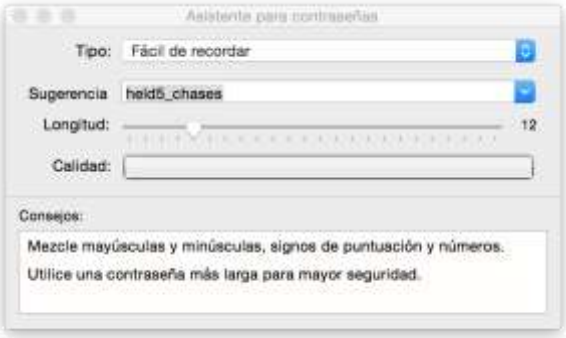


568. Tras proporcionar un nombre para el nuevo llavero, por ejemplo "admin", éste se almacenará bajo "~/Library/Keychains/admin.keychain".

569. Durante el proceso de creación de un nuevo llavero es necesario proporcionar una contraseña para cifrar sus contenidos. Se recomienda hacer uso de una contraseña suficientemente robusta teniendo en cuenta la sensibilidad de los datos almacenados en los llaveros, y que la misma sea diferente a la contraseña de inicio de sesión, para que el acceso al llavero de inicio de sesión y al resto de llaveros adicionales sea independiente (esta recomendación también se puede aplicar a los otros llaveros existentes por defecto, como por ejemplo, el de ítems locales):

570. "Acceso a Llaveros" proporciona un asistente para la gestión de certificados digitales, disponible a través del menú "Acceso a Llaveros - Asistente para Certificados", y un asistente para la generación de contraseñas robustas, disponible desde el icono con forma de llave junto al campo "Contraseña" a la hora de añadir un nuevo elemento al llavero:





571. Este asistente permite seleccionar el tipo de contraseña a generar en función de su complejidad (por defecto emplea "Fácil de recordar"), con las sugerencias ofrecidas empleando palabras en inglés, así como seleccionar la longitud de la misma.

572. El "Acceso a llaveros" almacena y proporciona acceso a las contraseñas desde otras aplicaciones, como por ejemplo el navegador web Safari, automática o manualmente.

573. La funcionalidad de notas seguras permite almacenar en el llavero información en formato texto cifrada. Una vez creada una nota segura, para poder ver sus contenidos es necesario proporcionar la contraseña del llavero dónde ha sido almacenada.

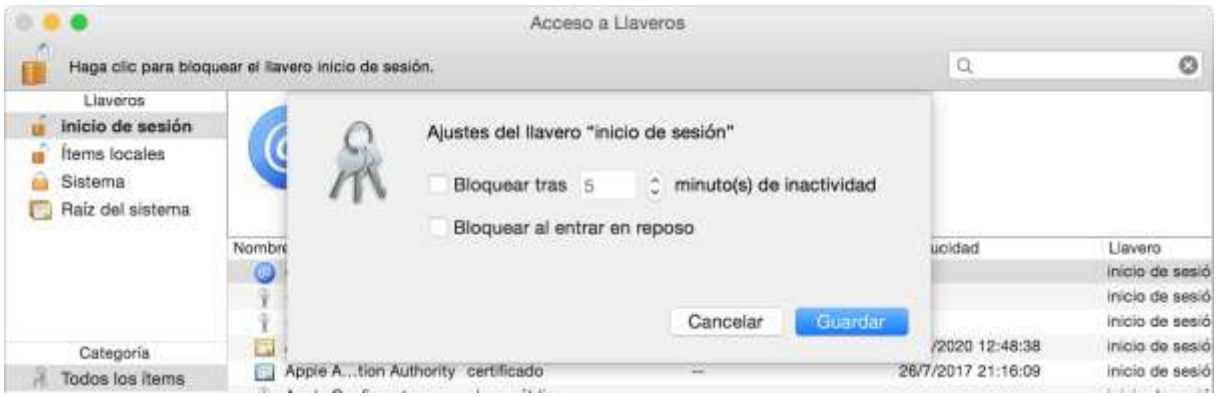
574. Debe tenerse en cuenta que si el llavero de inicio de sesión (o cualquier otro llavero) no está bloqueado, si un potencial atacante dispone de acceso a la cuenta de un usuario podrá acceder a todas las credenciales almacenadas en estos llaveros sin introducir ninguna contraseña.

575. Es posible bloquear manualmente el llavero actualmente seleccionado en el panel de la izquierda desde el menú "Archivo - Bloquear llavero '<nombre de llavero>'", o bloquear el acceso a todos los llaveros simultáneamente desde el menú "Archivo - Bloquear todos los llaveros".

576. El siguiente comando permitiría obtener todas las contraseñas almacenadas en el llavero de inicio de sesión del usuario si no está bloqueado[104]:

```
$ security dump-keychain -d ~/Library/Keychains/login.keychain
```

577. Adicionalmente, es posible bloquear automáticamente el llavero de inicio de sesión (o cualquier otro llavero seleccionado), estableciendo un temporizador por ausencia de actividad, desde el menú "Edición - Cambiar ajustes del llavero '<nombre de llavero>'…", mediante la opción "Bloquear tras <valor> minuto(s) de inactividad":



578. Se recomienda establecer un valor para el temporizador por inactividad del llavero que permita disponer de un equilibrio entre seguridad y funcionalidad, sin que el usuario reciba solicitudes repetidas y frecuentes de la contraseña del llavero, como por ejemplo 6 horas (ó 360 minutos, ó 21600 segundos).

579. Añadiendo un nivel extra de seguridad, se recomienda activar la opción "Bloquear al entrar en reposo" (deshabilitada por defecto) para que el llavero también se bloqueé al entrar el equipo en el estado de reposo.

580. El siguiente comando permite obtener los detalles de configuración, y en concreto del temporizador y del bloqueo al entrar en reposo ("lock-on-sleep"), asociados al llavero de inicio de sesión del usuario. Por defecto no se dispone de ningún temporizador establecido:

```
$ security show-keychain-info
Keychain "<NULL>" no-timeout

$ security show-keychain-info
Keychain "<NULL>" lock-on-sleep timeout=21600s
```

581. Se recomienda hacer un uso prudencial de la funcionalidad de "Acceso a llaveros" de OS X, especialmente teniendo en cuenta la sensibilidad y criticidad del tipo de información que suele almacenarse en los llaveros, como credenciales de acceso a otros servicios y entornos.

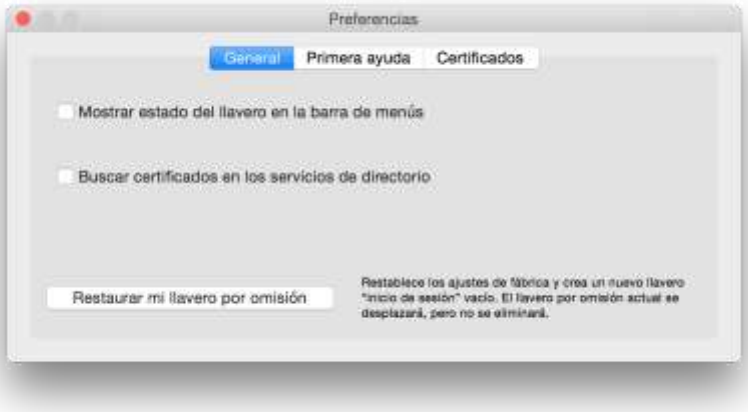
[104] Ejemplo para obtener las contraseñas de las cuentas de Google: $ security find-internet-password -s accounts.google.com -w

582. Potencialmente, una vulnerabilidad en la implementación de llaveros de OS X podría poner en riesgo toda la información protegida por esta tecnología, como por ejemplo, las vulnerabilidades en el acceso no autorizado a recursos compartidos entre aplicaciones en OS X e iOS, publicadas en junio de 2015 y apodadas XARA (*unauthorized Cross-App Resource Access*) [Ref.- 84].

583. Esta vulnerabilidad, identificada con el CVE-2015-3786, fue solucionada por Apple en OS X 10.10.5 [Ref.- 85].

584. Finalmente, la funcionalidad de "Acceso a Llaveros" ofrece un mecanismo de seguridad adicional y no directamente relacionado con los llaveros, para permitir de forma rápida y sencilla bloquear la pantalla del equipo y requerir la autentificación del usuario para volver a hacer uso del mismo. Se recomienda habilitar estas capacidades para poder bloquear el equipo de manera rápida y sencilla.

585. Para ello, desde "Acceso a Llaveros - Preferencias", en la pestaña "General", se debe habilitar la opción "Mostrar estado del llavero en la barra de menús":



586. Como resultado aparecerá un nuevo icono en la barra de menús correspondiente a un candado (abierto o cerrado), desde el que es posible, mediante su pulsación, bloquear la pantalla a través de la opción "Bloquear pantalla":

5.8.8 ACCESO A LLAVEROS EN ICLOUD

587. Desde la versión OS X 10.9 Mavericks (o iOS 7.0.3)[105], la funcionalidad de llaveros fue extendida a iCloud, el servicio de Apple de sincronización y almacenamiento de información en la nube.

[105] https://support.apple.com/en-us/HT204085

588. Llaveros en iCloud funciona de manera similar a llaveros en el equipo local, empleando cifrado basado en AES de 256 bits, pero la información de credenciales es almacenada en iCloud en su lugar, permitiendo al usuario sincronizarla entre todos sus equipos Apple: OS X (ordenadores Mac) e iOS (dispositivos móviles iPhone, iPad, etc).

589. Al visitar un sitio web, llaveros en iCloud consultará y proporcionará las credenciales de acceso para que el usuario pueda autentificarse automáticamente, pudiendo también proporcionar de manera automática información de tarjetas de crédito.

590. Es posible verificar si se dispone de llaveros en iCloud habilitado para el usuario de iCloud empleado en OS X desde "Preferencias del Sistema - iCloud", comprobando si la categoría "Llaveros" del panel de la derecha está o no activa.

591. Desde el punto de vista de seguridad, se recomienda de manera general encontrar el equilibrio entre seguridad y funcionalidad, evitando el uso de servicios de terceros para tareas críticas asociadas a la seguridad, como por ejemplo, las capacidades de almacenamiento de contraseñas de llaveros en iCloud.

5.8.9 BORRADO SEGURO DE FICHEROS

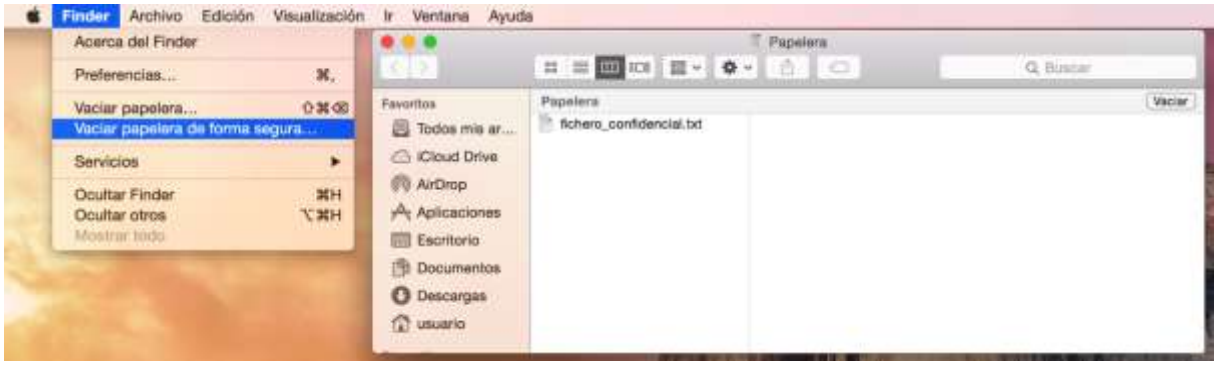
592. El borrado de ficheros en OS X no elimina necesariamente los contenidos de los ficheros del disco duro, sino que los marca como borrados, liberando su espacio a nivel del sistema de ficheros para que pueda ser reutilizado por el sistema operativo, por ejemplo, a la hora de crear nuevos ficheros o de aumentar el tamaño de ficheros ya existentes.

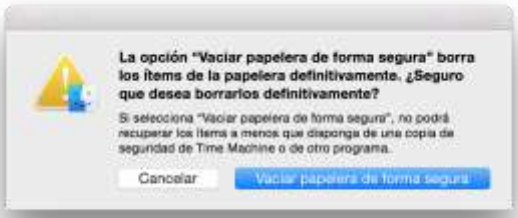
593. Por tanto, existe la posibilidad de recuperar el contenido de ficheros borrados anteriormente en OS X.

594. Habitualmente, los ficheros borrados son almacenados temporalmente en la Papelera (de reciclaje o *Trash*), desde donde también pueden ser recuperados (mediante la opción "Sacar de la papelera", disponible con el botón derecho) o eliminados definitivamente.

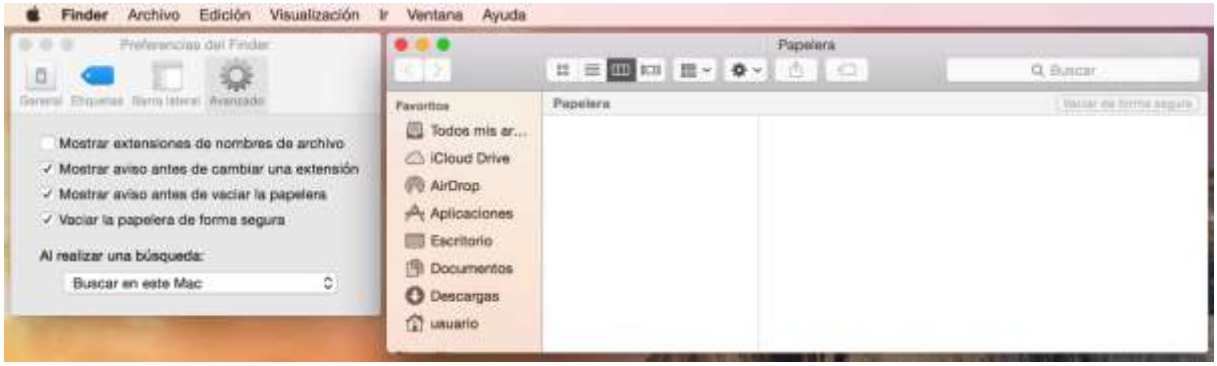
595. Por defecto, el proceso de borrado o vaciado de la Papelera en OS X, a través del botón "Vaciar" de la parte superior derecha, no borra el contenido de los ficheros y directorios de forma definitiva, siendo aún posible su recuperación.

596. Si se desea eliminar de forma segura el contenido de los ficheros borrados desde la Papelera se debe hacer uso de la funcionalidad que permite vaciar la Papelera de forma minuciosa, disponible desde el menú de "Finder - Vaciar papelera de forma segura…" (siendo necesaria la confirmación por parte del usuario), tanto para el disco duro del equipo como, especialmente, en discos o unidades de almacenamiento externas conectadas a través de USB:





597. Si se desea que por defecto siempre la acción de vaciar la Papelera se lleve a cabo de forma segura, desde "Finder - Preferencias…" y la pestaña "Avanzado", se dispone de la opción "Vaciar la papelera de forma segura" (deshabilitada por defecto):



598. Esta cambio de la configuración modificará el botón "Vaciar" de la parte superior derecha de la Papelera por el botón "Vaciar de forma segura", así como la opción "Vaciar papelera", disponible con el botón derecho dentro de la Papelera, que se mostrará como "Vaciar papelera de forma segura".

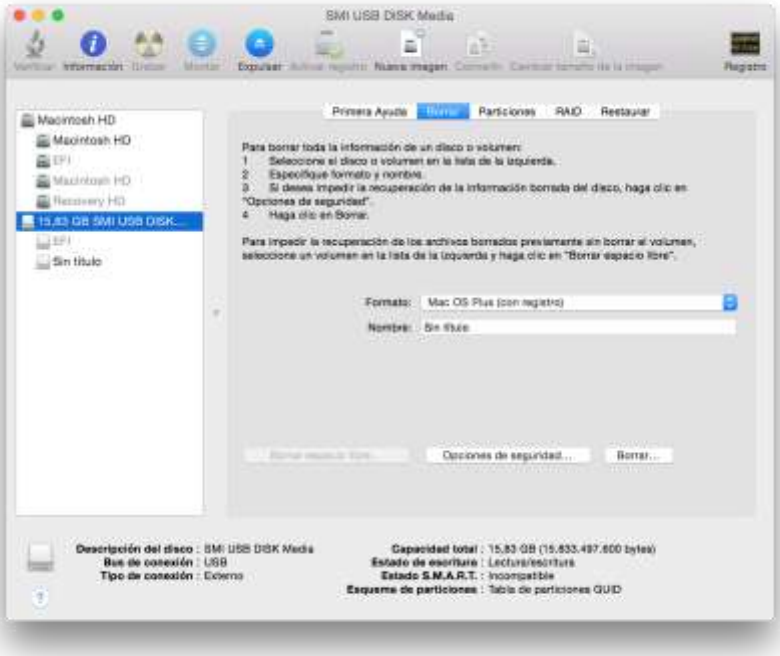
599. Adicionalmente, existe la posibilidad de borrar de forma segura todo los contenidos asociados al espacio vacío o libre (no utilizado por ficheros) existente en un volumen montado actualmente. El siguiente comando elimina de forma segura el espacio libre del volumen principal de OS X (por ejemplo, "Macintosh HD"):

```
$ sudo diskutil secureErase freespace <level> /Volumes/Macintosh\ HD
```

600. El parámetro "<level>" recibe un valor numérico que indica como se llevará a cabo el proceso de borrado: 0 ó 1 (una única pasada escribiendo ceros u unos, respectivamente), 2 (realizando siete pasadas de sobrescritura aleatorias, en base a las directivas del US DoD), 3 (método Gutmann que realiza 35 pasadas de sobrescritura) o 4 (realizando tres pasadas de sobrescritura aleatorias, en base a las directivas del US DoE).

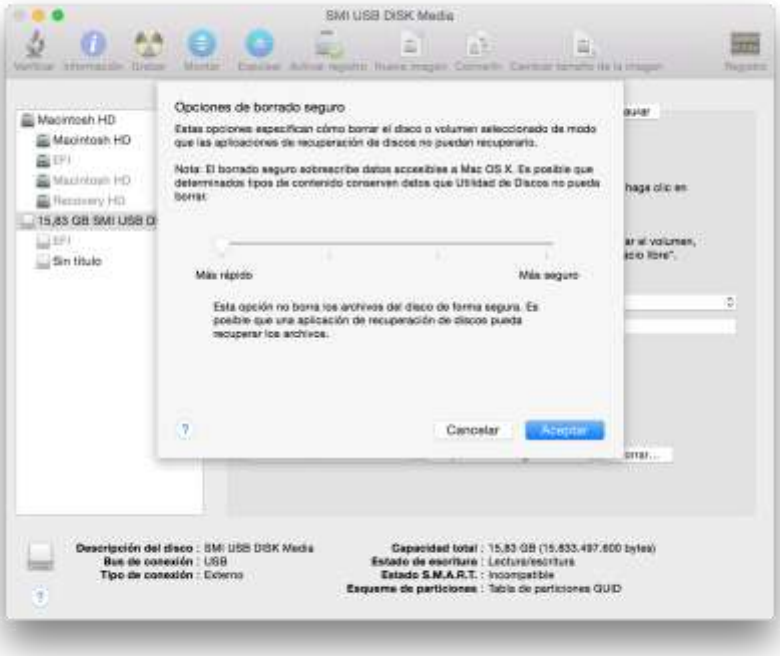
601. Se recomienda hacer uso de este comando periódicamente, especialmente si se ha eliminado recientemente información confidencial y/o sensible, empleando los niveles 2 ó 3. En función del tamaño del disco duro y del espacio libre disponible, esta acción de borrado, empleando por ejemplo el nivel 2, puede llevar entre 4 y 5 horas.

602. Adicionalmente, desde la "Utilidad de Discos", seleccionando el disco duro o unidad de almacenamiento externa, desde la pestaña "Borrar" y mediante el botón "Opciones de seguridad…" es posible establecer las opciones de borrado seguro:



603. Por defecto OS X no hace uso de mecanismos de borrado seguro, opción "Más rápido", lo que mejora el rendimiento del proceso de borrado.

604. Se recomienda desde el punto de vista de seguridad cambiar la configuración a la opción "Más seguro", situada más a la derecha de la barra de configuración (y que tiene asociado un proceso de borrado mediante 7 sobrescrituras - correspondiente al nivel 2 detallado previamente):



605. Se dispone de tres opciones de borrado más seguro en función de su nivel de seguridad (un subconjunto de las opciones de borrado detalladas previamente).

5.8.10 BASE DE DATOS DE AUTORIZACIONES DE SEGURIDAD

606. Desde la versión OS X Mavericks, el sistema operativo hace uso de una base de datos de autorizaciones (en formato SQLite 3.x) disponible en "/var/db/auth.db".

607. Esta base de datos de autorizaciones es creada inicialmente a partir de una plantilla contenida en el fichero PLIST "/System/Library/Security/authorization.plist".

608. Esta base de datos registra los derechos o privilegios de autorizaciones de OS X. Estos derechos o privilegios determinan qué usuarios pueden o no acceder a cierta funcionalidad, como por ejemplo, a las diferentes secciones de las "Preferencias del Sistema".

609. Las opciones disponibles para gestionar la base de datos de autorizaciones pasan por hacer uso de la utilidad "security", editar la base de datos mediante la utilidad "sqlite3" o modificar el fichero "authorization.plist" y borrar la base de datos actual, para que sea recreada de nuevo con los nuevos contenidos de dicho fichero PLIST[106].

610. El comando "security", a través de la opción "authorizationdb", permite gestionar (leer, escribir, o eliminar) los derechos declarados en la base de datos de autorizaciones.

611. Por ejemplo, el siguiente comando permite obtener (en formato de fichero PLIST) los derechos de autorización de las preferencias del sistema, dentro de los cuales se encuentra, entre otros, el parámetro que determina si se debe solicitar la contraseña de un usuario administrador para acceder a las preferencias de todo el sistema (parámetro "shared", si la opción no está activa su valor es true; ver apartado "5.7.7. Solicitar contraseña de administrador para modificar preferencias del sistema"):

```
$ security authorizationdb read system.preferences
...
    <key>shared</key>
    <true/>
```

612. Aunque el fichero "auth.db" solo es legible por root, cualquier usuario puede leer sus contenidos a través de los comandos "security authorizationd read …". Para poder modificarlos ("write"), o borraros ("remove"), es necesario disponer de permisos de administrador.

613. Se dispone de una tabla pública con el conjunto de derechos o privilegios de autorizaciones disponibles en función de la versión de OS X empleada [Ref.- 35].

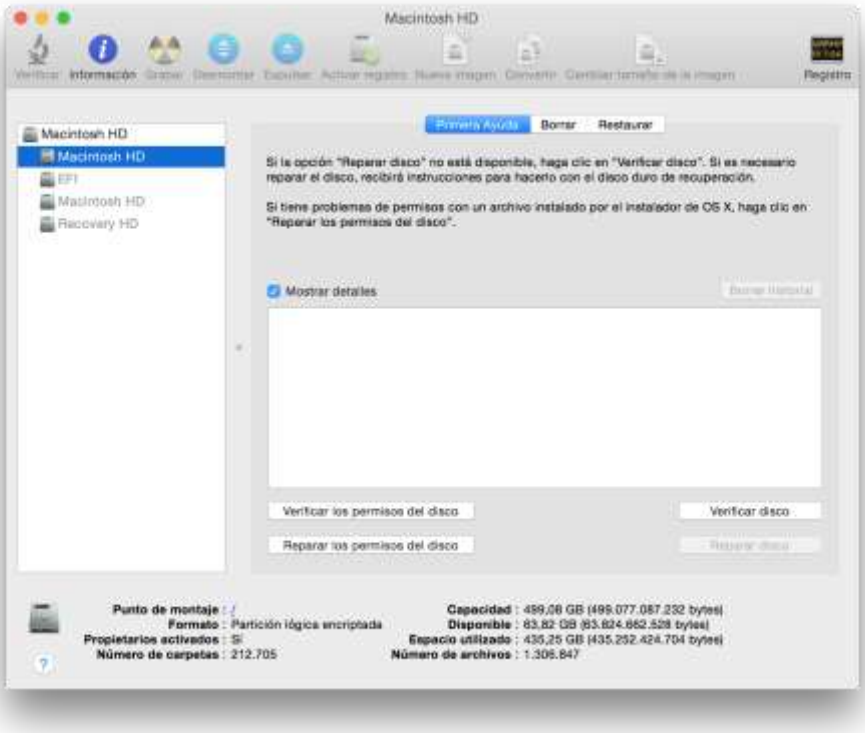
5.8.11 PERMISOS DEL SISTEMA DE FICHEROS

614. OS X dispone de capacidades para reparar los permisos asociados a ficheros y directorios a nivel del sistema de ficheros, restaurando los permisos y controles de acceso originales asociados a la instalación del sistema operativo.

615. Se recomienda restaurar los permisos del sistema de ficheros periódicamente, para regular los cambios y modificaciones que hayan podido ser llevados a cabo por la instalación de software y/o actualizaciones.

[106] https://derflounder.wordpress.com/2014/02/16/managing-the-authorization-database-in-os-x-mavericks/

616. Desde la "Utilidad de Discos", tras seleccionar el volumen de arranque de OS X ("Macintosh HD"), se dispone del botón "Verificar los permisos del disco" para evaluar las posibles modificaciones existentes, y del botón "Reparar los permisos del disco", para proceder a su restauración:



617. Adicionalmente es posible realizar esta tarea desde un terminal, así como planificarla periódicamente desde "/etc/periodic/weekly" [Ref.- 86], como alternativa al resto de planificación de tareas (ver apartado "5.6. Ejecución de tareas programadas en OS X") :

```
$ diskutil repairPermissions /
```

618. Finalmente, se recomienda mostrar la extensión asociada a cada fichero o archivo, con el objetivo de identificar potencialmente su tipo y el tipo de datos que contiene. Desde el Finder, a través del menú "Preferencias" y la pestaña "Avanzado", se debe seleccionar la opción "Mostrar extensiones de nombre de archivo":

619. El siguiente comando permite habilitar que se muestre la extensión de los archivos:

```
$ sudo defaults write NSGlobalDomain AppleShowAllExtensions -bool true
```

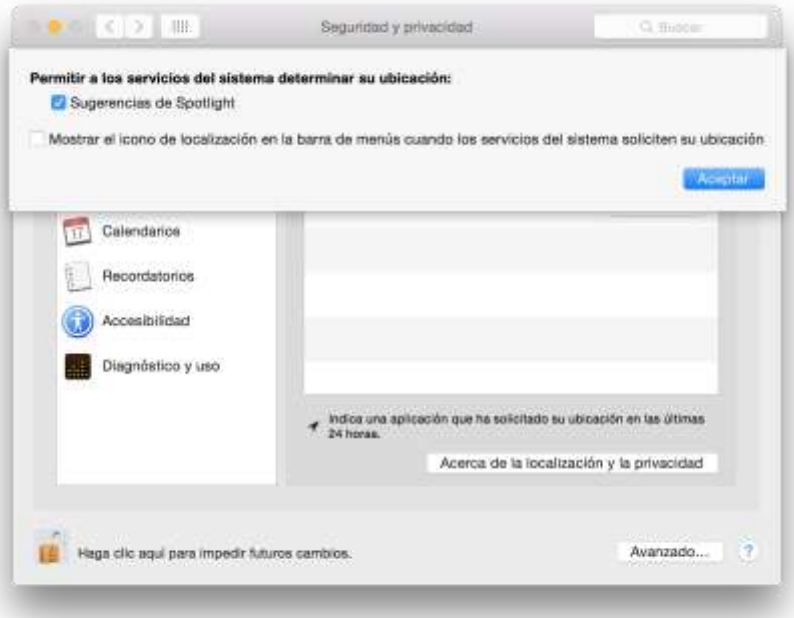
5.9 PRIVACIDAD

620. Desde "Preferencias del Sistema - Seguridad y privacidad", a través de la pestaña "Privacidad", es posible configurar controles de acceso para permitir a las aplicaciones instaladas, y que lo han solicitado previamente, acceso a ciertos servicios y/o conjuntos de datos personales que impactan directamente sobre la privacidad del usuario:

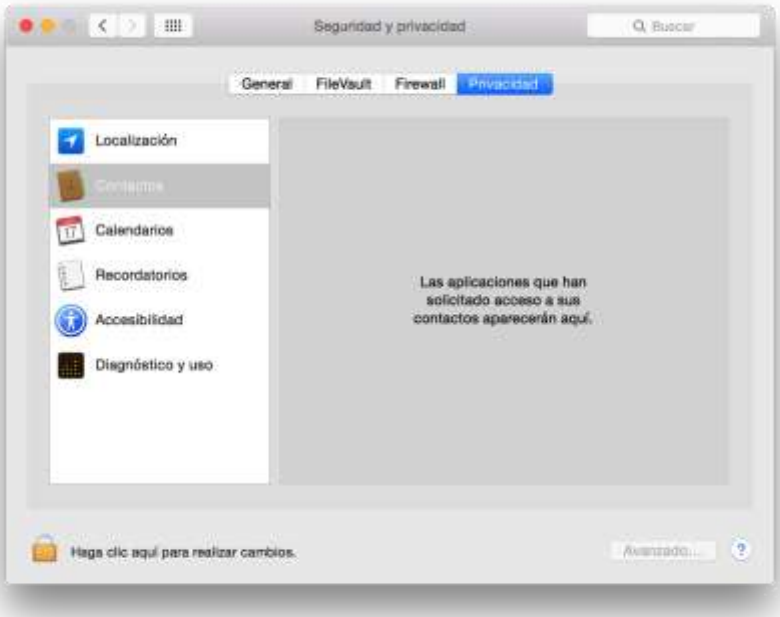
621. Dentro de las categorías de servicios y conjuntos de datos personales asociados a la privacidad del usuario se dispone de los servicios de localización, los contactos, los calendarios, los recordatorios, e información de accesibilidad (descrita en detalle posteriormente) y de diagnóstico y uso.

622. El servicio de localización está activo por defecto, e incluye por defecto los "Servicios del sistema" y en concreto "Sugerencias de Spotlight", disponible mediante el botón "Detalles…" (ver apartado "5.9.1. Deshabilitar las sugerencias de Spotlight").

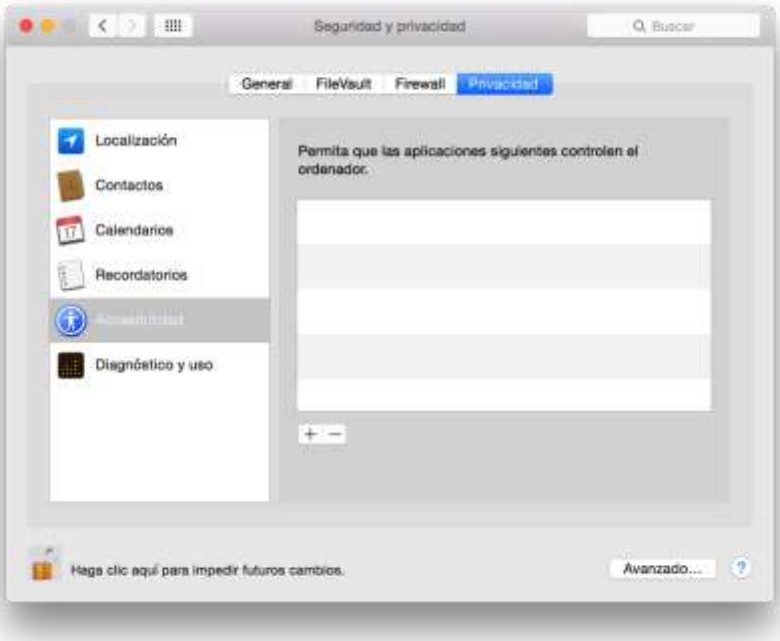
623. Se recomienda desactivar esta opción si no se desea remitir información de localización en las búsquedas de Spotlight, así como activar la opción "Mostrar el icono de localización en la barra de menús cuando los servicios del sistema soliciten su ubicación", para poder ser consciente de su utilización:



624. Por defecto, ninguna aplicación ha solicitado, ni dispone de, acceso a los contactos, calendarios, recordatorios o accesibilidad:



625. La categoría "Accesibilidad" de los ajustes de privacidad emplea un término confuso, ya que las opciones de accesibilidad generales están directamente disponibles en "Preferencias del Sistema - Accesibilidad":



626. Esta categoría establece qué aplicaciones (supuestamente con el objetivo de mejorar la accesibilidad del usuario a OS X) pueden controlar el ordenador, es decir, permite a ciertas aplicaciones el envío y ejecución de comandos en OS X, como por ejemplo el "Editor de Scripts" (*Script Editor*), usado para crear y ejecutar AppleScripts.

627. Algunas aplicaciones al ser ejecutadas solicitan a través de una ventana de diálogo disponer de acceso para controlar el equipo y, como resultado, serán incluidas bajo está categoría.

628. Debido a la criticidad y al acceso privilegiado de este tipo de aplicaciones, se recomienda evaluar en detalle la lista de aplicaciones que disponen de este tipo de permisos.

629. La categoría "Diagnóstico y uso" solicita la colaboración del usuario para enviar datos de diagnóstico y uso a Apple y a los desarrolladores de aplicaciones, así como compartir datos de los errores con estos, con el objetivo de mejorar sus productos y servicios:

630. Estos ajustes corresponden a los solicitados durante el proceso inicial de instalación y configuración del equipo (ver apartado "ANEXO A. Proceso de instalación y configuración inicial"). Desde el punto de vista de la privacidad, se recomienda deshabilitar ambas opciones (las dos activas por defecto en dicho proceso de instalación y configuración inicial).

631. Existe la posibilidad de revocar todos los permisos otorgados a las diferentes aplicaciones desde un terminal, individualmente para cada uno de los servicios o conjuntos de datos personales asociados a la información privada del usuario, a través de la utilidad "tccutil", encargada de la gestión de la base de datos de privacidad[107] (en formato SQLite 3.x) que almacena las decisiones tomadas por el usuario respecto al acceso a sus datos personales:

```
$ sudo tccutil reset AddressBook

$ sudo tccutil reset CoreLocationAgent
```

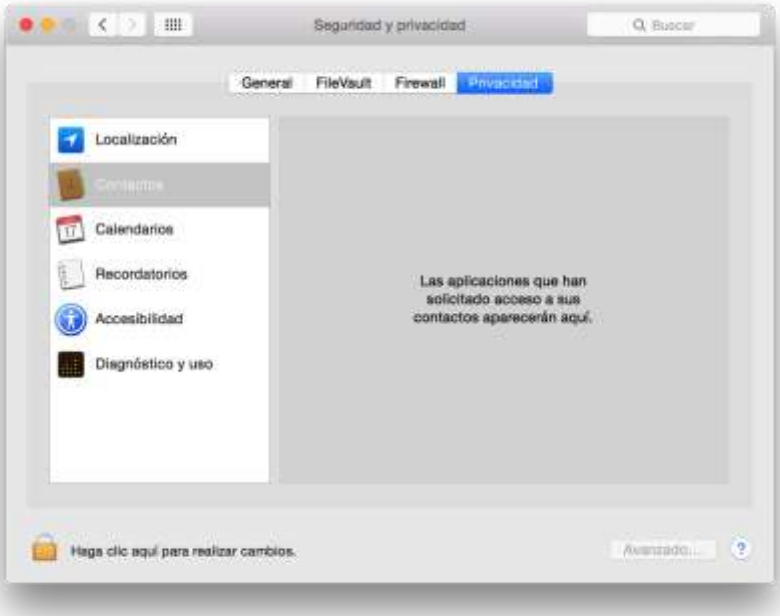
632. La referencia a "AddressBook", en el ejemplo superior, revoca todos los accesos a los datos de los contactos del usuario, mientras que la referencia a "CoreLocationAgent" revoca todos los accesos a los datos y servicios de localización.

633. El listado de referencias para cada uno de los servicios y conjuntos de datos personales soportados es el siguiente (pudiendo emplearse la referencia "All" para eliminar la base de datos de privacidad de todos los servicios y conjuntos de datos conjuntamente):

[107] /Library/Application\ Support/com.apple.TCC/TCC.db: A nivel de sistema y en el directorio principal o *home* del usuario (~).

- Localización: CoreLocationAgent
- Contactos: AddressBook
- Calendarios: Calendar
- Recordatorios: Reminders
- Accesibilidad: Accessibility
- Otros: Facebook, Twitter, etc.

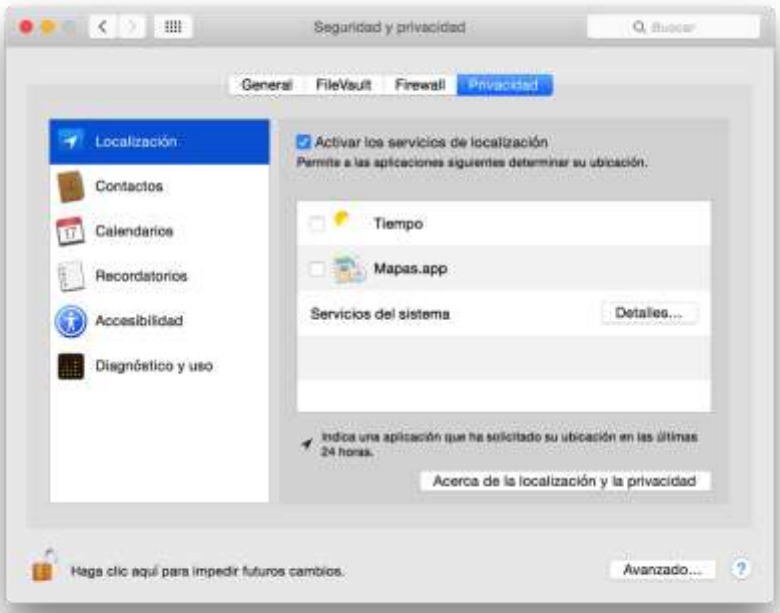
634. Como resultado del reseteo de la base de datos de un servicio o conjunto de datos concreto, todas las aplicaciones que previamente habían solicitado acceso a esos datos personales (por ejemplo, los contactos del usuario) desaparecerán de la lista asociada a los ajustes de privacidad de esos datos (por ejemplo, de los "Contactos"), independientemente de sí tenían o no permiso. Es decir, el conjunto de datos reseteados queda con la configuración inicial de fábrica, sin ninguna aplicación asociada[108]:



635. No se dispone de ningún método a través de "Preferencias del Sistema" para eliminar aplicaciones de la lista asociada a la privacidad de cada servicio o conjunto de datos.

636. La próxima vez que una aplicación solicite acceso a esos datos el usuario será consultado de nuevo, debiendo aprobar o rechazar dicho acceso, y añadiéndose una nueva entrada en la categoría correspondiente de la sección de privacidad (que puede ser habilitada o deshabilitada en cualquier momento):

[108] Existen diferentes herramientas de terceros (basadas en Python) que permiten gestionar la base de datos de privacidad con mayor granularidad: (https://github.com) /jacobsalmela/tccutil, /univ-of-utah-marriott-library-apple/privacy_services_manager o /timsutton/scripts/blob/master/tccmanager/tccmanager.py.



5.9.1 DESHABILITAR LAS SUGERENCIAS DE SPOTLIGHT

637. Spotlight, un sistema de búsqueda rápida de información local en OS X, introducido en la versión OS X 10.4 y también disponible en iOS, ha sido rediseñado en OS X Yosemite 10.10 (e iOS 8) con capacidades para ofrecer sugerencias de búsqueda, no sólo locales al equipo, sino también desde Internet.

638. La configuración por defecto de OS X Yosemite puede desvelar información privada del usuario hacia Internet, y en concreto, hacia Apple y hacia otros servicios, como el buscador Microsoft Bing [Ref.- 70].

639. Para poder obtener sugerencias de Internet (de fuentes como la Wikipedia, iTunes Store, App Store o Mapas) sobre las búsquedas realizadas en Spotlight, este servicio debe de enviar remotamente los términos de búsqueda del usuario, pudiendo poner en riesgo su privacidad[109]. Asimismo, para optimizar el resultado y la precisión de las búsquedas, hace uso de información de contexto y de la localización del usuario.

640. Si se dispone de los servicios de localización habilitados (ver apartado "5.8.11. Permisos del sistema de ficheros") en el momento de realizar la búsqueda a través de Spotlight, la información de localización del equipo Mac será enviada a Apple.

641. Igualmente, los términos de búsqueda son compartidos por Apple con Microsoft para realizar búsquedas complementarias a través del motor de búsqueda Bing.

642. Es posible deshabilitar la funcionalidad de búsquedas remotas en Internet de Spotlight a través de las "Preferencias del Sistema - Spotlight", desde la pestaña "Resultados de la búsqueda", desactivando las siguientes opciones (habilitadas por defecto):

[109] http://www.apple.com/privacy/privacy-built-in/

- Sugerencias de Spotlight
- Búsquedas web de Bing
- Correo y mensajes

643. Es especialmente relevante la desactivación de la opción "Correo y mensajes", ya que se descubrió que Spotlight ignora algunos mecanismos de protección establecidos a través de la aplicación Mail.

644. Desde el punto de vista de la privacidad, y con el objetivo de que un tercero no pueda conocer la dirección IP del usuario, se recomienda deshabilitar la opción "Cargar contenido remoto en mensajes" (habilitada por defecto), disponible a través de "Mail - Preferencias…", desde la pestaña "Visualización"[110]:

645. Al desactivar esta opción, la aplicación Mail no cargará por defecto las imágenes incluidas en los mensajes de correo electrónico, evitando así que un tercero pueda incluir imágenes individualizadas en los mensajes de correo electrónico para saber si el menaje ha sido o no leído y, a su vez, obtener la dirección IP del usuario a la hora de leer el mensaje y cargar la imagen.

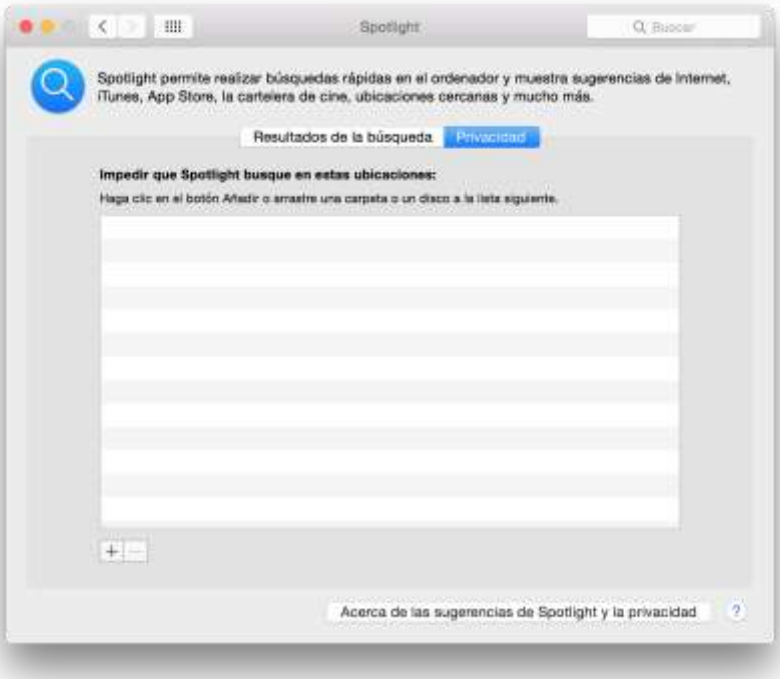
646. Las búsquedas en Spotlight, y en concreto las capacidades de previsualización de los resultados de Spotlight, muestran los mensajes de correo electrónico completos, incluyendo las imágenes referencias desde los mismos, e ignorando el ajuste de configuración de Mail descrito previamente.

647. Spotlight permite previsualizar incluso los mensajes almacenados en la carpeta de correo electrónico de Spam (o *Junk*) y que no han sido abiertos, independientemente de su dudosa naturaleza o contenido.

648. Adicionalmente, desde la pestaña "Privacidad" de Spotlight es posible definir una lista de ubicaciones (carpetas individuales o discos) que serán excluidas de las búsquedas de

[110] Imagen: http://mecambioamac.com/wp-content/uploads/2015/01/Captura_de_pantalla_2015-01-16_a_las_16_45_44.png.

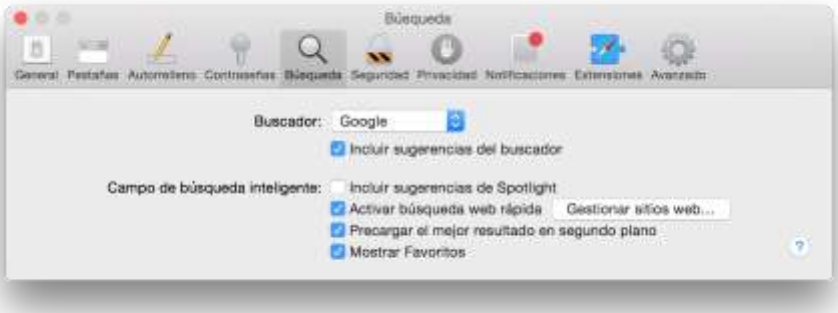
Spotlight. Se recomienda añadir carpetas con información crítica o sensible para evitar la posible revelación de sus contenidos a través de Spotlight:



649. El botón "Acerca de las sugerencias de Spotlight y la privacidad" muestras los términos y condiciones del servicio donde se describen estas capacidades.

650. Además de remitirse esta información hacia Internet desde Spotlight, el navegador web por defecto de OS X, Safari, dispone de capacidades similares.

651. Se recomienda deshabilitar la integración de Spotlight en Safari mediante el menú "Safari - Preferencias…", desde la pestaña "Búsqueda", y la opción "Incluir sugerencias de Spotlight" (habilitada por defecto):



5.10 EVENTOS DE SEGURIDAD

652. Durante el proceso de autentificación o inicio de sesión de un usuario en OS X, se almacenan registros correspondientes a estos eventos de seguridad en utmpx (en versiones previas de OS X, hasta 10.4 inclusive, también se hacía uso de utmp, wtmp y lastlog).

653. utmpx utiliza la base de datos de auditoría (*accounting*) del fichero "/var/run/utmpx", donde se almacena la información de los usuarios actualmente activos (información disponible mediante los comandos "who" y "w"). Tradicionalmente, la información de registro de inicio y finalización de las sesiones de los usuarios (histórico) se almacenaba en wtmpx (asociado a los comandos "last" y "ac") y el último inicio de sesión de cada usuario en lastlogx.

654. Al disponer OS X del Apple System Log (ASL), estos tres ficheros son reemplazados por entradas de log de ASL que son generadas al escribirse eventos en utmpx.

655. El Apple System Log (ASL) almacena la información y registros de log bajo "/var/log/asl/*.asl".

656. Esta información de registro de eventos en OS X se complementa con la existencia de numerosos otros ficheros de log, almacenados bajo "/var/log/*.log".

657. Concretamente, los eventos de sistema se almacenan bajo "/var/log/system.log", los eventos del cortafuegos bajo "/var/log/appfirewall.log", los eventos de autorización de derechos y privilegios bajo "/var/log/authd.log", los eventos de actualizaciones e instalación de software bajo "/var/log/install.log", etc.

658. La configuración de ASL (del gestor de ASL y del proceso syslogd) está disponible en "/etc/asl.conf".

659. Se recomienda establecer una política de almacenamiento, retención y rotación de ficheros de registro o *logs* definida por la organización, configurando adecuadamente las directivas del fichero "asl.conf" para precisar el tamaño de los ficheros de log individuales ("file_max"), el tamaño máximo de todos los ficheros de log ("all_max"), el tiempo de reteción en días ("ttl"), incluir información de la fecha y hora en el proceso de rotación de los logs ("rotate=utc"), etc [Ref.- 86].

660. La información recolectada por ASL está disponible a través de la Consola ("Aplicaciones - Utilidades - Consola"), que debe ser ejecutada desde una cuenta de usuario con permisos de administrador para disponer de acceso a todos los ficheros de log.

661. Adicionalmente es posible acceder a los registros de los logs desde un terminal mediante el comando "syslog -C".

5.11 COPIAS DE SEGURIDAD (*BACKUPS*)

5.11.1 COPIAS DE SEGURIDAD LOCALES O EN RED

662. Con el objetivo de proteger los datos almacenados en los equipos con OS X es necesario disponer de copias de seguridad (*backups*) de los mismos.

663. Se recomienda hacer uso de Time Machine para realizar copias de seguridad de los contenidos completos del sistema de almacenamiento del equipo en (al menos) un disco USB externo o un disco de red (como por ejemplo el Airport Time Capsule).

5.11.2 COPIAS DE SEGURIDAD EN ICLOUD

664. Las copias de seguridad en iCloud permiten almacenar distintos tipos de información del equipo en los servicios de almacenamiento de Apple "en la nube".

665. Es posible verificar que información está siendo sincronizada o copiada en iCloud, en concreto en la cuenta de usuario de iCloud empleada en OS X, desde "Preferencias del

Sistema - iCloud" (una vez se ha iniciado sesión con las credenciales de iCloud o ID de Apple), comprobando las categorías habilitadas en el panel de la derecha: Fotos y vídeos (tanto fotos en *streaming* como en iCloud[111]), Mail, Contactos, Calendario, Recordatorios, Safari (Favoritos), y Notas[112]:

666. Al iniciar sesión por primera vez en iCloud desde OS X, se solicita al usuario confirmar si desea usar iCloud para los contactos, calendarios, recordatorios y Safari, y si desea usar "Buscar mi Mac":

[111] Ambas opciones habilitadas por defecto.

[112] https://support.apple.com/es-es/HT204055

667. Si se dejan las dos opciones activas, habilitadas en su configuración por defecto, todas las opciones de sincronización de datos de iCloud estarán activas excepto Mail, Notas y Volver a mi Mac (junto a iCloud Drive y Llaveros, detalladas a continuación):

668. Durante el proceso de configuración de iCloud se solicita la contraseña del ID de Apple del usuario para configurar el llavero de iCloud. Mediante el botón "Cancelar" es posible no habilitar el uso del llavero de iCloud (ver apartado "5.8.8. Acceso a Llaveros en iCloud"):

669. Igualmente, durante el proceso de configuración de iCloud se solicita al usuario si permite que "Buscar mi Mac" utilice la ubicación del ordenador Mac (ver apartado "5.12. iCloud: Buscar mi Mac"):

670. Si se desea hacer uso de esta funcionalidad, es necesario permitir este acceso, aunque "Buscar mi Mac" no se mostrará como una aplicación que está haciendo uso de los servicios de localización.

671. Finalmente, se consulta con el usuario si desea actualizar a iCloud Drive (descrito posteriormente). Se recomienda no actualizar a iCloud Drive durante el proceso de inicio de sesión y evaluar su utilización posteriormente, opción disponible mediante el botón "Cancelar":

672. En la actualidad, por defecto, Apple proporciona 5GB de espacio de almacenamiento gratuito al registrarse en iCloud, pudiendo ampliar dicha capacidad mediante varias opciones de pago:

673. Adicionalmente, desde OS X Yosemite se dispone de iCloud Drive, un servicio de almacenamiento de ficheros y documentos "en la nube", integrado en el sistema operativo, pudiendo guardar los documentos desde diferentes aplicaciones directamente en iCloud Drive, de la misma manera que se almacenan en el disco duro local.

674. Desde el punto de vista de seguridad, se recomienda de manera general encontrar el equilibrio entre seguridad y funcionalidad, evitando el uso de servicios de terceros para tareas críticas asociadas a la seguridad, como por ejemplo, las capacidades de sincronización y/o almacenamiento de información, datos y ficheros de iCloud.

5.12 ICLOUD: BUSCAR MI MAC

675. iCloud, el servicio de Apple de sincronización y almacenamiento de información en la nube, proporciona capacidades de sincronización de datos, almacenamiento de ficheros, y realización y restauración de copias de seguridad remotas entre los dispositivos de Apple (tanto móviles, iOS, como tradicionales, OS X) y los servicios de Apple asociados "en la nube".

676. Dentro de las diferentes capacidades disponibles a través de iCloud, algunas de ellas tienen implicaciones directas desde el punto de vista de seguridad, como por ejemplo el acceso a llaveros en iCloud (ver apartado "5.8.8. Acceso a Llaveros en iCloud"), las copias de seguridad en iCloud (ver apartado "5.11.2. Copias de seguridad en iCloud"), o la funcionalidad "Buscar mi Mac", descrita en el presente apartado.

677. El apartado "5.11.2. Copias de seguridad en iCloud" describe algunos de los detalles relevantes desde el punto de vista de seguridad asociados al proceso de inicio de sesión en iCloud desde OS X.

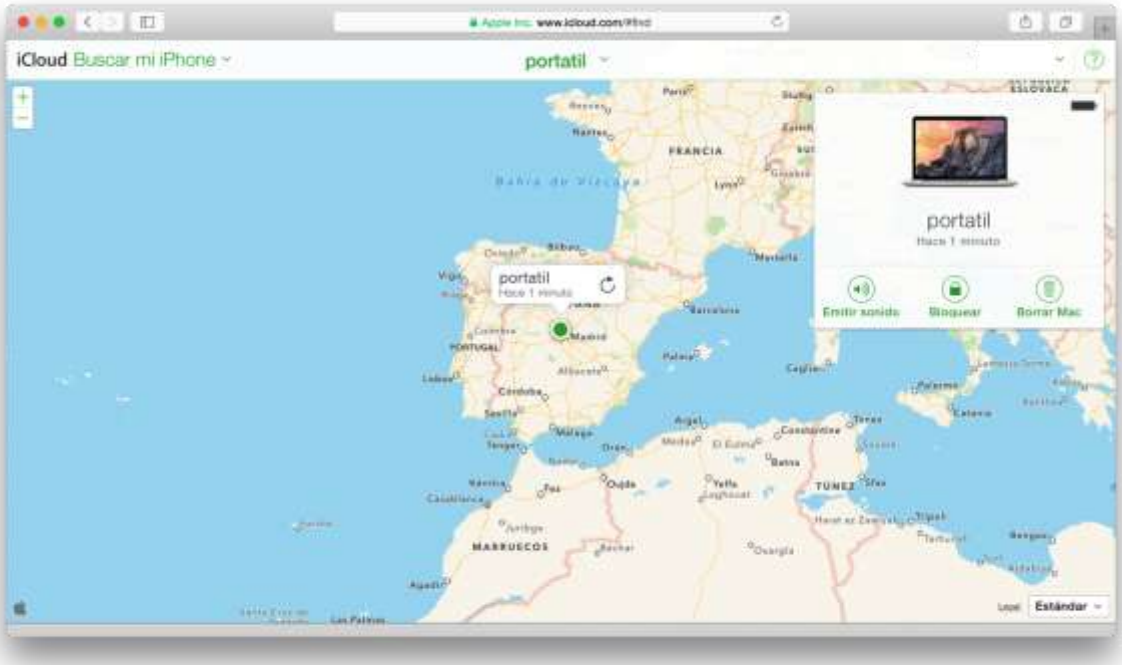
678. El servicio "Buscar mi Mac" ("Find My Mac"), integrado en iCloud, permite a los usuarios de ordenadores Apple (desde OS X Lion) localizar la ubicación del equipo si éste ha sido extraviado o sustraído.

679. Es posible localizar un equipo Mac perdido desde iCloud accediendo a las capacidades de "Buscar mi Mac" directamente desde la web o a través de la app de iOS "Buscar mi iPhone" ("Find My iPhone", o iPad).

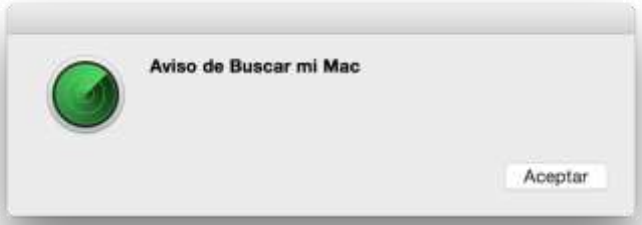
680. A través de iCloud (icloud.com), no sólo se dispone de capacidades para localizar el equipo Mac, sino que adicionalmente el servicio proporciona capacidades para bloquear de forma remota el ordenador con un código de acceso, ejecutar un borrado de datos remoto (*remote wipe*), o hacer que suene el ordenador para intentar localizar su ubicación cercana (con el objetivo de intentar recuperarlo):

681. El acceso al servicio está disponible desde la web de iCloud (https://www.icloud.com), mediante el botón "Buscar", protegido mediante el usuario y contraseña asociados a la cuenta de usuario de iCloud o ID de Apple:

682. Desde la opción superior "Todos los dispositivos" es posible seleccionar el ordenador Mac concreto para poder acceder a más funciones de gestión remota del equipo, pudiendo incluso obtenerse el nivel de batería del mismo:



683. Al hacer sonar el ordenador remotamente (durante 120 segundos en el volumen más alto, aunque estuviese en silencio el altavoz), e incluso aunque la pantalla estuviera bloqueada, el equipo muestra un mensaje indicando que su propietario está buscando el ordenador, "Aviso de Buscar mi Mac":



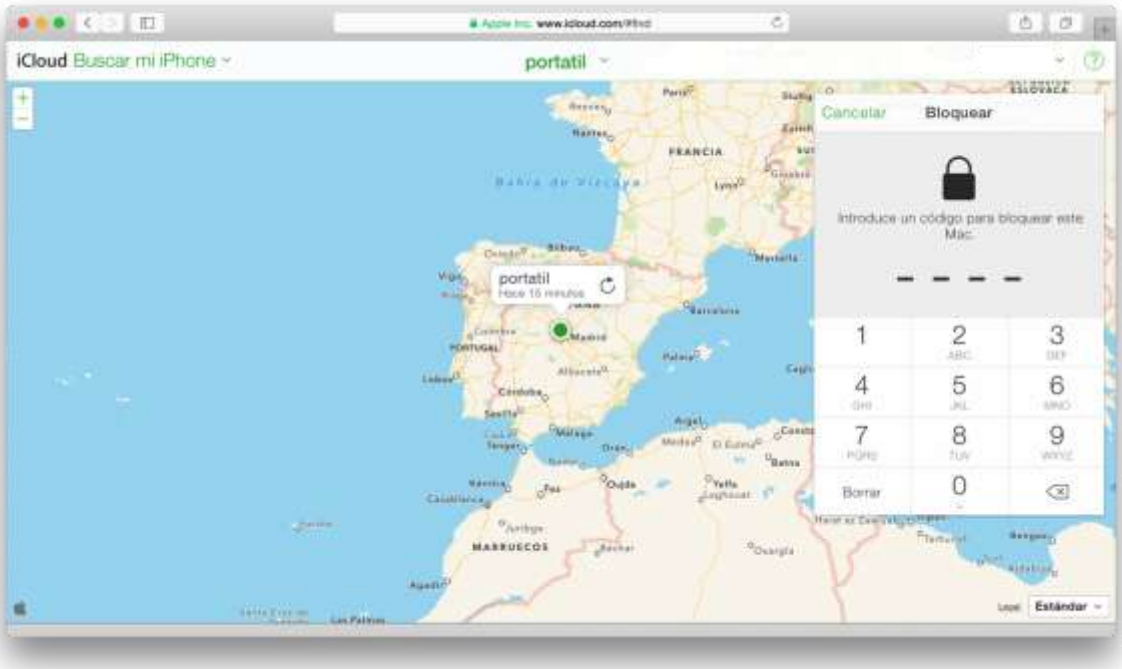
684. Si el equipo está apagado en el momento de intentar localizarlo, existe la posibilidad de recibir un correo electrónico de notificación tan pronto dispone de conectividad en Internet, por ejemplo, a través de una red Wi-Fi.

685. Por tanto, debe tenerse en cuenta que para poder hacer un uso efectivo de estas capacidades, el equipo Mac debe de estar conectado a Internet.

5.12.1.1 BLOQUEO REMOTO DE OS X DESDE ICLOUD

686. Si se hace uso de las capacidades de "Buscar mi Mac" disponibles en iCloud, y en concreto de la funcionalidad que permite bloquear el ordenador Mac remotamente, a través del botón "Bloquear", no será posible reiniciar el equipo, ya que se establece una contraseña tanto en el firmware del mismo (para modos de arranque especiales) como en el modo de arranque normal.

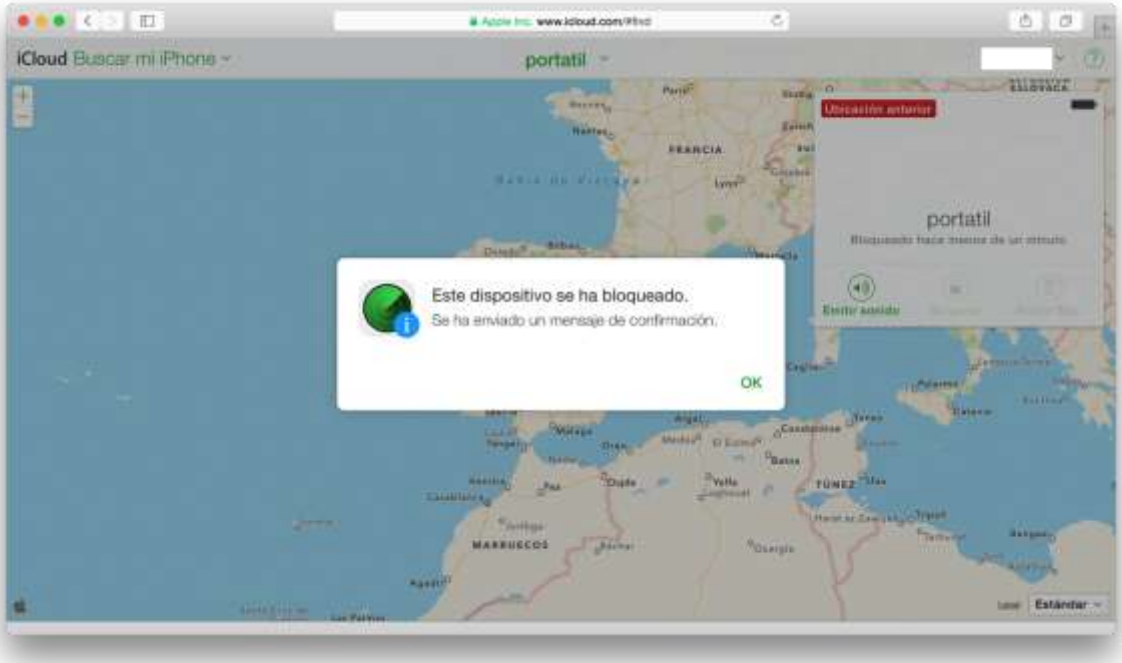
687. Tan pronto OS X recibe la instrucción desde iCloud de bloquear el equipo, mostrará una pantalla de bloqueo solicitando 4 dígitos, correspondientes a la clave de acceso fijada mediante "Buscar mi Mac" en el momento de ejecutar la acción de bloqueo:



688. Adicionalmente, es posible introducir un mensaje personalizado que se mostrará en la pantalla del ordenador Mac, con el objetivo de intentar recuperarlo, por ejemplo, indicando que su propietario está buscando el equipo:

689. Si se hace uso de la funcionalidad para bloquear el ordenador Mac, no podrá hacerse uso de la funcionalidad de borrado remoto, siendo ambas excluyentes entre sí:

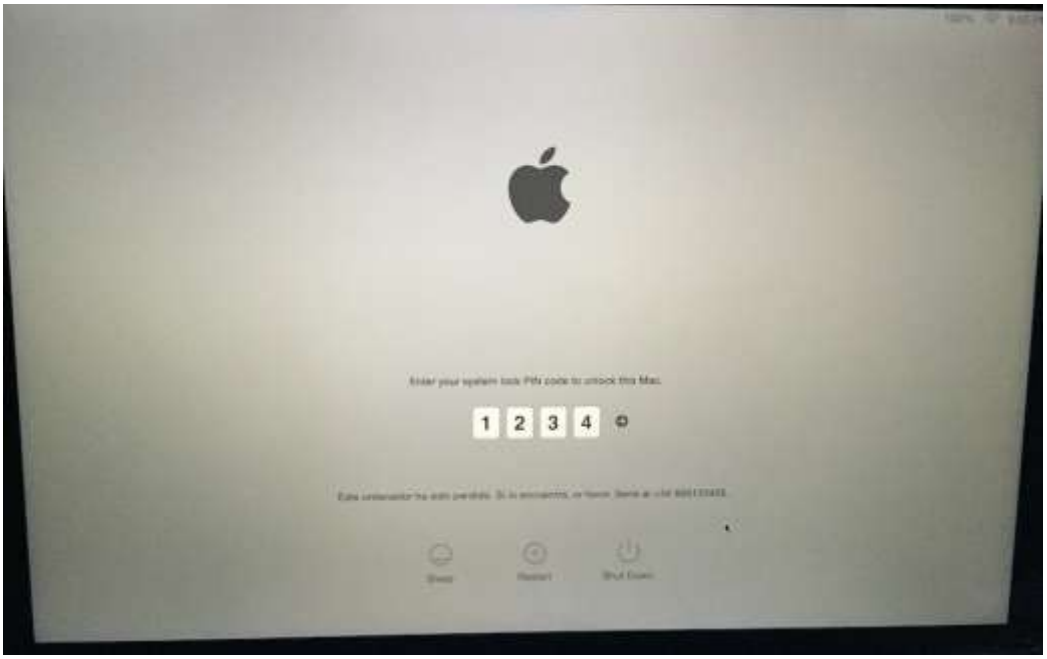
690. Tras la confirmación de la acción de bloqueo, unos segundos después, el ordenador se apagará y mostrará una carpeta blanca con un símbolo de interrogación parpadeando, sobre un fondo negro (de forma similar al escenario en el que el equipo no puede identificar un disco de arranque válido)[113]:



691. Es necesario apagar el equipo, arrancar del gestor de arranque (Alt) o en el modo de recuperación (Cmd+R) y proporcionar en la pantalla estándar que solicita la contraseña del firmware el código de bloqueo establecido en "Buscar mi Mac".

692. Tras progresar con el proceso de arranque del equipo, se mostrará una pantalla con el fondo gris, que solicita de nuevo el código de 4 dígitos de bloqueo establecido en "Buscar mi Mac". Asimismo, esta pantalla muestra el mensaje fijado durante la acción de bloqueo:

[113] Se entiende que este no es el comportamiento esperado ya que, entre otros aspectos, no permite mostrar directamente el mensaje establecido mediante la acción de bloqueo, por lo que está más asociado a un bug en OS X 10.10 Yosemite (ver también un bug asociado en el apartado "5.4.9. Establecer una contraseña en el firmware del equipo").



693. Una vez proporcionado el código correcto, el equipo arrancará normalmente, con la peculiaridad de que en la pantalla de inicio de sesión de FileVault mostrará al "Usuario invitado", y una vez arrancado el sistema operativo, mantendrá el estado en el que se encontraba el equipo en el momento del bloqueo desde iCloud.

5.12.1.2 ELIMINACIÓN DEL PIN DE BLOQUEO DE ICLOUD DESDE OS X

694. En el caso del modo de arranque normal, la protección se establece a nivel de OS X, almacenándose el PIN de bloqueo bajo "/Users/<usuario>/Library/Application Support/iCloud", en concreto en un fichero con nombre "<dígitos>.lock", donde "<dígitos>" corresponde a un conjunto de dígitos (por ejemplo, 10)[114].

695. Existe, por tanto, la posibilidad de extraer el disco duro o sistema de almacenamiento del equipo (si el modelo de ordenador Mac empleado dispone de esta posibilidad[115], o potencialmente con la modalidad de disco de destino), montarlo y acceder a sus contenidos desde otro equipo (Mac o Windows).

696. Una vez identificado el nombre del fichero "<dígitos>.lock", el PIN de bloqueo de iCloud corresponderá a una secuencia de 4 dígitos dentro del conjunto "<dígitos>".

697. Por ejemplo, si el nombre del fichero es "0123456789.lock", las opciones posibles para el valor del PIN son conjuntos secuenciales de 4 dígitos en dicho nombre, es decir, "0123", "1234", "2345", etc.

698. En el caso de llevar a cabo 5 intentos de acceso fallidos, no será posible realizar un intento adicional de acceso hasta pasado un minuto. Este mecanismo de retardo frente a ataques de fuerza bruta incrementa el temporizador exponencialmente, debiendo esperar 5 minutos tras el sexto intento, etc:

[114] http://forums.macrumors.com/threads/how-to-unlock-system-lock-pin-code.1438822/

[115] https://www.ifixit.com/Device/Mac

699. No existe la posibilidad de reiniciar el equipo para que dicha limitación temporal sea eliminada y poder continuar introduciendo combinaciones del valor del PIN. Tras reiniciar desde la espera de 5 minutos, se muestra directamente la espera posterior, de 15 minutos, y posteriormente de 60 minutos, valor límite que permanece constante tras cada intento posterior.

700. Una vez se introduce el valor correcto del PIN de iCloud, el equipo reiniciará en el estado en el que se encontraba en el momento del bloqueo, y el PIN de bloqueo de iCloud será eliminado.

5.12.1.3 FUERZA BRUTA DEL PIN DE BLOQUEO DE ICLOUD

701. En el caso de los modos de arranque especiales, la protección se establece a nivel del firmware, y la pantalla de bloqueo es similar a la pantalla de arranque que solicita la contraseña de firmware (ver apartado "5.4.9. Establecer una contraseña en el firmware del equipo").

702. Al igual que en el caso de dicha pantalla, la pantalla de bloqueo inicial no dispone de ningún mecanismo frente ataques de fuerza bruta para la adivinación de la contraseña, salvo que en este caso se basa en un PIN de 4 a 6 dígitos (escenario que facilita la obtención del PIN) [Ref.- 31]. La segunda pantalla de bloqueo donde debe introducirse de nuevo el código de bloqueo de iCloud sí dispone de mecanismos frente a ataques de fuerza bruta (tal como se ha detallado en el apartado previo).

5.12.1.4 BORRADO REMOTO DESDE ICLOUD

703. Las capacidades de "Buscar mi Mac" disponibles en iCloud también permiten llevar a cabo un borrado remoto del equipo (*remote wipe*) a través del botón "Borrar Mac".

5.13 COMUNICACIONES

704. Los siguientes apartados describen las recomendaciones de seguridad asociadas a los interfaces de red y las capacidades de comunicaciones de OS X.

5.13.1 INTERFACES DE RED

705. Los interfaces de red (o comunicaciones) de OS X emplean la nomenclatura de BSD, que consiste en usar dos o tres letras en función del tipo de interfaz, y un número que corresponde al identificador único del interfaz.

706. Los interfaces de comunicaciones, en función de su tipo (ordenados alfabéticamente), emplean la siguiente nomenclatura, visible mediante el comando "ifconfig":

- awdlX: Apple Wireless Direct Link (AirDrop, AirPlay, etc)[116].
- bridgeX: Puente entre dos o más interfaces.
- enX: Ethernet o Wi-Fi.
- fwX: FireWire.
- gifX: Generic tunnel Interface (GIF) - IPv[46] sobre IPv[46].
- loX: Loopback.
- p2pX: Peer to peer (AirDrop).
- stfX: 6to4 tunnel interface (IPv6 sobre IPv4).

707. En los últimos modelos de MacBook el principal interfaz de comunicaciones de datos es el interfaz Wi-Fi (tarjeta Airport), por lo que es asignado al primer interfaz de red, en0.

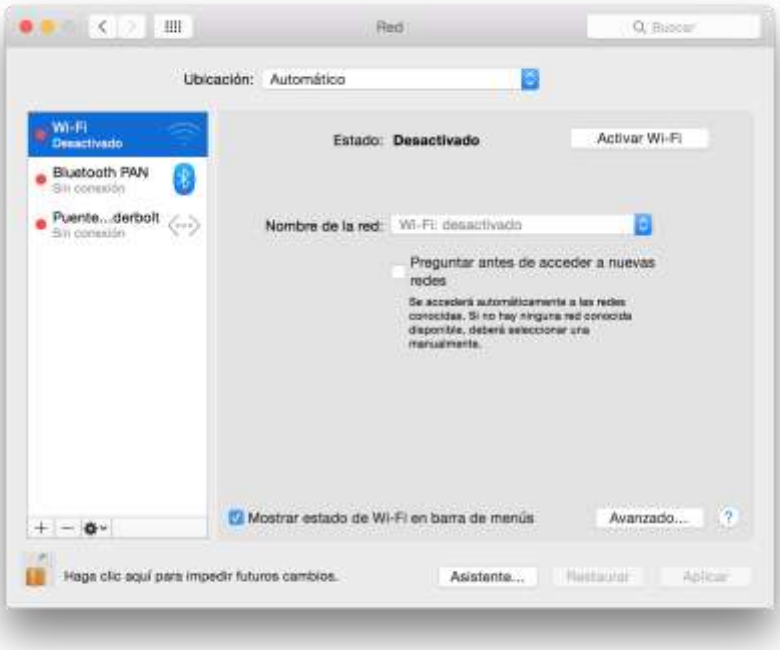
708. Por defecto, para el MacBook Pro empleado para la elaboración de la presente guía, OS X Yosemite dispone de:

- El interfaz de loopback, lo0.
- Un interfaz awdl0 y un interfaz p2p0, para las conexiones mediante AirDrop.
- Un interfaz gif0 y stf0, para los túneles entre los protocolos IPv4 e IPv6.
- Un interfaz bridge0, asociado a los interfaces en1 y en2, es decir, un puente entre los dos puertos Thunderbolt disponibles en el equipo.
- Tres interfaces enX:
  - en0, correspondiente al interfaz Wi-Fi integrado.
  - en1 y en2, correspondientes a los dos puertos Thunderbolt disponibles en el equipo.

709. El conjunto de interfaces de red disponibles por defecto puede variar dependiendo del modelo de ordenador Mac empleado y de su hardware asociado.

710. No es sencillo establecer un paralelismo directo entre los interfaces de red disponibles a través del comando "ifconfig" y los interfaces de red mostrados en el panel de la izquierda desde "Preferencias del Sistema - Red", ya que en el mismo (con la ubicación "Automático" definida por defecto) sólo aparecen el interfaz Wi-Fi, el interfaz Bluetooth PAN (*Personal Area Network*), y el "Puente Thunderbolt":

[116] https://medium.com/@mariociabarra/wifriedx-in-depth-look-at-yosemite-wifi-and-awdl-airdrop-41a93eb22e48

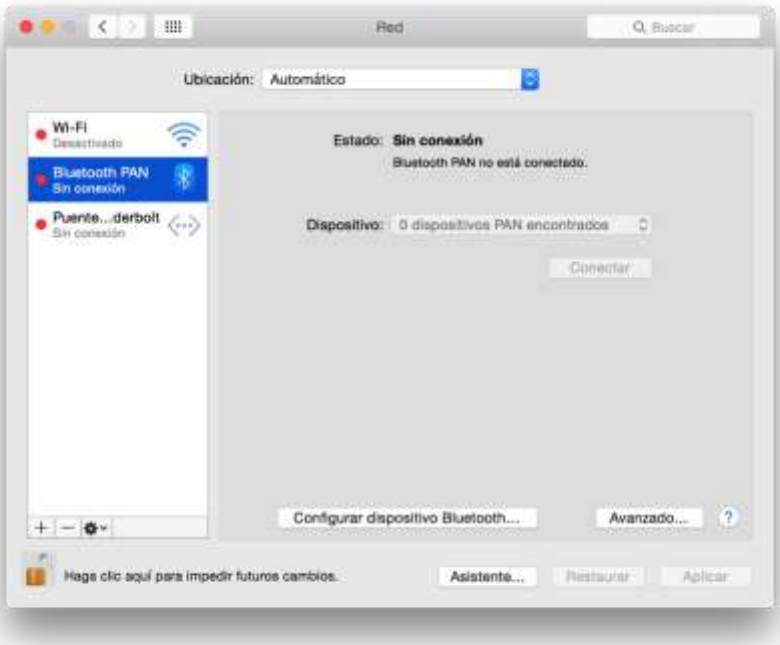


711. Adicionalmente, la utilidad "networksetup" permite consultar los interfaces de red disponibles en el equipo junto a sus direcciones físicas o MAC, así como llevar a cabo su gestión, desde un terminal:

```
$ networksetup -listallhardwareports
```

712. La salida de "networksetup" muestra la existencia del interfaz Bluetooth DUN (*Dial-Up Networking*, o módem Bluetooth), no visible previamente, así como la asignación del interfaz "en3" a Bluetooth PAN (no visible a través de "ifconfig"), y la asignación de "en1" y "en2" a los puertos Thunderbolt.

713. Si no se va a hacer uso de la conexión de red de "Bluetooth PAN" se recomienda eliminarla mediante el botón "-". Para que los cambios surtan efecto es necesario pulsar el botón "Aplicar". A través del botón "Avanzado…" se puede establecer la configuración TCP/IP y DNS para este interfaz:



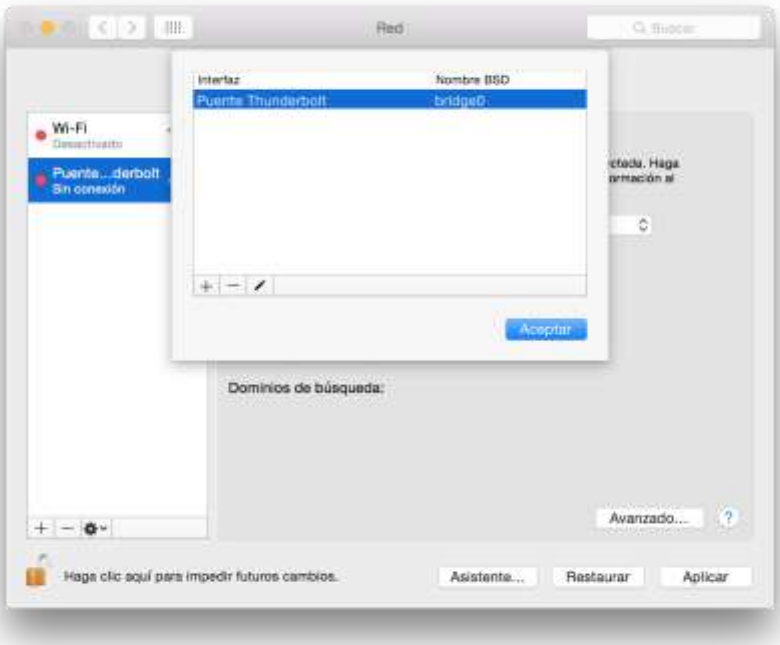
714. El "Puente Thunderbolt" se engloba dentro de la categoría de interfaces virtuales en OS X, disponibles desde la configuración de red, a través del botón o icono con un engranaje (a la derecha de los botones "+" y "-"), mediante la opción "Gestionar interfaces virtuales…". Desde esta opción de configuración es posible gestionar interfaces de red de tipo puente, VLAN (*Virtual LAN*) y agregaciones de enlaces:

715. El propósito del "Puente Thunderbolt" creado por defecto por OS X es poder transferir datos directamente entre equipos Mac (con OS X Mavericks o superior) a través de un cable Thunderbolt sin necesidad de hacer uso de otros métodos, como los servicios compartidos (ver apartado "5.13.6. Servicios compartidos": AFP o SMB, SSH, etc), AirDrop, etc[117]:

[117] Imagen obtenida de: http://arstechnica.com/apple/2013/10/os-x-10-9-brings-fast-but-choppy-thunderbolt-networking/.

716. Las conexiones Thunderbolt ofrecen un interfaz de comunicación de muy alta velocidad, pudiendo alcanzar los 10 Gb/s (o incluso 20 Gb/s para los puertos Thunderbolt 2[118]), y son utilizados, por ejemplo, por el Asistente de Migración para traspasar todos los datos de un equipo Mac antiguo a uno nuevo.

717. Si no se va a hacer uso de la conexión de red del "Puente Thunderbolt" se recomienda eliminarla mediante el botón "-". Para que los cambios surtan efecto es necesario pulsar el botón "Aplicar". A través del botón "Avanzado…" se puede ver el estado del puente y sus interfaces, así como establecer la configuración TCP/IP, DNS, WINS, de proxies y del hardware para este interfaz:



718. En caso de requerir hacer uso de esta conexión en el futuro, puede volver a agregarse mediante el botón "+", seleccionando en el tipo de interfaz "Puente Thunderbolt":

[118] http://www.apple.com/thunderbolt/

719. La eliminación de los interfaces de red de la ubicación empleada en las preferencias de red no elimina dichos interfaces a nivel de sistema operativo, por lo que siguen siendo visibles mediante el comando "ifconfig".

720. Finalmente, el interfaz "Wi-Fi" (integrado en los equipos Mac portátiles) constituye el interfaz de red principal para su conexión hacia redes de datos y comunicaciones, salvo que se haga uso de un interfaz de red Gigabit Ethernet conectado a uno de los puertos Thunderbolt del equipo (identificado como "Thunderbolt Ethernet"):

721. En la nomenclatura de OS X, los interfaces de red son denominados servicios, y desde la configuración de red, a través del botón o icono con un engranaje (a la derecha de los botones "+" y "-"), es posible gestionar los servicios (o interfaces de red) duplicándolos, renombrándolos o desactivándolos. Asimismo, se puede establecer el orden de prioridad de los servicios en el caso de que varios estén activos simultáneamente, como por ejemplo el interfaz Wi-Fi y el interfaz Ethernet. Por último, es posible importar la configuración de red desde un fichero.

722. De manera general, se recomienda deshabilitar todos los interfaces de red (o servicios), protocolos y capacidades de comunicaciones que no están siendo utilizados, con el objetivo de limitar las posibles puertas de entrada no autorizadas al equipo.

5.13.2 CONFIGURACIÓN DE LOS INTERFACES DE RED

723. El presente apartado se centra principalmente en la configuración del interfaz de red Wi-Fi disponible por defecto en OS X, e integrado en los equipos Mac portátiles, considerando que constituye el interfaz de red principal para la conexión del ordenador hacia redes de datos y comunicaciones externas.

724. En el caso de hacer uso de un interfaz de red Gigabit Ethernet conectado a uno de los puertos Thunderbolt del equipo (identificado como "Thunderbolt Ethernet"), el proceso de configuración es muy similar, debiendo obviar los aspectos propios de las redes Wi-Fi.

725. Se recomienda llevar a cabo la configuración del interfaz de red Wi-Fi antes de activarlo, con el objetivo de evitar potenciales ataques durante el proceso de configuración.

726. Desde "Preferencias del Sistema - Red", tras seleccionar el interfaz de red Wi-Fi y mediante el botón "Avanzado…", es posible configurar diferentes aspectos del interfaz, como la configuración Wi-Fi (ver apartado "5.13.12. Wi-Fi"), TCP/IP, DNS, WINS, 802.1X, de proxies y del hardware.

727. La configuración y recomendaciones de seguridad de otros aspectos asociados al interfaz Wi-Fi, como sus capacidades de bajo nivel respecto a los protocolos Wi-Fi (IEEE 802.11), la configuración de proxies o la configuración IPv6, son detalladas en apartados posteriores (ver apartados "5.13.12. Wi-Fi", "5.13.3. Proxies" y "5.13.5. IPv6" respectivamente).

728. Desde la pestaña "TCP/IP" es posible establecer la configuración de IPv4, asignando una dirección IP dinámicamente mediante DHCP (opción por defecto), una dirección IP estática configurada manualmente, o incluso deshabilitar (o desactivar) la pila TCP/IP (versión 4) en el interfaz de red asociado:

729. La pestaña "DNS" permite especificar (o mostrar en el caso de una configuración mediante DHCP) los servidores DNS y los dominios de búsqueda.

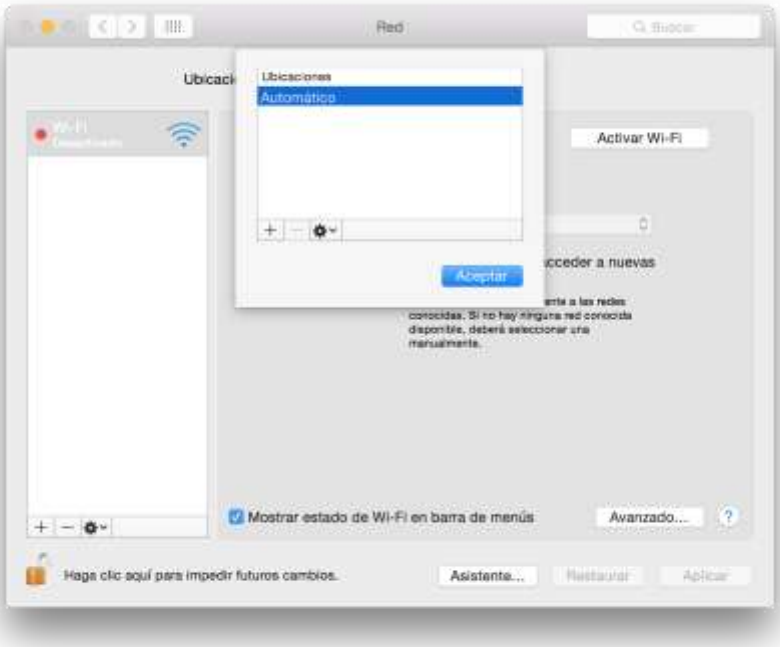
730. La pestaña "WINS" permite definir el nombre NetBIOS del equipo (por defecto con el mismo valoe que el nombre del equipo pero en mayúsculas, ver apartado "5.2. Nombre de equipo"), el grupo de trabajo (por defecto, "WORKGROUP") y los servidores WINS.

731. La pestaña "802.1X" permite mostrar los datos de conexión mediante 802.1X. El administrador del entorno puede definir perfiles de autorización 802.1X para la conexión del equipo a la red, mediante el uso de perfiles de configuración (".mobileconfig") de OS X[119].

732. La pestaña "Hardware" muestra la dirección física o MAC del interfaz de red, y la configuración (automática, por defecto, o manual) del tamaño máximo de trama (MTU, *Maximum Transmission Unit*) o de otros aspectos relacionados con la velocidad y el modo (*duplex*) del interfaz de red (en el caso de interfaces Ethernet).

733. La gestión de las configuraciones de red en OS X se lleva a cabo a través de ubicaciones (o localizaciones), que permiten almacenar diferentes perfiles o configuraciones de red.

734. Por defecto OS X crea la ubicación "Automático" (referenciada como "Automatic" internamente), con la configuración de interfaces de red detallada en el apartado previo:



735. Cada ubicación tiene definido el conjunto de interfaces de red a emplear. Cuando se crea una nueva ubicación, mediante los ajustes de red, desde la lista de ubicaciones superior y la opción "Editar ubicaciones…" (junto al botón "+"), por defecto se añaden todos los interfaces de red detallados en el apartado previo para la ubicación "Automático".

736. La utilidad "networksetup" permite llevar a cabo la gestión de las ubicaciones desde un terminal:

[119] https://support.apple.com/kb/PH18542

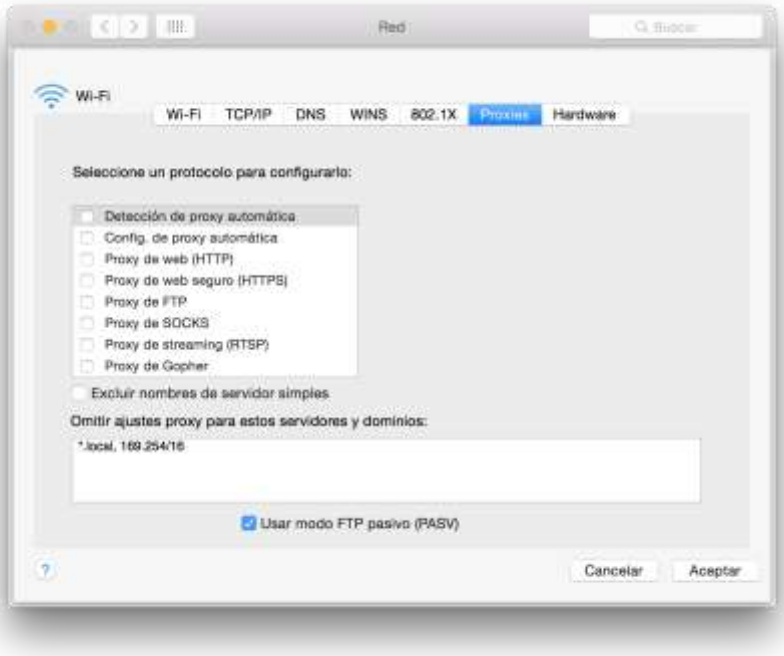
```
$ networksetup -listlocations
Automatic
$ networksetup -createlocation <nombre-ubicacion> populate
$ networksetup -switchtolocation <nombre-ubicacion>
$ networksetup -deletelocation Automatic
```

737. Se recomienda limitar el número de ubicaciones definidas, en función del uso y tipo de redes a las que se conecta el equipo habitualmente, y configurar exhaustivamente cada una de ellas, limitando la lista de interfaces de red (o servicios) disponibles y aplicando las recomendaciones de seguridad a cada uno de los interfaces de red descritas en la presente guía.

5.13.3 PROXIES

738. En el caso de ser necesario configurar un proxy[120] para poder establecer conexiones hacia Internet o hacia otros servicios o redes remotas, se recomienda no hacer uso de las capacidades automáticas de detección de proxies, ya que estos protocolos pueden ser manipulados por un potencial atacante y, como resultado, redirigir el tráfico del ordenador Mac hacia el equipo del atacante.

739. Se recomienda por tanto no habilitar la opción "Detección de proxy automática" disponible desde "Preferencias del Sistema - Red", tras seleccionar el interfaz de red y hacer uso del botón "Avanzado…", desde la pestaña "Proxies":



[120] https://support.apple.com/kb/PH18553

740. Por otro lado, si se hace uso de la opción "Config. de proxy automática" desde la misma pantalla de configuración, se recomienda verificar que la dirección o URL que especifica el archivo de configuración de proxy hace uso del protocolo HTTPS (en lugar de HTTP), para evitar manipulaciones del fichero ".pac" o PAC (*Proxy Automatic Configuration*):

741. El resto de opciones de configuración de la pestaña "Proxies" simplemente permiten configurar la dirección IP o el nombre del servidor proxy, y el puerto donde ofrece su servicio, para distintos protocolos: HTTP, HTTPS, FTP, SOCKS, RTSP y Gopher. Adicionalmente esta pantalla permite configurar el uso de FTP en modo pasivo, mediante la opción "Usar modo FTP pasivo (PASV)" (habilitada por defecto).

5.13.4 BONJOUR

742. En OS X Yosemite es posible deshabilitar Bonjour mediante los siguientes comandos, asociados a los procesos "discoveryd" y "discoveryd_helper". En versiones previas de OS X se hacía uso de "/usr/bin/mDNSResponder" (y la opción "-NoMulticastAdvertisements"):

```
$ sudo launchctl unload -w
/System/Library/LaunchDaemons/com.apple.discoveryd.plist
$ sudo launchctl unload -w
/System/Library/LaunchDaemons/com.apple.discoveryd_helper.plist
```

743. Como resultado se finalizará la ejecución de ambos procesos, disponibles bajo "/usr/libexec/".

744. Mediante los siguientes comandos es posible volver a activar Bonjour, incluyendo los dos procesos mencionados:

```
$ sudo launchctl load -w
/System/Library/LaunchDaemons/com.apple.discoveryd_helper.plist
$ sudo launchctl load -w
/System/Library/LaunchDaemons/com.apple.discoveryd.plist
```

5.13.5 IPV6

745. Desde "Preferencias del Sistema - Red", tras seleccionar el interfaz de red Wi-Fi y mediante el botón "Avanzado…", es posible configurar diferentes aspectos del interfaz, como la configuración TCP/IP, y en concreto, IPv6.

746. Desde la pestaña "TCP/IP" es posible establecer la configuración de IPv6 (habilitado por defecto desde OS X 10.3[121]), asignando una dirección IP automáticamente (opción por defecto), una dirección IP estática configurada manualmente, o definiendo que se trata de un enlace local de IPv6.

747. Sin embargo, desde el interfaz gráfico de usuario no es posible deshabilitar la pila TCP/IP versión 6 en el interfaz de red asociado, opción recomendada desde el punto de vista de seguridad si no se está haciendo uso de IPv6, sino únicamente de IPv4.

748. Para ello es necesario emplear el siguiente comando desde un terminal, que deshabilitará la pila IPv6 para los interfaces de red indicados. En el caso de hacer uso de una ubicación con múltiples interfaces de red (o servicios), será necesario deshabilitarlo para cada uno de ellos:

```
$ networksetup -listallnetworkservices
Bluetooth DUN
Wi-Fi

$ sudo networksetup -setv6off Wi-Fi
$ sudo networksetup -setv6off "Bluetooth DUN"

$ networksetup -getinfo Wi-Fi
...
IPv6: Off
```

749. El primer comando muestra todos los servicios (o interfaces de red) definidos en la ubicación actual. Como se puede ver, el servicio "Bluetooth DUN" aparece listado aunque no se muestre en la configuración de red gráfica de OS X[122].

750. Para cada servicio definido es necesario ejecutar el segundo conjunto de comandos[123], deshabilitando de manera efectiva IPv6, tal como denotan los ajustes de configuración de red.

[121] http://support.apple.com/kb/HT4667

[122] Incluso aún desactivando la ejecución del proceso de Bluetooth (blued), el servicio sigue apareciendo listado.

[123] En el caso de no hacer uso de "sudo", se solicitarán al usuario estándar las credenciales de un usuario adminstrador.

751. Accediendo a "Preferencias del Sistema - Red", tras seleccionar el interfaz de red Wi-Fi y mediante el botón "Avanzado…", desde la pestaña "TCP/IP", es posible confirmar que la opción "Configurar IPv6" muestra el valor "Desactivada", no disponible previamente:

752. Adicionalmente es posible confirmar el cambio de configuración desde un terminal mediante el tercer comando, que obtiene información de la configuración del servicio.

753. Adicionalmente, si se crea una nueva ubicación, será de nuevo necesario deshabilitar la pila de IPv6 en cada uno de los interfaces de red definidos en la nueva ubicación.

5.13.6 SERVICIOS COMPARTIDOS

754. OS X dispone de la posibilidad de habilitar numerosos servicios compartidos, que facilitan el acceso remoto a través de la red al equipo o la compartición de datos, información y archivos con otros ordenadores o servicios.

755. A través de "Preferencias del Sistema - Compartir", además de establecer el nombre del equipo, desde la columna de la izquierda, es posible configurar cada uno de los servicios compartidos existentes:

756. Por defecto, todos los servicios compartidos están deshabilitados en OS X. Se recomienda deshabilitar completamente todas las capacidades de compartición de OS X para evitar la posibilidad de recibir conexiones entrantes solicitando acceso a los contenidos o al propio equipo.

757. En caso de requerir hacer uso de alguno de los servicios de compartición, se recomienda activarlos temporalmente, hacer uso de los mismos, y desactivarlos inmediatamente tras finalizar la sesión asociada.

758. Los diferentes servicios compartidos permiten múltiples accesos remotos a OS X a través de la red[124]:

- Compartir pantalla: acceso remoto gráfico al ordenador, para poder ver y manejar el escritorio, hacer uso del portapapeles compartido[125], e incluso reiniciar el equipo.
- Compartir archivos: acceso a las carpetas compartidas del ordenador.
- Compartir impresora: acceso a las impresoras definidas y/o conectadas al ordenador.
- Sesión remota: acceso mediante SSH y SFTP.
- Gestión remota: acceso mediante Apple Remote Desktop.
- Eventos Apple remotos: recepción de eventos Apple desde otros ordenadores OS X.

[124] En base al modelo de ordenador Mac empleado y sus características hardware, también se puede disponer del servicio "Compartir CD o DVD": https://support.apple.com/kb/PH18717.

[125] https://support.apple.com/kb/PH18693

- Compartir Internet: compartir la conexión a Internet (de uno de los interfaces de red) del ordenador con otros ordenadores a través de la red local.
- Compartir Bluetooth: acceso a archivos a través de Bluetooth.

759. Algunos servicios compartidos disponen de opciones de configuración comunes, mientras que otros presentan opciones de configuración propias y más avanzadas.

760. Los servicios con opciones de configuración comunes, como son Compartir pantalla, Sesión remota, Gestión remota, y Eventos Apple remotos, permiten habilitar o deshabilitar el servicio de compartición, así como definir a quién se le permite acceso al servicio: "Todos los usuarios" (es decir, cualquier usuario con cuenta en el ordenador) o "Solo a estos usuarios", definiendo una lista de usuarios específicos permitidos (que pueden ser tanto usuarios o grupos locales, como de red).

761. Por defecto, Compartir pantalla y Sesión remota soló permiten el acceso al grupo de administradores (*Administrators*), mientras que Gestión remota y Eventos Apple remotos permiten el acceso a todos los usuarios por defecto, opciones que deberían ser restringidas y personalizadas si se hace uso de estos servicios.

762. Para la mayoría de servicios compartidos, una vez activados, el panel de configuración muestra los detalles necesarios para establecer la conexión con el servicio y su estado.

5.13.6.1 COMPARTIR PANTALLA

763. Compartir pantalla [Ref.- 62], a través del botón "Ajustes del ordenador…", permite definir si otros usuarios pueden compartir su pantalla sin tener una cuenta de usuario en el ordenador:

764. Mediante la primera opción cualquier usuario puede pedir permiso para compartir o controlar la pantalla, en lugar de autentificarse con una cuenta de usuario. La segunda opción permite establecer una contraseña para que las aplicaciones cliente VNC (*Virtual Network Computing*, por ejemplo, desde un equipo Windows o un iPad) puedan compartir la

pantalla, tras introducir la contraseña especificada. Ambas opciones están deshabilitadas por defecto:

765. En caso de hacer uso de este servicio, desde el punto de vista de seguridad, se recomienda habilitar la primera opción de manera temporal, y en caso de habilitar la segunda opción, establecer una contraseña suficientemente robusta.

766. En caso de hacer un uso esporádico, pero reiterado de este servicio, se recomienda crear una cuenta de usuario sólo para compartir (ver apartado "5.13.6.2. COMPARTIR ARCHIVOS").

767. Si el servicio Gestión remota está activo, debe deshabilitarse para poder activar Compartir pantalla.

768. El acceso al servicio Compartir pantalla se puede realizar desde otro ordenador con OS X a través del Finder y de la categoría Compartido, seleccionando el ordenador con el que compartir la pantalla (qué tiene el servicio activo)[126].

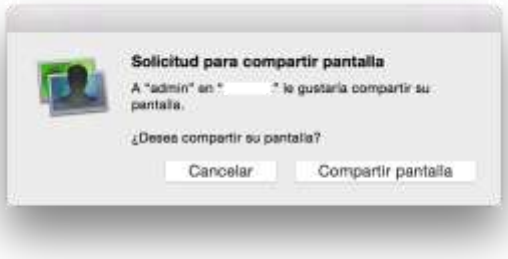
769. Adicionalmente se puede acceder al otro ordenador desde el Finder, mediante la opción "Ir - Conectarse al servidor…" y especificando "vnc://<dirección IP o nombre del equipo>" como dirección del servidor:

[126] https://support.apple.com/kb/PH18688

770. Es posible acceder al servicio como invitado, pudiendo visualizar la pantalla pero no controlarla, solicitando permiso (si no se dispone de cuenta de usuario en el ordenador remoto), mediante una cuenta de usuario autorizada, o con un ID de Apple si está registrado como usuario en ambos equipos.

771. Es posible que varios usuarios accedan al servicio Compartir pantalla simultáneamente, compartiendo la misma pantalla o pantallas (o sesiones) independientes, y es posible ajustar las preferencias[127] y opciones de visualización[128] desde la sesión actual de Compartir pantalla.

772. En el caso de compartir la misma pantalla, se solicita autorización al usuario antes de permitir el acceso (independientemente de que se disponga de una cuenta de usuario válida):



[127] https://support.apple.com/kb/PH18691

[128] https://support.apple.com/kb/PH18692

773. En el caso de compartir la pantalla en una sesión independiente, se indica la existencia de una sesión desde la barra de menús, a través del icono de Compartir pantalla, desde donde se dispone de la opción "Desconectar <dirección IP>" para cerrar la sesión del cliente actualmente conectado desde la dirección IP indicada:

774. El cierre de sesión será notificado al cliente de Compartir pantalla, indicando que la sesión ha finalizado porque ha sido cerrada por un usuario remoto.

775. Existe la posibilidad de habilitar (o deshabilitar) Compartir pantalla desde un terminal, empleando el proceso estándar de habilitar una propiedad en el fichero de configuración PLIST correspondiente mediante "defaults", y cargando el servicio mediante "launchctl":

```
$ sudo defaults write
/System/Library/LaunchDaemons/com.apple.screensharing.plist Disabled 0

$ sudo launchctl load -w
/System/Library/LaunchDaemons/com.apple.screensharing.plist
```

Nota: si se emplea este método manual para habilitar y deshabilitar Compartir pantalla, también convendría parar manualmente el proceso de kerberos (kdc) asociado a Compartir pantalla.

776. Si se emplea el proceso de activación desde un terminal, el servicio es activado y aparece como tal en el panel de detalles de preferencias de "Compartir", aunque el símbolo de la columna "Activo" no refleja adecuadamente el estado del servicio (esta situación es similar para todos los servicios compartidos).

777. Al activar Compartir pantalla por primera vez se solicita autorización al usuario por parte del cortafuegos para que la aplicación (o procesos) "launchd" y "kdc" (kerberos) puedan aceptar conexiones entrantes:

778. Compartir pantalla hace uso del puerto TCP/5900 (rfb o vnc-server), como del puerto TCP/88 y UDP/88 (kerberos), tanto empleando IPv4 como IPv6.

5.13.6.2 COMPARTIR ARCHIVOS

779. El panel de la izquierda de Compartir archivos [Ref.- 63] permite definir las carpetas compartidas, creándose por defecto una para cada usuario existente con el nombre "Carpeta pública de '<nombre de usuario>'" (estas carpetas corresponden a la carpeta "Public"

disponible bajo "/Users/<usuario>" para cada usuario, que contiene una carpeta "Drop Box" por defecto), y el panel de la derecha permite establecer qué usuarios tendrán acceso a cada carpeta y con qué permisos:

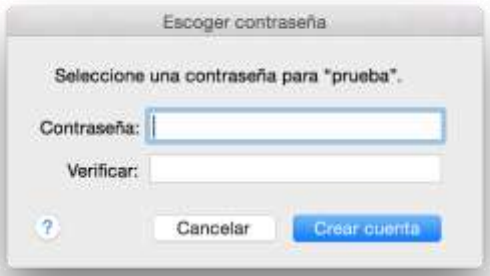
780. Por defecto, el propio usuario dispone de permiso de lectura y escritura a su carpeta compartida (el usuario puede ver y copiar archivos en y desde la carpeta), mientras que el grupo "Staff" y el grupo "Todos" sólo disponen de permiso de lectura. Adicionalmente se puede asignar el permiso de sólo escritura, para implementar la funcionalidad de un buzón de entrada o recepción de archivos. En el caso del grupo "Todos" alternativamente se puede asignar el permiso "Sin acceso", bloqueando el acceso a la carpeta.

781. Se recomienda evaluar y ajustar en detalle las carpetas que son compartidas y los usuarios y grupos qué tendrán acceso a las mismas, y con qué y permisos, debiéndose reducir el acceso al mínimo imprescindible para el propósito por el que ha sido habilitado el servicio.

782. Existe la posibilidad de crear una cuenta de usuario sólo para hacer uso de las capacidades de compartir de OS X, en concreto, desde los ajustes de la columna de "Usuarios" de Compartir archivos, mediante el botón que permite añadir un usuario o grupo ("+").

783. Para ello, es necesario crear en primer lugar un contacto con el nombre de la cuenta de usuario deseado, y posteriormente, tras seleccionar la categoría "Contactos" (tras pulsar el botón "+") y tras seleccionar el contacto concreto (botón "Seleccionar"), se le puede asignar una contraseña[129] (por defecto este usuario tiene asignado el permiso de "Solo lectura"):

[129] https://support.apple.com/kb/PH18695

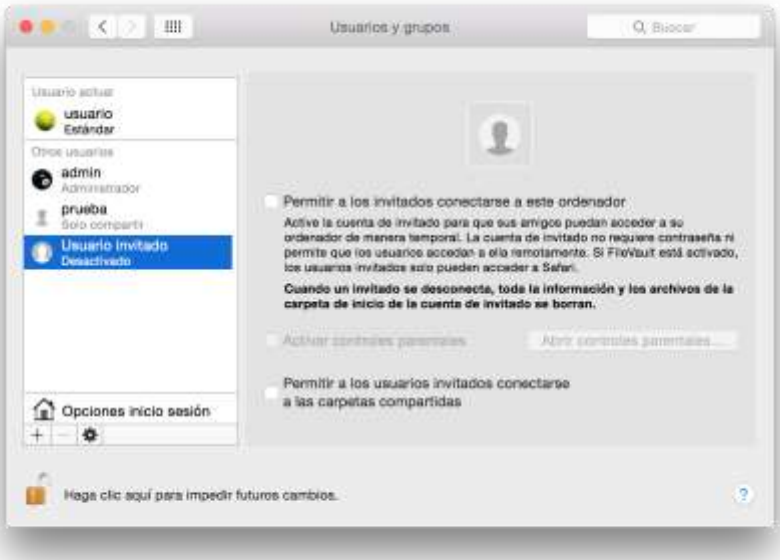


784. Como resultado, se creará una nueva cuenta de usuario, visible desde "Preferencias del Sistema - Usuarios y grupos", cuyo tipo es "Solo compartir" y para la que sólo es posible modificar la contraseña (no siendo además necesario introducir la contraseña actual para realizar el cambio de la misma):

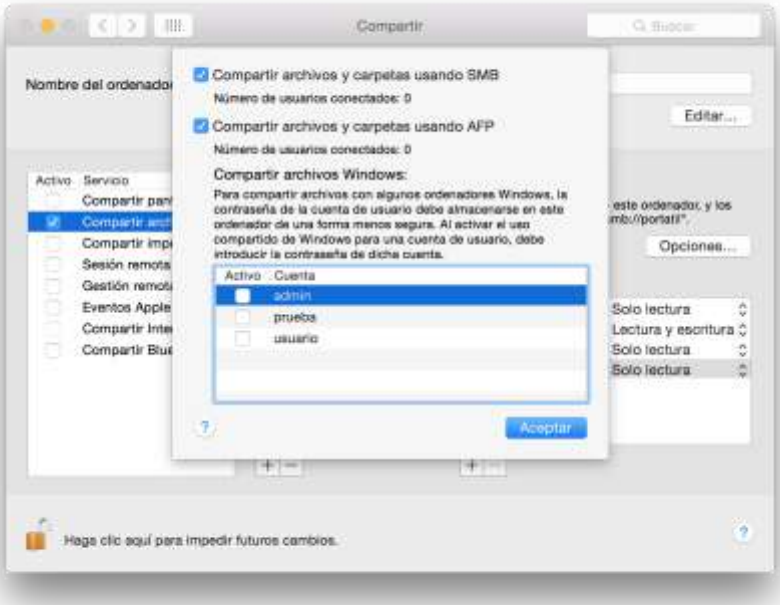
785. En caso de hacer un uso esporádico, pero reiterado de este servicio de compartición de archivos, se recomienda crear una cuenta de usuario solo para compartir, en lugar de una cuenta de usuario estándar.

786. OS X dispone de la capacidad de permitir a los usuarios invitados acceder a las carpetas compartidas del equipo.

787. Se recomienda deshabilitar esta funcionalidad (desactivada por defecto) mediante la desactivación de la opción “Permitir a los usuarios invitados conectarse a las carpetas compartidas” desde "Preferencias del Sistema - Usuarios y grupos”, dentro de la cuenta de "Usuario invitado”:



788. El botón "Opciones…" de Compartir archivos permite definir los protocolos que serán empleados para la compartición de archivos, SMB (*Server Message Block*, empleado por Windows) y/o AFP (*Apple Filing Protocol*, empleado por equipos Apple), ambos habilitados por defecto una vez se activa el servicio:



789. Por defecto, OS X Yosemite intenta hacer uso de la versión 3 de SMB (SMB3) [Ref.- 87] (por ejemplo, entre equipos Mac o con Windows 8 ó 10), la cual dispone de numerosos mecanismos de seguridad asociados, como cifrado extremo a extremo mediante AES-CCM, firma de paquetes mediante AES-CMAC para asegurar la integridad de los datos intercambiados, y autentificación mediante Kerberos y/o NTLMv2.

790. Desde esta misma pantalla es posible monitorizar el número de usuarios conectados actualmente al servicio independientemente para cada tipo de protocolo empleado.

791. Asimismo se puede activar la compartición de archivos con ordenadores Windows, pero se advierte de que puede ser necesario almacenar la contraseña en OS X de manera menos segura. A la hora de activar este servicio para cada usuario, es necesario introducir su contraseña, con el objeto de almacenarla en el formato adecuado para disponer de compatibilidad con algunas versiones de Windows.

792. Se recomienda intentar evitar llevar a cabo la compartición de archivos entre ordenadores Mac y ordenadores Windows, y en caso de hacerlo, comprobar en detalle todas las opciones de configuración en ambos sistemas operativos para hacer uso de los mecanismos de autentificación compatibles más robustos, como NTLMv2 o Kerberos.

793. En caso de que fuese necesario habilitar el almacenamiento inseguro de la contraseña para algún usuario específico, se recomienda eliminar la contraseña mediante el botón de la columna "Activo" para dicho usuario tan pronto se finalice la utilización del servicio, y se recomienda hacerlo incluso antes de deshabilitar el servicio. Para deshabilitar esta funcionalidad para un usuario específico, es necesario introducir su contraseña.

794. El acceso al servicio Compartir archivos se puede realizar desde otro ordenador con OS X a través del Finder y de la categoría Compartido, seleccionando el ordenador al que se desea acceder a sus carpetas compartidas (qué tiene el servicio activo)[130].

795. Adicionalmente se puede acceder al otro ordenador desde el Finder, mediante la opción "Ir - Conectarse al servidor…" y especificando "afp://<dirección IP o nombre del equipo>" o "smb://<dirección IP o nombre del equipo>" como dirección del servidor.

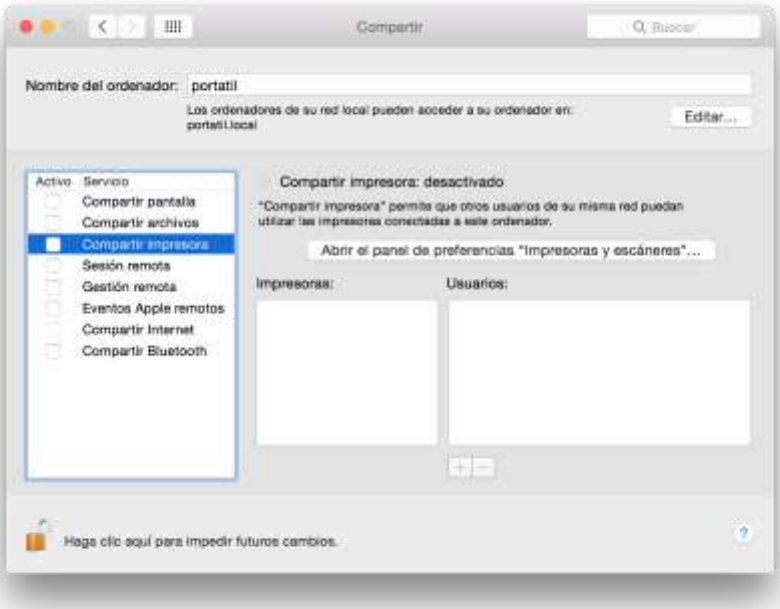
796. Compartir archivos hace uso de los puertos TCP/445 (microsoft-ds), TCP/548 (afpovertcp), así como del puerto TCP/88 y UDP/88 (kerberos), tanto empleando IPv4 como IPv6.

5.13.6.3 COMPARTIR IMPRESORA

797. El panel de la izquierda de Compartir impresora [Ref.- 64] permite seleccionar las impresoras compartidas, de la lista de impresoras locales o de red[131] definidas en OS X, y el panel de la derecha permite establecer qué usuarios tendrán acceso a cada impresora (debiendo estar en la misma red local que el equipo) y con qué permisos:

[130] https://support.apple.com/kb/PH18718

[131] Habitualmente el servicio Compartir impresora se emplea para compartir impresoras locales directamente conectadas al ordenador Mac, pero nada impide re-compartir una impresora actualmente disponible en la red local.



798. Por defecto, el grupo "Todos" dispone de permiso para imprimir. Adicionalmente se pueden añadir excepciones más restrictivas para que ciertos usuarios y/o grupos no dispongan de este acceso existente por defecto.

799. Sin embargo, al añadir un nuevo usuario específico para una impresora, el acceso por defecto de "Todos" cambia automáticamente a "Sin acceso", ya que el único permiso disponible es el que permite al nuevo usuario tener acceso y, por tanto, imprimir en la impresora.

800. Se recomienda evaluar y ajustar en detalle las impresoras que son compartidas y los usuarios y grupos que tendrán capacidad para imprimir en las mismas, debiéndose minimizar el acceso a aquel imprescindible para el propósito por el que ha sido habilitado el servicio.

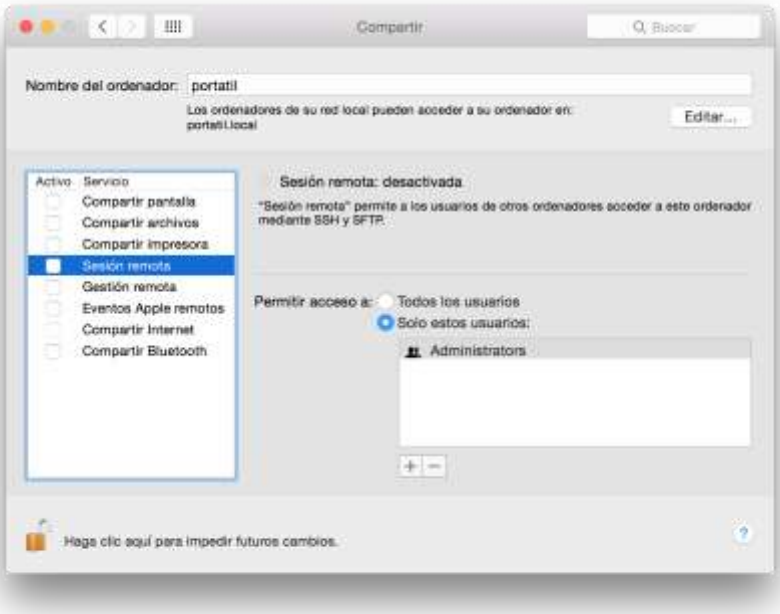
801. El botón "Abrir el panel de preferencias 'impresoras y escáneres'…" permite abrir los ajustes de configuración de impresoras y escáneres.

802. Compartir impresora hace uso del puerto TCP/631 (ipp, *Internet Printing Protocol*), tanto empleando IPv4 como IPv6, en todos los interfaces de red, en lugar de sólo en el interfaz de loopback (como ocurre en el escenario por defecto), asociado al proceso "cupsd".

5.13.6.4 SESIÓN REMOTA

803. Las capacidades del servicio de Sesión remota [Ref.- 65] permiten acceder remotamente a OS X a través de SSH y SFTP, empleando el puerto TCP/22.

804. Se recomienda modificar la configuración por defecto de acceso de usuarios y grupos y solo permitir el acceso a usuarios específicos (preferiblemente no administradores) si se desea hacer uso de este servicio. Sería posible obtener acceso como administrador posteriormente mediante SSH empleando los comandos "su" y/o "sudo":



805. El acceso al servicio de Sesión remota se puede realizar desde otro ordenador con un cliente SSH o SFTP, especificando el nombre de usuario y la dirección IP o nombre del equipo: "`$ ssh usuario@<dirección IP o nombre del equipo>`".

806. El puerto TCP empleado por defecto por Sesión remota para el servicio SSH (TCP/22) puede ser modificado en el fichero PLIST de configuración, "/System/Library/LaunchDaemons/ssh.plist", sustituyendo el valor de la directiva "SockServiceName", que por defecto indica "ssh", por el número de puerto a emplear:

```
<key>SockServiceName</key>
<string>ssh</string>

<key>SockServiceName</key>
<string>22222</string>
```

807. Existe la posibilidad de comprobar el estado del servicio Sesión remota, así como habilitar y deshabilitar Sesión remota desde un terminal:

```
$ sudo systemsetup -getremotelogin

$ sudo systemsetup -setremotelogin on
$ sudo systemsetup -setremotelogin off
```

808. Existe también la posibilidad de habilitar o deshabilitar un servidor SSH, y servidores FTP o Telnet, en OS X desde un terminal, opciones desaconsejadas desde el punto de vista de seguridad, en el primer caso porque no se aplicarán los controles de acceso del servicio de

Sesión remota, y en el segundo debido a la ausencia de mecanismos de seguridad de los protocolos FTP y Telnet[132]:

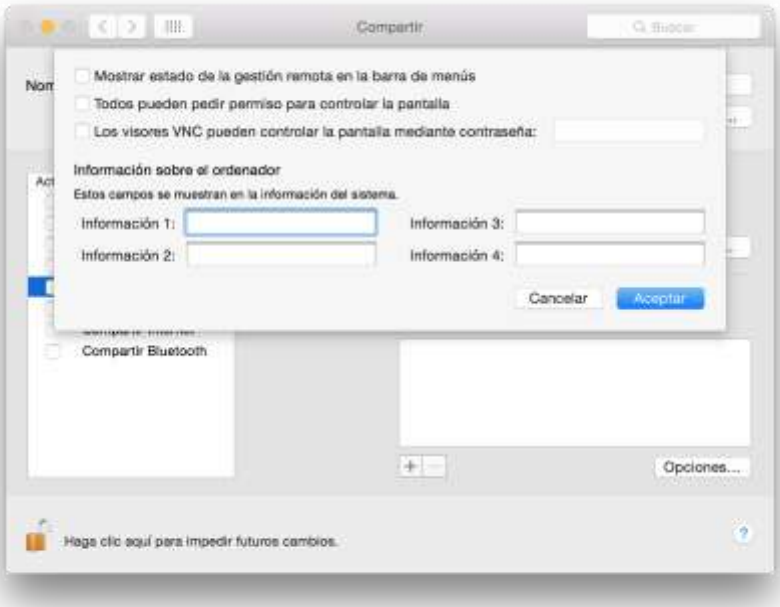
```
$ sudo launchctl load -w /System/Library/LaunchDaemons/ssh.plist
$ sudo launchctl unload -w /System/Library/LaunchDaemons/ssh.plist

$ sudo launchctl load -w /System/Library/LaunchDaemons/ftp.plist
$ sudo launchctl unload -w /System/Library/LaunchDaemons/ftp.plist

$ sudo launchctl load -w /System/Library/LaunchDaemons/telnet.plist
$ sudo launchctl unload -w /System/Library/LaunchDaemons/telnet.plist
```

5.13.6.5 GESTIÓN REMOTA

809. Gestión remota [Ref.- 66], o *Apple Remote Desktop*, se utiliza para gestionar de forma remota ordenadores Mac en entornos empresariales:

810. A través del botón "Ajustes del ordenador…", permite definir múltiples ajustes asociados a este servicio, todos ellos deshabilitados por defecto:

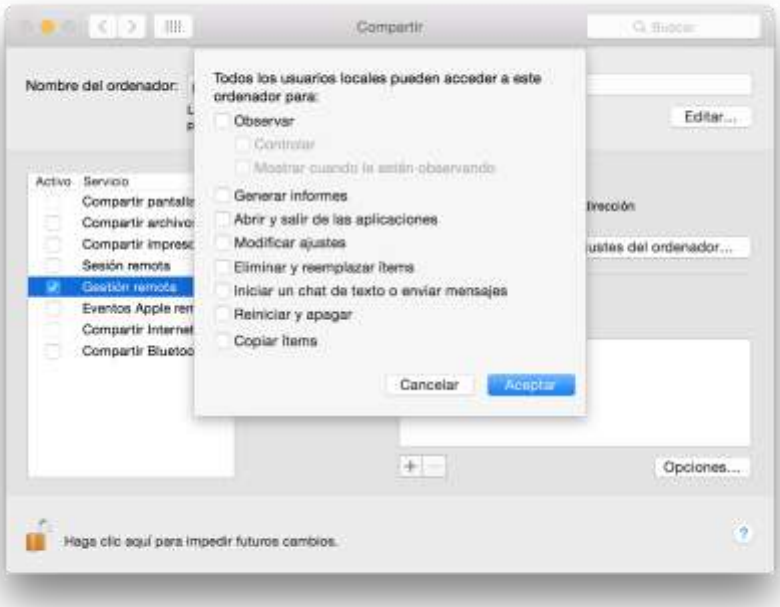
[132] En culauqier caso, sería necesaria la configuración de estos servicios y la definición de reglas en el cortafuegos.



811. En caso de hacer uso de este servicio, desde el punto de vista de seguridad, se recomienda habilitar la primera opción para mostrar el estado del servicio en la barra de menús, y seguir las mismas recomendaciones que para "Compartir pantalla" (ver apartado "5.13.6.1. COMPARTIR PANTALLA") para las siguientes dos opciones.

812. Asimismo, se debe restringir la información facilitada mediante los campos de información sobre el ordenador.

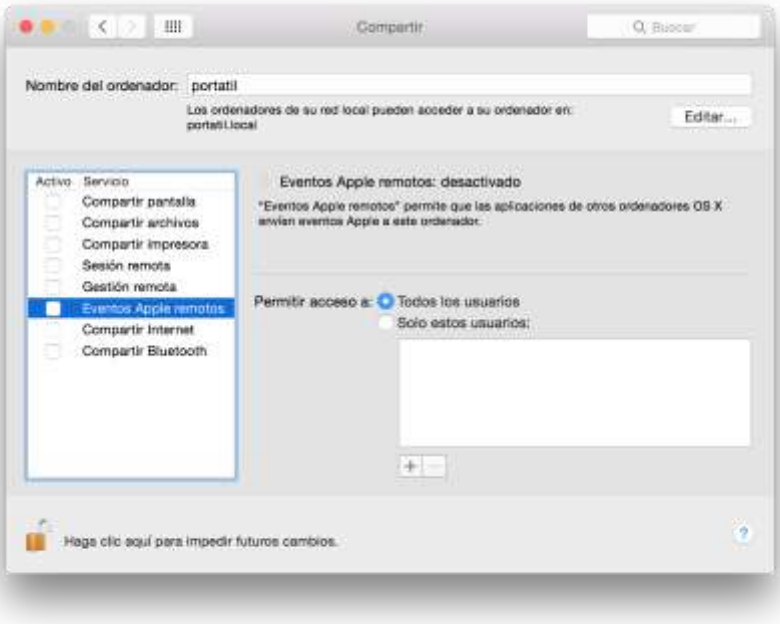
813. A la hora de activar el servicio se muestra un panel de configuración que permite definir que funcionalidad estará disponible para todos los usuarios locales a través del servicio:



814. Gestión remota hace uso de los mismos puertos TCP/IP empleados por Compartir pantalla (ver apartado "5.13.6.1. COMPARTIR PANTALLA"), de ahí que sean excluyentes.

5.13.6.6 EVENTOS APPLE REMOTOS

815. Las capacidades del servicio de Eventos Apple remotos [Ref.- 67] permite recibir eventos de las aplicaciones que son ejecutadas en otros equipos Mac, en concreto, de las acciones que van siendo llevadas a cabo:



816. Mediante los Eventos Apple remotos, un programa AppleScript que se ejecute en otro ordenador Mac puede interactuar con el equipo, con las implicaciones de seguridad asociadas.

817. Se recomienda comprobar que el servicio de los Eventos Apple remotos está deshabilitado y, en caso contrario, deshabilitarlo, desde el interfaz gráfico o desde un terminal:

```
$ sudo systemsetup -getremoteappleevents
Remote Apple Events: Off

$ sudo systemsetup -setremoteappleevents off
```

Nota: el análisis de la funcionalidad y de todas las capacidades de AppleScript, un lenguaje de programación o *scripting* para la realización de tareas automáticas en OS X, y de Automator[133] (una herramienta existente por defecto en OS X para la automatización de tareas), queda fuera del alcance de la presente guía. Se dispone de una visión detallada de AppleScript en la librería para desarrolladores de Mac [Ref.- 59].

[133] https://developer.apple.com/library/mac/documentation/AppleScript/Conceptual/AppleScriptX/Concepts/automator.html#//apple_ref/doc/uid/TP40006469-SW1

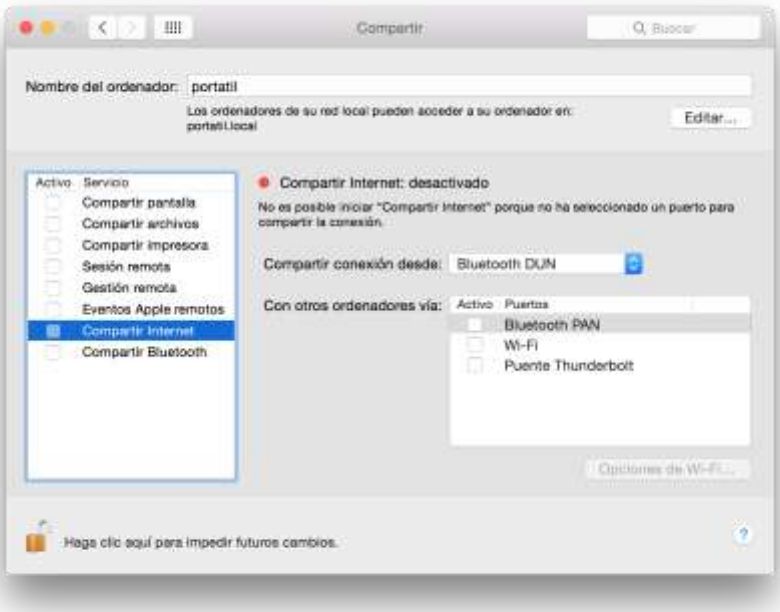
El potencial de AppleScript y de Automator podría ser empleado para automatizar la aplicación de las recomendaciones de seguridad proporcionadas en la presente guía.

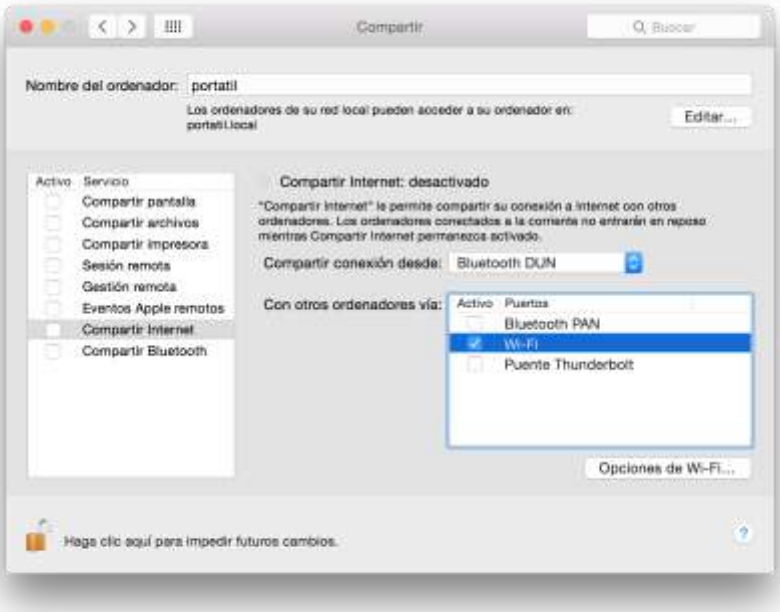
818. Eventos Apple remotos hace uso del puerto TCP/3031 (eppc, *Remote AppleEvents/PPC Toolbox*).

5.13.6.7 COMPARTIR INTERNET

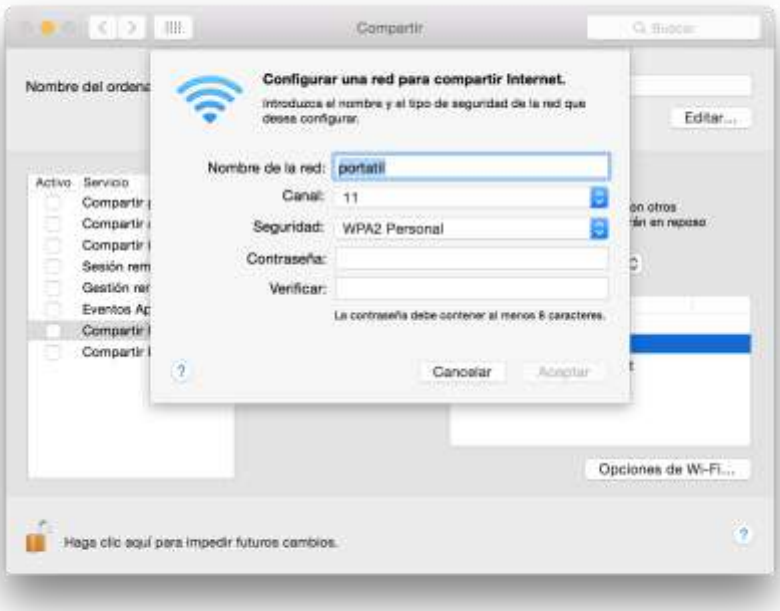
819. Las capacidades del servicio Compartir Internet [Ref.- 68] permiten compartir la conexión existente hacia Internet disponible en el interfaz de red especificado por la opción "Compartir conexión desde:" (Bluetooth DUN o PAN, Wi-Fi, Thunderbolt Ethernet, etc) con los ordenadores disponibles a través del interfaz de red especificado por la opción "Con ordenadores vía:", donde es necesario activar los interfaces (o puertos) con los que se desea compartir: Bluetooth, Wi-Fi, Thunderbolt Ethernet, etc.

820. Si se va a compartir la conexión a Internet (por ejemplo, Thunderbolt Ethernet) a través del interfaz Wi-Fi, se recomienda, antes de habilitar el servicio, seleccionar el puerto "Wi-Fi" con el objetivo de habilitar el botón "Opciones de Wi-Fi…":





821. A través del botón "Opciones de Wi-Fi…" es posible definir el nombre de la red Wi-Fi que será creada, el canal empleado, y el tipo de seguridad (por defecto, "Ninguna"):



822. Se recomienda hacer uso de un nombre de red que no desvele detalles del equipo y/o su propietario, y hacer uso de seguridad basada en "WPA2 Personal", con una contraseña suficientemente robusta.

5.13.6.8 COMPARTIR BLUETOOTH

823. Las capacidades del servicio Compartir Bluetooth [Ref.- 69] dispone de numerosas opciones de configuración que permiten, entre otros:

- Definir la acción que debe llevarse a cabo al recibir ítems (por defecto "Aceptar y guardar"). Se recomienda emplear "Preguntar qué hacer" en su lugar para solicitar autorización al usuario, o la opción "No permitir nunca" si se desea enviar elementos vía Bluetooth pero no recibirlos.
- Definir la carpeta donde se almacenarán los ítems aceptados (por defecto "-", que corresponde a la carpeta "Descargas"). Mediante la opción "Otra…" es posible establecer una carpeta destino diferente.
- Definir los permisos asociados a otros dispositivos que intenten explorar las capacidades Bluetooth del equipo (por defecto "Permitir siempre"). Se recomienda emplear "Preguntar qué hacer" en su lugar para solicitar autorización al usuario, o la opción "No permitir nunca" si se desea que otros dispositivos no puedan explorar el equipo.
- Definir las carpetas que otros dispositivos pueden explorar (por defecto "-", que corresponde a la carpeta "Pública"). Mediante la opción "Otra…" es posible establecer una carpeta origen diferente.

824. El botón "Abrir el panel de preferencias Bluetooth…" permite abrir los ajustes de configuración de Bluetooth.

5.13.7 AIRDROP

825. Una alternativa con carácter más temporal para la compartición de datos entre dispositivos Apple, en concreto con otros equipos Mac (con OS X Yosemite y empleando uno de los modelos soportados) o dispositivos móviles de Apple soportados[134] (con iOS 7 o posterior), a través de conexiones Wi-Fi y Bluetooth, es AirDrop [Ref.- 58].

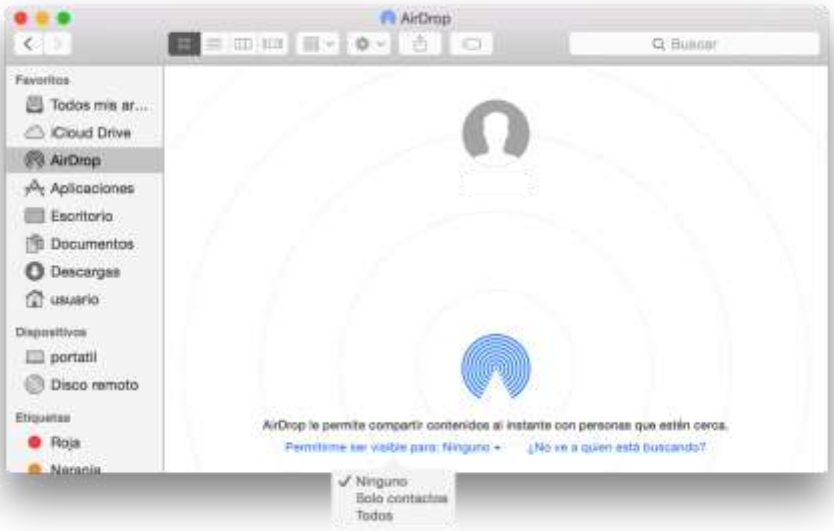
826. Para hacer uso de AirDrop no es necesario que los ordenadores (o dispositivos) estén conectados a la misma red Wi-Fi, ya que crean una red Wi-Fi directa entre ellos para comunicarse. Sin embargo, sí es necesario que el interfaz Wi-Fi esté activo. Adicionalmente, AirDrop también requiere disponer del interfaz Bluetooth del equipo activo:

[134] https://support.apple.com/es-es/ht5887

827. Incluso aunque el ordenador Mac esté actualmente conectado a una red Wi-Fi, sigue siendo posible hacer uso de AirDrop.

828. AirDrop puede ser activado desde el Finder y el menú "Ir - AirDrop", desde donde el ordenador Mac comenzará la búsqueda de otros equipos compatibles con AirDrop:

829. Por defecto, el ordenador no es visible para ningún equipo, definido mediante la opción inferior "Permitirme ser visible para:". Además de la opción recomendada desde el punto de visa de seguridad, "Ninguno", puede establecerse ser visible sólo para los contactos ("Solo contactos"), o para todo el mundo ("Todos"):



830. Es posible compartir archivos simplemente arrastrándolos sobre el icono correspondiente a los otros equipos, siendo necesario que el usuario del equipo destino acepte la recepción del archivo, que será almacenando automáticamente en la carpeta "Descargas" ("cd ./Downloads"):

831. Los atributos de cuarentena de archivos asociados al fichero en el ordenador origen son propagados a través de la transferencia mediante AirDrop hacia el ordenador destino. Adicionalmente se añaden nuevos atributos para reflejar el nombre del equipo desde el que se ha recibido el fichero ("com.apple.metadata:kMDItemWhereFrom") y la asignación de una etiqueta ("com.apple.metadata:kMDLabel_<etiqueta>").

5.13.8 VOLVER A MI MAC

832. OS X proporciona el servicio Volver a mi Mac [Ref.- 57], que permite conectarse de forma remota a equipos Mac a través de Internet empleando una cuenta de usuario de iCloud.

833. Para poder hacer uso de Volver a mi Mac es necesario activar el servicio Compartir pantalla (ver apartado "5.13.6.1. COMPARTIR PANTALLA") e iniciar sesión en iCloud desde "Preferencias del Sistema - iCloud".

834. En los servicios de iCloud disponibles a la derecha, se debe activar "Volver a mi Mac" (deshabilitado por defecto):

835. Se recomienda, en caso de hacer uso de este servicio, deshabilitar el mismo desde los ajustes de configuración de iCloud tan pronto haya finalizado la sesión asociada.

836. Volver a mi Mac requiere hacer uso de un *router* compatible con el protocolo de asignación de puertos NAT (NAT-PMP) o Plug and Play universal (UPnP) para poder compartir este servicio.

837. El acceso al servicio Volver a mi Mac se puede realizar desde otro ordenador con OS X a través del Finder y de la categoría Compartido (subcategoría Volver a mi Mac), seleccionando el ordenador con el que compartir la pantalla (qué tiene el servicio activo)[135].

5.13.9 SERVICIOS Y APLICACIONES TCP/IP DISPONIBLES POR DEFECTO

838. Por defecto, OS X dispone de un número reducido de servicios y aplicaciones escuchando activamente en puertos TCP o UDP a la espera de recibir conexiones entrantes[136]:

- TCP:

  - Internet Printing Protocol (ipp):

    631/tcp: launchd (loopback: IPv4 & IPv6)

[135] https://support.apple.com/kb/PH18688

[136] La información mostrada refleja el nombre genérico del servicio y su identificación en "/etc/services", el número de puerto TCP o UDP asociado, el proceso vinculado a ese puerto, y los interfaces (loopback o any, cualquiera) y versiones del protocolo IP en los que escucha.

- UDP:
  - Multicast DNS (mdns):

    5353/udp: discovery(d) (any: IPv4 & IPv6)
  - NetBIOS Name Service (netbios-ns):

    137/udp: launchd (any: IPv4)
  - NetBIOS Datagram Service (netbios-dgm):

    138/udp: launchd (any: IPv4)

839. Esta información puede ser obtenida mediante los siguientes comandos:

```
$ netstat -an -p tcp
$ netstat -an -p udp

$ sudo lsof -i | grep LISTEN
$ sudo lsof -i | grep UDP

$ cat /etc/services | grep <PUERTO>
```

840. Sin embargo, este escenario puede cambiar drásticamente una vez se instala nuevo software, servicios y aplicaciones en OS X, por lo que se recomienda evaluar periódicamente el estado del equipo empleando los comandos indicados previamente.

5.13.10 CORTAFUEGOS

5.13.10.1 APPLICATION LAYER FIREWALL (ALF)

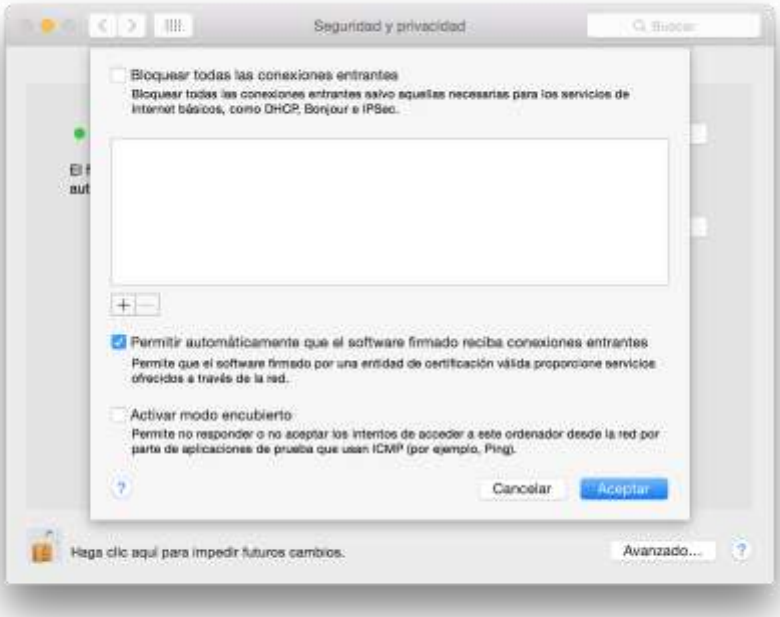
841. OS X dispone de un cortafuegos personal (o *firewall*), también denominado *Application Layer Firewall* (ALF) o *Application Firewall*, en adelante cortafuegos, que permite bloquear las conexiones y el tráfico entrante hacia el equipo [Ref.- 47].

842. Por defecto, el cortafuegos de OS X está desactivado, por lo que se recomienda su activación (mediante un usuario administrador) como parte de las tareas iniciales de configuración de OS X, a través de "Preferencias del Sistema - Seguridad y privacidad", desde la pestaña "Firewall", mediante el botón "Activar firewall":

843. En ocasiones, esta configuración inactiva por defecto del cortafuegos es justificada por el reducido número de servicios y aplicaciones escuchando en puertos TCP o UDP en OS X en su configuración inicial o por defecto (ver apartado "5.13.9. Servicios y aplicaciones TCP/IP disponibles por defecto"). Sin embargo, con el objetivo de proteger el equipo es fundamental activar de manera restrictiva las capacidades de filtrado existentes.

844. Es posible configurar los ajustes del cortafuegos mediante la opción "Opciones de firewall…" desde "Preferencias del Sistema - Seguridad y privacidad" y la pestaña "Firewall", una vez activado:

845. La configuración del cortafuegos permite bloquear todas las conexiones entrantes hacia el equipo (excepto las conexiones necesarias para el funcionamiento de servicios básicos como DHCP, Bonjour (mDNS) o IPSec), mediante la opción "Bloquear todas las conexiones entrantes", o seleccionar cuáles de las aplicaciones instaladas permitirán conexiones entrantes, a través de la opción "Permitir automáticamente que el software firmado reciba conexiones entrantes":



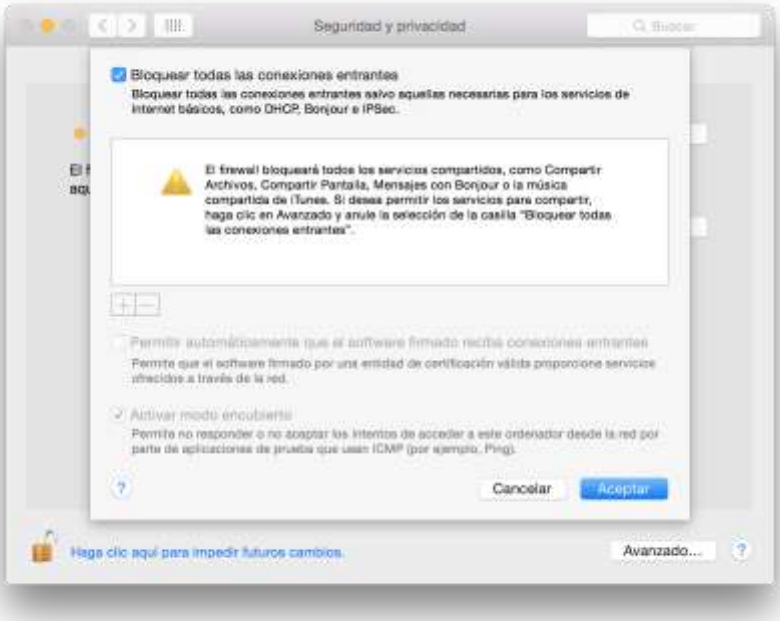
846. Por defecto, la configuración del cortafuegos una vez activado permite que el software firmado (por una autoridad certificadora de confianza) reciba conexiones entrantes, es decir, bloqueará únicamente conexiones entrantes hacia aplicaciones, programas y servicios no autorizados. Es decir, por defecto todo el software de Apple, y las aplicaciones obtenidas de la Mac App Store o de desarrolladores identificados, permitidas por Gatekeeper, podrán recibir conexiones entrantes si está opción está habilitada, como por ejemplo, la aplicación iTunes firmada por Apple.

847. Si se desea disponer de un control exhaustivo sobre las capacidades de comunicaciones de todas las aplicaciones, se recomienda deshabilitar esta opción.

848. Asimismo, se recomienda activar la opción "Activar modo encubierto", para evitar que el equipo responda a intentos de descubrimiento o acceso remotos mediante protocolos como ICMP, y en concreto, tráfico de ping (otros tipos de tráfico ICMP, como *timestamp* or *address subnet mask* están deshabilitados en todos los casos):

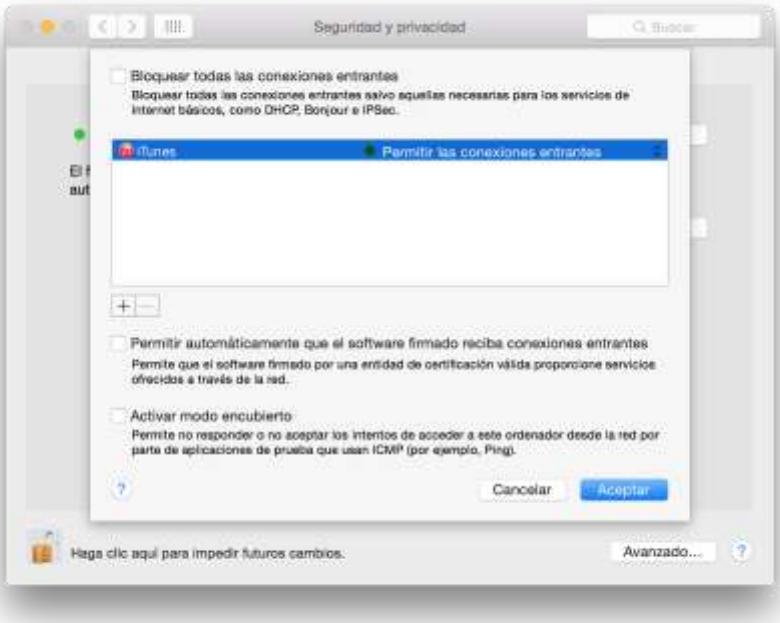
849. Aunque esta opción esté habilitada, el equipo todavía aceptará conexiones hacia las aplicaciones autorizadas (según la configuración de las opciones previas).

850. Preferiblemente, se recomienda activar la opción "Bloquear todas las conexiones entrantes", con el objetivo de no desvelar la presencia del equipo en la red. Al activar esta opción, el cortafuegos bloqueará todos los servicios compartidos (ver apartado "5.13.6. Servicios compartidos"):



851. Una vez activada dicha opción más restrictiva del cortafuegos, todavía está disponible desde el exterior el puerto UDP/5353 (Bonjour, zeroconf o mDNS). Este estado por defecto puede variar, ya que es dependiente de los servicios y aplicaciones que estén ejecutando en OS X en un momento dado, y potenciamente pueden estar disponibles también otros servicios básicos.

852. En el caso de requerir que algunas aplicaciones reciban conexiones entrantes, se recomienda no habilitar esa opción y, a través del botón "+", gestionar la lista concreta de aplicaciones que dispondrán de autorización para recibir conexiones. Para ello se debe seleccionar la aplicación o binario concreto, y establecer la política de filtrado: "Permitir las conexiones entrantes" (activa por defecto) o "Bloquear las conexiones entrantes":



853. Por defecto, cuando se activa alguno de los servicios compartidos (ver apartado "5.13.6. Servicios compartidos"), OS X automáticamente añade una nueva regla en la lista del cortafuegos para dicho servicio permitiendo las conexiones entrantes:

854. Una vez se deshabilita el servicio compartido, la regla es automáticamente eliminada del cortafuegos.

855. En cualquier momento es posible gestionar las aplicaciones y políticas de filtrado que serán aplicadas por el cortafuegos desde esta ventana de configuración:

856. Si OS X detecta un intentos de conexión hacia el puerto asociado a una aplicación que no está en la lista de aplicaciones del cortafuegos, mostrará un cuadro de diálogo solicitando autorización al usuario para incluir una nueva regla para dicha aplicación, autorizando o denegando las conexiones entrantes hacia la misma.

857. Por ejemplo, este es el caso de la aplicación "netbiosd", que solicita permiso tan pronto el equipo con OS X dispone de conectividad tras configurar por primera vez su interfaz de red, creando una regla para el tráfico UDP/137 (netbios-ns):

858. Mientras el usuario no responda a dicho cuadro de diálogo, los intentos de conexión hacia la aplicación permanecerán bloqueados[137].

[137] https://support.apple.com/kb/PH18645

859. El proceso asociado al cortafuegos personal de OS X (ALF), descrito previamente, es "/usr/libexec/ApplicationFirewall/socketfilterfw" (con PID "/var/run/appfwd.pid").

860. El fichero de configuración del cortafuegos en OS X es el siguiente, y contiene la configuración del cortafuegos, incluyendo la lista de aplicaciones definidas y cuyo tráfico es gestionado por el cortafuegos, junto al comportamiento a aplicar para los servicios compartidos:

```
$ plutil -convert xml1 -o - /Library/Preferences/com.apple.alf.plist
```

861. Las herramientas de gestión del cortafuegos desde un terminal están disponibles bajo "/usr/libexec/ApplicationFirewall/" [Ref.- 49].

862. El fichero "/usr/libexec/ApplicationFirewall/Firewall" es el propio binario del cortafuegos (ALF, o *useragent*), mientras que "socketfilterfw" es la herramienta que permite configurar el cortafuegos (o *agent*, en terminología de Apple).

863. Si el fichero de configuración del cortafuegos se corrompe, puede volverse al estado inicial restaurando el fichero "/usr/libexec/ApplicationFirewall/com.apple.alf.plist" en su lugar.

864. Este fichero permite identificar el conjunto de servicios básicos que son permitidos por defecto incluso aunque se bloqueen todas las conexiones entrantes hacia el equipo, es decir, las excepciones definidas por Apple. Estas excepciones incluyen los procesos configd (System Configuration Daemon), mDNSResponder (Bonjour o mDNS, Multicast & Unicast DNS Daemon), racoon (IPSec IKE/ISAKMP key management daemon), nmblookup (NetBIOS), readconfig (Admin Framework), y discoveryd (System daemon for DNS, Bonjour and other Discovery).

865. Adicionalmente, el cortafuegos incluye otras excepciones explicitas, asociadas a los intérpretes de algunos lenguajes de programación como Python, Ruby, Java, PHP, etc.

866. Los siguientes comandos permiten gestionar la configuración del cortafuegos desde un terminal, como por ejemplo comprobar su estado, verificar si se están bloqueando todas las conexiones entrantes, o verificar si se permiten conexiones hacia aplicaciones firmadas o si el modo encubierto está habilitado, respectivamente [Ref.- 49]:

```
$ /usr/libexec/ApplicationFirewall/socketfilterfw --getglobalstate
Firewall is enabled. (State = 1)

$ /usr/libexec/ApplicationFirewall/socketfilterfw --getblockall
Firewall is set to block all non-essential incoming connections
(vs. Block all DISABLED!)

$ /usr/libexec/ApplicationFirewall/socketfilterfw --getallowsigned
Automatically allow signed software ENABLED

$ /usr/libexec/ApplicationFirewall/socketfilterfw --getstealthmode
Stealth mode enabled
```

867. Adicionalmente, es posible modificar la configuración del cortafuegos, cambiando el estado de cualquiera de las comprobaciones previas (*on* u *off*), así como modificar la configuración

de los logs, añadir nuevas aplicaciones a la política de filtrado o comprobar su estado, individual o colectivo:

```
$ /usr/libexec/ApplicationFirewall/socketfilterfw --listapps
ALF: total number of apps = 5

1 :
/System/Library/Frameworks/JavaVM.framework/Versions/A/Commands/java
    ( Allow incoming connections )

2 :  /Applications/iTunes.app
    ( Allow incoming connections )
...
```

868. También es posible activar o desactivar el cortafuegos mediante la directiva "setglobalstate" (*on* u *off*) o mediante launchd (hasta el siguiente rearranque del equipo):

```
$ launchctl unload -w
/System/Library/LaunchAgents/com.apple.alf.useragent.plist

$ sudo launchctl unload -w
/System/Library/LaunchDaemons/com.apple.alf.agent.plist
```

869. El fichero de log por defecto del cortafuegos (ALF) está disponible en "/var/log/alf.log".

870. El cortafuegos existente por defecto en OS X sólo filtra el trafico entrante, es decir, el establecimiento de conexiones dirigidas hacia el equipo. Se recomienda adicionalmente disponer de capacidades para filtrar el establecimiento de conexiones salientes, u originadas, desde el equipo.

871. Se dispone de aplicaciones comerciales de terceros para OS X, como por ejemplo Little Snitch[138], que proporcionan un cortafuegos con capacidades avanzadas, por ejemplo, para bloquear las conexiones y el tráfico saliente, así como monitorizar y generar alertas en tiempo real sobre el tráfico de red.

5.13.10.2 PACKET FILTER (PF)

872. Adicionalmente al cortafuegos personal de OS X, descrito previamente y denominado *Application Layer Firewall* (ALF), OS X dispone de un cortafuegos a más bajo nivel, en adelante pf.

873. Desde la versión OS X Lion el sistema operativo integra el cortafuegos o firewall pf (*Packet Filter*) del proyecto OpenBSD[139], referenciado por Apple como cortafuegos adaptable (o *adaptative firewall*, af), y diseñado fundamentalmente para OS X Server[140].

[138] https://www.obdev.at/products/littlesnitch/index.html

[139] http://www.openbsd.org/faq/pf/

[140] https://support.apple.com/es-es/HT200259

874. pf dispone tanto de capacidades de filtrado de tráfico, tanto entrante (in) como saliente (out), como de traducción de direcciones o NAT (*Network Address Translation*)[141].

875. La opción "-e" (*enable*) de pf, recomendada para su utilización en OS X Server, activa el filtrado de paquetes de pf. La opción "-f" de pf configura las reglas definidas en el fichero de configuración indicado, pero no activa sus capacidades de filtrado.

876. Es posible consultar el estado actual de pf mediante el siguiente comando:

```
$ sudo pfctl -s state
```

877. La utilidad "pfctl" (*pf controller*) permite llevar a cabo la configuración detallada de pf, así como la gestión de reglas de filtrado y de NAT.

878. El fichero de configuración por defecto de pf, "/etc/pf.conf", está prácticamente vacío en OS X, con referencias a "/etc/pf.anchors/com.apple"[142], que a su vez incluye políticas para AirDrop y para el ApplicationFirewall (o cortafuegos personal descrito previamente).

879. En pf, los *anchors* son conjuntos de reglas de filtrado identificadas por nombre. Es posible disponer de más *anchors* definidos en función, por ejemplo, de los servicios compartidos activados en OS X [Ref.- 48] (ver apartado "5.13.6. Servicios compartidos").

880. Los ficheros de configuración de arranque de pf en OS X son los siguientes, que se encargan de ejecutar "/sbin/pfctl -f /etc/pf.conf" (activado por defecto en el arranque para configurar las reglas de pf) y "/usr/libexec/pfd -d" (desactivado por defecto), respectivamente:

```
$ less /System/Library/LaunchDaemons/com.apple.pfctl.plist

$ plutil -convert xml1 -o -
/System/Library/LaunchDaemons/com.apple.pfd.plist
```

881. Mediante los siguientes comandos es posible consultar información de estadísticas y uso de pf, así como las reglas de filtrado disponibles, respectivamente:

```
$ sudo pfctl -sa

$ sudo pfctl -sr
```

882. Complementariamente, es posible verificar las capacidades de reenvío de tráfico (IP *forwarding*) del kernel de OS X a través del siguiente comando:

```
$ sysctl net.inet.ip.forwarding
net.inet.ip.forwarding: 0
```

[141] Capacidades que pueden ser empleadas, por ejemplo, para la redirección transparente de tráfico de red mediante pf: https://mitmproxy.org/doc/transparent/osx.html.

[142] Adicionalmente, pf dispone de identificación pasiva de sistemas operativo en base a las firmas existentes en "/etc/pf.os".

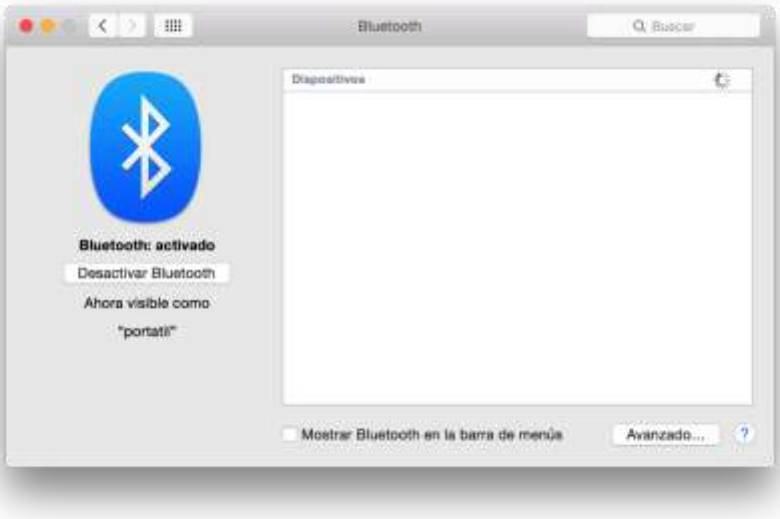
883. Por defecto, OS X no tiene activadas estas capacidades de reenvío de tráfico, y desde el punto de vista de seguridad no se recomienda habilitarlas, salvo que se deseé que el equipo haga de *router* o *gateway*. En caso de estar activas y no hacer uso de ellas, se recomienda deshabilitarlas:

```
$ sysctl net.inet.ip.forwarding=0
net.inet.ip.forwarding: 1 -> 0
```

5.13.11 BLUETOOTH

884. La principal recomendación de seguridad asociada a las comunicaciones Bluetooth (IEEE 802.15) en ordenadores Mac es no activar el interfaz inalámbrico Bluetooth salvo en el caso en el que se esté haciendo uso del mismo, evitando así la posibilidad de ataques sobre el hardware del interfaz, el driver o la pila de comunicaciones Bluetooth, incluyendo los perfiles Bluetooth disponibles.

885. Por defecto OS X activa el interfaz Bluetooth tras el proceso de instalación inicial, por lo que se recomienda deshabilitarlo lo antes posibles desde "Preferencias del Sistema - Bluetooth", mediante el botón "Desactivar Bluetooth":



886. Asimismo, por defecto, OS X no muestra ninguna indicación de que el interfaz Bluetooth está activo, por lo que se recomienda mostrar el interfaz Bluetooth en la barra de menús mediante "Preferencias del Sistema - Bluetooth" y la opción inferior "Mostrar Bluetooth en la barra de menús":

887. El ordenador Mac sólo será visible mientras el usuario permanece en la pantalla de Bluetooth, por lo que se recomienda hacer uso de la misma el menor tiempo posible si no se desea que otros dispositivos puedan detectar la presencia del equipo mediante Bluetooth.

888. Es posible comprobar si el equipo se encuentra en el estado visible en un momento dado a través del siguiente comando:

```
$ /usr/sbin/system_profiler SPBluetoothDataType | grep -i discoverable
```

889. Para no entrar en el estado visible, es posible habilitar el interfaz Bluetooth desde el icono asociado de la barra de menús, mediante la opción "Activar Bluetooth".

890. Es posible verificar el estado del interfaz Bluetooth ("0" = off y "1" = on), y activar (o desactivar) el interfaz Bluetooth desde un terminal, evitando así también entrar en el estado visible, mediante los siguientes comandos:

```
$ defaults read /Library/Preferences/com.apple.Bluetooth.plist
ControllerPowerState
0

$ sudo defaults write /Library/Preferences/com.apple.Bluetooth.plist
ControllerPowerState 1

$ sudo defaults write /Library/Preferences/com.apple.Bluetooth.plist
ControllerPowerState 0
```

891. El proceso asociado a la pila de comunicaciones Bluetooth en OS X es "/usr/sbin/blued".

892. Tras cambiar el estado de la propiedad "ControllerPowerState" es necesario recargar el demonio o servicio "blued", mediante los dos siguientes comandos, para que los cambios tengan efecto:

```
$ sudo launchctl unload -w
/System/Library/LaunchDaemons/com.apple.blued.plist

$ sudo launchctl load -w
/System/Library/LaunchDaemons/com.apple.blued.plist
```

893. Adicionalmente se dispone de herramientas de terceros que permiten gestionar el interfaz Bluetooth en OS X, como blueutil[143].

894. Mediante el botón "Avanzado…" del panel de configuración de Bluetooth es posible especificar si se desea abrir el Asistente de Configuración Bluetooth al arrancar si no se detecta ningún teclado (para poder conectar un teclado Bluetooth al ordenador), si no se detecta ningún ratón o *trackpad* (para poder conectar un ratón o *trackpad* Bluetooth al ordenador) y si se desea poder activar el ordenador mediante dispositivos Bluetooth cuando este se encuentra en modo reposo. Las tres opciones están habilitadas por defecto:

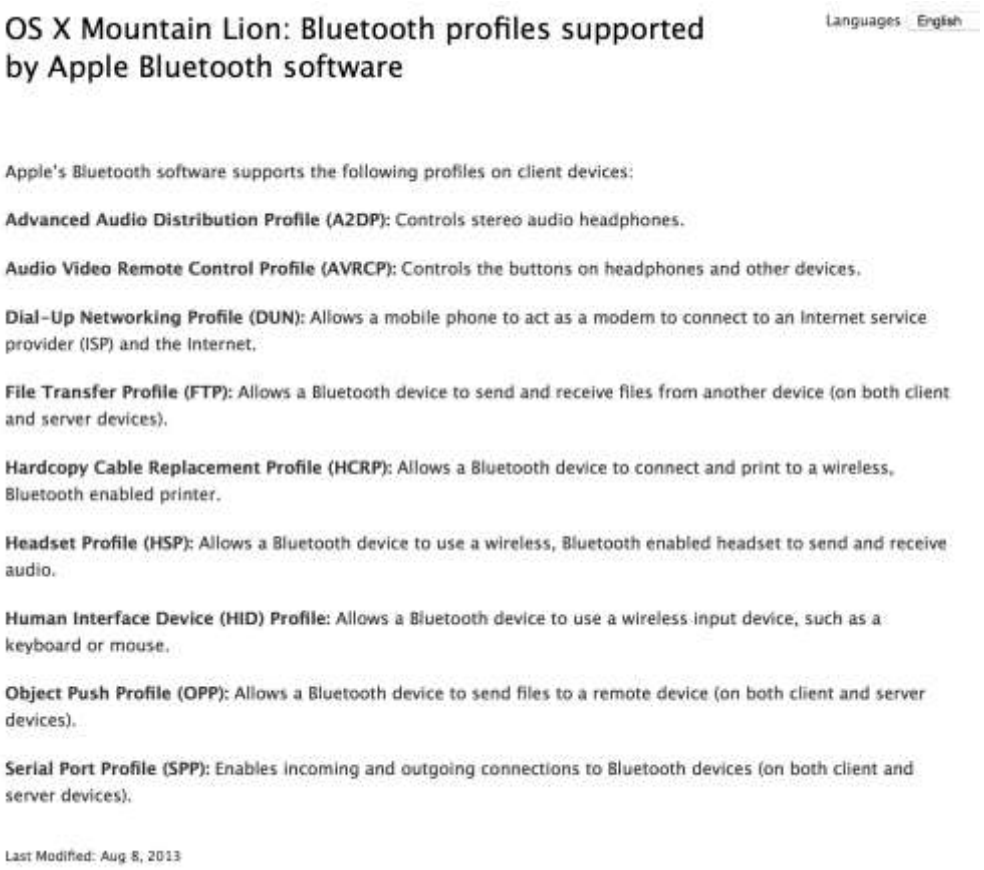
895. Se recomienda, desde el punto de vista de seguridad, deshabilitar todas las opciones, y hacer uso únicamente de ellas si se considera necesario desde el punto de vista de su funcionalidad (debiendo disponer de un teclado o ratón/*trackpad* conectados directamente al ordenador si se deshabilitan las dos primeras opciones y no se dispone del dispositivo Bluetooth equivalente), y dependiendo del modelo de ordenador Mac empleado (por ejemplo, es menos frecuente hacer uso de un teclado o ratón/*trackpad* Bluetooth con ordenadores portátiles de Apple, como el MacBook Pro empleado para la elaboración de la presente guía, que con un ordenador de escritorio).

896. Los perfiles Bluetooth soportados por OS X (desde la versión Mountain Lion) están referenciados desde la página web de documentación de Bluetooth para desarrolladores de Apple[144] (no así desde la página web de soporte de Bluetooth de Apple[145]), no

[143] http://www.frederikseiffert.de/blueutil/

[144] https://developer.apple.com/bluetooth/

disponiéndose en el interfaz de usuario de ninguna opción para su configuración detallada [Ref.- 80]:



OS X Mountain Lion: Bluetooth profiles supported by Apple Bluetooth software

Languages English

Apple's Bluetooth software supports the following profiles on client devices:

Advanced Audio Distribution Profile (A2DP): Controls stereo audio headphones.

Audio Video Remote Control Profile (AVRCP): Controls the buttons on headphones and other devices.

Dial-Up Networking Profile (DUN): Allows a mobile phone to act as a modem to connect to an Internet service provider (ISP) and the Internet.

File Transfer Profile (FTP): Allows a Bluetooth device to send and receive files from another device (on both client and server devices).

Hardcopy Cable Replacement Profile (HCRP): Allows a Bluetooth device to connect and print to a wireless, Bluetooth enabled printer.

Headset Profile (HSP): Allows a Bluetooth device to use a wireless, Bluetooth enabled headset to send and receive audio.

Human Interface Device (HID) Profile: Allows a Bluetooth device to use a wireless input device, such as a keyboard or mouse.

Object Push Profile (OPP): Allows a Bluetooth device to send files to a remote device (on both client and server devices).

Serial Port Profile (SPP): Enables incoming and outgoing connections to Bluetooth devices (on both client and server devices).

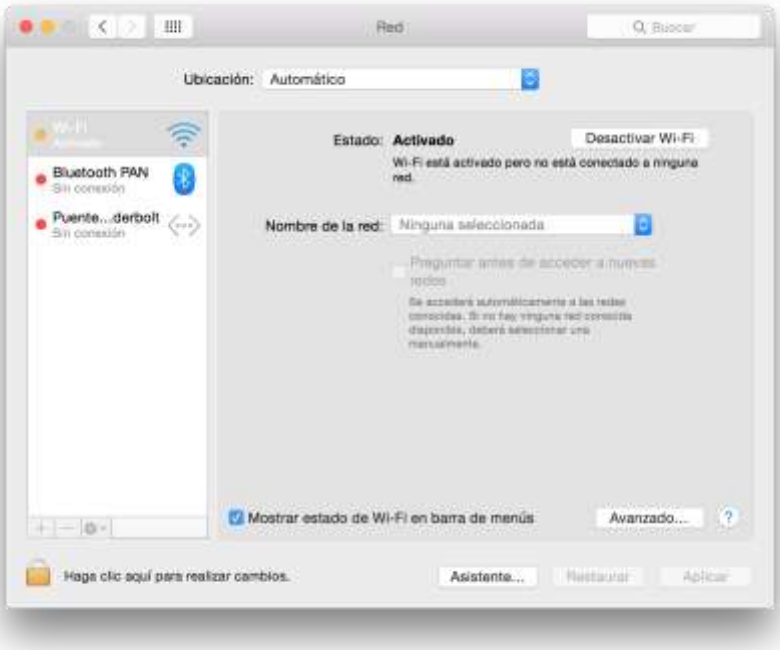
Last Modified: Aug 8, 2013

5.13.12 WI-FI

897. La principal recomendación de seguridad asociada a las comunicaciones Wi-Fi (IEEE 802.11) en ordenadores Mac es no activar el interfaz inalámbrico Wi-Fi salvo en el caso en el que se esté haciendo uso del mismo, evitando así la posibilidad de ataques sobre el hardware del interfaz, el driver o la pila de comunicaciones Wi-Fi.

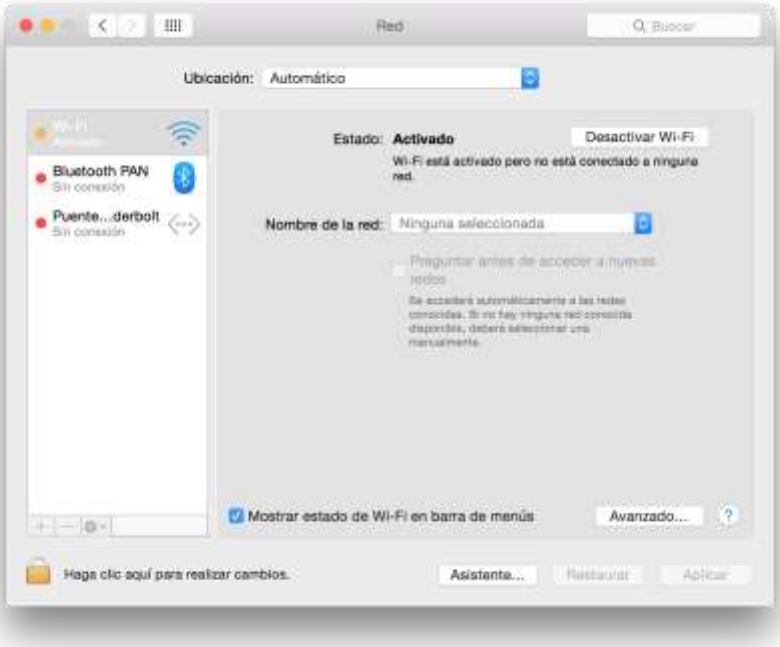
898. Por defecto OS X activa el interfaz Wi-Fi tras el proceso de instalación inicial, por lo que se recomienda deshabilitarlo lo antes posible desde "Preferencias del Sistema - Red", seleccionando el interfaz Wi-Fi del panel de la izquierda, mediante el botón "Desactivar Wi-Fi":

[145] https://www.apple.com/support/bluetooth/



899. Por defecto, OS X muestra en la barra de menús una indicación del estado del interfaz Wi-Fi (no activo, activo, o conectado a una red Wi-Fi), opción recomendada desde el punto de vista de seguridad.

900. Aunque no se recomienda deshabilitarla, la opción que permite gestionar el icono del estado del interfaz Wi-Fi en la barra de menús está disponible a través de "Preferencias del Sistema - Red", tras seleccionar el interfaz de red Wi-Fi, mediante la opción inferior "Mostrar estado de Wi-Fi en barra de menús":



901. La pantalla de configuración de los ajustes de red generales, desde "Preferencias del Sistema - Red", tras seleccionar el interfaz de red Wi-Fi, muestra la opción "Preguntar antes de acceder a nuevas redes" (deshabilitado por defecto), que en caso de ser activado, cuando OS X no detecte ninguna red conocida, preguntará al usuario a qué red abierta de las disponibles desea conectarse. Se recomienda dejar esta opción deshabilitada, de forma que el usuario deba seleccionar manualmente la red a la que se desea conectar si no hay ninguna red conocida próxima.

902. Desde "Preferencias del Sistema - Red", tras seleccionar el interfaz de red Wi-Fi y mediante el botón "Avanzado…", mediante la pestaña "Wi-Fi", es posible configurar diferentes aspectos de esta tecnología:

903. Por defecto, OS X almacenará en su lista de redes preferidas (PNL, *Preferred Network List*) o redes conocidas, aquellas redes Wi-Fi a las que se ha conectado en el pasado. Las mismas aparecerán en la pantalla de lista de redes preferidas.

904. Esta es la opción más cómoda para el usuario, pero si se quiere restringir desde el punto de vista de seguridad el almacenamiento de las redes Wi-Fi, se recomienda deshabilitar la opción "Recordar las redes a las que este ordenador se ha conectado".

905. Es posible añadir un perfil de una red Wi-Fi mediante el botón "+", proporcionando el nombre de la red (o SSID), el tipo de seguridad y la contraseña o credenciales de acceso. Se recomienda hacer uso únicamente de redes Wi-Fi "WPA2 Personal" o "WPA2 Empresa":

906. En ningún caso se debe hacer uso de la opción "Cualquiera (personal o empresa)", ya que en ese caso OS X considerará válida cualquier red Wi-Fi cuyo nombre de red coincide con el de una de las redes conocidas, independientemente del tipo de seguridad empleado, lo que facilita la realización de ataques de suplantación de la red Wi-Fi legítima:

907. Si se desea añadir la red Wi-Fi de la lista de redes Wi-Fi disponibles en el momento de llevar a cabo la configuración, se puede hacer uso del botón "Mostrar redes" (siendo necesario activar el interfaz Wi-Fi previamente):

908. Se recomienda en su lugar añadir la red Wi-Fi manualmente sin habilitar el interfaz Wi-Fi hasta que no se haya completado la configuración del mismo[146].

909. OS X, una vez dispone de redes Wi-Fi configuradas en su lista de redes preferidas (PNL, *Preferred Network List*), siempre se conectará a las mismas automáticamente (en base al orden de prioridad de estas) una vez detecte su presencia:

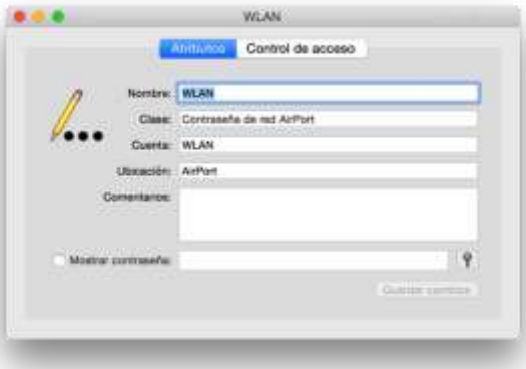
[146] Salvo que la versión de OS X empleada presente vulnerabilidades similares a las existentes en iOS durante el proceso que permite añadir manualmente una red Wi-Fi, dónde dicha red se considera automáticamente como una red oculta, desvelándose su nombre en el proceso de búsqueda de redes Wi-Fi conocidas.

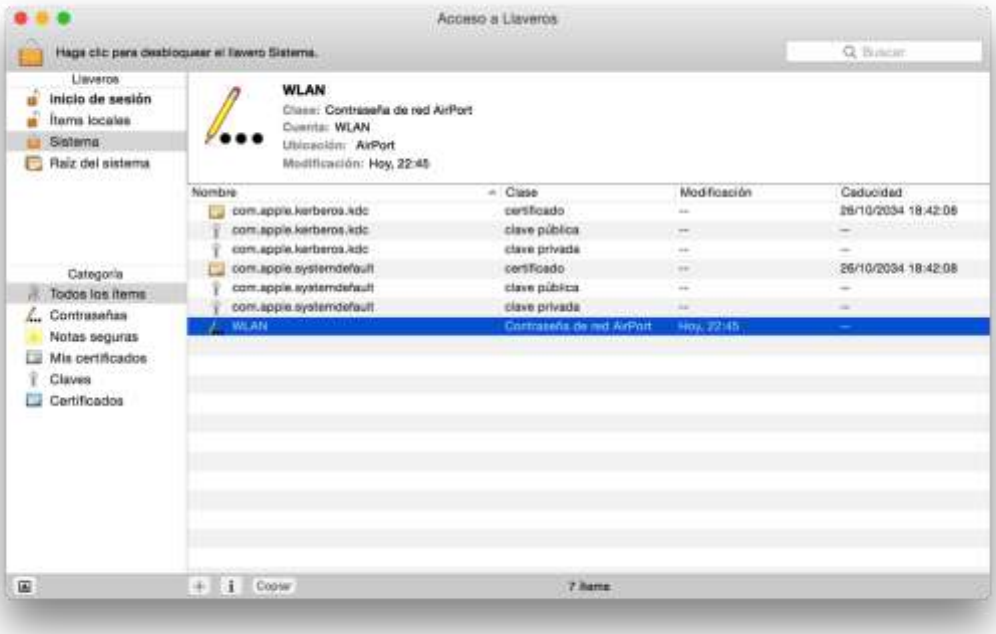
910. En el caso de disponerse de varias redes conocidas simultáneamente, OS X se conectará a la primera de ellas en la lista, ya que están ordenadas por prioridad.

911. OS X no proporciona ningún ajuste de configuración que permita deshabilitar la conexión automática a redes Wi-Fi conocidas, salvo la eliminación de las mismas de la PNL, alternativa que no es muy práctica, ya que la próxima vez que se desee establecer una conexión con una de estas redes Wi-Fi será necesario configurarla de nuevo y proporcionar todos los detalles de conexión:

912. Sin embargo, mediante la siguiente configuración a medida es posible evitar la conexión automática de OS X a redes Wi-Fi conocidas. Para ello, se debe desactivar la opción "Recordar las redes a las que este ordenador se ha conectado" (una vez ya se dispone de la(s) red(es) Wi-Fi a utilizar en la lista de redes preferidas).

913. Desde "Acceso a Llaveros", se debe acceder al llavero de "Sistema", seleccionar la red Wi-Fi (mediante una doble pulsación o seleccionando "Obtener información" con el botón derecho) y desde la pestaña "Control de Acceso", habilitar la opción "Solicitar contraseña del llavero" y guardar los cambios:





914. Adicionalmente se deben eliminar todas las entradas de la sección "Permitir siempre el acceso en estas aplicaciones", que por defecto incluye "airportd" y "AirPort". La única opción que estará finalmente habilitada será "Confirmar antes de permitir el acceso". Este proceso se debe repetir para cada una de las redes Wi-Fi conocidas:

915. Como resultado, OS X no se conectará automáticamente a las redes Wi-Fi conocidas, debiendo el usuario seleccionar la red Wi-Fi manualmente desde la lista de redes visibles (asociada al icono Wi-Fi de la barra de menús), para establecer la conexión.

916. Es posible desconectarse de la red Wi-Fi actual pulsando la tecla Alt a la vez que se selecciona el icono del interfaz Wi-Fi en la barra de menús, mediante la opción "Desconectar de <nombre de red Wi-Fi>" (si se desea que el interfaz Wi-Fi permanezca activo pero sin estar conectado a ninguna red Wi-Fi, por ejemplo, para hacer uso de manera independiente de AirDrop).

917. Adicionalmente, puede restringirse el uso y la configuración del interfaz Wi-Fi habilitando las opciones disponibles bajo la sección "Solicitar la autorización del administrador para:", que solicitarán las credenciales de un usuario administrador si se crear una red Wi-Fi entre ordenadores (P2P o *adhoc*, es decir, sin infraestructura o punto de acceso), si se cambia de una red Wi-Fi a otra, o se activa o desactiva el interfaz Wi-Fi:

918. Se recomienda habilitar estas tres opciones para tener un mayor control sobre los cambios asociados al interfaz Wi-Fi, así como tener conocimiento de los eventos asociados.

919. OS X lleva a cabo una comprobación automática para verificar si una red Wi-Fi dispone de un portal cautivo (*captive portal*), siendo necesario que el usuario lleve a cabo un proceso de autentificación antes de disponer de conectividad completa a la red Wi-Fi[147].

920. Para ello, OS X intenta verificar la conectividad generando tráfico HTTP hacia una URL de pruebas, "http://captive.apple.com/hotspot-detect.html", en el caso de OS X Yosemite (y por defecto, ya que pueden definirse otras URLs para redes Wi-Fi específicas), tal y como se establece en el fichero PLIST de la aplicación cliente encargada de estas tareas, "/Library/Preferences/SystemConfiguration/CaptiveNetworkSupport/Settings.plist".

921. Desde el punto de vista de la seguridad, existe la posibilidad no documentada de manipular la URL de pruebas empleada para llevar a cabo esta comprobación, apuntando por ejemplo a localhost, y evitando que se genere ningún tráfico (no cifrado) automáticamente y, por tanto, ser víctima de potenciales ataques derivados de este tráfico.

5.13.13 VERIFICACIÓN DE CERTIFICADOS DIGITALES

922. OS X permite de manera general verificar la validez de los certificados digitales recibidos mediante OCSP (*Online Certificate Status Protocol*) y CRL (*Certificate Revocation List)*:

```
$ defaults read com.apple.security.revocation CRLStyle
BestAttempt
$ defaults read com.apple.security.revocation OCSPStyle
BestAttempt
```

923. Por defecto OS X intenta verificar la validez del certificado para ambos protocolos de comprobación, pero si no es posible confirmarla, prosigue con la comunicación.

924. Es posible establecer una configuración más restrictiva, donde únicamente se permita las comunicaciones si ha sido posible verificar la validez del certificado digital:

```
$ sudo defaults write com.apple.security.revocation CRLStyle -string
RequireIfPresent
$ sudo defaults write com.apple.security.revocation OCSPStyle -string
RequireIfPresent
```

925. Aunque esta es una configuración más segura, en el pero de los casos se puede ver afectada por problemas de conectividad hacia los servidores de validación de los certificados digitales correspondientes, no siendo posible establecer comunicaciones con los servidores finales que han presentado el certificado.

147 https://grpugh.wordpress.com/2014/10/29/an-undocumented-change-to-captive-network-assistant-settings-in-os-x-10-10-yosemite/

5.13.14 NAVEGACIÓN WEB

926. OS X dispone de la posibilidad de instalar múltiples navegadores web para el acceso a páginas y aplicaciones web, tanto en Internet como en la Intranet de la organización: Safari (único navegador web disponible por defecto en OS X), Firefox, Chrome, Opera, etc.

5.13.14.1 MÓDULOS DEL NAVEGADOR WEB

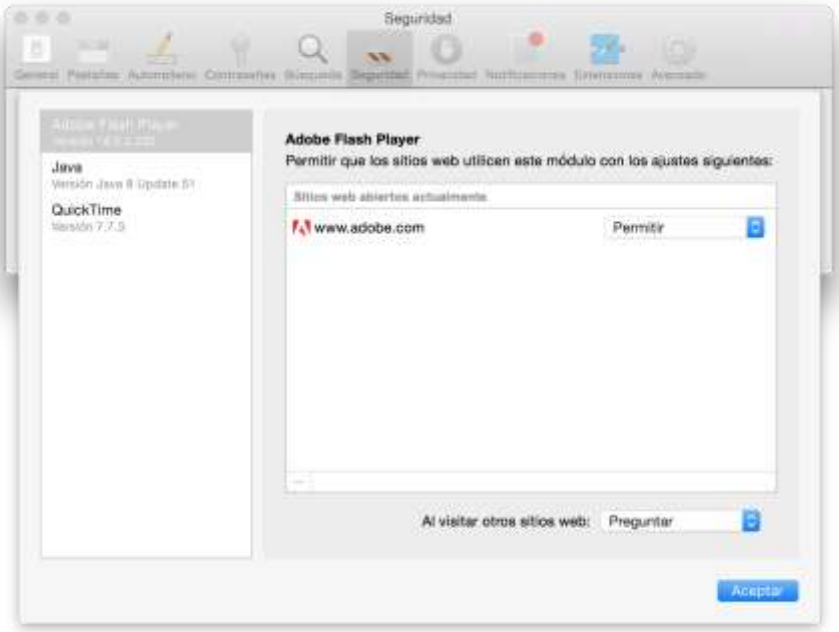
927. Desde la versión 6.1 de Safari en adelante es posible definir qué módulos o *plug-ins* o complementos estarán disponibles para qué sitios web, pudiéndose activar o desactivar cada uno de los *plug-ins* disponibles de manera individualizada para cada sitio web [Ref.- 18].

Nota: las instrucciones de configuración de la presente guía que hacen uso de un navegador web emplean Safari como referencia, al ser este el navegador web disponible por defecto en OS X, siendo posible llevar a cabo una configuración similar en otros navegadores web en OS X.

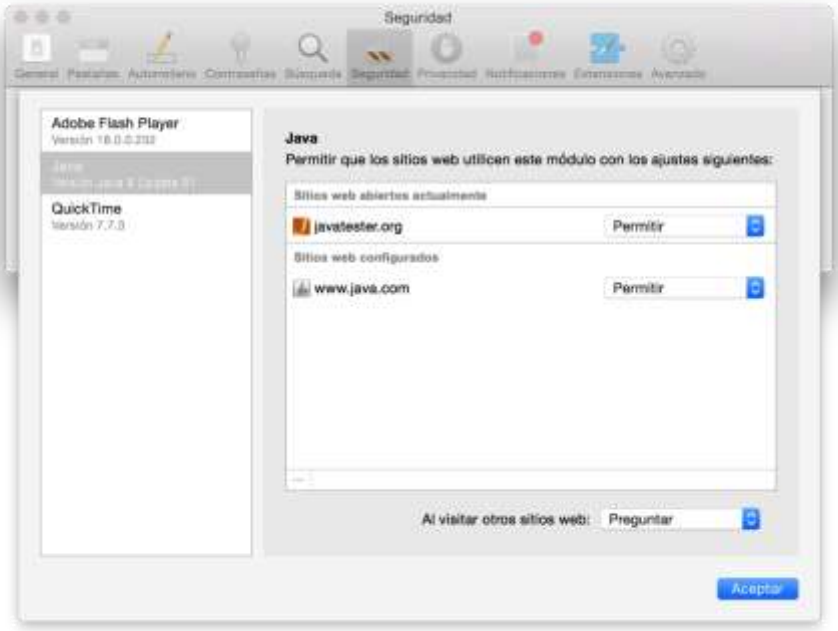
Las opciones de configuración de Safari detalladas a lo largo de la presente guía corresponden a la versión 8.0 (OS X 10.10) o 8.0.7 (OS X 10.10.4) de Safari.

928. Safari permite deshabilitar los diferentes *plug-ins* disponibles y establecer políticas de uso personalizadas desde el menú "Safari - Preferencias…", y en concreto mediante la opción "Módulos de Internet" (o *plug-ins*) de la pestaña "Seguridad", a través del botón "Ajustes de sitios web…":

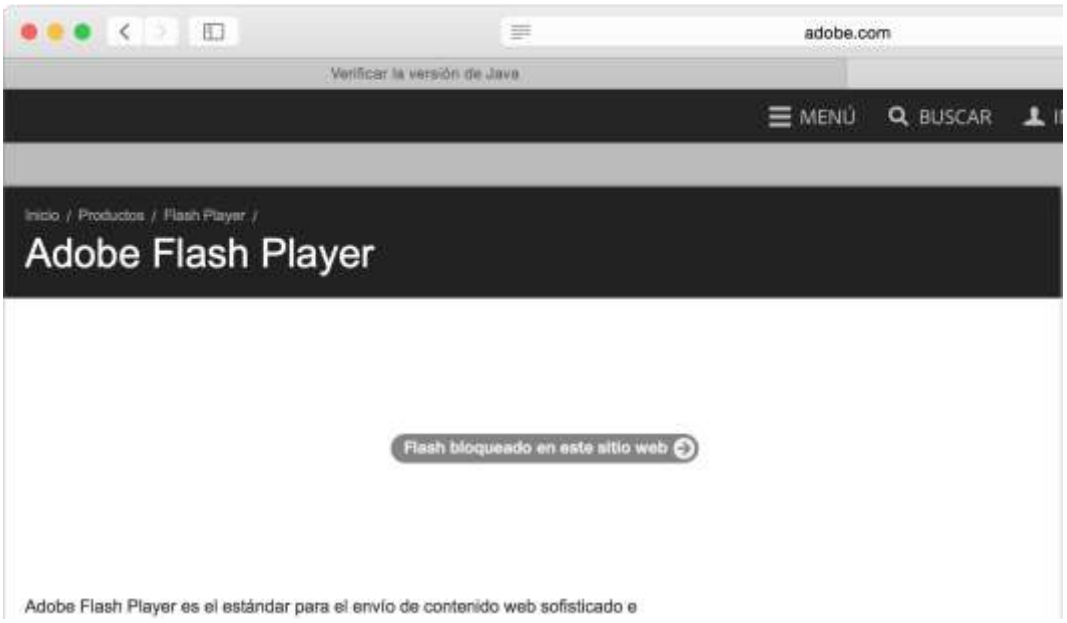
929. La ventana de ajustes de los sitios web permite establecer políticas de ejecución de los diferentes módulos o *plug-ins* para sitios web concretos, y declarar una política por defecto para cada *plug-in*, que será de aplicación para el resto de sitios web no incluidos en la lista superior (la opción por defecto puede ser diferente para cada módulo):



930. Los módulos instalados en OS X aparecen listados en la columna de la izquierda. Mediante la selección de cualquiera de ellos es posible visualizar los sitios web asociados (tanto los que están abiertos actualmente como los que han sido configurados previamente) y su configuración: "Preguntar", "Bloquear", "Permitir" o "Permitir siempre", y "Ejecutar en modo no seguro".



931. Cuando el usuario accede por primera vez a un sitio web que hace uso de una tecnología soportada por uno de los *plug-ins* disponibles, si la política por defecto (o para ese sitio web en concreto) es "Preguntar", visualizará un componente que indica que se dispone de contenido en la página web asociado a un *plug-in*, pero que éste no ha sido cargado. Si se pulsa sobre dicho componente, aparecerá una ventana de diálogo que le pregunta al usuario si confía en el sitio web para ejecutar contenido para un *plug-in* concreto:


adobe.com
Verificar la versión de Java
MENÚ
BUSCAR
Inicio / Productos / Flash Player /
Adobe Flash Player
Flash bloqueado en este sitio web
Adobe Flash Player es el estándar para el envío de contenido web sofisticado e


adobe.com
Verificar la versión de Java
Adobe - Flash Player
Adobe
Inicio / Productos / Flash Player /
Adobe Flash Player
¿Desea confiar en el sitio web "www.adobe.com" para que utilice el módulo "Adobe Flash Player"?
En el panel Seguridad de las preferencias de Safari, puede gestionar los sitios web en los que desea confiar para que utilicen este módulo.
Confiar
Cancelar


java.com
Verificar la versión de Java
Adobe - Flash Player
Java
Buscar
Descargar
Ayuda
Recursos de ayuda
¿Qué es Java?
Preguntas frecuentes sobre Mac
Mac OS X Chrome
¿Por qué no puedo usar Chrome con Java 7 en mi
Verificando la instalación
Detectando Java en su equipo
Java bloqueado en este sitio web


java.com
Verificar la versión de Java
Adobe - Flash Player
Java
Buscar
¿Desea confiar en el sitio web "www.java.com" para que utilice el módulo "Java"?
En el panel Seguridad de las preferencias de Safari, puede gestionar los sitios web en los que desea confiar para que utilicen este módulo.
Confiar
Cancelar
Recursos de ayuda
¿Qué es Java?
Preguntas frecuentes sobre Mac

932. Si el usuario selecciona "Confiar", ese sitio web será añadido a la lista blanca de sitios web que pueden hacer uso de esa tecnología automáticamente en accesos futuros, mediante la directiva "Permitir". El botón "Cancelar" deniega la posibilidad de cargar los contenidos asociados al *plug-in*, y añade el sitio web a la lista junto a la directiva "Bloquear":

933. Si la política es "Bloquear", el usuario visualizará un componente que indica que el contenido de la página web asociado a un *plug-in* ha sido bloqueado. Si se pulsa sobre dicho componente, aparecerá una alerta dónde el usuario puede decidir si desea ejecutar dicho contenido.

934. Si la política es "Permitir", el contenido asociado al *plug-in* es cargado sin consultar al usuario, a menos que el *plug-in* esté bloqueado por la funcionalidad de cuarentena de archivos de OS X (ver apartado "5.8.2. Gatekeeper y Cuarentena de archivos").

935. Si la política es "Permitir siempre", el contenido asociado al *plug-in* es cargado sin consultar al usuario, incluso aunque el *plug-in* esté bloqueado por la funcionalidad de cuarentena de archivos de OS X (ver apartado "5.8.2. Gatekeeper y Cuarentena de archivos"). Se recomienda limitar el uso de esta opción desde el punto de vista de seguridad.

936. La opción "Ejecutar en modo no seguro" permite la carga de contenidos por parte del *plug-in* sin ninguna comprobación de seguridad frente a software o contenidos maliciosos, por lo que nunca debería ser empleada.

937. Por ejemplo, el apartado "5.3.4. Actualizaciones de aplicaciones de terceros" detalla como actualizar, deshabilitar y/o gestionar los *plug-ins* asociados a Java y Flash en el navegador web Safari.

5.13.14.2 DESCARGA DE ARCHIVOS

938. Safari, por defecto, abre automáticamente los archivos "seguros" descargados, considerando "seguros" vídeos, imágenes, sonidos, documentos de texto y PDF, y archivos comprimidos.

939. Desde "Safari - Preferencias…", y en concreto desde la pestaña "General", se recomienda deshabilitar ese comportamiento desactivando la opción "Abrir archivos 'seguros' al descargarlos":

5.13.14.3 AUTORELLENO DE FORMULARIOS WEB Y CONTRASEÑAS

940. Safari, por defecto, auto rellena formularios web empleando la información de la tarjeta de contacto del usuario, nombres de usuario y contraseñas, tarjetas de crédito y otros formularios.

941. Desde "Safari - Preferencias…", y en concreto desde la pestaña "Autorelleno", se recomienda deshabilitar ese comportamiento desactivando todas las opciones disponibles:

942. Mediante el botón "Editar…" de cada una de las opciones es posible editar los campos de la tarjeta de contacto, acceder a la pestaña "Contraseñas", y gestionar la información de tarjetas de crédito y de campos a completar en otros formularios.

943. La pestaña "Contraseñas", por defecto, tiene habilitada la opción "Rellenar automáticamente nombres de usuario y contraseñas" (sincronizada con la pestaña previa), y permite gestionar la asignación de credenciales a diferentes sitios web:

944. Realmente esta pantalla corresponde a un acceso directo a las credenciales web disponibles para Safari desde la aplicación "Acceso a Llaveros" (ver apartado "5.8.7. Acceso a Llaveros").

945. El "Generador de contraseñas" de Safari (integrado con "Acceso a Llaveros") permite obtener sugerencias de contraseñas robustas y emplear contraseñas diferentes para cada sitio web, evitando así su reutilización.

5.13.14.4 SITIOS WEB FRAUDULENTOS

946. Safari proporciona tecnologías anti-phishing con el objetivo de detectar sitios web fraudulentos, que están suplantando otro sitio web legítimo con el objetivo de robar las credenciales e información sensible de sus usuarios.

947. En el caso de visitar un sitio web sospechoso, Safari bloqueará el acceso y mostrará un mensaje de alerta indicando el motivo.

948. Para hacer uso del servicio "Google Safe Browsing Service" en Safari puede ser necesario (según la versión de OS X) modificar la configuración del cortafuegos. En caso contrario, la pantalla de configuración de Safari, desde el menú "Safari - Preferencias…", y la pestaña "Seguridad", mediante su opción "Advertir al visitar un sitio web fraudulento" (*Fraudulent Sites*), mostrará que no es posible comunicarse con este servicio y el número de días que han transcurrido desde la última conexión.

5.13.14.5 SEGURIDAD

949. También desde la pestaña de "Seguridad" de las preferencias de Safari se dispone de opciones para gestionar el uso de Javascript, bloquear ventanas emergentes, y permitir el uso de WebGL, todas ellas habilitadas por defecto. Se recomienda usar las opciones por defecto, salvo en el caso de WebGL si no se hace uso de esta tecnología:

5.13.14.6 COOKIES

950. Safari proporciona adicionalmente capacidades para gestionar el uso de cookies desde el menú "Safari - Preferencias…", y la pestaña "Privacidad", desde donde es posible definir si se aceptarán cookies de sitios web. Se recomienda usar la opción por defecto, "Permitir de los sitios que visito":

5.13.14.7 SERVICIOS DE UBICACIÓN Y SEGUIMIENTO

951. Asimismo, desde el mismo menú de configuración de Safari es posible especificar qué sitios web tendrán acceso a los servicios o información de localización. Se recomienda emplear la opción "Denegar sin avisar", en lugar de la opción por defecto "Preguntar una vez al día para cada sitio web" (ver imagen superior).

952. Desde la misma pantalla se recomienda activar la opción "Pedir a los sitios web que no me rastreen" (deshabilitada por defecto), para que Safari haga uso de la cabecera HTTP "Do Not Track" ("DNT") en sus peticiones HTTP(S).

5.13.14.8 AJUSTES DE CONFIGURACIÓN AVANZADOS

953. Desde la pestaña de configuración de Safari "Avanzado" es posible especificar qué se desea visualizar la dirección completa del sitio web en el campo destinado para la URL (opción deshabilitada por defecto):

954. Se recomienda habilitar esta opción para poder ver todos los detalles del sitio web con el que se establece una conexión sin tener que seleccionar activamente el campo de la URL, incluyendo el protocolo empleado (http:// o https://), el recurso web concreteo y los parámetros de tipo GET empleados en la petición:

5.13.15 VPN

955. Con el objetivo de proteger el tráfico de red gestionado por OS X, especialmente en redes inseguras como por ejemplo *hotspots* Wi-Fi, se recomienda hacer uso de tecnologías VPN (*Virtual Private Network*) que permiten cifrar todo el tráfico enviado y recibido desde el equipo, como por ejemplo, OpenVPN [Ref.- 61].

5.14 ANTIVIRUS

956. Como mecanismo de seguridad complementario para proteger el sistema operativo OS X, así como las tareas y actividades diarias del usuario, se recomienda evaluar la posibilidad de instalar un producto o solución antivirus, que debe mantenerse permanentemente actualizada [Ref.- 60].

957. La utilización o no de una solución antivirus en OS X es dependiente del tipo de perfil asociado al usuario principal que hace uso del equipo, de la sensibilidad, criticidad y confidencialidad de la información que gestiona, y del tipo de tareas comunes que desempeña.

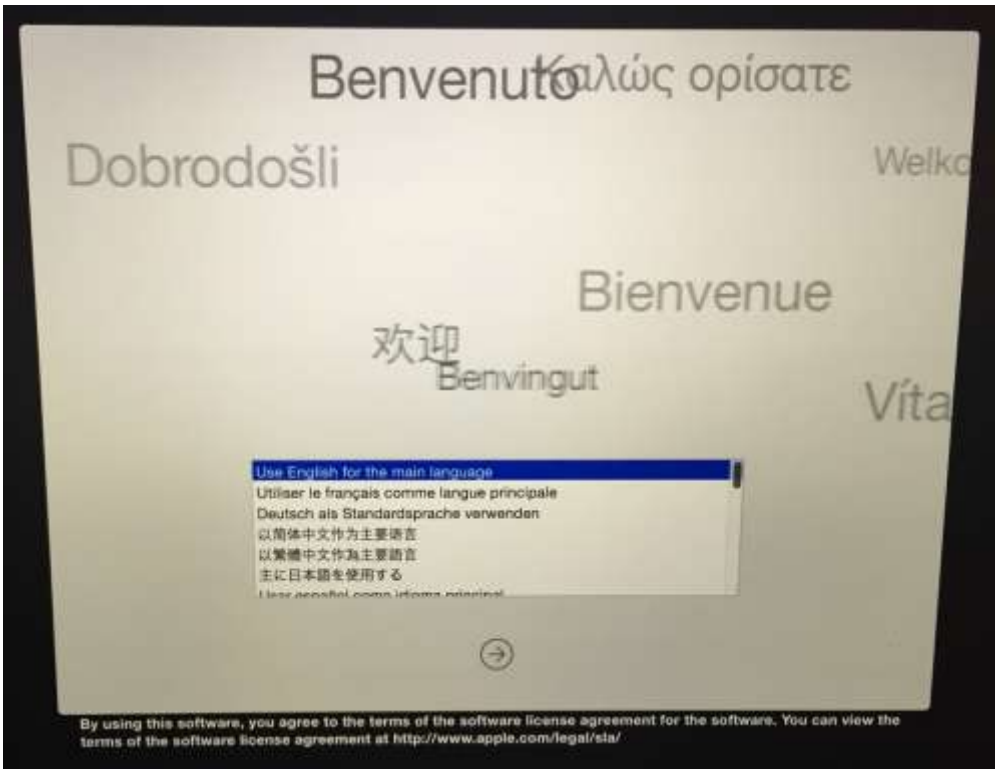
5.15 SISTEMA DE DETECCIÓN DE INTRUSOS (IDS)

958. Complementariamente, es posible aumentar el nivel de seguridad y las capacidades de detección de incidentes del sistema operativo OS X y los equipos Mac mediante la utilización de un sistema de detección de intrusos (IDS, *Intrusion Detection System*) local (o de *host*) que permita identificar situaciones anómalas, habitualmente asociadas a una infección del ordenador o a una intrusión de seguridad [Ref.- 81].

ANEXO A. PROCESO DE INSTALACIÓN Y CONFIGURACIÓN INICIAL DE OS X

El presente apartado detalla el proceso de instalación y configuración inicial de OS X 10.10.x (Yosemite) al encender por primera vez el ordenador tras su adquisición (o tras restablecer los ajustes de fábrica o formatearlo).

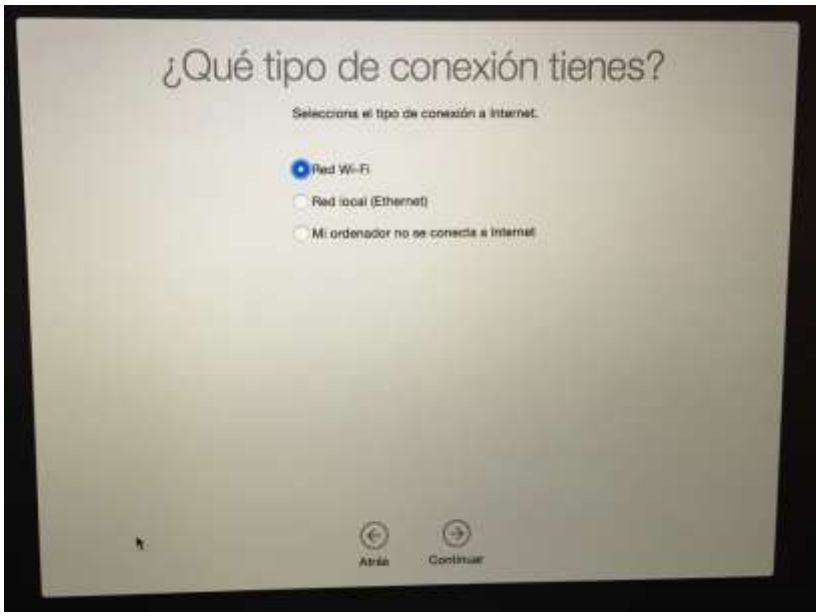
Al arrancar el ordenador por primera vez, se muestra una pantalla de bienvenida, "Welcome" ("Bienvenido"), donde se debe seleccionar el idioma (por defecto inglés) con el que se desea configurar el dispositivo y que también se empleará durante el proceso de instalación (por ejemplo, "Usar español como idioma principal"):



Mediante la selección de cada una de las opciones (con la tecla enter o retorno, o posteriormente con el icono con una flecha hacia la derecha, "Continuar") es posible progresar a través de los diferentes menús, pasos o pantallas del proceso de configuración inicial.

A continuación se muestran las pantallas que permiten seleccionar el país ("España") y el teclado ("Español - ISO"):

Posteriormente se muestra la pantalla de conectividad, donde es posible seleccionar la red Wi-Fi que será empleada durante el proceso de configuración. También se dispone de la posibilidad de conectarse a través de una red cableada (Ethernet) mediante el botón "Otras opciones de red" o de configurar la conexión de red más tarde:

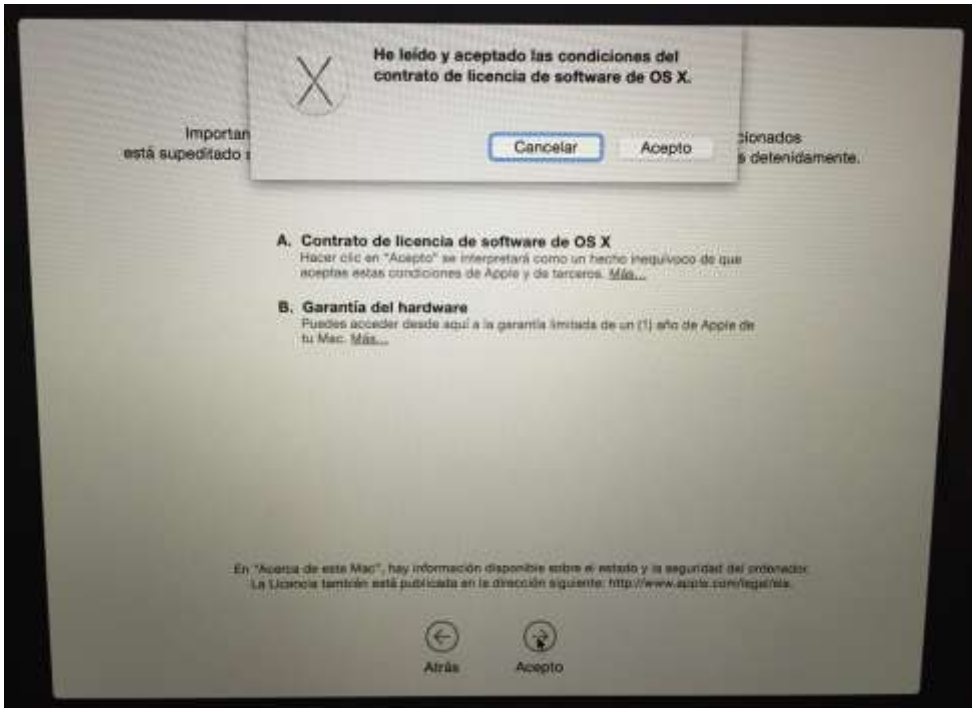


La configuración de algunos servicios requieren disponer de conexión a Internet. Sin embargo, se sugiere realizar la instalación inicial sin conectividad para disponer de mayor control sobre la configuración de red y del equipo:

Nota: el proceso de instalación y configuración inicial descrito no habilita la conexión a Internet. En el caso de configurar la conectividad hacia Internet durante el proceso de instalación y configuración inicial, los pasos y opciones disponibles pueden variar.

A continuación se permite transferir información a este Mac desde otro Mac, PC con Windows, o desde una copia de seguridad (asociada a Time Machine u a otro disco de arranque). Para realizar una instalación inicial limpia debe seleccionarse la opción "No transferir ninguna información ahora", siendo posible realizar la transferencia posteriormente con el Asistente de Migración:

Es necesario a continuación aceptar los "Términos y Condiciones" del contrato de licencia de software de OS X:



El siguiente paso insta al usuario a crear una cuenta de usuario en el ordenador. Esta cuenta de usuario inicial dispone de permisos de administrador, por lo que se recomienda crear una cuenta de administrador (por ejemplo, "admin"), qué sólo será utilizada para realizar tareas administrativas que requieren privilegios elevados:

Debe introducirse el nombre del usuario, nombre de la cuenta y la contraseña asociada suficientemente robusta (opcionalmente se puede seleccionar la imagen asociada a la cuenta). El nombre de la cuenta será empleado como nombre del directorio principal o home (o carpeta de inicio) asociada al usuario bajo "/Users/" (por ejemplo, "/Users/admin/").

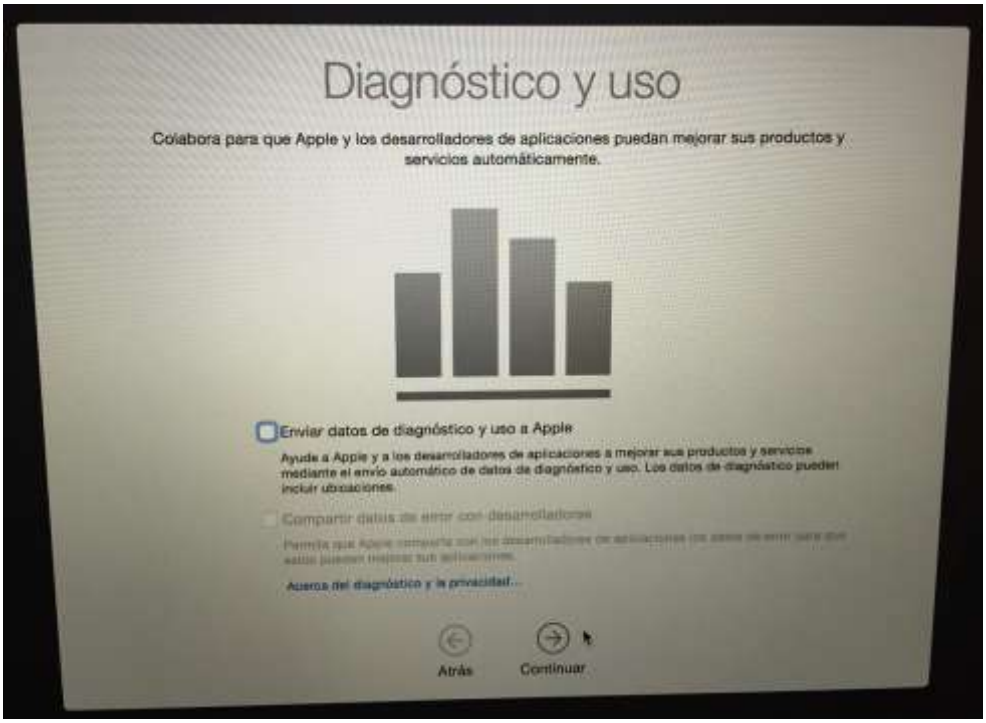
No se recomienda hacer uso del nombre real del propietario a la hora de seleccionar el nombre de la cuenta de usuario, independientemente de si es un administrador o un usuario estándar.

No se recomienda añadir ninguna indicación o recordatorio de la contraseña del usuario.

Si se desea que OS X sincronice la zona horaria del equipo según la ubicación actual del mismo, puede seleccionarse dicha opción (activa por defecto). Estas capacidades están disponibles en OS X desde "Preferencias del Sistema - Fecha y hora" mediante la opción "Ajustar fecha y hora automáticamente" y la posibilidad de poder seleccionar diferentes servidores de tiempos (NTP) de Apple: América/EEUU, Asia o Europa.

Se recomienda hacer uso de esta opción en OS X para disponer de la información de fecha y hora lo más precisa posible, ya que la misma es empleada para numerosos aspectos asociados a la seguridad, como la sincronización de registros, autentificación mediante kerberos, etc.

La siguiente pantalla solicita la colaboración del usuario para enviar datos de diagnóstico y uso a Apple y a los desarrolladores de aplicaciones, así como compartir datos de los errores con estos, con el objetivo de mejorar sus productos y servicios:



Desde el punto de vista de la privacidad, se recomienda deshabilitar ambas opciones (las dos activas por defecto).

A continuación, la pantalla "Configurando el Mac" llevará a cabo el proceso de configuración del ordenador, presentándose el escritorio de OS X al finalizar:

Una vez se dispone de acceso al escritorio de OS X, ha finalizado el proceso de instalación y configuración inicial, y es posible empezar a hacer uso de OS X y aplicar las recomendaciones de seguridad de la presente guía:

El siguiente paso recomendado desde el punto de vista de seguridad es llevar a cabo la creación de una cuenta de usuario estándar o no privilegiada (ver apartado "5.7.1. Creación de una cuenta de usuario estándar") con la que implementar el resto de tareas de configuración, proporcionando las credenciales de la cuenta de administrador creada previamente cuando sea necesario.

ANEXO B. PROCESO DE RESTAURACIÓN DE LOS AJUSTES DE FÁBRICA O FORMATEO DE OS X

El presente apartado detalla el proceso de restauración de los ajustes de fábrica o formateo completo de OS X 10.10.x (Yosemite) si se desea eliminar todos los datos e información que contiene el ordenador, por ejemplo, para reemplazarlo.

En primer lugar se recomienda realizar una copia de seguridad de todos los datos, por ejemplo, mediante Time Machine.

Se recomienda desactivar previamente todas las cuentas asociadas al equipo, como por ejemplo:

- iTunes: Desde el menú "Store - Retirar autorización a este ordenador" es posible eliminar la vinculación entre la cuenta de usuario en iTunes, y en la App Store, y el ordenador.

Se recomienda restaurar la memoria NVRAM (ver apartado "5.4.5. Modo de restablecimiento de la NVRAM").

Se recomienda restaurar el controlador de administración del sistema (SMC) (ver apartado "5.4.6. Modo de restablecimiento del SMC").

Por último, se recomienda restaurar el equipo a los ajustes de fábrica, arrancando el equipo a la vez que se presionan las teclas Cmd+R para entrar en el modo de recuperación y acceder a la pantalla "Utilidades de OS X" (ver apartado "5.4.4. Recuperación de OS X").

Desde este modo es posible acceder a la "Utilidad de Discos", y tras seleccionar la partición principal del disco duro, asociada por defecto a la partición lógica "Macintosh HD" (disponible habitualmente en la parte superior izquierda, correspondiente a la segunda entrada: "Partición lógica (cifrada)" frente a "Grupo de volúmenes lógico"), se debe acceder a la pestaña "Borrar", que permite borrar todos los contenidos del disco duro.

Debe seleccionarse el formato "Mac OS Plus (con registro)" en el menú "Formato", proporcionar un nombre para el disco desde el menú "Nombre" (por ejemplo, "Macintosh HD"), y pulsar el botón "Borrar…".

Adicionalmente, si se desean eliminar todos los contenidos del disco duro de forma segura (ver apartado "5.8.9. Borrado seguro de ficheros"), se puede emplear el siguiente comando desde un terminal para borrar de forma segura el disco duro completo, incluyendo todas sus particiones:

```
$ sudo diskutil secureErase 2 /Volumes/Macintosh\ HD
```

En el caso de discos SSD, el método recomendado pasa por hacer uso de FileVault (ver apartado "5.8.4. Cifrado completo del disco: FileVault") y emplear la funcionalidad de borrado remoto (remote wipe) de "Buscar mi Mac" en iCloud (ver apartado "5.12. iCloud: Buscar mi Mac") [Ref.- 72]. Esta acción eliminará las claves de cifrado del disco, haciendo que los datos almacenados en él no sean recuperables.

Finalmente, si se desea, se debe proceder a reinstalar el sistema operativo OS X en el ordenador, saliendo de la "Utilidad de Discos" y empleando la opción "Reinstalar OS X".

Alternativamente se dispone de otras opciones para reinstalar OS X:

- Si no se desea hacer uso de las capacidades de reinstalación de OS X a través de Internet es posible, durante el proceso de arranque del equipo, reiniciar el mismo desde un CD, DVD o unidad de memoria USB externa de arranque, mediante la tecla C (ver apartado "5.4.2.1. ARRANCAR DESDE UN CD/DVD O UNA MEMORIA USB EXTERNA").

  Si la unidad externa dispone de una copia del disco de instalación de OS X [Ref.- 26], desde el mismo es posible llevar a cabo la instalación de OS X empleando el método tradicional, haciendo uso de una unidad local.

  Si la unidad externa dispone de un sistema de recuperación de OS X [Ref.- 25] (ver apartado "5.4.4.3. ASISTENTE DE DISCO DE RECUPERACIÓN"), desde el mismo es posible acceder a la misma funcionalidad asociada al modo de recuperación integrado en OS X (ver apartado "5.4.4. Recuperación de OS X"), pero que requiere disponer de conexión a Internet.

- Durante el proceso de arranque, si se dispone de una conexión hacia Internet con un ancho de banda aceptable, se puede iniciar el equipo en modo de recuperación a través de Internet, mediante las teclas Cmd+Alt+R.

  Tras configurar la conexión de red, la opción "Reinstall OS X" descargará e instalará OS X desde Internet en el equipo.

A partir de ese momento se debería disponer de un nuevo equipo basado en OS X.

ANEXO C. LISTADO DE EXTENSIONES DE KERNEL POR DEFECTO

El siguiente listado incluye las extensiones de kernel que están disponibles bajo "/System/Library/Extensions/*.kext" y "/Library/Extensions/*.kext" por defecto en OS X 10.10 Yosemite para el modelo de equipo Mac empleado para la elaboración de la presente guía:

/Library/Extensions/:

- ACS6x.kext
- ATTOCelerityFC8.kext
- ATTOExpressSASHBA2.kext
- ATTOExpressSASRAID2.kext
- ArcMSR.kext
- CalDigitHDProDrv.kext
- HighPointIOP.kext
- HighPointRR.kext
- PromiseSTEX.kext
- SoftRAID.kext

/System/Library/Extensions/:

- ALF.kext
- AMD2400Controller.kext
- AMD2600Controller.kext
- AMD3800Controller.kext
- AMD4600Controller.kext
- AMD4800Controller.kext
- AMD5000Controller.kext
- AMD6000Controller.kext
- AMD7000Controller.kext
- AMD8000Controller.kext
- AMD9000Controller.kext
- AMDFramebuffer.kext
- AMDRadeonVADriver.bundle
- AMDRadeonX3000.kext
- AMDRadeonX3000GLDriver.bundle
- AMDRadeonX4000.kext
- AMDRadeonX4000GLDriver.bundle
- AMDSupport.kext
- ATIRadeonX2000.kext
- ATIRadeonX2000GA.plugin
- ATIRadeonX2000GLDriver.bundle
- ATIRadeonX2000VADriver.bundle
- Apple16X50Serial.kext
- AppleACPIPlatform.kext
- AppleAHCIPort.kext
- AppleAPIC.kext
- AppleBMC.kext
- AppleBacklight.kext
- AppleBacklightExpert.kext
- AppleBluetoothMultitouch.kext
- AppleCameraInterface.kext
- AppleCredentialManager.kext
- AppleEFIRuntime.kext
- AppleFDEKeyStore.kext
- AppleFSCompressionTypeDataless.kext

- AppleFSCompressionTypeZlib.kext
- AppleFWAudio.kext
- AppleFileSystemDriver.kext
- AppleGraphicsControl.kext
- AppleGraphicsPowerManagement.kext
- AppleHDA.kext
- AppleHIDKeyboard.kext
- AppleHIDMouse.kext
- AppleHPET.kext
- AppleHSSPIHIDDriver.kext
- AppleHSSPISupport.kext
- AppleHV.kext
- AppleHWAccess.kext
- AppleHWSensor.kext
- AppleIRController.kext
- AppleIntelCPUPowerManagement.kext
- AppleIntelCPUPowerManagementClient.kext
- AppleIntelFramebufferAzul.kext
- AppleIntelFramebufferCapri.kext
- AppleIntelHD3000Graphics.kext
- AppleIntelHD3000GraphicsGA.plugin
- AppleIntelHD3000GraphicsGLDriver.bundle
- AppleIntelHD3000GraphicsVADriver.bundle
- AppleIntelHD4000Graphics.kext
- AppleIntelHD4000GraphicsGLDriver.bundle
- AppleIntelHD4000GraphicsVADriver.bundle
- AppleIntelHD5000Graphics.kext
- AppleIntelHD5000GraphicsGLDriver.bundle
- AppleIntelHD5000GraphicsVADriver.bundle
- AppleIntelHDGraphics.kext
- AppleIntelHDGraphicsFB.kext
- AppleIntelHDGraphicsGA.plugin
- AppleIntelHDGraphicsGLDriver.bundle
- AppleIntelHDGraphicsVADriver.bundle
- AppleIntelHSWVA.bundle
- AppleIntelIVBVA.bundle
- AppleIntelLpssDmac.kext
- AppleIntelLpssGspi.kext
- AppleIntelLpssI2C.kext
- AppleIntelLpssI2CController.kext
- AppleIntelLpssSpiController.kext
- AppleIntelLpssUART.kext
- AppleIntelMCEReporter.kext
- AppleIntelSNBGraphicsFB.kext
- AppleIntelSNBVA.bundle
- AppleKextExcludeList.kext
- AppleKeyStore.kext
- AppleKeyswitch.kext
- AppleLPC.kext
- AppleLSIFusionMPT.kext
- AppleMCCSControl.kext
- AppleMCEDriver.kext
- AppleMCP89RootPortPM.kext
- AppleMIDIBluetoothDriver.plugin
- AppleMIDIFWDriver.plugin

- AppleMIDIIACDriver.plugin
- AppleMIDIRTPDriver.plugin
- AppleMIDIUSBDriver.plugin
- AppleMatch.kext
- AppleMikeyHIDDriver.kext
- AppleMobileDevice.kext
- AppleMobileFileIntegrity.kext
- AppleMultitouchDriver.kext
- AppleOSXWatchdog.kext
- ApplePlatformEnabler.kext
- AppleRAID.kext
- AppleRAIDCard.kext
- AppleRTC.kext
- AppleSDXC.kext
- AppleSEP.kext
- AppleSMBIOS.kext
- AppleSMBusController.kext
- AppleSMBusPCI.kext
- AppleSMC.kext
- AppleSMCLMU.kext
- AppleSRP.kext
- AppleSmartBatteryManager.kext
- AppleStorageDrivers.kext
- AppleThunderboltDPAdapters.kext
- AppleThunderboltEDMService.kext
- AppleThunderboltIP.kext
- AppleThunderboltNHI.kext
- AppleThunderboltPCIAdapters.kext
- AppleThunderboltUTDM.kext
- AppleTopCase.kext
- AppleTyMCEDriver.kext
- AppleUSBAudio.kext
- AppleUSBDisplays.kext
- AppleUSBEthernetHost.kext
- AppleUSBMultitouch.kext
- AppleUSBTopCase.kext
- AppleUpstreamUserClient.kext
- AppleVADriver.bundle
- AppleWWANAutoEject.kext
- AppleXsanFilter.kext
- Apple_iSight.kext
- AudioAUUC.kext
- BootCache.kext
- CellPhoneHelper.kext
- CoreStorage.kext
- DSACL.ppp
- DSAuth.ppp
- DVFamily.bundle
- Dont Steal Mac OS X.kext
- EAP-KRB.ppp
- EAP-RSA.ppp
- EAP-TLS.ppp
- GeForce.kext
- GeForceGA.plugin
- GeForceGLDriver.bundle

- GeForceTesla.kext
- GeForceTeslaGLDriver.bundle
- GeForceTeslaVADriver.bundle
- GeForceVADriver.bundle
- IO80211Family.kext
- IOACPIFamily.kext
- IOAHCIFamily.kext
- IOATAFamily.kext
- IOAVBFamily.kext
- IOAccelerator2D.plugin
- IOAcceleratorFamily.kext
- IOAcceleratorFamily2.kext
- IOAudio2Family.kext
- IOAudioFamily.kext
- IOBDStorageFamily.kext
- IOBluetoothFamily.kext
- IOBluetoothHIDDriver.kext
- IOCDStorageFamily.kext
- IODVDStorageFamily.kext
- IOFireWireAVC.kext
- IOFireWireFamily.kext
- IOFireWireIP.kext
- IOFireWireSBP2.kext
- IOFireWireSerialBusProtocolTransport.kext
- IOGraphicsFamily.kext
- IOHDIXController.kext
- IOHIDFamily.kext
- IONDRVSupport.kext
- IONetworkingFamily.kext
- IOPCIFamily.kext
- IOPlatformPluginFamily.kext
- IOReportFamily.kext
- IOSCSIArchitectureModelFamily.kext
- IOSCSIParallelFamily.kext
- IOSMBusFamily.kext
- IOSerialFamily.kext
- IOSlowAdaptiveClockingFamily.kext
- IOStorageFamily.kext
- IOStreamFamily.kext
- IOSurface.kext
- IOThunderboltFamily.kext
- IOTimeSyncFamily.kext
- IOUSBAttachedSCSI.kext
- IOUSBFamily.kext
- IOUSBMassStorageClass.kext
- IOUserEthernet.kext
- IOVideoFamily.kext
- L2TP.ppp
- Libm.kext
- NVDAGF100Hal.kext
- NVDAGK100Hal.kext
- NVDANV50HalTesla.kext
- NVDAResman.kext
- NVDAResmanTesla.kext
- NVDAStartup.kext

- NVSMU.kext
- OSvKernDSPLib.kext
- PPP.kext
- PPPSerial.ppp
- PPPoE.ppp
- PPTP.ppp
- Quarantine.kext
- Radius.ppp
- SMARTLib.plugin
- SMCMotionSensor.kext
- Sandbox.kext
- System.kext
- TMSafetyNet.kext
- acfs.kext
- acfsctl.kext
- autofs.kext
- cd9660.kext
- cddafs.kext
- corecrypto.kext
- exfat.kext
- iPodDriver.kext
- mcxalr.kext
- msdosfs.kext
- ntfs.kext
- pthread.kext
- smbfs.kext
- triggers.kext
- udf.kext
- vecLib.kext
- webcontentfilter.kext
- webdav_fs.kext

ANEXO D. REFERENCIAS

La siguiente tabla muestra las fuentes de información a las que se hace referencia a lo largo de la presente guía:

Nota: la mayoría de las referencias mostradas a continuación con el formato "http://support.apple.com/en-us/NNNN" pueden ser modificadas, sustituyendo en la URL el valor "/en-us/" (o "/en-gb/") por "/es-es/", para traducirlas de inglés a español (si están disponibles). Debe tenerse en cuenta que la versión en español podría no estar tan actualizada como la versión en inglés. Se ha empleado la versión en inglés o español indistintamente en función de su disponibilidad y contenidos en el momento de elaboración de la presente guía.

De manera similar, a la mayoría de las referencias mostradas a continuación con el formato "http://support.apple.com/kb/NNNN" se les puede añadir el parámetro "?viewlocale=es_ES" para traducirlas de inglés a español (si están disponibles).

Referencia	Título, autor y ubicación
[Ref.- 1]	"A Technical History of Apple's Operating Systems". Amit Singh. v2.0.1. July 2006. URL: http://osxbook.com/book/bonus/chapter1/ URL: http://osxbook.com/book/bonus/chapter1/pdf/macosxinternals-singh-1.pdf
[Ref.- 2]	"Mac OS X Internals: A Systems Approach". Amit Singh. Addison-Wesley Professional. 2006. URL: http://osxbook.com
[Ref.- 3]	"Mac OS X and iOS Internals: To The Apple's Core". 1st Ed. Jonathan Levin. Wiley. 2012. URL: http://www.newosxbook.com
[Ref.- 4]	"Mac OS X and iOS Internals: To The Apple's Core". 2st Ed. Volume I. Jonathan Levin. Wiley. 2015. URL: http://newosxbook.com/2ndKickoff.html
[Ref.- 5]	"Mac OS X Security Configuration Guides". Apple. URL: https://www.apple.com/support/security/guides/
[Ref.- 6]	"Actualizaciones de seguridad de Apple". Apple. URL: https://support.apple.com/es-es/HT201222 (ES) URL: https://support.apple.com/en-us/HT201222 (EN)
[Ref.- 7]	"Downloads ". Apple. URL: https://support.apple.com/downloads/
[Ref.- 8]	"Apple Developer Resources: Xcode". Apple. URL: https://developer.apple.com/resources/ URL: https://developer.apple.com/xcode/
[Ref.- 9]	"Downloads - Peripherals". Apple. URL: https://support.apple.com/downloads/peripherals
[Ref.- 10]	"Acerca de las actualizaciones de firmware EFI y SMC para ordenadores Mac con procesador Intel". Apple. URL: https://support.apple.com/es-es/HT201518 (HT1237)
[Ref.- 11]	"Cómo restablecer el controlador de gestión del sistema (SMC) del Mac". Apple. URL: https://support.apple.com/es-es/HT201295
[Ref.- 12]	"Mac EFI Security Update 2015-001". Apple. URL: https://support.apple.com/kb/DL1823 URL: https://support.apple.com/en-us/HT204934
[Ref.- 13]	"Acerca de las actualizaciones del firmware de EFI". Apple. URL: https://support.apple.com/es-es/HT201947
[Ref.- 14]	"OS X: Server addresses used by Software Update". Apple. URL: https://support.apple.com/en-us/HT202943 URL: https://support.apple.com/en-us/HT201962 (How to cascade Software Update Servers from a Central Software Update Server)
[Ref.- 15]	"Featured Manuals". Apple. URL: https://support.apple.com/manuals/
[Ref.- 16]	"New binaries in Yosemite". Justim Rummel. October, 2014. URL: https://www.justinrummel.com/new-binaries-in-yosemite/
[Ref.- 17]	"Flash Player Help / Uninstall Flash Player | Mac OS". Adobe. URL: https://helpx.adobe.com/flash-player/kb/uninstall-flash-player-mac-os.html
[Ref.- 18]	"Safari: About Internet plug-in management". Apple. URL: https://support.apple.com/en-us/HT202819

Referencia	Título, autor y ubicación
[Ref.- 19]	"Combinaciones de teclas de arranque para Mac". Apple. URL: https://support.apple.com/es-es/HT201255
[Ref.- 20]	"Try safe mode if your Mac doesn't finish starting up". Apple. URL: https://support.apple.com/en-us/HT201262
[Ref.- 21]	"Cómo elegir un disco de arranque en tu Mac". Apple. URL: https://support.apple.com/es-es/HT204417
[Ref.- 22]	"Cómo utilizar el Apple Hardware Test". Apple. URL: https://support.apple.com/es-es/HT201257
[Ref.- 23]	"Cómo utilizar Diagnósticos de Apple". Apple. URL: https://support.apple.com/es-es/HT202731
[Ref.- 24]	" OS X: Acerca de la recuperación de OS X". Apple. URL: https://support.apple.com/es-es/HT201314
[Ref.- 25]	"OS X: Acerca del Asistente de disco de recuperación". Apple. URL: https://support.apple.com/es-es/HT202294 URL: https://support.apple.com/kb/DL1433?locale=en_US&viewlocale=es_ES
[Ref.- 26]	"Crear un instalador ejecutable para OS X Mavericks o Yosemite". Apple. URL: https://support.apple.com/es-es/HT201372
[Ref.- 27]	"Cómo restablecer la NVRAM del Mac". Apple. URL: https://support.apple.com/en-us/HT204063
[Ref.- 28]	"Use a firmware password on your Mac". Apple. URL: https://support.apple.com/en-us/HT204455
[Ref.- 29]	"efipw". Paul Makowski. URL: https://code.google.com/p/efipw/ URL: https://paulmakowski.wordpress.com/2009/03/30/fun-with-apple-efi-firmware-passwords/ URL: https://paulmakowski.wordpress.com/tag/efi/
[Ref.- 30]	"Automated brute force attack against the EFI PIN". orvtech. February 2013. URL: https://github.com/orvtech/efi-bruteforce URL: http://orvtech.com/atacar-efi-pin-macbook-pro-en.html
[Ref.- 31]	"Brute force attack against the iCloud PIN lock". orvtech. March 2013. URL: http://orvtech.com/ataque-fuerza-bruta-pin-icloud-en.html
[Ref.- 32]	"Thunderstrike". Trammell Hudson. December 2014. URL: https://trmm.net/Thunderstrike URL: https://trmm.net/Thunderstrike_31c3 URL: https://trmm.net/Thunderstrike_FAQ
[Ref.- 33]	"Acerca del contenido de seguridad de OS X Yosemite v10.10.2 y de la Actualización de seguridad 2015-001". Apple. Enero 2015. URL: https://support.apple.com/es-es/HT204244
[Ref.- 34]	"Mac OS X: cómo iniciar en modo de un solo usuario o en modo verboso". Apple. URL: https://support.apple.com/es-es/HT201573
[Ref.- 35]	"Authorisation Rights". DssW. URL: http://www.dssw.co.uk/reference/authorization-rights/index.html
[Ref.- 36]	"Acerca del mensaje de alerta "¿Seguro que desea abrirlo?" (cuarentena de archivos / detección de software malicioso conocido) en OS X". Apple. URL: https://support.apple.com/es-es/HT201940
[Ref.- 37]	"How to hide a user account in OS X". Apple. URL: https://support.apple.com/en-us/HT203998
[Ref.- 38]	"The Early Boot Process - Kernel Programming Guide". Mac Developer Library. Apple. URL:https://developer.apple.com/library/mac/documentation/Darwin/Conceptual/KernelProgramming/booting/booting.html
[Ref.- 39]	"OS X: Acerca de Gatekeeper". Apple. URL: https://support.apple.com/es-es/HT202491
[Ref.- 40]	"DYLIB HIJACKING ON OS X". Patrick Wardle. Synack, USA. March 2015. URL: https://www.virusbtn.com/pdf/magazine/2015/vb201503-dylib-hijacking.pdf
[Ref.- 41]	"Malware Persistence on OS X Yosemite". Patrick Wardle. RSA Confrence 2015. URL: https://www.rsaconference.com/writable/presentations/file_upload/ht-r03-malware-persistence-on-os-x-yosemite_final.pdf
[Ref.- 42]	"Google Project Zero". Google. URL: https://code.google.com/p/google-security-research/issues/list?can=1 URL: https://googleprojectzero.blogspot.com

Referencia	Título, autor y ubicación
[Ref.- 43]	"Technical Note TN2206: OS X Code Signing In Depth". Mac Developer Library. Apple. URL: https://developer.apple.com/library/mac/technotes/tn2206/_index.html
[Ref.- 44]	"Thunderstrike 2". Trammel Hudson & Xeno Kovah & Corey Kallenberg. August 2015. URL: https://trmm.net/Thunderstrike_2 URL: https://trmm.net/Thunderstrike2_details URL: https://www.youtube.com/watch?v=Jsdqom01XzY
[Ref.- 45]	"Entitlement Key Reference". Mac Developer Library. Apple. URL: https://developer.apple.com/library/mac/documentation/Miscellaneous/Reference/EntitlementKeyReference/Chapters/AboutEntitlements.html#//apple_ref/doc/uid/TP40011195-CH1-SW1
[Ref.- 46]	"Gatekeeper Fundamentals, Part 1 & Part 2". The Instructional. February 2014. URL: http://www.theinstructional.com/guides/gatekeeper-fundamentals-part-1 URL: http://www.theinstructional.com/guides/gatekeeper-fundamentals-part-2
[Ref.- 47]	"OS X Yosemite: Firewall pane of Security & Privacy preferences". Apple. URL: https://support.apple.com/kb/PH18635
[Ref.- 48]	"A Cheat Sheet For Using pf in OS X Lion and Up". krypted. July 2012. URL: http://krypted.com/mac-security/a-cheat-sheet-for-using-pf-in-os-x-lion-and-up/
[Ref.- 49]	"Command Line Firewall Management In OS X 10.10". krypted. July 2015. URL: http://krypted.com/mac-security/command-line-firewall-management-in-os-x-10-10/
[Ref.- 50]	"OS X 10.10 DYLD_PRINT_TO_FILE Local Privilege Escalation Vulnerability". Stefan Esser. July 2015. URL: https://www.sektioneins.de/en/blog/15-07-07-dyld_print_to_file_lpe.html
[Ref.- 51]	"Hidden backdoor API to root privileges in Apple OS X" (RootPipe). Emil Kvarnhammar. April 2015. URL: https://truesecdev.wordpress.com/2015/04/09/hidden-backdoor-api-to-root-privileges-in-apple-os-x/
[Ref.- 52]	"About the security content of OS X Yosemite v10.10.3 and Security Update 2015-004". Apple. URL: https://support.apple.com/en-us/HT204659
[Ref.- 53]	"Phoenix: RootPipe lives! ...even on OS X 10.10.3". Patrick Wardle. April 2015. URL: https://objective-see.com/blog.html#blogEntry3 URL: https://vimeo.com/125345793
[Ref.- 54]	"Exploiting rootpipe again". Emil Kvarnhammar. July 2015. URL: https://truesecdev.wordpress.com/2015/07/01/exploiting-rootpipe-again/
[Ref.- 55]	"About the security content of OS X Yosemite v10.10.4 and Security Update 2015-005". Apple. URL: https://support.apple.com/en-us/HT204942
[Ref.- 56]	"CVE-2015-3673: Goodbye Rootpipe...(for now?)". Patrick Wardle. July 2015. URL: https://objective-see.com/blog.html#blogEntry5
[Ref.- 57]	"OS X Yosemite: Compartir la pantalla usando “Volver a mi Mac”". Apple. URL: https://support.apple.com/kb/PH18696?locale=es_ES&viewlocale=es_ES
[Ref.- 58]	"El ABC del Mac: AirDrop permite enviar archivos desde tu Mac a otros dispositivos iOS y ordenadores Mac cercanos". Apple. URL: https://support.apple.com/es-es/HT203106
[Ref.- 59]	"Introduction to AppleScript: Overview & Language Guide". Apple. URL:https://developer.apple.com/library/mac/documentation/AppleScript/Conceptual/AppleScriptX/AppleScriptX.html URL:https://developer.apple.com/library/mac/documentation/AppleScript/Conceptual/AppleScriptLangGuide/introduction/ASLR_intro.html
[Ref.- 60]	"Best Antivirus Software and Apps 2015". Tom's Guide. July 2015. URL: http://www.tomsguide.com/us/best-antivirus,review-2588-6.html
[Ref.- 61]	"Why You Should Connect to a VPN on Mac and iOS — and How To". The Mac Security Blog. Intego. August 2015. URL: http://www.intego.com/mac-security-blog/why-you-should-connect-to-a-vpn-on-mac-and-ios-and-how-to/
[Ref.- 62]	"OS X Yosemite: Compartir su pantalla". Apple. URL: https://support.apple.com/kb/PH18686?locale=es_ES&viewlocale=es_ES
[Ref.- 63]	"OS X Yosemite: Compartir sus archivos con usuarios de Mac". Apple. URL: https://support.apple.com/kb/PH18697?locale=es_ES&viewlocale=es_ES
[Ref.- 64]	"OS X Yosemite: Compartir su impresora". Apple. URL: https://support.apple.com/kb/PH18703?locale=es_ES&viewlocale=es_ES
[Ref.- 65]	"OS X Yosemite: Permitir a un ordenador remoto acceder al Mac". Apple. URL: https://support.apple.com/kb/PH18726?locale=es_ES&viewlocale=es_ES

Referencia	Título, autor y ubicación
[Ref.- 66]	"OS X Yosemite: Permitir acceso con Remote Desktop". Apple. URL: https://support.apple.com/kb/PH18687?locale=es_ES&viewlocale=es_ES
[Ref.- 67]	"OS X Yosemite: Aceptar Eventos Apple remotos". Apple. URL: https://support.apple.com/kb/PH18721?locale=es_ES&viewlocale=es_ES
[Ref.- 68]	"OS X Yosemite: Compartir su conexión a Internet". Apple. URL: https://support.apple.com/kb/PH18704?locale=es_ES&viewlocale=es_ES
[Ref.- 69]	"OS X Yosemite: Compartir archivos mediante Bluetooth". Apple. URL: https://support.apple.com/kb/PH18714?locale=es_ES&viewlocale=es_ES
[Ref.- 70]	"Spotlight Suggestions in OS X Yosemite and iOS: Are You Staying Private?". Intego. October 2014. URL: http://www.intego.com/mac-security-blog/spotlight-suggestions-in-os-x-yosemite-and-ios-are-you-staying-private/ URL: http://www.intego.com/mac-security-blog/spotlight-search-osx-yosemite-privacy-glitch/
[Ref.- 71]	"Utilizar FileVault para encriptar el disco de arranque del Mac". Apple. URL: https://support.apple.com/es-es/HT204837
[Ref.- 72]	"Securely Erasing a Mac SSD". Systems Boy. March 2012. URL: http://malcontentcomics.com/systemsboy/2012/03/securely-erasing-a-mac-ssd.html
[Ref.- 73]	"Best Practices for Deploying FileVault 2". Apple. URL: http://training.apple.com/pdf/WP_FileVault2.pdf
[Ref.- 74]	"Managing Yosemite's FileVault 2 with fdesetup". Der Flounder. February 2015. URL: https://derflounder.wordpress.com/2015/02/02/managing-yosemites-filevault-2-with-fdesetup/
[Ref.- 75]	"OS X: How to create and deploy a recovery key for FileVault 2". Apple. URL: https://support.apple.com/en-us/HT202385
[Ref.- 76]	"FileVault 2 Institutional Recovery Keys – Creation, Deployment and Use". Der Flounder. August 2014. URL: https://derflounder.wordpress.com/2014/08/13/filevault-2-institutional-recovery-keys-creation-deployment-and-use/
[Ref.- 77]	"Decrypting FileVault 2 on Mac OS X 10.8.4 – Unlock first, then decrypt". Der Flounder. June 2013. URL: https://derflounder.wordpress.com/2013/06/11/decrypting-filevault-2-on-mac-os-x-10-8-4-unlock-first-then-decrypt/
[Ref.- 78]	"Unlock or decrypt your FileVault 2-encrypted boot drive from the command line". Der Flounder. November 2011. URL: https://derflounder.wordpress.com/2011/11/23/using-the-command-line-to-unlock-or-decrypt-your-filevault-2-encrypted-boot-drive/
[Ref.- 79]	"Ten Things You Might Not Know About FileVault 2". Der Flounder. December 2014. URL: https://derflounder.wordpress.com/2014/12/18/ten-things-you-might-not-know-about-filevault-2/
[Ref.- 80]	"OS X Mountain Lion: Bluetooth profiles supported by Apple Bluetooth software". Apple. URL: https://support.apple.com/kb/PH10549
[Ref.- 81]	"MIDAS: Mac Intrusion Detection Analysis System". Etsy & Facebook. URL: https://github.com/etsy/MIDAS
[Ref.- 82]	"KON-BOOT For Apple Mac OSX Guide". Kon-Boot. URL: http://www.thelead82.com/kon-boot/konbootMAC_guide.pdf URL: http://www.piotrbania.com/all/kon-boot/
[Ref.- 83]	"XNU: a security evaluation". D Keuper. December 2012. URL: https://reverse.put.as/wp-content/uploads/2011/06/XNU_-a-security-evaluation-Daan_Keuper_2012-12-14-xnu.pdf
[Ref.- 84]	"Unauthorized Cross-App Resource Access on MAC OS X and iOS". June 2015. (by Indiana University, Georgia Tech, and China's Peking University) URL: https://drive.google.com/file/d/0BxxXk1d3yyuZOFlsdkNMSGswSGs/view URL: https://sites.google.com/site/xaraflaws/
[Ref.- 85]	"About the security content of OS X Yosemite v10.10.5 and Security Update 2015-006". Apple. URL: https://support.apple.com/en-us/HT205031
[Ref.- 86]	"CIS Apple OSX 10.10 Benchmark v1.0.0". Center for Internet Security (CIS). April 2015. URL: https://benchmarks.cisecurity.org/downloads/show-single/?file=osx1010.100
[Ref.- 87]	"OS X Yosemite - Core Technologies Overview". Apple. October 2014. URL: https://www.apple.com/osx/pdf/OSXYosemite_TO_FF1.pdf