CCN
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 458

Guía práctica de seguridad de macOS 10.14 Mojave

Julio 2019

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.03.20 11:42:28 +01'00'

NIPO: 083-19-210-1

Fecha de Edición: julio de 2019
Mónica Salas y Raúl Siles (DinoSec) han participado en la realización y modificación del presente documento y sus anexos.

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), 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 (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de enero, actualizado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, 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.

Julio de 2019

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

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

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

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

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

2. OBJETO

La presente guía proporciona un análisis general de los mecanismos y la configuración de seguridad recomendados para el sistema operativo macOS 10.14 de Apple©, también conocido como "Mojave", soportado para los ordenadores de sobremesa iMac, Mac Mini, Mac Pro, los portátiles MacBook, MacBook Air y MacBook Pro, y los servidores Mac Mini Server y Mac Pro Server [Ref.- 1], referenciados de manera genérica como ordenadores o equipos Mac. Se proporcionan detalles específicos de aplicación e implementación de las recomendaciones de seguridad y buenas prácticas necesarias para la prevención de los riesgos, amenazas, y vulnerabilidades de seguridad a las que están expuestos estos equipos en la actualidad, y se ha redactado para ofrecer un equilibrio entre seguridad y funcionalidad.

Antes de aplicar esta guía en un entorno de producción, debe confirmarse su adecuación a la organización objetivo, siendo validada previamente en un entorno aislado y controlado en el que se puedan realizar las pruebas necesarias y aplicar cambios en la configuración que se ajusten a los criterios específicos de la organización. El espíritu de esta guía no es reemplazar políticas ya consolidadas y probadas en 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 exhaustivo de los protocolos de comunicaciones basados en HTTPS (o TLS) y empleados entre los equipos con macOS y los diferentes servicios de Apple o de terceros.

Tampoco cubre de forma detallada la securización de los servicios de Apple ligados a la cuenta de usuario de iCloud y/o al Apple ID, que serán abordados en la "Guía CCN-STIC-459 - Cuenta de usuario, servicios y aplicaciones de Apple" [Ref.- 404].

Dada la interrelación entre los ordenadores y los dispositivos móviles basada en la compartición de la cuenta de usuario de iCloud y del Apple ID[1], se recomienda la lectura de las guías CCN-CERT asociadas a otros sistemas operativos de Apple, tanto de macOS como de plataformas móviles iOS, entre ellos:

- CCN-STIC-454(A) - Seguridad de dispositivos móviles: iPad (iOS 7.x) [Ref.- 400].
- CCN-STIC-455(A) - Seguridad de dispositivos móviles: iPhone (iOS 7.x) [Ref.- 401].
- CCN-STIC 455C - Guía Práctica de Seguridad en Dispositivos Móviles iPhone iOS 11.x [Ref.- 402].
- CCN-STIC 455D - Guía Práctica de Seguridad en Dispositivos Móviles iPhone iOS 12.x [Ref.- 403].

Al final de la presente guía se proporciona la tabla con los recursos web de las referencias citadas ("21. Anexo B. Referencias") y el índice de figuras ("22. Anexo C. Índice de figuras").

[1] El CCN-CERT tiene prevista la publicación de la guía "CCN-STIC-459 - Cuenta de usuario, servicios y aplicaciones de Apple" [Ref.- 404] para finales de 2019.

3. macOS

macOS (previamente denominado OS X) es el sistema operativo que Apple Computer introdujo en su primer ordenador personal Macintosh en 1984, pionero en la utilización en exclusiva de una interfaz gráfica de usuario. Desde su versión 10.8, OS X pasó a denominarse macOS, siendo ésta su denominación oficial actual.

macOS es un sistema operativo multicapa de tipo Unix, cuya versión 10.0 (Cheetah) salió al mercado en 2001. La versión 10.14 (Mojave) fue liberada en septiembre de 2018 y, a fecha de mayo de 2019, su cuota de mercado sobre el total de equipos con el sistema operativo macOS rondaba el 46%[2].

El *kernel* actual de macOS de 64 bits es XNU (X is Not Unix), basado en FreeBSD, capaz de ejecutar aplicaciones de 32 y 64 bits, y su arquitectura incluye [Ref.- 2]:

- *Drivers* y librerías del *kernel*:
  - Sistema de ficheros: soporta diferentes formatos de volúmenes, como NTFS, ExFAT, FAT, HFS+ y APFS (*Apple File System*, sistema de ficheros por defecto en Mojave), así como diferentes protocolos para el acceso a sistemas de ficheros a través de la red (AFP, *Apple(Talk) Filing Protocol*, NFS, y SMB).
  - Capa de red: implementa la pila TCP/IP de BSD 4.4 y sus APIs de sockets, soportando NAT, *multicast*, enrutamiento y filtrado de paquetes, entre otras características.
  - Mach (OSFMK, *kernel*): es el gestor de los recursos del procesador, como la CPU y la memoria, responsable de la memoria virtual, la multitarea, la comunicación entre procesos y los servicios en tiempo real.
  - IOKit (o I/O Kit): responsable de la gestión de dispositivos y de la carga de controladores (o *drivers*) bajo demanda.
- *Core Services*: proporcionan un interfaz para los servicios de comunicaciones de red de bajo nivel, que incluye la autentificación de los usuarios y del acceso a las credenciales.
- *Media Layer*: responsable de la gestión de los dispositivos gráficos y de audio.
- *Cocoa Layer*: responsable de la interacción con el usuario, ya que gestiona los eventos desencadenados por él, el interfaz gráfico y el comportamiento de las aplicaciones.

A lo largo de la presente guía, se proporcionarán nombres de comandos, utilidades y procesos del sistema, para los cuales se recomienda consultar la página "`man`" correspondiente. Aunque en el pasado Apple proporcionaba documentación sobre estas páginas, el enlace al recurso no está disponible a fecha de elaboración de este documento[3]: https://developer.apple.com/library/archive/documentation/Darwin/Reference/ManPages/

[2] http://gs.statcounter.com/macos-version-market-share/desktop/worldwide

[3] https://stackoverflow.com/questions/53220058/darwin-reference-manual-pages-missing

3.1 CARACTERÍSTICAS DE SEGURIDAD DE MACOS

El presente apartado proporciona una breve descripción de las características de seguridad que, habiendo sido introducidas en versiones anteriores (desde macOS 10.11, liberada en 2015), siguen vigentes en macOS Mojave. Durante la presente guía se indicará cómo aplicar los ajustes de configuración necesarios para sacar el máximo beneficio de ellas.

Adicionalmente, se recomienda la lectura de la guía de seguridad oficial de macOS [Ref.- 110], así como la lectura de los diferentes volúmenes de los libros "MacOS and iOS Internals" [Ref.- 89] para aquellos interesados en disponer de los detalles de más bajo nivel del funcionamiento interno del sistema operativo macOS.

CARACTERÍSTICAS INTRODUCIDAS EN MACOS 10.11 "EL CAPITAN"

Las características de seguridad vigentes en macOS que fueron introducidas en la versión 10.11 se pueden consultar en el WWDC de 2015 [Ref.- 20], "*Security and your Apps*":

- **System Integrity Protection** (SIP): apartado "9.10. SIP: System Integrity Protection".
- **App Transport Security** (ATS): apartado "9.13. ATS (App Transport Security)".
- **FileVault**: apartado "15.1. FileVault".
- **Keychain**: apartado "9.7. Gestión de llaveros".

CARACTERÍSTICAS INTRODUCIDAS EN MACOS 10.12 "SIERRA"

- Mejoras en el "**Gatekeeper**": introducido en macOS 10.8 (Lion), su cometido inicial era intentar impedir la ejecución inconsciente de programas descargados de Internet, de forma que el usuario debiera especificar activamente si admitía descargas solo de la Apple Store, desde la Apple Store y de desarrolladores identificados, o de cualquier fuente. En macOS Sierra (macOS 10.12), la opción de descarga de aplicaciones desde cualquier fuente dejó de estar disponible. Para más información, consultar el apartado "9.2. Gatekeeper y cuarentena de archivos".
- Soporte de *smart-cards* como segundo factor de autentificación: apartado "8.1.2. Opciones de inicio de sesión".
- A pesar de no haber introducido nuevas características muy relevantes desde el punto de vista de seguridad, macOS Sierra incluyó los parches para un elevado número de vulnerabilidades de seguridad que afectaban a versiones anteriores (muchas de ellas existentes desde macOS 10.7.5) [Ref.- 21].

CARACTERÍSTICAS INTRODUCIDAS EN MACOS 10.13 "HIGH SIERRA"

- **APFS**: apartado "15.5. APFS (Apple File System)". APFS se convirtió en macOS 10.13 en el sistema de ficheros por defecto en macOS.
- Se elimina el soporte para las conexiones TLS con servidores que proporcionen certificados firmados con SHA-1, incluyendo servidores de correo y de VPN.

- Se incrementa el control sobre las extensiones de *kernel* (kext, *kernel extension*) para evitar que el software malicioso haga uso de ellas para, por ejemplo, interceptar pulsaciones del teclado. Para ello, la primera vez que se cargue una extensión, se solicitará aprobación al usuario (ver apartado "9.5. Firma y verificación de aplicaciones y del kernel").
- Validación del *firmware*: consiste en una comprobación del *hardware ID* del *firmware* del equipo contra una base de datos de Apple que contiene las versiones de *firmware* válidas para un modelo concreto de equipo. Esta comprobación es semanal y, si se detecta alguna anomalía, se generará una advertencia que permite al usuario enviar un informe a Apple (o ignorarla).
- Las actualizaciones de seguridad que se incluyeron en la primera versión de macOS High Sierra están disponibles en la [Ref.- 22]. La última actualización de seguridad disponible a fecha de elaboración de la presente guía (principios de julio de 2019) es la de mayo de 2019 [Ref.- 23].
- High Sierra introdujo novedades para configuraciones empresariales de tipo MDM (*Mobile Device Management*), como:
    - Gestión de contraseñas de *firmware* y de cuentas de usuario.
    - Herramientas para reiniciar y/o apagar los equipos de forma remota.
    - Claves de FileVault custodiadas.
    - Restricciones de acceso a iCloud.
    - Capacidad para posponer las actualizaciones de *software* hasta 90 días, con el fin de dar un margen de prueba a los administradores.
- Bloqueo automático de audio y vídeo en los sitios web por parte de Safari, hasta que el usuario acepte su reproducción activamente a través de una ventana de diálogo. Adicionalmente, Safari introdujo bloqueos en los anuncios cruzados (ver apartado "14. Navegador web Safari").
- Soporte para autentificación basada únicamente en *smart-cards*: apartado "8.1.2. Opciones de inicio de sesión".
- ***Secure Token***: apartado "15.1.3. Secure Token".

3.2 MOJAVE (MACOS 10.14)

En este apartado se enumeran las características introducidas por la versión 10.14 de macOS, en particular, las relevantes desde el punto de vista de seguridad. En la [Ref.- 50] se dispone del enlace al WWDC de 2018, en el que se detallan estas características.

- Soporte nativo ampliado para el inicio de sesión mediante tarjetas inteligentes o *smart-cards*: apartado "8.1.2. Opciones de inicio de sesión".
- Introducción de mecanismos de control de acceso más restrictivos: apartado "8.2.4. TCC: Transparency, Consent and Control".
- Mejoras en la prevención de rastreo en la navegación web: apartado "14. Navegador web Safari".
- Control por parte de Safari sobre la reutilización de las contraseñas que el usuario guarda: apartado "14. Navegador web Safari".

- Cambios en el sistema de *logging* o registro de eventos: apartado "9.11. Supervisión de eventos".
- Mejoras específicas para los ordenadores comercializados con el chip T2: apartados "15.4. Cifrado de almacenamiento APFS con chip T2" y "18.9. Secure Boot para chip T2".
- macOS Mojave es la última versión de macOS que soporta aplicaciones de 32 bits, según anunció Apple en el WWDC 2018 [Ref.- 134].

4. ORDENADOR EMPLEADO

La presente guía ha sido probada y verificada con la versión 10.14.4 (liberada en abril de 2019) y 10.14.5 (liberada en mayo de 2019) sobre un equipo de pruebas MacBook Pro[4] configurado en español. De forma esporádica, algunas de las pruebas se han realizado sobre un MacBook Air perteneciente a un entorno de producción con la misma versión de Mojave, configurado en inglés.

```
$ uname -a
Darwin MacBook-Pro-de-CCN.local 18.5.0 Darwin Kernel Version 18.5.0: Mon Mar
11 20:40:32 PDT 2019; root:xnu-4903.251.3~3/RELEASE_X86_64 x86_64
```

Figura 1 - Versión de macOS

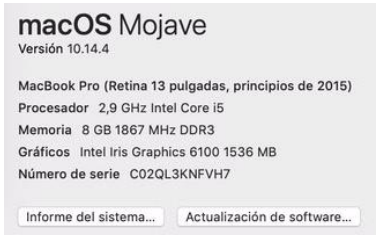


Figura 2 - Menú "Acerca de este Mac"

Se recomienda recabar e inventariar la información de versiones, tanto hardware como software, de los equipos a proteger, con el objetivo de disponer de todos los elementos necesarios a la hora de tomar decisiones relativas a la aplicación de nuevas actualizaciones y medidas de seguridad.

También ***se recomienda obtener periódicamente los ajustes de configuración y personalización activos en el sistema***, para lo cual puede emplearse el comando "`defaults read`". A través de la opción "`write <parámetro> nuevo_valor`" del comando "`defaults`" se puede modificar un ajuste concreto.

A fecha de elaboración de la presente guía, el recurso oficial relativo a la seguridad en macOS es el listado de las actualizaciones de seguridad recientes de los productos de Apple [Ref.- 3]. Se recomienda consultar su versión en inglés (EN), ya que es habitual que las últimas actualizaciones no aparezcan publicadas en la versión en español (ES) hasta días o semanas después de estar disponibles. La dirección de correo para notificar problemas de seguridad o privacidad a Apple se proporciona en la [Ref.- 41].

[4] La relación entre las versiones de macOS y Darwin siguen la fórmula: Versión macOS==10.x → Versión Darwin = (x+4). Así, la versión de macOS Mojave 10.14 corresponde a la versión de Darwin 18.

5. PROCESO DE INSTALACIÓN Y ACTUALIZACIÓN DE MACOS MOJAVE

En este apartado se describe el proceso para llevar el equipo a la última versión disponible de macOS Mojave, tanto para actualizaciones de equipos que dispongan de versiones previas de macOS como para equipos que ya la incorporan de fábrica. El equipo debe cumplir los requisitos de compatibilidad especificados en la documentación oficial de Apple [Ref.- 12].

5.1 ACTUALIZACIÓN DE MACOS

En términos generales, ***se recomienda mantener actualizada la versión de macOS***, ya que cada nueva versión, además de corregir problemas de seguridad detectados en versiones previas, incorpora mejoras y nuevas características que afectan a la seguridad del sistema operativo y del propio equipo. ***Se recomienda realizar una copia de seguridad previa*** (ver apartado "16. Copias de seguridad y restauración").

La versión 10.14 de macOS introduce como una de sus novedades la supresión de las actualizaciones de sistema operativo de la App Store, que pasan a estar disponibles bajo "Preferencias del sistema - Actualizaciones de software". Este cambio permite definir ajustes específicos para las actualizaciones de sistema operativo, en lugar de compartirse los ajustes de actualizaciones de aplicaciones de la App Store.

5.1.1 ACTUALIZACIÓN AUTOMÁTICA

Para equipos que cuenten con una versión de macOS 10.11.5 (El Capitán) o superior, y que tengan habilitada la opción "App Store - Preferencias - Actualización automática" (ver apartado "13.2. App Store"), la descarga de Mojave se iniciará en segundo plano y:

- Descargará el fichero de instalación "Install macOS Mojave" en la carpeta "Aplicaciones".
- El sistema avisará mediante una notificación de la disponibilidad de la actualización para ser instalada.
    - Esta notificación incluye el botón "Instalar", desde el que se puede iniciar la instalación.
    - Para posponer la instalación, se puede rechazar la notificación. Una vez se esté en disposición de iniciarla, deberá abrirse el fichero "Install macOS Mojave".

A pesar de la conveniencia de mantener el equipo actualizado, ***se recomienda realizar la instalación de forma manual,*** una vez se haya comprobado que la nueva versión no incorpora modificaciones o cambios de funcionalidad que afecten a la operativa del usuario, y se haya realizado una copia de seguridad del sistema.

5.1.2 ACTUALIZACIÓN MANUAL

Para actualizar de forma manual el equipo a macOS 10.14, es preciso descargar el instalador de Mojave desde la App Store. Tras completarse la descarga, se abrirá el menú de instalación, que conservará los datos de usuario existentes en el equipo.

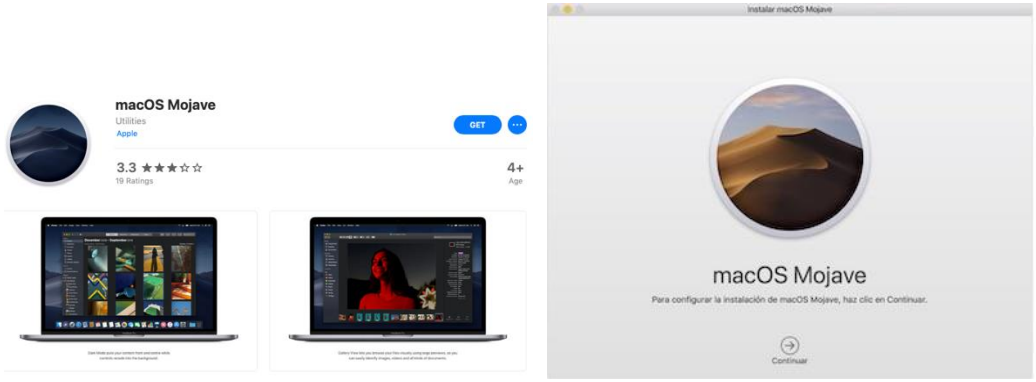


Figura 3 - Descarga de macOS Mojave desde la App Store y menú de instalación

5.1.3 INSTALACIÓN SOBRE UN DISCO VACÍO

Para instalar macOS sobre un disco vacío es preciso iniciar el sistema desde una unidad que cuente con un instalador de arranque (ver apartados "16.3. Creación de un instalador de arranque en una unidad USB o un disco externo" y "18.3. Gestor de arranque").

El proceso de arranque mostrará el menú "Utilidad de discos". A través de la opción "Instalar macOS" - "Continuar" se lanzará la utilidad de instalación de Mojave.

Una vez se muestre el asistente de configuración, se podrá optar por realizar la configuración inicial o salir del asistente mediante "⌘+ Q" (Comando + Q) si no se desea proceder con ella.

5.1.4 ACTUALIZACIÓN DE LA VERSIÓN DE MOJAVE

Las actualizaciones de macOS, además de afectar al sistema operativo, incluyen actualizaciones de otras aplicaciones proporcionadas con el sistema, como iTunes o App Store. Se recomienda mantener el sistema actualizado, especialmente tras la liberación de parches de seguridad que resuelvan vulnerabilidades importantes, previa realización de una copia de seguridad[5].

La actualización puede llevarse a cabo de forma manual (recomendado) o de manera automática, en función del ajuste ' - Preferencias del sistema - Actualización de software".

[5] La [Ref.- 3] proporciona el recurso oficial donde Apple publica las actualizaciones de seguridad disponibles para todos sus productos.

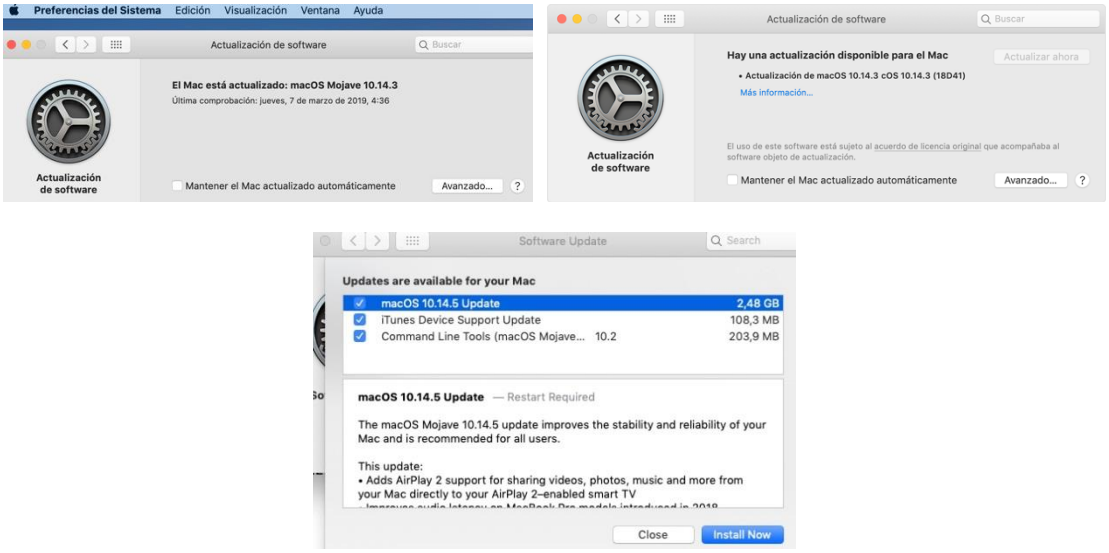


Figura 4 - Detalles sobre la actualización de macOS disponible para el sistema

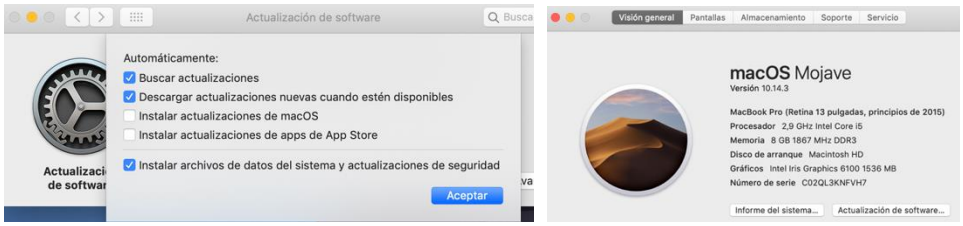


Figura 5 - Ajustes avanzados para controlar la actualización manual o automática de macOS Mojave

macOS realiza la comprobación sobre la existencia de actualizaciones de forma periódica (cada 6 horas, o 21.600 segundos) a través del demonio "`softwareupdated`":

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

Figura 6 - Comprobación de actualizaciones de macOS

La comprobación de actualizaciones se puede activar o desactivar a través del comando "`softwareupdate --schedule on|off`".

La información relativa a la última actualización de macOS aplicada en el sistema se puede obtener mediante el siguiente comando:

```
$ defaults read /Library/Preferences/com.apple.SoftwareUpdate
{
AutomaticCheckEnabled = 0;
AutomaticallyInstallMacOSUpdates = 0;
ConfigDataInstall = 0;
    CriticalUpdateInstall = 0;
    LastAttemptBuildVersion = "10.14.4 (18E226)";
    LastAttemptSystemVersion = "10.14.4 (18E226)";
    LastFullSuccessfulDate = "2019-04-03 11:26:22 +0000";
    LastRecommendedUpdatesAvailable = 0;
    LastResultCode = 2;
    LastSessionSuccessful = 1;
    LastSuccessfulDate = "2019-04-03 11:26:22 +0000";
```

```
    LastUpdatesAvailable = 0;
    PrimaryLanguages =      (
        es,
        "es-ES"
    );
    RecommendedUpdates =    (
    );
    SkipLocalCDN = 0;
}
```

Figura 7 - Parámetros relativos a la última actualización de macOS

El parámetro "`AutomaticallyInstallMacOSUpdates`" representa la configuración relativa a la aplicación de actualizaciones automáticas.

ACTUALIZACIÓN MANUAL

Al acceder al menú "🍎 - Preferencias del sistema - Actualización de software" o "🍎 - Acerca de este Mac - Actualización de software", el equipo iniciará una conexión con los servidores de Apple y, en caso de detectar la disponibilidad de una nueva versión de macOS, ofrecerá la opción "Actualizar ahora". La sección "Más información" presenta más detalles sobre la actualización y sobre otros componentes que se pueden actualizar, que pueden seleccionarse de forma independiente (ver la imagen inferior de la <Figura 4>).

El comando "`softwareupdate -l`" muestra la disponibilidad de nuevas versiones de componentes del sistema. Si no hay actualizaciones se muestra el mensaje "*No new software available*":

```
$ sudo softwareupdate -l
Software Update Tool

Finding available software
Software Update found the following new or updated software:
   * macOS 10.14.5 Update-
     Actualización de macOS 10.14.5 ( ), 2420848K [recommended] [restart]
   * MobileDeviceSU-
     Actualización de Compatibilidad de Dispositivos con iTunes ( ), 105795K
[recommended] [restart]
```

Figura 8 - Comando con la información de actualizaciones de sistema disponibles

Para instalar desde línea de comandos un componente, se dispone de la opción "`softwareupdate --install <componente>`".

ACTUALIZACIÓN AUTOMÁTICA

Cuando la opción "🍎 - Preferencias del sistema - Actualización de software - Mantener el Mac actualizado automáticamente" está activa, el equipo iniciará una conexión periódica con los servidores de Apple y procederá según lo definido en las opciones de la <Figura 5>. ***Se recomienda establecer los siguientes ajustes*** para lograr un mayor control manual sobre las actualizaciones:

- "Buscar actualizaciones": ***activar*** para recibir notificaciones sobre la disponibilidad de nuevas versiones de macOS. Estas notificaciones permiten iniciar la instalación o fijar un recordatorio para el siguiente día.

- "Descargar actualizaciones nuevas cuando estén disponibles": ***desactivar*** para evitar la descarga silenciosa de nuevas versiones de macOS, especialmente si existen restricciones de espacio en disco.
- "Instalar actualizaciones de macOS": ***desactivar***, ya que, en caso contrario, el sistema aplicará las actualizaciones de macOS sin consentimiento explícito del usuario.
- "Instalar actualizaciones de apps de App Store": ***desactivar*** para evitar la instalación automática de actualizaciones de las apps desde la App Store.

NOTA: a lo largo del presente documento se hará un uso indistinto de los términos "apps" (por abreviar) y "aplicaciones" para referenciar a las aplicaciones de software, siguiendo la terminología usada por la propia Apple en algunos de sus menús (como el aquí mencionado), que es similar a la terminología del ecosistema móvil (apps).

- "Instalar archivos de datos del sistema y actualizaciones de seguridad": ***desactivar***, ya que, en caso contrario, el sistema aplicará las actualizaciones de seguridad de macOS sin consentimiento explícito del usuario.

5.2 ACTUALIZACIÓN DE FIRMWARE

La mayoría de las actualizaciones de *firmware* se instalan automáticamente cuando se actualiza el sistema operativo macOS. Sin embargo, en versiones anteriores de macOS, algunas actualizaciones de *firmware* para equipos Mac con procesador Intel también estaban disponibles para su descarga independiente [Ref.- 10], pudiendo ser instaladas manualmente.

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

Mediante la opción "- Acerca de este Mac - [Visión general] - Informe del sistema", es posible acceder a la información del identificador con el modelo del equipo (por ejemplo, "MacBookPro12,1") y a los detalles de la versión del SMC ("Versión SMC (sistema)") y del EFI ("Versión de la ROM de arranque"):

Figura 9 - Informe del sistema

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.

Las actualizaciones de *firmware* y *software* para otros periféricos y dispositivos *hardware* de Apple están disponibles para su descarga desde la página oficial [Ref.-11].

5.3 REINSTALACIÓN DE MACOS

Es posible proceder a la reinstalación de macOS sin perder los datos ni los ajustes del equipo de diversas formas. Previamente es necesario reiniciar el sistema, y, tan pronto se reinicie, elegir la opción adecuada dentro de las siguientes.

5.3.1 A TRAVÉS DE INTERNET

- Instalación de la versión más reciente de macOS compatible con el equipo y disponible en los servidores de Apple: para ello, se pulsará "⌥ + ⌘ + R" (`Opción + Comando + R`) hasta que se muestre un globo giratorio.
- Reinstalación de la versión de macOS instalada en el equipo actualmente con la última actualización de macOS disponible hasta la fecha: se pulsará "⇧ + ⌥ + ⌘+ R" (`Cambio + Opción + Comando + R`) hasta que se muestre un globo giratorio.

5.3.2 DESDE EL DISCO DE RECUPERACIÓN

El menú "Utilidades de macOS" del modo de recuperación (descrito en el apartado "18.2. Modo "Recuperación" (Recovery)") proporciona la opción "Reinstalar macOS", que permite reinstalar el sistema operativo disponiendo de conexión a Internet, cableada o inalámbrica (ya que es posible configurar el acceso a una red Wi-Fi desde el menú "" situado en la parte superior izquierda del citado menú).

La versión que se vuelque en el Mac dependerá de la combinación de teclas empleada para iniciar el modo de recuperación.

La opción "Reinstalar macOS" iniciará el instalador de macOS, y, tras aceptarse las condiciones del contrato de licencia de software y seleccionarse el disco de destino, solicitará la contraseña del usuario administrador existente en el sistema.

El usuario puede optar por haber reformateado previamente el disco (ver apartado "17.1. Borrado del disco de Sistema"), pero este paso no es necesario a menos que el ordenador vaya a cambiar de propietario o exista un problema en la unidad de disco destino que el sistema no pueda reparar.

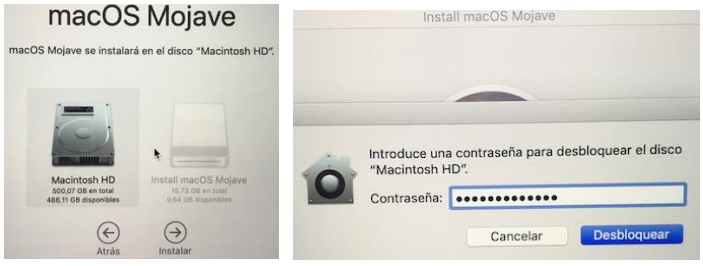


Figura 10 - Reinstalación de macOS: solicitud de la contraseña del administrador

En caso de que el sistema se reinstale sobre la misma unidad destino sin reformateo previo, se conservará el Apple ID existente previamente en el equipo (aunque la sesión estará cerrada mientras no se inicie activamente introduciendo la contraseña asociada). Por este motivo, si se debe a un cambio de propietario, es preciso eliminar primero todos los datos del usuario previo (ver apartado "17.3. Acciones de borrado por cambio de usuario"); en caso contrario, el nuevo propietario podría experimentar problemas para actualizar apps que se proporcionen con la plataforma macOS, al estar esa instalación vinculada al Apple ID del usuario original.

El programa de instalación proseguirá hasta su compleción, por lo que, en el caso de ordenadores portátiles, no debe cerrarse la pantalla para evitar que entre en reposo.

6. PRIMERAS ACCIONES PARA PROTEGER EL ORDENADOR MACOS

Las primeras recomendaciones de seguridad a aplicar una vez finalizada la instalación o configuración inicial de un ordenador con macOS Mojave son:

1. Creación de una cuenta de usuario estándar (sin privilegios) y eliminación de la cuenta "Invitado"(ver apartado "8.1. Usuarios y grupos"). Desde esta nueva cuenta de usuario se aplicarán el resto de recomendaciones de seguridad detalladas en la presente guía.
2. Si el equipo se actualizó a macOS Mojave desde una versión anterior de macOS, comprobar el estado de cifrado del volumen de arranque, así como su formato, que se recomienda sea APFS. Si se está utilizando HFS+, seguir el procedimiento descrito en el apartado "15.5. APFS (Apple File System)". Si el volumen no está cifrado, proceder a cifrarlo según se detalla en el apartado "15. Cifrado del almacenamiento".
3. Proteger el arranque del ordenador mediante una contraseña de *firmware*: ver apartado "18.1. Contraseña de firmware".
4. Desactivar los interfaces de comunicaciones que no se vayan a utilizar: ver apartado "12. Comunicaciones".
5. Establecer las opciones de inicio de sesión y política de contraseñas de los usuarios del sistema: ver apartado "8.1.2. Opciones de inicio de sesión".
6. Revisar los controles de acceso a elementos sensibles del equipo: ver apartado "8.2.4. TCC: Transparency, Consent and Control".
7. Personalizar el escritorio, eliminando componentes no necesarios: ver apartado "8.5. Pantalla de inicio (Home)".
8. Configurar las notificaciones de forma que no se muestre su contenido con la pantalla bloqueada: ver apartado "8.5.3. Centro de Notificaciones".
9. Desinstalar las apps de las que no se vaya a hacer uso.
10. Realizar una copia de seguridad completa del sistema: ver apartado "16. Copias de seguridad y restauración".

7. ACTIVACIÓN DE SERVICIOS Y APLICACIONES EN EL PROCESO DE ARRANQUE DE MACOS

En este apartado se persigue dar una visión general sobre la gestión de los servicios y aplicaciones que estarán disponibles en un ordenador macOS una vez se complete la carga inicial del *kernel* (incluyendo sus extensiones).

El proceso completo de arranque desde que el usuario inicia el equipo está disponible en el anexo "20. Anexo A. Proceso de arranque de macOS". Los puntos abordados en el presente apartado corresponden a los puntos 6, 7 y 8 de dicho anexo.

7.1 DEMONIOS, AGENTES Y SERVICIOS XPC

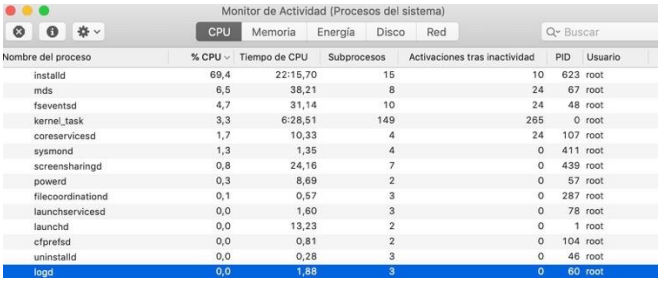
En macOS 10.14, el mecanismo de ejecución de actividades o tareas (*jobs*) durante el proceso de arranque se lleva a cabo por parte del servicio "`launchd`", que es el primer proceso ejecutado por el sistema, y que gestiona los siguientes componentes (consultar [Ref.- 81][Ref.- 82][Ref.- 83] para más información):

- Demonios (*daemons*): son tareas que ejecutan a nivel de sistema, no interactivos, de los cuales hay una única instancia para todos los usuarios. Se lanzan durante el proceso de arranque del sistema por una instancia de "`launchd`" propiedad de *root*, antes de que cualquier usuario inicie sesión. Los ficheros "`.plist`" que definen el arranque de un demonio (ver apartado "7.1.1. Ficheros PLIST de configuración") están disponibles genéricamente bajo:
  - "`/System/Library/LaunchDaemons/`": proporcionados por macOS.
  - "`/Library/LaunchDaemons/`": creados por apps de terceros.
- Agentes (*agents*): son tareas que ejecutan a nivel de usuario cuando éste inicia sesión y suele ser posible interactuar con ellos a través del interfaz gráfico de macOS. Son lanzados por una instancia de "`launchd`" propiedad del usuario. Los ficheros "`.plist`" que definen el arranque de un agente (ver apartado "7.1.1. Ficheros PLIST de configuración") están disponibles genéricamente bajo:
  - "`/System/Library/LaunchAgents/`": agentes de sistema proporcionados por macOS que ejecutan en nombre del usuario que ha iniciado sesión (por ejemplo, el "Dock", "Siri" y "Finder").
  - "`/Library/LaunchAgents`": creados por el administrador o por apps de terceros, y se cargarán para todos los usuarios (por ejemplo, un antivirus o un *firewall* diferente al proporcionado por defecto por macOS).
  - "`~/Library/LaunchAgents`": creados por un usuario concreto.

- Servicios XPC: ejecutan en el contexto de un usuario y proporcionan servicios para una única aplicación. Su principal propósito es dividir una misma aplicación en componentes más pequeños, que se comunican entre sí, de forma que, si un componente falla, la app pueda seguir ejecutando. El servicio XPC fallido será reiniciado por "`launchd`". Los ficheros "`.plist`" que definen el arranque del servicio pueden residir en diversas ubicaciones, en función de la naturaleza del servicio, incluyendo "`/System/Library/CoreServices`", "`/System/Library/Framework`", y otros.

  Los ejecutables correspondientes a los servicios de macOS pueden residir en diversas ubicaciones, entre ellas: "`/sbin`", "`/usr/libexec`", "`/System/Library/PrivateFrameworks`", "`/System/Library/CoreServices`", etc. La ubicación exacta de cada ejecutable se proporciona en el fichero "`.plist`" del servicio al que corresponde.

Es posible consultar información sobre los procesos asociados a demonios, agentes y servicios XPC de sistema mediante la app "Monitor de Actividad" desde su menú "Visualización", filtrando por tipo de proceso (por ejemplo, procesos del sistema):



Nombre del proceso	% CPU	Tiempo de CPU	Subprocesos	Activaciones tras inactividad	PID	Usuario
installd	69,4	22:15,70	15	10	623	root
mds	6,5	38,21	8	24	67	root
fseventsd	4,7	31,14	10	24	48	root
kernel_task	3,3	6:28,51	149	265	0	root
coreservicesd	1,7	10,33	4	24	107	root
sysmond	1,3	1,35	4	0	411	root
screensharingd	0,8	24,16	7	0	439	root
powerd	0,3	8,69	2	0	57	root
filecoordinationd	0,1	0,57	3	0	287	root
launchservicesd	0,0	1,60	3	0	78	root
launchd	0,0	13,23	2	0	1	root
cfprefsd	0,0	0,81	2	0	104	root
uninstalld	0,0	0,28	3	0	46	root
logd	0,0	1,88	3	0	60	root

Figura 11 - Monitor de actividad (procesos del sistema)

NOTA: en versiones antiguas de macOS, los servicios y aplicaciones lanzados durante el proceso de arranque del sistema operativo se denominaban "*Startup Items*" [Ref.- 17], y residían en "`/System/Library/StartupItems`" y "`/Library/StartupItems`". Adicionalmente, y también heredado de los sistemas Unix más antiguos, macOS tiene la capacidad de ejecutar tareas que han sido definidas en el fichero "`/etc/rc.common`" durante el arranque del equipo. Aunque ambos mecanismos son obsoletos, se recomienda verificar el contenido de esos directorios y del fichero "`rc.common`" para confirmar que no existe ningún *Startup Item* indeseado.

NOTA: en versiones anteriores de macOS, existía la capacidad de ejecutar tareas durante el arranque del equipo definidas en el fichero "`/etc/launchd.conf`". Este fichero, según muestra la página "`man`" de "`launchctl`", no está soportado en macOS Mojave.

En adelante, se utilizará la denominación "servicios" (por ejemplo, en el apartado "7.1.3. Impedir el arranque de servicios en macOS") para referenciar el conjunto de demonios, agentes y servicios XPC, tanto de usuario como de sistema, de macOS.

La ejecución de muchos servicios de macOS está vinculada a usuarios especiales existentes en el sistema, que se pueden examinar desde "Preferencias del sistema - Usuarios y grupos - Opciones de inicio - Servidor de cuentas de red - Acceder - Abrir Utilidad de Directorios" (a modo de ejemplo, ver el resto de las entradas de usuarios no recuadradas en color rojo en la utilidad de directorios de la <Figura 44>).

7.1.1 FICHEROS PLIST DE CONFIGURACIÓN DE SERVICIOS

El comportamiento de cada programa (demonio, agente, servicio XPC o aplicación) se define en un fichero XML binario, propietario de Apple, de tipo PLIST (*Property List*) y con extensión ".plist", que alberga los ajustes y parámetros de arranque del servicio en cuestión mediante etiquetas "<key>".

Algunos de los principales elementos (*key*) de estos ficheros ".plist" son:

- Label (etiqueta): el identificador único de la tarea asociada al demonio, agente, o servicio XPC. La nomenclatura de la etiqueta corresponde al nombrado inverso "<dominio>.<fabricante>.<nombre_servicio>" de los servicios en Internet.
- MachServices: indica a "launchd" que debe crear un "Mach port" y registrarlo en el servicio "bootstrap" con el identificador que define esta *key*. Si un cliente de "bootstrap" quiere comunicarse con el servicio, pide a "bootstrap" el identificador, y así obtiene la capacidad de poder enviar mensajes a dicho puerto. Cuando un cliente envía un mensaje al puerto, "launchd" arrancará el servicio y éste procesará el mensaje.
- ProgramArguments (argumentos del programa): parámetros que se pasan al binario o *script* que se ejecuta, incluyendo el nombre del binario.

Existen otras etiquetas opcionales, en función del servicio, entre ellas:

- RunAtLoad: toma valor *true/false*, y especifica si la tarea debe/no debe ejecutarse tan pronto haya sido cargada por "launchd".
- KeepAlive: toma valor *true/false*, y especifica si la tarea debe iniciarse bajo demanda (valor por defecto) o si debe estar siempre en ejecución.
- Disabled: antes de iniciar una tarea asociada a un demonio, agente o servicio XPC, "launchd" comprobará si esta propiedad booleana está presente, o si la tarea ha sido incluida en la denominada "*override database*". Esta base de datos incluye las tareas que han sido deshabilitadas manualmente por el usuario mediante la opción "unload -w" o "disable" del comando "launchctl" (ver apartado "7.1.3. Impedir el arranque de servicios en macOS" para más información sobre este comando).

"launchd" carga todos los servicios, pero solo inicia en el arranque los que incluyan las propiedades "RunAtLoad" o "KeepAlive" con valor *true*.

7.1.2 INTERACCIÓN CON "launchd"

Para interactuar con "launchd" y alterar la ejecución de agentes, demonios y servicios XPC (en adelante "servicios") desde la línea de comandos, se dispone de la utilidad "launchctl" (*launchd control*).

"launchctl" requiere acceso privilegiado como administrador, mediante "sudo", si el objeto de la interacción es un servicio de sistema.

NOTA: la sintaxis de los comandos "launchctl" que incluyen como parámetro "<domain-target>/<uid>/<service-id>" puede resultar confusa, y la página del manual de dicha

utilidad es muy poco descriptiva. Para pasar como parámetro el <uid> del usuario que invoca el comando, se puede utilizar la sintaxis: "`id -u`". Los "<domain-target>" más relevantes son "gui", "system" y "user" [Ref.- 87].

La <Figura 12> muestra algunos ejemplos de uso de este comando.

```
* Comando para ver el estado de inhabilitación de servicios en el dominio
"system":

$ launchctl print-disabled system

disabled services = {
      "com.apple.CSCSupportd" => true
      "com.apple.ftpd" => true
      "at.obdev.littlesnitchd" => false
      "org.ntp.ntpd" => false
}

* Comando para ver los servicios del dominio "gui" para el usuario que lo
invoca (buscar la sección "services"):

$ launchctl print gui/`id -u` | more

services = {
                        0      0         com.apple.syncdefaultsd
                      368      -         com.apple.assistantd
                        0      0         com.apple.DataDetectorsLocalSources
                        0      0         com.apple.unmountassistant.useragent
                        0      -         com.apple.tiswitcher
                        0      -         com.apple.SafariHistoryServiceAgent
                        0      0
com.apple.preference.displays.MirrorDisplays
                        0      -         com.apple.contacts.donation-agent
                      370      -         com.apple.corespeechd
                        0      -         com.apple.java.InstallOnDemand
                        0      -         com.apple.ServicesUIAgent
                        0      -         com.apple.progressd
                    37250      -         com.apple.fileprovider.fileproviderd
                    22653      -         com.apple.Notes.5220
                    …
}

* Tareas iniciadas por "launchd" (incluyen el PID del proceso asociado, lo
que facilita su identificación mediante el comando "ps -ef"). La salida del
comando dependerá del UID (identificador de usuario) que lo invoca:

$ launchctl list
…
PID     Status  Label
263     0       com.apple.Finder
329     0       com.apple.homed
…

$ ps -ef | grep 263
  502   263     1   0 Fri09AM ??         5:49.53
/System/Library/CoreServices/Finder.app/Contents/MacOS/Finder


* Servicios deshabilitados en el dominio "gui" para el usuario que invoca el
comando:

$ launchctl print-disabled gui/`id -u`
disabled services = {
      "at.obdev.LittleSnitchHelper" => false
      "com.apple.ManagedClientAgent.enrollagent" => true
```

```
      "com.apple.DeviceSupportUpdater" => false
      "com.apple.Siri.agent" => true
      "at.obdev.LittleSnitchUIAgent" => false
      "com.apple.FileStatsAgent" => true
      "com.hp.productresearch" => true
      "com.apple.FolderActionsDispatcher" => true
      "com.hp.devicemonitor" => true
      "com.apple.appleseed.seedusaged.postinstall" => true
      "org.gpgtools.Libmacgpg.xpc" => false
      "com.apple.ScriptMenuApp" => true
}
login item associations = {
}

* Inhabilitación del servicio "com.apple.commerce" en el dominio "gui" por
parte del usuario que lo invoca:

$ launchctl disable user/`id -u`/com.apple.commerce

$ launchctl print-disabled user/`id -u`
disabled services = {
      "at.obdev.LittleSnitchHelper" => false
      "com.apple.commerce" => true
       …
}
```

Figura 12 - Ejemplos de uso de la utilidad "launchctl"

```
* Carga un agente de usuario:

$ launchctl load ~/Library/LaunchAgents/<agent>.plist

* Arranque de un agente de usuario ya cargado (no necesario si incluye
RunAtLoad o KeepAlive a true):

$ launchctl start ~/Library/LaunchAgents/<agent>.plist
```

Figura 13 - Comandos "launchctl" para la interacción con agentes de usuario

El comando "`launchctl`" puede utilizarse dentro de un fichero PLIST para invocar acciones, por ejemplo, establecer el valor de una variable de entorno mediante:

```
…
<string>launchctl setenv PATH /usr/local/bin:/usr/bin:/bin:/usr/sbin:/sbin</string>
…
```

Figura 14 - Uso de "launchctl" dentro de un fichero PLIST

Se recomienda analizar el contenido de los ficheros PLIST ***para identificar posibles invocaciones no deseadas de*** "`launchctl`". Adicionalmente, en la [Ref.- 102] se proporciona una técnica basada en las notificaciones "*Folder Actions*" de AppleScript para monitorizar el contenido de las carpetas "`~/Library/LaunchAgents`" y "`/Library/LaunchDaemons`" y que se lance una alerta si se detectan cambios.

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

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 macOS y genera una alerta cuando se añaden nuevos elementos a las mismas, permitiendo incluso que el usuario tome acciones al respecto.

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

7.1.3 IMPEDIR EL ARRANQUE DE SERVICIOS EN MACOS

Con la introducción de SIP en macOS se impide la modificación de ficheros del sistema por parte de cualquier usuario (incluido *root*), lo cual afecta a todos los demonios y agentes de sistema (que residen en "`/System`"). Por este motivo, si se desea deshabilitar cualquier servicio de sistema gestionado por "`launchd`", es preciso en primer lugar desactivar SIP (ver apartado "9.10. SIP: System Integrity Protection").

Desde el punto de vista de seguridad, ***se recomienda inhabilitar todos los servicios que no se utilicen***, con lo que se evitará que vulnerabilidades asociadas a ellos sean potencialmente explotables.

SERVICIOS DE SISTEMA

Para excluir servicios del sistema durante el proceso de arranque, macOS dispone de un fichero en el que definen los servicios que no deben ser lanzados por "`launchd`", ubicado en "`/System/Library/Sandbox/com.apple.xpc.launchd.rootless.plist`".

Para añadir un servicio a esta lista de exclusión, basta con editar el fichero e incluir una entrada para él con este formato:

```
<key>servicio</key>
<true></true>
```

Donde "`servicio`" corresponde al parámetro "`Label`" de su fichero "`.plist`".

Por tanto, el procedimiento para excluir un servicio de sistema durante el proceso de arranque de macOS es:

1. Reiniciar en modo de recuperación y deshabilitar SIP (ver apartado "9.10. SIP: System Integrity Protection").
2. Añadir una entrada para el servicio en el fichero de configuración "`/System/Library/Sandbox/com.apple.xpc.launchd.rootless.plist`".
3. Descargar el fichero "`.plist`" del servicio mediante "`launchctl unload -w`".
4. Reiniciar en modo de recuperación y volver a habilitar SIP.

A continuación se proporciona un ejemplo para inhabilitar el arranque del demonio "`CrashReporterSupportHelper`":

```
* Servicio a deshabilitar:
/System/Library/CoreServices/CrashReporterSupportHelper server-init

* Fichero PLIST asociado:
/System/Library/LaunchDaemons/com.apple.CrashReporterSupportHelper.plist

* Sección "Label":
 <key>Label</key>
        <string>com.apple.CrashReporterSupportHelper</string>
```

```
* Entrada a añadir a la lista de exclusión definida en el fichero
"/System/Library/Sandbox/com.apple.xpc.launchd.rootless.plist":
<key>com.apple.CrashReporterSupportHelper</key>
<true></true>

* Descarga del fichero PLIST asociado mediante "lauchctl":
$ sudo launchctl unload -w /System/Library/LaunchDaemons/
com.apple.CrashReporterSupportHelper.plist
```

Figura 15 - Inhabilitación del arranque del demonio "CrashReporterSupportHelper"

SERVICIOS DE USUARIO

Para inhabilitar un agente de usuario, es suficiente con ejecutar el siguiente comando (ver NOTAS a continuación):

```
$ launchctl unload -w <PATH>/<servicio>.plist
```

Figura 16 - Inhabilitación de un agente de usuario

NOTA: La opción "-w" solo se precisa si se quiere inhabilitar el arranque del agente de forma permanente.

NOTA: Si el agente a deshabilitar pertenece a la categoría de agentes de sistema que ejecutan en nombre del usuario (los residentes en "/System/Library/LaunchAgents"), es preciso inhabilitar SIP previamente. Para que la inhabilitación afecte a un usuario concreto, debe lanzarse desde una sesión de ese usuario, sin privilegios de administrador.

Una vez ejecutado el comando, macOS añadirá el servicio a la correspondiente "*override database*", una base de datos en la que se listan los agentes que "`launchd`" no debe iniciar. Las bases de datos "*override*" se encuentran en el directorio "`/var/db/com.apple.xpc.launchd/`". macOS implementa una lista "`disabled.<user_id>`" por cada usuario del sistema, una para los agentes de terceros (que aplica a todos los usuarios) y una para los "*login items*" de cada usuario:

```
$ cat /var/db/com.apple.xpc.launchd/disabled.`id -u`.plist
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>com.apple.TMHelperAgent.SetupOffer</key>
        <false/>
        <key>com.apple.ManagedClientAgent.enrollagent</key>
        <true/>
        <key>com.apple.Siri.agent</key>
        <true/>
        <key>com.apple.FolderActionsDispatcher</key>
        <true/>
        <key>com.apple.appleseed.seedusaged.postinstall</key>
        <true/>
        <key>com.apple.ScriptMenuApp</key>
        <true/>
</dict>
</plist>
```

Figura 17 - Contenido de una "override database" de un usuario

7.2 EJECUCIÓN DE APLICACIONES EN EL INICIO Y EL FIN DE SESIÓN

En macOS, los elementos o ítems de arranque (*login items*) son aplicaciones que serán ejecutadas durante el proceso de inicio de sesión de un usuario determinado, y se definen en la pestaña "Ítems de inicio" del menú "Preferencias del Sistema - Usuarios y grupos - <Usuario>", mostrándose los correspondientes al usuario actual. La opción "+" permite añadir nuevos elementos, desplegando por defecto la carpeta "Utilidades". La casilla "Ocultar" permite determinar si la app correspondiente será o no visible en el inicio de sesión:

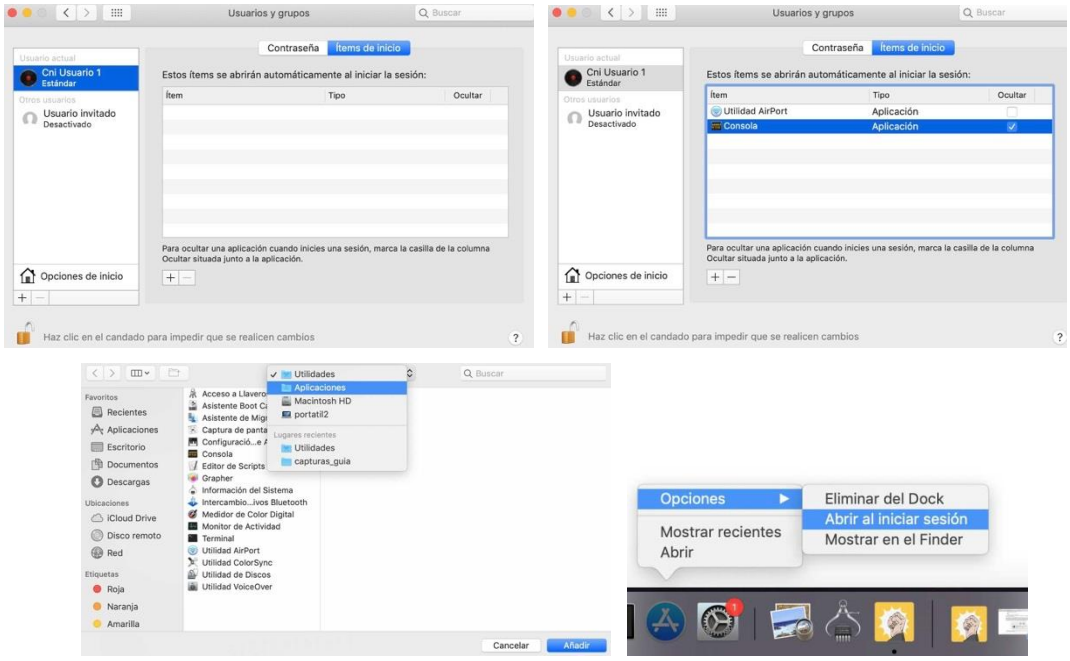


Figura 18 - Menú "Usuarios y grupos - Ítems de inicio"

También es posible añadir añadir ítems de inicio directamente desde el "Dock", pulsando con el botón derecho sobre el icono de la app deseada y seleccionando "Opciones - Abrir al iniciar sesión" (ver imagen inferior derecha de la <Figura 18>).

Las aplicaciones disponibles en la lista son almacenadas en el fichero PLIST:

"`~/Library/Application Support/com.apple.backgroundtaskmanagementagent/backgrounditems.btm`"

Este fichero, particular para cada usuario, contiene objetos referenciados por UUID, por lo que no es fácilmente editable directamente; no obstante, es posible añadir ítems de inicio mediante un lenguaje de *scripting* (por ejemplo, AppleScript)[6].

NOTA: en versiones anteriores hasta macOS 10.12 Sierra, los ítems de inicio se incluían en el fichero de configuración "`~/Library/Preferences/com.apple.loginitems.plist`" del usuario. Los datos contenidos en este fichero (`<data>…</data>`) estaban codificados en base64.

6 https://eclecticlight.co/2018/05/22/running-at-startup-when-to-use-a-login-item-or-a-launchagent-launchdaemon/

Se recomienda verificar para cada usuario, y especialmente para los usuarios administradores, ***la lista de ítems de inicio definidos***, y permitir únicamente la ejecución de aquellos de los que se realmente sean necesarios. La <Figura 19> incluye un script creado con la app "Editor de Scripts" (proporcionada por defecto con macOS) que muestra los ítems de inicio del usuario que lo ejecuta:

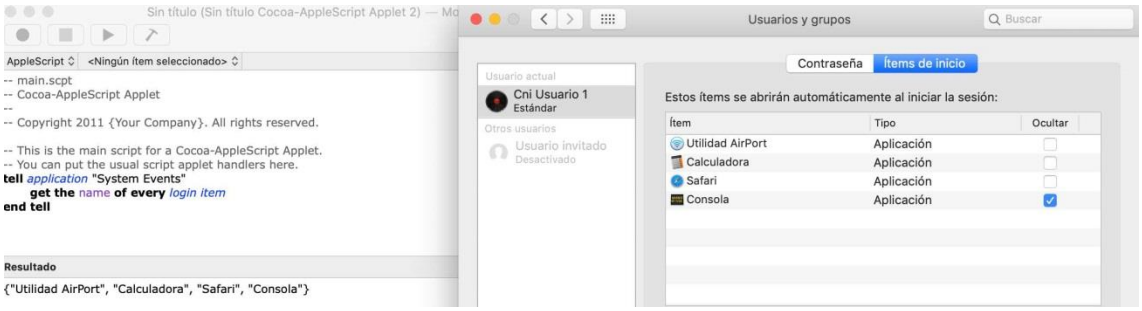


Figura 19 - Script para mostrar los ítems de inicio de un usuario desde la app "Editor de Scripts"

Adicionalmente, la utilidad "`osascript`" permite ejecutar desde línea de comandos sentencias AppleScript:

```
* Lista de ítems de inicio del usuario:

$ osascript -e 'tell app "System Events" to get the name of every login
item'
Utilidad AirPort, Calculadora, Safari, Consola

* Adición de un ítem de inicio sin usar modo oculto:

$ osascript -e 'tell application "System Events" to make login item at end
with properties {path:"/Applications/TextEdit.app", hidden:false}'

$ osascript -e 'tell app "System Events" to get the name of every login
item'
TextEdit, Utilidad AirPort, Calculadora, Safari, Consola

* Borrado de un ítem de inicio:

$ osascript -e 'tell application "System Events" to delete login item
"TextEdit"'

$ osascript -e 'tell app "System Events" to get the name of every login
item'
Utilidad AirPort, Calculadora, Safari, Consola
```

Figura 20 - Comandos "osascript" para gestionar ítems de inicio de un usuario

NOTA: los lenguajes de *scripting* de macOS quedan fuera del alcance de la presente guía. Si se desea profundizar en la utilización de AppleScript, existen diversos recursos en Internet, como por ejemplo los incluidos en la [Ref.- 15].

NOTA: debido al modelo de permisos de macOS Mojave (ver apartado "8.2.4. TCC: Transparency, Consent and Control"), más restrictivo que versiones anteriores de macOS, el comando "`osascript`" puede fallar para ciertos recursos si se ejecuta como usuario administrador. En ese caso, típicamente se obtendrá el error "`44:48: execution error: Se ha producido un error de tipo -610. (-610)`", que se resolverá añadiendo el fichero "`/usr/bin/osascript`" a la categoría "Seguridad y privacidad - Acceso total al disco".

7.2.1 LOGIN & LOGOUT HOOKS

Los denominados "*login/logout hooks*" son scripts que el usuario configura para que se ejecuten cuando inicie/cierre sesión respectivamente [Ref.- 16]. Sin embargo, a diferencia de los ítems de inicio, los *hooks* ejecutan como "*root*", por lo que ***su uso está desaconsejado desde el punto de vista de seguridad***. En su lugar, se recomienda utilizar ítems de inicio o agentes de usuario "*user agents*" (a través de "`launchd`").

7.3 EJECUCIÓN DE TAREAS PROGRAMADAS EN MACOS

En macOS es posible programar la ejecución de tareas en un momento temporal concreto a través de "`launchd`" y de "`cron`", siendo el primero de estos el método oficial a fecha de elaboración de la presente guía [Ref.- 18].

La planificación de tareas mediante "`launchd`" se lleva a cabo a través del fichero de configuración de los correspondientes demonios o agentes de usuario, incluyendo en el mismo la directiva "`StartCalendarInterval`" seguida del intervalo en el que debe ser ejecutado. Si el equipo se encuentra en modo suspendido cuando se alcance el intervalo definido para una tarea, "`launchd`" la ejecutará cuando salga de ese estado y se active. Si está apagado, no se ejecutará hasta el siguiente momento temporal planificado en el que el equipo esté encendido.

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`". A diferencia de lo que sucede con las tareas definidas mediante "`StartCalendarInterval`" de "`launchd`", las tareas de "`cron`" que deberían ejecutarse en un período en el que el equipo está suspendido no se ejecutarán cuando el equipo se active.

Para identificar agentes de usuario creados por el administrador que dispongan de acciones programadas actualmente, se recomienda ejecutar el comando:

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

Figura 21 - Comando para identificar agentes de usuario con acciones planificadas

Para revisar las tareas actualmente programadas a través de "`cron`" por cada uno de los usuarios existentes en el sistema, se recomienda invocar el siguiente comando como administrador (sudo):

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

Figura 22 - Comando para listar las tareas planificadas mediante "cron" para todos los usuarios

Con la introducción de los mecanismos de control de acceso de Mojave (ver apartado "8.2.4. TCC: Transparency, Consent and Control"), es posible que las tareas de "`cron`" que funcionaban en versiones anteriores de macOS fallen por no poder acceder a determinados directorios. Si, a pesar de estar desaconsejado desde el punto de vista

de seguridad, fuese necesario ejecutar ese tipo de tareas de "`cron`", se añadirá el binario "`/usr/sbin/cron`" a la categoría "Seguridad y privacidad - Acceso total al disco".

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. Por defecto, en macOS solo existe el fichero "`/usr/lib/cron/cron.deny`", que únicamente contiene al usuario invitado (Guest).

8. PREFERENCIAS DEL SISTEMA

El menú "Preferencias del sistema", accesible desde el icono '' o desde la app "Preferencias del sistema" proporciona acceso a los diversos parámetros de configuración de macOS, que se dividen en una serie de categorías, desde las cuales el usuario puede realizar cambios de ajustes.

Algunos de estos cambios pueden requerir privilegios de administrador por lo que, si el menú "Preferencias del sistema" se lanza desde una sesión asociada a un usuario sin este privilegio, se mostrará el símbolo de un candado cerrado '' en el margen inferior izquierdo de la pantalla que, al ser pulsado, solicitará las credenciales de un usuario administrador, y pasará a estar abierto y permitir la realización de cambios en los ajustes de configuración.

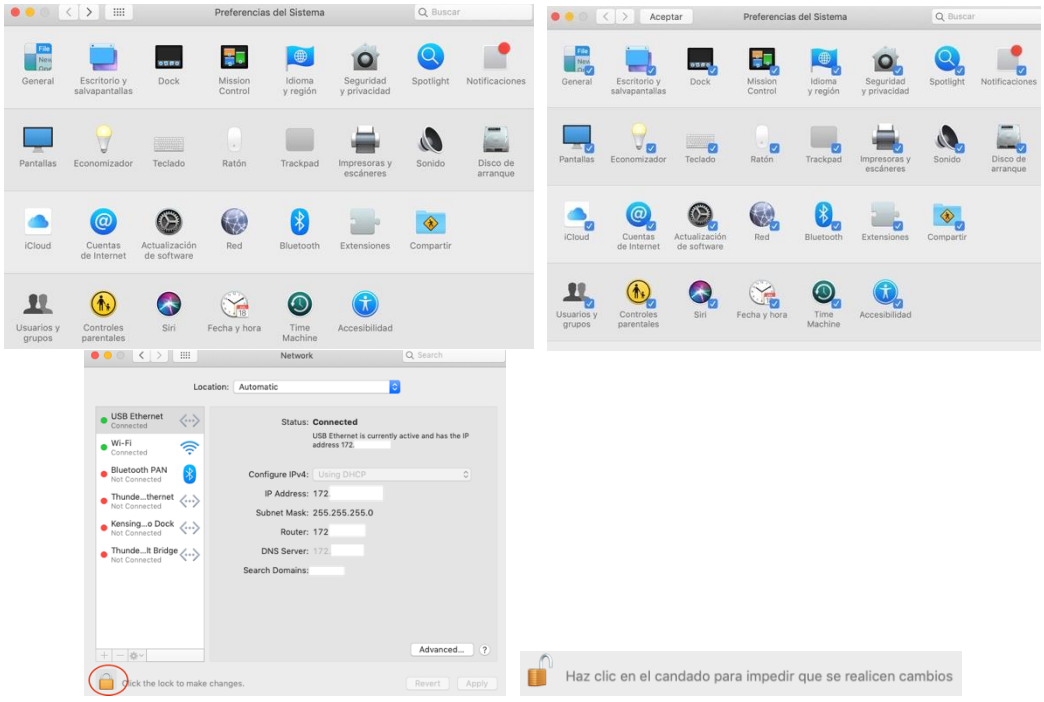


Figura 23 - Menú "Preferencias del sistema"

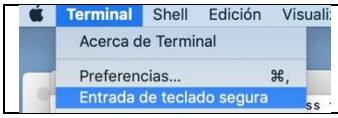
Se recomienda volver a pulsar en el candado una vez finalizados los cambios de los ajustes objetivo, a fin de evitar que se puedan modificar ajustes involuntariamente.

A través del menú "🍎 - Acerca de este Mac - [Visión general] Informe del sistema - Software - Paneles de preferencias" es posible obtener información de los componentes que forman parte del menú "Preferencias del sistema", incluida su versión, su visibilidad en el panel y si ha sido incluido por una app de Apple o de terceros.

Es posible suprimir secciones del menú "Preferencias del sistema" abriendo esta app, seleccionando en su barra superior "Visualización - Personalizar" y desmarcando aquellos elementos que no se desea que estén accesibles. Esta personalización no requiere de privilegios de administración, pero puede ser interesante tenerla en cuenta para suprimir secciones que no se desea que estén visibles para usuarios no experimentados de macOS.

A lo largo del presente apartado se describirán las secciones del menú "Preferencias del sistema" que tienen relación con la seguridad y/o la privacidad del equipo y/o del usuario, quedando excluidas las secciones que únicamente albergan elementos de personalización sin relevancia para dichos aspectos.

Adicionalmente, es posible utilizar la app "Terminal" para hacer uso de la línea de comandos y realizar consultas y modificaciones en los ajustes. ***Se recomienda activar la opción*** "Entrada de teclado segura" **de la app "Terminal", tal como muestra la siguiente imagen, *para evitar que otras apps tengan acceso a la información y comandos tecleados en el terminal***. Para verificar el valor de este parámetro, se puede ejecutar también el siguiente comando:




```
$ defaults read -app Terminal SecureKeyboardEntry
1
```

Figura 24 - "Entrada de teclado segura" de la app "Terminal"

8.1 USUARIOS Y GRUPOS

Los ajustes relativos a perfiles y cuentas de usuario están accesibles desde la sección "Usuarios y grupos", que incluye acceso al "directorio de servicios" proporcionado por defecto en macOS (ver apartado "8.1.6. Directorio de Servicios"). Existen 4 tipos de perfiles de usuario en macOS [Ref.- 91]:

- **Administrador**: es un usuario con acceso privilegiado (ver apartado "8.1.1. Acceso privilegiado"). Este perfil se asigna por defecto al usuario que configura el sistema por primera vez.
- **Estándar**: no dispone de capacidades para modificar ajustes de sistema ni de otros usuarios, pero sí los propios. También puede instalar apps.
- Sometido a **controles parentales**: ver apartado "9.12. Controles parentales".
- **Invitado (Guest)**: este perfil existe por defecto en macOS, y permite acceder al sistema sin introducir ninguna contraseña. Los contenidos de su directorio de inicio se borran cuando se cierra la sesión.

- "**Solo compartir**": este perfil permite compartir el contenido de las carpetas de denominación "Pública" existentes en el equipo con cualquier individuo que disponga de acceso a él a través de la red. Estas cuentas se crean, por ejemplo, cuando un usuario añade a un contacto (desde la funcionalidad descrita en el apartado "8.1.5. Compartición de ficheros") con el que desea compartir ficheros. Este perfil no puede iniciar sesión en el sistema (su *shell* es "`/usr/bin/false`").

Se recomienda crear una cuenta de usuario estándar o no privilegiada inmediatamente tras completar el proceso de instalación y configuración inicial de macOS, desde la que se realizará el resto de tareas de configuración. 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, salvo cuando alguna de esas tareas precise de acceso privilegiado (ver apartado "8.1.1. Acceso privilegiado"), para lo que será necesario introducir las credenciales del usuario administrador (pero no abrir sesión como él).

Para suprimir el acceso como administrador para un usuario que tiene este privilegio, se debe desmarcar la opción "Permitir al usuario administrar este ordenador" desde el panel con todos los detalles del perfil de usuario en "Usuarios y grupos".

Desde el menú "+" se accede al interfaz de creación de un usuario; macOS solicitará mediante un cuadro de diálogo las credenciales de un usuario administrador con privilegios suficientes para poder realizar dichos cambios.

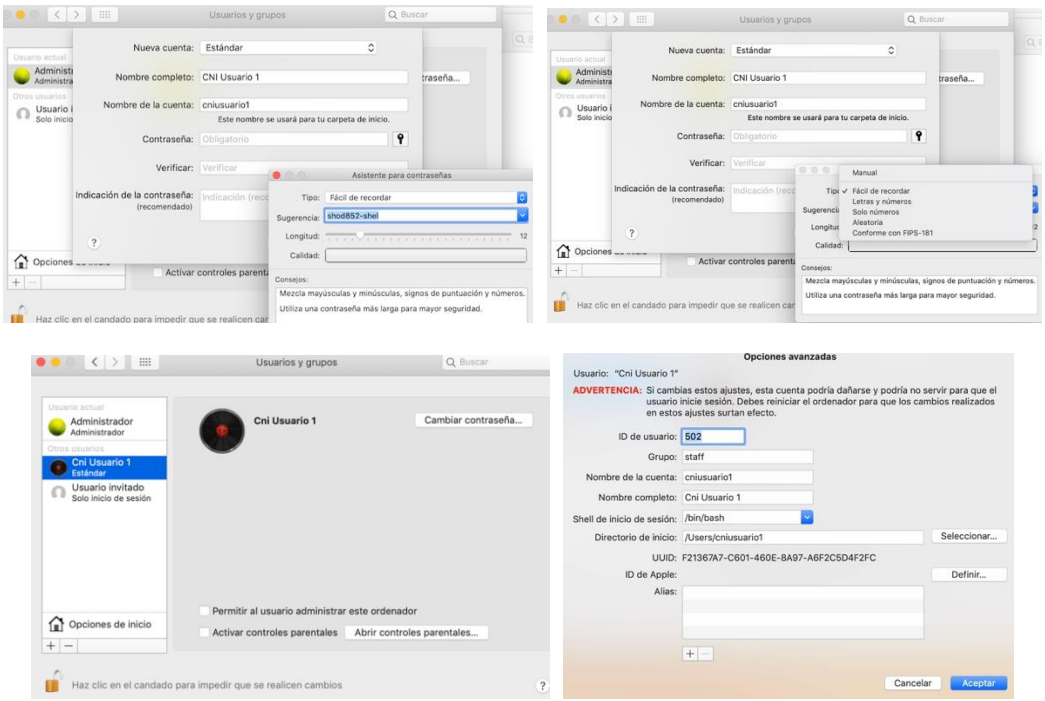


Figura 25 - Creación de un usuario estándar en macOS

Durante el proceso de creación de la cuenta de usuario, ***se recomienda***:

- ***Forzar la utilización de contraseñas robustas***, requiriendo al menos 16 caracteres entre letras y números con intención de hacer uso de frases de paso, mediante la utilidad "`pwpolicy`", que permite definir políticas para las contraseñas de usuario, por ejemplo, su composición y complejidad (letras, números, símbolos, etc.), su longitud mínima, y el número máximo de intentos de acceso fallidos tras el cual la cuenta de usuario será bloqueada. Se recomienda consultar la página "`man`" asociada a esta utilidad para evaluar las diferentes opciones.
  Durante el proceso de creación de un usuario y la configuración de su contraseña de acceso, si existen políticas de contraseñas definidas mediante "`pwpolicy`", se mostrará una ventana (ver <Figura 26>) en la que se marcarán con puntos verdes los criterios que, hasta ese momento, cumple la contraseña introducida, y en gris los que aún no. El usuario no se creará en el sistema mientras su contraseña no cumpla todos los criterios.
- ***Desactivar la opción*** "Indicación de contraseña", que proporcionaría una pista a un potencial atacante que quisiera autenticarse de forma ilegítima o no autorizada con las credenciales del usuario.

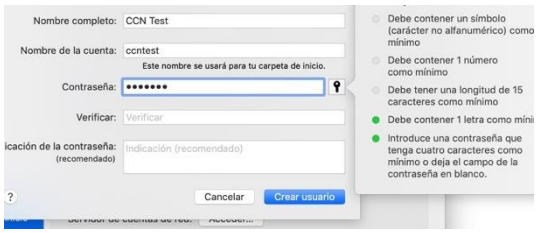


Figura 26 - Creación de contraseña de un usuario nuevo

- ***Evitar reutilizar la contraseña de acceso al sistema como contraseña del ID de Apple*** (ver apartado "11. Servicios de Apple"), a fin de independizar ambos accesos y que el eventual compromiso de una contraseña no afecte a la otra.

Adicionalmente, se recomienda ***desactivar el usuario invitado (Guest)***; en caso de puntual necesidad por la que se requiera utilizarlo, se aconseja deshabilitarlo tan pronto finalice dicha necesidad. Para inhabilitar el acceso de invitado, se desmarcará la opción "Permitir a los invitados conectarse a este ordenador":

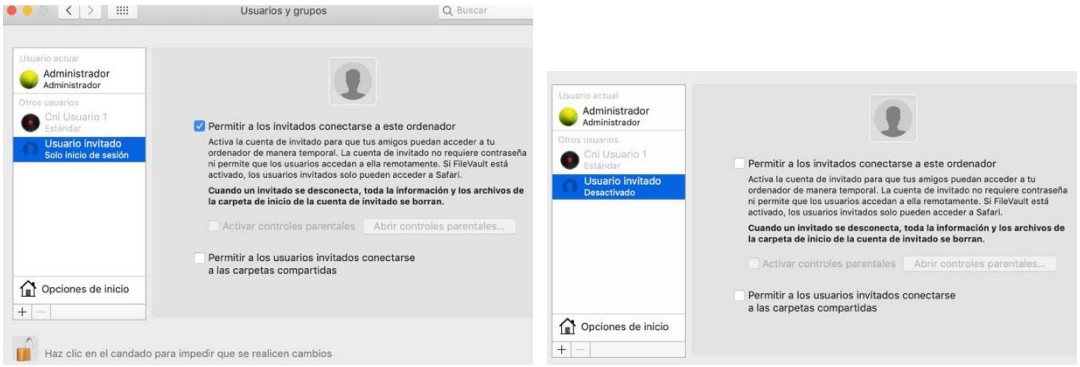


Figura 27 - Desactivación de la cuenta de usuario invitado

Si FileVault está deshabilitado (opción totalmente desaconsejada según se describe en el apartado "15.1. FileVault"), se dispone adicionalmente de opción "Permitir restablecer la contraseña con el Apple ID" (consultar la sección "Restablecer el ID de Apple" de la [Ref.- 19]) para poder recuperar una contraseña olvidada. ***Se recomienda determinar si esta opción debe estar disponible para los usuarios***, ya que, en caso de compromiso de su Apple ID, un tercero podría cambiar la contraseña de sistema operativo del usuario en el equipo Mac.

Por defecto, el directorio principal o *home* de un nuevo usuario estándar se crea bajo "`/Users/<nombre_usuario>`", y el grupo asignado es "`staff`" (gid=20). Seleccionando con el botón derecho un usuario, se presenta el menú "Opciones avanzadas", desde el cual es posible cambiar estos parámetros de bajo nivel del sistema operativo, incluso el "ID de Apple" asociado a la cuenta (se asigna el uid=502 al segundo usuario estándar que se ha recomendado crear, empleándose el uid=501 para el primer usuario administrador empleado en la configuración inicial de macOS).

Alternativamente, se dispone de la utilidad "`sysadminctl`", que permite gestionar las cuentas de usuario desde un terminal, incluyendo su creación, borrado, o modificación, o incluso para el restablecimiento de la contraseña.

La utilidad "`dscacheutil -q user`" permite obtener información sobre todos los usuarios (estándar, administradores y de sistema) disponibles. Con la opción "`-a name <nombre_usuario>`" se restringe la salida al usuario designado:

```
$ dscacheutil -q user -a name admin
name: admin
password: ********
uid: 501
gid: 20
dir: /var/admin
shell: /bin/bash
gecos: Administrador
```

Figura 28 - Comando "dscacheutil" para obtener información de un usuario

Es posible cambiar el nombre de un usuario existente en el sistema siguiendo el procedimiento documentado en la [Ref.- 130].

Algunas funciones relacionadas con la accesibilidad suelen exponer más la información del equipo desde el punto de vista de seguridad, por lo que se recomienda no habilitarlas salvo que la condición del usuario lo requiera. ***Se debe intentar evitar el uso del servicio*** "VoiceOver", ***particularmente en la pantalla de bloqueo***, asegurándose de que la opción "Usuarios y grupos - Opciones de inicio - Opciones de accesibilidad... - VoiceOver" está desactivada.

8.1.1 ACCESO PRIVILEGIADO

Desde el punto de vista de seguridad, ***se aconseja la utilización del equipo macOS con un perfil de usuario "normal" o estándar, reservando el acceso de administrador únicamente a aquellas tareas que lo exijan***.

Desde la interfaz gráfica, cuando se inicie una acción que requiera permiso de administrador, macOS solicitará al usuario (mediante un cuadro de diálogo) las

credenciales de un usuario administrador antes de conceder los privilegios requeridos para llevar a cabo los cambios indicados.

Desde línea de comandos, para el acceso a operaciones que requieran de privilegios de superusuario es necesario hacer uso del comando "sudo" (Super User DO), que implementa una política de seguridad basada en controles de acceso sobre los comandos disponibles para cada tipo de usuario[7]. La política de seguridad por defecto en macOS es "sudoers", configurable mediante el fichero "/etc/sudoers", que se puede editar a través del comando "visudo". Cuando un usuario invoca un comando precedido de "sudo", el sistema solicitará que introduzca su propia contraseña (la asociada a su usuario estándar, vinculada a su UID, o *userid*, real) y:

- Si la contraseña es correcta, consultará la política de seguridad para ver si el usuario dispone de permisos de "sudo" para ejecutar el comando:
  - En caso afirmativo, el comando se lanzará con el *userid* del usuario efectivo (el especificado con la opción "-u <usuario>" del comando "sudo", o, si no se especificó esta opción, como superusuario). Por defecto, el comando "sudo" almacena en caché las credenciales del usuario que lo invoca durante 5 minutos, por lo que los comandos lanzados en ese período no requerirán la reintroducción de la contraseña. Este comportamiento se puede alterar a través del parámetro "timestamp_timeout" del fichero "/etc/sudoers". Desde el punto de vista de seguridad, se recomienda fijar este parámetro al intervalo más reducido posible. Un valor de "0" provocará que las credenciales nunca sean cacheadas y sea necesario introducirlas en cada invocación.
  - En caso negativo, informará del error por pantalla. Por defecto, en macOS sólo los usuarios administradores están incluidos en el fichero "/etc/sudoers" y, por tanto, sólo estos pueden ejecutar comandos de superusuario mediante "sudo" (tal como se detalla a continuación):

```
$ sudo who
Password:
cniusuario1 is not in the sudoers file.  This incident will be
reported.
```

Figura 29 - Error del comando "sudo" invocado por un usuario sin permisos de "sudo"

- Si la contraseña no es correcta, permitirá dos intentos más para introducirla antes de abortar su ejecución.

Para realizar acciones que requieran acceso privilegiado desde una *shell*, ***se aconseja lanzar un terminal desde una cuenta de usuario estándar, ejecutar el comando*** "su - <usuario_admin>" ***para obtener acceso como usuario administrador***, y proceder a invocar el comando que requiera permisos de superusuario precedido de "sudo". Tan pronto finalice la operación, ***se recomienda cerrar la sesión de administrador*** (abierta mediante el comando "su" previo).

[7] El comando "sudo" no está restringido a la invocación de comandos únicamente como superusuario (o administrador), sino que puede utilizarse para ejecutar comandos como cualquier otro usuario del sistema con la opción "-u <usuario>".

Por defecto, macOS otorga por defecto permisos de administración al usuario `root` y a cualquier usuario del grupo `admin`:

```
# root and users in group wheel can run anything on any machine as any user
root            ALL = (ALL) ALL
%admin          ALL = (ALL) ALL
```

Figura 30 - Fichero "/etc/sudoers", editable con "visudo"

En macOS, el grupo "`admin`" tiene asignado el gid=80; para ver los grupos a los que pertenece cualquier usuario, se dispone del comando "`id <usuario>`".

8.1.2 OPCIONES DE INICIO DE SESIÓN

Desde "Preferencias del Sistema - Usuarios y grupos - Opciones de inicio" es posible configurar diferentes aspectos de seguridad asociados al inicio de sesión por parte de los usuarios en macOS (estos ajustes son globales para todos ellos, no únicamente para la cuenta del usuario que tiene la sesión activa en el equipo). Desde el punto de vista de seguridad, ***se recomienda:***

- ***Desactivar*** "Inicio de sesión automático": en caso contrario, sería posible iniciar sesión en macOS automáticamente con el usuario indicado al arrancar el equipo sin conocer su contraseña. Las opciones para este ajuste se ven afectadas por:
  - Si el disco del ordenador está cifrado con FileVault (opción por defecto en Mojave y recomendada desde el punto de vista de seguridad), la opción "Inicio de sesión automático" no podrá habilitarse (ver apartado "15.1. FileVault").
  - La casilla "Seguridad y privacidad - General - Desactivar el inicio de sesión automático": corresponde al mismo ajuste del punto anterior (disponible únicamente si FileVault está deshabilitado).

  Si se habilita el "Inicio de sesión automático" (***desaconsejado***), la contraseña del llavero de inicio de sesión del usuario seleccionado es cifrada mediante XOR[8] y almacenada en el fichero "`/etc/kcpassword`", accesible por `root`. Mediante el siguiente comando, cualquier usuario administrador podría extraer la contraseña del llavero del usuario asociado al inicio de sesión automático:

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

Figura 31 - Descifrar la contraseña del usuario asociado al "Inicio de sesión automático"

Importante: en la versión de macOS 10.14.4 empleada en la elaboración de la presente guía, el fichero "`/etc/kcpassword`" no se elimina cuando se desactiva el inicio de sesión automático, por lo que, en caso de que esta opción haya sido habilitada en algún momento, se recomienda proceder a eliminarlo manualmente mediante el comando "`sudo rm /etc/kcpassword`".

[8] La clave empleada para este cifrado XOR (mostrada en la figura) no ha cambiado desde la versión 10.4 de macOS.

- ***Desactivar*** "Mostrar menú cambio rápido usuario como", que provoca que en la barra superior de estado se muestre un campo con el nombre del usuario activo y que, al pincharse, despliega la lista de usuarios disponibles en el sistema, lo cual podría utilizarse por parte de un potencial atacante, que conocería el nombre del usuario activo (y del resto de usuarios si tiene acceso a la lista). Si se desea hacer uso de esta funcionalidad, se recomienda que el valor de la opción sea "icono" (por defecto, la opción seleccionada es "nombre completo").

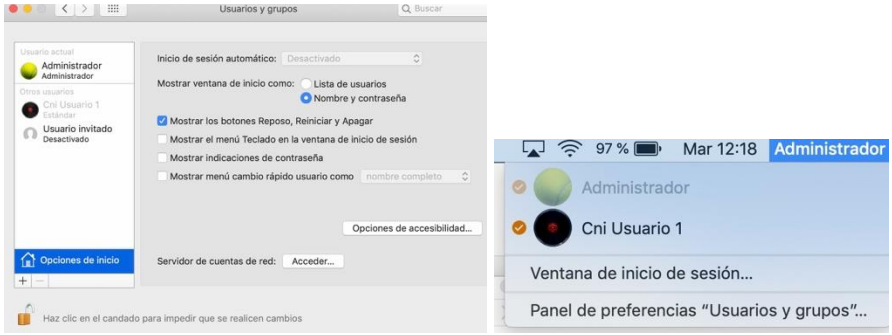


Figura 32 - Opciones de inicio de sesión. Menú "Cambio rápido de usuario"

- ***Desactivar*** "Mostrar indicaciones de contraseña", a fin de no proporcionar pistas sobre credenciales a usuarios no autorizados.
- ***Desactivar*** "Mostrar los botones Reposo, Reiniciar y Apagar" para evitar que un tercero pueda llevar estas acciones en el equipo desde la pantalla de login sin conocer las credenciales de un usuario legítimo. Si no se desea ocultar las tres opciones en su conjunto, se puede optar por hacerlo selectivamente a través de las propiedades:

```
$ sudo defaults write /Library/Preferences/com.apple.loginwindow
ShutDownDisabled -bool true

$ sudo defaults write /Library/Preferences/com.apple.loginwindow
RestartDisabled -bool true

$ sudo defaults write /Library/Preferences/com.apple.loginwindow
SleepDisabled -bool true
```

Figura 33 - Ocultación selectiva de los botones "Apagar", "Reiniciar" y "Suspender" ("Reposo")

- ***Activar*** "Mostrar el menú Teclado en la ventana de inicio de sesión", 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 solo 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 macOS **no** es necesario tenerlos definidos en la sección "Preferencias del Sistema - Teclado - Fuentes de entrada".

Figura 34 - Menú Teclado en la pantalla de login

- ***Fijar el valor de*** "Mostrar ventana de inicio como:" a "Nombre y contraseña", para impedir ofrecer a un potencial atacante la lista de usuarios existentes (junto a sus imágenes o iconos) en la pantalla de login de macOS.

Figura 35 - Ventanas de login según las opciones definidas en "Mostrar ventana de inicio como:"

En el caso de querer hacer uso de la opción "Lista de usuarios", ***se recomienda al menos ocultar las cuentas de usuario con permisos de administrador*** de esta lista mediante el siguiente comando "`dscl`", o mediante la creación de un atributo "IsHidden" en la sección asociada al usuario del interfaz "Utilidad de Directorios - Editor de directorios" (ver apartado "8.1.6. Directorio de Servicios"). Para esos usuarios, la ventana de login será la situada en tercera y cuarta posición se la <Figura 35>:

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

Figura 36 - Eliminación de usuarios de la lista de usuarios de la ventana de login

Esta opción aplica al escenario de cierre de sesión por parte de un usuario: si se recurre a la opción "Bloquear pantalla", el sistema mostrará el nombre del usuario que la ha bloqueado. Si se reinicia el sistema, se mostrará la lista de usuarios que tienen acceso a desbloquear el disco cifrado con FileVault.

En caso de haber ocultado la cuenta de usuario mediante el atributo "IsHidden", ésta también desaparece de la sección "Preferencias del Sistema - Usuarios y grupos - Otros usuarios", pudiendo confirmarse que existe el usuario al intentar crear otra cuenta de usuario con el mismo nombre o a través del comando:

```
$ dscl . list /Users
…
admin
cniusuario1
daemon
Guest
nobody
root
```

Figura 37 - Lista de usuarios del sistema

Es posible revertir la ocultación de usuarios fijando el valor "IsHidden" a 0.

UTILIZACIÓN DE TARJETAS INTELIGENTES COMO MÉTODO DE INICIO DE SESIÓN

macOS soporta, desde la versión 10.12 (Sierra) la utilización de tarjetas inteligentes (*smart-card*) como segundo factor de autentificación. Adicionalmente,

desde macOS 10.13 (High Sierra), se soporta su uso como medio de autenticación exclusivo.

macOS Mojave incluye soporte nativo para *smart-cards* en tres ámbitos:

- Autentificación:
  - Para el inicio de sesión en macOS: en este caso, la tarjeta inteligente debe incluir un certificado de autorización y, si se desea poder utilizarla para desbloquear el llavero, también una clave de cifrado (conocida como KMK, *Key Management Key*), empleada para envolver la clave del llavero y evitar que el sistema la solicite permanentemente (ver apartado "9.7. Gestión de llaveros" para más información sobre el uso del llavero).
  - En sitios web, para autentificar al usuario a través de certificados digitales cliente desde el navegador web Safari.
  - Como segundo factor de autentificación (2FA).
  - Autentificación mediante Kerberos, basada en pares de claves (PKINIT), para los servicios que lo admiten.
- Firma digital y cifrado: si la tarjeta almacena el certificado digital asociado a la dirección de correo del remitente de la app Mail, se mostrará el botón de firma en la barra de menú de composición del mensaje.
- Carga útil en entornos de gestión empresarial (*smart-card payload*) [Ref.- 60]: para definir parámetros específicos asociados a las tarjetas inteligentes, por ejemplo, si se permite su uso para el inicio de sesión en macOS.

El uso de tarjetas inteligentes o *smart-cards* está recomendado desde el punto de vista de seguridad, aunque su proceso de configuración queda fuera del ámbito de la presente guía. Si se desea obtener más información, se recomienda consultar las referencias [Ref.- 25] (genérica) y [Ref.- 26] (particular de las *smart-cards* YubiKey).

OCULTACIÓN DEL DIRECTORIO "HOME" DE UN USUARIO

En ocasiones puede ser preciso ocultar una cuenta de usuario para evitar que otros usuarios puedan conocer su existencia, como en el caso en que un usuario administrador ha de acceder a un equipo ajeno para solucionar un problema técnico. Para ello, además de realizar los pasos descritos en la <Figura 36>, se recomienda ocultar el directorio de inicio y la carpeta pública compartida siguiendo la [Ref.- 7]. Es importante indicar que, por defecto, en macOS Mojave no es posible ejecutar ciertos comandos, como "`mv`" y "`rm`" desde una ventana de terminal para algunos ficheros y/o directorios. Si se requiere ejecutarlos, hay que conceder a la app "Terminal" el permiso "Acceso total al disco" (ver apartado "8.2.4. TCC: Transparency, Consent and Control").

Se aconseja la lectura del apartado "8.2. Seguridad y privacidad" para consultar otras recomendaciones asociadas a las cuentas de usuario existentes en el sistema.

8.1.3 RECUPERACIÓN DE UNA CONTRASEÑA OLVIDADA

Ante una situación de olvido de contraseña por parte de un usuario, la [Ref.- 19] proporciona diversos métodos disponibles para intentar su restablecimiento.

CONTRASEÑA MAESTRA

Durante el proceso de activación de *FileVault* (ver apartado "15.1. FileVault"), es posible decidir entre utilizar la cuenta de usuario de iCloud (Apple ID) para restablecer la contraseña de cifrado del disco o crear una clave de recuperación que permita desbloquearlo en caso de olvido de la contraseña de acceso.

Figura 38 - Selección del método de desbloqueo del disco con FileVault

Para modificar la clave de cifrado del disco de arranque, es preciso desactivar FileVault y volverlo a activar [Ref.- 9].

RESETEO DE LA CONTRASEÑA DE USUARIO POR PARTE DEL ADMINISTRADOR

Si un usuario olvida su contraseña y FileVault está habilitado (opción recomendada desde el punto de vista de seguridad), y el método de "Contraseña maestra" ha resultado exitoso, será preciso iniciar sesión como usuario administrador y utilizar la opción "Cambiar contraseña…" del menú "Usuarios y grupos". La nueva contraseña definida mediante este método se trasladará el mecanismo de FileVault como clave de cifrado derivada (*Derived Encryption Key* o DEK), de forma que el usuario pueda descifrar el disco con su contraseña (ver apartado "15.1. FileVault").

8.1.4 GESTIÓN DE GRUPOS

macOS implementa la funcionalidad de grupos de usuarios, principalmente orientada al establecimiento de controles de acceso a archivos y carpetas.

La creación de grupos se gestiona a través de la opción "+", seleccionando "Grupo" en el campo "Nueva cuenta". Los miembros que se pueden añadir a un grupo pueden ser tanto usuarios individuales como otros grupos existentes en el sistema.

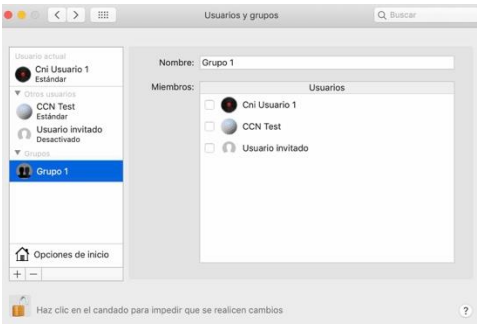


Figura 39 - Creación de grupos en macOS

La pertenencia de un usuario a un grupo en macOS puede provenir de[9]:

- Pertenencia directa (atributo "`PrimaryGroupID`").
- Presencia del usuario en el atributo "`GroupMembership`" del grupo.
- UID del usuario presente en la lista del atributo "`GroupMembers`" del grupo.
- Herencia de la pertenencia al grupo a través de relaciones anidadas (un grupo puede estar compuesto de usuarios o de otros grupos, por lo que los miembros del grupo "hijo" son también miembros del grupo padre).
- Pertenencia determinada por el sistema operativo.

En macOS, el grupo "`admin`" tiene asignado el guid=80; para ver los grupos a los que pertenece un usuario, se dispone del comando "`id <usuario>`".

En la <Figura 40> se ilustran algunos comandos útiles para obtener información sobre los grupos existentes en el sistema operativo y los usuarios pertenecientes a determinados grupos. Es importante destacar que las utilidades "`dscl`" y "`dscacheutil`" proporcionan información parcial de pertenencia, fundamentalmente la directa, no la obtenida por herencia (tampoco informan de la pertenencia que todos los usuarios de macOS tienen al grupo "`staff`"). El script de Perl publicado en el foro superuser.com[9] sí permite obtener la información completa de usuarios y grupos:

```
* Grupos existentes en el sistema:

$ dscl . list /groups

* Miembros del grupo "Grupo1":

$ dscacheutil -q group -a name Grupo1
name: Grupo1
password: *
gid: 504
users: ccntest

$ dscl . -read /Groups/Grupo1
...
GroupMembers:  DE3727E8-0231-4279-8937-9D982FFE1AA9
GroupMembership: ccntest
Password: *
PrimaryGroupID: 504
RealName:
 Grupo 1
RecordName: Grupo1
RecordType: dsRecTypeStandard:Group
```

[9] https://superuser.com/questions/279891/list-all-members-of-a-group-mac-os-x/395738#395738

```
* Grupos a los que pertenece el usuario "ccntest":

$ id -nG ccntest
staff everyone localaccounts Grupo1 com.apple.sharepoint.group.1
com.apple.sharepoint.group.2 com.apple.sharepoint.group.3 _lpoperator
com.apple.sharepoint.group.4

* Nombres de usuarios que son miembros del grupo "admin":

$ dscacheutil -q group -a name admin | grep -e '^users:' | sed 's/users: //'
root admin
```

Figura 40 - Comandos para consultar información sobre los grupos existentes en macOS

GRUPO "EVERYONE"

macOS dispone de un grupo especial, denominado "everyone", ligado a la funcionalidad de compartición de ficheros que se describe a continuación. Este grupo representa tanto a la totalidad de los usuarios que tienen cuenta en el sistema operativo, como a cualquier usuario de la red.

8.1.5 COMPARTICIÓN DE FICHEROS

macOS permite a los usuarios de un equipo compartir sus archivos con [Ref.- 90]:

- Usuarios que se conectan a través de la red (sin necesidad de iniciar sesión local): ver apartado "10.1. Servicios compartidos".
- Otros usuarios del equipo (que pueden iniciar sesión en él): requiere modificar los permisos de aquellos archivos propiedad del usuario que se quieran compartir. Para ello, desde la app Finder, se debe seleccionar la carpeta o archivo a compartir y seleccionar la opción "Obtener información" mediante el botón derecho. Se desplegará el menú de la <Figura 41>, que ofrece el *flag* "Carpeta compartida" y en cuya parte inferior se encuentra la sección "Compartir y permisos" (se requerirá introducir las credenciales de administración en caso de habilitar este flag si el servicio de compartición de archivos no estaba aún habilitado, y se desea habilitar en ese momento, ver apartado "10.1. Servicios compartidos", o en caso de intentar compartir archivos o carpetas que no sean propiedad del usuario, mediante el candado cerrado situado en la parte inferior derecha; ver la <Figura 41>):
  - A través de la opción "+" es posible añadir usuarios y/o grupos que tendrán acceso al elemento que se comparte.
  - La opción "-" permite suprimir usuarios y grupos con los que no se desea seguir compartiendo un elemento. Es importante reseñar que el grupo "Everyone" no puede eliminarse mediante este método, pero sí es posible ***establecer para él el privilegio*** "Sin acceso" (desde la parte derecha de la tabla, sección "Privilegios"), lo cual ***se recomienda***; de ser necesario proporcionar acceso al grupo "Everyone" por cualquier circunstancia, ***se debería restablecer el privilegio a*** "Sin acceso" ***tan pronto sea posible***.
  - Pinchando con el botón izquierdo sobre cualquier entrada de la sección "Privilegios" se puede modificar el tipo de acceso permitido.

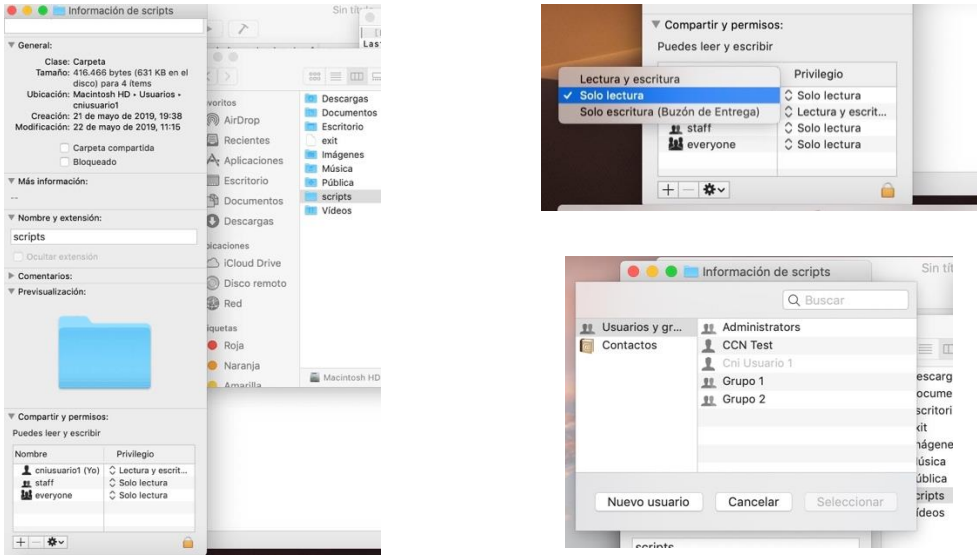
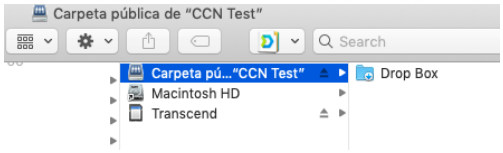


Figura 41 - Menú de compartición de carpetas y archivos

Desde el punto de vista de seguridad, ***se recomienda restringir el tipo de acceso al mínimo imprescindible***. En función de las necesidades, la opción recomendable será "Solo leer" (para impedir que otro usuario o grupo pueda modificar el contenido del elemento) o "Solo escribir (Buzón de Entrega)", que impide que los usuarios con los que se comparte puedan ver el resto de contenidos de la carpeta (lógicamente, este privilegio no está disponible para archivos).

Si se usa el método de compartición "Buzón de Entrega", se creará una carpeta "`Drop Box`" (que no debe confundirse con el servicio *Dropbox*) dentro de la carpeta "Pública" del usuario que comparte: "`/Users/<usuario>/Public/Drop Box`".




```
$ ls -ld /users/ccntest/Public/Drop\ Box/

drwx-wx-wx+ 3 ccntest  staff  96 Jun 26
15:14 /users/ccntest/Public/Drop Box/
```

Figura 42 - Carpeta Drop Box para compartición de tipo "Solo escritura"

macOS crea carpeta "Pública" en el directorio *home* de todos los usuarios del sistema operativo. Esta carpeta "Pública" está compartida por defecto y permite acceso de lectura a cualquier usuario del sistema (*everyone*), pero también a cualquier usuario de la red si el servicio "Compartir archivos" está habilitado (opción desaconsejada desde el punto de vista de seguridad; ver apartado "10.1. Servicios compartidos"). Por tanto, esta carpeta debe utilizarse con extrema precaución. Es importante además reseñar que las operaciones de "arrastrar y soltar" (*drag and drop*) de archivos sobre esta carpeta implican una operación de tipo "*move*" (mover).

La opción "Contactos", disponible a la hora de elegir con qué usuarios se compartirá el elemento seleccionado, permitirá elegir un contacto de la lista de contactos del usuario, para el cual se creará (previa introducción de las credenciales de administrador) una cuenta de usuario especial en el sistema operativo con el perfil "Solo compartir".

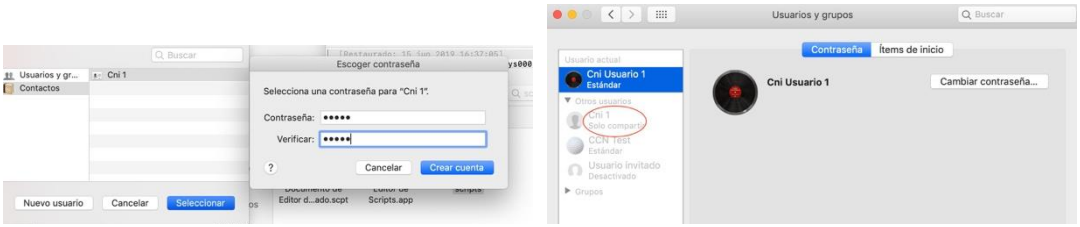


Figura 43 - Creación de una cuenta "Solo compartir"

Se recomienda revisar periódicamente los elementos compartidos, y suprimir los permisos de aquéllos que ya no deben estar accesibles para terceros.

8.1.6 DIRECTORIO DE SERVICIOS

La gestión avanzada de usuarios se puede realizar desde el submenú "Preferencias del Sistema - Usuarios y grupos - Opciones de inicio - [Servidor de cuentas de red] - Acceder - Abrir Utilidad de Directorios". Desde la parte superior del interfaz de usuario de la "Utilidad de Directorios" se dispone del botón "Editor de directorios" para su configuración.

NOTA: la descripción exhaustiva de la arquitectura y funcionamiento del directorio de servicios de Apple queda fuera del alcance de la presente guía.

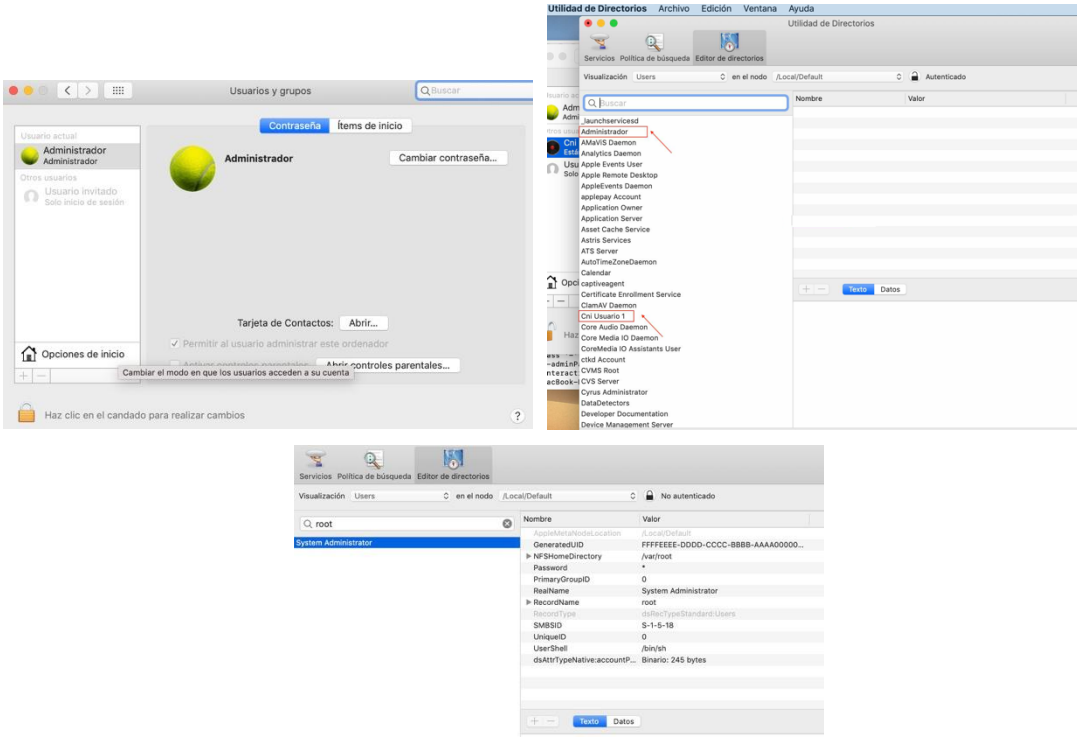


Figura 44 - Menú "Usuarios y grupos", opciones de inicio y gestión del directorio de servicios

Desde este menú ("Visualización - Users - Buscando por el usuario 'root' ") se puede constatar que, por defecto, la cuenta de usuario "`root`" se encuentra deshabilitada en macOS 10.14, al tener el campo "`password *`". ***Se recomienda mantener la cuenta de*** "Administrador de Sistema" ***o root inhabilitada.***

La utilidad "`dscl`" (ver página "`man`") permite gestionar el directorio de servicios desde línea de comandos.

8.2 SEGURIDAD Y PRIVACIDAD

Esta sección, disponible desde "Preferencias del Sistema - Seguridad y privacidad", alberga cuatro subsecciones, cada una de las cuales se describe en los siguientes subapartados.

8.2.1 GENERAL

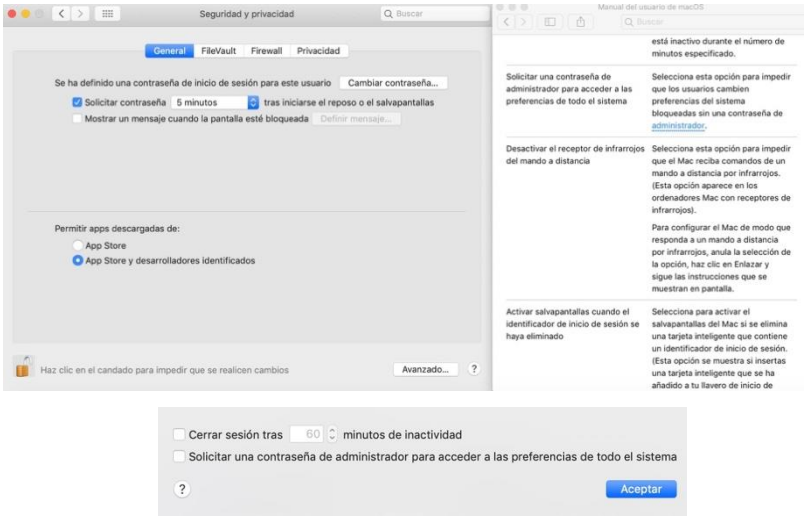


Figura 45 - Seguridad y privacidad (General)

Se recomienda establecer los siguientes ajustes en la sección "Seguridad y privacidad - General":

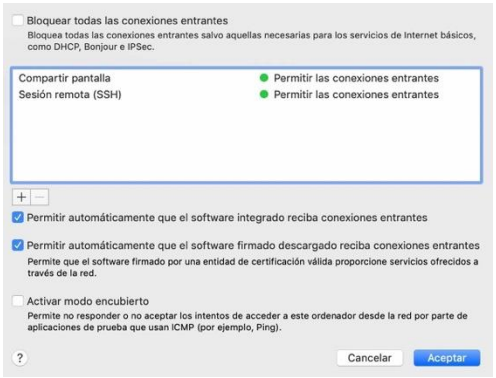
- ***Activar*** "Mostrar un mensaje cuando la pantalla esté bloqueada": permite personalizar un texto, que aparecerá en la parte inferior central de la pantalla de inicio de sesión de macOS; el contenido puede ser, por ejemplo, un texto legal o de autorización de acceso al equipo asociado al propietario u organización.
  El mensaje será añadido como atributo "`LoginwindowText`" en el fichero de preferencias "`com.apple.loginwindow.plist`", que se puede consultar a través del comando: "`defaults read /Library/Preferences/com.apple.loginwindow.plist`".
  Si se desea establecer una política de acceso que el usuario deba aceptar antes de iniciar sesión, consultar la [Ref.- 8].
- ***Activar*** "Solicitar contraseña tras iniciarse el reposo o el salvapantallas": se recomienda establecer un valor de compromiso entre la usabilidad y la seguridad, que dependerá de las políticas de seguridad de la organización; de manera general, se recomienda fijar un valor de 5 minutos.
- "Avanzado...": a través de este botón, disponible en la parte inferior derecha, es posible:

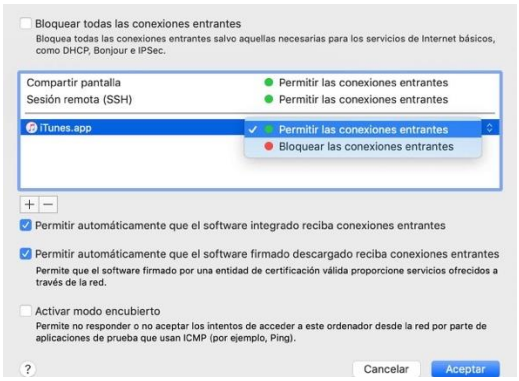
- ***Activar*** "Cerrar sesión tras NN minutos de inactividad": se recomienda establecer un límite adecuado a las políticas de seguridad de la organización, superado el cual macOS cerrará una sesión que ha estado inactiva durante el periodo definido.
- ***Activar*** "Solicitar una contraseña de administrador para acceder a las preferencias de todo el sistema": en macOS 10.14 Mojave se constata que el comportamiento es idéntico esté o no esta opción activa, exigiéndose introducir credenciales de un usuario administrador para realizar cambios en ajustes considerados "críticos". Este comportamiento también se ha constatado en todas las versiones de macOS desde Yosemite 10.10. Pese a ello, se aconseja tener la opción activa por si alguna futura actualización modificara este comportamiento.

NOTA: En la versión de Mojave utilizada en la elaboración de la presente guía (10.14.4 y 10.14.5), se ha comprobado que, si se pincha en el candado para modificar un ajuste de una sección de "Preferencias del Sistema" y se introduce correctamente la contraseña de administrador, durante un breve espacio de tiempo es posible salir de esa sección, volver a entrar a ella, y proceder a realizar modificaciones sin que sea necesario acreditarse de nuevo como administrador, ya que el candado permanece desbloqueado durante cierto tiempo.

8.2.2 FIREWALL (CORTAFUEGOS)

macOS dispone de un cortafuegos personal (o *firewall*), también denominado *Application Layer Firewall* (ALF) o *Application Firewall*, que permite bloquear las conexiones y el tráfico entrante hacia el equipo a nivel de aplicación (en vez de a nivel de puertos) [Ref.- 85]. Su activación y configuración (que deben realizarse como usuario administrador) se encuentran disponibles en la pestaña "Seguridad y privacidad - Firewall".





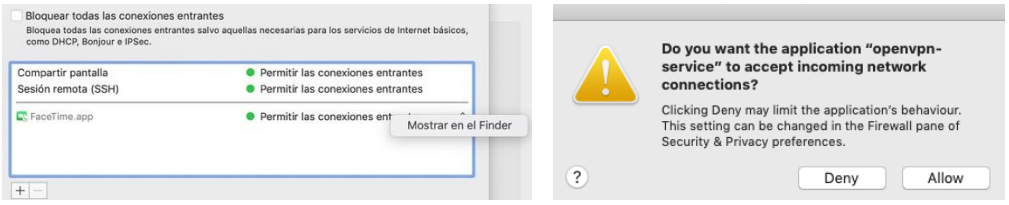


Figura 46 - Opciones de configuración del cortafuegos (AFL) de macOS

En la configuración inicial de macOS el cortafuegos está desactivado por defecto. Sin embargo, con el objetivo de proteger el equipo, ***se recomienda activarlo y configurar de manera restrictiva las capacidades de filtrado existentes***. Previamente deberán analizarse los puertos requeridos por el sistema y las apps instaladas, de forma que no se bloqueen conexiones necesarias. La información relativa a los puertos TCP y UDP utilizados por el propio macOS está disponible en la [Ref.- 108].

El estado de activación del cortafuegos se puede también consultar mediante:

```
$ defaults get /Library/Preferences/com.apple.alf globalstate
0
```

Figura 47 - Comprobación del estado de activación del cortafuegos (AFL) en macOS

El ALF de macOS solo filtra a nivel del trafico entrante (conexiones establecidas hacia el equipo). Se recomienda añadir algún *software de firewall* con capacidades para filtrar el establecimiento de conexiones salientes (originadas desde el equipo).

La configuración del cortafuegos se realiza a nivel de sistema (con privilegios de administración), por lo que se aplica a todos los usuarios del equipo.

La configuración avanzada (accesible desde "Opciones de firewall…") permite por omisión las conexiones entrantes de las apps firmadas (todo el *software* de Apple, las aplicaciones obtenidas de la App Store y las apps de desarrolladores que firmen sus apps con un *developer ID* legítimo obtenido de Apple), mediante la opción "Permitir automáticamente que el software firmado descargado reciba conexiones entrantes", e igualmente mediante "Permitir automáticamente que el software integrado reciba conexiones entrantes". Para las apps que no estén firmadas, el servicio *Gatekeeper* (ver apartado "9.2. Gatekeeper y cuarentena de archivos") actuará del siguiente modo:

- Cuando se inicia la conexión desde la app no firmada que aún no está en la lista de apps del cortafuegos, el sistema abrirá una ventana solicitando "Permitir" o "Denegar" sus conexiones:
  - Si se selecciona "Permitir", macOS firmará la app y la añadirá a la lista de apps permitidas del cortafuegos[10].
  - Si se selecciona "Denegar", macOS bloqueará todas las conexiones entrantes hacia esta app.

Desde el punto de vista de seguridad, ***se recomienda:***

[10] Según Apple, la excepción a este comportamiento son las apps que no están firmadas por el desarrollador pero que validan su propia integridad al iniciar su ejecución. En este caso, macOS mostrará el cuadro de diálogo para permitir/denegar sus conexiones cada vez que se abra la app [Ref.- 85].

- ***Seleccionar 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* o *address subnet mask* están deshabilitados en todos los casos). Aun con esta opción activa, el equipo seguirá aceptando conexiones hacia las aplicaciones autorizadas (según la configuración de las opciones previas).
- ***Activar la opción*** "Bloquear todas las conexiones entrantes", con el objetivo de no desvelar la presencia del equipo en la red, siempre que no se haga uso de servicios que las requieran. Al activar esta opción, el cortafuegos bloqueará todos los servicios compartidos (ver apartado "10.1. Servicios compartidos"), por lo que será necesario desactivarla cuando se precise hacer uso momentáneamente de alguno de ellos, y, posteriormente, volverla a habilitar. Se constata que, con esta opción activa:
  - Todos los puertos TCP están cerrados, y el sistema se comporta descartando todos los paquetes TCP entrantes:

```
Nmap scan report for 192.168.1.100
Host is up, received user-set.
All 65536 scanned ports on 192.168.1.100 are filtered because
of 65536 no-responses

Nmap done: 1 IP address (1 host up) scanned in 13267.44 seconds
```

Figura 48 - Puertos TCP cerrados con el cortafuegos (AFL) habilitado

  - Sigue estando accesible desde el exterior el puerto UDP/5353 (*Bonjour*, *zeroconf* o *mDNS*) y UDP/137 (resolución de nombres, *Name Service*, de NetBIOS), junto a UDP/88 (Kerberos) y UDP/138 (NetBIOS):

```
88/udp   open|filtered kerberos-sec no-response
137/udp  open          netbios-ns   udp-response ttl 63
138/udp  open|filtered netbios-dgm  no-response
5353/udp open          zeroconf     udp-response ttl 254
```

Figura 49 - Puertos UDP abiertos con el cortafuegos (AFL) habilitado

IMPORTANTE: las conexiones que estén activas en el momento de activar esta opción no se finalizarán. Por ejemplo, si se está compartiendo pantalla desde otro equipo, la compartición se mantendrá activa hasta que finalice la sesión.

- En caso de requerirse utilizar de manera regular algún servicio o aplicación que admita conexiones entrantes, ***configurar la lista de admisión/exclusión***. Esta lista se configura desmarcando la opción "Bloquear todas las conexiones entrantes" y, pinchando sobre el símbolo "+", lo que abrirá una instancia de Finder que permitirá añadir el fichero binario correspondiente a la aplicación. Desde esta ventana es posible pulsar sobre el icono '⇕' de cualquier app y modificar su condición de app con conexiones permitidas o bloqueadas.
  Cuando el filtrado se lleva a cabo mediante este mecanismo, se comprueba que el puerto TCP asociado a Kerberos (TCP/88) se pone a la escucha, aunque el usuario no haya definido ninguna app específica para este servicio.

```
PORT      STATE SERVICE       REASON
22/tcp    open  ssh           syn-ack ttl 63
88/tcp    open  kerberos-sec  syn-ack ttl 63
5900/tcp  open  vnc           syn-ack ttl 63
```

Figura 50 - Puertos TCP abiertos con conexiones entrantes SSH y "Compartir pantalla" permitidas

Para eliminar una app de la lista y que el sistema vuelva a solicitar al usuario permisos cuando se inicien conexiones hacia ella, se puede eliminar la app seleccionándola y pinchando sobre el botón "-". Si se pulsa sobre la entrada de una app con el botón derecho, aparecerá el menú "Mostrar en Finder", que abrirá una instancia de Finder con la ruta exacta al binario de la app. Esto puede permitir comprobar de forma efectiva su autenticidad.

macOS implementa el servicio de cortafuegos (AFL) en base a:

- Un demonio de sistema, que reside bajo "`/System/Library/LaunchDaemons/com.apple.alf.agent.plist`", y cuyo fichero de configuración actual es "`/Library/Preferences/com.apple.alf.plist`" (el fichero que incluye los ajustes por defecto del cortafuegos AFL es "`/usr/libexec/ApplicationFirewall/com.apple.alf.plist`"). Este demonio de sistema invoca al binario "`/usr/libexec/ApplicationFirewall/socketfilterfw`".
- Un agente de sistema residente en "`/System/Library/LaunchAgents/com.apple.alf.useragent.plist`", que invoca al binario "`/usr/libexec/ApplicationFirewall/Firewall`".

El fichero de configuración principal del cortafuegos (AFL) "`/Library/Preferences/com.apple.alf.plist`" se puede consultar mediante el comando:

```
$ plutil -convert xml1 -o - /Library/Preferences/com.apple.alf.plist
```

Figura 51 - Fichero de configuración del cortafuegos (AFL) de macOS

Adicionalmente, el binario "`/usr/libexec/ApplicationFirewall/socketfilterfw`" permite interaccionar con el ALF desde la línea de comandos (ver página "`man`"):

```
* Consultar la lista de aplicaciones explícitamente definidas en la
configuración:

$ /usr/libexec/ApplicationFirewall/socketfilterfw --listapps
ALF: total number of apps = 2

1 :  /Applications/iTunes.app
      ( Allow incoming connections )

2 :  /Library/Frameworks/OpenVPN.framework/Versions/Current/bin/openvpn-
service
      ( Block incoming connections )

* Comprobar el estado del cortafuegos:

$ /usr/libexec/ApplicationFirewall/socketfilterfw --getglobalstate
Firewall is enabled. (State = 1)
```

```
* Desactivar el cortafuegos:

$ /usr/libexec/ApplicationFirewall/socketfilterfw --setglobalstate off

* Verificar el estado de bloqueo de las conexiones entrantes:

$ /usr/libexec/ApplicationFirewall/socketfilterfw --getblockall
Firewall is set to block all non-essential incoming connections
(vs. Block all DISABLED!)

* Verificar el estado de bloqueo de las apps firmadas:

$ /usr/libexec/ApplicationFirewall/socketfilterfw --getallowsigned
Automatically allow signed built-in software ENABLED
Automatically allow downloaded signed software ENABLED

* Añadir manualmente un proceso a la lista de conexiones permitidas:

$ sudo /usr/libexec/ApplicationFirewall/socketfilterfw --add
/System/Library/CoreServices/RemoteManagement/screensharingd.bundle/Contents/M
acOS/screensharingd
```

Figura 52 - Opciones de socketfilterfw para consultar o modificar la configuración de ALF

Es posible deshabilitar el arranque tanto del agente como del demonio de AFL siguiendo las pautas del apartado "7.1.3. Impedir el arranque de servicios en macOS".

8.2.2.1 PACKET FILTER (PF)

Adicionalmente al cortafuegos personal (ALF) descrito previamente, macOS dispone de un cortafuegos de bajo nivel denominado "*Packet Filter*", en adelante PF, habitual en entornos BSD. PF dispone tanto de capacidades de filtrado de tráfico, entrante (*in o ingress*) y saliente (*out o egress*), como de traducción de direcciones o NAT (*Network Address Translation*).

El fichero de configuración por defecto de PF es "`/etc/pf.conf`", y referencia a "`/etc/pf.anchors/com.apple`", que a su vez incluye políticas para *AirDrop* y para el *ApplicationFirewall* (o ALF).

Los demonios asociados a PF son:

- "`/System/Library/LaunchDaemons/com.apple.pfctl.plist`" (formato ASCII): es el fichero de configuración del demonio `pfctl` (PF o *pf controller*), que lee sus parámetros de "`/etc/pf.conf`" para activar las reglas de PF.
- "`/System/Library/LaunchDaemons/com.apple.pfd.plist`": correspondiente al proceso "`/usr/libexec/pfd`", que implementa la funcionalidad PF.

Para usuarios avanzados, el comando "`sudo pfctl -sa`" permite obtener las estadísticas de PF.

Las reglas de filtrado se agrupan en lo que se denomina "*anchors*", que son conjuntos de reglas de filtrado identificadas por nombre [Ref.- 86].

8.2.3 PRIVACIDAD

Desde esta sección, disponible a través de la pestaña "Seguridad y privacidad - Privacidad", es posible configurar controles de acceso para permitir o denegar 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.

Con macOS Mojave, esta sección ha incluido servicios relacionados con el TCC (Transparency, Consent, and Control), descrito a continuación.

8.2.4 TCC: TRANSPARENCY, CONSENT AND CONTROL

TCC (Transparency, Consent, and Control) es una funcionalidad de control de acceso introducida por macOS 10.14, cuyo objetivo es otorgar al usuario la potestad de permitir o denegar las solicitudes de acceso a aquellos datos, componentes y servicios (asociados a repositorios y bases de datos de Apple[11]) que las apps de terceros tratan de obtener en tiempo de ejecución, incrementando así la protección de la privacidad del usuario.

Las apps disponen de la API "`Security.Authorization`" para acceder a los servicios del demonio "`securityd`" (*Security Server*), que gestiona las autorizaciones de macOS [Ref.- 133]. A través de esta API las apps declaran los permisos para acceder a determinados recursos del sistema. Este demonio invoca a su vez al agente "`Security Agent`" para que muestre el correspondiente menú de diálogo cuando el permiso solicitado por la app debe otorgarse/denegarse por parte del usuario.

La configuración de la funcionalidad TCC está disponible en la sección "Seguridad y privacidad - Privacidad" y, para ordenadores de gestión empresarial, a través del *payload* "`com.apple.tcc`".

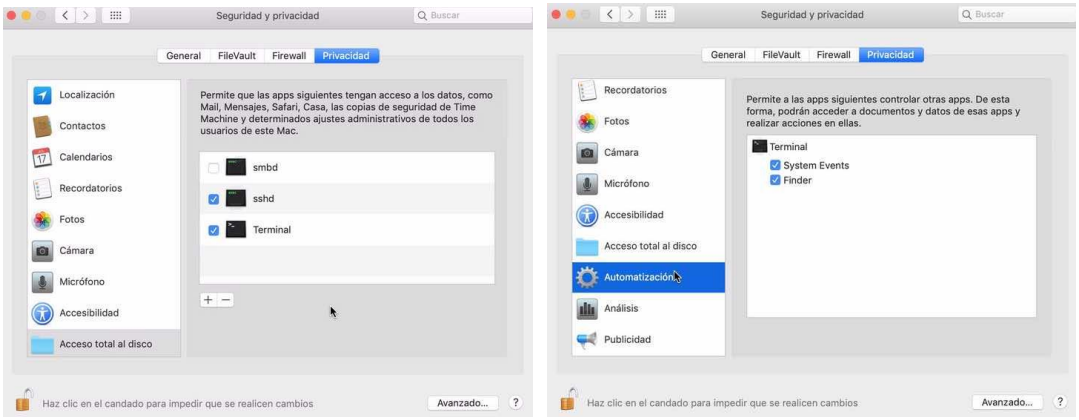


Figura 53 - Ajustes de "Controles de privacidad" de macOS

El paradigma de este mecanismo es similar al utilizado para la carga de extensiones de *kernel* (ver apartado "9.5. Firma y verificación de aplicaciones y del

[11] Las aplicaciones de terceros, que tienen sus propias bases de datos y repositorios para almacenar los datos con los que trabajan, no están incluidas en este mecanismo de protección.

kernel"), y define tres categorías de acceso, que afectan a datos de aplicación, a servicios y a componentes.

Las apps desarrolladas por Apple no requieren concesión explícita de permisos sobre estas categorías. Las categorías principales son:

- Acceso a la cámara y al micrófono: macOS Mojave impide a todas las apps que hacen uso de la API AVFoundation y compiladas con el SDK 10.14 acceder a ambos componentes hasta que el usuario conceda el permiso[12].

NOTA: los ordenadores Mac equipados con chips T1 y T2 [Ref.- 42] gestionan el acceso a la cámara y al micrófono a través de estos chips, mejorando la seguridad del equipo.

- Comunicación entre aplicaciones a través de eventos Apple (*Apple Events*): ver apartado "8.2.4.3. Automatización (Apple Events)".
- Acceso a almacenes de datos privados: incluye servicios como la localización y la accesibilidad, y el acceso a otros datos almacenados por el sistema, como contactos, fotos, calendarios o recordatorios (descritos a continuación).

Las categorías de acceso a datos privados incluidas en este paradigma son:

- Localización: acceso a los servicios de ubicación o geolocalización (ver apartado "8.2.4.4. Localización").
- Contactos: acceso a los contenidos de la app Contactos, disponibles en la carpeta "`~/Library/Application\ Support/AddressBook`".
- Calendarios: acceso a los contenidos de la app Calendario, disponibles en la carpeta "`~/Library/Calendars`".
- Recordatorios: acceso a los contenidos de la app Recordatorios, también disponibles en la carpeta de calendarios "`~/Library/Calendars`", bajo "`./<UUID>.calendar/Events/<UUID2>.ics`".
- Fotos: acceso a los ficheros "`*.photoslibrary`" de la carpeta "`~/Pictures`".
- Accesibilidad: este permiso controla qué apps tienen acceso a las funciones que permiten monitorizar y controlar el equipo (supuestamente con el objetivo de mejorar la accesibilidad del usuario a macOS), por ejemplo, el servicio de grabación y *playback* de "Automator" o apps para la conexión de un ordenador Mac a un replicador de puertos. Las aplicaciones con este permiso están autorizadas para el envío y ejecución de comandos en macOS, y a capturar las pulsaciones de teclado. Debe concederse cautelosamente, porque las técnicas de captura de pulsaciones de teclado (*keyloggers*) son comunes en el *malware*.
- Acceso total al disco (*Full Disk Access, FDA*): ver apartado "8.2.4.2. Acceso total al disco (Full Disk Access)".
- Análisis: 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 errores con estos, con el objetivo de mejorar sus productos y servicios. Se aconseja desmarcar todos los elementos de esta sección.

[12] https://www.idownloadblog.com/2018/08/16/howto-mac-camera-microphone-permission/

- Publicidad: esta sección permite limitar el seguimiento por parte de las redes de anuncios, evitando que se puedan recibir anuncios personalizados, tanto en las apps de Apple como en macOS, en función de los intereses del usuario. Se recomienda habilitar esta limitación, así como resetear el identificador de anuncios periódicamente, mediante el botón disponible en esta sección.

Para revocar de forma temporal el permiso de acceso a un elemento determinado, se puede desmarcar el "*tick*" correspondiente; para las categorías "Accesibilidad" y "Acceso total al disco" se puede seleccionar el botón "-" para eliminar la entrada de una app, y sus permisos, de forma permanente.

Uno de los inconvenientes de la implementación actual de TCC es que, si el usuario deniega el permiso a la app solicitante en un momento concreto (bien a propósito, bien por error) pero más adelante necesita concederlo, la app no volverá a solicitar el permiso. El usuario no dispone de ningún mecanismo para forzar a la app a solicitar el permiso de nuevo, sino que deberá restablecer los permisos de toda la categoría de privacidad asociada de forma manual. Para ello, Mojave incorpora la utilidad "`tccutil reset <categoría>`", que restaura los controles de acceso originales para esta categoría de permisos, de forma que las apps que quieran disponer de ellos tendrán que solicitar de nuevo el consentimiento del usuario. Por ejemplo, con el elemento "`SystemPolicyAllFiles`" se restablecen los permisos de la categoría "Acceso total al disco". Para restablecer los ajustes de la categoría "Automatización", el parámetro es "`AppleEvents`" (con nombres poco intuitivos).

NOTA: la página de ayuda de "`tccutil`" es poco detallada. Para identificar las categorías que se pueden restablecer a través de esta herramienta, es posible ejecutar el comando[13] (es necesario eliminar el prefijo "kTCCService" de los nombres de las categorías):

```
$ strings /System/Library/PrivateFrameworks/TCC.framework/TCC | grep kTCCService
```

Otro inconveniente comúnmente señalado por los desarrolladores de apps es la indisponibilidad de una "lista blanca", que permita que el usuario pre-apruebe las solicitudes procedentes de apps en las que confía [Ref.- 51]. El único modo de conceder acceso a una categoría de permisos es abrir la app que los requiere y aceptar la solicitud de forma expresa. Las únicas excepciones son: "Acceso total al disco" y "Accesibilidad", a las que se puede añadir elementos mediante el botón "+" (ver <Figura 53>).

8.2.4.1 BASE DE DATOS DE TCC

macOS emplea dos bases de datos bajo "`~Library/Application\ Support/com.apple.TCC/tcc.db`" y "`/Library/Application\ Support/com.apple.TCC/tcc.db`", donde almacena los ajustes del subsistema TCC. Estas bases de datos SQLite pueden consultarse mediante la utilidad "`sqlite3`"[14]:

```
$ sudo sqlite3 /Library/Application\ Support/com.apple.TCC/TCC.db 'select * from access'
```

[13] https://bitsplitting.org/2018/07/11/reauthorizing-automation-in-mojave/

[14] https://applehelpwriter.com/2018/07/06/accessing-tcc-db-without-privileges/

```
kTCCServicePostEvent|DisplayLink.DisplayLinkUserAgent|0|1|1|??|||UNUSED||0|155
1001519
kTCCServicePostEvent|com.apple.helpviewer|0|0|1||||UNUSED||0|1551967652
kTCCServicePostEvent|com.apple.screensharing.agent|0|1|1||||UNUSED||0|15616236
18
kTCCServiceSystemPolicyAllFiles|com.apple.Terminal|0|1|1|??|||UNUSED||0|156165
0339
```

Figura 54 - Consulta de la base de datos de autorizaciones de TCC

Por otra parte, en el fichero de configuración "`/System/Library/Sandbox/TCC_Compatibility.bundle/Contents/Resources/AllowApplicationsList.plist`", macOS define las versiones y detalles de las apps que disponen de acceso a elementos controlados por el TCC.

El fichero "`~/Library/Preferences/com.apple.universalaccessAuthWarning.plist`" guarda registro de todas las apps que han solicitado en algún momento permiso para controlar elementos del sistema. Con el comando "`defaults`" es posible consultarlas, así como saber qué respondió el usuario (0 - denegó el acceso, 1 - permitió el acceso):

```
$ defaults read
~/Library/Preferences/com.apple.universalaccessAuthWarning.plist
{
    "1::/System/Library/CoreServices" = 1;
    "1::/System/Library/CoreServices/HelpViewer.app" = 1;
}
```

Figura 55 - Solicitudes de permisos del TCC para controlar el sistema por parte de las apps

8.2.4.2 ACCESO TOTAL AL DISCO (FULL DISK ACCESS)

Esta categoría, gestiona el acceso completo al disco, sin granularidad respecto a los datos a los que permite acceso, como las categorías anteriores, afecta a los datos asociados a las ciertas aplicaciones como "Mail", "Mensajes", "Safari", "Home" y "Time Machine" y a ciertos ajustes administrativos que afectan a todos los usuarios del sistema.

Numerosas aplicaciones y utilidades del sistema existentes en macOS desde versiones anteriores a Mojave han experimentado problemas (viendo su ejecución terminada por el sistema) por no disponer de este permiso, al no haberlo solicitado de forma explícita al usuario. En estos casos, el usuario tendrá que añadir de forma manual la app o la utilidad a la sección "Acceso total al disco". Para ello, tras pinchar sobre el candado e introducir las credenciales de administrador, se procederá a:

- En el caso de comandos ejecutados desde la app "Terminal", habrá que añadir esta app mediante el botón "+", y seleccionarla tras navegar hasta la carpeta "Utilidades" en la que reside ("Aplicaciones - Utilidades - Terminal.app").
  Un ejemplo de este escenario es el fallo de los comandos "`mv`" y "`defaults`" para ciertos archivos y carpetas, aun siendo ejecutados incluso con privilegios de administrador.

- En el caso de querer añadir otros binarios o scripts, tras pulsar el botón "+" y obtener la ventana de aplicaciones, se pulsará la combinación de teclas "⌘+⇧ + G" (`Comando + Cambio + G`), "Ir a la carpeta", en la que se introducirá la ruta completa al script o binario que se desea incluir.
  Un ejemplo de este escenario es el uso de tareas programadas mediante "`cron`" que ejecutan scripts situados en un directorio de usuario.
  El menú "+" también soporta la función "*drag & drop*" para arrastrar elementos.

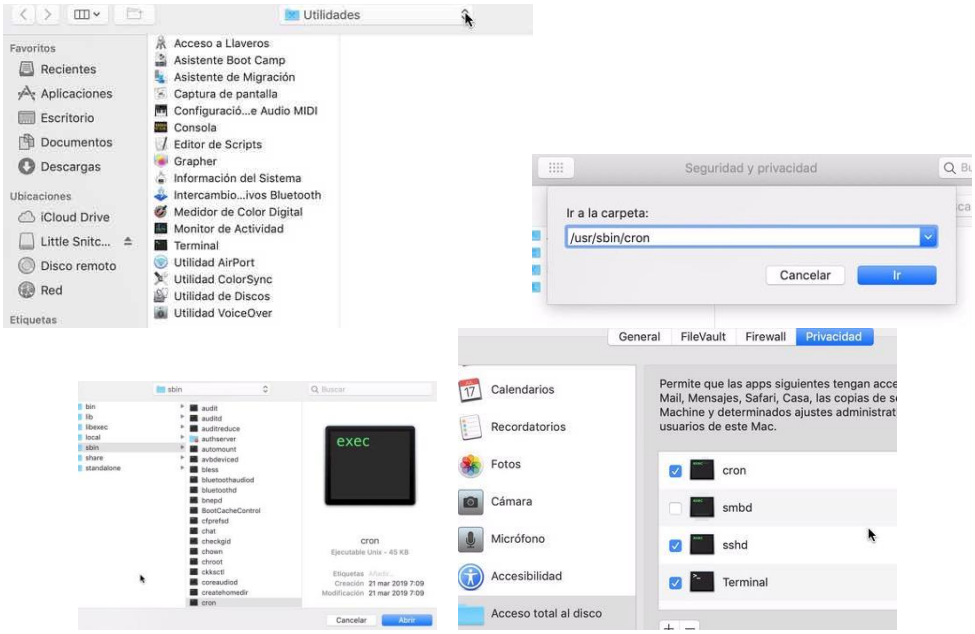


Figura 56 - Gestión del permiso de "Acceso total al disco" del TCC

"Acceso total al disco", además de permitir trascender el directorio *home* del usuario y acceder a otros ficheros según el modelo de permisos estándar de Unix, otorga acceso a los siguientes contenidos [Ref.- 52]:

- Mail: `~/Library/Mail`.
- Mensajes: `~/Library/Messages`.
- Historia de navegación de Safari: `~/Library/Safari`.
- Cookies: `~/Library/Cookies`.
- Backups de "iTunes".
- Backups de "Time Machine".
- Varios: `~/Library/HomeKit`, `~/Library/IdentityServices`, `~/Library/Suggestions`, `~/Library/Metadata/CoreSpotlight`, `~/Library/PersonalizationPortrait`.

8.2.4.3 AUTOMATIZACIÓN (APPLE EVENTS)

Esta categoría de permisos afecta a los "*Apple Events*", un mecanismo de comunicación entre procesos que permite que una aplicación invoque a otra (o solicite acceso a sus datos) durante su ejecución. Un ejemplo de eventos Apple es la funcionalidad de abrir un editor desde el menú de otra aplicación, que desencadenará

una solicitud para controlar la app "Finder", ilustrado en la <Figura 57> con la app "Terminal".

Con el objetivo de impedir que los datos de usuario puedan ser comprometidos por este mecanismo, macOS 10.14 incorpora la categoría "Automatización", por la cual, cuando una app solicitante envía un evento a una app receptora, se lanza una solicitud de confirmación a través de una ventana de diálogo, con dos opciones para el usuario:

- **Permitir**: el hilo (*thread*) de la app solicitante (la que envía el "*Apple Event*") puede continuar su ejecución, y los eventos de este tipo que envíe en el futuro serán admitidos por el sistema.
- **No permitir**: el hilo de la app solicitante recibe un código de error, que el sistema enviará también a todos los eventos futuros que se emitan por parte de la app solicitante a la app receptora.

La concesión de este permiso por parte del usuario añadirá la app solicitante a la categoría "Automatización" (ver <Figura 57>).

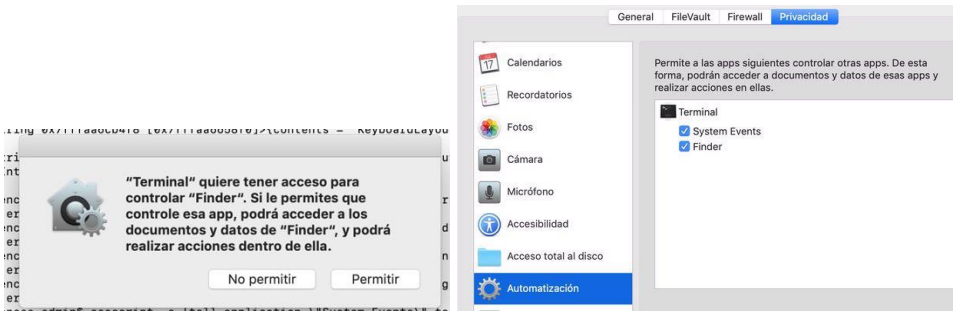


Figura 57 - Notificaciones de acceso a recursos protegidos por TCC y autorizaciones concedidas

Si la aplicación solicitante ha sido compilada con la versión de Xcode específica de Mojave (10.14), el texto de la notificación incluirá una descripción genérica proporcionada por Apple más el contenido que haya proporcionado el desarrollador en la propiedad "`NSAppleEventsUsageDescription`" del fichero "`Info.plist`" de la app (ver apartado "13.4.1. Ficheros PLIST de una app"); en caso contrario, el texto será únicamente el genérico proporcionado por Apple. Si el usuario da su autorización, la app se incluirá dentro de la categoría correspondiente de la sección "Privacidad - Automatización". Si la deniega, la app puede, bien abortar, bien manejar la condición si ha sido programada para ello.

8.2.4.4 LOCALIZACIÓN

El servicio de localización en macOS se obtiene principalmente a partir de las redes Wi-Fi existentes en la zona de cobertura actual del ordenador Mac, y, atendiendo a los términos y condiciones mostrados a través del botón "Acerca de los servicios de localización & privacidad", de forma que no se identifique al usuario (según se describe en el texto asociado). Cuando se activa el servicio por primera vez a través de la casilla "Activar los servicios de localización", se incluye por defecto "Siri y Dictado" (desactivado) y "Servicios del sistema", que mediante el botón "Detalles...", permite establecer un control más granular sobre los diferentes servicios que pueden acceder a la localización.

Desde el punto de vista de seguridad, ***el único ajuste de los servicios del sistema con acceso a la localización considerado necesario es*** "Buscar mi Mac" (ver apartado "11.3. Buscar mi Mac"). El ajuste "Sugerencias según la ubicación", estando activo, provoca que la información de localización se envíe a Apple para obtener información basada en la ubicación en las búsquedas de Siri. Pese a ello, Apple puede utilizar la dirección IP del equipo para estimar la ubicación del ordenador Mac.

Adicionalmente, si se va a hacer uso de la funcionalidad "Night Shift" (ver apartado "8.5.3. Centro de Notificaciones") mediante la opción "De la puesta a la salida del sol", se requerirá que la localización esté habilitada para "Servicios del sistema - Personalización del sistema y la zona horaria".

La localización también se enviará a Apple (si el servicio está activo) durante las búsquedas de Spotlight, incluyendo detalles sobre suscripciones a servicios de contenido audiovisual. Para impedir este comportamiento, se debe acceder al menú "Preferencias del sistema - Spotlight" y desactivar la casilla "Permitir las sugerencias de Spotlight en Consultar".

En el menú de localización se mostrará también la lista de aplicaciones que han solicitado acceso a la ubicación, junto a la casilla desde la cual se puede controlar el permiso. El símbolo "➚" junto a una aplicación indica que dicha app ha utilizado los servicios de localización en las últimas 24 horas.

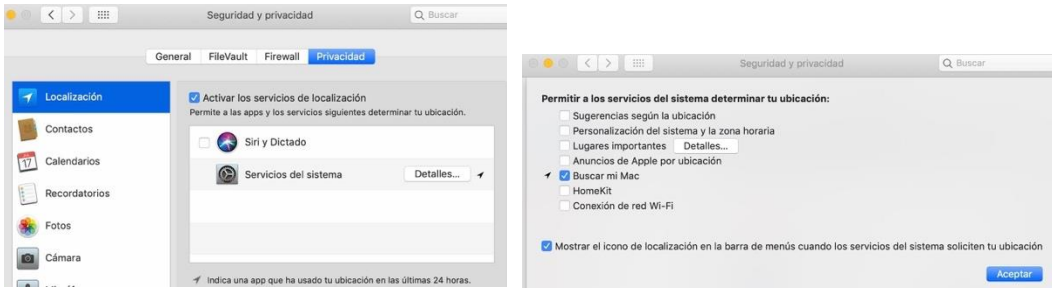


Figura 58 - Ajustes de localización

Se recomienda limitar el acceso de las apps a la ubicación, denegando el permiso solicitado a cualquier app cuyo cometido no sea explícitamente el uso de este servicio, y habilitarlo para ellas únicamente cuando se vaya a hacer uso del mismo**.** ***También se recomienda seleccionar la opción*** "Mostrar el icono de localización en la barra de menús cuando los servicios del sistema soliciten tu ubicación" de los servicios del sistema, para tener conciencia de su utilización.

El ajuste de localización se almacena como un parámetro de la NVRAM (ver apartado "18.5.1. NVRAM"), por lo que puede determinarse su estado desde la línea de comandos mediante "`nvram -p`". Si el parámetro "`LocationServicesEnabled %01`" figura en la salida, la localización está habilitada en el equipo.

8.2.4.5 ACCESIBILIDAD

Los servicios de accesibilidad han sido frecuentemente objetivo de ataques, ya que las apps con este privilegio pueden emular pulsaciones de ratón del usuario (por ejemplo, para aceptar las preguntas de ventanas de diálogo).

Por este motivo, solo se recomienda conceder este privilegio en caso de que las circunstancias lo requieran y solo a apps de confianza.

8.2.5 OTROS AJUSTES RELATIVOS A LA PRIVACIDAD

En este apartado se describen ajustes que, aun accesibles desde otras secciones del menú de "Preferencias del sistema", tienen impacto sobre la privacidad.

8.2.5.1 MENÚ "TECLADO"

Dentro de este menú se encuentra la sección "Dictado", que hace uso de las capacidades de reconocimiento de voz de macOS para reemplazar la entrada de texto mediante teclado con el procesamiento de la voz del usuario. El botón "Acerca de Dictado y la privacidad" describe el procedimiento empleado para el reconocimiento de voz. Salvo que se requiera hacer uso de la funcionalidad de dictado, ***se recomienda desactivarla***.

En caso de ser necesaria, ***se recomienda la utilización de*** "Usar "Dictado mejorado"", que utiliza servicios del sistema sin enviar información a Apple y permite el uso de las capacidades de dictado de manera *offline*, sin conexión (requiere la descarga de unos 400-900MB de datos, según el equipo). En caso contrario, además de la voz, se enviará a Apple información adicional, que incluye datos de los contactos, incluidas relaciones personales inferidas de ellos, nombres de álbumes de fotos, etc., además de la información de ubicación si la localización está activada durante el uso de la función de dictado.

Se recomienda desmarcar la opción "Preferencias del sistema - Seguridad y privacidad - [Privacidad] - Localización - "Siri y Dictado"".

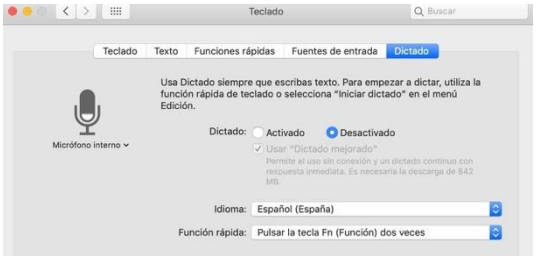


Figura 59 - Opciones de "Dictado"

8.2.5.2 MENÚ "SIRI"

La configuración del asistente personal digital de Apple queda fuera del ámbito de la presente guía. Desde el punto de vista de la privacidad, y debido a la naturaleza de la información que el sistema envía a Apple durante su uso, ***se aconseja desactivar los servicios de Siri***. Para ello, se debe desmarcar el ajuste "Preferencias del sistema - Siri - Activar "Consultar a Siri"".

En caso de querer hacer uso del servicio, se recomienda acceder al botón "Sugerencias de Siri y privacidad" y suprimir las apps que aparezcan en esta sección y cuyos datos no se desee incluir como parte de las sugerencias de Siri.

Figura 60 - Configuración de "Siri"

En caso de activar Siri, se recomienda seleccionar la opción "Mostrar Siri en la barra de menús", para tener conciencia de su utilización y poder disponer de un acceso rápido.

8.2.6 EXTENSIONES

Las extensiones son componentes que añaden funcionalidad adicional a las apps, el Finder, el Centro de Notificaciones, el menú "Compartir" y la "Touch Bar" (para aquellos equipos Mac que dispongan de ella, que son los equipados con "Touch ID"). La configuración de las extensiones está disponible desde "Preferencias del sistema - Extensiones".

Desde el punto de vista de la privacidad y la seguridad, el "Menú Compartir" ("Share Menu"), disponible también en diversas aplicaciones a través del icono "⎙" o "Share" (por ejemplo, Finder y Safari), ofrece un mecanismo rápido de envío de información a otros dispositivos y aplicaciones, por lo que se aconseja eliminar todas aquellas extensiones que no se utilicen, para evitar fugas de información no deseadas. A fecha de elaboración de la presente guía, en Mojave, las opciones de compartición de "Mail", "Mensajes", "AirDrop", y "Añadir a personas" no pueden ser desactivadas.

Mojave limita las extensiones disponibles en este menú respecto a sus antecesores, quedando excluida la integración con cuentas de terceros configuradas en el sistema (por ejemplo, ciertos servicios de correo ajenos a "Mail" y los asociados a redes sociales como Facebook y Twitter, previamente integrados en macOS[15]).

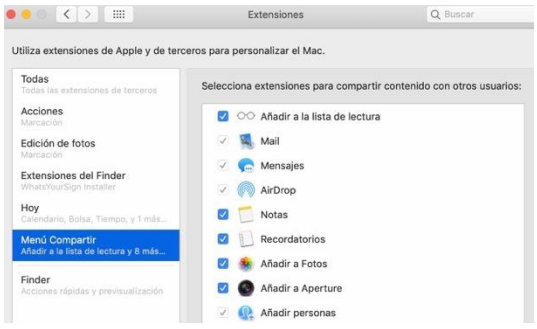


Figura 61 - Menú "Compartir" de los ajustes de "Extensiones"

Las categorías de extensiones disponibles en macOS Mojave son:

15 https://appleinsider.com/articles/18/06/06/apple-strips-facebook-twitter-integration-from-macos-mojave

- **Todas**: incluye todas las extensiones disponibles e instaladas en macOS.
- **Acciones**: extensiones con fines de edición y visualización de contenidos.
- **Edición de fotos**: extensiones para edición de imágenes y fotografías.
- **Extensiones del Finder:** extensiones que añaden personalizaciones al interfaz de usuario de la app Finder.
- **Hoy**: extensiones relativas a la funcionalidad de vista del día (*Today view*) del Centro de Notificaciones.
- **Menú Compartir**: extensiones que se admiten en la función de compartición de contenidos entre apps.
- **Finder**: permite seleccionar las acciones rápidas (*Quick Actions*) y los proveedores de contenidos que serán mostrados en la app Finder.

Se recomienda deshabilitar las extensiones que no se utilicen, especialmente en las categorías "Extensiones del Finder", "Finder" y "Compartir".

8.3 SPOTLIGHT

Spotlight, disponible como categoría de configuración dentro de "Preferencias del sistema", es un sistema de búsqueda rápida de información en macOS con capacidades para ofrecer sugerencias de búsqueda, tanto locales al equipo como obtenidas remotamente desde Internet. Para ello, este servicio envía remotamente los términos introducidos por el usuario, pudiendo poner en riesgo su privacidad. Asimismo, como se describe en el apartado "8.2.4.4. Localización", las búsquedas de Spotlight pueden enviar a Apple información privada del usuario si la localización está activa, por lo que ***se recomienda desmarcar la casilla*** "Permitir las sugerencias de Spotlight en Consultar".

Desde la pestaña "Privacidad" de Spotlight es posible definir una lista de ubicaciones (carpetas individuales o discos) que serán excluidas de las búsquedas de Spotlight. ***Se recomienda añadir en esta sección las carpetas con información crítica o sensible del usuario***, que podría ser enviada a los servidores de Apple como parte de los datos que remite Spotlight.

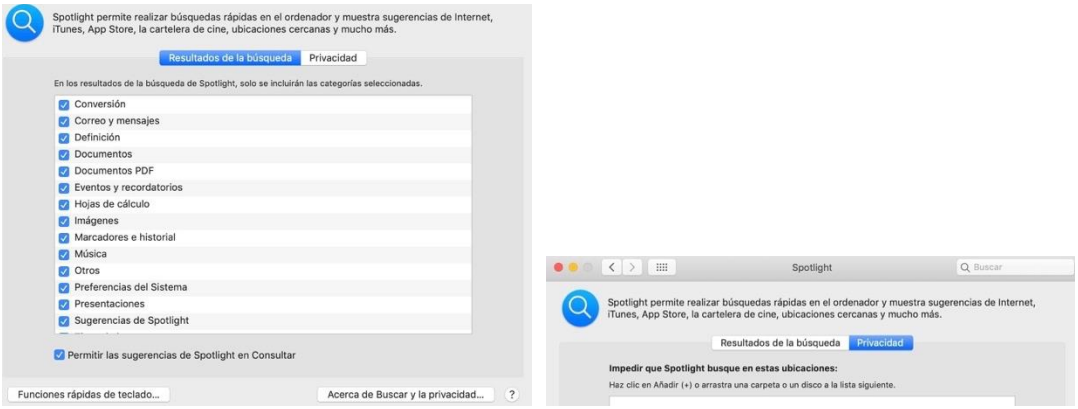


Figura 62 - Opciones de búsqueda de Spotlight

Es especialmente relevante la desactivación de la opción "Correo y mensajes", ya que en la versión de macOS Yosemite se descubrió que Spotlight ignora algunos mecanismos de protección establecidos a través de la aplicación Mail, como la carga

de contenido remoto en mensajes, y que permite obtener la dirección IP del usuario cuando se lee un mensaje de correo electrónico que contiene una imagen, y la imagen se descarga desde el servidor remoto[16].

La función de búsqueda de Spotlight se invoca desde el icono de lupa "🔍" de la barra de estado (ver apartado "8.5. Pantalla de inicio (Home)").

Para agilizar el resultado de las búsquedas, Spotlight indexa los ítems que están marcados en su sección "Resultados de la búsqueda", con una amplia lista de categorías. En ocasiones, se ha observado que esta indexación ocasiona problemas de rendimiento, por lo que se aconseja dejar marcados solo los elementos que realmente se necesita incluir en los resultados, en caso de hacer uso de Spotlight.

Es posible deshabilitar Spotlight para un usuario concreto según el procedimiento descrito en el apartado "7.1.3. Impedir el arranque de servicios en macOS", aunque ello requiere deshabilitar SIP momentáneamente:

```
$ launchctl list | grep -i spot
429   0     com.apple.corespotlightd
309   0     com.apple.Spotlight

$ launchctl unload -w /System/Library/LaunchAgents/com.apple.Spotlight.plist

$ launchctl unload -w
/System/Library/LaunchAgents/com.apple.corespotlightd.plist

$ launchctl list | grep -i spot
-     0     com.apple.corespotlightservice

$ cat /var/db/com.apple.xpc.launchd/disabled.`id -u`.plist
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        ...
        <true/>
        <key>com.apple.corespotlightd</key>
        <true/>
        <key>com.apple.Spotlight</key>
        <true/>
</dict>
</plist>
```

Figura 63 - Desactivación de Spotlight para un usuario concreto

8.4 MISSION CONTROL

Mission Control permite al usuario visualizar todos los escritorios disponibles, las vistas divididas (*Split Views*) y las apps en ejecución. El uso general de este elemento se describe en la [Ref.- 72], y su personalización está accesible desde el menú "Preferencias del sistema - Mission Control".

[16] https://www.imore.com/spotlight-spam-email-and-what-you-need-know
https://www.pcworld.com/article/2867212/glitch-in-os-x-search-can-expose-private-details-of-apple-mail-users.html

Se considera interesante desde el punto de vista de privacidad y seguridad la asignación de "Bloquear pantalla" a alguna de las "Esquinas activas", lo que permite bloquear el acceso a la sesión del usuario de forma rápida en caso de necesidad.

En Mojave, el escritorio *Dashboard* en el que se muestran *widgets* está desactivado por defecto. Si se desea utilizar su funcionalidad en Mojave, se dispone de dos opciones:

- Ejecutar la app Dashboard desde el Launchpad.
- Seleccionar la opción "Dashboard" desde los ajustes de "Mission Control" y elegir "Como espacio" (se mostrará en un escritorio independiente) o "Como superposición" (los *widgets* se mostrarán en el escritorio activo), y asignarle una tecla de función rápida o una de las "Esquinas activas".

Figura 64 - Configuración del Dashboard para visualización de elementos en el escritorio

macOS permite incluir/suprimir nuevos elementos en el *Dashboard* mediante los botones "⊕" y "⊖" que aparecen en la esquina inferior izquierda del *Dashboard*. Si se desea que estos *widgets* aparezcan en primer plano superpuestos sobre las apps en ejecución del escritorio, hay que[17]:

- Ejecutar los comandos de la <Figura 65>.
- Eliminar (mediante el símbolo "-") todos los *widgets* presentes en el panel de *Dashboard* (o reiniciar la sesión del usuario).
- Entrar en el *Dashboard* y elegir (mediante el símbolo "+") los *widgets* que se desea superponer.

Se recomienda evitar** widgets **que revelen información sensible, por ejemplo, "Contactos" o "Postits". Una vez finalizada la personalización del panel del *Dashboard*, la opción "`devmode`" deberá cambiarse a "`NO`" (el cambio tendrá efecto cuando se cierre y se reabra la sesión del usuario).

```
$ defaults write com.apple.dashboard devmode YES
$ killall Dock
```

Figura 65 - Opción para añadir widgets al Dashboard directamente en el escritorio

[17] https://www.youtube.com/watch?v=7m57oX0Cc1s (referente a macOS High Sierra, pero vigente en Mojave).

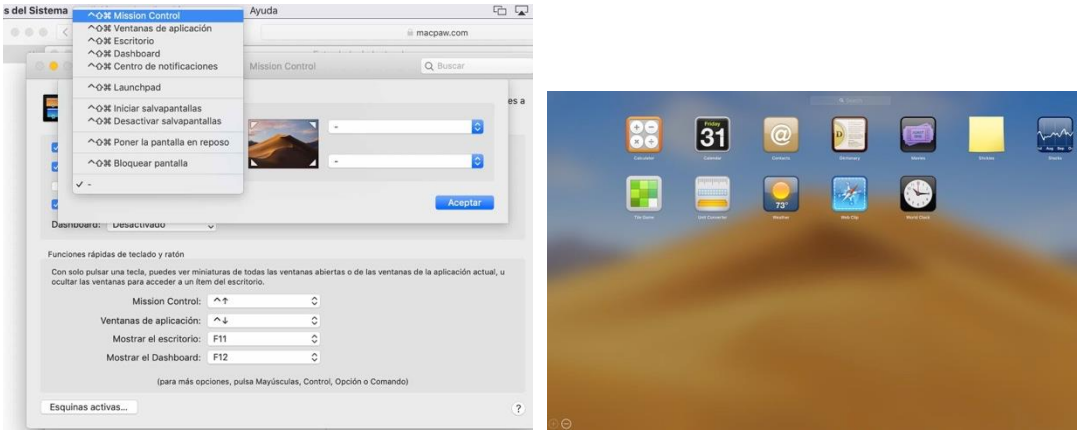


Figura 66 - Personalización de Mission Control y de la vista del Dashboard

8.5 PANTALLA DE INICIO (HOME)

La pantalla de inicio, también denominada escritorio, se muestra al iniciar sesión y salir de la pantalla de bloqueo [Ref.- 73]. Está formada por:

- Una zona de escritorio, que, tras iniciar el sistema, presenta un fondo de pantalla estándar. ***Se recomienda cambiar la imagen de este fondo***, para evitar que revele la versión de macOS empleada (ya que cada versión de macOS hace uso de un fondo de pantalla diferente y característico), por una imagen que no revele información sobre el usuario. El menú para ello está disponible en "Escritorio y salvapantallas - Escritorio - Botón + ".
- Una barra de menús, situada en la parte superior de la pantalla, formada por:
  - El menú "Apple", accesible desde el icono "", en la esquina superior izquierda.
  - La barra de menús de la app que está en primer plano de ejecución, a lo largo de toda la zona superior (junto al menú "Apple"). La barra de menús se describe en la [Ref.- 74].

  Se recomienda activar la opción "Preferencias del sistema - General - Ocultar y mostrar la barra de menús automáticamente", que implica que la barra estará oculta hasta que el usuario quiera acceder a ella y desplace el puntero del ratón por el margen superior. De este modo, la información sobre el estado del sistema queda oculta a la vista de manera permanente.
- Una barra de estado, en la esquina superior derecha, formada por:
  - Los menús de estado: ver apartado "8.5.1. Menús de estado".
  - El icono para abrir "Spotlight", accesible desde el icono de lupa "". Se recomienda consultar el apartado "8.3. Spotlight" para obtener información sobre este servicio, incluido el procedimiento para deshabilitarlo completamente.
  - El icono para acceder al Centro de Notificaciones: ver apartado "8.5.3. Centro de Notificaciones".
- El "Dock": ver apartado "8.5.2. Dock".

8.5.1 MENÚS DE ESTADO

La barra de menús de estado incluye los iconos que informan sobre múltiples aspectos del estado del sistema. Adicionalmente, al pinchar sobre cada uno de ellos, macOS ofrece acceso directo a ciertas funcionalidades relacionadas con el elemento en cuestión (conocidas como *menulets*).

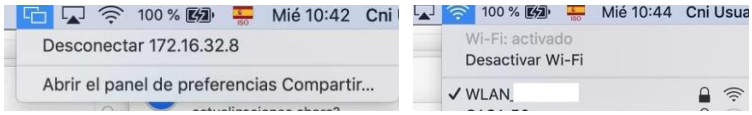


Figura 67 - Menús de estado

Es posible intercambiar la posición de los iconos de estado, pulsando la tecla "⌘" (`Comando`) mientras se arrastra el icono, así como suprimir iconos y añadirlos.

- Los iconos asociados a elementos del sistema se pueden eliminar pulsando la tecla "⌘" (`Comando`) y arrastrándolo hacia el escritorio, fuera de la barra de menús.
- Para añadir iconos de apps/servicios del sistema, normalmente se debe acceder al menú "Preferencias del sistema - [Elemento] - Mostrar [Elemento] en la barra de menús". Hay algunas excepciones, como el nombre del usuario asociado a la sesión, que se aconseja eliminar de la barra de menús desactivando la opción "Usuarios y grupos - Opciones de inicio - Mostrar menú cambio rápido usuario como" (ver apartado "8.18.1. Usuarios y grupos").
- Los iconos asociados a apps de terceros no se pueden eliminar por el procedimiento anterior, y la opción "Quit" o "Salir" suele implicar que la ejecución de la aplicación finalice.
- Solo algunas apps de terceros incluyen en su sección "Preferencias" una opción para gestionar la presencia de su icono en la barra de menús de estado.
- Bajo la carpeta "`/System/Library/CoreServices/Menu\ Extras`" se incluyen algunas opciones de menú adicionales, que pueden ser añadidas a la barra de menús de estado accediendo a la carpeta desde Finder y pinchando dos veces sobre el elemento deseado.

Desde el punto de vista de seguridad, ***se aconseja suprimir los elementos que desvelan información relevante del sistema, como el que muestra el nombre del usuario propietario de la sesión***.

En la [Ref.- 75] se proporciona un tutorial descriptivo para la personalización de la barra de menús de estado.

8.5.2 DOCK

El Dock está compuesto por iconos de apps y servicios, de forma que se pueda acceder a ellos de forma rápida y sencilla. Puede estar ubicado bien en la parte inferior, bien en uno de los márgenes laterales, según se haya definido en el menú "Preferencias del Sistema - Dock".

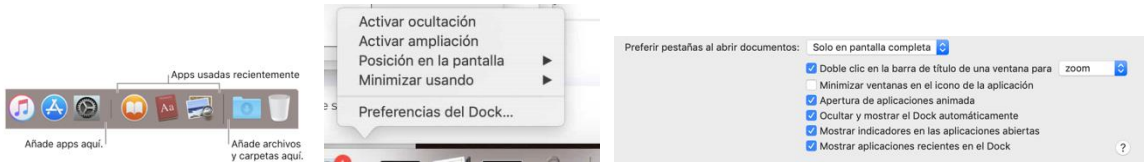


Figura 68 - Menú del Dock [Ref.- 76]

Un icono de círculo rojo con un número en su interior "1" indica que hay "N" acciones pendientes o notificaciones en la app asociada. Un pequeño punto bajo un icono de app indica que la app está actualmente en ejecución (este comportamiento se controla mediante la opción "Mostrar indicadores en las aplicaciones abiertas"). En Mojave, el Dock incluye además una sección en la que se muestran las tres apps que se han usado más recientemente. Para eliminar esa sección, se debe desmarcar la casilla "Mostrar aplicaciones recientes en el Dock".

Se recomienda ocultar el Dock, a fin de no desvelar las apps instaladas y las que se están utilizando actualmente, a través de la opción "Preferencias del Sistema - Dock - Ocultar y mostrar el Dock automáticamente".

macOS permite personalizar el Dock [Ref.- 76], incluyendo la posibilidad de añadir y eliminar elementos. Aunque el Dock facilita la usabilidad de macOS, puede ser recomendable prescindir de aquellos iconos que potencialmente desvelan costumbres de uso del equipo.

En su parte derecha (cuando se usa la vista inferior del Dock), macOS Mojave incluye el icono de la papelera, los documentos y la funcionalidad "*Stacks*" (pilas) para la carpeta "Descargas" (en la que se almacenan los ficheros descargados como adjuntos, de Internet, o a través de AirDrop). El Dock permite que el usuario añada nuevos ficheros, carpetas o pilas, para la cual crea un "alias", es decir, un enlace al elemento original que permite acceder a él de forma rápida pero que, si se elimina, no implica la eliminación del elemento original. Para información sobre las pilas, tanto en el Dock como en el escritorio, consultar la [Ref.- 77].

8.5.3 CENTRO DE NOTIFICACIONES

El denominado "Centro de Notificaciones" es un panel que se presenta al pulsar sobre el icono "≡" situado en la parte superior derecha de la barra de menús de estado (ver apartado "8.5.1. Menús de estado"), y que se divide en dos secciones o pestañas (ambas presentan el menú de activación del modo "No molestar" y de "Night Shift" (descritos más adelante):

- **Hoy**: proporciona acceso a los *widgets* habilitados, por defecto, "Calendario", "Tiempo", "Bolsa" y mañana (ver primera imagen de la <Figura 70>). Se pueden añadir/eliminar *widgets* mediante el menú "Editar", desde el que adicionalmente se pueden descargar nuevos elementos de la App Store.
- **Notificaciones**: muestra las notificaciones activas. En función del parámetro "Preferencias del sistema - Notificaciones - Orden en el centro de notificaciones", este campo mostrará:

- "Recientes": se muestran las apps con una antigüedad inferior a 7 días, ordenadas de más reciente a más antigua.
- "Recientes por app": macOS agrupará las notificaciones procedentes de una misma app en una pila, que permite procesarlas o eliminarlas individualmente o en su conjunto. En este caso, se mostrarán todas las notificaciones de cada app que no se hayan procesado o descartado (sin importar la antigüedad). El orden de presentación es de más reciente a más antigua (segunda imagen de la <Figura 70>).
- "Manualmente por app": el comportamiento es idéntico al anterior, pero las apps se pueden ordenar por parte del usuario desplazándolas en el menú de la lista de aplicaciones (tercera imagen de la <Figura 70>). Éste es el único mecanismo que macOS Mojave ofrece para que el usuario pueda determinar prioridades de las notificaciones.

Desde el icono '⚙' situado en el margen inferior derecho se abre el menú "Preferencias del sistema - Notificaciones", en el que se definen las políticas de gestión de notificaciones.

Si se mantiene pulsada la tecla "⌥" (Opción) mientras se pulsa el icono del Centro de Notificaciones, solo se mostrarán las notificaciones que requieren acción por parte del usuario, las cuales permanecerán en pantalla hasta que se repita esta misma acción o se actúe sobre la notificación (ver cuarta imagen de la <Figura 70>).

El Centro de Notificaciones puede deshabilitarse siguiendo el procedimiento descrito en el apartado "7.1.3. Impedir el arranque de servicios en macOS":

```
$ launchctl unload -w
/System/Library/LaunchAgents/com.apple.notificationcenterui.plist
```

Figura 69 - Comando para deshabilitar el Centro de Notificaciones

Mediante este procedimiento, el icono asociado al Centro de Notificaciones estará presente en la barra de menús de estado, pero no lanzará ninguna acción al pinchar sobre él, ni se recibirán notificaciones.

8.5.3.1 NOTIFICACIONES

Una interrupción es un evento generado por una app, que normalmente ejecuta en segundo plano, destinado a atraer la atención del usuario para informarle de eventos que se consideran relevantes desde el punto de vista de la app, interfiriendo con el uso que está haciendo del equipo en un momento concreto. Es la aplicación la que define cuándo enviar una interrupción, pero es el usuario quien establece el comportamiento del equipo frente a la interrupción.

Una notificación es la manifestación de una interrupción, que una aplicación o servicio genera para ser mostrada al usuario fuera de su interfaz propio. El sistema procesa las notificaciones conforme a la configuración definida por el usuario en relación con la política de interrupciones activa en el equipo en el momento de recibirse la notificación. La [Ref.- 78] proporciona la documentación oficial de Apple para la configuración de notificaciones a nivel de usuario, que se realiza a través del menú "Preferencias del sistema - Notificaciones".

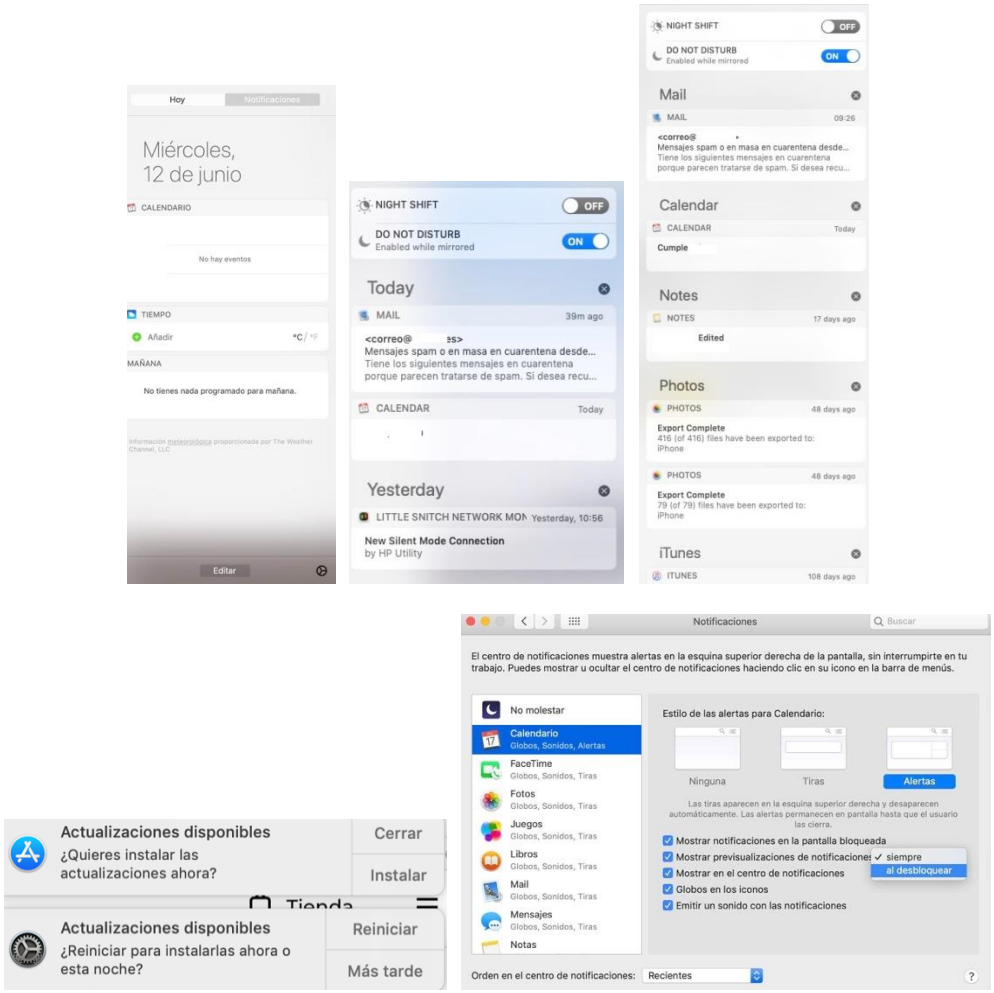


Figura 70 - Centro de Notificaciones y menú de configuración de notificaciones

La aparición de las notificaciones en la pantalla de bloqueo puede controlarse por aplicación. Los ajustes a tener en cuenta desde ***el punto de vista de seguridad y privacidad*** son (ver quinta imagen de la <Figura 70>):

- "Mostrar notificaciones en la pantalla bloqueada": en términos generales, ***se recomienda deshabilitar esta opción***, que permitiría a cualquier persona con acceso visual a la pantalla del equipo saber qué aplicaciones están instaladas, disponer de acceso a sus notificaciones, y establecer patrones de uso de las mismas.
- "Mostrar previsualizaciones de notificaciones": la recomendación de privacidad y seguridad depende del tipo de aplicación. En todo caso, ***se aconseja establecer el valor a*** "al desbloquear", porque, en caso contrario, el mensaje de previsualización podría revelar información no deseada en la pantalla de inicio de sesión:
    - Para apps que pueden desvelar información sensible, como "Mensajes" o "Mail", ***se recomienda deshabilitar esta opción***, ya que permite que un tercero no autorizado pueda acceder a los contenidos sensibles

mostrados por las notificaciones sin más que disponer de acceso visual a la pantalla en el momento de la llegada de la notificación.

- Para apps que comunican eventos de seguridad, como apps de banca, o de inicio de sesión (por ejemplo, apps para segundo factor de autentificación), ***la recomendación es habilitarlas***, ya que la recepción de la notificación podrá permitir la detección de usos no autorizados (como pagos realizados, intentos de inicio de sesión, etc.). En estos casos, ***es muy importante fijar el valor a*** "al desbloquear", ya que es habitual que estas notificaciones muestren contenidos sensibles, como los códigos de validación.

- "Mostrar en el centro de notificaciones": permite incluir las notificaciones de la app en el Centro de Notificaciones.
- Si se desea disponer de un elemento que permita de forma sencilla saber si una app tiene notificaciones pendientes, ***se aconseja activar el parámetro*** "Globos en los iconos", que indicará cuántas notificaciones recientes ha emitido la app, frente al uso de previsualizaciones.
- Adicionalmente, las notificaciones de algunas apps pueden acompañarse de un sonido y/o una vibración, pero se permite al usuario controlar este comportamiento a través del los ajuste "Emitir un sonido con las notificaciones".
- "Estilo de las alertas": este campo, situado en la parte superior de los ajustes, determina si la presentación de la notificación interrumpirá al usuario y en qué medida lo hará. Si se selecciona el modo "Alertas", la notificación no desaparecerá de la pantalla hasta que el usuario la cierre o la procese. Por ello, ***debe considerarse el carácter de la información potencialmente expuesta si la notificación queda presente en pantalla durante ciertos periodos de tiempo***.

Al pinchar sobre una notificación se abrirá la app que la generó, normalmente con el foco en el elemento que dio lugar a ella. Mediante el símbolo "x", se descartará la notificación (o pila de notificaciones) correspondiente. ***Se recomienda suprimir las notificaciones no necesarias del Centro de Notificaciones, a fin de no presentar en pantalla información que ya no es útil para el usuario pero que podría desvelar detalles a terceros***.

Para más información sobre el control de notificaciones relativas a sitios web, consultar el apartado "14. Navegador web Safari".

macOS Mojave no dispone de ningún mecanismo que permita al usuario establecer el carácter de las notificaciones de una app.

MODO "NO MOLESTAR"

Permite detener por completo la recepción de notificaciones cuando se activa. La activación puede planificarse de forma puntual o de forma automática en un rango horario definido por el usuario.

Con este modo activo, las notificaciones irán directamente al Centro de Notificaciones, sin mostrase en pantalla y sin interrumpir al usuario.

Desde el punto de vista de seguridad y privacidad, este modo resulta útil en diversas situaciones, por ejemplo, para recibir notificaciones en una situación inoportuna, como durante una sesión de demostración a un tercero. Adicionalmente, ***se aconseja habilitar el interruptor*** "Al duplicar pantalla en televisores y proyectores", que impedirá que las notificaciones se muestren durante una presentación en público.

Es posible habilitar la recepción de llamadas en este modo mediante el parámetro "Permitir llamadas de cualquiera" (macOS no dispone de la granularidad de iOS para este elemento, ya que iOS permite determinar qué llamadas se cursarán: "Favoritos | Nadie | Contactos | Todos"); por su parte, el parámetro "Llamadas repetidas" habilitará la interrupción si un mismo número llama en un intervalo menor de 3 minutos.

MODO "NIGHT SHIFT"

Este modo, que puede ser activado de forma manual desde el "Preferencias del sistema - Pantallas - Night Shift", no afecta en realidad a las notificaciones, sino al espectro de colores que se mostrarán en la pantalla, a fin de que el usuario sufra menos de la exposición a la luz azul en horas nocturnas. Los detalles de la configuración de "Night Shift" están disponibles en la [Ref.- 79].

Desde el punto de vista de la privacidad y la seguridad, el impacto que tiene este servicio está en la selección del parámetro "Preferencias del sistema - Pantallas - [Night Shift] - Programar" a "De la puesta a la salida del sol", ya que este ajuste requiere que la localización esté habilitada para "Servicios del sistema - Zona horaria" (ver apartado "8.2.4.4. Localización"). Para evitar tener que habilitar la localización para este escenario, se aconseja establecer de forma manual el periodo de activación de "Night Shift".

8.5.4 FINDER

La app "Finder" es un explorador de archivos desde el que se realizan multitud de tareas, ya que, además de permitir localizar ficheros y directorios, dispone de una barra lateral con accesos directos a otros servicios, como "AirDrop", "iCloud Drive" y "Ubicaciones" (por ejemplo, elementos habilitados en equipos remotos para compartición de ficheros y mapeados por SMB en el Mac). Pinchando con el botón derecho sobre cualquier archivo en Finder, se despliega un menú con diversos componentes, que incluye la función "Compartir". El uso de Finder se describe en la [Ref.- 131].

Finder ofrece opciones adicionales, o teclas rápidas, que se inician pulsando sobre ciertas teclas a la vez que se selecciona el nombre de un archivo:

- "⌘+I" (Comando + I): despliega la información del fichero, que incluye sus permisos (con posibilidad de modificarlos) y la app con que se abrirá de forma predeterminada (menú "Abrir con" de la imagen izquierda de la <Figura 71>).
- "⌥" (Opción): altera las opciones disponibles al pinchar sobre el elemento con el botón derecho. Por ejemplo, permite copiar el nombre del archivo.

- Mostrar archivos ocultos: por defecto, macOS oculta determinadas ubicaciones y directorios de sistema (con el objetivo de impedir que el usuario realice modificaciones de forma accidental), por lo que no se mostrarán en Finder. Existen diversas alternativas para acceder a estos contenidos desde Finder:
  - Menú "Ir": permite acceder a la carpeta "`Biblioteca`" ("`Library`"), no visible por defecto, siempre que esté activa la opción de Finder "Visualización - Mostrar opciones de visualización - Mostrar carpeta Biblioteca - Usar por omisión".
  - Desde una ventana de terminal añadir el atributo "`defaults write com.apple.finder AppleShowAllFiles TRUE`". Para que se aplique, es preciso cerrar todas las instancias de Finder mediante "`killall Finder`".
  - Mediante la opción "⌘ + ⇧ + ." (`Comando + cambio + .`): permite visualizar temporalmente los archivos ocultos, hasta que se vuelva a teclear esta combinación.
  - Abriendo una ventana de terminal y lanzando el comando "`chflags nohidden <path>`" y, desde Finder, arrastrar la carpeta que tiene archivos ocultos a la ventana del terminal, para que se complete el valor de "`<path>`". Para volver a ocultar los contenidos de la carpeta, se realizará la misma operación con la opción "`chflags hidden <path>`". También es posible utilizar estos comandos sobre archivos o carpetas concretos directamente desde línea de comandos, sin usar Finder.

La mayor parte de ajustes de Finder se pueden modificar a través de su menú "Preferencias" (1), si bien existen algunos ajustes en "Visualización - Mostrar opciones de visualización" (2).

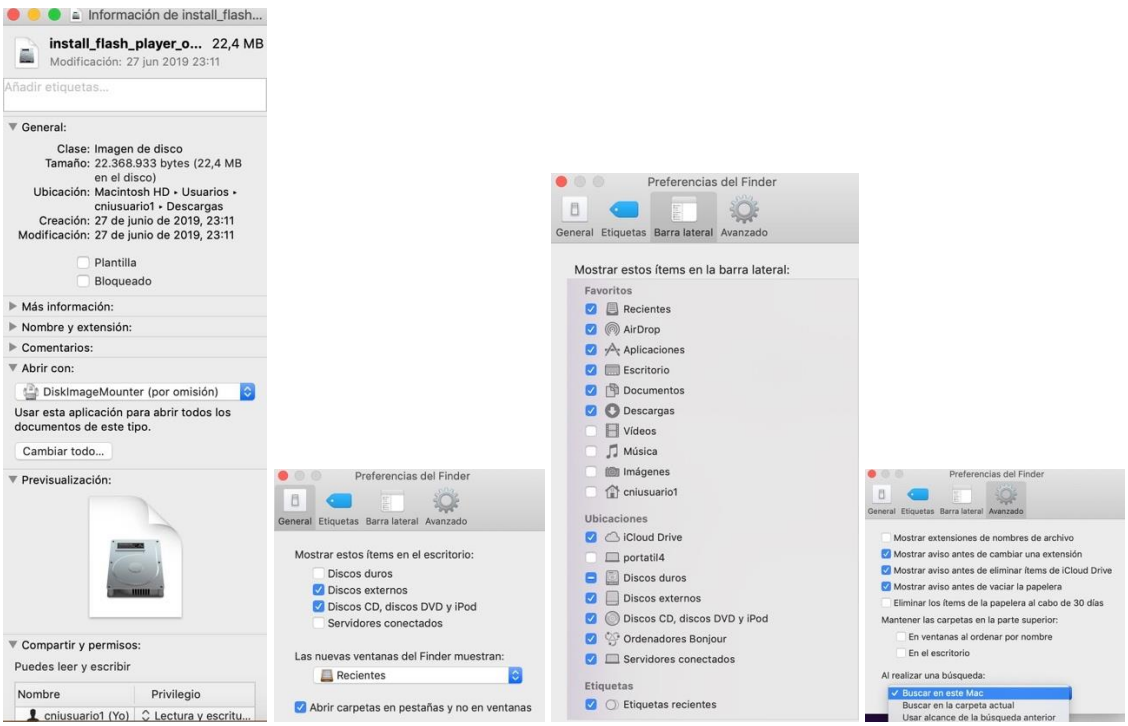


Figura 71 - Ajustes y uso de Finder

Desde el punto de vista de seguridad, ***se recomienda***:

- Añadir a "Favoritos" la carpeta "Home" del usuario: habilitar en el menú (1) la opción "[Barra lateral] Favoritos - cniusuario1 ", correspondiente al nombre de usuario.
- Seleccionar la carpeta "Home" en la barra lateral y habilitar "Mostrar información" y "Mostrar carpeta Biblioteca" en el menú (2), a fin de detectar ficheros que el usuario no reconoce como propios. Si el número de elementos de una carpeta no concuerda con el que se aprecia al acceder a ella, seguir el procedimiento para mostrar archivos ocultos para determinar si existe alguno sospechoso.

8.6 BATERÍA

Mantener un nivel de carga de batería adecuado afecta a la seguridad a la hora de garantizar la disponibilidad del ordenador Mac, especialmente si éste ha sido sustraído y es preciso hacer uso del servicio "Buscar mi Mac".

La carga de la batería (así como su duración estimada, o el tiempo que lleva conectado a la corriente) se puede comprobar mediante la app "Monitor de actividad - [Energía]". Por su parte, el menú "Preferencias del sistema - Economizador" permite configurar ciertos parámetros para optimizar el consumo de batería:

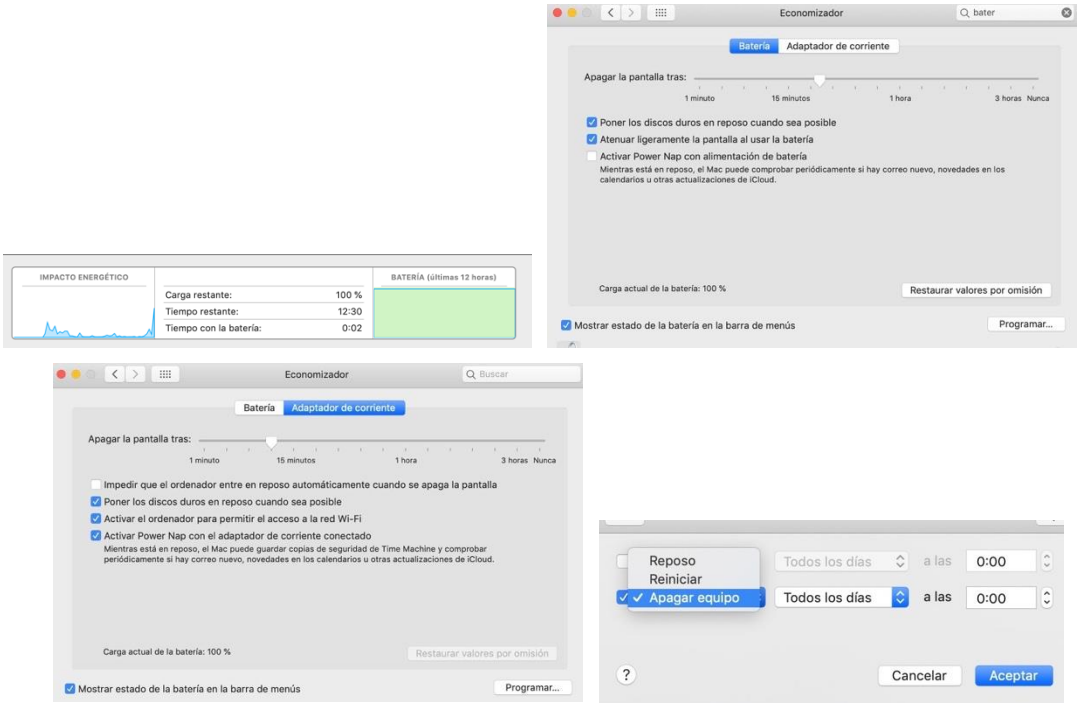


Figura 72 - Informe sobre la carga de la batería y opciones del "Economizador"

Con la opción "Mostrar estado de la batería en la barra de menús" se mostrará el icono "", y, al pinchar sobre él, se indicará qué apps son las que el sistema identifica como principales consumidoras de batería. Esto puede ayudar a aislar problemas de descarga anormal de la batería o de consumo de energía excesivo.

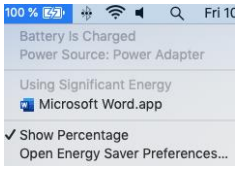


Figura 73 - Visualización de apps consumidoras de energía (en inglés)

El botón "Programar" permite automatizar el apagado y arranque del ordenador. Dado que la recomendación general es cerrar la sesión de usuario tan pronto finalice su utilización, establecer la opción "Apagar equipo" puede ser aconsejable en entornos donde los equipos permanecen en el sitio de trabajo durante la noche, permitiendo que el equipo se apague si el usuario olvidó cerrar sesión y ésta se encuentra activa a la hora definida del apagado. De este modo, si el equipo fuese sustraído y hubiese configurada una contraseña de *firmware* (opción recomendada desde el punto de vista de seguridad según lo descrito en el apartado "18.1. Contraseña de firmware") o el disco estuviese cifrado con FileVault (opción también recomendada según lo descrito en el apartado "15. Cifrado del almacenamiento") el acceso a la información por parte de terceros se vería dificultado.

NOTA: el apagado programado no se efectuará si el Mac ha entrado en estado de reposo, y puede ser interrumpido si existen apps con tareas pendientes, como edición de documentos que no han sido guardados. Por tanto, si la opción "Impedir que el ordenador entre en reposo automáticamente cuando se apaga la pantalla" está desactivada, y ha transcurrido el tiempo definido en la regleta "Apagar la pantalla tras:", el equipo habrá entrado en reposo y no se apagará. Para securizar al máximo este escenario, se recomienda establecer el parámetro "Solicitar contraseña" a "Inmediatamente" en la sección "Seguridad y privacidad - General" (ver apartado "8.2.1. General").

Las recomendaciones generales para los ajustes que afectan al consumo de batería se describen en la sección "Cambiar las preferencias de Economizador en el Mac" del manual de usuario de macOS, accesible desde el símbolo "?" de cualquier submenú de "Preferencias del sistema" y disponible en versión *on-line* en la [Ref.- 98]. En general, se recomienda desactivar los interfaces de comunicaciones (Wi-Fi y Bluetooth) siempre que no se precisen, así como cerrar las aplicaciones que no se estén utilizando, para evitar que realicen operaciones en segundo plano. Es importante tener en cuenta que el pinchar sobre el icono "" no cierra la app, sino que debe emplearse la opción "Salir".

Por otra parte, es importante tener en cuenta que todas las baterías de litio soportan un máximo número de ciclos de carga que condicionan su vida útil. El número de ciclos de carga está disponible desde el menú - Información del Sistema - Hardware - Alimentación - Número de ciclos" [Ref.- 101].

Los parámetros de configuración de la batería se pueden modificar desde la línea de comandos mediante la utilidad "`pmset`".

9. MECANISMOS DE PROTECCIÓN Y TECNOLOGÍAS DE SEGURIDAD EN MACOS

macOS dispone de diferentes mecanismos de protección y tecnologías de seguridad que son añadidas, o mejoradas, con la incorporación de nuevas versiones o nuevas actualizaciones del sistema operativo [Ref.- 44].

9.1 TECNOLOGÍAS GENÉRICAS DE SEGURIDAD

Las tecnologías genéricas de seguridad ampliamente reconocidas en la industria que macOS implementa incluyen:

- XD (*eXecute Disabled*), que permite establecer qué secciones de memoria almacenan datos y cuáles almacenan código y, por tanto, define cuáles pueden ser ejecutadas, excluyendo la posibilidad de ejecutar código desde secciones de datos. Esta protección se aplica tanto a la pila (*stack*) como al *heap*.
- ASLR (*Address Space Layout Randomization*), que 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. Para beneficiarse de esta capacidad, las aplicaciones deben haber sido compiladas con el *flag* PIE (*Position Independent Executable*), lo cual se puede comprobar mediante el comando "`otool`":

```
$ 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    18       1336
NOUNDEFS DYLDLINK TWOLEVEL PIE
```

Figura 74 - Comprobación del flag PIE de un binario

- Kernel ASLR: capacidades de ASLR no solo para las apps, sino para la asignación de secciones de memoria del propio kernel.

9.2 GATEKEEPER Y CUARENTENA DE ARCHIVOS

Se recomienda descargar todas las aplicaciones y software de fuentes de confianza, a través de canales de comunicación seguros, cifrados mediante HTTPS, y que aseguren una correcta validación del certificado digital asociado.

El "*Gatekeeper*" es un servicio con capacidades de validación de archivos a través de firmas digitales y políticas de cuarentena, responsable de supervisar los denominados "controles de acceso obligatorios" (*Mandatory Access Control,* MAC), que son políticas del sistema que las apps deben cumplir para que su ejecución sea permitida.

Las apps descargadas de la App Store son firmadas por Apple antes de ser distribuidas por este medio; para las apps obtenidas de otras fuentes, macOS también verifica la firma del desarrollador y comprueba su validez e integridad.

Para ser considerado como desarrollador identificado por Apple, los desarrolladores deben obtener un identificador de desarrollador (*Developer ID*) [Ref.- 53] de Apple y emplearlo para firmar sus aplicaciones (empleando su clave privada asociada), *plug-ins*, y paquetes de instalación de cara a distribuirlas tanto dentro como fuera de la App Store. Este ID de desarrollador 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. *Gatekeeper* verifica también las librerías externas cargadas adicionalmente junto al paquete de la aplicación [Ref.- 46].

Las políticas de exclusión de *Gatekeeper* afectan a las aplicaciones distribuidas en mercados ajenos a la App Store y a aplicaciones con capacidades de descargar ficheros desde Internet como por ejemplo Safari, o desde fuentes externas, como ficheros adjuntos a un correo electrónico. La verificación de la firma asociada al ID de desarrollador solo aplica a las aplicaciones descargadas de Internet. Las aplicaciones obtenidas de otras fuentes como servidores de archivos en red y unidades de almacenamiento externas, salvo que hubieran sido descargadas originalmente de Internet y aún dispongan de los atributos de cuarentena, están excluidas de *Gatekeeper*.

NOTA: durante la elaboración de la presente guía, en junio de 2019, se publicó una vulnerabilidad de *Gatekeeper*, referenciada también como el exploit "Cavallarin", que permitía a un atacante eludir las restricciones de Gatekeeper mediante la distribución de un fichero ZIP con un enlace simbólico a un servidor en red, lo que hace que no se apliquen las protecciones, al tratarse de una ubicación fuera del ámbito de Gatekeeper:
https://www.fcvl.net/vulnerabilities/macosx-gatekeeper-bypass[18]

La configuración de *Gatekeeper* desde el interfaz gráfico de macOS se encuentra en la sección "Seguridad y privacidad - [General] Permitir apps descargadas de:". Si se intenta instalar una app de una fuente que no cumpla esa configuración, macOS avisará de ello e interrumpirá la instalación, añadiendo a la sección de ajustes un mensaje que informa de cuál ha sido la última app bloqueada. No obstante, el usuario puede forzar la instalación mediante el botón "Abrir igualmente", así como seleccionando desde la app "Finder" el fichero mientras se pulsa la tecla "^" (`Control`) y seleccionando la opción "Abrir", disponible al pinchar con el botón derecho. Para más información sobre la instalación de apps o paquetes provenientes de distintas fuentes, consultar la ayuda oficial de Apple disponible en la [Ref.- 45]:

[18] https://lifehacker.com/how-to-protect-yourself-from-the-new-macos-security-vul-1835845551

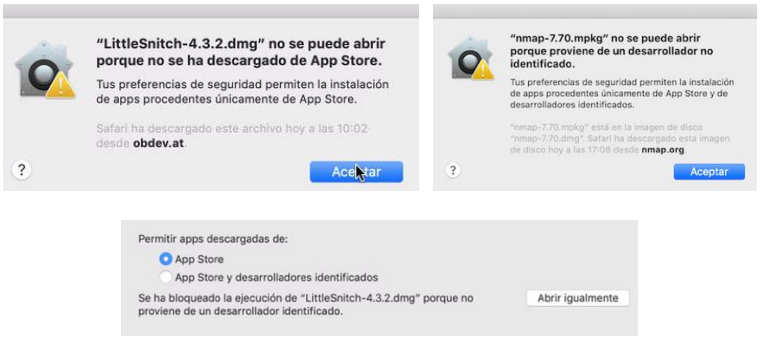


Figura 75 - Configuración de Gatekeeper para bloqueo de aplicaciones

Las aplicaciones que hacen uso de las capacidades de cuarentena de archivos (por ejemplo, Safari, Mensajes, y Mail), asignan los atributos de cuarentena a los ficheros descargados: fecha, hora y un registro de la procedencia del archivo. Estos 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 (rwx), el fichero correspondiente dispone de atributos extendidos. El comando "`ls -l@`" muestra la información general de dichos atributos. Adicionalmente, mediante el comando "`xattr`" (*extended attributes*) es posible consultar todos los contenidos de los atributos extendidos asociados a un archivo, tanto en formato hexadecimal como ASCII, incluidos los atributos de cuarentena:

```
$ ls -l
total 81568
drwxr-xr-x  3 cniusuario1  staff        96 23 abr 03:09 DHS.app
drwxr-xr-x@ 3 cniusuario1  staff        96 23 dic 23:24 KnockKnock.app
-rw-r--r--@ 1 cniusuario1  staff  40847205  5 jun 10:02 LittleSnitch-
4.3.2.dmg
drwxr-xr-x  3 cniusuario1  staff        96 10 mar 02:46 TaskExplorer.app

$ ls -l@ LittleSnitch-4.3.2.dmg
-rw-r--r--@ 1 cniusuario1  staff  40847205  5 jun 10:02 LittleSnitch-
4.3.2.dmg
     com.apple.diskimages.fsck                      20
     com.apple.diskimages.recentcksum                   80
     com.apple.lastuseddate#PS                      16
     com.apple.metadata:kMDItemDownloadedDate           53
     com.apple.metadata:kMDItemWhereFroms      173
     com.apple.quarantine                           57


$ xattr -l LittleSnitch-4.3.2.dmg
com.apple.lastuseddate#PS:
00000000  28 77 F7 5C 00 00 00 00 58 F4 66 1B 00 00 00 00
|(w.....X.f.....|
00000010
com.apple.metadata:kMDItemDownloadedDate:
00000000  62 70 6C 69 73 74 30 30 A1 01 33 41 C1 53 D7 54
|bplist00..3A.S.T|
...  |................|
00000030  00 00 00 00 13                                    |.....|
00000035
com.apple.metadata:kMDItemWhereFroms:
00000000  62 70 6C 69 73 74 30 30 A2 01 02 5F 10 45 68 74
|bplist00..._.Eht|
00000010  74 70 73 3A 2F 2F 6F 62 64 65 76 2E 61 74 2F 66
|tps://obdev.at/f|
00000020  74 70 2F 70 75 62 2F 50 72 6F 64 75 63 74 73 2F
```

```
|tp/pub/Products/|
00000030  6C 69 74 74 6C 65 73 6E 69 74 63 68 2F 4C 69 74
|littlesnitch/Lit|
00000040  74 6C 65 53 6E 69 74 63 68 2D 34 2E 33 2E 32 2E  |tleSnitch-
4.3.2.|
00000050  64 6D 67 5F 10 34 68 74 74 70 73 3A 2F 2F 6F 62
|dmg_.4https://ob|
00000060  64 65 76 2E 61 74 2F 70 72 6F 64 75 63 74 73 2F
|dev.at/products/|
00000070  6C 69 74 74 6C 65 73 6E 69 74 63 68 2F 64 6F 77
|littlesnitch/dow|
00000080  6E 6C 6F 61 64 2E 68 74 6D 6C 08 0B 53 00 00 00
|nload.html..S...|
00000090  00 00 00 01 01 00 00 00 00 00 00 00 03 00 00 00
|................|
000000A0  00 00 00 00 00 00 00 00 00 00 00 00 8A           |.............|
000000ad
com.apple.quarantine: 0083;5cf77728;Safari;48786886-3233-4ADF-B052-
67F6BB31F5F0
```

Figura 76 - Atributos de cuarentena de un fichero

También es posible obtener el valor de los diferentes atributos en formato PLIST, (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 LittleSnitch-4.3.2.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://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<array>
     <date>2019-06-05T08:02:48Z</date>
</array>
</plist>
```

Figura 77 - Obtención de los atributos de un fichero en formato PLIST

Al abrir por primera vez un fichero con atributos de cuarentena asociados, macOS informa al usuario de su procedencia a través de un cuadro de diálogo y solicita autorización para abrirlo. El mensaje incluye la fecha en que fue descargado, desde qué servidor web y qué aplicación lo descargó:

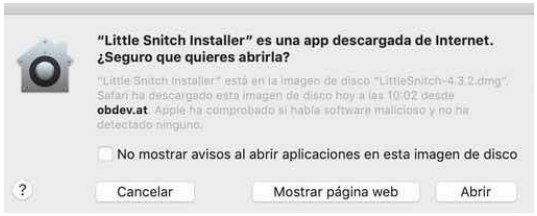


Figura 78 - Mensaje de alerta al abrir un fichero con atributos de cuarentena

Solo el usuario que descargó el archivo, y el usuario administrador, tienen la capacidad de eliminar los atributos de cuarentena del archivo mediante el comando "`xattr -c <fichero>`".

Una vez el fichero ya ha sido abierto la primera vez, macOS no volverá a solicitar autorización al usuario, para lo cual modificará sus atributos de cuarentena.

```
$ xattr -l WhatsYourSign\ Installer.app/
com.apple.quarantine: 0083;5cf77c17;Safari;F9A3A0C2-C130-45A0-80A4-
0CE05E74FD67

--- Tras aceptar la apertura del fichero la primera vez ---

$ xattr -l WhatsYourSign\ Installer.app/
com.apple.quarantine: 00c3;5cf77c17;Safari;F9A3A0C2-C130-45A0-80A4-
0CE05E74FD67
```

Figura 79 - Modificación de los atributos de cuarentena tras abrir un fichero por primera vez

Gatekeeper almacena una lista blanca de *hashes* (denominados CDHash), que contiene los *hashes* asociados a las aplicaciones que Apple ha considerado de confianza a lo largo del tiempo, y que está disponible en el fichero de base de datos SQLite 3.x "`/var/db/gkopaque.bundle/Contents/Resources/gkopaque.db`". El valor del CDHash de una aplicación puede ser obtenido a través de la utilidad "`codesign`", lo cual permite determinar si su CDHash está incluido en la lista blanca de Gatekeeper. En el caso de Mojave, el hash de muchas de las apps estándar de macOS curiosamente no está incluido en esta base de datos, pese a contener más de 74.000 entradas en la lista blanca:

```
$ codesign -dvvv /Applications/Home.app 2>&1 | grep CDHash
CandidateCDHash sha256=2d391ffb7fb00e921343347b79a7165d6741f297
CDHash=2d391ffb7fb00e921343347b79a7165d6741f297

$ sqlite3 /var/db/gkopaque.bundle/Contents/Resources/gkopaque.db "select
quote(current), quote(opaque) from whitelist" | grep -i
2d391ffb7fb00e921343347b79a7165d6741f297

$ sqlite3 /var/db/gkopaque.bundle/Contents/Resources/gkopaque.db "select
COUNT(*) from whitelist"
74245
```

Figura 80 - Verificación del CDHash de una app a través de codesign

Gatekeeper utiliza la "aleatorización de rutas". Este mecanismo hace que las apps descargadas queden en una ubicación de solo lectura antes de ser ejecutadas, impidiendo que accedan a rutas relativas o que se actualicen si se lanzan desde esta ubicación. Es importante añadir que, si la app se traslada mediante Finder a otra carpeta, este mecanismo dejará de ser efectivo (ver sección "*Gatekeeper*" de la [Ref.-58]).

El *Gatekeeper* controla también las conexiones que una app realiza a través del *firewall* ALF suministrado con macOS (ver apartado "8.2.2. Firewall (Cortafuegos)").

En ocasiones, tras una actualización de una app a través de Internet, macOS puede presentar la siguiente advertencia al usuario, solicitando su confirmación al abrir la app por primera vez:

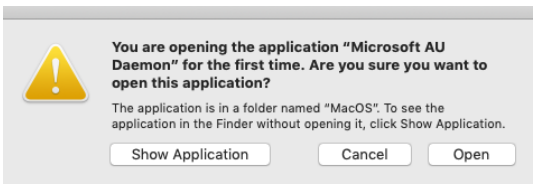


Figura 81 - Solicitud de confirmación para abrir una app por primera vez

9.2.1 SERVICIO DE NOTARÍA

macOS 10.14 introduce el servicio de "notaría", por el cual los desarrolladores pueden remitir las aplicaciones firmadas con su ID de desarrollador a Apple para que Apple realice comprobaciones de seguridad sobre éstas. Si estas comprobaciones son exitosas, Apple añadirá un "*ticket*" al *software* o app atestiguando su confiabilidad, que será utilizado por el *Gatekeeper*: cuando el usuario ejecute la app, se mostrará una ventana de diálogo que informará al usuario de que Apple lo ha escaneado sin encontrar *malware*.

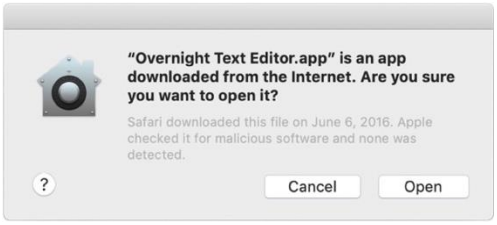


Figura 82 - Mensaje de Gatekeeper al abrir una app certificada mediante el servicio de notaría

El ticket puede validarse *on-line* por parte del Gatekeeper si existe conexión a Internet durante la primera ejecución de la app; si no, validará el ticket "grapado" (*stapled*) a la app.

Para remitir un *software* al servicio de notaría de Apple, el desarrollador deberá utilizar Xcode [Ref.- 54].

9.2.2 GESTIÓN DEL GATEKEEPER DESDE LÍNEA DE COMANDOS

La herramienta "`spctl`" (*Security Assessment o SecAssesment system policy security*) permite la gestión de *Gatekeeper* desde línea de comandos [Ref.- 47]. Por ejemplo, esta utilidad 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 (primer comando de la <Figura 83>).
- Conocer qué apps han sido aprobadas explícitamente por el usuario (a través del segundo comando de la <Figura 83>).
- Habilitar y deshabilitar el *Gatekeeper*: mediante las opciones "`--master-enable`" y "`--master-disable`", respectivamente. La primera de ellas permitirá aplicaciones de la App Store y de desarrolladores identificados.
- Aprobar o bloquear determinadas aplicaciones, asignándoles etiquetas y habilitando o deshabilitando estas etiquetas (<Figura 84>).

```
$ spctl -vva KnockKnock.app/
KnockKnock.app/: accepted
source=Notarized Developer ID
origin=Developer ID Application: Objective-See, LLC (VBG97UB4TA)

$ sudo spctl --list| grep -i UNLABELED
2714[UNLABELED] P0 allow execute [/Users/cniusuario1/Downloads/platform-
tools/adb]
```

Figura 83 - Obtención de información del Gatekeeper a través de spctl

```
$ spctl --add --label "AppsPermitidas" /Users/cniusuario1/Downloads/App1.app
$ spctl --enable --label "AppsPermitidas"

$ spctl --add --label "AppsProhibidas" /Users/cniusuario1/Downloads/App2.app
$ spctl --disable --label "AppsProhibidas"
```

Figura 84 - Aprobación/denegación de apps a través de spctl

NOTA: La herramienta de libre uso "DHS" (Dylib Hijack Scanner) de Objective-see© permite identificar tanto aplicaciones susceptibles de ser vulnerables a inyección de librerías dinámicas (dylib), como escenarios de ataque donde 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

Por su parte, la herramienta "Task Explorer", similar al "Monitor de Actividad", permite explorar todos los procesos en ejecución de macOS 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, y tiene integración con VirusTotal.

"Task Explorer" muestra el árbol jerárquico de procesos para 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

9.3 XPROTECT: SOFTWARE MALICIOSO (*MALWARE*)

A través de la tecnología XProtect, integrada en la funcionalidad "*Gatekeeper*", macOS comprueba, a la hora de abrir un fichero con atributos de cuarentena asociados, si contiene software malicioso (*malware*) conocido[19]. En caso afirmativo, se mostrará una alerta al usuario con el texto "(Nombre del archivo) dañará tu ordenador. Deberías enviarlo a la papelera" [Ref.- 49].

Apple mantiene una lista con definiciones de software malicioso conocido (lista negra), que se emplea durante el proceso de verificación de los ficheros descargados. Esta lista se almacena localmente en el fichero "`/System/Library/CoreServices/XProtect.bundle/Contents/Resources/XProtect.plist`" y se actualiza periódicamente, por lo que es posible verificar la fecha de la última actualización del fichero con las definiciones de software malicioso.

Adicionalmente, para limitar la exposición frente a amenazas, XProtect también define controles respecto a las versiones de los *plug-ins* 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
```

Figura 85 - Lista negra de XProtect para plugins asociados a los navegadores web

[19] Al igual que sucede con la operativa de Gatekeeper, la detección de software malicioso de XProtect solo aplica a las aplicaciones descargadas de Internet. Las aplicaciones obtenidas de otras fuentes, como servidores de archivos en red y unidades de almacenamiento externas, quedan excluidas.

Apple ha integrado el proceso de actualización de XProtect en el proceso estándar de actualizaciones de sistema operativo, por lo que se lleva a cabo mediante la utilidad "`softwareupdate`". La opción no documentada "`--background-critical`" permite forzar la verificación y actualización del fichero de definición de software malicioso de XProtect[20]. El resultado de su invocación se puede supervisar mediante el comando "`tail -f /var/log/install.log`".

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.- 48].

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. Se dispone de detalles sobre las versiones mínimas permitidas para los *plug-ins* bloqueados en los ficheros públicos oficiales de configuración asociados, por ejemplo desde la web de Apple: "`http://configuration.apple.com/configurations/macosx/xprotect/3/clientConfiguration.plist`".

Complementariamente a XProtect, desde la versión 10.8.3 de macOS, se dispone de la tecnología MRT (*Malware Removal Tool*). MRT ejecuta automáticamente de fondo como demonio, verificando y eliminando software malicioso detectado en el equipo, y que haya podido comprometerlo evitando los mecanismos de protección previos, o por otras vías, por ejemplo, explotando vulnerabilidades en los *plug-ins* del navegador web, como Java o Flash. La app "`MRT.app`" reside en "`/System/Library/CoreServices`", y puede lanzarse como agente mediante:

```
$ /System/Library/CoreServices/MRT.app/Contents/MacOS/MRT -a
2019-06-05 01:06:50.921 MRT[1024:15812813] Running as agent
2019-06-05 01:06:51.079 MRT[1024:15812813] Agent finished.
2019-06-05 01:06:51.080 MRT[1024:15812813] Finished MRT run
```

Figura 86 - Ejecución de MRT como agente

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.

A fecha de elaboración de la presente guía, la última versión de MRT disponible era la 1.41[21]. Apple no proporciona detalles sobre los mecanismos de verificación de MRT[22], ni tampoco sobre los especímenes de *malware* que incluye.

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

[21] https://eclecticlight.co/2019/05/02/apple-has-pushed-updates-to-both-xprotect-and-mrt/

[22] https://www.sentinelone.com/blog/apples-malware-removal-mrt-tool-update/

9.4 SANDBOX

El concepto de "*sandbox*" (contenedor) hace referencia a una tecnología que pretende aislar o confinar las aplicaciones, a fin de que solo ejecuten las acciones que se espera de ellas sin interferir con otros componentes críticos del sistema, con los datos de usuario y/o con otras aplicaciones. De este modo, si una aplicación es comprometida por software malicioso, el *sandbox* restringe qué componentes se ven afectados. Las apps eligen cómo limitar el acceso a los recursos a través de los *entitlements* (privilegios) que declaran [Ref.- 56].

El modelo de *sandbox* de macOS proporciona un nivel de seguridad adecuado siempre que no se identifiquen vulnerabilidades a nivel de *kernel* que permitan evitar sus mecanismos de protección y "escapar" del sandbox [Ref.- 48].

Las capacidades del *sandbox* de macOS están disponibles por defecto para las apps proporcionadas con el sistema operativo (por ejemplo, la App Store, Mensajes, Calendario, Contactos, Diccionario, Photo Booth, vistas rápidas (*Quick Look Previews*), Notas, Recordatorios, Safari, Mail y FaceTime) y para otras apps descargadas de la App Store.

Las apps que ejecutan como contenedor no disponen de permiso para escribir en cualquier lugar del sistema de ficheros (por ejemplo, "`/Library/Preferences`"), sino que macOS traducirá sus peticiones de escritura de forma que se lleven a cabo sobre el directorio de la app bajo "`~/Library/Containers`".

Para las apps desarrolladas por terceros, las APIs de *sandboxing* permiten especificar las acciones que una app realizará durante su ejecución normal. El sistema velará por que la app no ejecute acciones fuera de esa lista (por ejemplo, una app editora de texto no debería establecer conexiones de red).

La combinación de técnicas de *sandboxing* con la estructuración de apps en servicios XPC (ver apartado "7.1. Demonios, agentes y servicios XPC") facilita que la funcionalidad de cada servicio sea limitada y disminuye las acciones que un atacante puede realizar si compromete la app (por ejemplo, separando la escritura/lectura en disco del acceso a la red).

El mecanismo TCC introducido por macOS Mojave (ver apartado "8.2.4. TCC: Transparency, Consent and Control") extiende el modelo de *sandboxing* para que cualquier aplicación, y no solo las apps descargadas de la App Store, se beneficien del esquema de protección.

Mojave[23] introduce nuevas características en Xcode 10, que imponen validación de librerías, limitaciones de depuración y restricciones para que solo el código firmado pueda ejecutar, dificultando así operaciones llevadas a cabo por los atacantes para comprometer aplicaciones y escalar privilegios en el sistema.

[23] https://devblogs.microsoft.com/xamarin/macos-hardened-runtime-notary/

LIMITACIONES DE DEPURACIÓN

Desde macOS 10.14, el depurador de macOS exige el privilegio "`com.apple.security.get-task-allow`" para permitir depurar la app en Xcode o mediante "`/usr/bin/lldb`". Este privilegio se añade de forma automática por parte de Xcode cuando se compila una app, pero solo para su desarrollador (no se añade si se exporta la app para su distribución). Cuando se intenta acceder al depurador, se solicitará la contraseña de administrador, o haberse autentificado a través de la utilidad "`/usr/sbin/DevToolsSecurity -enable`".

HARDENED RUNTIME

Esta característica, disponible en Xcode 10, permite compilar una aplicación añadiendo un *flag* especial de protección. Si se intenta depurar esta aplicación y SIP está habilitado (ver apartado "9.10. SIP: System Integrity Protection"), el entorno Cocoa aplicará una serie de restricciones:

- Denegación de ejecución si el código ha sido automodificado.
- Impedimento de cargar librerías dinámicas no firmadas.

Estas restricciones pueden ser evitadas por parte del desarrollador de la app a través del uso de los *entitlements* (privilegios), por ejemplo "`com.apple.security.get-task-allow`". En caso contrario, el depurador no podrá enlazarse al proceso[24]. Para más información, consultar [Ref.- 55].

El uso del "*Hardened Runtime*" es obligatorio para las apps que quieran acceder al servicio de notaría (ver apartado "9.2.1. Servicio de Notaría").

9.5 FIRMA Y VERIFICACIÓN DE APLICACIONES Y DEL KERNEL

macOS 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 o entorno de ejecución de macOS, el sistema abortará la ejecución del proceso asociado.

Las capacidades de firma digital de código son empleadas por macOS 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.

También el código del sistema operativo, así como sus extensiones de *kernel*, debe estar firmado para poder ser ejecutado, con el objetivo de evitar la ejecución de componentes no autorizados con el máximo nivel de privilegios del sistema operativo (*ring 0* o *kernel*).

macOS introdujo en High Sierra 10.13.2 el concepto de "*Secure Kernel Extension Loading, SKEL*" (carga segura de extensiones de *kernel*), un servicio que actúa como guardián, permitiendo que solo se ejecuten las extensiones de *kernel* pre-aprobadas, ya sea por parte del usuario (de forma interactiva) o a través de un perfil de

[24] https://lapcatsoftware.com/articles/debugging-mojave.html

configuración (en entornos MDM). En este sentido, es importante reseñar que no se requiere autorización para las extensiones que reemplacen a una extensión previamente aprobada, ni para las existentes en un ordenador con una versión de macOS anterior a la 10.13. En las [Ref.- 58] y [Ref.- 59] se puede consultar el detalle de esta funcionalidad.

Las extensiones del *kernel* añaden funcionalidad al núcleo del sistema operativo (como los antivirus), y son cargadas dinámicamente por el demonio "`kextd`"; el comando "`kextstat`" proporciona información sobre su estado.

La funcionalidad de carga de extensiones de *kernel* aprobadas por el usuario podría deshabilitarse (***desaconsejado desde el punto de vista de seguridad***), invocando el comando "`spctl kext-consent disable`" desde el modo de arranque de recuperación. Esta acción podría llevarse a cabo por parte de cualquier usuario, por lo que se aconseja proteger la NVRAM mediante una contraseña de *firmware*. Puede comprobarse el estado actual con el comando "`spctl kext-consent status`".

NOTA: en el *post* "High Sierra's 'Secure Kernel Extension Loading' is Broken" de Objective-See© se describe una forma de evitar el mecanismo de SKEL. URL: https://objective-see.com/blog/blog_0x21.html.

Adicionalmente, en macOS Mojave se exige que las extensiones de *kernel* hayan pasado por el servicio de notaría (ver apartado "9.2.1. Servicio de Notaría"), a menos que hayan sido incluidas en el fichero "`ExceptionLists.plist`". Mojave incluye también un fichero "`AppleKextExcludeLList.kext`", en el que se recogen extensiones de *kernel* reconocidas por originar *panics*, y que no serán cargadas por el sistema operativo[25].

NOTA: el análisis de la funcionalidad y de todas las capacidades de firma digital de código en macOS, orientadas principalmente a desarrolladores de aplicaciones para macOS, queda fuera del alcance de la presente guía. Para más información, se recomienda consultar la [Ref.- 57].

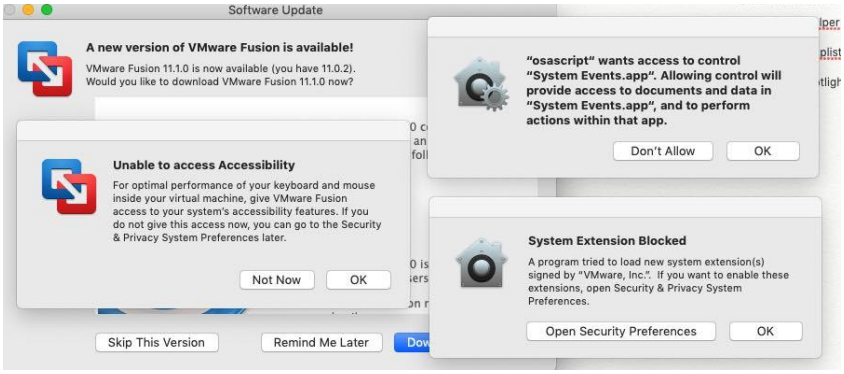


Figura 87 - Detección de un intento de carga de una extensión de kernel en macOS

Cuando se bloquea por parte de macOS la carga de una extensión de kernel, el usuario puede aprobarla manualmente desde la sección de ajustes "Preferencias del Sistema - Seguridad y privacidad - General".

[25] https://eclecticlight.co/2019/05/13/mojave-10-14-5-changes-kernel-extension-security/

Una vez instalada una extensión de *kernel* incluida por una app de terceros, puede descargarse mediante la utilidad "`kextunload -b`".

9.6 TOUCH BAR Y TOUCH ID

Desde 2016, algunos modelos de MacBook Pro incorporan el denominado "Touch ID", botón que reemplaza al botón de arranque y que incorpora un lector de huella dactilar digital que permite autentificar al usuario con su huella en lugar de mediante credenciales (una vez ya ha iniciado sesión tras el arranque del equipo), tanto para acceder a ciertos elementos del sistema que requieran de autentificación (por ejemplo, la sección "Contraseñas" de Safari) como para compras en las "Store(s)" (App, iBooks e iTunes) de Apple y en Apple Pay. El acceso de administración a las secciones de ajustes "Seguridad y Privacidad" y "Usuarios y grupos" sigue requiriendo acreditación mediante contraseña si FileVault está activado. La configuración de Touch ID puede consultarse en la [Ref.- 70].

Por su parte, la "Touch Bar" es una barra táctil situada en la parte superior del teclado, que se adapta a las operaciones que esté realizando en cada momento el usuario y proporciona controles específicos sobre estas operaciones (por ejemplo, control de volumen, menú "Compartir", desplazamiento entre elementos, etc.). Los detalles de su configuración están disponibles en la [Ref.- 71].

Los ordenadores Mac equipados con Touch Bar y Touch ID hasta 2018 incluyen, además del procesador principal Intel, un chip T1, en el que reside el "*Secure Enclave*" (ver apartado "9.6.1. Secure Enclave Processor (SEP)"). Los modelos fabricados a partir de 2018 se comercializan con el nuevo chip T2 [Ref.- 42], que añade un coprocesador al "*Secure Enclave*" que, además de proteger los datos de biometría, es responsable del nuevo nivel de seguridad asociado a FileVault 2 y del arranque seguro.

9.6.1 SECURE ENCLAVE PROCESSOR (SEP)

El "*Secure Enclave Processor*" (SEP) es un coprocesador de seguridad en el que se apoya el cifrado del almacenamiento mediante FileVault y APFS, el mecanismo de arranque seguro o "*Secure Boot*" (ver apartado "18.9. Secure Boot") y el "Touch ID" (ya que es responsable del manejo de la información biométrica, incluyendo las transacciones involucradas en el mecanismo de Touch ID [Ref.- 43]). Apple permite que apps de terceros también almacenen claves en él, pero de forma que estas apps nunca tendrán acceso a las propias claves, lo que dificulta que sean comprometidas.

Este elemento ejecuta al margen del sistema operativo, ya que dispone de su propio *microkernel* (denominado "eOS", basado en "watchOS") que realiza un proceso de arranque seguro propio (lo cual añade seguridad ante un eventual compromiso del sistema operativo) y de una memoria *flash* de 4MB cifrada en la que únicamente se almacenan claves privadas de 256 bits de curva elíptica que nunca abandonan el SEP. Estas claves son las que se utilizan para acceder a los datos de biometría, que no residen en el SEP.

El *Secure Enclave* está diseñado para crear y custodiar claves localmente, no permitiendo importarlas desde, o exportarlas hacia, otros equipos.

Cuando arranca, el *Secure Enclave* genera una clave de cifrado de un solo uso y la ofusca con un UID. Esta clave se combina con un contador para impedir la manipulación de los datos que se escriben en el almacenamiento NAND.

NOTA: aunque en agosto de 2017 unos investigadores revelaron una clave para descifrar el *firmware* del SEP[26], hasta la fecha no ha sido posible acceder a los datos almacenados en él.

9.7 GESTIÓN DE LLAVEROS

Hoy en día son muchos los servicios web que requieren que el usuario se registre e inicie sesión para acceder a ellos. Esto conlleva que los usuarios deban llevar registro de multitud de credenciales, por lo que es común que se haga uso de malas prácticas, como reutilizar contraseñas, elegir credenciales poco robustas, o apuntarlas en sitios poco seguros.

El uso de gestores de contraseñas, como el llavero de macOS, simplifica enormemente la tarea de recordar (incluso de rellenar automáticamente) credenciales y otros datos considerados sensibles, por ejemplo, identificadores del usuario o certificados digitales. También permiten almacenar datos de formularios (como direcciones para un contacto) e información de tarjetas de crédito. Por ello, en términos generales, el uso de llaveros ayuda a evitar las malas prácticas anteriormente citadas.

Desde el punto de vista de su ubicación, los llaveros pueden residir en:

- Un servicio en la nube (como el llavero de iCloud): permiten que los elementos almacenados en el gestor o llavero estén disponibles para el usuario en todos los dispositivos vinculados a una determinada cuenta de usuario de iCloud. Su ventaja desde el punto de vista de la usabilidad es clara, ya que no requieren que el usuario tenga que almacenar en distintos repositorios los mismos elementos. Su desventaja principal viene desde el punto de vista de seguridad ya que, si la cuenta del usuario de iCloud donde se almacenan los datos del gestor (o la base de datos del gestor) es comprometida, un potencial atacante tendrá acceso remoto a todos los elementos almacenados.
- En el almacenamiento interno de un equipo: son accesibles únicamente desde el equipo en el que residen.

Para encontrar un compromiso entre la seguridad y la usabilidad, con respecto a los gestores de contraseñas en general, y los llaveros de macOS, ***se recomienda***:

- ***Elegir un llavero residente en el almacenamiento interno***, de forma que se requiera acceso físico al equipo para entrar en la app de gestión de credenciales.

[26] https://github.com/xerub/img4lib

- ***Proteger el acceso al llavero con una contraseña robusta***, que no se anote en ningún sitio ni se reutilice en ningún otro servicio, ***preferiblemente asociada a un nombre de usuario/e-mail de usuario empleado exclusivamente para este servicio***, a fin de que un potencial atacante no pueda extrapolarlo a partir de otros elementos, como un correo electrónico de uso general.
- Elegir un gestor de contraseñas que ***permita usar un segundo factor de autentificación (2FA)***, y configurarlo para que lo requiera obligatoriamente.
- Analizar la arquitectura de seguridad del llavero a implantar: entre otros elementos, se debe asegurar que cifre sus contenidos de forma segura y que no haya presentado vulnerabilidades críticas en el pasado.
- ***Mantener las contraseñas más sensibles fuera del llavero***, la cuenta de usuario vinculada al Apple ID y el servicio iCloud, correo electrónico, servicios corporativos, servicios de banca on-line y servicios relacionados con la salud.

9.7.1 LLAVERO (KEYCHAIN)

El llavero de macOS (*Keychain*) es un gestor de información considerada sensible que reside en una base de datos cifrada que existe en macOS desde principios de los años 90. Los llaveros pueden albergar contraseñas para acceder a sitios web, recursos de red, credenciales para acceso a redes Wi-Fi, contraseñas de cifrado de discos, certificados digitales (de usuario y de CA), notas seguras, etc.

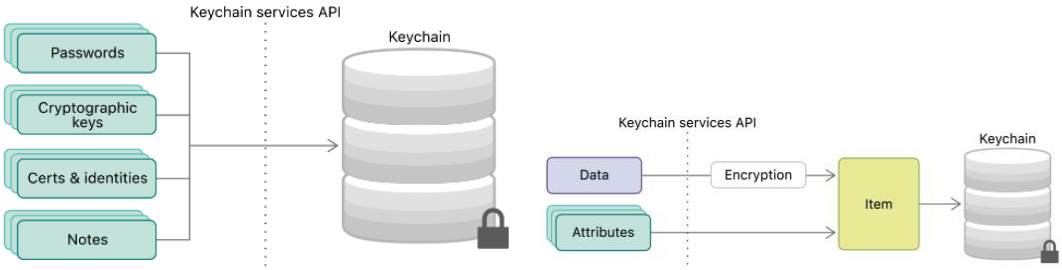


Figura 88 - Esquema de un llavero de macOS [Ref.- 69]

El objetivo del uso de este llavero es favorecer la usabilidad del sistema, evitando la solicitud de introducción de credenciales de acceso a servicios y apps. Las apps pueden almacenar sus elementos sensibles (certificados, credenciales, etc.) en el llavero, y macOS emplea listas de control de acceso (*Access Control Lists,* ACL) para que cada app pueda acceder solo a sus elementos dentro del llavero, y no a los de otras apps.

Cada usuario del sistema tiene sus propios llaveros, asociados de forma dinámica a sus credenciales, de forma que, al iniciar sesión, el llavero se desbloquea y sus elementos quedan disponibles para el sistema operativo y las aplicaciones particulares.

El llavero principal se crea cuando se añade un usuario, y su contraseña coincidirá con la de inicio de sesión. Si el usuario modifica su contraseña de inicio de sesión, macOS actualizará automáticamente la contraseña del llavero (si es el administrador el que cambia la contraseña de inicio de sesión del usuario, la contraseña del llavero no se actualiza, por lo que seguirá coincidiendo con la última

que haya fijado el propio usuario). Si es preciso restablecer la contraseña de inicio de sesión por olvido del usuario, se creará un nuevo llavero.

Algunos elementos del llavero, como las URLs, se almacenan en texto plano, mientras que los elementos sensibles (contraseñas, notas seguras, etc.) se almacenan cifrados con Triple DES. Para acceder a estos elementos sensibles, el usuario deberá introducir la contraseña del llavero que los contiene. Cada elemento almacenado en el llavero lleva asociada una instancia que contiene una lista de control de acceso (ACL), de forma que, cuando una app intenta acceder a dicho elemento, el sistema consulta la ACL y responde en consecuencia. Las ACLs se asocian a llaveros locales, no al llavero de iCloud[27]. Adicionalmente, la app que añade un elemento a un llavero puede establecer limitaciones de acceso a dicho elemento asociadas al estado de bloqueo del equipo (por ejemplo, acceso solo si el equipo está desbloqueado, acceso siempre tras el primer desbloqueo de sesión, etc.).

macOS dispone por defecto de tres llaveros, enumerados a continuación, que corresponden a ficheros cifrados en los que se almacena la información sensible. Adicionalmente, se muestra en la lista de llaveros el repositorio de autoridades certificadoras raíz de confianza proporcionados por macOS ("**Raíz del sistema**"):

- **Inicio de sesión** (*login*): contiene los elementos que están disponibles para un usuario una vez inicia sesión en el equipo (por ejemplo, los vinculados al Apple ID y a los servicios de iCloud). Sus ficheros residen en "`~/Library/Keychains`". La contraseña que protege este llavero es la misma que la del usuario, ya que este llavero se crea durante la configuración inicial de su cuenta. Por ello, este llavero se desbloquea automáticamente cuando se inicia sesión[28].
- **Ítems locales**: alberga los elementos que el usuario ha elegido salvar en el llavero explícitamente, por ejemplo, en servicios web. También se almacenan en él las contraseñas de las redes Wi-Fi configuradas en macOS.
  Está disponible bajo "`~/Library/Keychains/<GUID>/`", donde "`<GUID>`" (*Generated UID*) es un identificador único creado por macOS. Dentro de esta carpeta se encuentran, entre otros, los ficheros "`keychain-2.db`" (base de datos SQLite) y "`user.kb`".
- **Sistema**: contiene elementos para servicios del sistema, disponibles para todos los usuarios del equipo. Reside en "`/Library/Keychains/System.keychain`".

En los equipos que disponen de "Secure Enclave" (ver apartado "9.6.1. Secure Enclave Processor (SEP)"), éste se emplea para proteger las claves privadas.

9.7.2 APP "ACCESO A LLAVEROS"

Los llaveros de macOS se pueden gestionar a través de la app "Acceso a Llaveros" ("Keychain Access"), disponible bajo "Aplicaciones - Utilidades". Bajo la sección

[27] https://developer.apple.com/documentation/security/keychain_services/access_control_lists

[28] Puede ocurrir que se produzca una desincronización entre la contraseña del llavero y la de inicio de sesión. En ese caso, consultar la [Ref.- 62].

"Categoría" (a la izquierda) se agrupan los tipos de elementos que pueden almacenarse en los llaveros. Para cada elemento protegido por el llavero es posible especificar una política de control de acceso, que establece:

- Qué aplicaciones pueden acceder a ese elemento.
- Si se debe solicitar confirmación por parte del usuario antes de permitir el acceso al elemento.
- Si se deberá solicitar al usuario la contraseña del llavero para permitir el acceso: ésta es la opción recomendada desde el punto de vista de seguridad, particularmente para llaveros que almacenan información muy sensible. Para el resto, debe buscarse el equilibrio entre usabilidad y seguridad.

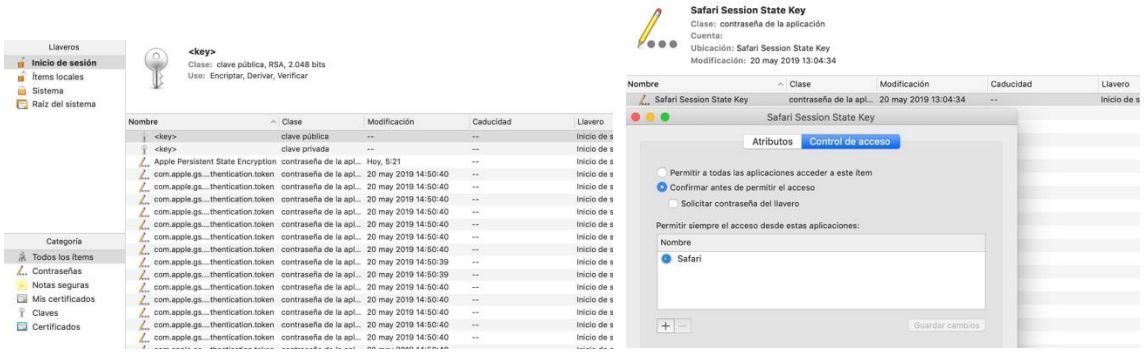


Figura 89 - App "Acceso a llaveros"

La app "Acceso a Llaveros" permite crear:

- Nuevos llaveros, independientes del llavero por omisión de inicio de sesión (login), a través del menú "Archivo - Nuevo llavero…", con lo cual se creará un nuevo fichero bajo "`~/Library/Keychains/<nombre>.keychain`".
- Nuevos elementos dentro de un llavero: adicionalmente, incorpora un asistente para la generación de contraseñas robustas, disponible desde el icono "🔑" junto al campo "Contraseña" del menú de creación de un nuevo elemento del llavero:

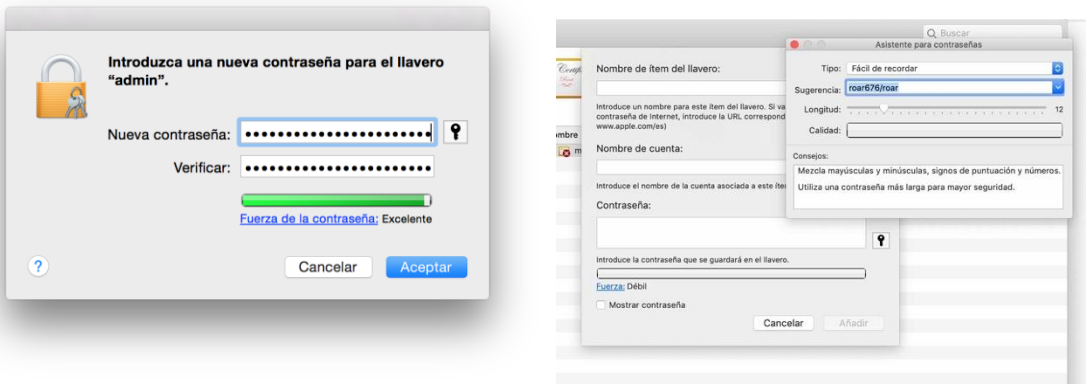


Figura 90 - Creación de un llavero y de un elemento en el llavero mediante la app "Acceso a llaveros"

Durante el proceso de creación de un nuevo llavero se deberá proporcionar una contraseña con la que 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 sea diferente a la contraseña de inicio de sesión***, ***y a la de cualquier otro llavero***, a fin de minimizar el impacto ante un compromiso.

Si el llavero no está protegido con una contraseña, cualquier tercero con acceso a la cuenta del usuario podría consultar toda la información sensible almacenada en él. Por tanto, ***se recomienda que todos los llaveros estén protegidos por una contraseña robusta, y establecer opciones de bloqueo automático*** mediante la opción "Cambiar ajustes del llavero <nombre>" que se obtiene pulsando sobre el botón derecho sobre él. A través de este menú es posible también bloquear manualmente el llavero, al igual que desde el menú "Acceso a llaveros - Archivo", que permite bloquear instantáneamente todos los llaveros del usuario.

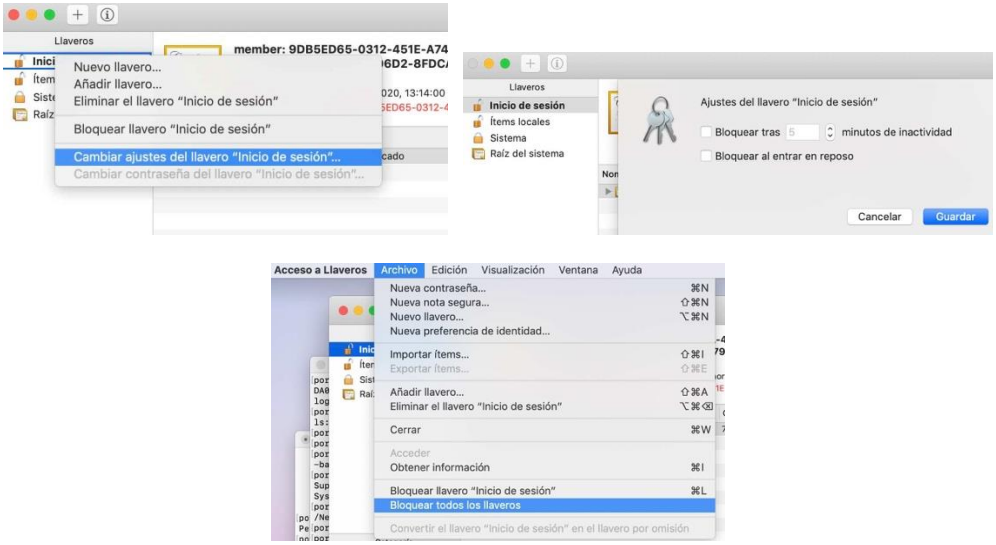


Figura 91 - Opciones de protección de los llaveros

"Acceso a Llaveros" custodia y ofrece acceso (automático o manual) a las contraseñas almacenadas en un llavero desde otras aplicaciones, por ejemplo, el navegador web Safari.

La utilidad "`security`" proporciona un interfaz de línea de comandos para gestionar los llaveros (se recomienda consultar su página del manual para ver las distintas opciones). En la <Figura 92> se proporcionan algunos ejemplos de uso:

```
$ security list-keychains
    "/Users/cniusuario1/Library/Keychains/login.keychain-db"
    "/Library/Keychains/System.keychain"

$ security default-keychain
    "/Users/cniusuario1/Library/Keychains/login.keychain-db"

$ security login-keychain
    "/Users/cniusuario1/Library/Keychains/login.keychain-db"

$ security show-keychain-info
Keychain "<NULL>" lock-on-sleep timeout=21600s

$ sudo security find-internet-password -gs <URL>
version: 512
class: "inet"
attributes:
   0x00000007 <blob>="www.dominio.com"
   0x00000008 <blob>=<NULL>
   "acct"<blob>="email@dominio.com"
   "atyp"<blob>="form"
   "crtr"<uint32>="rimZ"
   ...
   "path"<blob>="/"
   "port"<uint32>=0x00000000
   "prot"<blob>=<NULL>
   "ptcl"<uint32>="https"
...
   "srvr"<blob>="www.dominio.com"
   "type"<uint32>=<NULL>
password: "laclavedelservicio"
```

Figura 92 - Ejemplos de uso de la utilidad "security" para gestionar llaveros

Se recomienda hacer un uso responsable de la funcionalidad de custodia de credenciales en los llaveros de macOS, especialmente teniendo en cuenta la sensibilidad y criticidad del tipo de información que suele almacenarse en los llaveros:

- Utilizar contraseñas muy robustas para proteger los llaveros.
- Mantener los llaveros bloqueados cuando no se esté haciendo uso de ellos.
- Preferir el almacenamiento de credenciales en los llaveros frente al uso de contraseñas repetidas o sencillas de recordar, o a anotaciones en medios potencialmente accesibles visualmente por parte de terceros (como *post-its*).
- Hacer uso del asistente para contraseñas con un tipo de fortaleza robusto a la hora de añadir elementos al llavero asociados a recursos sensibles.

NOTA: en febrero de 2019 se publicó una vulnerabilidad por parte de Linus Henze en la que se demostraba un método para conseguir todas las contraseñas almacenadas en el llavero. El exploit está disponible en https://github.com/LinusHenze/Keysteal y se solucionó en la actualización de seguridad 10.14.4 (CVE-2019-8526).

En la [Ref.- 61] se proporciona el enlace oficial al manual de usuario de la app "Acceso a Llaveros" de Apple.

9.7.3 CERTIFICADOS

macOS gestiona los certificados digitales requeridos por el sistema y/o por el usuario dentro de los respectivos llaveros.

Complementariamente, la app "Acceso a Llaveros" proporciona un asistente para la gestión de certificados digitales, disponible a través del menú "Asistente para Certificados", que permite la creación de certificados tanto de autoridad certificadora o CA ("tipo de identidad = Raíz autofirmada") como certificados hoja ("tipo de identidad = Terminal").

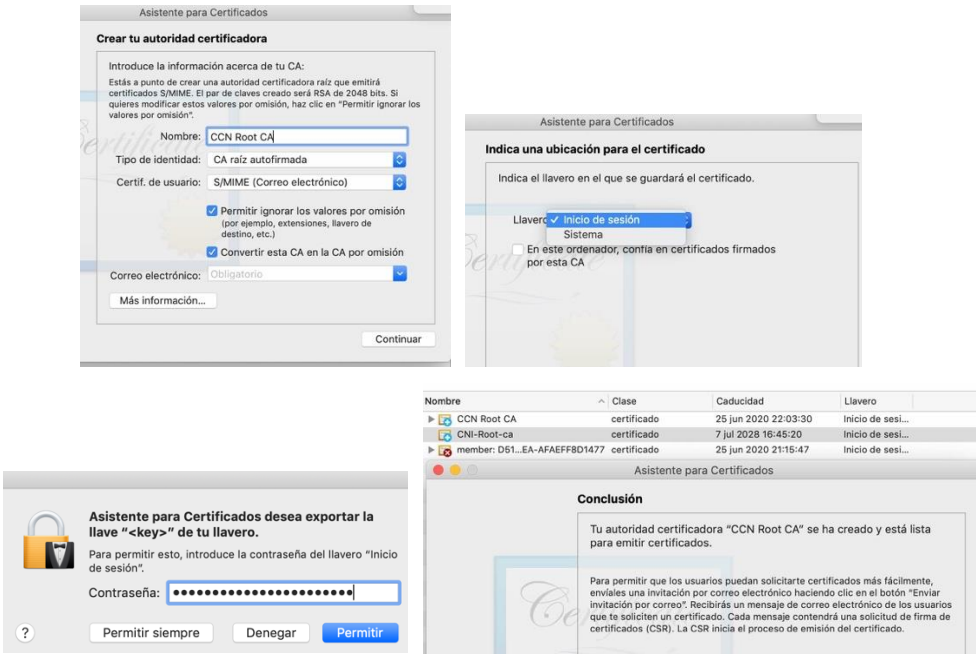


Figura 93 - Creación de una CA desde el "Asistente para certificados" de "Acceso a Llaveros"

9.7.3.1 CERTIFICADOS DE CA

Los equipos Apple disponen de los denominados "*Trust Store*" (almacén de confianza) en los que se definen tres categorías de confianza para los certificados raíz preinstalados con cada versión correspondiente del sistema operativo macOS.

Este almacén se encuentra en el contenedor "`/System/Library/Security/Certificates.bundle/Contents/Resources/`", que puede accederse desde el Finder mediante la opción "Ir - Ir a la carpeta" y abriendo el archivo "`TrustStore.html`" [Ref.- 119].

Estos certificados se almacenan en el llavero "Raíz del sistema" disponible desde "Acceso a Llaveros", dentro de la categoría "Certificados". El usuario puede elegir para cada certificado qué nivel de confianza deposita en él. Para ello, seleccionando la entrada correspondiente al certificado mediante una doble pulsación se abrirán los detalles del certificado, y se dispone del menú "Confiar" (ver <Figura 94>).

macOS permite añadir nuevas CAs (autoridades certificadoras) de confianza a través del llavero de dos formas:

- Botón "+", que abre una instancia de Finder para seleccionar el archivo que contiene el certificado de la CA.
- Arrastrando el fichero del certificado de la CA desde una ventana de Finder que lo contenga.

Los certificados añadidos por este método se consideran "No fiables" por omisión, pero el usuario dispone de capacidad para determinar su nivel de confianza (ver <Figura 94>).

Adicionalmente, es posible añadir certificados a través de perfiles de configuración, por ejemplo, creados mediante "Apple Configurator 2"[29] o "macOS Server Profile Manager"[30].

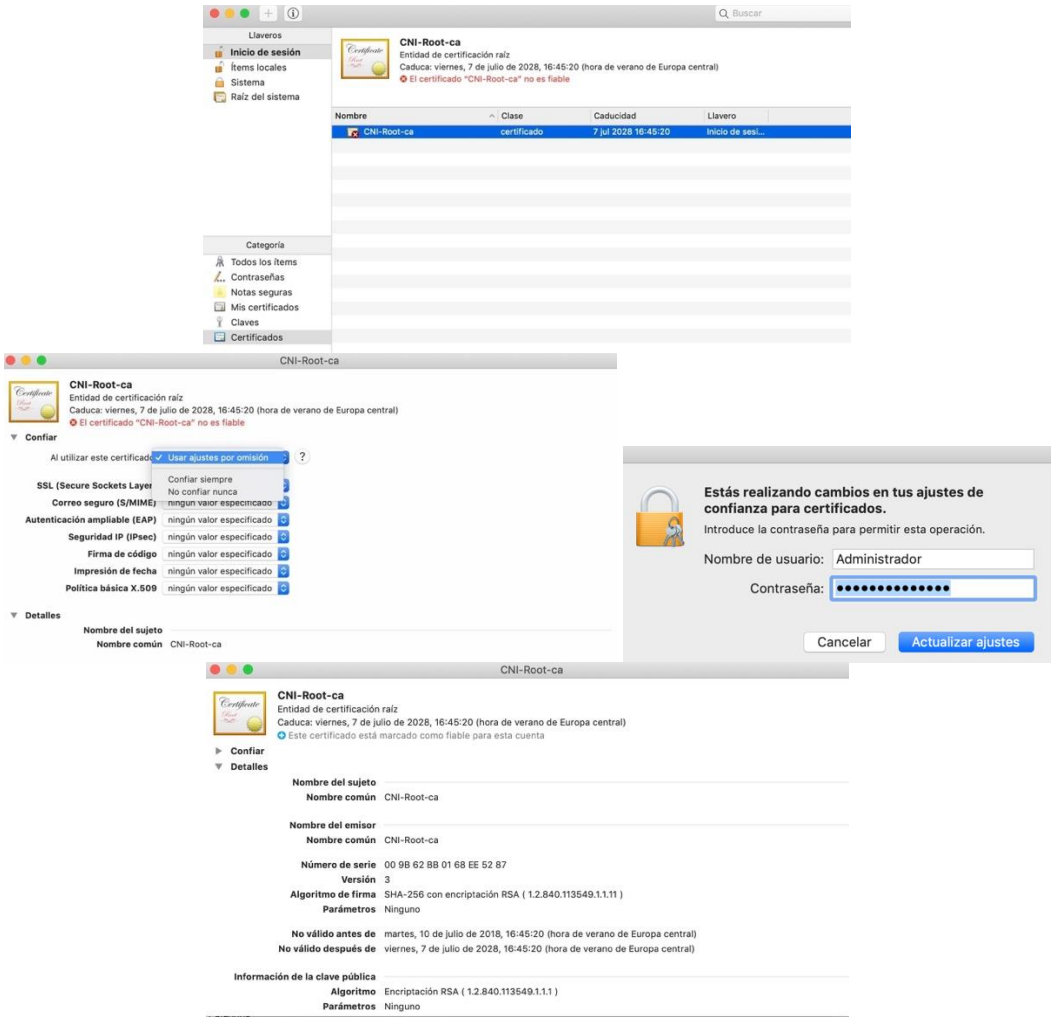


Figura 94 - Declaración de una CA de confianza y de su nivel de confianza

Si un certificado de CA es comprometido, un usuario con acceso privilegiado puede establecer el nivel de confianza a "No confiar nunca" para revocarla localmente.

9.7.3.2 CERTIFICADOS HOJA

Estos certificados pueden añadirse desde el menú "Asistente para certificados", así como crearse desde él si previamente se ha añadido una entidad certificadora (CA).

[29] https://support.apple.com/es-es/apple-configurator

[30] https://support.apple.com/profile-manager

9.8 BORRADO SEGURO DE FICHEROS

El borrado de ficheros a través del interfaz gráfico de usuario en macOS no implica necesariamente la eliminación de sus contenidos del disco físico; en realidad, lo que hace el sistema es marcar sus bloques como borrados, liberando el espacio a nivel del sistema de ficheros para que pueda ser reutilizado a la hora de crear nuevos ficheros o de aumentar el tamaño de ficheros ya existentes. Esto implica que, con el borrado estándar, todavía existe la posibilidad de recuperar el contenido de los ficheros que el usuario haya borrado.

Los ficheros eliminados de una carpeta mediante la opción "Mover a la papelera" pueden ser recuperados accediendo a ella y seleccionando "Sacar de la papelera", o bien ser eliminados definitivamente. El vaciado completo de la Papelera (*Trash*) tampoco elimina sus contenidos físicamente, posibilitando su recuperación. La opción "Eliminar los ítems de la papelera al cabo de 30 días" del menú de "Preferencias - Avanzado" de Finder provoca la eliminación de los ficheros tras 30 días de su borrado, pero tampoco garantiza su completa desaparición.

Figura 95 - Menú "Preferencias - Avanzado" de Finder

No obstante, el uso de los mecanismos de cifrado de almacenamiento proporcionados con FileVault 2 (ver apartado "15.1. FileVault") imposibilita por sí mismo el acceso a los datos de un fichero borrado si el disco es extraído del equipo físico y/o no se dispone de la clave de cifrado, lo que ha provocado modificaciones tanto en las opciones de borrado proporcionadas con macOS como en la disponibilidad de las propias herramientas. Por tanto, una vez más, ***se recomienda hacer uso del cifrado del almacenamiento de FileVault en macOS***.

Por ejemplo, en versiones antiguas de macOS existía la opción "Vaciar papelera de forma segura..." en la app Finder, tanto para contenidos del disco duro del equipo como, especialmente, en discos o unidades de almacenamiento externas conectadas a través de USB. Sin embargo, con la adopción de almacenamiento SSD (*Solid State Drive*), no existe forma de garantizar que el borrado de ficheros resulte efectivo (consultar la [Ref.- 63] para obtener detalles sobre el borrado de datos en unidades SSD), por lo que la opción se suprimió desde macOS 10.11 (El Capitán)[31].

[31] https://support.apple.com/en-us/HT205267 (CVE-2015-5901).

El comando "`diskutil secureErase freespace <level>`" permite borrar de forma segura todos los contenidos asociados al espacio vacío o libre (no utilizado por ficheros) existente en un volumen sobre un disco magnético tradicional (HDD, *Hard Disk Drive*) que está montado actualmente. El parámetro "`<level>`" corresponde a un valor numérico que indica cómo se llevará a cabo el proceso de borrado:

- **0** ó **1**: una única pasada escribiendo ceros u unos, respectivamente, en los bloques del disco.
- **2**: siete pasadas de sobrescritura aleatorias, en base a las directivas del US DoD.
- **3**: método Gutmann, que realiza 35 pasadas de sobrescritura.
- **4**: tres pasadas de sobrescritura aleatorias, en base a las directivas del US DoE.

El siguiente comando elimina de forma segura el espacio libre del volumen principal de macOS ("Macintosh HD"):

```
$ sudo diskutil secureErase freespace 3 /Volumes/Macintosh\ HD
```

Figura 96 - Borrado seguro del espacio libre del disco mediante diskutil

Se recomienda hacer uso de este comando periódicamente en sistemas de almacenamiento HDD, y, especialmente siempre que se elimine 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 puede requerir varias horas.

Cuando se desea borrar todo el contenido de una unidad, desde la app "Utilidad de Discos", a través de la pestaña "Borrar" y mediante el botón "Opciones de seguridad..." que se habilita una vez se ha seleccionando el disco duro o unidad de almacenamiento externa, es posible establecer las opciones de borrado seguro (la opción por defecto **no** corresponde a un borrado seguro, sino a un borrado rápido, por lo que el sistema advierte de que sería posible recuperar los contenidos del disco utilizando herramientas de recuperación y/o análisis forense):

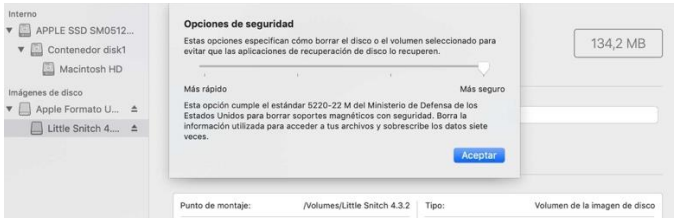


Figura 97 - Opción de borrado seguro de la app "Utilidad de discos"

Se recomienda cambiar la opción a la opción "Más seguro", situada a la derecha de la barra de configuración, que corresponde al nivel 2 del comando "`diskutil secureErase`" descrito anteriormente.

Para conocer el procedimiento de borrado completo del disco, consultar el apartado "17. Eliminación de los datos del ordenador".

9.9 BASE DE DATOS DE AUTORIZACIONES DE SEGURIDAD

macOS hace uso de una base de datos de autorizaciones (en formato SQLite 3.x) disponible en "`/var/db/auth.db`", creada inicialmente a partir de la plantilla contenida en el fichero PLIST "`/System/Library/Security/authorization.plist`", que registra los derechos (privilegios de autorizaciones) de macOS. Estos privilegios determinan qué usuarios pueden o no acceder a cierta funcionalidad, por ejemplo, a las diferentes secciones de las "Preferencias del Sistema".

Las opciones disponibles para gestionar la base de datos de autorizaciones son:

- La utilidad de línea de comandos "`security`", que requiere privilegios de administración para la modificación de los contenidos (opciones "`write`" y "`remove`"), pero no para consulta (opción "`read`"):

```
$ security authorizationdb read system.preferences
```

Figura 98 - Consulta de la lista de autorizaciones sobre la categoría "Preferencias del sistema"

- La edición de la base de datos mediante la utilidad "`sqlite3`".
- La modificación del fichero "`authorization.plist`", seguida del borrado de la base de datos actual, para que sea recreada de nuevo con los nuevos contenidos de dicho fichero PLIST.

En la [Ref.- 64] se dispone de una tabla pública con el conjunto de derechos o privilegios de autorizaciones disponibles en función de la versión de macOS empleada.

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. Desde macOS 10.11 (El Capitán) los permisos de los archivos se sistema se protegen de forma automática[32], mediante SIP (ver apartado "9.10. SIP: System Integrity Protection"). Como referencia, en versiones de macOS previas bastaba con seleccionar la opción "Primera Ayuda" desde la parte superior de la app "Utilidad de Discos", una vez seleccionado el disco o volumen con el sistema de ficheros a restaurar, y hacer uso de las opciones "Verificar los permisos del disco" y "Reparar permisos del disco".

9.10 SIP: SYSTEM INTEGRITY PROTECTION

System Integrity Performance (SIP), también conocida como "*rootless*" [Ref.- 65], es una tecnología que se introdujo en macOS 10.11 (El Capitán), con el objetivo primordial de limitar las capacidades del usuario administrador. SIP restringe la capacidad de modificar, por parte de cualquier usuario, incluido *root*, ciertos ficheros, aplicaciones de sistema y procesos, entre otros:

[32] https://support.apple.com/es-co/HT201560

- Ningún usuario, aplicación o proceso podrá escribir o modificar los contenidos de los directorios en los que residen los ficheros del sistema: `/bin`, `/sbin`, `/System` y `/usr`, así como los de las apps proporcionadas de fábrica por Apple. Adicionalmente, estos directorios estarán ocultos por defecto en "Finder". Únicamente los procesos asociados al instalador (*Apple Installer*) y al actualizador (*Software Update*) de Apple podrán modificarlos. Para ello, el instalador marcará los directorios de sistema con un *flag* especial (para los volúmenes *root* y *boot*), de forma que el *kernel* abortará los procesos que traten de escribir sobre recursos protegidos, dispositivos de bloques en los que dichos recursos residan, u operaciones de montaje sobre contenido protegido.
- Las actualizaciones de *software* podrán suprimir contenidos de estos directorios que se consideren innecesarios, y reparar los permisos que hayan cambiado.
- Las extensiones de *kernel* (*kexts*) con capacidad para modificar los componentes del núcleo de macOS que gestionan las capacidades de I/O (entrada/salida) y que lanzan procesos en segundo plano tendrán que estar firmadas por un desarrollador que disponga de un certificado válido emitido por Apple (ver apartado "9.5. Firma y verificación de aplicaciones y del kernel").
- Se impide la inyección de código y el anclaje (mediante el comando "`lldb -n`") a binarios del sistema.
- Se proporciona un mecanismo de configuración que no pueda ser comprometido de forma automática por *root*: ciertos ajustes se almacenarán en la NVRAM (ver apartado "18.5.1. NVRAM") en lugar de en el sistema de ficheros, de forma que persistan durante la instalación del sistema operativo y afecten a todo el sistema. Algunos parámetros de la NVRAM no pueden ser alterados si SIP está habilitado.

El directorio "`/System/Library/Sandbox`" contiene información sobre los ficheros y directorios protegidos por SIP [Ref.- 84]. Para determinar de forma más fiable qué ficheros de un directorio están protegidos por SIP, se puede ejecutar el comando "`ls`" con el flag "`-O`" y buscar las entradas marcadas como "`restricted`". Las entradas con el flag "`+`" indican que hay listas de controles de acceso especiales sobre esos ficheros, por lo que también se deben revisar:

```
$ ls -laO / | grep -e "+" -e "restr"
...
drwxrwxr-x+  72 root  admin  sunlnk             2304 Jun  6 08:16
Applications
drwxr-xr-x+  67 root  wheel  sunlnk             2144 Mar  8 18:25 Library
drwxr-xr-x@   5 root  wheel  restricted          160 Feb  5 05:41 System
drwxr-xr-x@  37 root  wheel  restricted,hidden  1184 Apr  1 09:52 bin
lrwxr-xr-x@   1 root  wheel  restricted,hidden    11 Feb 24 10:31 etc ->
private/etc
drwxr-xr-x@  64 root  wheel  restricted,hidden  2048 Apr  1 09:52 sbin
lrwxr-xr-x@   1 root  wheel  restricted,hidden    11 Feb 24 10:31 tmp ->
private/tmp
...
```

Figura 99 - Listado de directorios protegidos por SIP

Solo los binarios que contengan el "entitlement" "com.apple.rootless.install" y estén correctamente firmados por Apple pueden actualizar ficheros del sistema evitando las protecciones de SIP[33]:

```
$ codesign -d --entitlements -
/System/Library/PrivateFrameworks/PackageKit.framework/Versions/A/Resources/system_shove

<?xml version="1.0" encoding="UTF-8"?>
<plist version="1.0">
   <dict>
      <key>com.apple.rootless.install</key>
      <true/>
   </dict>
</plist>
```

Figura 100 - Permiso "com.apple.rootless.install" para evitar SIP

La introducción de SIP conllevó la desaparición de la opción "repairPermissions" del comando "diskutil", que proporcionaba 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. También se suprimió la opción "Reparar los permisos del disco" del menú "Primera Ayuda" de la app "Utilidad de discos".

Existe una opción no documentada en la página del manual de "diskutil" que restaura los permisos del directorio *home* de un usuario (requiere privilegios de administración)[34]:

```
$ diskutil resetUserPermissions / `id -u`
```

Figura 101 - Opción de diskutil para restaurar los permisos del directorio home de un usuario

Se recomienda mostrar la extensión asociada a los archivos en la app Finder, con el objetivo de identificar de forma rápida su tipo y el tipo de datos que contienen (ver <Figura 95 >). Tras habilitar la opción "Mostrar extensiones de nombres de archivo", será necesario reiniciar todas las instancias de la app Finder, lo cual se puede llevar a cabo mediante el comando "killall Finder".

9.10.1 MODIFICACIÓN DEL ESTADO DE SIP

El menú "Acerca de este Mac - Informe del sistema - Software" (ver <Figura 9>) incluye el campo "Protección de la integridad del sistema", que permite determinar el estado de SIP. Adicionalmente, el comando "csrutil" permite interaccionar con SIP. La opción "status" muestra el estado de activación de SIP, mientras que las opciones "disable" y "enable" desactivan y activan SIP respectivamente.

El estado de activación de SIP es un parámetro de la NVRAM, que solo puede alterarse desde un terminal lanzado en modo de recuperación de macOS (ver apartado

[33] En la [Ref.- 129] se proporciona una referencia a un mecanismo para comprometer SIP en base a este atributo. La vulnerabilidad asociada (CVE-2017-6974) fue resuelta en 2017 por Apple.

[34] https://eclecticlight.co/2018/07/14/should-you-try-repairing-permissions-in-high-sierra-or-later/

"18.2. Modo "Recuperación" (Recovery)"). Por tanto, si se dispone de dos imágenes de disco de arranque en un ordenador, el deshabilitar SIP para una de ellas provocará que también se desactive para la otra[35]. Del mismo modo, es importante tener en cuenta que el estado de activación de SIP en macOS Mojave persiste frente a una reinstalación o una actualización de sistema operativo, por lo que conviene consultar el estado actual tras haber llevado a cabo alguna operación de activación/desactivación.

```
* Ejecutando el sistema en modo de arranque normal:

$ csrutil status
System Integrity Protection status: disabled.

$ sudo csrutil enable
Password:
csrutil: failed to modify system integrity configuration. This tool needs to
be executed from the Recovery OS.

* Tras reiniciar el sistema en modo de recuperación:

[-bash-3.2]$ csrutil enable
Successfully enabled System Integrity Protection. Please restart the machine
for the changes to take effect.

* Tras reiniciar el sistema en modo de arranque normal:

$ csrutil status
System Integrity Protection status: enabled.
```

Figura 102 - Comandos csrutil para interactuar con SIP

NOTA: La opción "`-without`" del comando "`csrutil`" que permitía desactivar componentes de SIP (por ejemplo, `kext`, `fs`, `nvram`) de forma selectiva ya no está disponible en Mojave.

Desde el punto de vista de seguridad, si se precisa realizar alguna tarea de administración que requiera la desactivación temporal de SIP, ***se recomienda volver a habilitar SIP tan pronto sea posible***.

Algunas de las operaciones que requieren la desactivación temporal de SIP son:

- La modificación de ciertos parámetros de la NVRAM (ver apartado "18.5.1. NVRAM").
- La inhabilitación de demonios y agentes del sistema (ver apartado "7.1.3. Impedir el arranque de servicios en macOS").

9.11 SUPERVISIÓN DE EVENTOS

macOS 10.14 dispone de un mecanismo de registro (*logging*) unificado en el que se centraliza la captura de eventos, que se almacenan en memoria y en repositorios de datos [Ref.- 66]. Este mecanismo unificado reemplaza al ASL (*Apple System Log*), que a su vez sustituyó a la funcionalidad de registro vía las APIs de Syslog, que escribían en ubicaciones específicas del disco como "`/etc/system.log`".

[35] https://blog.macsales.com/45473-we-explain-what-system-integrity-protection-on-mac-is-and-how-to-control-it/

Existen varios niveles de registro para los eventos, para los que el sistema establece una serie de comportamientos, alterables a través del comando "`log`": por defecto (*default*), informativos (*info*), de depuración (*debug*), de error (*error*) y de fallo (*fault*). Para ver el nivel actual, se puede lanzar el comando:

```
$ sudo log config --status
Password:
System mode = INFO
```

Figura 103 - Comando "log" para consultar el nivel de registro del sistema

La función "`os_log`" permite a las apps enviar un objeto a un nivel de registro concreto.

Mojave conserva algunos de los ficheros de log de ASL bajo:

- `/var/log`: logs del sistema de servicios de bajo nivel.
- `/Library/Logs`: logs de apps del sistema.
- `/Library/Logs/DiagnosticReports`: informes del sistema y apps del sistema (incluye *logs* de fallos irrecuperables o de congelación), incluyendo periféricos y hardware.
- `~/Library/Logs`: logs de aplicaciones de usuario.
- `~/Library/Logs/DiagnosticReports`: informes de apps de usuario (incluye *logs* de fallos irrecuperables o de congelación).

Adicionalmente, Mojave almacena los ficheros de log unificados bajo "`/var/db/diagnostics`"[36]. Dentro de este directorio, macOS Mojave añade la carpeta "`Signpost`", que alberga los ficheros de log con extensión "`.tracev3`", cuyo formato es propietario de Apple, y que son una nueva característica enfocada a que los desarrolladores puedan mejorar sus análisis de rendimiento en macOS [Ref.- 67] [Ref.- 68].

Para visualizar los eventos registrados, se dispone de la app "Consola", ubicada en "`/Applications/Utilities`", así como de la utilidad de línea de comandos "`log`":

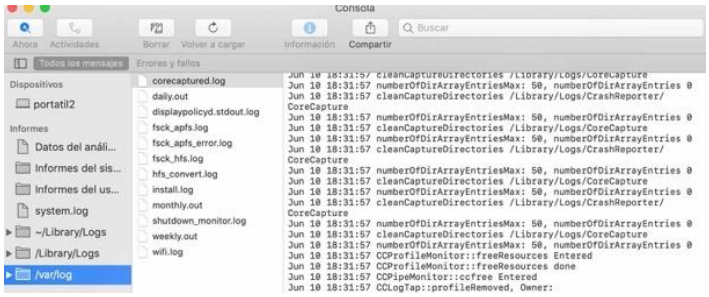


Figura 104 - Visualización de registros de macOS mediante la app "Consola"

Complementariamente, mediante el menú " - Acerca de este Mac - Informe del sistema - [Software] Registros" también es posible acceder a algunos de estos registros y salidas de otros comandos que proporcionan información sobre el sistema:

[36] En "`/var/db/uuidtext`" residen referencias a los elementos anteriores.

Figura 105 - Visualización de registros mediante el menú "Acerca de este Mac"

Los *logs* asociados a elementos concretos pueden consultarse haciendo uso del parámetro "`--predicate`" del comando "`log`". La <Figura 106> muestra diversos ejemplos de obtención de información de *logs*:

```
* Mostrar las actividades iniciadas por un elemento (proceso "sudo") durante
las últimas 24 horas:

$ log show --style syslog --predicate 'process == "sudo"' --last 24h

2019-06-10 13:52:54.891037+0200  localhost sudo[3652]:    admin : TTY=ttys000
; PWD=/private/var/admin ; USER=root ; COMMAND=/usr/bin/defaults write
NSGlobalDomain AppleShowAllExtensions -b


* Intentos de invocar el comando "sudo" por parte de un usuario sin
privilegios de administración:

$ log show --style syslog --predicate 'process == "sudo" and eventMessage
contains "user NOT in sudoers"'

Filtering the log data using "process == "sudo" AND composedMessage CONTAINS
"user NOT in sudoers""
Skipping info and debug messages, pass --info and/or --debug to include.
Timestamp                       (process)[PID]
2019-05-06 12:05:45.292961+0200  localhost sudo[543]: cniusuario1 : user NOT
in sudoers ; TTY=ttys000 ; PWD=/Users/cniusuario1 ; USER=root ;
COMMAND=/bin/hostname portatil1
2019-05-20 10:15:34.760264+0200  localhost sudo[876]: cniusuario1 : user NOT
in sudoers ; TTY=ttys000 ; PWD=/Users/cniusuario1 ; USER=root ;
COMMAND=/usr/bin/who

* Eventos del subsistema "TimeMachine":

$ log show --predicate 'subsystem == "com.apple.TimeMachine"' --info

2019-06-10 19:24:05.586116+0200 0x143fc0   Info        0x0                  80
0    backupd-helper: (TimeMachine) [com.apple.TimeMachine:TMLogInfo] Not
starting scheduled Time Machine backup: Automatic backups disabled
-------------------------------------------------------------------------------
------
Log      - Default:          0, Info:            4,610, Debug:             0,
Error:          0, Fault:          0
Activity - Create:           0, Transition:          0, Actions:           0

* Intentos de introducción de la contraseña de administrador junto al comando
"sudo" que dio lugar a que dicha contraseña fuera solicitada:

$ sudo log show --style syslog --predicate 'eventMessage contains "Failed to
authenticate user"' --info --last 3h

2019-06-10 20:03:29.500678+0200  localhost sudo[4500]:  admin : 3 incorrect
password attempts ; TTY=ttys001 ; PWD=/private/var/log ; USER=root ;
COMMAND=/usr/bin/log show --style syslog --predicate eventMessage contains
"Failed to authenticate user" --info --last 1d
2019-06-10 20:03:36.713321+0200  localhost sudo[4501]:  admin: TTY=ttys001 ;
PWD=/private/var/log ; USER=root ; COMMAND=/usr/bin/log show --style syslog --
predicate eventMessage contains "Failed to authenticate user" --info --last 1d
```

Figura 106 - Ejemplos del comando "log" para ver intentos de invocación fallidos de "sudo"

Para poder ver las entradas de Signpost, es preciso especificar el parámetro "`--signpost`" del comando "`log show`".

9.12 CONTROLES PARENTALES

macOS permite tanto crear cuentas para uso específico con control parental, como asignar controles parentales a cuentas ya existentes a través del menú "Usuarios y grupos - [Seleccionar usuario] - Abrir controles parentales...", que requiere autentificarse como administrador. Ambos escenarios se describen detalladamente en la documentación oficial de soporte de Apple [Ref.- 88].

Si bien los controles parentales están orientados a la utilización del equipo en un entorno personal en lugar de profesional, en ocasiones pueden ser una alternativa para configurar una cuenta de usuario con acceso limitado. Las restricciones disponibles que se pueden imponer a una cuenta asociadas al control parental se describen en el propio interfaz de usuario de los ajustes de macOS.

Se recomienda establecer restricciones del siguiente tipo:

- "[Apps] - Limitar aplicaciones en este Mac" (seleccionando únicamente las apps que puedan ser requeridas).
- "[Tiendas] - Desactivar iTunes Store".
- "[Privacidad]": desmarcar todas las opciones bajo "Permitir cambios en".
- "[Otros]": Desactivar "Siri y dictado".

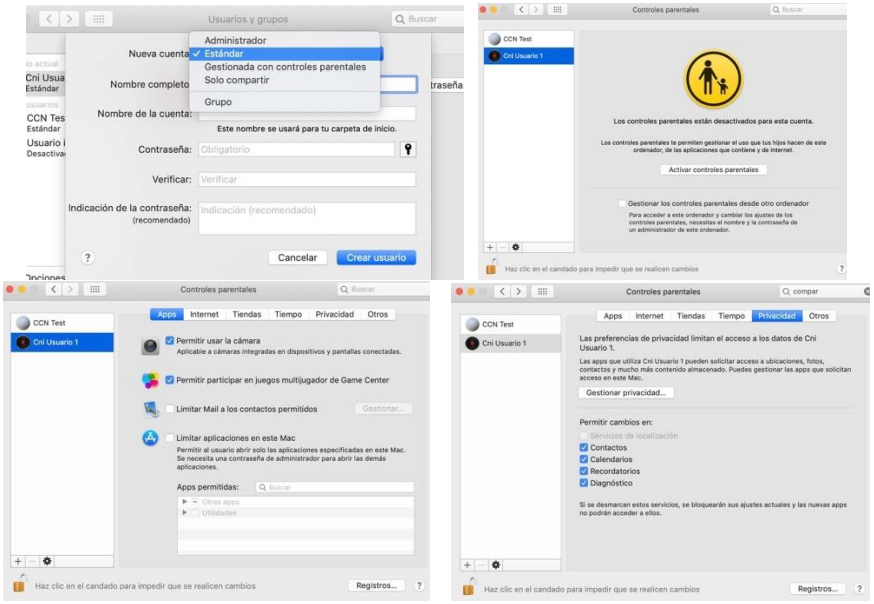


Figura 107 - Configuración de los controles parentales de macOS

Si una cuenta configurada con controles parentales intenta hacer una operación no permitida, el sistema mostrará un mensaje como el de la <Figura 108> y, en caso de seleccionarse una de las opciones de "Permitir...", se solicitarán las credenciales de una cuenta de administrador.

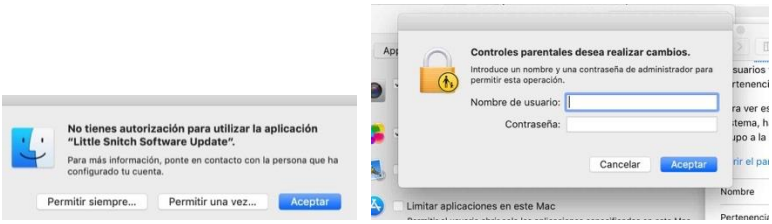


Figura 108 - Mensaje de intento de violación de los controles parentales

9.13 ATS (APP TRANSPORT SECURITY)

La tecnología ATS de Apple impone a las apps y extensiones el uso del protocolo TLS basado en certificados y algoritmos de cifrado considerados seguros por Apple, bloqueando las conexiones que no cumplan los requisitos mínimos. Las conexiones TLS requerirán el cumplimiento de las buenas prácticas de la industria actuales:

- TLS v1.2 con "*forward secrecy*", y con un tamaño mínimo de clave de 2.048 bits para RSA y 256 bits para curva elíptica.

No obstante, la app puede establecer excepciones a ATS en su fichero "`Info.plist`" (ver apartado "13.4.1. Ficheros PLIST de una app"), que deberán ser aprobadas en función de las políticas y requisitos impuestos por Apple en la App Store[37].

9.14 CERTIFICATE PINNING

Los mecanismos de *certificate pinning* (CP) proporcionan validación y protección de las comunicaciones autentificadas y cifradas mediante HTTPS (TLS), por ejemplo, durante la descarga de apps de la Apple Store y en la comprobación de actualizaciones.

El CP consiste en una validación del certificado proporcionado por el servicio en el lado cliente, sin hacer uso de la infraestructura pública (PKI) de certificados de Internet asociada a las autoridades certificadoras o CAs. Para que esta verificación sea posible, la app debe conocer previamente el certificado del servidor esperado (o su *fingerprint* criptográfico, también conocido como "*pin*"). De este modo, cuando se establezca la conexión con el servidor, la app podrá comparar el *fingerprint* (o *pin* conocido) con el del certificado digital recibido desde el servidor remoto. Si son idénticos, la conexión se considerará válida y la transferencia de datos se iniciará. Si no lo son, la app deberá interrumpir la negociación TLS y rechazar la conexión.

10.SERVICIOS DEL SISTEMA

10.1 SERVICIOS COMPARTIDOS

macOS proporciona numerosos servicios compartidos desde el menú "Preferencias del Sistema - Compartir", que facilitan el acceso remoto a través de la red al equipo o la compartición de datos, información y archivos con otros ordenadores y

[37] https://developer.apple.com/documentation/security/preventing_insecure_network_connections

servicios (remotos o locales). Por su naturaleza, se debe prestar especial atención a cuáles están habilitados, y en qué ámbito.

El parámetro "Nombre del ordenador", descrito en el apartado "12.1.1. Nombre del equipo", será el identificador del Mac de cara a estos servicios.

Por defecto, todos los servicios están deshabilitados, ***opción recomendada desde el punto de vista de seguridad***, para impedir las conexiones entrantes y el acceso a recursos del equipo. En caso de requerirse hacer uso puntual de alguno de los servicios de compartición, ***se recomienda activarlos temporalmente, y desactivarlos inmediatamente tras finalizar la sesión asociada***.

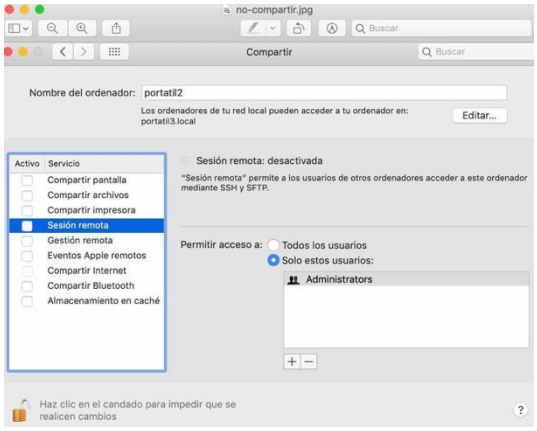


Figura 109 - Menú "Compartir"

Para la mayoría de servicios compartidos que se activen, el panel de configuración muestra los detalles necesarios para establecer la conexión con el servicio y su estado.

Los servicios de compartición están estrechamente ligados a la configuración del cortafuegos personal de macOS, por lo que se recomienda consultar el apartado "8.2.2. Firewall (Cortafuegos)", tanto para establecer las reglas adecuadas como para diagnosticar problemas de conectividad.

A continuación se describen los diferentes servicios de compartición de macOS.

10.1.1 COMPARTIR PANTALLA

Este servicio posibilita la utilización del ordenador desde un equipo externo a modo de escritorio remoto, desde el que se puede controlar completamente el Mac, incluyendo la ejecución de apps y el reinicio del sistema [Ref.- 92].

La sección "Permitir acceso a:" posibilita la conexión a (ver <Figura 110>):

- **Todos los usuarios**: cualquier usuario que tenga cuenta en el ordenador con perfil administrador o estándar puede pedir permiso para compartir o controlar la pantalla. Quedan excluidas las cuentas "Solo compartir" e "Invitado".
- **Solo estos usuarios**: únicamente se permite conexiones para las cuentas de usuario designadas en este campo.

En cualquiera de los casos, si en ambos equipos la sesión está iniciada con una cuenta asociada al mismo Apple ID, no se solicitará contraseña para acceder al Mac.

El botón "Ajustes del ordenador..." permite definir si otros usuarios pueden compartir su pantalla incluso sin tener una cuenta de usuario en el ordenador:

- "Todos pueden pedir permiso para controlar la pantalla": el sistema notificará por pantalla al usuario que actualmente tiene la sesión local abierta sobre esta solicitud, requiriendo su autorización. ***Desde el punto de vista de seguridad, se recomienda elegir esta opción***.
- "Los visores VNC pueden controlar la pantalla mediante contraseña:": las conexiones entrantes desde un cliente VNC (*Virtual Network Computing*) requerirán la introducción de una contraseña específica. ***Esta opción se considera menos segura***, ya que la contraseña debe ser conocida por usuarios externos. Si esta opción fuese imprescindible, la contraseña debería ser lo más robusta posible y renovarse frecuentemente.

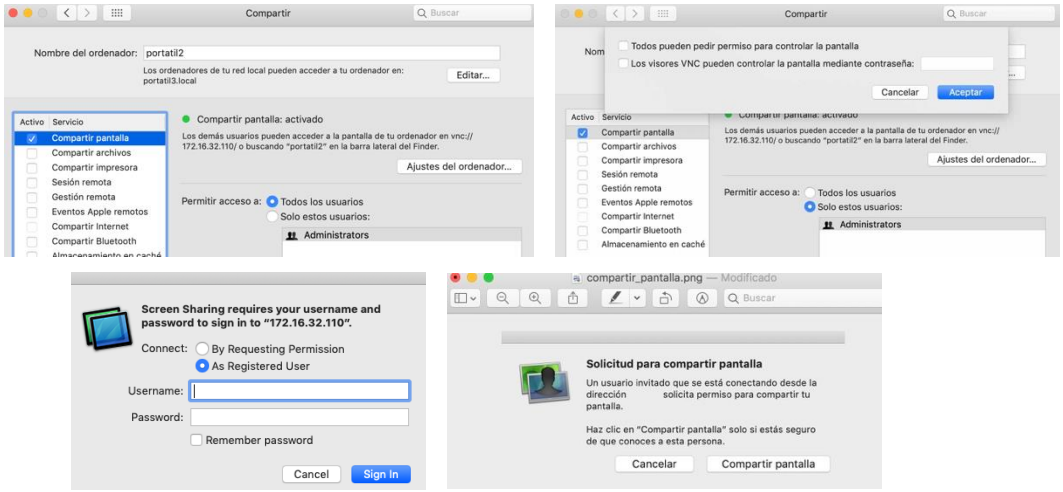


Figura 110 - Ajustes de "Compartir pantalla"

La compartición se puede realizar a través de diversos servicios:

- Desde el Finder del equipo solicitante, a través de la opción "Ir - Conectarse al servidor...", especificando como recurso "`vnc://<dirección IP o nombre del equipo>`". Si existe un usuario conectado localmente en ese momento y su Apple ID no coincide con el del usuario que inicia la conexión, en el equipo origen de la solicitud se mostrará la ventana:

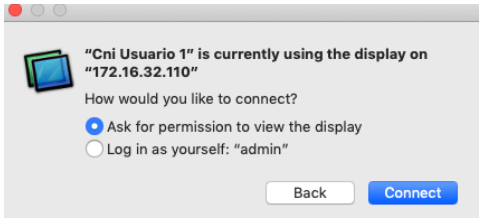


Figura 111 - Notificación de usuario activo en el equipo remoto

Si se selecciona la segunda opción, la sesión local se mantendrá de forma independiente de la sesión remota.

- A través de los servicios de Mensajes o FaceTime: mediante el icono "" se puede solicitar tanto compartir la pantalla propia como la del usuario remoto. Si un tercero está intentando acceder a la compartición de pantalla del Mac, se recibirá un mensaje de solicitud para aceptar o declinar la petición. Si se opta por "Rechazar", se presentará la opción para bloquear al usuario.

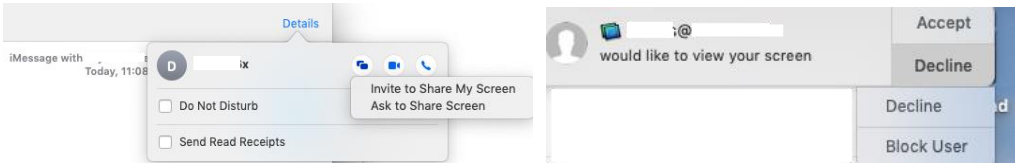


Figura 112 - Uso de "Compartir pantalla" desde Mensajes

Mientras se comparte la pantalla, aparecerá en la barra de menús de estado del equipo un indicador de que se está compartiendo la pantalla mediante el icono "", desde el cual se pueden finalizar las conexiones remotas. ***Se recomienda prestar atención a la presencia de este icono,*** que puede revelar conexiones no deseadas. Cuando la compartición se lleva a cabo desde Mensajes o FaceTime, el icono parpadeará en color azul (""). No se observa este comportamiento cuando la compartición se lleva a cabo mediante una conexión VNC:

Figura 113 - Desconexión de "Compartir pantalla"

El menú "Preferencias" de la app "Compartir pantalla" (*Screen Sharing*) define ajustes a dos niveles:

- Desde las pestañas "Pantalla" y "Calidad" se controlan ajustes de visualización.
- Desde la pestaña "Usuarios bloqueados", es posible bloquear usuarios por su Apple ID, de modo que sus solicitudes de compartición a través de apps como Mensajes o Facetime no se recibirán (aunque en el equipo solicitante no se recibirá ninguna indicación de que ha sido bloqueado). ***Se recomienda limitar la compartición a solo contactos*** (por defecto, se permite a todo el mundo).

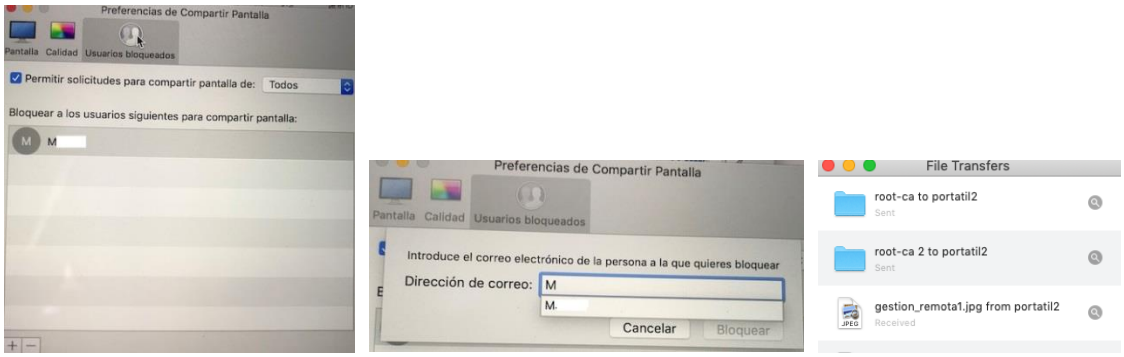


Figura 114 - Compartición de pantalla y transferencia de ficheros: bloqueo de usuarios por Apple ID

La app "Compartir pantalla" también dispone de un menú "Visualización", que ofrece las opciones "Cambiar al modo de control" y "Cambiar al modo de observación", en función de si se precisa realizar operaciones sobre el ordenador desde el equipo

remoto (opción habilitada por defecto) o simplemente observar la pantalla. ***Se recomienda cambiar al modo de observación salvo que se precise lo contrario***.

Durante la compartición de pantalla es posible transferir contenidos entre los equipos conectados (arrastrando los ficheros de uno a otro), así como utilizar el portapapeles para copiar texto o imágenes entre ambos. La recepción de un archivo en el ordenador destino se notificará mediante una ventana emergente y se dispondrá de un histórico de trasferencias de ficheros (ver imagen derecha de la <Figura 114>). El modo de uso del portapapeles compartido se controla desde el menú de "Compartir pantalla - Edición". ***Se recomienda no hacer uso del portapapeles compartido***, sino utilizar las opciones de "Obtener" y "Enviar" cuando se precise.

A nivel de sistema, el fichero de configuración del demonio de compartición reside en "`/System/Library/LaunchDaemons/com.apple.screensharing.plist`". Cuando se recibe una conexión al puerto 5900 (`rfb` o `vnc-server`), "`launchd`" arrancará[38]:

- El servidor de compartición (asociado al binario "`/System/Library/CoreServices/RemoteManagement/screensharingd.bundle/Contents/MacOS/screensharingd`"): se encarga de la autentificación y de la gestión de las conexiones a nivel de red.
- Un agente de compartición (asociado al binario "`/System/Library/CoreServices/RemoteManagement/ScreensharingAgent.bundle/Contents/MacOS/ScreensharingAgent`"): se encarga de la interacción con el usuario.

El servicio de compartición arrancará además una serie de procesos "*helper*" para proporcionar funcionalidad adicional, entre ellos:

- `SSPasteboardHelper`: gestiona la capacidad de copiar y pegar (portapapeles compartido) entre ambos sistemas.
- `SSFileCopyReceiver` y `SSFileCopySender`: gestiona el intercambio de ficheros.
- Extensiones propias de Apple (por ejemplo, para la interpretación y transmisión de gestos).

```
launchd      1     root    8u  IPv6        0t0    TCP *:rfb (LISTEN)
launchd      1     root    9u  IPv4        0t0    TCP *:rfb (LISTEN)
kdc       5609     root    5u  IPv6        0t0    TCP *:kerberos (LISTEN)
kdc       5609     root    7u  IPv4        0t0    TCP *:kerberos (LISTEN)
screensha 6353     root  fp.u  IPv4        0t0    TCP *:rfb (LISTEN) (fileport=0x1d03)
screensha 6353     root  fp.u  IPv6        0t0    TCP *:rfb (LISTEN) (fileport=0x2603)
screensha 6353     root    3u  IPv6        0t0    TCP *:rfb (LISTEN)
screensha 6353     root    4u  IPv4        0t0    TCP *:rfb (LISTEN)
```

Figura 115 - Puertos abiertos por el servicio "Compartir pantalla"

Desde el punto de vista de seguridad, ***la compartición de pantalla debe habilitarse tan solo de manera puntual, y deshabilitarse nada más finalice la actividad que la requiere***.

NOTA: si la conexión a través del servicio "Compartir pantalla" falla estando el cortafuegos activo, se debe verificar si los siguientes dos procesos están en la lista de aplicaciones autorizadas. Si no, tratar de añadirlos a través de "`socketfilterfw --add`". La operación

[38] https://apple.stackexchange.com/questions/114023/how-does-a-macs-screen-sharing-service-work

puede requerir reiniciar el demonio responsable del cortafuegos (ver apartado "8.2.2. Firewall (Cortafuegos"):

```
"/System/Library/CoreServices/RemoteManagement/screensharingd.bundle/Contents/MacOS/screensharingd"
"/System/Library/CoreServices/RemoteManagement/ScreensharingAgent.bundle/Contents/MacOS/ScreensharingAgent"
```

10.1.2 GESTIÓN REMOTA

Esta opción posibilita la conexión al ordenador desde equipos que utilicen "*Apple Remote Desktop*", un sistema de administración para entornos empresariales [Ref.-93]. Su configuración pormenorizada queda fuera del alcance de la presente guía.

La funcionalidad "Gestión remota" es incompatible con la de "Compartir pantalla" (ver apartado "10.1.1. Compartir pantalla"), dado que los puertos TCP/IP empleados por ambas son los mismos. Por este motivo, al activar una de ellas, la otra será deshabilitada automáticamente (tanto del sistema como del interfaz de macOS), sin que se informe de ello expresamente al usuario. La ventaja de la opción "Gestión remota" es que permite definir de forma mucho más granular los permisos de que dispondrá el usuario remoto que se conecta al ordenador local utilizando esta funcionalidad.

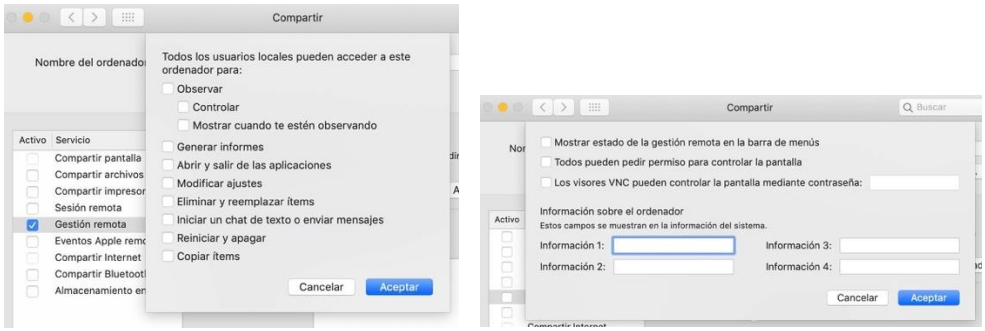


Figura 116 - Opciones de "Gestión remota"

Los ajustes asociados a este servicio (todos deshabilitados por defecto) están accesibles desde el botón "Ajustes del ordenador...", y las recomendaciones de seguridad son:

- Habilitar "Mostrar estado de la gestión remota en la barra de menús", de forma que el usuario tenga conocimiento de la existencia de conexiones remotas.
- Restringir la información facilitada sobre el ordenador en los campos "Información <N>:".
- Aplicar las mismas recomendaciones que las descritas en la sección "10.1.1. Compartir pantalla" para los ajustes "Todos pueden pedir permiso para controlar la pantalla" frente a "Los visores VNC pueden controlar la pantalla mediante contraseña:".

10.1.3 COMPARTIR ARCHIVOS

Tal y como se describe en el apartado "8.1. Usuarios y grupos", los usuarios estándar de macOS disponen por defecto de una carpeta "Pública" "`/Users/<usuario>/Public`", así como de la posibilidad de establecer otras carpetas como públicas para permitir el acceso a sus contenidos por parte de otros usuarios que se conecten desde sistemas remotos.

Los tipos de privilegios (a la derecha de la lista de usuarios) y los roles de la sección "Usuarios" son los mismos que los descritos en el apartado "8.1. Usuarios y grupos". Para añadir/suprimir usuarios o grupos a la lista de autorizaciones, se dispone de los botones "+" y "-", respectivamente, de la sección "Usuarios".

Los puertos utilizados por este servicio son: TCP/445 (`microsoft-ds`), TCP/548 (`afpovertcp`), así como del puerto TCP/88 y UDP/88 (`kerberos`), tanto en IPv4 como IPv6.

```
$ sudo  lsof -i | grep LISTEN

launchd      1            root    8u  TCP     *:rfb (LISTEN)
launchd      1            root    9u  TCP     *:rfb (LISTEN)
launchd      1            root   16u  TCP     *:microsoft-ds (LISTEN)
launchd      1            root   55u  TCP     *:microsoft-ds (LISTEN)
launchd      1            root   58u  TCP     *:afpovertcp (LISTEN)
launchd      1            root   59u  TCP     *:afpovertcp (LISTEN)
launchd      1            root   60u  TCP     *:afpovertcp (LISTEN)
launchd      1            root   61u  TCP     *:afpovertcp (LISTEN)
kdc       5609            root    5u  TCP     *:kerberos (LISTEN)
kdc       5609            root    7u  TCP     *:kerberos (LISTEN)
smbd      6542            root    3u  IPv6   TCP *:microsoft-ds (LISTEN)
smbd      6542            root    4u  IPv4   TCP *:microsoft-ds (LISTEN)
```

Figura 117 - Comprobación de los puertos utilizados por los procesos de "Compartir archivos"

Desde el punto de vista de seguridad, ***se recomienda aplicar las mismas recomendaciones que en el citado apartado de "Usuarios y grupos", y, en particular***:

- ***Establecer el permiso*** "Sin acceso" para el grupo "Todos" ("Everyone").
- Evaluar y ajustar en detalle las carpetas que son compartidas y los usuarios y grupos que dispondrán de acceso a las mismas, junto a sus permisos, ***reduciendo el acceso al mínimo imprescindible*** para el propósito por el que se ha habilitado el servicio.
- ***Mantener desactivada la opción*** "Preferencias del Sistema - Usuarios y grupos - Permitir a los usuarios invitados conectarse a las carpetas compartidas" para el usuario invitado (*Guest*), en caso de que la cuenta de invitado esté habilitada en el sistema (lo cual está desaconsejado).
- ***Crear una cuenta de tipo*** "Solo compartir" si se hace un uso reiterado del servicio de compartición de archivos, frente a la compartición a través de la cuenta de usuario estándar.
- ***Controlar el número de usuarios conectados a las carpetas compartidas*** para detectar situaciones anómalas (ver imagen inferior izquierda de la <Figura 118>, concretamente, el campo "Número de usuarios conectados").

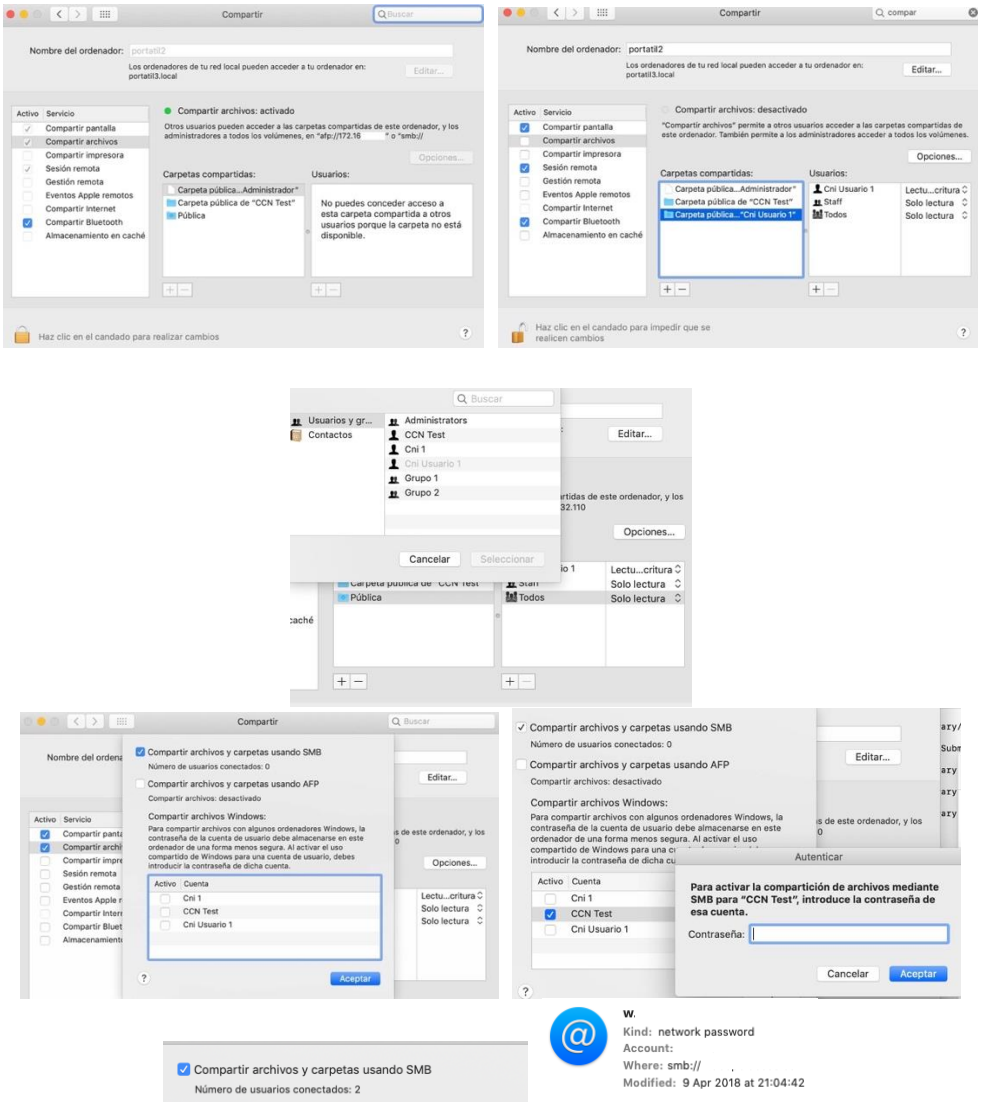


Figura 118 - Menú "Compartir archivos"

Como ilustra la <Figura 118>, el protocolo de compartición utilizado por defecto es SMB (*Server Message Block*, empleado ampliamente por Windows) sobre TCP/IP, aunque también se permite utilizar (en paralelo o de forma exclusiva) AFP (*Apple Filling Protocol*), si bien esta opción no permite la compartición de volúmenes APFS, que es el sistema de archivos utilizado por defecto en Mojave (ver apartado "15.5. APFS (Apple File System)").

La opción "Compartir archivos Windows" requerirá, para cada usuario de macOS seleccionado, la introducción de la contraseña de su cuenta de macOS, que será almacenada de forma menos segura debido a que se usa un formato que permite compatibilidad con versiones de Windows antiguas[39]. Tal y como se describe en la ayuda de macOS accesible desde el botón "?", antes de desactivar "Compartir Archivos" debe anularse la opción "Activado" de cada cuenta, porque, en caso contrario, las contraseñas seguirán estando almacenadas en el llavero de macOS con un elemento

[39] https://apple.stackexchange.com/questions/306151/where-does-file-sharing-store-smb-passwords

de tipo "Network password" (la desactivación de la cuenta requerirá volver a introducir su contraseña).

Al pinchar con el botón derecho sobre una carpeta compartida de la lista (ver <Figura 119>), se desplegará un menú que incluye "Opciones avanzadas…", desde el cual se puede establecer que solo se permitan conexiones SMB encriptadas. Esta opción hace uso de SMB3 [Ref.- 94], que cifra las conexiones extremo a extremo, además de añadir una firma a cada paquete que se transmite. Desde el punto de vista de seguridad, ***esta opción es la recomendada***, pero puede tener implicaciones de rendimiento y compatibilidad.

Se aconseja desactivar la opción "Permitir usuarios invitados", dentro de las opciones avanzadas de una carpeta, que se activa por defecto:

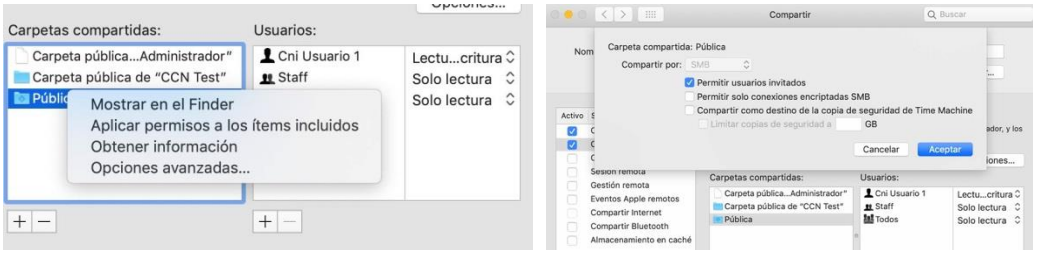


Figura 119 - Opciones avanzadas del menú de "Carpetas compartidas"

El acceso a una carpeta compartida desde otro equipo macOS se puede iniciar desde el Finder del equipo solicitante, mediante la opción "Ir - Conectarse al servidor…" y especificando "`afp://<dirección IP o nombre del equipo>`" o "`smb://<dirección IP o nombre del equipo>`". La conexión por SMB desde un equipo macOS a otro solicitará las credenciales y, una vez validadas, mostrará las carpetas disponibles. Si las credenciales introducidas corresponden con las de un usuario del sistema operativo, todos sus archivos serán accesibles, quedando mapeados bajo una localización asociada a su nombre de usuario:

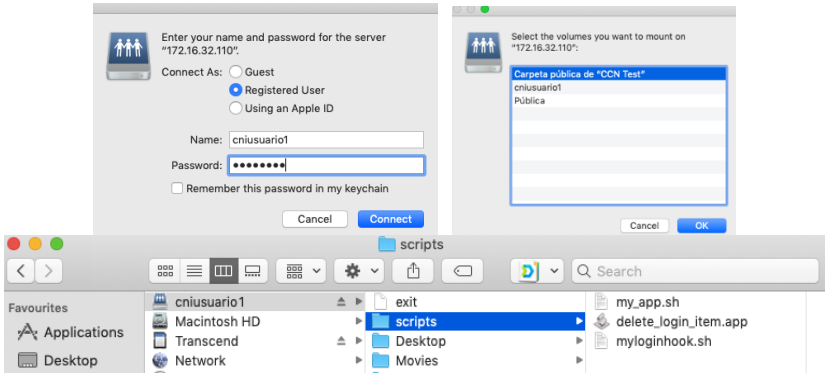


Figura 120 - Establecimiento de una conexión SMB entre equipos macOS

Es posible determinar las conexiones SMB activas (incluyendo los atributos específicos de cada conexión) mediante:

```
$ smbutil statshares -a
```

Figura 121 - Comando para obtener información sobre las conexiones SMB activas

Si se deshabilita el servicio mientras existen usuarios conectados, el sistema presentará un mensaje proponiendo dar un tiempo antes de cerrar las conexiones:

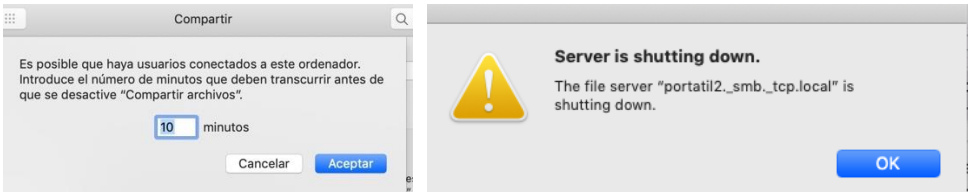


Figura 122 - Confirmación para deshabilitar "Compartir archivos" mientras hay usuarios conectados

La funcionalidad de compartición de archivos permite que el Mac pueda ser configurado como destino de copias de seguridad de Time Machine de otros equipos de la misma red local (ver apartado "16.1.1. Configuración de otro Mac como destino de copias de seguridad de Time Machine").

10.1.4 COMPARTIR IMPRESORA

El panel de la izquierda de la funcionalidad "Compartir impresora" [Ref.- 95] permite seleccionar, de la lista de impresoras locales o de red definidas en macOS, cuáles serán compartidas; en el panel de la derecha, se establece qué usuarios de la red local del equipo tendrán acceso a cada impresora y con qué permisos:

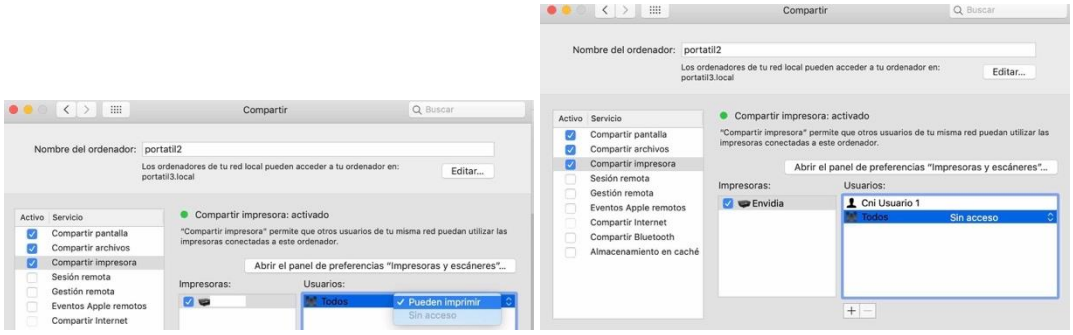


Figura 123 - Compartir impresora

Por defecto, el grupo "Todos" dispone de permiso para imprimir. La forma de impedir este acceso global es añadir, mediante "+", usuarios o grupos específicos.

"Compartir impresora" hace uso del puerto TCP/631 (`ipp`, *Internet Printing Protocol*), tanto en IPv4 como IPv6, en todos los interfaces de red, asociado al proceso "`cupsd`":

```
$ lsof -i | grep LISTEN | grep ipp
cupsd     6788            root    7u  IPv6        0t0     TCP *:ipp (LISTEN)
cupsd     6788            root    8u  IPv4        0t0     TCP *:ipp (LISTEN)
```

Figura 124 - Puertos asociados a "Compartir impresora"

Se recomienda evaluar y ajustar en detalle las impresoras que son compartidas, así como los usuarios y grupos que tendrán capacidad para imprimir en ellas, debiéndose ***minimizar el acceso a lo imprescindible*** para el propósito por el que ha sido habilitado el servicio.

10.1.5 SESIÓN REMOTA

Desde macOS High Sierra 10.13, las utilidades de terminal "`telnet`" y "`ftp`" no están incluidas en macOS, recomendándose el uso de "`ssh`" (sesión remota) y "`sftp`" (transferencia segura de archivos) en su lugar.

El servicio "Sesión remota" (*Remote Login*) no está activo por defecto. Cuando se habilita marcando el "*tick*", se habilitará por defecto el acceso a usuarios "Administradores". Desde el punto de vista se seguridad, ***se recomienda inhabilitar el acceso de usuarios privilegiados***, modificando 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. Una vez establecida la sesión, se podrá invocar el comando "`su -`" para obtener acceso como administrador:

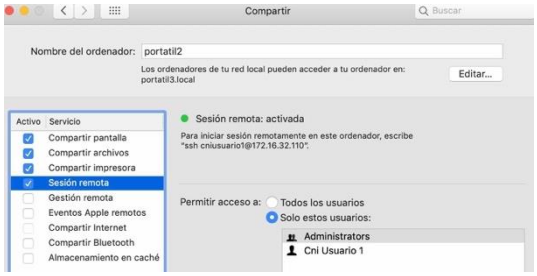


Figura 125 - Menú de configuración de "Sesión remota"

La conexión al equipo a través de otro ordenador con un cliente SSH o SFTP, se hará especificando el nombre de usuario y la dirección IP o nombre del equipo: "`ssh usuario@<dirección IP o nombre del equipo>`".

El puerto TCP empleado por defecto por Sesión remota para el servicio SSH (TCP/22) puede ser modificado en el fichero PLIST de configuración del demonio "`sshd`", "`/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>
```

Figura 126 - Modificación del puerto para sesión remota en el fichero "ssh.plist"

El comando "`systemsetup`" permite, a través de las opciones "`-getremotelogin`" y "`-setremotelogin on|off`", consultar, habilitar y deshabilitar respectivamente las sesiones remotas.

A través del "Monitor de Actividad" (*Activity Monitor*) se puede determinar qué sesiones SSH están activas en el sistema:

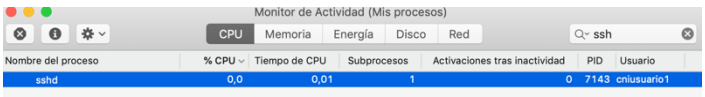


Figura 127 - Sesiones "ssh" activas en el sistema

10.1.6 EVENTOS APPLE REMOTOS

El servicio de "Eventos Apple remotos" habilita a un programa AppleScript que esté ejecutando en otro equipo a realizar acciones sobre el ordenador propio, incluyendo la ejecución de comandos y el acceso a ficheros.

La directriz "`of machine "eppc://<dirección_IP>"`" en el script establece que el recurso referenciado no es local, sino un servidor remoto al que se debe pasar un evento Apple. El sistema solicitará las credenciales de usuario la primera vez que se invoque el script, permitiendo su almacenamiento en el llavero.

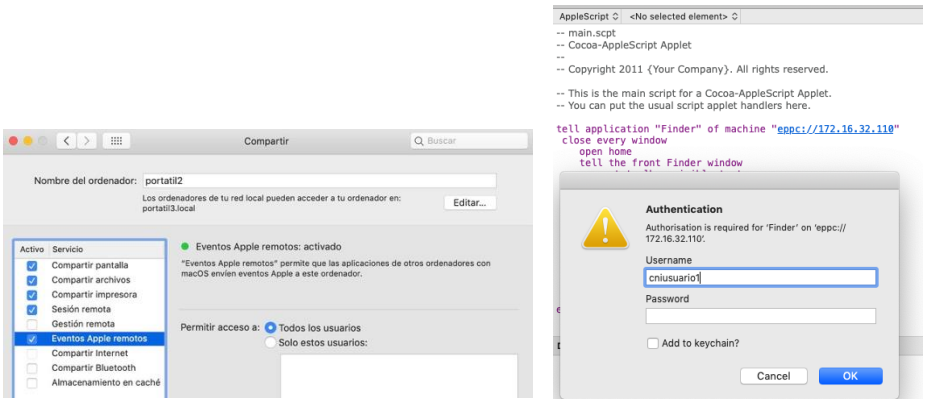


Figura 128 - Configuración y ejemplo de ejecución de un script basado en Eventos Apple remotos

NOTA: los lenguajes de scripting quedan fuera del alcance de la presente guía. Si se desea profundizar en la utilización de AppleScript, existen diversos recursos en Internet. Por ejemplo, el incluido en la [Ref.- 15].

Debido a las implicaciones de seguridad que tiene esta funcionalidad, ***la recomendación general es asegurarse de que está deshabilitada***, bien mediante el interfaz gráfico, bien a través de la utilidad "`systemsetup`". En caso de requerirse por cualquier razón su utilización, se debe restringir qué usuarios podrán hacer uso de esta funcionalidad, intentando evitar el acceso como administrador.

```
$ sudo systemsetup -getremoteappleevents
Remote Apple Events: On

$ sudo systemsetup -setremoteappleevents off
```

Figura 129 - Uso de la herramienta "systemsetup" para la gestión de Eventos Apple remotos

El servicio de "Eventos Apple remotos" escucha en el puerto TCP/3031 (`eppc`, *Remote AppleEvents/PPC Toolbox*):

```
launchd    1    root    63u  IPv6 0x2af9b8ff5c659d9f      0t0     TCP *:eppc (LISTEN)
launchd    1    root    64u  IPv4 0x2af9b8ff5cd5b71f      0t0     TCP *:eppc (LISTEN)
launchd    1    root    65u  IPv6 0x2af9b8ff5c659d9f      0t0     TCP *:eppc (LISTEN)
launchd    1    root    66u  IPv4 0x2af9b8ff5cd5b71f      0t0     TCP *:eppc (LISTEN)
```

Figura 130 - Puertos utilizados por el servicio "Eventos Apple remotos"

El fichero de configuración del demonio reside en "`/System/Library/LaunchDaemons/com.apple.eppc.plist`". Se recomienda proceder a

deshabilitarlo si no se va a hacer uso del servicio (ver apartado "7.1.3. Impedir el arranque de servicios en macOS").

10.1.7 COMPARTIR INTERNET

El servicio "Compartir Internet" permite compartir la conexión existente en el ordenador Mac hacia Internet, disponible a través del interfaz de red especificado por la opción "Compartir conexión desde:" (Bluetooth PAN, Wi-Fi, Thunderbolt Ethernet, Puente Thunderbolt, etc.) con los equipos disponibles a través del interfaz de red especificado por la opción "Con ordenadores vía:" (Bluetooth PAN, Wi-Fi, Thunderbolt Ethernet, etc.); es necesario que los interfaces (o puertos) a través de los cuales se desea compartir la conexión estén activos [Ref.- 96].

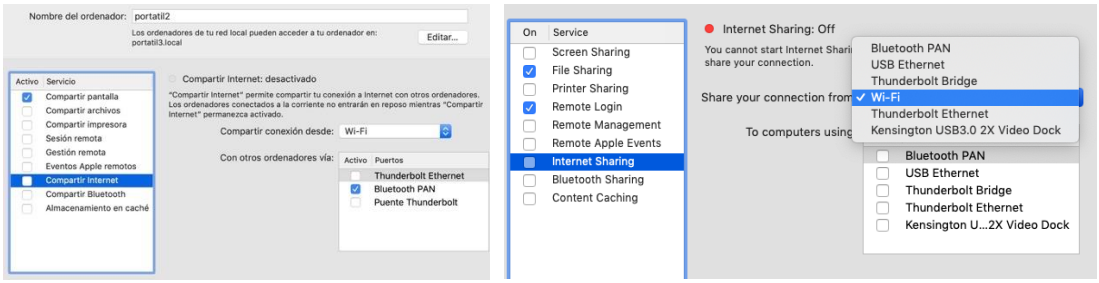


Figura 131 - Menú "Compartir Internet" (en español e inglés)

Si la compartición de la conexión con otros equipos se va a realizar mediante un *hotspot* Wi-Fi (opción "Con ordenadores vía:" con valor "Wi-Fi"), el menú "Opciones de Wi-Fi..." permitirá definir el nombre de la red Wi-Fi que será creada, el canal empleado, y el tipo de seguridad (abiertas o WPA2 Personal). ***Se recomienda utilizar*** "WPA2 Personal" y ***asignarle una contraseña suficientemente robusta***. También ***se recomienda cambiar el nombre de la red de forma que no coincida con el definido en el campo*** "Nombre del ordenador", para no permitir la fácil identificación del mismo:

Figura 132 - Creación de un hotspot Wi-Fi

En la [Ref.- 97] se proporcionan detalles sobre el uso de *hotspots* Wi-Fi en los que el Mac actúa de cliente de la conexión.

Por su parte, la opción "Compartir - Conexión a Internet" también habilita la compartición de la conexión a Internet del Mac con dispositivos iOS (iPhone y iPad) que se encuentren conectados a través de un puerto USB (esta arquitectura se denomina *tethering*, aunque en este caso es inversa, al compartir el Mac su conexión con el dispositivo iOS, y no al revés - situación más habitual de *tethering*).

Desde el punto de vista de seguridad, ***se recomienda la utilización de un* hotspot *Wi-Fi propio frente a conectar el equipo a redes Wi-Fi públicas***.

Se recomienda desactivar la compartición de Internet tan pronto finalice la necesidad de utilizarla.

10.1.8 COMPARTIR BLUETOOTH

El servicio "Compartir Bluetooth" permite configurar el intercambio de archivos a través de Bluetooth (en adelante, referenciado como BT por abreviar) con otros dispositivos. La opción "Abrir el panel de preferencias Bluetooth..." permite acceder al menú "Preferencias del sistema - Bluetooth".

Si el servicio se habilita, los dispositivos conectados con el equipo mediante BT tendrán la capacidad de intercambiar archivos con él y de explorar la carpeta configurada en la sección "Carpetas que otros pueden explorar". Desde el punto de vista de seguridad, ***se recomienda establecer las siguientes opciones***:

- **Al recibir ítems**: fijar a "Preguntar qué hacer" para solicitar autorización al usuario, o la opción "No permitir nunca" si se desea enviar elementos vía BT, pero no recibirlos.
- **Cuando exploren otros dispositivos**: fijar a "Preguntar qué hacer" para solicitar autorización al usuario, o la opción "No permitir nunca" si no se desea que otros dispositivos puedan explorar el equipo.
- ***No habilitar la compartición vía BT*** salvo que no exista una alternativa mejor, y, en ese caso, ***proceder a deshabilitarla tan pronto finalice la necesidad***.

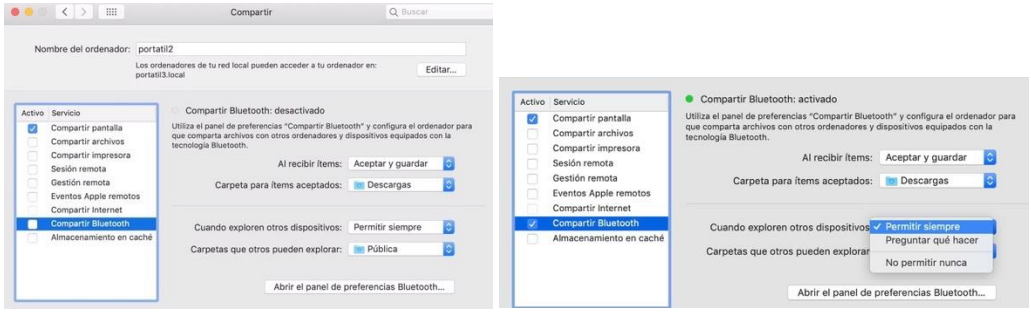


Figura 133 - Menús para "Compartir Bluetooth"

El envío de archivos mediante BT se lleva a cabo accediendo al icono de BT de la barra de menús de estado, pinchando sobre el dispositivo emparejado y eligiendo "Enviar archivo al dispositivo...". Esta acción lanzará la app "Intercambio de archivos Bluetooth", que se mostrará en el Dock. Al seleccionarla, se desplegará una ventana de Finder desde la que se puede navegar para elegir el archivo a enviar. macOS mostrará una ventana de diálogo solicitando permisos de acceso a esta app por el sistema:

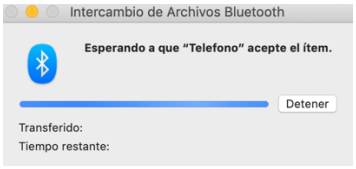


Figura 134 - Proceso de intercambio de archivos mediante Bluetooth

El agente encargado de la transferencia de archivos a través de BT reside en "`/System/Library/CoreServices/ObexAgent.app`".

10.1.9 ALMACENAMIENTO EN CACHÉ

Una "caché de contenido" es un servicio por el cual el *software* distribuido por Apple y los datos descargados de iCloud por un equipo concreto son almacenados en este servicio y puestos a disposición de otros equipos de la misma red, con el fin de acelerar descargas de grandes cantidades de datos (por ejemplo, actualizaciones de sistema operativo, *drivers*, documentos de iCloud, etc.).

La descripción detallada de este servicio puede encontrarse en la sección "Acerca del almacenamiento en caché del contenido en el Mac" del "Manual de usuario de macOS", accesible desde el símbolo "?" de cualquier submenú de "Preferencias del sistema" y disponible en versión *on-line* en la [Ref.- 98].

El servicio "Compartir Almacenamiento en caché" permite configurar el Mac como un servidor de caché de contenido, al cual, una vez activado, se podrán conectar otros equipos de la red para descargar dicho contenido.

Por su parte, en el equipo cliente macOS, existe un *framework* denominado "`AssetCacheLocatorService`", que se gestiona desde el agente de sistema "`/System/Library/LaunchAgents/com.apple.AssetCacheLocatorService.plist`", y que inicia un proceso de descubrimiento periódico o siempre que alguna app consumidora de contenidos se inicia (por ejemplo, la App Store). El proceso recopila la información de la IP de la red local, busca un registro DNS TXT especial (`_aaplcache._tcp.`), y envía la información a "lcdn-locator.apple.com". Apple analiza los rangos de IPs de la red WAN (pública) y los de la red LAN (privada) y envía una configuración que se escribe en el fichero "`$DARWIN_USER_CACHE_DIR/C/com.appleAssetCacheLocatorService/diskcache.plist`"[40].

Al activar por primera vez la opción del menú "Almacenamiento en caché", aparecerá un mensaje "Iniciando almacenamiento en caché de contenido" según lo establecido en los menús "Caché" y "Opciones". Cuando finalice la inicialización, se mostrará la siguiente ventana:

[40] https://themacwrangler.wordpress.com/2016/06/14/when-apple-caching-server-just-cant-even-right-now/

Figura 135 - Inicialización del servicio de caché de contenido

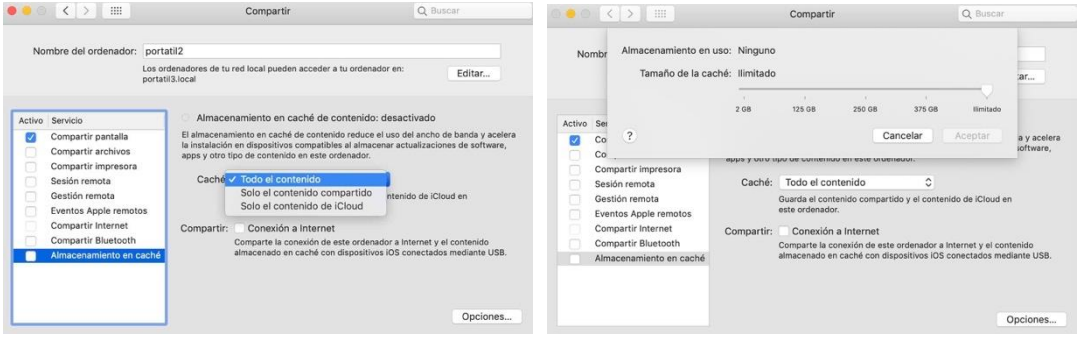


Figura 136 - Opciones de "Almacenamiento en caché"

Se recomienda limitar el contenido que se comparte a lo mínimo necesario:

- **Todo el contenido**: actualizaciones de sistema operativo, apps descargadas de Apple y contenido de iCloud.
- **Solo el contenido compartido**: actualizaciones de sistema operativo y apps descargadas de Apple.
- **Solo el contenido de iCloud**: incluyendo fotos, documentos, etc., pero no descargas de *software*.

La detección de servidores de caché de contenido por parte de otros ordenadores Mac en diferentes escenarios (ordenadores que están en la misma red local, que utilizan la misma dirección IP pública para conectarse a Internet, conectados a otra red local, etc.) puede configurarse desde el menú "Compartir - Almacenamiento en caché": al pulsar sobre la tecla "⌥ " (`Opción`), el botón "Opciones..." se transformará en "Opciones avanzadas...", que, al pulsarse, desplegará una ventana con las diversas opciones de configuración como, por ejemplo, la pestaña "Clientes" que permite configurar los distintos escenarios mencionados previamente (ver <Figura 137>).

El fichero de configuración del servicio reside en "`/Library/Preferences/com.apple.AssetCache.plist`"; su configuración avanzada se detalla en las referencias [Ref.- 100] y [Ref.- 99].

Figura 137 - Opciones avanzadas de configuración de "Almacenamiento en caché"

La utilidad "AssetCacheManagerUtil" permite gestionar el servidor de almacenamiento en caché. Con la opción "deactivate" deshabilitará el servicio, y con "activate" lo activará.

La utilidad "AssetCacheLocatorUtil" permite obtener información en el cliente sobre el servidor de caché de contenidos descubierto. Por ejemplo, el siguiente comando proporciona información sobre el servidor de contenidos descubierto en el cliente donde se ejecuta[41]:

```
$ AssetCacheLocatorUtil 2>&1 | grep guid | awk '{print$4}' | sed
's/^\(.*\):.*$/\1/' | uniq
```

Figura 138 - Comando para obtener la IP del servidor de caché de contenidos utilizado en un cliente

Por su parte, el siguiente comando permite monitorizar la actividad del servidor de caché de contenidos:

```
$ log show --style compact --predicate 'subsystem == "com.apple.AssetCache"'
| tail
```

Figura 139 - Comando para la monitorización del servidor de caché de contenidos

Desde el punto de vista de seguridad, ***se aconseja deshabilitar en el cliente la detección de servidores de caché de contenidos***, ya que cualquier vulnerabilidad en la implementación del servicio podría dar lugar a ataques de suplantación que permitieran la carga de contenidos maliciosos en los clientes macOS.

El servicio de caché de contenidos se puede deshabilitar siguiendo el procedimiento descrito en el apartado "7.1.3. Impedir el arranque de servicios en macOS":

```
$ launchctl unload -w
/System/Library/LaunchAgents/com.apple.AssetCacheLocatorService.plist
```

Figura 140 - Inhabilitación del agente cliente de servidores de caché de contenidos

11.SERVICIOS DE APPLE

Los servicios de Apple están estrechamente ligados al ID de Apple (Apple ID) y a la cuenta de iCloud con la que se haya iniciado sesión en el equipo. La descripción exhaustiva de estos servicios queda fuera del ámbito de la presente guía, pero se proporcionará una breve descripción de los principales servicios y funcionalidades, y de las principales recomendaciones de seguridad asociadas[42].

[41] https://krypted.com/tag/mac-servers/

[42] La descripción detallada de los servicios de Apple se abordará en una guía CCN-CERT independiente [Ref.- 404].

11.1 CUENTAS ASOCIADAS A LOS SERVICIOS DE APPLE

11.1.1 APPLE ID

El ID de Apple (o Apple ID) es un identificador o cuenta de usuario que identifica al usuario en la base de datos de servicios de Apple, así como en diversas aplicaciones y productos de Apple, como la App Store e iCloud [Ref.- 112].

Cuando se da de alta un nuevo usuario en el sistema operativo y éste accede por primera vez, se le solicitará aceptar la política de privacidad y se le sugerirá la configuración para iniciar sesión con un ID de Apple, o la creación de uno nuevo si no se dispone de él, así como la activación de Siri (***que se recomienda denegar***), y el aspecto que se desea para el interfaz gráfico. El ID de Apple no es requisito indispensable para el acceso del usuario al sistema, ni para que se pueda utilizar el equipo, pero sin él ciertos servicios no estarán disponibles (por ejemplo, la instalación y actualización de apps del mercado oficial o App Store):

Figura 141 - Configuración del ID de Apple al iniciar sesión por primera vez en el Mac

El Apple ID actúa como un vínculo entre todos los dispositivos Apple del usuario que lo comparten, y en el caso de macOS, solo puede existir un Apple ID dado de alta en el equipo por cada usuario (vinculado al perfil de usuario de sistema operativo). ***Se recomienda que el correo electrónico utilizado como Apple ID no contenga el nombre de usuario de sistema operativo***.

Dada la extrema sensibilidad de los servicios vinculados al ID de Apple, ***se recomienda proteger esta cuenta con un doble factor de autentificación*** (2FA; los ID de Apple creados con macOS Mojave lo tienen habilitado por defecto) siguiendo las instrucciones de la [Ref.- 111]. Además, ***la contraseña deberá ser suficientemente robusta, se deberá cambiar con regularidad y no deberá coincidir con ninguna otra contraseña que el usuario emplee para otros servicios***.

El ID de Apple se puede añadir o modificar desde el menú "Usuarios y grupos - <botón derecho sobre un usuario> - Opciones avanzadas - [ID de Apple] - Definir../Cambiar...". El ID de Apple se vincula a una cuenta de correo electrónico propiedad del usuario:

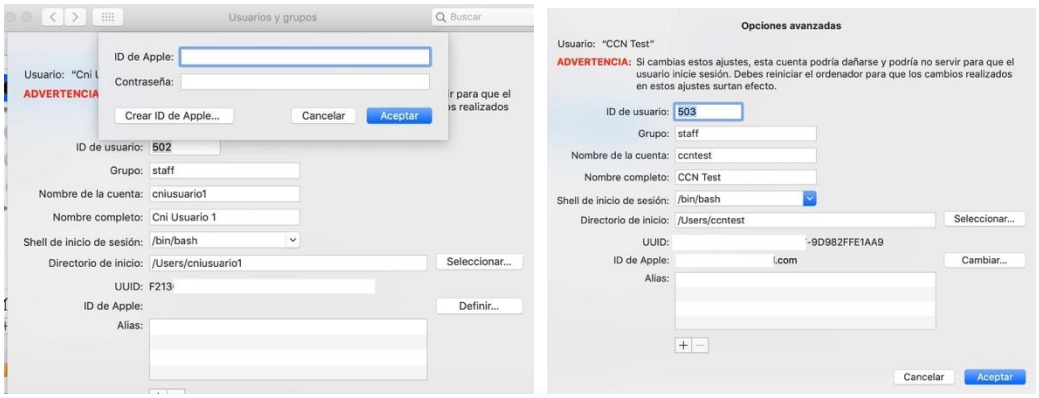


Figura 142 - Creación/modificación del ID de Apple de un usuario en macOS

A la hora de añadir el ID de Apple ("Definir..."), si se opta por hacer uso del botón "Crear ID de Apple...", se abrirá un navegador web con "https://appleid.apple.com", desde donde se debe indicar qué cuenta de correo electrónico se vinculará a este Apple ID. Una vez validado el código que Apple enviará a dicha cuenta de correo, el sistema solicitará al usuario confirmación para utilizarla en otras apps de macOS (imagen izquierda de la <Figura 143>).

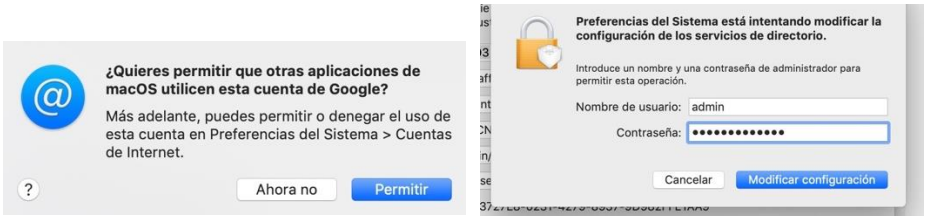


Figura 143 - Confirmación para utilizar la cuenta de correo electrónico vinculada al ID de Apple

Para poder añadir la cuenta al directorio de servicios, el sistema solicitará volver a introducir las credenciales de administrador (imagen derecha de la <Figura 143>).

11.1.2 CUENTA DE ICLOUD

iCloud es un servicio proporcionado por Apple que se emplea por parte de múltiples herramientas y servicios de sincronización y acceso a datos desde diferentes dispositivos (por ejemplo, contactos, calendarios, recordatorios, etc.). Para hacer uso de este servicio es necesario disponer de una cuenta de usuario en iCloud (en adelante abreviada como "cuenta de iCloud"), que está asociada o corresponde a un Apple ID.

Es posible prescindir de esta cuenta durante el uso del sistema, pero determinados servicios no podrán ser utilizados. La principal utilidad de la cuenta de iCloud desde el punto de vista de seguridad es que el servicio "Buscar mi Mac" está vinculado a ella.

Cuando se da de alta la cuenta de iCloud en el equipo, debe especificarse el ID de Apple que se desea utilizar. Para dar de alta una cuenta de iCloud, se debe acceder a "Preferencias del sistema - iCloud":

Figura 144 - Proceso de alta de una cuenta de iCloud para el usuario

Se recomienda valorar cuidadosamente la sensibilidad de la información asociada a los distintos servicios compartidos y disponibles vía iCloud, y deshabilitar todos aquellos cuyos datos no se desea almacenar en la nube de Apple. La opción más conservadora (y recomendada desde el punto de vista de privacidad) es elegir "No fusionar" para los servicios propuestos en la <Figura 144> y proceder posteriormente a deshabilitar otros servicios sobre los cuales el sistema no solicita autorización.

El proceso de alta de la cuenta de iCloud solicitará permiso de ubicación para la funcionalidad "Buscar mi Mac", que se recomienda conceder.

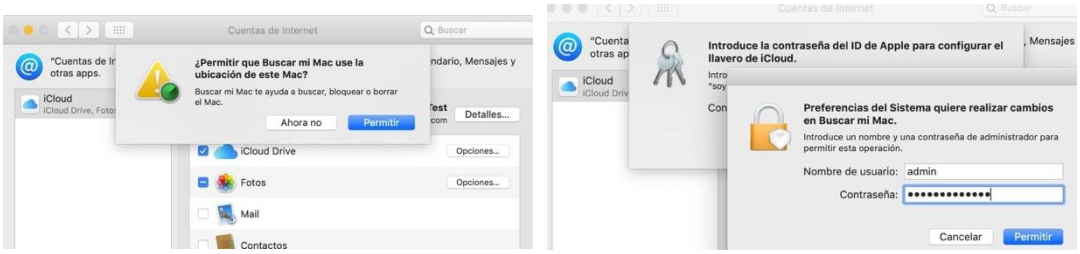


Figura 145 - Permiso de ubicación para "Buscar mi Mac" mediante iCloud

Por último, macOS solicitará de nuevo la contraseña asociada al ID de Apple para proceder a configurar el llavero de iCloud (debe de evaluarse minuciosamente si se hará uso del llavero de iCloud, ya que los datos más sensibles serán almacenados en la nube):

Figura 146 - Solicitud de la contraseña del ID de Apple para configurar el llavero de iCloud

Una vez configurada la cuenta de iCloud para el usuario, ***se recomienda:***

- ***Suprimir todas las apps que almacenen contenido sensible*** del menú o pestaña "Documentos" disponible desde el botón "Opciones..." de la categoría "iCloud Drive", accesible desde "Preferencias del sistema - iCloud".
- ***Desmarcar todas las opciones o categorías de sincronización salvo*** "Buscar mi Mac".

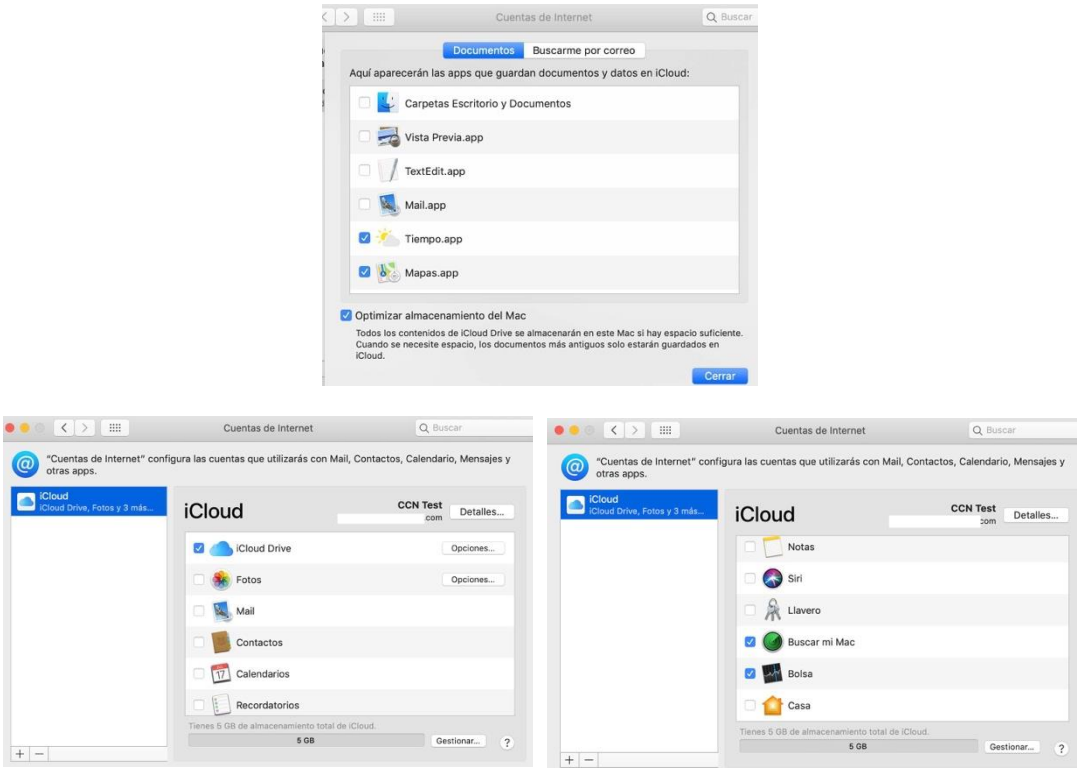


Figura 147 - Selección de los elementos a gestionar a través de iCloud

Además de por cuestiones de privacidad, las recomendaciones anteriormente expuestas se deben al enorme impacto de seguridad y privacidad que tendría que un tercero tomase control sobre la cuenta de iCloud del usuario.

Es posible otorgar permiso de acceso a la cuenta de iCloud a apps de terceros (por ejemplo, para hacer copias de seguridad de sus datos).

11.1.2.1 DISPOSITIVOS ASOCIADOS A LA CUENTA DE ICLOUD

Los dispositivos que tengan configurada una misma cuenta de iCloud aparecerán en el menú "Mis dispositivos" dentro del interfaz web de "icloud.com" y en el menú del Mac "Preferencias del sistema - iCloud - Detalles de la cuenta - Dispositivos".

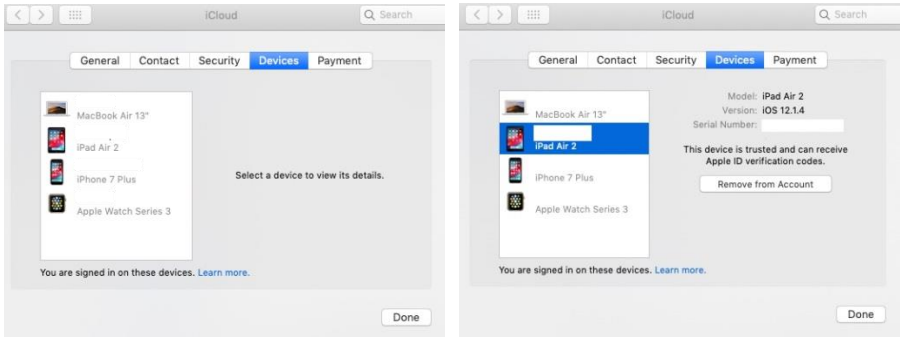


Figura 148 - Dispositivos vinculados a la cuenta de iCloud (inglés)

Seleccionando un dispositivo concreto, es posible darlo de baja de la cuenta, con lo que dejará de ser un dispositivo de confianza. Si se habían invocado operaciones de gestión remota de este dispositivo mediante la funcionalidad "Buscar mi Mac" descrita en el apartado "11.3. Buscar mi Mac (Find my Mac)", que hubiesen sido encoladas por encontrarse el dispositivo inaccesible vía Internet cuando se solicitaron, estas operaciones se desestimarán, y no tendrán efecto.

Desde el punto de vista de seguridad, ***es muy importante dar de baja de la cuenta de iCloud aquellos dispositivos que dejen de pertenecer al usuario***, evitando así que puedan recibir códigos de segundo factor de autentificación si el dispositivo está considerado como de confianza (*trusted*). Previamente, se recomienda proceder al borrado completo de los datos de dichos dispositivos.

Para dar de baja el propio Mac de la cuenta de iCloud, se puede:

- Deshabilitar el componente "Buscar mi Mac" de la lista de apps de iCloud.
- Cerrar la sesión de iCloud (los datos asociados a iCloud serán eliminados del equipo): esta opción es la recomendada si el equipo va a pasar a manos de un tercero.

En ambos casos se solicitará confirmación de la contraseña asociada al Apple ID.

Se recomienda la lectura del apartado "17. Eliminación de los datos del ordenador" para disponer de una visión detallada de las acciones necesarias que deben llevarse a cabo para restablecer el equipo a fábrica completamente.

11.2 GAME CENTER

"Game Center" es una red social de Apple vinculada a juegos en red, cuyo objetivo es proporcionar una experiencia de usuario centrada en la interconexión entre miembros de un mismo grupo.

Esta cuenta se crea por defecto bajo "Preferencias del sistema - Cuentas de Internet"; por defecto, al acceder a ella se dará la opción de vincularla al Apple ID del usuario.

Desde el punto de vista se seguridad, ***se aconseja eliminar esta cuenta de Game Center del sistema***.

11.3 BUSCAR MI MAC (FIND MY MAC)

El servicio "Buscar mi Mac" ("*Find my Mac*", FMM), vinculado a la existencia de una cuenta de iCloud activa con permisos para utilizar este servicio en el ordenador, permite gestionar remotamente el equipo Mac, incluyendo:

- Ubicarlo en un mapa: si en el momento actual el equipo no dispone de conexión a Internet, se mostrará la última ubicación obtenida.
- Hacer que emita una señal acústica, bloquearlo o eliminar todos tus datos: todos estos servicios requieren que el Mac disponga de conexión a Internet; en caso contrario, las peticiones se encolarán y se enviarán al equipo una vez sea posible contactar con él a través de la red. Si el equipo se da de baja de la cuenta de iCloud por parte del usuario, las peticiones encoladas se desestimarán.

Cuando FMM está habilitado, escribe en la NVRAM los siguientes parámetros (disponibles mediante "`nvram -p -x`"), que persisten aunque cambie la versión del sistema operativo, incluso si se lleva a cabo un volcado completo de la imagen de sistema.

- `fmm-mobileme-token-FMM <token>`: corresponde a un fichero "`.plist`" binario codificado en base64 que contiene la configuración de FMM. Entre otros elementos, incluye el authToken, el ID de Apple del usuario y otros metadatos del equipo.
- `fmm-mobileme-token-FMM-BridgeHasAccount BridgeHasAccountValue`: *no existe ninguna documentación pública sobre este parámetro*.
- `fmm-computer-name`: corresponde al "*Computer Name*" (ver apartado "12.1.1. Nombre del equipo").

Los servicios asociados a FMM se definen desde:

- "`/System/Library/LaunchDaemons/com.apple.findmymac.plist`".
- "`/System/Library/LaunchAgents/com.apple.icloud.findmydeviced.findmydevice-user-agent.plist`".

Tras el arranque del sistema, el demonio FMM establece una conexión con el servidor de iCloud, enviándole los datos para la geolocalización del equipo cuando se le requieran y escuchando los comandos que dicho servidor le envíe.

El borrado de las variables "`fmm-computer-name`" y "`fmm-mobileme-token-FMM`" a través del comando "`nvram -d <variable>`" invocado con privilegios de administración inhabilitaría la función "Buscar mi Mac"[43]. Consecuentemente, el restablecimiento de la NVRAM también inhabilitaría FMM (ver apartado "18.5. Modo de restablecimiento de la NVRAM"), por lo que, para evitar ese escenario, ***se recomienda establecer una contraseña de firmware en el ordenador*** (ver apartado "18.1. Contraseña de firmware").

[43] https://clburlison.com/find-my-mac/
https://ilostmynotes.blogspot.com/2013/11/disable-find-my-mac-by-modifiying-nvram.html

El proceso de configuración de "Buscar mi Mac" se describe en la página oficial de soporte de Apple [Ref.- 113]. De forma resumida, requiere que el servicio de localización esté activo para el componente "Buscar mi Mac" (ver apartado "8.2.4.4. Localización") y que se haya concedido a iCloud el correspondiente permiso para hacer uso de este servicio (ver <Figura 145> y <Figura 147>).

Para utilizar el servicio, se dispone de dos alternativas:

- Acceder mediante un navegador web a la dirección "https://icloud.com/#find".
- Abrir la app "Buscar mi iPhone" en un dispositivo iOS que tenga el Mac dado de alta en la app (esto sucederá si comparten el mismo ID de Apple).

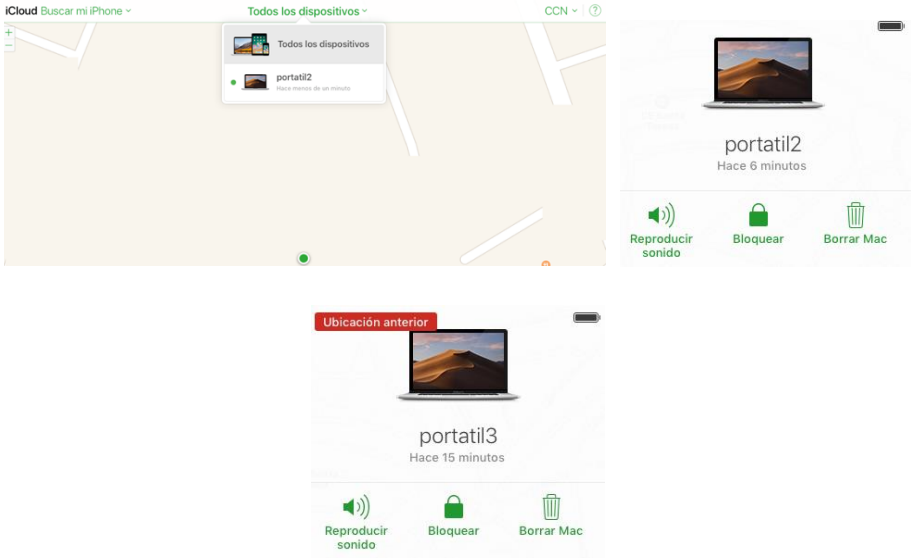


Figura 149 - Pantalla de "icloud.com/#find" con la ubicación de los dispositivos

Si se intenta cerrar sesión en la cuenta de iCloud en el equipo, el sistema desactivará la funcionalidad "Buscar mi Mac", pero para ello solicitará la contraseña del ID de Apple, impidiendo que un tercero que desconozca la contraseña pueda deshabilitar la cuenta. Si esta contraseña no es proporcionada, el sistema no cerrará la sesión de iCloud. El cierre de la sesión provocará que el campo "ID de Apple" de la sección "Usuarios y grupos - <Usuario> Opciones avanzadas" se resetee, ya que el ID de Apple vinculado al usuario de sistema operativo corresponde al de la cuenta de iCloud (y no al ID de Apple que se puede usar en otros servicios adicionales de Apple, como App Store).

Figura 150 - Solicitud de la contraseña del ID de Apple para proceder al cierre de sesión en iCloud

Es importante reseñar que la funcionalidad "Buscar mi Mac" permanece operativa aunque la pantalla esté bloqueada y aunque el usuario haya cerrado su sesión en el sistema. Sin embargo, si el equipo se reinicia y ningún usuario inicia sesión, "Buscar mi Mac" no podrá conectar con el equipo si el disco está cifrado con FileVault (opción recomendada desde el punto de vista de seguridad). Todas las acciones que se inicien desde el interfaz de "Buscar mi Mac" quedarán pendientes hasta que el disco sea desbloqueado mediante un inicio de sesión válido.

Figura 151 - "Buscar mi Mac": notificación de "Sonido pendiente" de la opción "Reproducir sonido"

NOTA: es importante diferenciar entre la contraseña de *firmware* establecida desde el menú de recuperación (ver apartado "18.1. Contraseña de firmware") y la contraseña de *firmware* de un solo uso que se establece desde el menú "Bloquear mi Mac" disponible como parte del servicio "Buscar mi Mac" de iCloud.

Existe un usuario en el sistema que gestiona el servicio FMM, y que se puede visualizar desde la "Utilidad de Directorios - Editor de directorios" (ver apartado "8.1.6. Directorio de Servicios"):

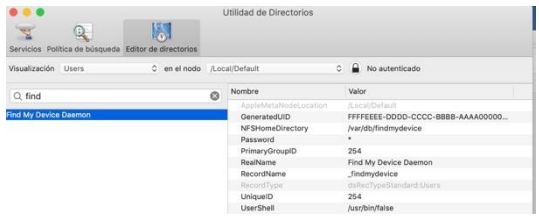


Figura 152 - Usuario de sistema asignado a "Buscar mi Mac"

REPRODUCIR SONIDO

Al seleccionar esta opción, iCloud enviará al equipo un comando o evento para que emita una señal sonora, incluso aunque el equipo tenga el volumen desactivado. Paralelamente, se mostrará en pantalla el siguiente mensaje:

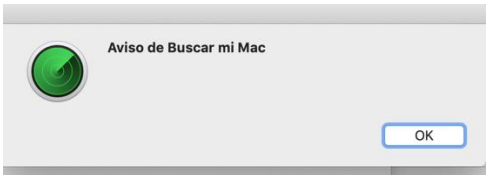


Figura 153 - "Buscar mi Mac": mensaje mostrado en el equipo al seleccionar "Reproducir sonido"

Un inconveniente detectado en la versión 10.14.5 de Mojave empleada en la elaboración de la presente guía es que el mensaje "Aviso de Buscar mi Mac" de la funcionalidad "Reproducir sonido" se muestra varios segundos antes de que el equipo

emita el sonido, lo cual es suficiente para que se acepte el mensaje y que el sonido no se llegue a reproducir, lo que permitiría que un potencial atacante con acceso a la pantalla pudiese desactivarlo.

BLOQUEAR

IMPORTANTE: si se desea realizar pruebas de esta funcionalidad, se recomienda realizar una copia de seguridad completa del ordenador, que permita restaurarlo en caso de un fallo en el proceso de desbloqueo.

La función "Bloquear" reinicia el equipo en un modo especial de recuperación, del que solo es posible salir tecleando físicamente en el equipo el código PIN de 6 dígitos que el usuario haya configurado en el menú de FMM en iCloud. También permite definir un mensaje, típicamente invitando a quien esté en posesión del ordenador a que se ponga en contacto con el propietario:

Figura 154 - "Buscar mi Mac": opción "Bloquear" del servicio de iCloud

En el menú de iCloud asociado a FMM, se mostrará la indicación de que el equipo ha sido bloqueado, y se ofrece la opción "Desbloquear", consistente en mostrar al usuario en la pantalla de iCloud la contraseña de bloqueo (previa comprobación de su identidad mediante la solicitud de la contraseña del ID de Apple asociado a la cuenta de iCloud, y de dos de las preguntas de seguridad que el usuario definió cuando dio de alta dicho ID):

Figura 155 - "Buscar mi Mac": opción "Desbloquear" del servicio de iCloud

Cuando el Mac perdido esté accesible a través de Internet, el servidor de iCloud enviará un comando "`lock`", que provoca que el equipo se reinicie en un modo especial

de recuperación (en las pruebas realizadas existe un retardo de más de 10 segundos) y almacene en NVRAM los siguientes valores[44]:

- "`good-samaritan-message`": corresponde al texto que se mostrará en la pantalla del equipo bloqueado, que incluye un texto fijo establecido por iCloud y el texto definido por el usuario durante la solicitud de bloqueo:

```
$ nvram -p | grep -i samaritan
good-samaritan-message    This Mac has been locked with Find My Mac.
%0a Didn't lock this Mac? Go to www.icloud.com/find to get the PIN to
unlock it.%0a"Contactar con <propietario>"
```

Figura 156 - "Buscar mi Mac": variable "good-samaritan-message" de la función "Bloquear"

- "`fmm-password-hash`": corresponde a un hash del PIN fijado en la acción "Bloquear" por parte del propietario de la cuenta de iCloud. Este valor se eliminará de la NVRAM una vez se desbloquee el equipo a través del PIN.
- "`security-pinType`": algoritmo de hash y cifrado del PIN.
- "`recovery-boot-mode=locked`": cuando el sistema arranca de la partición de recuperación o *recovery*, invoca a la app "Installer.app". Esta app comprueba el valor de la variable "`recovery-boot-mode`" y, si está "`locked`", invocará a la app "Lock.app", que muestra el PIN-Pad y el mensaje "`good-samaritan-message`" (ver imagen derecha de la <Figura 157>).
  Si se intenta reiniciar el equipo en modo de recuperación de forma manual, aparecerá en pantalla el menú de introducción de la contraseña de *firmware* (ver imagen izquierda de la <Figura 157>). Este modo de bloqueo impide que sea posible arrancar en modo de restablecimiento de la NVRAM:
  - Si el equipo dispone de contraseña de *firmware* (opción recomendada desde el punto de vista de seguridad), hay que introducirla.
  - Si no dispone de contraseña de *firmware*, se introducirá el código de desbloqueo configurado en FMM (teóricamente, esto implica que la función "Bloquear" de FMM está estableciendo como contraseña temporal de *firmware* el PIN de 6 dígitos definido en su menú).

  En ambos casos, una vez validada esta contraseña, se continuará con el proceso de arranque en modo de recuperación, que lanzará la app "Installer.app". De nuevo, esta app comprueba el valor de la variable "`recovery-boot-mode`" y, si está a "`locked`", invocará a la app "Lock.app", desde la que se lanza la pantalla de la imagen derecha de la <Figura 157>:

[44] https://www.ghostlyhaks.com/forum/macbook/65-icloud-wipeout-and-admin-access-on-efi-locked-mac

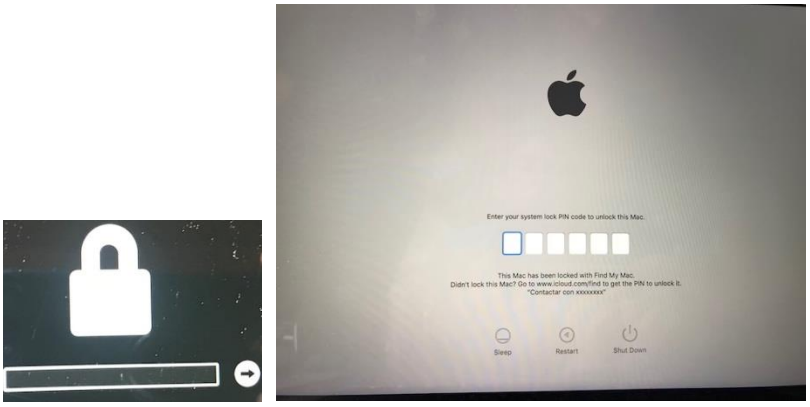


Figura 157 - "Buscar mi Mac": bloqueo del intento de arranque en modo de recuperación

Tras la validación del PIN, el Mac se reiniciará, presentando la pantalla de *login*. De este modo, si el disco está cifrado con FileVault, se impide que un tercero que llegase a introducir el código de desbloqueo correcto obtenga acceso a los datos.

BORRAR MAC

IMPORTANTE: si se desea realizar pruebas de esta funcionalidad, se recomienda realizar una copia de seguridad completa del ordenador, que permita restaurarlo en caso de un fallo en el proceso de recuperación.

La funcionalidad "Borrar Mac" [Ref.- 114] elimina los datos de los discos internos del Mac de forma permanente (no de las unidades externas conectadas), sin que sea posible volver a acceder a ellos aunque se disponga de todas las claves configuradas en el sistema. Únicamente se mantiene la partición de recuperación (*Recovery*).

Tras finalizar el borrado, el sistema entrará en modo de recuperación.

La clave "Media Key" de FileVault [Ref.- 43] se emplea por parte de la función "Borrar Mac": la operación sobrescribe los bloques de disco que contienen la clave y, sin ella, no es posible descifrar la clave de cifrado del volumen, por lo que, aunque el disco fuese extraído y montado en otro equipo, los datos no podrían accederse.

Si el equipo se ha dado por perdido, tras la compleción del comando "Borrar Mac" se aconseja eliminar el equipo de la cuenta de iCloud, a fin de que no quede ningún vínculo entre ambos. Para ello, una vez el equipo ya no es visible para iCloud (no puede establecer comunicación con él a través de Internet), se debe pulsar en el símbolo "x" a la derecha del nombre del equipo:

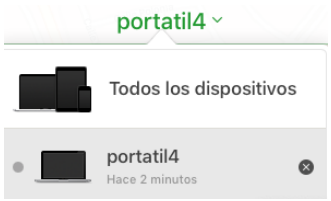


Figura 158 - Baja de un equipo de la cuenta de iCloud

11.4 SERVICIOS DE "CONTINUIDAD"

"Continuidad" (*Continuity*) es un conjunto de servicios que Apple introdujo con el propósito de permitir al usuario usar indistintamente los dispositivos vinculados a una misma cuenta de iCloud (es decir, vinculada al mismo Apple ID) para realizar una tarea determinada, que podía ser iniciada en cualquiera de ellos y retomada en otro, así como para establecer relaciones de confianza entre ellos.

El análisis detallado de los servicios de continuidad queda fuera del ámbito de la presente guía, y se abordará en la "Guía CCN-STIC-459 - Cuenta de usuario, servicios y aplicaciones de Apple" [Ref.- 404].

En la [Ref.- 116] se proporciona el recurso oficial de Apple para la configuración de los servicios de Continuidad, y en la [Ref.- 117] la lista con los dispositivos Apple para los cuales está soportada esta funcionalidad.

A modo de resumen, dado que los servicios de continuidad requieren que los dispositivos tengan habilitados los interfaces Wi-Fi y Bluetooth (BT), se desaconseja tenerlos permanentemente activos. Adicionalmente, el uso de estos servicios requiere que la mayoría de los contenidos que se intercambian pasen por los servidores de iCloud de Apple, por lo que debe sopesarse las implicaciones desde el punto de vista de la privacidad.

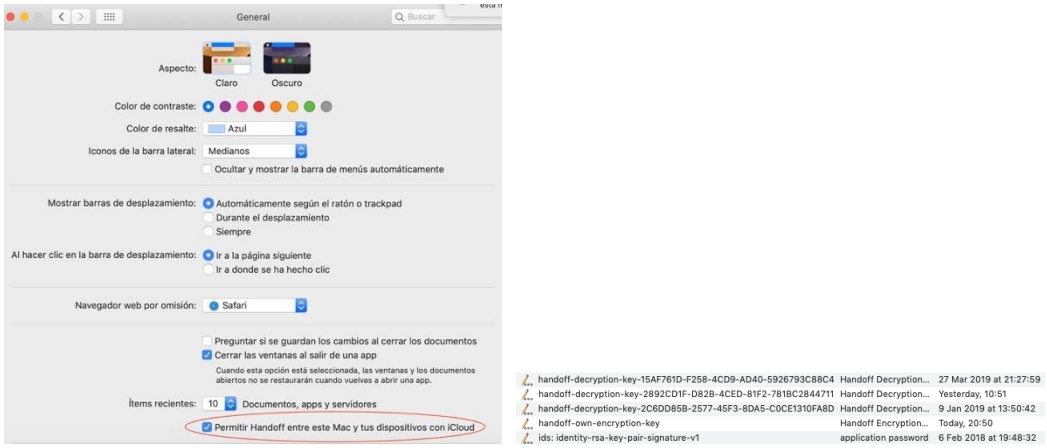


Figura 159 - Opción "Handoff" para servicios de "Continuidad" y claves asignadas a ellos

- **Handoff**: este servicio permite iniciar una app de Apple (por ejemplo, Mail o Safari) y retomar su actividad en otro dispositivo Apple que se encuentre en el rango de BT. Además de tener Handoff activado (en el Mac se controla desde el ajuste "Preferencias del Sistema - General - Permitir Handoff entre este Mac y tus dispositivos con iCloud"), requiere que los dispositivos tengan BT y Wi-Fi activos. Para evitar el uso accidental de Handoff, ***se aconseja mantener el ajuste desmarcado y proceder a su activación cuando se decida hacer uso del mismo***.
  Cuando se activa Handoff, el sistema añade unas claves de cifrado en la categoría "Contraseñas" del llavero "Inicio de sesión" (ver apartado "9.7. Gestión de llaveros").

- **Portapapeles universal**: este servicio permite que los contenidos que se copian en un dispositivo Apple se trasladen al portapapeles de otro dispositivo Apple cercano, desde el que se pueden pegar hasta que sean reemplazados por otro contenido o transcurra cierto tiempo. Sus requisitos son los mismos que los de Handoff, aplicando por tanto la misma recomendación de seguridad.
- **Recepción de llamadas telefónicas**: permite cursar y responder llamadas de un iPhone que se encuentre en la misma red Wi-Fi o Ethernet que el Mac. ***Se desaconseja su utilización en entornos laborales***, ya que podría ocurrir que el usuario se ausente brevemente de su puesto de trabajo y que un tercero pueda responder desde el Mac a la llamada que está siendo recibida en el teléfono del usuario.
- **Reenvío de mensajes**: permite el envío, recepción y sincronización de SMS desde cualquier dispositivo que comparta cuenta de iCloud, siempre que el iPhone disponga de conexión de red (vía Wi-Fi o de datos móviles). Las implicaciones de privacidad son especialmente importantes en este aspecto.
- **Instant Hotspot**: permite la utilización de un *hotspot* Wi-Fi proporcionado por un dispositivo móvil Apple, un iPhone o iPad, sin necesidad de autentificación por parte del dispositivo cliente (ordenador Mac), ni de habilitar expresamente el *hotspot* Wi-Fi en el dispositivo móvil. A diferencia de otros servicios de Continuidad, como Handoff, esta funcionalidad no exige ninguna acción expresa por parte del usuario, sino que está activa automáticamente por el mero hecho de tener ambos dispositivos con sesión iniciada en la misma cuenta de iCloud y los interfaces Wi-Fi y BT activos.
- **Desbloqueo automático**: permite el inicio de sesión en el Mac con un Apple Watch. Esta opción se considera muy peligrosa desde el punto de vista de seguridad, por lo que ***se desaconseja su utilización***. Esta funcionalidad puede ser desactivada mediante la opción "Preferencias del Sistema - Seguridad y privacidad - General - Permitir que el Apple Watch desbloquee el Mac".
- **Continuidad de cámara**: permite que las fotos tomadas con un iPhone, iPad y iPod se muestren en determinadas apps del Mac. Dado que requiere interacción voluntaria por parte del usuario en ambos dispositivos, y que la cuenta de iCloud disponga de doble factor de autentificación, este servicio se considera más seguro que otros.
- **Apple Pay**: solo está disponible para ordenadores Mac que dispongan de Touch ID.

11.5 SIRI

Siri es el asistente personal digital propietario de Apple, que incluye un sistema de reconocimiento de voz y lenguaje natural introducido por Apple en iOS 5.x, y que permite al usuario realizar multitud de tareas mediante comandos de voz.

El alcance de la presente guía no contempla la realización de un análisis de seguridad detallado de Siri y de sus protocolos de comunicaciones. Debido a que la información procesada por Siri es enviada a Apple (incluida la localización si la

funcionalidad "Siri y Dictado" está activa en la sección "Localización" del menú "Seguridad y privacidad - Privacidad") y a que, a lo largo de la historia, se han identificado numerosas vulnerabilidades en este servicio, ***la recomendación de seguridad y privacidad es evitar el uso de Siri en el Mac***. Para ello, desde el menú "Preferencias del sistema - Siri" hay que ***deshabilitar la opción*** "Activar "Consultar a Siri"".

Si, pese a la anterior recomendación, se decidiese hacer uso de Siri, ***se recomienda limitar las apps incluidas en el menú*** "Sugerencias de Siri y privacidad…", excluyendo la app Mail y la app Notas, que pueden albergar contenido sensible.

11.6 LLAVERO DE ICLOUD

El llavero de iCloud (iCloud *Keychain*) proporciona capacidades centralizadas de almacenamiento de credenciales en un repositorio vinculado a la cuenta de iCloud del usuario. En este repositorio se pueden almacenar credenciales (usuario y contraseña) de sitios web, apps, contraseñas de redes Wi-Fi, e información de tarjetas de crédito, entre muchos otros datos sensibles (ver apartado "9.7. Gestión de llaveros").

El llavero de iCloud permite almacenar el *keychain* local existente en macOS (ver apartado "9.7. Gestión de llaveros") en iCloud, de manera supuestamente segura, mediante la utilización de cifrado AES de 256 bits (AES 256), haciendo posible su utilización y compartición entre los diferentes dispositivos Apple asociados a una misma cuenta de iCloud, tanto móviles (iPhone, iPad, etc.) como tradicionales (Mac).

El llavero de iCloud solo sincroniza aquellos elementos del llavero del usuario que han sido identificados con el atributo que permite su sincronización entre dispositivos, es decir, que son exportables (o no son únicos para cada dispositivo). Por ejemplo, las identidades de redes VPN no son sincronizadas y compartidas, mientras que las credenciales empleadas por Safari o las contraseñas de redes Wi-Fi sí lo son. Por defecto, los elementos añadidos al llavero por las apps de terceros están identificados como no sincronizables, debiendo el desarrollador de la app modificar el atributo si desea que sea compartido entre diferentes dispositivos.

macOS se integra directamente con el llavero de iCloud, permitiendo el almacenamiento de credenciales y tarjetas de crédito, su reutilización, e incluso la generación y almacenamiento de nuevas contraseñas (a través de un generador de contraseñas). Esta funcionalidad se complementa con las capacidades de Safari para autocompletar formularios web.

La funcionalidad del llavero de iCloud se habilita/deshabilita a través de "Preferencias del sistema - iCloud - Llavero"). Si se desea desactivar el uso del llavero de iCloud, se podrá optar por mantener las credenciales almacenadas en el *keychain* local o eliminarlas del equipo.

Desde el punto de vista de seguridad, se debe valorar si se confía plenamente en Apple para la custodia en la nube de las contraseñas y otros datos sensibles, así como tener en cuenta que, al estar disponibles en todos los dispositivos de un usuario (se empleen o no todas las credenciales en todos los dispositivos), basta con que uno de ellos sea comprometido para que todas las contraseñas puedan quedar expuestas.

12. COMUNICACIONES

Los siguientes apartados describen las recomendaciones de seguridad asociadas a los interfaces de red y a las capacidades de comunicación de macOS.

12.1 AJUSTES DE RED A NIVEL DE SISTEMA

Los ajustes asociados al subsistema de red de macOS son gestionados por el demonio "`configd`" (*System configuration daemon*), quien mantiene la información sobre el estado actual del sistema y el estado al que se quiere llevar, y notifica a las apps sobre los cambios de configuración. Para ello, alberga una serie de subagentes, cada uno de los cuales es responsable de establecer y mantener una sección de la configuración:

- *KernelEventMonitor*: responsable de monitorizar eventos de kernel y transmitir el estado del enlace de red a otros agentes y apps interesadas.
- *InterfaceNamer*: responsable de asignar el nombre a los interfaces de red.
- *IPConfiguration* e *IP6Configuration*: gestionan el direccionamiento IPv4 e IPv6 respectivamente.
- *IPMonitor*: gestiona el enrutamiento, la configuración DNS y los proxies de red.
- *LinkConfiguration*: gestiona los interfaces de red Ethernet.
- *PreferencesMonitor*: traslada a los diferentes agentes los cambios de ajustes establecidos por el administrador del sistema.
- *PPPController*: gestiona las conexiones punto a punto (PPP).

Las características de seguridad a nivel de red implementadas por macOS Mojave se describen en la [Ref.- 58], sección "Seguridad de la red".

Los ajustes de red se encuentran accesibles, según la categoría, desde los menús "Preferencias del sistema - Red" y "Preferencias del sistema - Compartir". Alternativamente, se dispone de la utilidad de línea de comandos "`scutil`", que permite consultar (opción "`--get`") y modificar (opción "`--set`", que requiere permisos de administración) los ajustes de configuración.

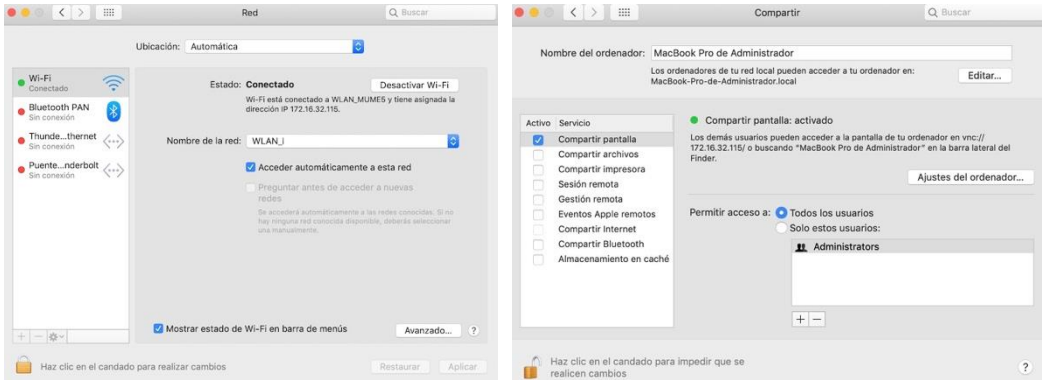


Figura 160 - Menús "Red" y "Compartir"

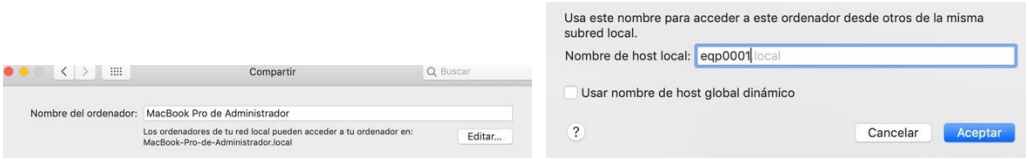
12.1.1 NOMBRE DEL EQUIPO

En macOS se distinguen tres atributos relacionados con el nombre del equipo, cada uno asignado a un propósito diferente:

- "Nombre de red" ("*HostName*"): representa el nombre que identifica de forma exclusiva al equipo en Internet (expresado como FQDN, *Fully Qualified Domain Name*), asociado a "`gethostname()`". El *hostname* se consulta y modifica a través de la utilidad "`scutil --get|--set HostName`" o del comando "`hostname`" (ver imagen inferior de la <Figura 161>).
- "Nombre del ordenador" ("*ComputerName*"): identifica al equipo dentro de la red local, para propósitos de compartición de elementos propios (ficheros, pantalla, impresión, etc.) con otros equipos miembros de la misma red. Este nombre también es el que identifica al equipo en las conexiones Bluetooth. Se configura desde el menú "Compartir", modificando directamente el campo "Nombre de host local" (ver imagen izquierda de la <Figura 161>).
- "Nombre local" ("*LocalHostName*" o "*Bonjour name*"): "Bonjour" es la implementación propia de Apple del denominado "*zeroconf*" (*zero-configuration networking [Ref.- 32]*). "Bonjour" permite la identificación del equipo dentro de la red local, y el descubrimiento de los servicios que el equipo ofrece, mediante mDNS (*multicast Domain Name System*), por ejemplo, AirDrop y compartición de iTunes. Por defecto, el "*Bonjour name*" toma el valor del "Nombre del ordenador" con la extensión "`.local`", pero se puede configurar uno alternativo desde el menú "Compartir - Editar - Nombre de host local" (ver imagen derecha de la <Figura 161>).

Por defecto, los distintos nombres de equipo asignados por macOS tras el proceso de configuración inicial son "`MacBook-Pro-de-<usuario>.local`", donde "`<usuario>`" es el nombre de la cuenta de usuario creada inicialmente durante este proceso inicial (en el ejemplo, "`Administrador`").

Se recomienda modificar los diferentes nombres del equipo de forma que no desvelen detalles ni del tipo de equipo, ni del sistema operativo empleado, ni del propietario u orgnización, ni de la cuenta de usuario. Tras esta operación, se recomienda limpiar la caché de DNS mediante el comando "`dscacheutil -flushcache`".




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

$ sudo hostname portatil
$ hostname
portatil
```

Figura 161 - Modificación de los diferentes nombres del equipo de macOS

12.2 INTERFACES DE RED

Los interfaces de red (o de comunicaciones) de macOS emplean para su designación la nomenclatura de BSD, que utiliza dos o tres letras en función del tipo de interfaz más un identificador numérico único del interfaz. El comando "`ifconfig`" mostrará la lista de interfaces del sistema en función de su tipo:

- `awdlX`: *Apple Wireless Direct Link* (AirDrop, AirPlay, etc).
- `bridgeX`: puente entre dos o más interfaces de red.
- `enX`: Ethernet, Wi-Fi, y Thunderbolt Ethernet.
- `fwX`: FireWire.
- `gifX`: *Generic tunnel Interface* (GIF) - IPv[4|6] sobre IPv[4|6].
- `loX`: Loopback.
- `p2pX`: Peer to Peer, P2P (AirDrop).
- `stfX`: 6to4 tunnel interface (IPv6 sobre IPv4).
- `utunX`: utilizado por el servicio "Volver a mi Mac" ("*Back to My Mac*") (aunque este servicio ya no está disponible en Mojave[45]) y otros servicios VPN.
- `XHC2X`: USB network interface.

Por su parte, 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. Por ejemplo, la salida del comando "`networksetup -listallnetworkservices`" refleja el estado de los servicios de red:

```
$ networksetup -listallnetworkservices
An asterisk (*) denotes that a network service is disabled.
Wi-Fi
Bluetooth PAN
Thunderbolt Bridge
VPN (Cisco IPSec)
```

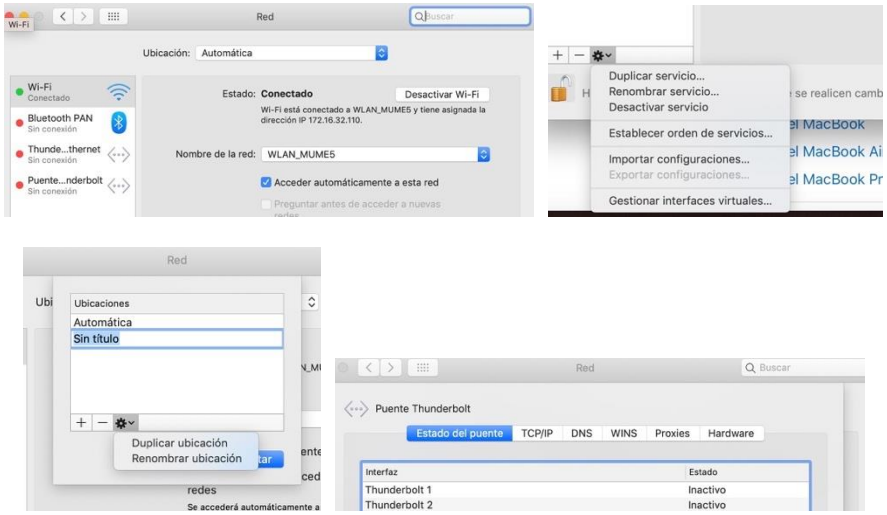
Figura 162 - Comando "networksetup" para listar los interfaces de red

El conjunto de interfaces de red disponibles por defecto puede variar dependiendo del modelo de ordenador Mac empleado y de su hardware asociado.

[45] https://support.apple.com/es-es/HT204618

No es sencillo establecer un paralelismo directo entre los interfaces de red mostrados por el comando "`ifconfig`" y los mostrados en el panel de la izquierda de "Preferencias del Sistema - Red", en el cual solo aparecen (con la ubicación "Automático" definida por defecto) el interfaz Wi-Fi, el interfaz Bluetooth PAN (*Personal Area Network*), el interfaz Thunderbolt Ethernet y el Puente Thunderbolt.

En la nomenclatura de macOS, los interfaces de red son denominados servicios, que se gestionan desde el icono " ", pudiendo ser duplicados, renombrados y desactivados; adicionalmente, se puede establecer el orden de prioridad de los servicios en el caso de que varios interfaces de red estén activos simultáneamente (por ejemplo, el interfaz Wi-Fi y el interfaz Ethernet), mediante la opción "Establecer orden de servicios...". Por último, es posible importar la configuración de red desde un fichero:




```
$ networksetup -listallhardwareports

Hardware Port: Wi-Fi
Device: en0
Ethernet Address: ac:bc:cc:b6:95:0b

Hardware Port: Bluetooth PAN
Device: en4
Ethernet Address: ac:bc:cc:b6:95:0c

Hardware Port: Thunderbolt 1
Device: en1
Ethernet Address: 4a:00:03:ad:44:70

Hardware Port: Thunderbolt 2
Device: en2
Ethernet Address: 4a:00:03:ad:44:71

Hardware Port: Thunderbolt Bridge
Device: bridge0
Ethernet Address: 4a:00:03:ad:44:70

VLAN Configurations
===================
```

Figura 163 - Menú "Red" y salida de "networksetup -listallhardwarereports"

Por su parte, el comando "`system_profiler SPNetworkDataType`" también proporciona información muy detallada sobre el estado actual de todos los interfaces de red, así como de su configuración.

Mediante el botón "-" es posible eliminar los interfaces del menú "Red". Sin embargo, a nivel de sistema operativo, los interfaces eliminados de este menú permanecen visibles mediante el comando "`ifconfig`". Para que los cambios surtan efecto, es necesario pulsar el botón "Aplicar". Posteriormente, a través del botón "+", será posible volver a añadir los interfaces de red que se precisen.

Figura 164 - Menú "Red" (+) para añadir interfaces

A través del botón "Avanzado…" se accede a parámetros de configuración de cada uno de los interfaces, además de establecer la configuración TCP/IP (ver apartado "12.7. Comunicaciones TCP/IP"), DNS, WINS, proxies y del *hardware* (dirección física o MAC del interfaz de red, tamaño máximo de trama (MTU, *Maximum Transmission Unit*), y otros aspectos relacionados con la velocidad y el modo (*duplex*) del interfaz de red, si aplican al tipo de interfaz de red).

La gestión de las configuraciones de red se lleva a cabo a través de ubicaciones (o localizaciones), que permiten almacenar diferentes perfiles o configuraciones de red para uno o varios interfaces de red. Por defecto, macOS crea la ubicación "Automática", que incluye la configuración de interfaces ilustrada a lo largo de este apartado.

Cada ubicación de red tiene definido el conjunto de interfaces de red a emplear. Cuando se crea una nueva ubicación, los interfaces de red de la ubicación "Automática" se añadirán a ella, y será posible añadirlos/eliminarlos según corresponda. La gestión de ubicaciones también puede llevarse a cabo desde línea de comandos mediante la utilidad "`networksetup`":

```
* Creación de una nueva ubicación:

$ networksetup -createlocation Trabajo populate
Populated

* Listado de ubicaciones:

$ networksetup -listlocations
Trabajo
Automatic

* Cambio a otro perfil de ubicación:

$ networksetup -switchtolocation Automatic
found it!

* Supresión de una ubicación:

$ networksetup -deletelocation Automatic
found it!
```

Figura 165 - Utilidad "networksetup" para la gestión de ubicaciones de red

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 configurarlas exhaustivamente***, ***limitando la lista de interfaces de red*** (o servicios) ***disponibles*** y aplicando las recomendaciones de seguridad descritas a lo largo de la presente guía a cada uno de los interfaces de red integrantes de cada ubicación.

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.

Además, ***se recomienda llevar a cabo el proceso de configuración de los respectivos interfaces de red antes de proceder a su activación***, con el objetivo de evitar potenciales ataques durante dicho proceso.

12.2.1 INTERFAZ DE RED BLUETOOTH

El interfaz Bluetooth PAN no es visible a través de "`ifconfig`". Este interfaz únicamente se emplea para conectar el Mac a un dispositivo que ofrece el servicio de compartición de Internet (*hotspot*) mediante "*Bluetooth tethering*". macOS mostrará el interfaz en verde cuando se haya establecido la conexión con un dispositivo mediante la opción "Configurar dispositivo Bluetooth" y dicho dispositivo comparta su conexión BT con el Mac:

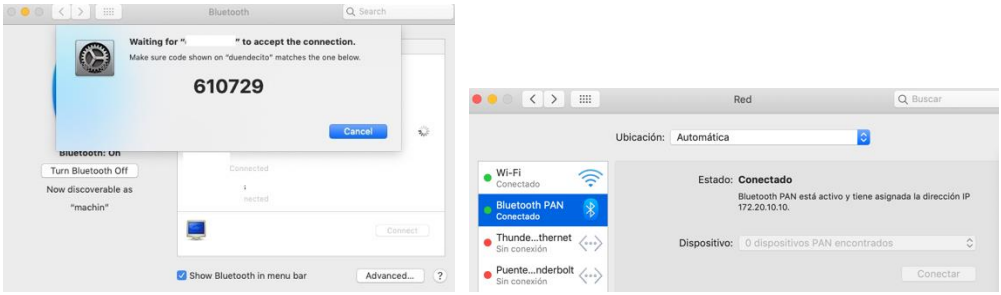


Figura 166 - Conexión a Internet mediante Bluetooth PAN

Desde el punto de vista de seguridad, ***se aconseja suprimir*** mediante el icono "-" ***el interfaz Bluetooth PAN*** si no se utiliza este tipo de conexión. A través del icono "+" siempre será posible añadirlo posteriormente, en caso necesario.

El estado del interfaz BT puede gestionarse a través del parámetro "`ControllerPowerState`" del fichero "`/Library/Preferences/com.apple.Bluetooth`" desde la línea de comandos. El cambio tendrá efecto una vez se reinicie el sistema:

```
* Consultar el estado del interfaz BT:

$ defaults read /Library/Preferences/com.apple.Bluetooth.plist ControllerPowerState
1
(el valor 1 indica que está habilitado, y 0 que está deshabilitado)

* Deshabilitar el estado del interfaz BT de forma que persista entre reinicios:

$ sudo defaults write /Library/Preferences/com.apple.Bluetooth.plist
ControllerPowerState 0
```

Figura 167 - Manejo del interfaz BT desde la línea de comandos

En ocasiones el interfaz BT de macOS presenta problemas de conectividad difíciles de analizar, que no se resuelven desactivando/activando el interfaz. Existe una opción de depuración desde la cual es posible restablecer el módulo BT, accesible pulsando las teclas "⇧+⌥" (`Cambio + Opción`) y el icono "" de la barra de menús de estado, que permite restablecer el módulo BT, eliminar todos los dispositivos BT que se descubrieron (incluyendo el registro de BT), e incluso restablecer a fábrica los dispositivos Apple conectados; desde este menú se puede ver la dirección MAC del interfaz.

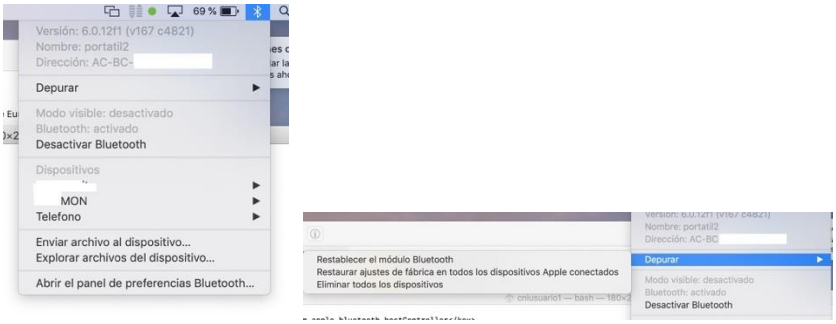


Figura 168 - Modo "debug" de Bluetooth

En macOS existen diversos servicios encargados de la funcionalidad de Bluetooth. El demonio principal se gestiona desde el fichero de configuración "`/System/Library/LaunchDaemons/com.apple.bluetoothd.plist`", pudiendo deshabilitarse según lo descrito en el apartado "7.1.3. Impedir el arranque de servicios en macOS".

Se recomienda consultar el apartado "10.1.8. Compartir Bluetooth" para información sobre la compartición de archivos a través de Bluetooth.

12.2.2 INTERFAZ DE RED "PUENTE THUNDERBOLT"

El propósito del "Puente Thunderbolt" creado por defecto en macOS es poder transferir datos directamente entre equipos Mac a través de un cable Thunderbolt, en vez de hacer uso de otros métodos de intercambio de datos, como los servicios compartidos (por ejemplo AFP, SMB, SSH, AirDrop, etc.).

Las conexiones Thunderbolt ofrecen un interfaz de comunicación de muy alta velocidad (hasta 40Gb/s)[46].

Figura 169 - Conexión física de dos ordenadores Mac a través del Puente Thunderbolt

[46] https://www.apple.com/thunderbolt/

El Puente Thunderbolt se engloba dentro de la categoría de interfaces virtuales, disponibles desde la configuración de red a través del icono "⚙", mediante la opción "Gestionar interfaces virtuales...", desde la cual es posible gestionar interfaces de red de tipo puente, VLAN (Virtual LAN) y agregaciones de enlaces:

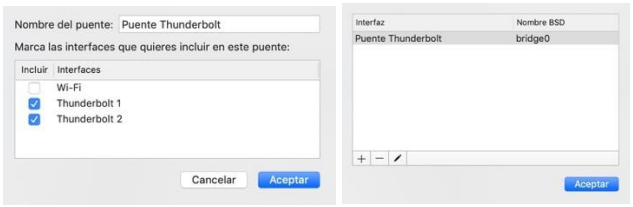


Figura 170 - Configuración del puente Thunderbolt

Mediante el comando "`system_profiler SPThunderboltDataType`" es posible determinar si existe algún dispositivo conectado a través de los puertos Thunderbolt.

Desde el punto de vista de seguridad, ***se aconseja eliminar el*** "Puente Thunderbolt" (a través del menú "-") ***si no se va a hacer uso de este tipo de conexión de red***. A través del icono "+" siempre será posible añadirlo posteriormente, en caso necesario.

12.2.3 INTERFAZ DE RED WI-FI

El interfaz "Wi-Fi" (también conocido como "Airport") integrado en los portátiles Mac 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 (identificado como "Thunderbolt Ethernet"):

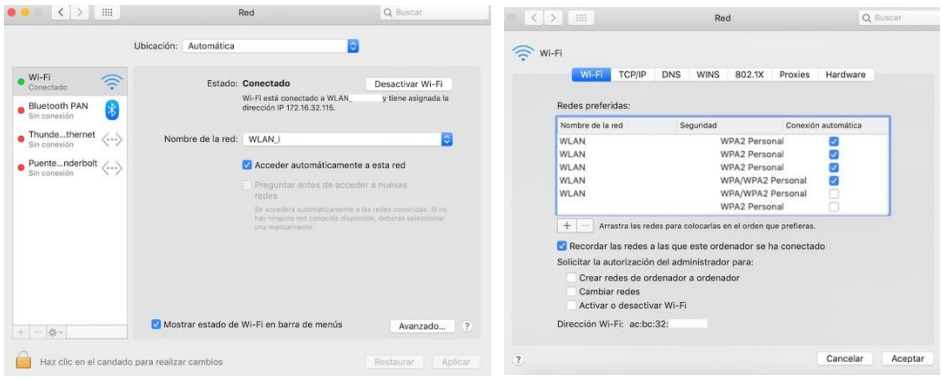


Figura 171 - Menú "Red - Wi-Fi"

Se puede obtener información detallada del interfaz Wi-Fi pulsando las teclas "⇧+⌥" (`Cambio + Opción`) y pulsando el icono "📶" de la barra de menús de estado, entre otras, el BSSID (o dirección MAC del AP Wi-Fi), el canal utilizado, la intensidad de la señal, la velocidad de la red Wi-Fi, o el tipo de red Wi-Fi 802.11<x> o "modo PHY":

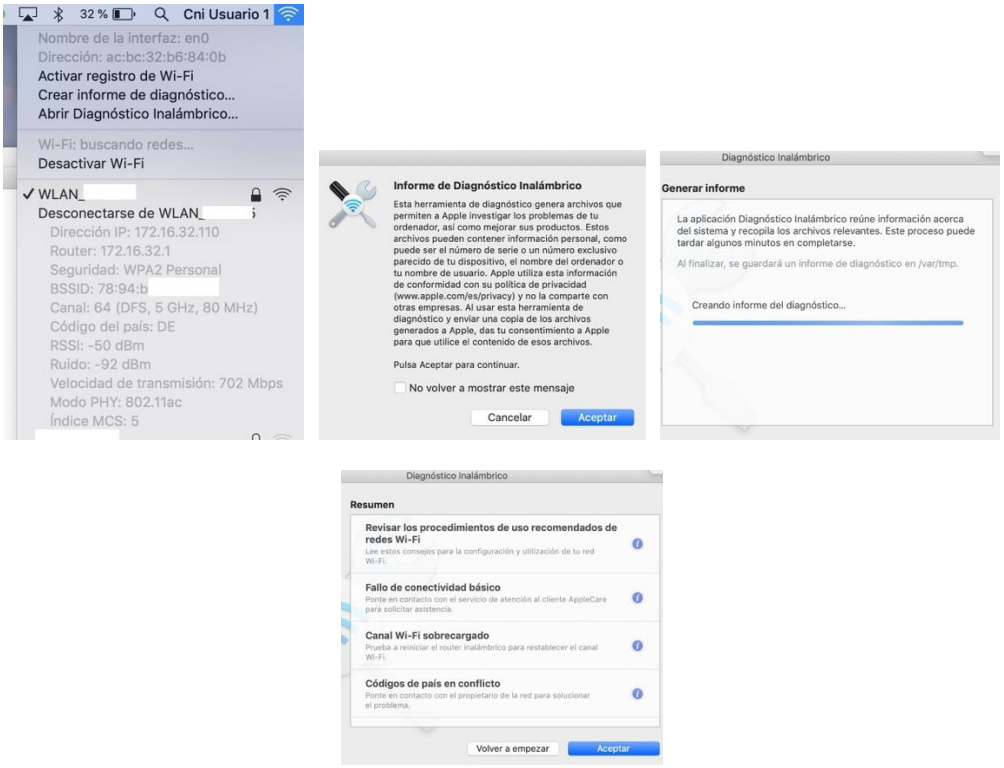


Figura 172 - Información detallada del interfaz de red Wi-Fi

Desde este menú es posible seleccionar "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).

También es posible generar desde este menú un informe de diagnóstico, si bien este informe puede enviarse a Apple, por lo que se solicita consentimiento al usuario. El fichero de diagnóstico se puede analizar desde el interfaz gráfico, pero también queda almacenado bajo "`/var/tmp/WirelessDiagnostics_<ID>_<fecha>_<hora>.tar.gz`".

Desde línea de comandos es posible desactivar/activar el interfaz Wi-Fi mediante el comando "`networksetup -setairportpower en0 off|on`".

La configuración de Wi-Fi se encuentra disponible en el fichero "`/Library/Preferences/SystemConfiguration/com.apple.airport.preferences.plist`".

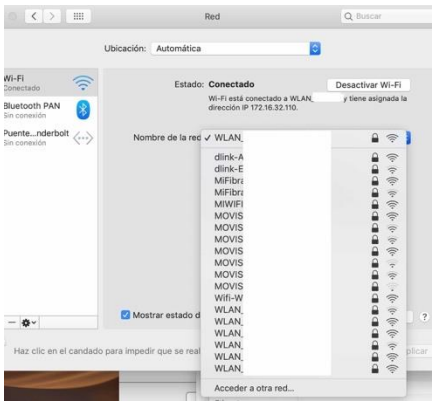


Figura 173 - Configuración del interfaz de red Wi-Fi

Por defecto, macOS 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 - <interfaz Wi-Fi> - Desactivar Wi-Fi". En la barra de menús de estado se mostrará un icono "" en función del estado (no activo, activo, o conectado a una red Wi-Fi), opción recomendada desde el punto de vista de seguridad para tener control del estado y sobre los cambios inesperados del interfaz de red Wi-Fi. La presencia de este icono se controla desde la opción "Mostrar estado de Wi-Fi en barra de menús". Adicionalmente, ***se recomienda***:

Figura 174 - Menú "Añadir un perfil de red Wi-Fi"

- ***Desactivar*** "Acceder automáticamente a esta red" para todas las redes configuradas: de esta forma, el usuario tendrá que elegir manualmente la red cuando active el interfaz Wi-Fi, dificultando los ataques de suplantación. Si, pese a esta recomendación, esta opción se habilita para varias redes conocidas, macOS las ordenará por orden de prioridad, de forma que, cuando trate de obtener conexión Wi-Fi y detecte varias redes conocidas disponibles, irá probando según el orden de esta lista.
- ***Desactivar*** "Preguntar antes de acceder a nuevas redes": de esta forma, el usuario deberá seleccionar manualmente la red a la que se desea conectar si no hay ninguna red conocida próxima. En caso contrario, cuando no se detecte ninguna red conocida, macOS preguntará al usuario a qué red abierta (sin ningún tipo de seguridad) de las disponibles desea conectarse.
- ***Restringir el uso y la configuración del interfaz*** Wi-Fi habilitando las opciones disponibles bajo la sección "Solicitar la autorización del administrador para:", en función del tipo de entorno, de forma que se precise acceso privilegiado para crear una red Wi-Fi entre ordenadores (P2P o adhoc, es decir, sin infraestructura o punto de acceso), para el cambio de una red Wi-Fi a otra, o para activar/desactivar el interfaz Wi-Fi.
- ***Añadir manualmente la red mediante el botón*** "+" ***del menú*** "Red - <Selección del interfaz Wi-Fi> - Pestaña "Wi-Fi" de la imagen derecha de la <Figura 171> ***con el interfaz Wi-Fi desconectado***, frente a añadirla a través del menú "Nombre de la red", que requiere que el interfaz esté activo. En el primer caso, ***se recomienda***:
    - ***Hacer uso únicamente de redes Wi-Fi*** "WPA2 Personal" o "WPA2 Empresa". En ningún caso se debe seleccionar "Cualquiera (personal)" ni "Cualquiera (empresa)", ya que, en ese caso, macOS considerará válida cualquier red Wi-Fi cuyo nombre de red coincida con el de una de las

redes conocidas, independientemente del tipo de seguridad, lo que facilita la realización de ataques de suplantación de la red Wi-Fi legítima.

- "Recordar las redes a las que este ordenador se ha conectado": macOS almacena las redes Wi-Fi a las que el equipo se ha conectado en el pasado en una lista de redes preferidas o conocidas, denominada PNL (*Preferred Network List*). Cuando se detecta una de estas redes en rango, el sistema se conectará a ella de forma automática (en función del ajuste de conexión automática previamente descrito), eliminando la necesidad de configurar la red cada vez que se pierda la conexión a las redes Wi-Fi. Pueden existir ocasiones en las que sea necesario restringir este comportamiento, por ejemplo, si se va a viajar y se precisa conectarse a redes públicas que no conviene tener almacenadas. ***En estos escenarios, se aconseja deshabilitar esta opción***.

macOS almacena las credenciales de las redes Wi-Fi que se añaden con la opción "Recordar las redes a las que este ordenador se ha conectado" en el llavero. Desde la app "Acceso a Llaveros", sección "Sistema", puede verse la lista de redes Wi-Fi cuyas credenciales están almacenadas. Al seleccionar una red concreta se accede a sus atributos, desde los cuales se puede ver la contraseña de la red mediante la opción "Mostrar contraseña" (previa introducción de las credenciales de administrador).

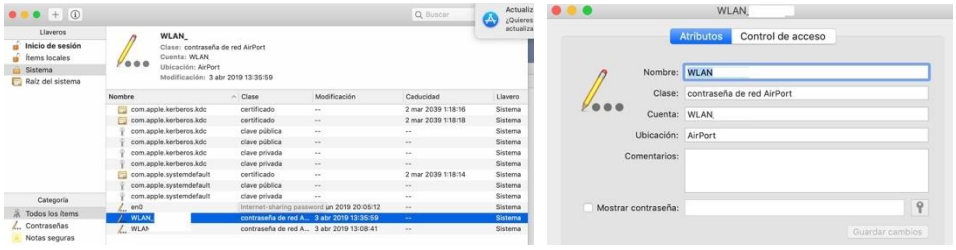


Figura 175 - Acceso a la información de credenciales de las redes Wi-Fi almacenadas en el llavero

Una alternativa para poder tener control sobre este comportamiento y establecer manualmente la red preferida por el usuario consiste en modificar las propiedades de todas las redes Wi-Fi almacenadas en el llavero del usuario, seleccionando la red Wi-Fi mediante una doble pulsación o pinchando en "Obtener información" con el botón derecho y, desde la pestaña "Control de Acceso":

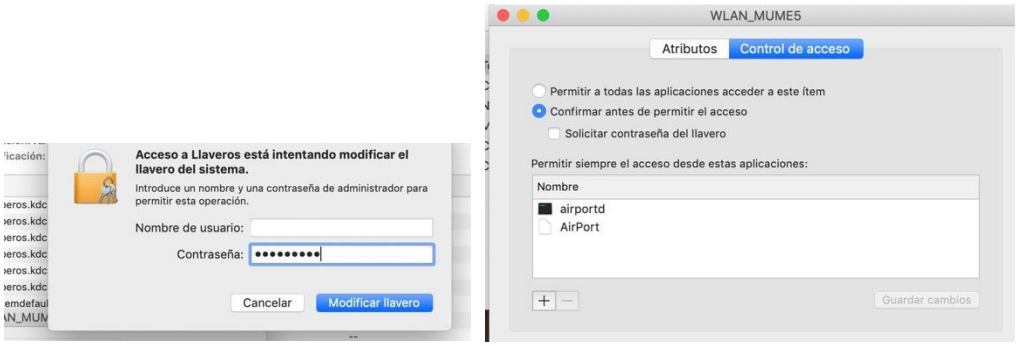


Figura 176 - Modificación de las propiedades de la red Wi-Fi en el llavero

El sistema se conectará automáticamente a las redes Wi-fi conocidas. ***Se recomienda limitar el permiso*** "Permitir siempre el acceso desde estas aplicaciones", ***admitiéndolo solo para las apps de sistema expuestas en la*** <Figura 176>.

12.2.3.1 USO DE CERTIFICADOS EN REDES WI-FI EMPRESARIALES

La configuración de una red Wi-Fi empresarial 802.1X se realiza en base a perfiles de configuración Wi-Fi (disponibles en la pestaña "Red - <entrada del interfaz de red Wi-Fi> - Avanzado - 802.1X") creados por el administrador, que deben incluir el certificado digital a utilizar, tanto de la propia red como del cliente Wi-Fi (según el tipo de red Wi-Fi).

NOTA: este tipo de perfiles se pueden crear con "macOS Server Profile Manager"[47], con la utilidad "Apple Configurator 2"[48] o con un servidor MDM de terceros.

Durante la negociación, el servidor RADIUS enviará al ordenador cliente su certificado digital. Si el certificado fue emitido por una CA (autoridad certificadora) no reconocida por el sistema como CA de confianza, se deberá indicar manualmente durante la configuración de la red Wi-Fi en el ordenador el certificado raíz correspondiente a la CA emisora del certificado digital del servidor RADIUS de la red Wi-Fi empresarial. Para ello es preciso haber importado previamente este certificado en el llavero, de forma que el mismo aparezca en la lista "Certificado de CA" del menú de configuración de la red Wi-Fi.

En el menú de configuración de la red Wi-Fi empresarial aparecerán tantas instancias del certificado como veces se haya importado con distinto nombre.

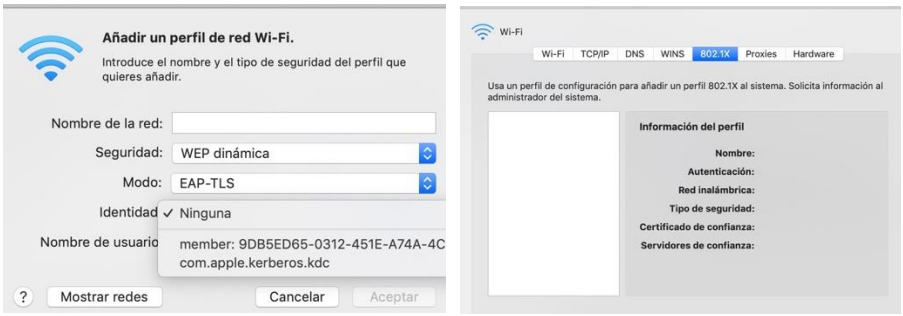


Figura 177 - Selección del certificado digital para redes Wi-Fi de uso empresarial

MÉTODOS EAP

Existen numerosos métodos EAP (*Extensible Authentication Protocol*) disponibles para la autentificación de los clientes Wi-Fi en una red Wi-Fi empresarial.

- Basados en nombre de usuario y contraseña (como PEAP, Protected EAP): el nombre de usuario y la contraseña pueden ser incluidos en el perfil o introducidos por el usuario cuando el sistema se lo solicite.

[47] https://support.apple.com/profile-manager
[48] https://support.apple.com/es-es/apple-configurator

- Basados en un certificado digital cliente de identidad (como EAP-TLS): se debe elegir el contenedor (*payload*) del certificado de identidad (`.p12` o `.pfx`): macOS soporta SCEP y Directorio Activo. El "*Common Name* (CN)" o "Alternate Name (AM)" del certificado se enviará por defecto al servidor RADIUS durante la negociación 802.1X/EAP.

CONFIANZA EN EL SERVIDOR RADIUS

- Certificados de confianza: el certificado hoja del servidor RADIUS viene incluido en el mismo perfil de configuración de 802.1X para la red Wi-Fi empresarial. En este caso, el cliente solo se conectará a la red Wi-Fi empresarial si el servidor RADIUS proporciona un certificado de esta lista.
- Nombres de certificados de servidor de confianza: el cliente se conectará a los servidores RADIUS que proporcionen un certificado cuyo "*Common Name* (CN)" o "Alternate Name (AM)" concuerde con los aquí definidos.

Para más información sobre el almacenamiento de certificados en macOS, ver el apartado "9.7.3. Certificados".

12.3 COMUNICACIONES BLUETOOTH

La principal recomendación de seguridad asociada a las comunicaciones Bluetooth (IEEE 802.15), en adelante "BT", en ordenadores Mac es ***no activar el interfaz inalámbrico Bluetooth salvo cuando se requiera***, evitando así la posibilidad de ataques sobre el *hardware* del interfaz, el *driver* o la pila de comunicaciones BT, incluyendo los perfiles BT disponibles (el proceso de instalación inicial de macOS activa el interfaz BT).

El estado del interfaz se controla mediante el botón "Preferencias del Sistema - Bluetooth - Desactivar Bluetooth" o, preferiblemente, a través del icono "" de la barra de menús de estado, que estará presente si la opción "Mostrar Bluetooth en la barra de menús" está habilitada.

La configuración de las conexiones BT se lleva a cabo desde el menú "Preferencias del Sistema - Bluetooth" [Ref.- 103].

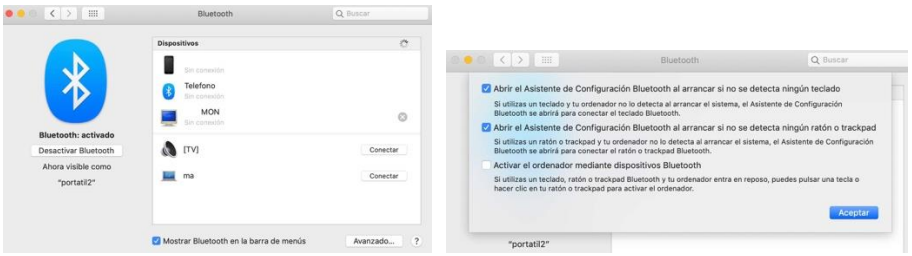


Figura 178 - Panel de preferencias de Bluetooth

Se recomienda habilitar la opción "Mostrar Bluetooth en la barra de menús" ya que:

- Permite ver el estado del interfaz BT, ya que el icono cambia en función del estado, lo cual permite al usuario tener más información sobre cuál es la situación actual:

Figura 179 - Menú Bluetooth accesible desde el icono BT de la barra de menús de estado

- "" representa un interfaz BT activo sin conexiones establecidas actualmente.
- "" representa un interfaz BT desactivado.
- "" representa un interfaz BT activo con conexiones establecidas actualmente. Al pinchar sobre este icono, se desplegará un menú desde el que se muestra las conexiones actualmente activas (en negrita) y los dispositivos con los que el equipo se ha emparejado previamente, pero con los que no existe actualmente conexión activa (sin negrita).
- "": el subsistema BT no está disponible (principalmente asociado a un fallo *hardware*). Se recomienda desconectar todos los periféricos y reiniciar el sistema.

- Permite modificar el estado del interfaz sin tener que acceder al menú "Preferencias del Sistema - Bluetooth": mientras se permanezca en este menú, el Mac será visible para otros dispositivos, lo cual permite detectar su presencia, su dirección MAC BT (BD_ADDR, *Bluetooth Device Address*) y sus propiedades.
- Pulsando sobre él mientras se presiona las teclas "⇧+⌥" (`Cambio + Opción`), presenta información detallada sobre el interfaz y sobre los dispositivos mostrados (ver <Figura 168>).
- Desde el menú "Avanzado", ***se aconseja deshabilitar*** "Activar el ordenador mediante dispositivos Bluetooth".

Si el interfaz BT está activo, desde el icono de menús de estado las opciones variarán en función del estado del interfaz. Para los dispositivos guardados, las opciones disponibles dependerán del perfil BT con el que cada dispositivo fue añadido:

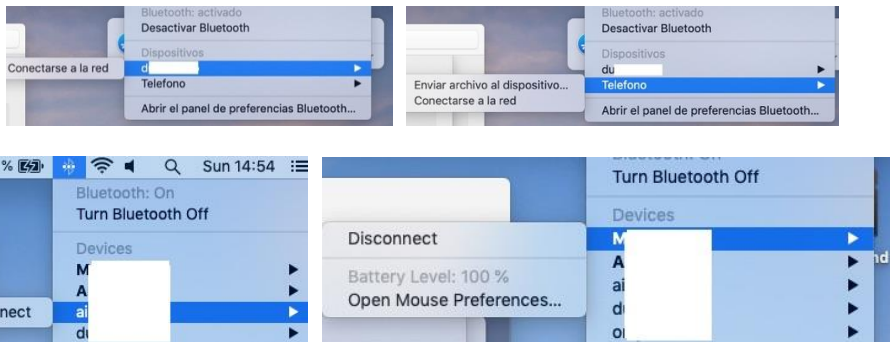


Figura 180 - Opciones de conexión desde el icono BT de la barra de menús de estado (inglés)

A través del siguiente comando es posible determinar el estado de visibilidad vía BT del dispositivo:

```
$ /usr/sbin/system_profiler SPBluetoothDataType | grep -i discoverable

2019-06-23 14:57:45.572 system_profiler[81684:13201319] SystemInfo-
AccessoryFW from dict - XXX = 0x0070
2019-06-23 14:57:45.578 system_profiler[81684:13201319] SystemInfo-
AccessoryFW from dict - YYY = 0x0067
2019-06-23 14:57:45.584 system_profiler[81684:13201319] SystemInfo-
AccessoryFW from dict - ZZZ = 0x0000
...
          Discoverable: Off
```

Figura 181 - Comando para obtener información de visibilidad del dispositivo BT

GESTIÓN DE DISPOSITIVOS BT

La gestión de dispositivos BT se realiza desde el menú principal "Preferencias del Sistema - Bluetooth". Al entrar en esta pantalla, macOS iniciará un escaneo BT para detectar nuevos dispositivos BT en rango, y presentará una ventana dividida en dos secciones:

- Dispositivos con los que se ha realizado un emparejamiento exitoso (parte superior): pinchando sobre cualquiera de ellos con el botón derecho se ofrece la opción "Eliminar" y las opciones de conexión, que dependerán del perfil BT con el que cada dispositivo fue añadido (ver <Figura 180>).
- Dispositivos visibles con los que no se ha llevado a cabo un emparejamiento (parte inferior). Al pinchar sobre cualquiera de ellos con el botón derecho, se mostrará la dirección BD_ADDR del dispositivo remoto, y se puede solicitar el emparejamiento mediante el botón "Conectar".

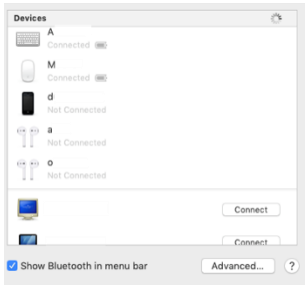


Figura 182 - Menú de gestión de dispositivos BT (inglés)

El comando "`/usr/sbin/system_profiler SPBluetoothDataType`" ofrece información muy detallada sobre todos los dispositivos BT conocidos por el sistema, incluidos los perfiles BT[49] detectados para cada uno de ellos (sección "`Services`").

```
$ system_profiler SPBluetoothDataType
...
<dispositivo>:
    Services: Wireless iAP v2, PAN Network Access Profile, Wireless iAP,
Handsfree
    Gateway, Audio Source, AVRCP Device, MAP MAS-iOS, AVRCP Device,
Phonebook
...
```

Figura 183 - Información sobre dispositivos BT - comando "system_profiler SPBluetoothDataType"

[49] https://es.wikipedia.org/wiki/Perfil_Bluetooth

NOTA: los perfiles BT soportados por macOS deberían estar accesibles en el enlace "macOS: Supported Bluetooth Profiles" de la página "https://support.apple.com/kb/PH10549" referenciada desde "https://developer.apple.com/bluetooth/". Sin embargo, a fecha de elaboración de la presente guía, ese enlace no está disponible.

macOS Mojave no permite limitar los perfiles BT propios o de los dispositivos descubiertos. Para desarrolladores, Apple dispone de la herramienta "Bluetooth Explorer", que sí lo permite.

El icono situado a la izquierda de los dispositivos BT descubiertos permite conocer su tipo (en base a su clase BT), y la selección de su nombre desde la lista iniciará el proceso de emparejamiento, que, dependiendo de la especificación BT soportada por aquel, puede requerir o no la introducción o aceptación de un código o PIN de emparejamiento, el cual se muestra en claro en la pantalla de macOS:

Figura 184 - Código o PIN de emparejamiento con dispositivos BT

Cuando se reactiva el interfaz Bluetooth después de haber sido inhabilitado, el sistema intentará establecer la conexión con todos los dispositivos de su lista de emparejamiento que estuviesen conectados en el momento de la desconexión y que estén disponibles en rango, sin requerir que el usuario introduzca de nuevo ningún código, ya que el emparejamiento se había realizado previamente y conservado (igual comportamiento se observa al reiniciar el ordenador).

Desde el punto de vista de seguridad, ***se recomienda eliminar de la lista de dispositivos BT emparejados aquellos con los que la conexión se realice de forma esporádica y con los que no vaya a volver a conectarse***.

COMPONENTES DE LA FUNCIONALIDAD BLUETOOTH

La implementación del protocolo BT en macOS se divide en diversos servicios:

- Un conjunto de demonios de sistema, cuyos ficheros de configuración residen bajo "`/System/Library/LaunchDaemons/`":
  - `com.apple.IOBluetoothUSBDFU.plist`
  - `com.apple.bluetoothReporter.plist`
  - `com.apple.bluetoothaudiod.plist`
  - `com.apple.diagnosticextensions.osx.bluetooth.helper`
  - `com.apple.bluetoothd.plist`: corresponde al núcleo principal de la funcionalidad BT, gestionada por el proceso `"/usr/sbin/bluetoothd"` .
- Dos agentes de sistema, cuyos ficheros de configuración residen bajo "`/System/Library/LaunchAgents`":
  - `com.apple.bluetoothUIServer.plist`
  - `com.apple.bluetooth.PacketLogger.plist`

- Una serie de extensiones de *kernel* (*drivers*), residentes bajo "`/System/Library/Extensions/`":
  - `AppleBluetoothDebug.kext`
  - `AppleBluetoothDebugService.kext`
  - `AppleBluetoothModule.kext`
  - `AppleBluetoothMultitouch.kext`
  - `AppleBluetoothRemote.kext`
  - `AppleMIDIBluetoothDriver.plugin`
  - `IOBluetoothFamily.kext`
  - `IOBluetoothHIDDriver.kext`
  - `com.apple.bluetoothReporter.plist`

12.3.1 RESUMEN DE LAS CONSIDERACIONES DE SEGURIDAD DE BLUETOOTH

La pila de comunicaciones Bluetooth (BT) ha sido históricamente fuente de diversas vulnerabilidades que han comprometido la seguridad de macOS. A continuación se facilita un listado con las recomendaciones de seguridad de BT:

- ***Desactivar el interfaz BT tras el proceso de configuración inicial del equipo***.
- ***Desactivar el interfaz BT una vez haya finalizado la conexión con los dispositivos emparejados y hasta que vuelva a ser necesaria su utilización***.
- ***Cambiar el nombre BT del ordenador*** para evitar revelar información sobre su tipo y modelo a través del menú "Preferencias del sistema - Compartir - Nombre del ordenador".
- ***Suprimir de la lista de dispositivos emparejados todo dispositivo Bluetooth con el que ya no se requiera conectar*** desde el menú "Preferencias del sistema - Bluetooth - <dispositivo> "x"".
- ***Comprobar las direcciones BD_ADDR de los dispositivos BT*** con los que se vaya a establecer un emparejamiento a través de la lista de dispositivos BT.
- ***Activar/desactivar el interfaz Bluetooth*** a través del icono BT de la barra de menús de estado o del comando descrito en la <Figura 167>, ***y mantenerlo en modo oculto*** siempre que sea posible.
- ***Minimizar la visibilidad del dispositivo únicamente al tiempo necesario durante la realización de emparejamientos***, no permaneciendo más tiempo del necesario en el menú "Preferencias del sistema - Bluetooth".
- ***Se aconseja evitar el uso de dispositivos BT (como Apple Watch) para el desbloqueo automático del equipo***[50], minimizando el riesgo de acceso si ambos dispositivos son sustraídos simultáneamente.
- ***Deshabilitar la compartición de la conexión de tipo tethering*** **mediante Bluetooth** tan pronto deje de utilizarse la misma (a través del menú "Preferencias del sistema - Compartir - Compartir Bluetooth").

[50] La configuración detallada del desbloqueo automático de macOS mediante Apple Watch queda fuera del ámbito de la presente guía (ver apartado "11.4. Servicios de "Continuidad"").

12.4 COMUNICACIONES PROPIETARIAS DE APPLE

12.4.1 BONJOUR

Bonjour (también conocido como "Rendezvous"), brevemente introducido en el apartado "12.1.1. Nombre del equipo", es una implementación desarrollada por Apple para las denominadas tecnologías "Zeroconf" (*zero-configuration networking [Ref.-32]*), basadas en establecer una red de ordenadores mediante el uso de direccionamiento a nivel local y del uso de paquetes DNS y mDNS (*multicast* DNS) para el nombrado e identificación de servicios. Su objetivo es el descubrimiento de servicios basados en TCP/IP dentro de una misma subred, sin que sea necesario ningún tipo de configuración previa [Ref.- 104].

Los servicios descubiertos mediante el uso de este protocolo se muestran bajo la sección "Compartido" (*Shared*) de la ventana de Finder.

A nivel de sistema, los ficheros de configuración asociados a Bonjour son:

- "`/System/Library/LaunchDaemons/com.apple.mDNSResponder.plist`": corresponde al proceso principal de mDNS, "`/usr/sbin/mDNSResponder`".
- "`/System/Library/LaunchDaemons/com.apple.mDNSResponderHelper.plist`".

Si no se desea hacer uso de los servicios compartidos de tipo "Bonjour", ***se recomienda desactivar ambos demonios*** mediante el procedimiento descrito en el apartado "7.1.3. Impedir el arranque de servicios en macOS".

12.4.2 AIRDROP

El servicio AirDrop es un servicio propietario de Apple basado en la tecnología "Bonjour" cuyo objetivo es la transferencia de ficheros de manera inalámbrica, punto a punto (P2P), utilizando cifrado TLS entre equipos compatibles mediante Wi-Fi y Bluetooth, sin hacer uso de una infraestructura de red o de un punto de acceso Wi-Fi (similar al estándar "Wi-Fi Direct").

Cuando se habilita AirDrop, el dispositivo crea y almacena una identidad RSA de 2.048 bits, y un *hash* asociado a esta identidad.

Cuando un usuario elige compartir un elemento a través de AirDrop, su equipo emite una señal BLE (*Bluetooth Low Energy*). Los equipos que se encuentren en rango y tengan AirDrop activo detectarán esta señal y responderán enviando una versión reducida de su propio "*identity hash*". Una vez el emisor selecciona el destino de la lista de dispositivos que han respondido, se inicia una conexión TLS (para más detalles sobre la seguridad de AirDrop, se recomienda la lectura de la [Ref.- 106]).

El menú de AirDrop está disponible en la barra lateral izquierda de Finder, requiriéndose que los interfaces Wi-Fi y BT estén activos en ambos dispositivos.

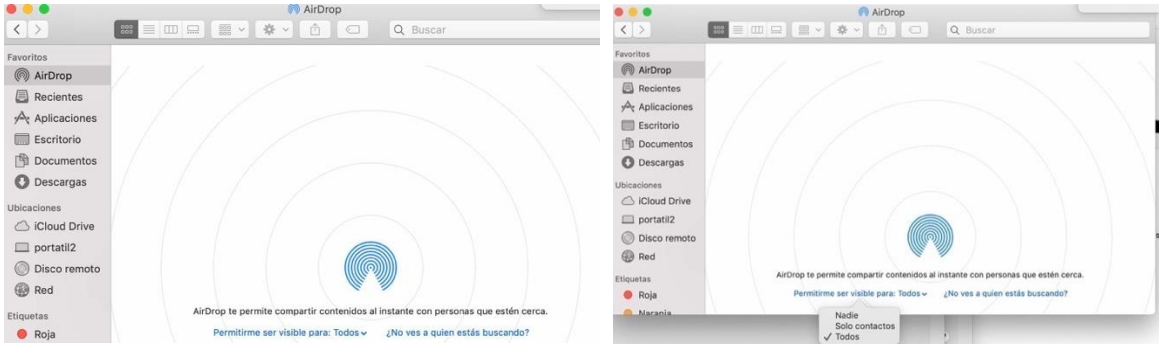


Figura 185 - Barra lateral de Finder y menú "AirDrop"

La recomendación de seguridad es ***mantener la opción*** "Permitirme ser visible para:" en "Nadie", de modo que no sea posible establecer conexión con el Mac y enviarle archivos. Únicamente deberá establecerse el valor a otra opción cuando se precise realizar la transmisión de ficheros, tras la cual se aconseja retornar al valor "Nadie". La opción "Solo contactos" requiere la existencia de una sesión de iCloud activa en el dispositivo.

Cuando el equipo es visible para otro dispositivo y éste intenta enviarle un archivo, el sistema mostrará una ventana de confirmación (salvo entre equipos que comparten un mismo Apple ID). Los archivos recibidos se almacenan en la carpeta "`Descargas`" ("`Downloads`") del usuario receptor:

Figura 186 - Solicitudes de aceptación de recepción de datos vía "AirDrop"

El envío de un archivo en el equipo origen se inicia desde el menú "Compartir" que se muestra al pinchar con el botón derecho de un elemento:

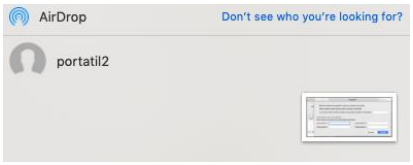


Figura 187 - Selección del destino de la transferencia de datos vía "AirDrop"

El establecimiento de conexiones AirDrop no impide que el equipo permanezca conectado de forma normal a una red Wi-Fi simultáneamente.

El proceso encargado de la transmisión vía AirDrop es "`/System/Library/PrivateFrameworks/FinderKit.framework/Versions/A/PlugIns/AirDrop.appex/Contents/MacOS/AirDrop`", que se lanza al solicitarse la transferencia y finaliza cuando esta concluye, haya tenido éxito o no.

Los atributos de cuarentena de los archivos asociados al fichero trasmitido en el ordenador origen son propagados a través de la transferencia 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>").

Desde el punto de vista de seguridad, puede considerarse que AirDrop es un mecanismo de transferencia preferible a otros (especialmente no cifrados). Sin embargo, ***se recomienda deshabilitar el servicio tan pronto finalice su necesidad de uso***.

12.4.3 IMESSAGE

iMessage es el servicio propietario de Apple para el envío de mensajes instantáneos (a través de redes Wi-Fi o de redes de datos de telefonía móvil), junto al envío de otros datos como imágenes, vídeos, contactos, localizaciones, etc.

Para disponer del servicio iMessage, es necesario asociar una cuenta de iCloud al Mac. Las capacidades de sincronización de iCloud hacen que los mensajes intercambiados a través de iMessage aparezcan de manera sincronizada en todos los dispositivos asociados al mismo ID de Apple o cuenta en iCloud.

La configuración de iMessage se realiza desde el menú de la app Mensajes "Preferencias - iMessage", que también se emplea para el envío y recepción de mensajes de texto SMS o MMS si el usuario dispone de un iPhone que se ha configurado con el mismo ID de Apple (ver apartado "12.5.1. iMessage" de la "Guía CCN-STIC-455D - Guía Práctica de Seguridad en Dispositivos Móviles iPhone (iOS 12.x)" [Ref.- 403]).

El sistema almacena en el llavero de inicio de sesión del usuario (dentro de la categoría "Claves") las claves de cifrado y de firma que se emplean en las comunicaciones de iMessage:

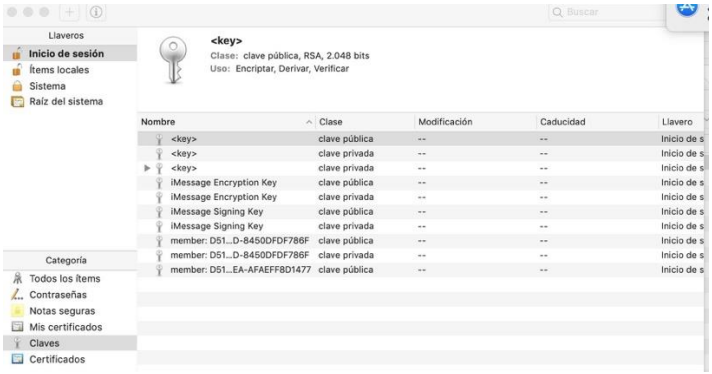


Figura 188 - Claves de cifrado y firma de iMessage en el llavero

Desde el punto de vista de seguridad y/o privacidad, se recomienda la configuración:

- "Notificar lectura": ***desactivado***. De este modo no se enviará acuse de recibo de la lectura de los mensajes al emisor. Se permite establecer este ajuste de forma granular para determinadas conversaciones.

- "Iniciar nuevas conversaciones desde": determina las direcciones empleadas para enviar y recibir mensajes por parte del usuario en el ordenador. La activación del servicio iMessage se asocia tanto a la dirección de e-mail vinculada al ID de Apple como al número de teléfono móvil del dispositivo móvil iOS vinculado a ese mismo Apple ID (en caso de que el usuario disponga de uno). Se recomienda eliminar aquellas direcciones que no se desea publicar para este servicio, así como el número de teléfono móvil si dicho dispositivo no es de uso empresarial.

El servicio de Mensajes está incluido en los denominados servicios de "Continuidad" (ver apartado "11.4. Servicios de "Continuidad"").

Asimismo, desde Mensajes es posible iniciar una compartición de pantalla (ver apartado "10.1.1. Compartir pantalla").

12.5 VPN

macOS proporciona soporte por defecto para el establecimiento de redes privadas virtuales y tecnologías VPN (*Virtual Private Network*) [Ref.- 28]:

- Cisco IP Security (IPSec, *Internet Protocol Security*):
  - Métodos de autentificación:
    - De usuario: contraseñas y *token* de segundo factor.
    - De servidor: certificados digitales y secreto compartido.
- IKEv2: incluye soporte tanto para IPv4 como IPv6 con:
  - Métodos de autentificación: secreto compartido, certificados, EAP-TLS y EAP-MSCHAPv2.
  - Algoritmos criptográficos: ECDSA, cifrado ESP con GCM y grupos ECP para Diffie-Hellman.
  - Características adicionales: *Split tunnel*, fragmentación IKE y redirección del servidor.
- L2TP (*Layer Two Tunneling Protocol*) sobre IPSec (L2TP: 1701/udp; LT2P/IPSec: 500/udp):
  - Métodos de autentificación:
    - De usuario: contraseña MSCHAPv2, *token* de segundo factor y certificados digitales.
    - De servidor: certificados digitales y secreto compartido (incluido Kerberos).
- VPN SSL con autentificación a través de aplicaciones cliente propietarias, tanto configuradas de forma manual como mediante perfiles de configuración gestionados por un MDM. También se soporta *split tunneling*.
  - Métodos de autentificación: contraseñas, *token* de segundo factor y certificados digitales.

En el caso de VPNs con autentificación cliente basada en certificados digitales, macOS soporta "*VPN On Demand*", método por el cual el establecimiento de la VPN se basa en la configuración de ciertos dominios o direcciones IP predefinidos. Las opciones de configuración disponibles en "*On Demand*" permiten:

- Establecer una VPN para cualquier dirección de un dominio.
- Nunca establecer la VPN para ciertos dominios (aunque, en el caso de estar previamente establecida, se hará uso de ella).
- Actuar bajo demanda, estableciéndose la VPN para ciertas direcciones de un dominio si la resolución de nombres falla.
- Configurar el acceso VPN por aplicación, de forma que cada app, tanto de las existentes por defecto en macOS (como Mail o Safari) como de terceros, pueda utilizar una VPN concreta. De este modo es posible independizar el tráfico de apps corporativas del tráfico de apps de usuario personales. Para ello se emplea un vector que mapea el identificador de la app con el UUID de la VPN.

En la página oficial de soporte de Apple [Ref.- 107] se proporcionan los detalles para configurar conexiones VPN en macOS, que se lleva a cabo desde "Preferencias del sistema - Red - +". Si se dispone de un perfil de configuración, éste puede importarse desde el icono "⚙" del menú "Red" seleccionando "Importar configuraciones…".

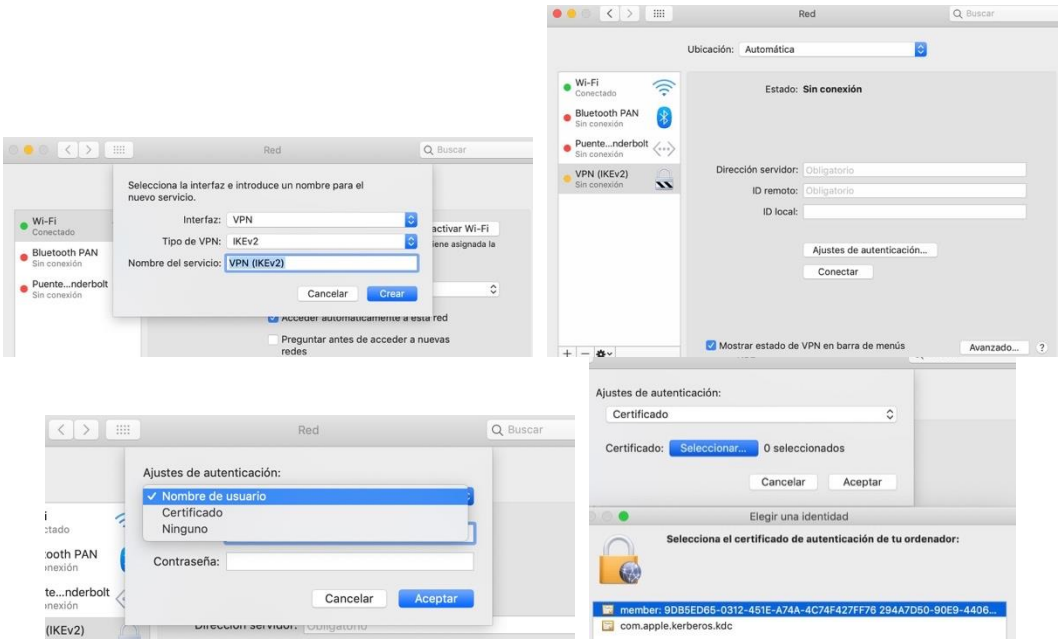


Figura 189 - Configuración de una conexión VPN

Se recomienda seleccionar "Mostrar estado de VPN en barra de menús" para tener control sobre el estado de la conexión VPN.

Los ajustes de autenticación basados en certificado digital requieren que dicho certificado se encuentre disponible en el llavero del usuario (ver apartado "9.7. Gestión de llaveros"); los basados en "nombre de usuario" requieren que el usuario los introduzca, y macOS los guardará en el llavero de sistema, permitiendo acceso por

defecto a diversos procesos involucrados en la gestión de la conexión. En el caso de redes IPSec basadas en un secreto, el secreto también se almacenará en el llavero:

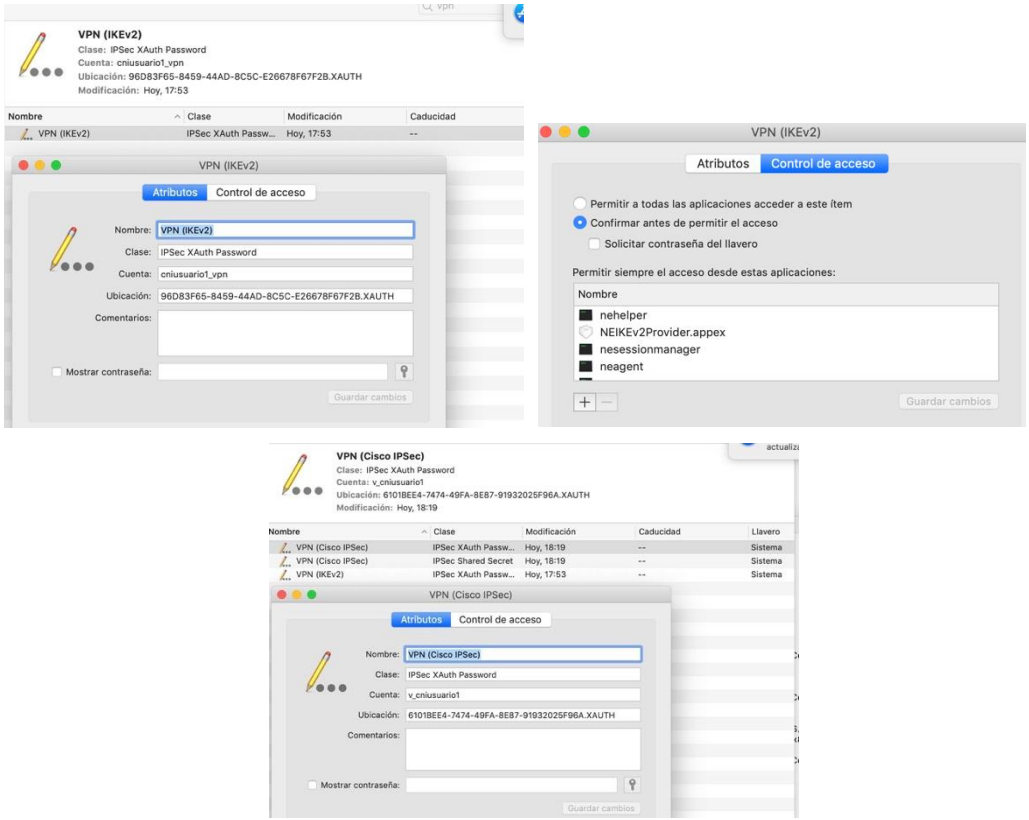


Figura 190 - Almacenamiento de las credenciales de VPN en el llavero

El uso de redes VPN se recomienda desde el punto de vista de seguridad para proteger el tráfico del equipo, especialmente si la conexión de red se realiza a través de redes inseguras, como *hotspots* Wi-Fi.

12.6 USB

Además de para conectar dispositivos periféricos de diversa índole, macOS permite arrancar el equipo desde una unidad de memoria USB externa de arranque en la que se haya volcado una copia del disco de instalación de macOS (ver apartado "16.3. Creación de un instalador de arranque en una unidad USB o un disco externo").

Desde el punto de vista de seguridad, la conexión de dispositivos USB al equipo presenta riesgos, por lo que es común en entornos corporativos que estos puertos sean deshabilitados por las políticas de gestión empresarial.

A nivel no empresarial, no existe una opción en macOS Mojave que permita deshabilitar los puertos USB.

12.7 COMUNICACIONES TCP/IP

macOS configura por defecto los interfaces de red a nivel IP como clientes DHCP, lo que implica que obtienen su dirección IP y el resto de parámetros de red asociados

(*router*, longitud del prefijo de red - o máscara de subred - y servidores DNS) dinámicamente mediante el protocolo DHCP. Sin embargo, todos estos ajustes se pueden configurar de forma estática y manual mediante el menú "Red - <interfaz> - Avanzado", tanto para IPv4 como para IPv6.

Mediante la opción "Renovar concesión de DHCP" el sistema volverá a solicitar al servidor DHCP que le asigne una IP, lo cual puede ser necesario si se están experimentando problemas de conectividad sin que se haya realizado ninguna operación de reconfiguración de ajustes de red por parte del usuario.

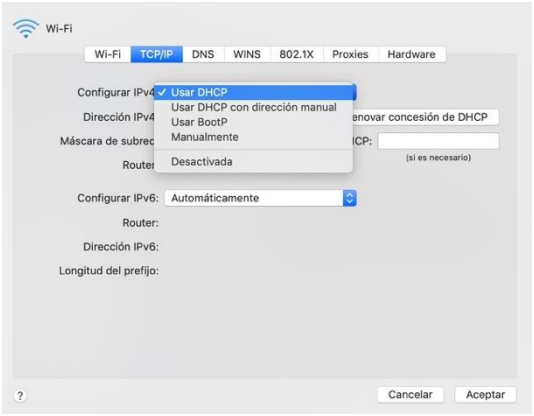


Figura 191 - Menú "Red - TCP/IP"

El *kernel* de macOS tiene capacidad de reenvío de tráfico entre los diferentes interfaces de red del equipo (técnica conocida como "IP *forwarding*"). Desde el punto de vista de seguridad, se desaconseja habilitar IP *forwarding* en el equipo, salvo que su propósito sea que haga de *router* entre dos subredes. Se puede comprobar si este comportamiento está activo mediante el siguiente comando (el valor "0" indica que el sistema no actúa como IP *forwarder* o *router*):

```
$ sysctl net.inet.ip.forwarding
net.inet.ip.forwarding: 0
```

Figura 192 - Comando para determinar la condición de "IP forwarding"

Se recomienda deshabilitar IPv6 para aquellas redes que no hagan uso de este protocolo de direccionamiento. Aunque la desactivación no es posible desde el interfaz gráfico, el comando "`networksetup -setv6off <servicio_de_red>`" cumple esa función. La nomenclatura necesaria para el parámetro "`<servicio_de_red>`" se obtiene a través del comando "`networksetup`" descrito en la <Figura 162>. La <Figura 193> muestra el estado de IPv6 en el interfaz gráfico de macOS para un servicio de red antes y después de la desactivación de IPv6 por línea de comandos:

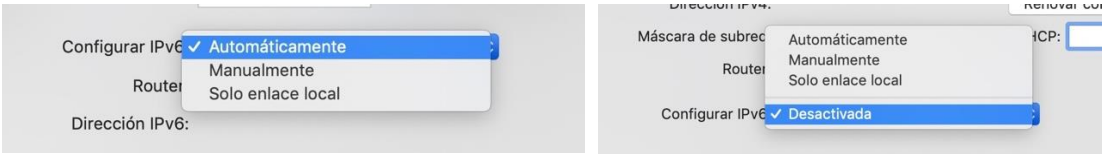


Figura 193 - Estado de IPv6 para un servicio de red determinado

Se recomienda la lectura del apartado "8.2.2. Firewall (Cortafuegos)" para obtener información sobre el filtrado de comunicaciones en macOS.

12.7.1 PROXIES

En el caso de ser necesario hacer uso de un *proxy* para el establecimiento de conexiones hacia Internet o hacia otros servicios o redes remotas, macOS dispone de soporte. El proceso de configuración de un *proxy* se detalla en la [Ref.- 109]. Desde el punto de vista de seguridad, ***se recomienda***:

- ***Evitar la opción*** de "Detección de proxy automática", ya que los protocolos involucrados en ella pueden ser manipulados por un potencial atacante para redirigir el tráfico del ordenador Mac hacia el equipo del atacante.
- Para la opción "Config. de proxy automática", ***asegurarse de que al menos la 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*).

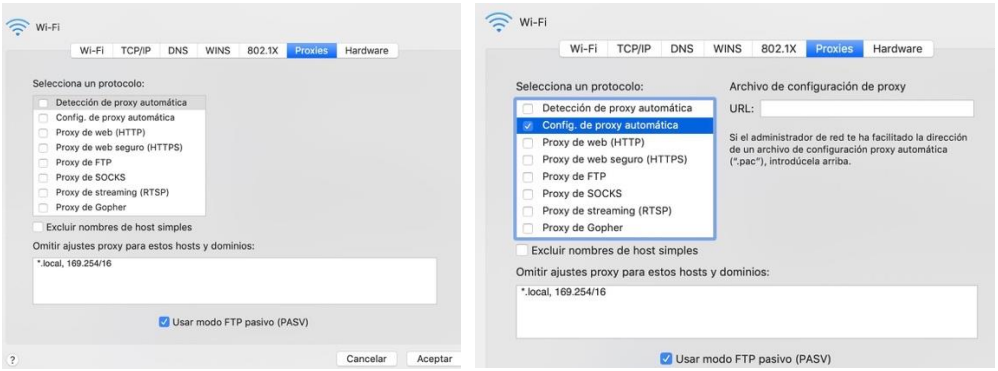


Figura 194 - Opciones de configuración de proxy

macOS Mojave incluye soporte para TLS 1.3, aunque está deshabilitado por defecto[51] [Ref.- 110]. Apple anunció que eliminará el soporte para TLS 1.0 y 1.1 definitivamente en marzo de 2020 [Ref.- 120].

12.7.2 DNS PRIVADO

En la actualidad existen diversas opciones para añadir privacidad y seguridad al servicio DNS, entre ellas:

- DNS sobre TLS (DoT, DNS *over* TLS), un estándar del IETF definido en el RFC 7858[52] que utiliza el protocolo TLS para establecer un canal seguro entre un equipo cliente y el servidor DNS de tipo *resolver* que tiene configurado. Una vez establecido este canal, las consultas DNS no pueden ser observadas, ni modificadas, por un tercero que monitorice la red, evitándose ataques de tipo

[51] https://developer.apple.com/videos/play/wwdc2017/701/?time=2261
[52] https://tools.ietf.org/html/rfc7858

MitM entre el dispositivo cliente y su *resolver*, y mejorando la confidencialidad y privacidad de DNS.

- DNS sobre HTTPS (DoH, DNS *over* HTTPS), un estándar del IETF definido en el RFC 8484[53] para establecer un canal DNS seguro entre el cliente y su *resolver* mediante HTTPS.

macOS no dispone de una opción específica para configurar DoT o DoH. Sin embargo, existen utilidades que actúan como *stub resolver* (cliente final) con capacidad para conectarse a un *open resolver* mediante TLS[54], y también para hacerlo vía HTTPS[55].

Algunos de los *resolvers* públicos que proporcionan servicios DoT son el 1.1.1.1 (Cloudflare, que también proporciona DoH), 8.8.8.8 (Google) y 9.9.9.9 (Quad 9). Todos ellos realizan además validación de las respuestas DNS mediante DNSSEC para los dominios firmados en Internet.

13.GESTIÓN DE APPS

El término apps engloba al conjunto de aplicaciones de sistema o de terceros que son compatibles con macOS y que pueden ser instaladas sobre el ordenador Mac.

El mercado oficial de apps está accesible desde la app "App Store" (icono "  "), desde el cual se gestiona tanto la instalación de nuevas apps como la actualización de apps ya instaladas, salvo para ciertos componentes del sistema, que se actualizan con el sistema operativo. Las apps descargadas de la App Store están firmadas por Apple con el objetivo de garantizar su integridad; su descarga utiliza conexiones cifradas y mecanismos de *certificate pinning* para evitar ataques de tipo MitM.

Además de los controles de seguridad propios del "*TrustedBSD Mandatory Access Control* (MAC) *Framework*"[56], macOS implementa los mecanismos descritos en la sección "9. Mecanismos de protección y tecnologías de seguridad en macOS" para dotar a las apps de seguridad[57], entre los que destacan:

- *Gatekeeper*: descrito en la sección "9.2. Gatekeeper y cuarentena de archivos".
- *Sandboxing*: descrito en la sección "9.4. Sandbox".
- *XProtect*: descrito en la sección "9.3. Xprotect: software malicioso (malware)".
- Acceso al llavero para el almacenamiento de elementos seguros de la app (identidades digitales y credenciales) protegido mediante listas de control de acceso (ACLs) que evitan que una app pueda acceder a los datos de llavero de otra; descrito en el apartado "9.7. Gestión de llaveros".

---

[53] https://tools.ietf.org/html/rfc8484

[54] https://blog.because-security.com/t/use-cloudflare-dns-with-tls-on-mac-os-x-gui-and-cli-way/315
https://phiffer.org/writing/dns-over-tls-on-macos/

[55] https://gist.github.com/soderlind/6a440cd3c8e017444097cf2c89cc301d

[56] http://www.trustedbsd.org/mac.html

[57] Los recursos de seguridad para los desarrolladores se pueden consultar en https://developer.apple.com/documentation/security.

- *Common Crypto*: macOS proporciona APIs de cifrado para que los datos de la app se cifren de forma simétrica[58].
- *Transparency, Consent and Control* (TCC): controla los permisos que se han concedido a la app (apartado "8.2.4. TCC: Transparency, Consent and Control").

Es posible acceder a todas las apps disponibles, e instaladas por el usuario, en el sistema desde '' - Acerca de este Mac - [Visión general] - Informe del sistema - Software - Aplicaciones, e Instalaciones":

Figura 195 - Listado de todas las apps disponibles en el sistema

Figura 196 - Listado de las apps instaladas con intervención del usuario

Para desinstalar extensiones añadidas al navegador web Safari a través de la instalación de una app, es preciso desinstalar dicha app.

13.1 INSTALACIÓN DE APPS EN MACOS

El usuario puede instalar apps en el Mac a través de diversas fuentes:

- El mercado oficial de Apple (ver apartado "13.2. App Store"), en el que se dispone de apps proporcionadas por Apple y por desarrolladores reconocidos por Apple.
- Mercados de apps alternativos de terceros.
- Descargando un paquete de instalación desde Internet: ver apartado "13.3. Paquetes de instalación". ***Se recomienda descargar estos paquetes del sitio web oficial del desarrollador***.

[58] https://developer.apple.com/library/archive/documentation/Security/Conceptual/cryptoservices/Introduction/Introduction.html

- A través de un recurso disponible en la red local o de un dispositivo de almacenamiento USB: en estos casos las políticas de cuarentena del *Gatekeeper* no tendrán efecto, salvo que el fichero de la app hubiese sido previamente descargado de Internet y aún conservase los atributos de cuarentena (ver apartado "9.2. Gatekeeper y cuarentena de archivos").
  En el caso de instaladores descargados en un equipo Windows© y copiados a una unidad USB con formato FAT32, no existirán atributos de cuarentena, por lo que no se aplicarán las protecciones del sistema *Gatekeeper*.
- Mediante un gestor de paquetes, como "Homebrew"[59], desde el que se pueden instalar herramientas *open-source* no disponibles en el mercado oficial.

Al margen de los controles de seguridad impuestos por macOS, la principal recomendación de seguridad es ***instalar únicamente apps de fuentes de confianza***.

13.2 APP STORE

La app "App Store" incluía, en versiones anteriores de macOS, la posibilidad de actualizar el software del sistema operativo. En Mojave, únicamente gestiona la actualización de apps, quedando la actualización del sistema operativo disponible a través de los ajustes descritos en el apartado "5.1. Actualización de macOS".

El acceso a la "App Store" está disponible a través del "Launcher" y mediante ' - App Store...".

El acceso a la funcionalidad ofrecida por la App Store precisa de la existencia de un Apple ID válido y activo en la app, que puede ingresarse a través de la opción "Iniciar sesión" de la pantalla principal de esta app (o del menú "Store"). Si ya existe un Apple ID activo, se mostrará en la parte inferior izquierda de la pantalla principal de la app. Si no se definió un Apple ID durante el proceso de configuración inicial, se dispone de la opción "Crear ID de Apple". ***Se recomienda independizar el Apple ID utilizado para la App Store del utilizado para los servicios de iCloud***, de forma que no sea fácil inferir uno a partir del otro, y que se independicen los servicios de iCloud del acceso y las compras de apps y contenidos en la App Store.

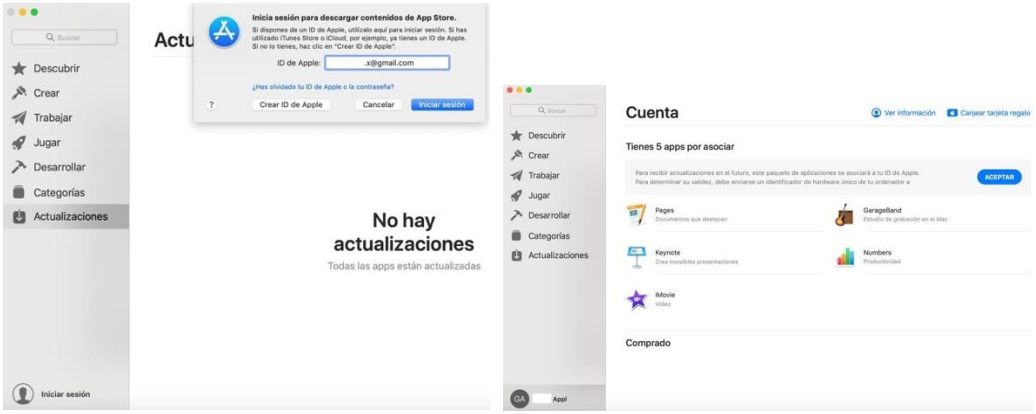


Figura 197 - Menú principal de la App Store

[59] https://brew.sh

La primera vez que se inicia sesión en la App Store, el usuario deberá aceptar la asociación de las apps mostradas en la imagen derecha de la <Figura 197>, distribuidas por defecto a todos los usuarios por Apple.

Se recomienda establecer las siguientes opciones de la sección [Preferencias***] del menú de la app App Store***:

Figura 198 - Preferencias de App Store

- **Actualización automática**: ***se recomienda desmarcar este valor***, y comprobar manualmente la disponibilidad de actualizaciones de apps, para disponer de un control más granular sobre las funcionalidades que éstas ofrecen y/o suprimen.
  Cuando este parámetro está desactivado, la disponibilidad de una nueva versión de una app se notifica a través de un número que acompaña al icono de la "App Store", y que representa el número de apps para las cuales se encuentra disponible una actualización. Esta información también se puede obtener desde el menú "" - App Store...":

Figura 199 - Icono de notificación de actualizaciones disponibles en la App Store

- **Descargar automáticamente las apps compradas en otros ordenadores**: a criterio del usuario del equipo.
- **Descargas gratuitas**: ***se recomienda seleccionar*** "Solicitar contraseña"; de este modo se solicitará al usuario las credenciales de su Apple ID antes de proceder a instalar apps gratuitas.
- **Compras y compras dentro de la app**: ***se recomienda elegir*** "Solicitar siempre"; de este modo se solicitará al usuario las credenciales de su Apple ID antes de proceder a obtener contenidos de pago o apps no gratuitas (compras).

13.2.1 ACTUALIZACIÓN DE APPS DE LA APP STORE

La primera recomendación de seguridad en relación con el uso de apps es mantenerlas siempre actualizadas, no sin antes verificar que las nuevas versiones no introducen comportamientos, o solicitan permisos, que pueden resultar indeseados.

La actualización de las apps puede llevarse a cabo de diversas formas y está condicionada por el valor del ajuste "Actualización automática" descrito en el apartado anterior. La actualización de las apps de sistema proporcionadas por macOS se realiza a través de la actualización del sistema operativo (ver apartado "5.1. Actualización de macOS").

Para reinstalar las apps que se incluyen en el sistema operativo (por ejemplo, "iTunes" y "Contactos"), es preciso reinstalar macOS (se mantendrán los datos de usuario, tanto ficheros y datos, como ajustes).

Desde la sección "Actualizaciones" de la app App Store se accederá a las apps pendientes de actualizar. Se recomienda actualizarlas una por una, tras comprobar que no introducen o eliminan comportamientos inesperados por parte del usuario. Para ello, se recomienda desplegar el menú "Más" de cada app a actualizar y consultar los detalles.

Las actualizaciones automáticas se inician cuando el desarrollador de una app marca la actualización como "liberada" (*released*). Apple liberó la característica "*Phased Release for Automatic Updates*"[60] en marzo de 2019, por la cual los desarrolladores pueden elegir escalonar las actualizaciones automáticas de sus apps en fases, a lo largo de 7 días, de forma que, si surgen problemas con la nueva versión, el porcentaje de usuarios afectado sea mínimo. El desarrollador puede pausar la fase de liberación de la app hasta un máximo de 30 días.

13.2.2 DESINSTALACIÓN DE APPS DE LA APP STORE

La desinstalación de apps obtenidas de la App Store se realiza a través abriendo el "Launchpad" y pinchando sostenidamente sobre el icono de la app, hasta que todos los iconos empiecen a vibrar y aparezca una "x" junto al icono. Al pinchar sobre la "x", macOS solicitará confirmación al usuario para la desinstalación:

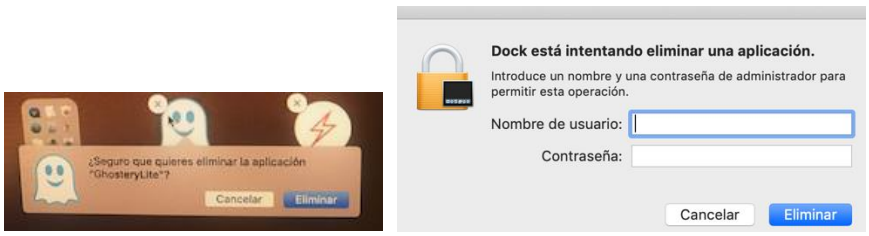


Figura 200 - Desinstalación de una app de la App Store

[60] https://developer.apple.com/app-store-connect/whats-new/?id=phased-release-macos

13.3 PAQUETES DE INSTALACIÓN

13.3.1 INSTALACIÓN DE APPS

Las apps descargadas de fuentes externas a la App Store estarán sujetas a las políticas de cuarentena explicadas en los apartados "9.2. Gatekeeper y cuarentena de archivos" y "9.3. Xprotect: software malicioso (malware)", por lo que se recomienda consultarlos para ver el procedimiento a seguir.

Antes de proceder a la instalación de un paquete descargado de una fuente externa, ***se recomienda utilizar un servicio de antivirus para su análisis***.

Los paquetes de instalación de macOS pueden proporcionarse en diversos formatos de ficheros:

- Fichero "`.dmg`": contienen imágenes de disco, que macOS gestiona como si se tratara de una unidad de disco virtual al hacer doble *click* sobre el fichero. Pueden contener un paquete de instalación, el cual guiará al usuario a través de un asistente o menú de instalación, o simplemente requerir arrastrar la aplicación a la carpeta "Aplicaciones" de forma manual. En ese caso, macOS solicitará las credenciales de administrador.
  Una vez finalice la instalación, se recomienda localizar la imagen de fichero "`.dmg`" en el panel de ubicaciones situado a la izquierda de Finder, expulsarlo y trasladarlo a la papelera.

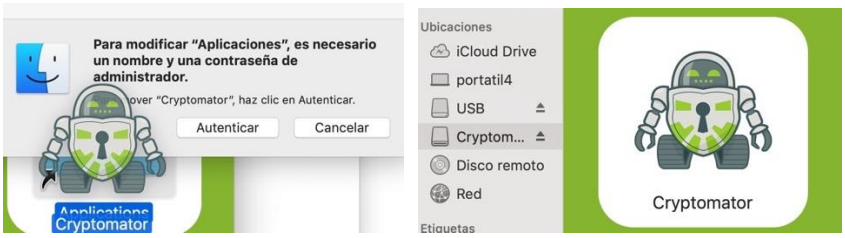


Figura 201 - Instalación de una app mediante un paquete ".dmg"

- Fichero "`.pkg`" o "`.mpkg`": son paquetes de instalación que incluyen *scripts* para la instalación directa de la app y de sus ficheros. La instalación se inicia haciendo doble *click* sobre el fichero, el cual guiará al usuario a través de los diversos pasos de instalación. Este formato es el que se emplea habitualmente para instalar apps que requieren ubicar componentes en otras carpetas de macOS (distintas a "`/Applications`"), extensiones de *kernel* o agentes de sistema.
- Fichero "`.zip`": suelen contener únicamente el fichero de la app, que se descomprimirá al hacer doble *click*, tras lo cual se trasladará manualmente a la carpeta "Aplicaciones".

NOTA: aunque el uso del directorio "Aplicaciones" para ubicar apps suele recomendarse por coherencia, algunas apps no ejecutarán si se ubican en otra carpeta diferente del sistema.

macOS solicitará introducir las credenciales de administración para proceder a la instalación de una app en la carpeta "Aplicaciones":

Figura 202 - Instalación de una app mediante un paquete de instalación

13.3.2 DESINSTALACIÓN DE APPS

Algunas apps procedentes de paquetes de instalación externos disponen de un menú de desinstalación propio.

Para las apps que no disponen de él, la instalación se suele realizar arrastrando el fichero de la app a la papelera de macOS. Esta forma de desinstalación puede dejar contenidos de la app en ciertos directorios del Mac, por lo que existen en el mercado utilidades específicas para suprimir todos los contenidos de estas apps y realizar una limpieza más exhaustiva de todos los contenidos remanentes de las apps.

13.4 AJUSTES ESPECÍFICOS DE UNA APP

13.4.1 FICHEROS PLIST DE UNA APP

En el apartado "7.1.1. Ficheros PLIST de configuración" se describió el uso y formato de los ficheros PLIST o "*Property List*" en relación a los servicios de macOS.

Complementariamente, los ajustes y parámetros de configuración de cualquier aplicación proporcionada con macOS, o instalada por el usuario, lleva asociados otros ficheros "`.plist`".

- El correspondiente a preferencias de la app, que el usuario puede personalizar. Los parámetros por omisión de estos ficheros son los definidos por el desarrollador, administrador o el *software* instalado en macOS (normalmente, con permisos de administrador)[61]. Su ubicación puede estar en:
  - "`/Library/Preferences`": para ajustes que afectan a todos los usuarios, y, particularmente, los que se aplican antes de que cualquier usuario inicie sesión.
  - "`~/Library/Preferences`": albergan opciones específicas de un usuario, y que entran en vigor cuando el usuario inicia sesión.
  - "`~/Library/Containers/`": almacena los "`.plist`" con los parámetros definidos por el usuario para las aplicaciones que ejecutan en un *sandbox* (ver apartado "9.4. Sandbox").

  Si un fichero de preferencias se corrompe, el usuario puede borrarlo, y la app lo recreará cuando vuelva a ser lanzada.

[61] https://eclecticlight.co/2016/10/25/preference-settings-where-to-find-them-in-macos-sierra/

- Un fichero "`Info.plist`" que reside bajo el directorio de instalación de la app, y que especifica datos y metadatos generales de la misma, como la versión, el desarrollador, la plataforma, etc.
  Los ficheros "`Info.plist`" contienen las claves (*key*) de tipo "`NS<recurso>UsageDescription`", en el que informan al usuario de por qué solicitan un permiso concreto asociado a los ajustes de privacidad. Para más información sobre el contenido de estos ficheros, consultar la [Ref.- 132].

Los ficheros PLIST tienen contenidos XML, y pueden ser almacenados en formato ASCII o en formato binario. La lectura de ficheros en formato binario puede realizarse a través de la utilidad "`plutil`" y del entorno de desarrollo de Apple Xcode [Ref.- 14]:

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

$ plutil -convert xml1 -o -
/Library/Preferences/com.apple.SoftwareUpdate.plist | less

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>AutomaticCheckEnabled</key>
        <false/>
        <key>AutomaticallyInstallMacOSUpdates</key>
        <false/>
...
```

Figura 203 - Comando "plutil" para el manejo de ficheros ".plist" en formato binario

Es posible modificar y añadir parámetros a ficheros de preferencias "`.plist`" desde la línea de comandos a través del comando "`defaults write <paramétro> <valor> <PATH_del_fichero_plist>`". Es importante destacar que para ello es preciso dotar a la app "Terminal" de acceso total al disco (ver apartado "8.2.4. TCC: Transparency, Consent and Control").

Adicionalmente, Apple proporciona la herramienta "`PlistBuddy`", ubicada en "`/usr/libexec`" (y no en el PATH por defecto), que permite realizar operaciones sobre un fichero PLIST (por ejemplo, añadir, borrar o editar valores) [Ref.- 80].

14.NAVEGADOR WEB SAFARI

Safari es el único navegador web suministrado por defecto con macOS.

Desde la versión 12 (la versión instalada con Mojave es la 12.1), Safari no soporta NPAPI, la arquitectura requerida por las *applets* de Java, por lo que no es posible ejecutar Java en el navegador web [Ref.- 121]. Entre las características de seguridad y privacidad de la versión de Safari de Mojave, se incluyen:

- Mejoras en la prevención del seguimiento de la actividad del usuario (*Intelligent Tracking Prevention*)[62]:
  - Safari proporciona a los sitios web un perfil de sistema simplificado, con el que se trata de evitar que obtengan una huella (*fingerprint*) del ordenador.
  - Se detecta la utilización de botones asociados a redes sociales, comentarios o compartición, destinados a obtener información del usuario.
- Algunas extensiones (*plug-ins*) están deshabilitadas por defecto, como la de QuickTime, y se ubican en el directorio "`/Library/Internet\ Plug-Ins/Disabled Plug-Ins`".
- Implementación de técnicas *antiphising* que alertan al usuario cuando visita un sitio web sospechoso de suplantar a uno legítimo.
- La barra de navegación muestra el icono "🔒" si se ha establecido conexión HTTPS con un sitio web. En caso contrario, se mostrará el texto "Not Secure".
- Safari 12.1 emplea TLS v1.3 de forma experimental, como puede comprobarse accediendo al recurso "https://www.ssllabs.com/ssltest/viewMyClient.html"):

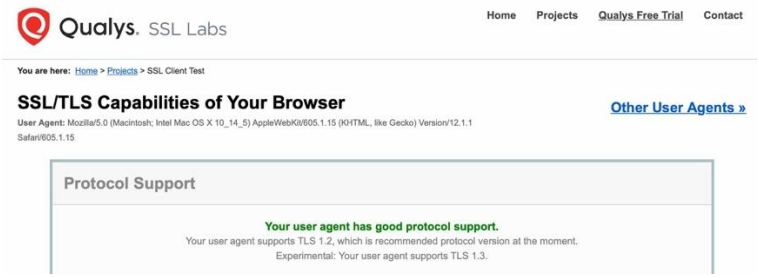


Figura 204 - Comprobación de la versión de TLS de Safari

- Safari muestra mensajes de aviso si el usuario accede a sitios web considerados inseguros, y no permite más de 20 redirecciones:

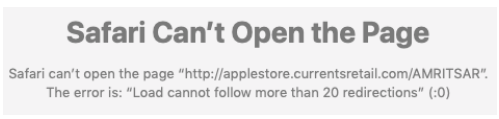


Figura 205 - Safari impide más de 20 redirecciones para un sitio web

[62] https://www.intego.com/mac-security-blog/macos-mojave-whats-new-in-security-and-privacy-features/

- Safari ofrece "navegación privada" (*private browsing*), que evita que se almacene en el dispositivo el histórico de navegación o las cookies de esa sesión, o que se sincronicen otros datos de navegación con otros dispositivos, para salvaguardar la privacidad del usuario. Para ello se dispone de la opción "Archivo - Nueva ventana privada".

Dado que Safari es una app de tipo *sandbox* (ver apartado "9.4. Sandbox"), su fichero de ajustes se encuentra en el directorio "`~/Library/Containers/`", en concreto en "`~/Library/Containers/com.apple.Safari/Data/Library/Preferences/com.apple.Safari.plist`", y está en formato binario.

A continuación se proporcionan las principales recomendaciones de seguridad a nivel de ajustes de configuración asociados a Safari.

14.1 AJUSTES DE SISTEMA PARA SAFARI

Dentro de la sección "Preferencias del sistema" se encuentran los ajustes:

- "General - Navegador web por omisión": la instalación de macOS Mojave establece que Safari será el navegador web que se empleará por defecto cuando se pinche sobre un enlace o URL en cualquier app. Este ajuste se puede cambiar para elegir otro navegador web.
- "Controles parentales - Internet": permite establecer límites en el acceso a sitios web si la cuenta de usuario está configurada con "Activar controles parentales".
- "iCloud": permite que los datos generados por Safari durante su uso se almacenen en la cuenta de iCloud del usuario, de forma que estén disponibles en todos los dispositivos vinculados a su cuenta. Se recomienda evaluar la sensibilidad de estos datos, especialmente si el Mac está destinado a uso empresarial, para evitar que los mismos sean custodiados por Apple en la nube.

14.2 AJUSTES ESPECÍFICOS DE SAFARI

La configuración específica de Safari se gestiona desde el menú de Safari, "Preferencias", y consta de un conjunto de secciones descritas a continuación.

- **General**: ***se aconseja***:
  - "Abrir archivos "seguros" al descargarlos": ***desactivar***. Es preferible proceder a la apertura de un archivo desde la carpeta seleccionada para su descarga en la sección "Ubicación de descarga de archivos" tras haber realizado comprobaciones adicionales del mismo (por ejemplo, a través de un antivirus).

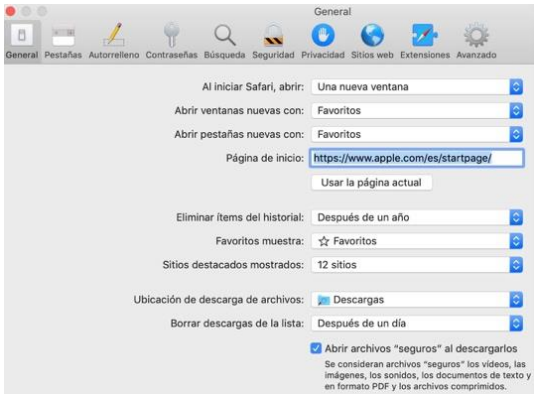


Figura 206 - Sección "General" de ajustes de Safari

- **Búsqueda**: ***deshabilitar la opción*** "Campo de búsqueda inteligente - Incluir sugerencias de Safari", que integra Safari con Spotlight (ver apartado "8.3. Spotlight") y que se use el navegador web como instrumento de las búsquedas de Spotlight asociadas a páginas web. Esta recomendación es aún más vigente si el navegador preferido (o por omisión) no es Safari.
- **Autorrelleno**: esta sección permite configurar si el navegador web puede completar automáticamente los campos de un formulario, accediendo a los elementos almacenados en un llavero (por defecto, el asociado al usuario en macOS, si bien también se permite la integración entre Safari y otros gestores de contraseñas).
  Aunque desde el punto de vista de usabilidad esta funcionalidad resulta muy práctica, también simplifica que un tercero con acceso eventual al navegador pueda autentificarse en sitios web sin necesidad de conocer las credenciales. Por tanto, ***se aconseja desactivar todos los componentes de la sección***. Otra opción aceptable desde el punto de vista de seguridad es almacenar solo información de sitios web para los que, aunque un tercero lograses acceso no autorizado, el impacto resulte mínimo para el usuario.

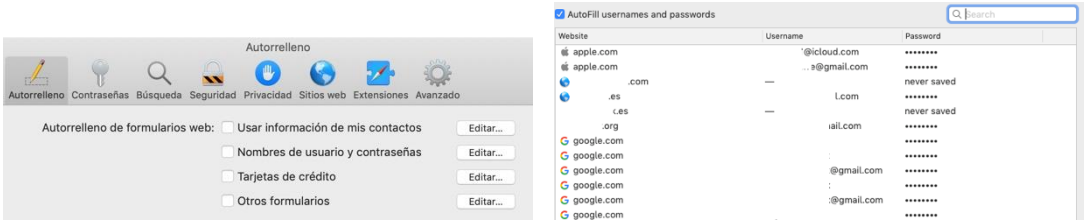


Figura 207 - Sección "Autorrelleno" de ajustes de Safari

Cuando Safari accede a una URL para la cual dispone de información personal almacenada, mostrará una ventana con un símbolo de llave para que el usuario seleccione qué elemento del llavero desea utilizar:

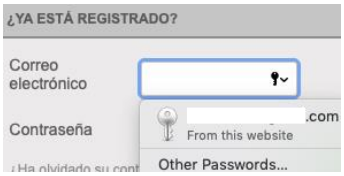


Figura 208 - Utilización de la función "Autorrelleno" de Safari

Cuando el usuario accede a un sitio web para el que Safari no dispone de información para las credenciales, mostrará la siguiente ventana:

Figura 209 - Solicitud de permiso para guardar contraseña en Safari

Safari se integra con el llavero del usuario, de forma que añade una entrada para el sitio web con los siguientes datos:

- Si el usuario acepta "Guardar contraseña", se almacenará la entrada en el llavero junto a la contraseña.
- Si el usuario elige "Nunca para este sitio web", se añadirá una entrada al llavero con la opción "Password not saved". De este modo, Safari no volverá a solicitar recordar la contraseña para ese sitio web.
- Si el usuario elige "Ahora no", no se añadirá ninguna información al llavero.

- **Contraseñas**: permite consultar qué contraseñas se han almacenado en el llavero (del usuario, ya sea en el sistema o en iCloud). Desde esta sección se puede visualizar la contraseña de cualquier sitio web para el que el usuario haya dado su consentimiento para que sea almacenada, previa introducción de las credenciales de usuario. ***Se desaconseja almacenar contraseñas de sitios web cuyo acceso resulte crítico***. Para obtener recomendaciones generales del almacenamiento de contraseñas, se aconseja consultar el apartado "9.7. Gestión de llaveros".

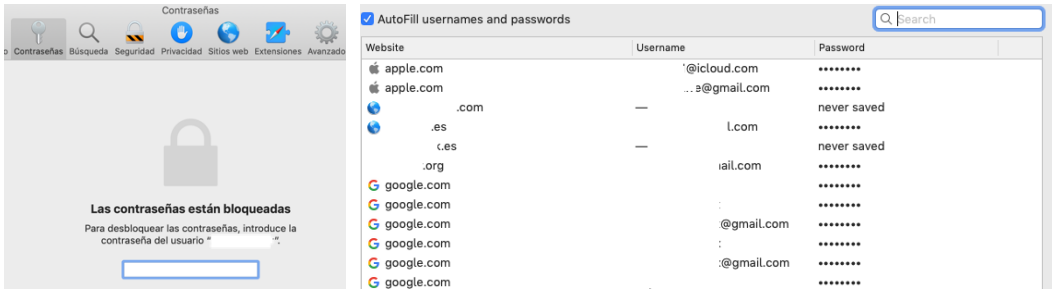


Figura 210 - Sección "Contraseñas" de ajustes de Safari

Safari controla si existe reutilización de contraseñas en distintos sitios web. En caso afirmativo, la entrada para ellas se marcará con un símbolo de aviso "⚠", desde el que se puede acceder directamente al sitio web para modificar las credenciales. ***La reutilización de credenciales está totalmente desaconsejada***, ya que, si un sitio web resulta comprometido, los atacantes podrán intentar acceder a otro de forma exitosa con las mismas credenciales.

- **Sitios web**: los ajustes de esta sección contienen distintos módulos, que se pueden habilitar/deshabilitar de forma global o granular (por sitio web específico). Los módulos de la sección superior vienen preinstalados con Safari, mientras que los que aparecen en la parte inferior (bajo el texto "Módulos") son los que ha instalado expresamente el usuario (normalmente, los módulos son componentes de alguna app que ha sido instalada).
  Si algún módulo tiene su ajuste definido como "Preguntar", la primera vez que se visite un sitio web que solicite acceso a la funcionalidad del módulo, Safari mostrará una ventana de diálogo solicitando confirmación.

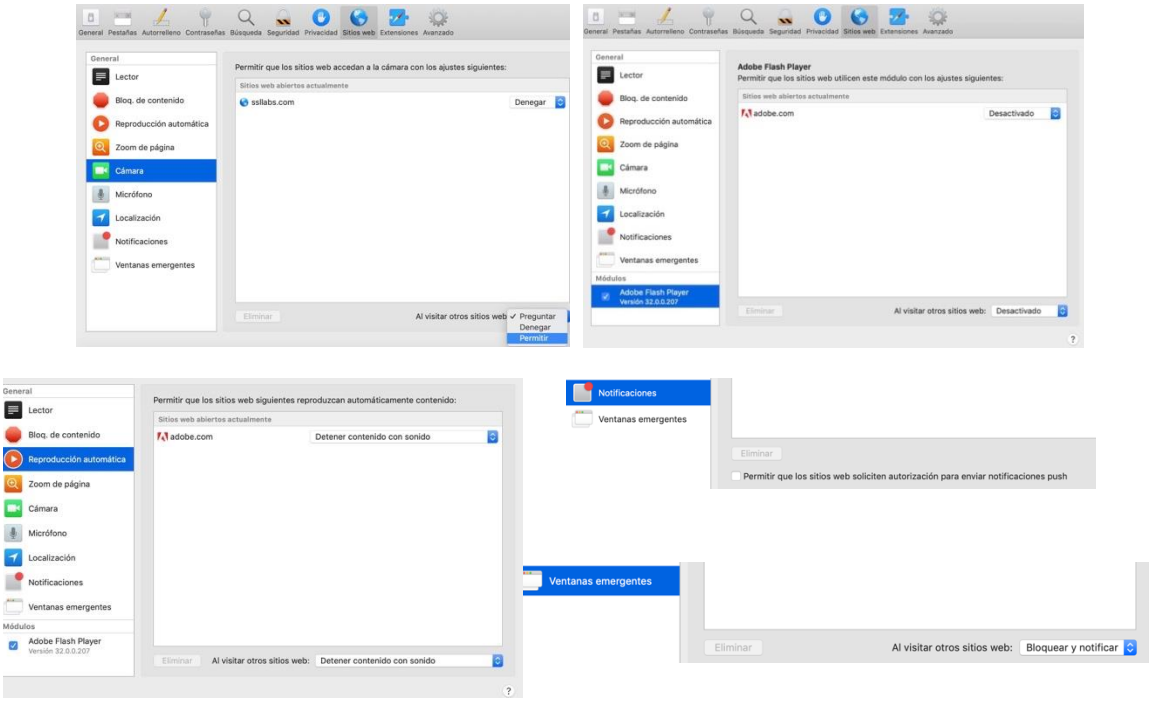


Figura 211 - Sección "Sitios web" de ajustes de Safari

  - **Cámara** y **Micrófono**: se recomienda ***establecer como opción general*** "Denegar", y, para sitios web de confianza que sí precisen el uso de estos recursos (por ejemplo, de videoconferencia), seleccionar "Preguntar" para tener control de cuándo están accediendo a ellos.
  - **Reproducción automática**: ***seleccionar*** "No reproducir nada automáticamente".
  - **Localización**: ***se aconseja*** "Denegar" ***el permiso de ubicación para sitios web***, de cara a salvaguardar la privacidad del usuario. Complementariamente, se debe ratificar que Safari no está entre las apps con acceso a los servicios de localización generales (ver apartado "8.2.4.4. Localización").
  - **Notificaciones**: este apartado se refiere a la recepción de notificaciones que los sitios web lanzan como ventanas de "*pop-up*", típicamente para que el usuario se suscriba al sitio. Si no se desea utilizar este mecanismo, que suele interrumpir bruscamente la navegación, se puede deshabilitar

la opción "Permitir que los sitios web soliciten autorización para enviar notificaciones push".

En ocasiones, algunos elementos emergentes no desaparecen, y presentan botones de "Cerrar" cuya función real es diferente. Se recomienda consultar la página de soporte de Apple [Ref.- 123], en la que se proporcionan indicaciones para bloquear elementos emergentes en Safari.

El uso de módulos está asimismo afectado por el ajuste "Avanzado - Detener módulos para ahorrar energía", que Safari tiene habilitado por omisión, y que bloquea el contenido que usa módulos transcurrido un tiempo desde su inicio.

- **Seguridad**:
  - "Advertir al visitar un sitio web fraudulento": ***se recomienda habilitarla***.
  - "Permitir Javascript": aunque desde el punto de vista de seguridad se recomienda deshabilitar esta opción, sin ella muchos sitios web no funcionarán correctamente.

Figura 212 - Sección "Seguridad" de ajustes de Safari

- **Privacidad**: para esta sección, se recomienda:

Figura 213 - Sección "Privacidad" de ajustes de Safari

  - "Impedir seguimiento entre sitios web": ***se recomienda habilitarla***, ya que minimiza el impacto que tiene el uso de servicios y contenedores externos que ciertos sitios web utilizan para rastrear la navegación del usuario y enviarle anuncios. No impide que se haga uso de contenedores, pero elimina los datos periódicamente.
  - "Bloquear todas las cookies": aunque desde el punto de vista de seguridad se recomienda marcar esta opción, la realidad es que muchos sitios web no funcionarán correctamente si no pueden utilizar cookies. Por tanto, a

nivel práctico, se puede habilitar la opción y ***utilizar la opción*** "Gestionar datos del sitio web..." ***para eliminar las cookies almacenadas que ya no se requieren*** a nivel de sitios web individuales.

Debe tenerse en cuenta que eliminar los datos de los sitios web también elimina su política de HSTS, por lo que habrá que prestar especial atención la primera vez que se vuelve a conectar por HTTP o HTTPS a dicho sitio web.

- En los equipos dotados de "Touch ID" o si el Mac ha iniciado sesión en una cuenta de iCloud asociada a un iPhone y *Handoff* está habilitado (ver apartado "11.4. Servicios de "Continuidad""), se dispone de la opción "Permitir a los sitios web que comprueben si está configurado Apple Pay", que hará que el sitio web de comercio electrónico muestre el botón para pagar con Apple Pay: ***se aconseja desmarcar esta opción***.

- **Extensiones**: las extensiones son módulos que añaden funcionalidad al navegador web. Sin embargo, se debe ser cuidadoso a la hora de instalar extensiones desde sitios web o desde otro *software* cuya procedencia no sea segura.
  Safari no permite seleccionar los permisos de una extensión de forma granular, por lo que, tras instalar una extensión, ***se recomienda ver los permisos de que dispone*** pinchando sobre su entrada de esta sección, como se ilustra a continuación, y desactivarla/desinstalarla si no se consideran seguros.
  Si la extensión fue instalada por una app, será preciso desinstalar dicha app (ver apartado "13. Gestión de apps").

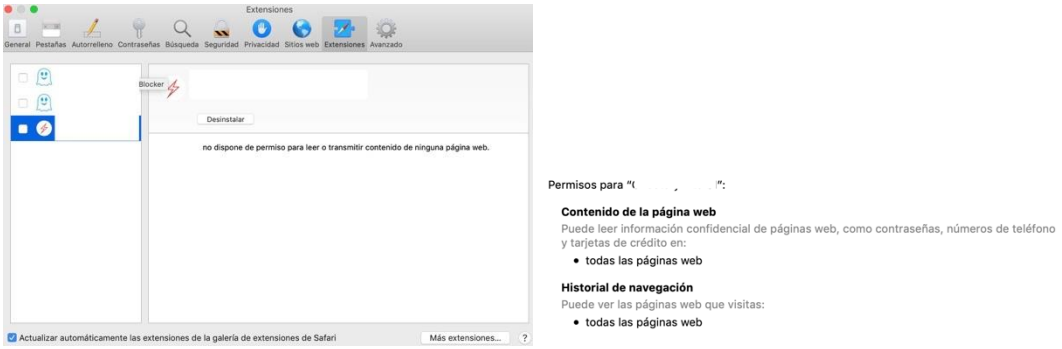


Figura 214 - Sección "Extensiones" de ajustes de Safari

Siempre que el navegador web Safari muestre un comportamiento anómalo o su rendimiento sea bajo, se aconseja desactivar las extensiones para ver si son la fuente del problema.

- **Avanzado**: ***se recomienda habilitar*** "Mostrar dirección completa del sitio web" 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 recurso web concreto y los parámetros de tipo GET empleados en la petición.

- El menú de Safari "Historial - Borrar historial..." permite eliminar el histórico de navegación de la última hora, el día de hoy, ayer y hoy, y todo el historial: ***se recomienda limpiar el historial periódicamente*** para proteger la privacidad del usuario.

14.3 GESTIÓN DE CERTIFICADOS EN SAFARI

macOS Mojave utiliza TLS 1.2 por defecto para las conexiones HTTPS. Las aplicaciones cliente, como Safari, hacen uso de estos protocolos si el acceso al servidor correspondiente solicita su utilización. Al acceder a un sitio web mediante HTTPS (y, por tanto, HTTP sobre TLS), Safari verificará el certificado digital asociado y su cadena de confianza, hasta llegar a validar la autoridad certificadora (*CA, Certificate Authority*) emisora de dicho certificado.

En caso de que no sea posible verificar la validez de un certificado, el navegador generará un mensaje de advertencia, indicando el motivo del error y permitiendo al usuario ver y analizar algunos detalles del certificado digital obtenido (mediante el botón "Mostrar detalles"). Si, pese a ello, se opta por aceptar el certificado, se volverá a pedir al usuario confirmación sobre la intención de visitar el sitio web:

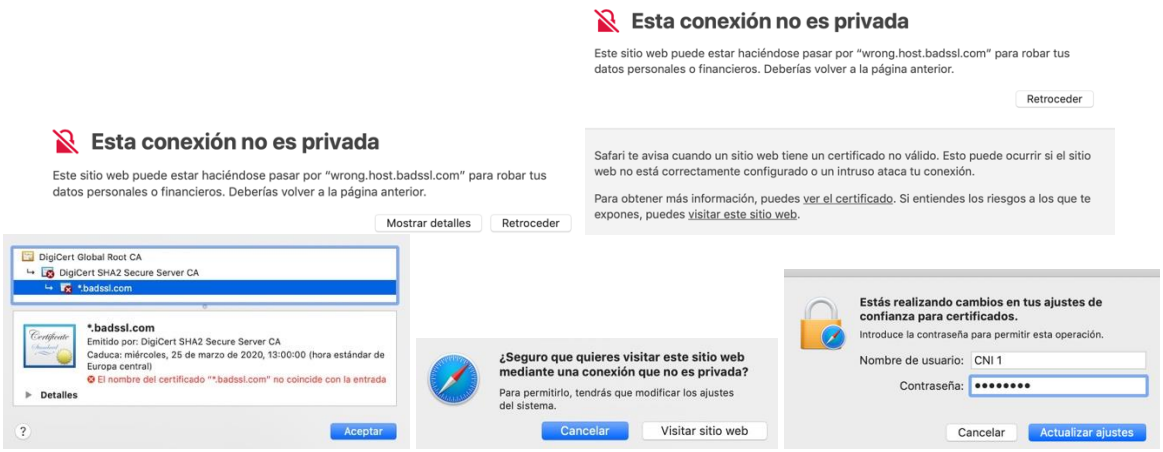


Figura 215 - Advertencia de Safari de un certificado digital que no es de confianza

Cuando se opta por hacer una excepción y aceptar el certificado pinchando en "Visitar sitio web", el sistema solicitará las credenciales del usuario y añadirá el certificado al llavero, con lo cual será aceptado de forma permanente para el sitio web a partir de ese momento, aunque se elimine el historial de navegación web y las *cookies*. La única forma de evitar que se siga haciendo uso de dicha excepción para un sitio web es modificar manualmente (o eliminar, ***que sería la opción recomendada***) su entrada en el llavero del usuario.

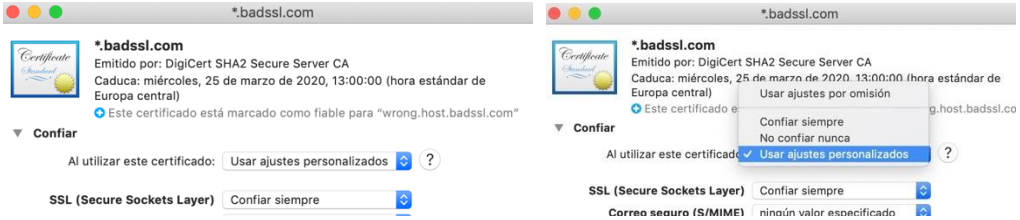


Figura 216 - Entrada en el llavero para un certificado no confiable que aceptó el usuario

La acción de aceptar un certificado no verificado tiene el riesgo de que el certificado digital aceptado (y desconocido) pertenezca a un potencial atacante realizando un ataque de interceptación, MitM (*Man in the Middle*), sobre el protocolo TLS y las comunicaciones (supuestamente) cifradas del usuario. Por ello, ***es extremadamente importante evitar aceptar un certificado que no sea de confianza y que no haya podido ser validado***.

Una vez se ha establecido una conexión de confianza mediante HTTPS con un sitio web, es posible ver su certificado pinchando sobre el símbolo "🔒", lo cual permite al usuario verificar que no ha habido un ataque de suplantación:

Figura 217 - Visualización de un certificado digital en Safari

Los perfiles de configuración de macOS (cuyo detalle excede el ámbito de la presente guía) disponen de un ajuste que posibilita configurar el ordenador para no permitir al usuario aceptar certificados digitales que no son de confianza ("*Allow user to accept untrusted certificates*"). Se recomienda hacer uso de este ajuste de configuración para limitar los riesgos asociados a permitir comunicaciones con un servicio remoto que emplea un certificado digital que no es de confianza.

Safari presenta carencias en la verificación de certificados digitales con validación extendida, ya que la única diferencia es el color del candado junto al título de la página web, que será de color verde si se trata de un certificado con validación extendida y negro o gris si no lo es.

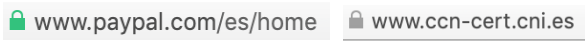


Figura 218 – Visualización del uso de un certificado digital en la barra de Safari

15.CIFRADO DEL ALMACENAMIENTO

macOS Mojave soporta diferentes técnicas de cifrado del almacenamiento, que se describen a continuación.

15.1 FILEVAULT

La tecnología FileVault, y, en concreto, FileVault 2, proporciona capacidades de cifrado para la totalidad del sistema de almacenamiento principal o disco duro del equipo, así como de unidades extraíbles, empleando XTS-AES-128 con claves de 256

bits [Ref.- 9], que se envuelven con las credenciales de los usuarios para los cuales FileVault se encuentra habilitado.

FileVault protege los datos ante cualquier intento de acceso a ellos que no conlleve la introducción de credenciales válidas o de la clave de recuperación, incluso si la unidad física se extrae del sistema y se conecta a otro ordenador, o si se realiza el arranque desde la unidad de almacenamiento en modo monousuario.

FileVault 2 se sustenta sobre una jerarquía de tres niveles de claves y dos variantes de claves de recuperación (PRK - *Personal Recovery Key,* e IRK - *Institutional Recovery Key*) [Ref.- 30]:

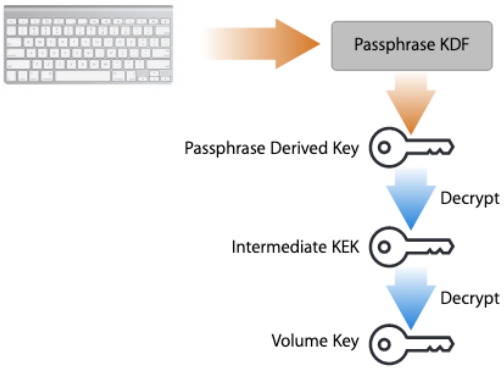


Figura 219 - Esquema de descifrado de FileVault [Ref.- 30]

- *Volume Encryption Key* (VEK): es la clave maestra que cifra el volumen lógico a nivel de bloque mediante AES, y que no varía a lo largo de su vida útil. Se genera de forma aleatoria para cada volumen lógico.
- *Key Encryption Key* (KEK): esta clave, aleatoria y simétrica, se genera cuando el volumen se inicializa, y envuelve a la clave VEK. Su propósito es independizar la VEK de las claves DEK (descritas a continuación), y viceversa.
- *Derived Encryption Key* (DEK): esta clave, que envuelve la KEK, sirve como inicio de la cadena de descifrado, permitiendo independizar la VEK de los cambios de contraseña que cada usuario puede llevar a cabo. Gracias a ella se evita la exposición del material criptográfico (o clave maestra, VEK).
  Existen dos tipos de DEK, según se basen en:
  - *Frase de paso* (*passphrase-based*)*:* una cadena de caracteres se convierte en una clave con el algoritmo de derivación de claves basado en PBKDF2 (*Password-Based Key Derivation Function*), que puede ser de dos tipos:
    - Clave basada en la contraseña del usuario: esta clave DEK se genera a partir de la contraseña de cada nuevo usuario que se habilita en el sistema para acceder a FileVault, y es exclusiva para él.
    - Clave basada en una contraseña de disco: éste es un caso especial de uso que permite descifrar el disco sin necesidad de que un usuario se haya autentificado en él.
  - Una identidad X.509 (o certificado digital): se usa en escenarios empresariales, para que no sea necesario, a la hora de descifrar los

volúmenes, disponer de usuarios locales de sistema operativo. La parte pública de la identidad envuelve la KEK, y, a su vez, la parte privada permite desenvolverla.

La información necesaria para descifrar el disco es obtenida de una partición de arranque alternativa no cifrada (de tipo "*Apple_Boot*"). En concreto, macOS emplea la partición de recuperación identificada con la etiqueta "*Recovery HD*".

NOTA: los mecanismos de protección de FileVault están asegurados cuando el equipo está apagado. Cuando el Mac entra en modo reposo (*standby*), la clave de cifrado de FileVault se almacena en memoria para acelerar el proceso de salida de este modo al levantar la pantalla del equipo, permitiendo, potencialmente, que se accediese a la información protegida por FileVault.

Si se desea evitar este comportamiento (***opción recomendada***), se puede utilizar el comando que se muestra a continuación. El usuario deberá introducir de nuevo su contraseña para descifrar el contenido del disco, lo que ralentiza unos segundos la entrada en servicio del equipo:

```
$ sudo pmset -a destroyfvkeyonstandby 1
```

El inconveniente de esta configuración es que las acciones que se llevan a cabo durante el tiempo en que el equipo está en reposo por parte de macOS (como la realización de copias de seguridad programadas) no podrán ejecutarse.

Por tanto, desde el punto de vista de seguridad, ***se recomienda proceder a cifrar el contenido del disco con FileVault*** tan pronto sea posible.

15.1.1 PROCESO DE CIFRADO MEDIANTE FILEVAULT

Los equipos suministrados de fábrica con macOS Mojave ya activan FileVault durante el proceso de configuración inicial. En todo caso, la activación manual de FileVault se realiza a través del menú "Preferencias del sistema - Seguridad y privacidad - [FileVault]", y requiere la introducción de las credenciales de un usuario administrador.

Los procesos de cifrado/descifrado mediante FileVault requieren que el equipo esté conectado a la corriente. En caso contrario, la operación no se realizará, aunque macOS no presenta en todos los escenarios un mensaje de error claro.

Antes de proceder al cifrado del disco, que se llevará a cabo en segundo plano, sin interferir con la actividad del usuario ni precisar que se reinicie el sistema, macOS consultará al usuario sobre el método de recuperación en caso de olvido de las credenciales de acceso al sistema, siendo las opciones:

- Clave de recuperación, que es una cadena compuesta por 6 grupos de 4 caracteres alfanuméricos (números y letras mayúsculas), la cual deberá anotarse y guardarse en lugar seguro. Esta clave será mostrada en pantalla por el asistente de activación de FileVault.
- Custodia de la clave de recuperación en la cuenta de iCloud del usuario (es decir, en los servidores de Apple en la nube).

NOTA: complementariamente, en entornos de gestión empresarial, la clave de recuperación de FileVault puede definirse como una clave institucional, no dependiente de cada equipo.

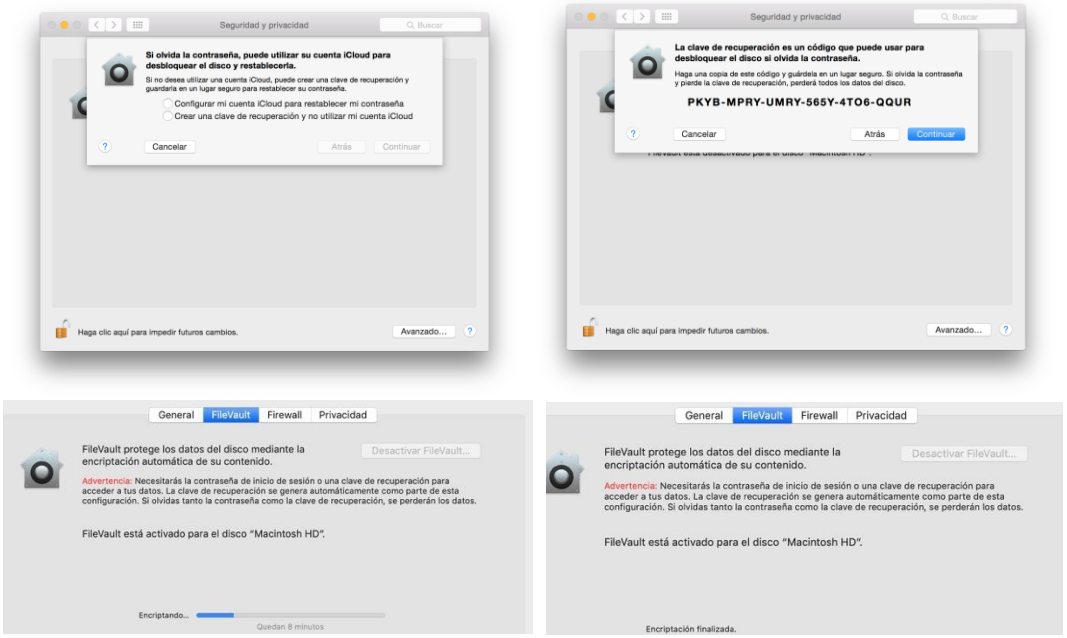


Figura 220 - Activación de "FileVault" desde el interfaz gráfico

El interfaz gráfico también permite proceder a la desactivación de FileVault (***desaconsejado desde el punto de vista de seguridad***), que también tendrá lugar en segundo plano:

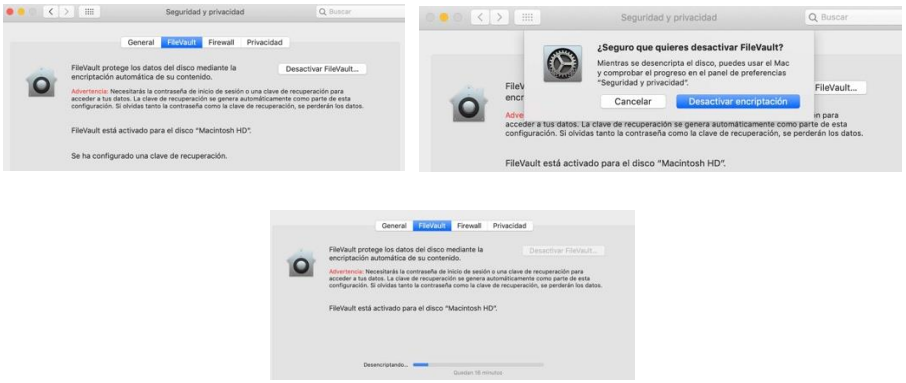


Figura 221 - Desactivación de "FileVault" (desaconsejado) desde el interfaz gráfico

NOTA: en versiones anteriores de macOS, la activación de FileVault requería indicar de forma expresa los usuarios para los cuales se deseaba habilitar FileVault mediante la opción "Activar usuario", lo cual requería que cada uno de ellos introdujese su contraseña.

En macOS Mojave, por defecto, la activación de FileVault se lleva a cabo para todos los usuarios existentes en el equipo, siendo necesario introducir únicamente la contraseña del usuario administrador que inicia la operación (ver apartado "15.1.3. Secure Token").

Alternativamente, el comando "`fdesetup`" permite gestionar la activación/desactivación de FileVault desde la línea de comandos. Durante las pruebas realizadas en la elaboración de la presente guía con la versión de Mojave 10.14.4, se ha

constatado que los botones de "Activar FileVault" y "Desactivar FileVault" pueden aparecer sombreados o no ser operativos, siendo la línea de comandos la única alternativa para interaccionar con las capacidades de FileVault (en caso de incongruencias):

```
$ fdesetup status
FileVault is Off.
```

```
$ sudo fdesetup enable
Password:
Enter the user name: admin
Enter the password for user 'admin':
Recovery key = 'XXXX-YYYY-ZZZZ-RRRR-SSSS-TTTT'

$ fdesetup status
FileVault is On.
Encryption in progress: Percent completed = 17

$ fdesetup status
FileVault is On.

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

```
$ sudo fdesetup disable
Enter the user name:admin
Enter the password for user 'admin':
FileVault has been disabled.

$ fdesetup status
FileVault is On.
Decryption in progress: Percent completed = 13
```

Figura 222 - Comandos para la administración de FileVault

El comando "`fdesetup`" de la <Figura 223> 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*). La lista general de usuarios y su UUID en macOS (independiente de FileVault) se puede obtener mediante el comando "`dscl`":

```
$ sudo fdesetup list -extended
ESCROW  UUID                                    TYPE
USER
        B0E40294-BF61-4D1A-98AD-C14986552410    OS User
admin
        EC1C2AD9-B618-4ED6-BD8D-50F361C27507    iCloud Recovery Record    -
        F21367A7-C601-460E-8A97-A6F2C5D4F2FC    OS User
cniusuario1
        EBC6C064-0000-11AA-AA11-00306543ECAC    Personal Recovery Record  -
        DE3727E8-0231-4279-8937-9D982FFE1AA9    OS User
ccntest

$ dscl /Search -list /Users GeneratedUID | grep -v '^_'
admin                   B0E40294-BF61-4D1A-98AD-C14986552410
ccntest                 DE3727E8-0231-4279-8937-9D982FFE1AA9
cniusuario1             F21367A7-C601-460E-8A97-A6F2C5D4F2FC
daemon                  FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000001
Guest                   FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000C9
nobody                  FFFFEEEE-DDDD-CCCC-BBBB-AAAAFFFFFFFE
root                    FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000000
```

Figura 223 - Usuarios con capacidades de descifrado del disco en FileVault

Por defecto, la clave de recuperación (*Recovery Key*) generada al habilitar FileVault es de tipo personal. A través del comando "`fdesetup`" se puede generar una clave de recuperación de tipo empresarial basada en un certificado digital X.509 (que debe estar disponible en "`/Library/Keychains/FileVaultMaster.keychain`"). Para más información sobre la gestión empresarial de FileVault, se recomienda consultar la [Ref.- 29] y la página del manual del comando "`fdesetup`".

Las cuentas de usuario que se creen después de activar FileVault en macOS se activarán automáticamente como usuarios de FileVault. A través del comando "`fdesetup`" con las opciones "`remove -user <user name>`" y "`add -usertoadd <user name>`" es posible gestionar los usuarios que pueden desbloquear un disco cifrado con FileVault. Los usuarios que sean excluidos no podrán descifrar el disco tras el arranque, pero, una vez que un usuario que sí tenga capacidades de FileVault habilitadas introduzca sus credenciales y lo descifre de forma exitosa, cualquier usuario existente en el sistema podrá iniciar sesión desde la pantalla de inicio de sesión. Los usuarios que no tengan FileVault habilitado tendrán el "*Secure Token*" deshabilitado (ver apartado "15.1.3. Secure Token").

```
$ sudo fdesetup add -usertoadd cniusuario1
Enter the user name: admin
Enter the password for user 'admin':
Enter the password for the added user 'cniusuario1':

$ sysadminctl -secureTokenStatus cniusuario1
2019-06-03 12:47:00.910 sysadminctl[546:7193] Secure token is ENABLED for
user Cni Usuario 1
```

Figura 224 - Habilitar FileVault para un usuario desde línea de comandos

15.1.2 ARRANQUE DEL EQUIPO CON FILEVAULT

Cuando FileVault está habilitado, 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 macOS. De hecho, la única indicación en el interfaz gráfico de usuario de macOS de que el usuario está activo en FileVault es que su entrada aparezca en la pantalla de arranque:

Figura 225 - Solicitud de credenciales para descifrar el disco mediante FileVault en el arranque

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`"). El comportamiento asociado a la pantalla de inicio de sesión de FileVault, en la que se desvela la lista de nombres de usuario que lo tienen habilitado, no puede ser modificado para que muestre en su lugar los campos de entrada de usuario y contraseña (lo cual sería más recomendable desde el punto de vista de seguridad).

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, se ofrecerá al usuario hacer uso de un mecanismo de recuperación:

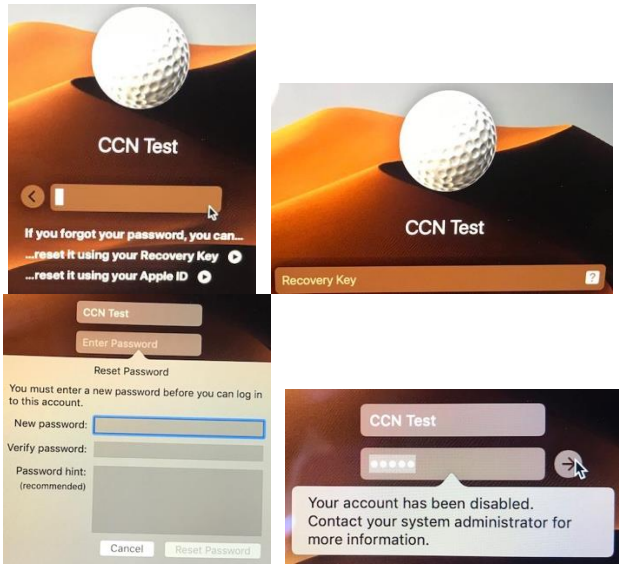


Figura 226 - Olvido de contraseña del usuario durante el arranque con FileVault

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 su contraseña del llavero (en este caso, sí es necesario conocer la contraseña previa del usuario para actualizar la contraseña del llavero); de lo contrario, será necesario crear un nuevo llavero accediendo al modo de recuperación. Si no se completa el proceso, se mostrará un mensaje que informa de que la cuenta ha sido deshabilitada (ver imágenes inferiores de la <Figura 226>).

NOTA: durante las pruebas llevadas a cabo en la versión de macOS 10.14.4, se constata que, a pesar del mensaje indicativo de que la cuenta ha sido deshabilitada, es posible reiniciar el equipo y acceder a la cuenta con la contraseña antigua.

La pantalla de inicio de sesión de FileVault traslada de forma automática las credenciales introducidas por el usuario, tras descifrar el disco, a la pantalla de inicio

de sesión estándar de macOS (proceso conocido como "*password-forwarding*"[63] [Ref.- 30]), con el objetivo de que el usuario no tenga que repetir su introducción.

FileVault simplifica el proceso de eliminación de los datos del equipo mediante el borrado instantáneo (*instant wipe*)[64], que elimina las claves de cifrado del volumen (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.

15.1.3 SECURE TOKEN

"*Secure Token*" es un atributo que se introdujo en macOS 10.13 para controlar las operaciones que los usuarios pueden realizar con FileVault en APFS (habilitarlo, deshabilitarlo, y tener la capacidad de descifrar un volumen cifrado). APFS cambia la forma en que se generan las claves de cifrado de FileVault ([Ref.- 28]). En los volúmenes APFS, las claves se generan:

- En el primer inicio de sesión interactivo del sistema: en el caso de un ordenador personal, el proceso de configuración de macOS se llevará a cabo a través de una cuenta de administrador local; en los entornos MDM, puede ser una cuenta de usuario estándar. En ambos casos, el "*Secure Token*" se otorga a esta cuenta.
- Durante el proceso de creación de usuarios a través del interfaz gráfico (menú de "Usuarios y grupos").

Tras su generación, las claves se almacenan como parte de un "*Secure Token*", que es el resultado de envolver una clave KEK (*Key Encryption Key*) con la contraseña del usuario.

Las cuentas creadas a través de línea de comandos no recibirán el "*Secure Token*", ni tampoco las cuentas móviles de "*Active Directory*". Para poder habilitar FileVault en estas cuentas, se recomienda consultar la [Ref.- 27].

NOTA: la configuración de las cuentas asociadas a entornos MDM con FileVault queda fuera del ámbito de la presente guía.

Complementariamente, el comando "`sysadminctl`" permite conocer específicamente el valor del "*Secure Token*" para un usuario concreto, tal como se ilustra en la <Figura 227>:

```
$ sysadminctl -secureTokenStatus cniusuario1
2019-05-31 12:43:49.692 sysadminctl[1280:28992] Secure token is ENABLED for
user Cni Usuario 1

$ sysadminctl -secureTokenStatus cniusuario2
2019-05-31 12:43:49.692 sysadminctl[1280:28992] Secure token is DISABLED for
user Cni Usuario 2
```

Figura 227 - Gestión del "Secure Token" a través de "sysadminctl"

[63] Esta funcionalidad estaba previamente documentada de manera oficial (enlace no disponible en el momento de elaboración de la presente guía): "http://training.apple.com/pdf/WP_FileVault2.pdf".
[64] http://www.apple.com/osx/what-is/security/

Aunque la opción "`-secureTokenOn <usuario>`" parece indicar que es posible habilitar el "*Secure Token*" para un usuario concreto, se ha constatado en la elaboración de la presente guía que el procedimiento para habilitar este *token* para un usuario pasa por ejecutar el comando descrito en la <Figura 224>.

15.2 CIFRADO DE ALMACENAMIENTO EXTERNO

macOS permite utilizar FileVault para llevar a cabo el cifrado completo de discos duros y unidades de almacenamiento externas que hagan uso de un esquema de particiones GPT (tabla de particiones GUID), por ejemplo, unidades de memoria USB externas, y las copias de seguridad de "Time Machine" (ver apartado "16.1. Time Machine"). Las unidades cifradas mediante este procedimiento solo serán accesibles desde otros equipos macOS.

Para formatear una unidad en modo GUID, debe accederse a la app "Utilidad de Discos" (los datos almacenados se perderán, por lo que habrá que realizar una copia de seguridad antes de proceder a esta operación) y:

- Seleccionar la entrada correspondiente a la unidad a formatear.
- Pinchar en la opción "Visualización - Mostrar todos los dispositivos".
- Elegir la entrada de nivel superior en la jerarquía correspondiente a la unidad.
- Con el botón derecho, seleccionar "Borrar". Esta operación lanzará un menú en el cual ha de elegirse el esquema "Mapa de particiones GUI". Desde este mismo menú, puede optarse por un formato que incluya cifrado (imagen inferior de la <Figura 228>).
- Confirmar la operación con el botón "Borrar".

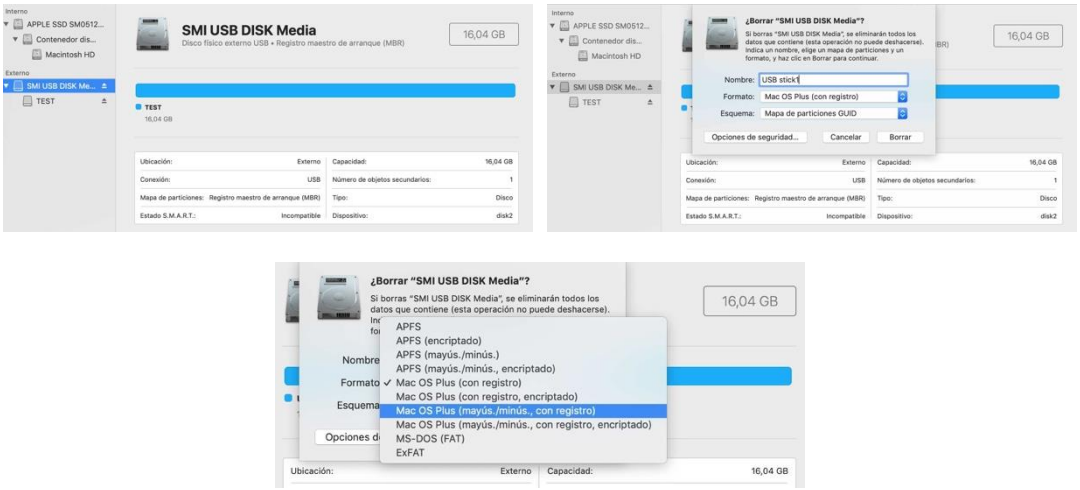


Figura 228 - Formateo de una unidad USB externa con esquema GUID

Una vez el dispositivo de almacenamiento esté formateado con esquema GUID, si se optó por un formato sin cifrado, es posible proceder a cifrar sus contenidos a través de la opción "Encriptar '<nombre de unidad>'" accesible desde el botón derecho de la app Finder, que emplea el cifrado XTS-AES de FileVault 2. 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 se

desconseja añadir cualquier tipo de indicación o recordatorio de la contraseña del usuario, se sugiere introducir el carácter de espacio en blanco:

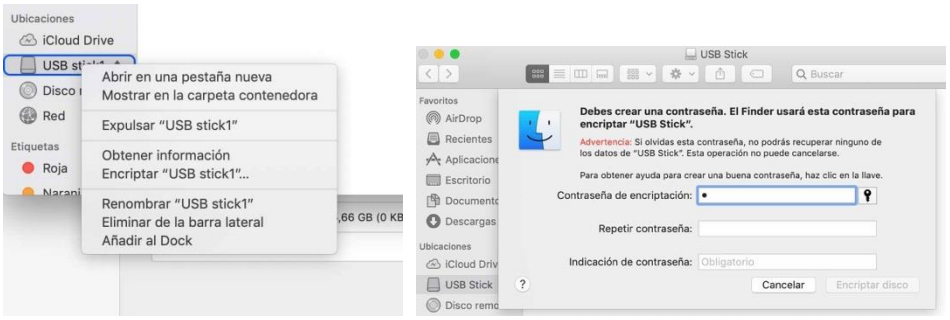


Figura 229 - Cifrado de una unidad USB externa a través de Finder

Al pulsar el botón "Encriptar disco" 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 macOS, únicamente pulsando el botón derecho sobre el disco o unidad externa, se puede ver el texto "Encriptando '<nombre de unidad>'..." en color gris, lo que indica que el proceso sigue activo:

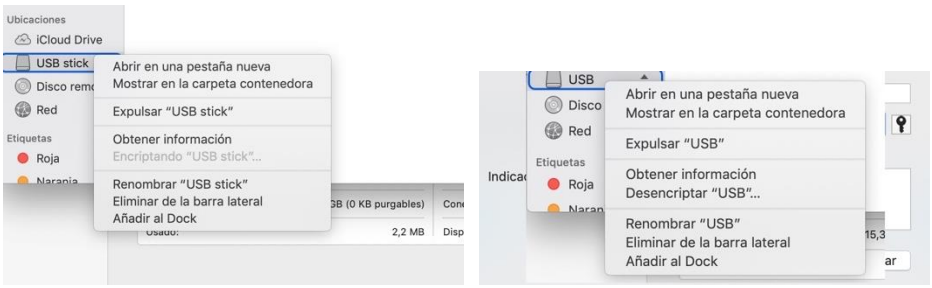


Figura 230 - Comprobación del proceso de cifrado de una unidad USB externa

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:

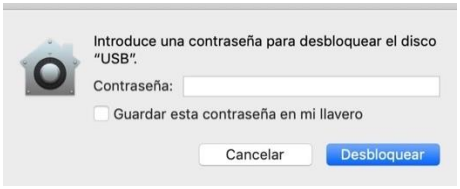


Figura 231 - Solicitud de contraseña para acceder a una unidad USB externa cifrada

Desde el punto de vista de seguridad, ***se desaconseja guardar las contraseñas de cifrado de las unidades de almacenamiento externas en el llavero***. Si, pese a esta recomendación, se opta por salvaguardar la contraseña en el llavero, la desconexión/reconexión de la unidad al equipo no exigirá reintroducir la contraseña.

Una unidad cifrada puede descifrarse a través del menú "Finder - <selección de la unidad> botón derecho - Desencriptar <nombre de unidad>". Para proceder, será necesario introducir la contraseña de cifrado.

15.3 CIFRADO DE FICHEROS "CONTENEDOR"

macOS permite crear un contenedor de ficheros cifrado, al que el usuario puede añadir ficheros cuyo contenido desea protegerse de forma individual. Un contenedor es una imagen de disco, que deberá ser montada y descifrada para poder acceder a sus contenidos.

El proceso para crear este contenedor cifrado consiste en:

- Abrir la "Utilidad de Discos" y seleccionar "Archivo - Nueva imagen - Imagen vacía".
- En la ventana que aparecerá, elegir la ruta y el nombre del fichero y establecer en el campo "Encriptación" el tipo de cifrado deseado. Este fichero tendrá extensión ".dmg".
- Introducir la contraseña de usuario que se utilizará para proteger la clave maestra de cifrado.

Una vez completado el proceso, el contenedor aparecerá en la sección de "Imágenes de disco" en el menú de "Utilidad de Discos", y en la sección "Ubicaciones" de la app "Finder". A través de la opción de "Expulsar" de cualquiera de ellas, se procederá a desmontar la imagen. Para volver a montarla, se accederá a la ruta del fichero ".dmg" asociado al contenedor y, al pinchar sobre él, el sistema solicitará la contraseña.

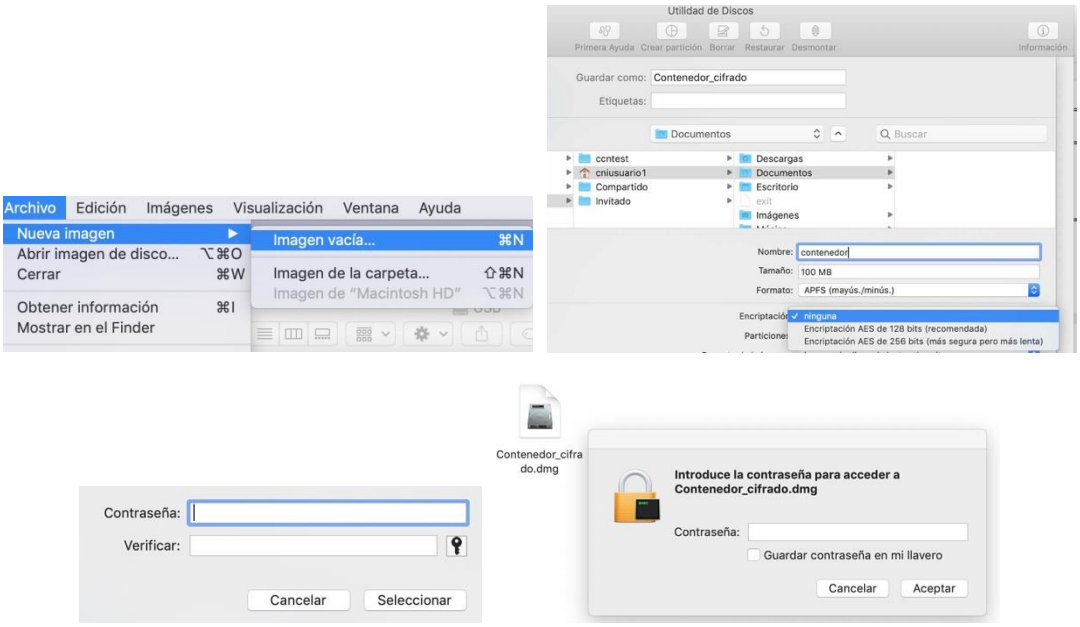


Figura 232 - Creación de un contenedor cifrado

15.4 CIFRADO DE ALMACENAMIENTO APFS CON CHIP T2

En los ordenadores Mac que incluyen el chip T2 [Ref.- 42], el cifrado del volumen interno mediante FileVault tiene lugar dentro del SEP (ver apartado "9.6.1. Secure Enclave Processor (SEP)"), y se basa en una jerarquía de claves que no se exponen de forma directa ante la CPU del sistema [Ref.- 43]:

- "*Volume key*": es una clave que se genera durante la creación de un volumen, y con la que se cifra tanto el volumen como sus metadatos.
- "*Class key*": es una clave que envuelve a la clave del volumen. Si FileVault está habilitado para el volumen, la clave de clase se protege mediante una combinación del UID del *hardware* (una clave única para el equipo que reside en el "*Secure Enclave*") y la contraseña del usuario. En caso contrario, la clave del volumen solo estará protegida por el UID de *hardware*.
- "*Media key*": esta clave envuelve a la clave de volumen, y su propósito es agilizar y permitir el borrado seguro de los datos. Esta clave reside en almacenamiento borrable, para que pueda ser suprimida de forma rápida a través de funcionalidades de borrado remoto como, por ejemplo, "Find My Mac" (ver apartado "11.3. Buscar mi Mac").

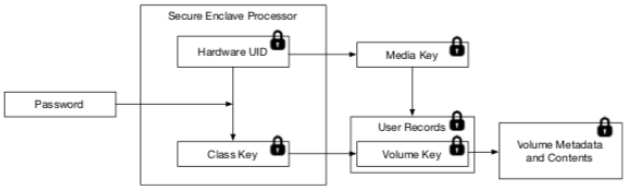


Figura 233 - Jerarquía de claves de FileVault en equipos con chip T2 [Ref.- 43]

Cuando se requiere llevar a cabo un proceso de autentificación basado en biometría, los datos recogidos por los sensores se envían al "*Secure Enclave*" a través de un bus serie, donde se procesan. Si el "*Secure Enclave*" los da por auténticos, envía una interrupción a la CPU.

El cifrado APFS se lleva a cabo mediante un motor AES dedicado, que se interpone entre la memoria principal del sistema y el almacenamiento *flash*. Durante el proceso de fabricación del "*Secure Enclave*", se generan dentro del él dos claves AES de 256 bits: el "*Mac unique ID*" (UID) y un "*Device Group ID*" (GID); estas claves no pueden ser leídas de manera directa ni por *software* ni por *firmware*, únicamente pueden ser accedidas por el motor AES dedicado dentro del SEP (teóricamente, ni siquiera Apple tiene acceso al UID). El UID protege a su vez secretos como los datos de Touch ID, las claves de FileVault y el Keychain.

Dado que el UID es exclusivo de un ordenador concreto, los contenidos del almacenamiento interno (ligados a las claves basadas en este UID) no podrán ser descifrados en ningún otro equipo.

Cuando se borra un volumen, la clave de volumen se elimina también a través del "*Secure Enclave*", lo cual impide que se pueda acceder a ella a posteriori, ni tan siquiera por el propio "*Secure Enclave*".

NOTA: el cifrado del almacenamiento externo no se realiza a través del chip T2, facilitando que dichas unidades de almacenamiento externas puedan ser compartidas entre distintos equipos.

PREVENCIÓN DE ATAQUES DE FUERZA BRUTA CON CHIP T2

El "*Secure Enclave*" implementa una serie de mecanismos para mitigar el impacto de los ataques de fuerza bruta sobre la contraseña del usuario, tanto en la ventana de

inicio como en modo de arranque "*Disco de destino*" (ver apartado "18.6. Modo "Target Disk""):

- Se limita a 30 los intentos de introducción de contraseña, tras los cuales:
  - Se permiten otros 10 arrancando en modo de recuperación de macOS (apartado "18.2. Modo "Recuperación" (Recovery)").
  - Se permiten 60 más para cada uno de los mecanismos de recuperación de FileVault definidos en el sistema (recuperación de iCloud, clave de recuperación de FileVault y clave institucional).

  Si se llega a agotar el número total de intentos, el "*Secure Enclave*" rehusará cualquier petición de descifrado del volumen, por lo que la unidad será irrecuperable.
- Se introducen retardos entre intentos fallidos, que se mantienen por parte del "*Secure Enclave*" aunque el equipo se reinicie:
  - 1 minuto: entre los intentos 15 y 17.
  - 5 minutos: entre los intentos 18 y 20.
  - 15 minutos: entre los intentos 21 y 26.
  - 1 hora: entre los intentos 27 y 30.

En caso de disponer de un equipo MAC dotado con Touch ID, las claves del *Secure Enclave* deben borrarse antes de traspasar el equipo mediante "`xartutil --erase-all`".

15.5 APFS (APPLE FILE SYSTEM)

El sistema de ficheros de Apple (APFS), introducido en macOS 10.13 (High Sierra) sustituye al previo denominado HFS+, más seguro, rápido y confiable, optimizado para almacenamiento en unidades SSD y *Flash*. Sus principales características son [Ref.-126]:

- La arquitectura de 64 bits de APFS soporta cifrado nativo, e incluye protección para evitar pérdida de datos ante fallos del sistema.
- Permite el cifrado tanto a nivel de disco completo como de ficheros individuales, con claves independientes entre el fichero y sus metadatos: esto permite que ciertos usuarios puedan alterar el contenido de un fichero sin tener acceso a los registros de modificaciones de dichos ficheros.
- Al activar FileVault para un volumen APFS durante la instalación de macOS, las claves de cifrado se generan durante la creación de un usuario o durante el primer inicio de sesión interactivo de un usuario del Mac, que dará lugar al *Secure Token* (ver apartado "15.1.3. Secure Token").
- Permite el clonado instantáneo de carpetas y unidades de disco.
- Mejora la utilización del espacio en disco, permitiendo que dos volúmenes APFS residentes en la misma unidad física puedan tomar espacio uno de otro si es necesario.

- Soporta ficheros denominados "dispersos" (*sparse*), que son aquellos que no ocupan todo el espacio real en disco que han reservado y que refleja su tamaño. Entre otras cosas, permite que una aplicación reserve un fichero de tamaño superior al espacio realmente disponible en disco.
- Optimiza el uso de almacenamiento de tipo *flash*.
- Incorpora una característica denominada "*fast directory sizing*", que mantiene registro del tamaño de los directorios, acelerando su cálculo.
- Al soportar el protocolo SMB, es posible acceder a volúmenes APFS desde otros equipos que no soporten APFS, como versiones antiguas de macOS o Windows.

Desde el punto de vista de seguridad, ***se recomienda el uso de* APFS**. Si el Mac procede de una versión anterior que hace uso de HFS+, la actualización a Mojave ofrecerá la posibilidad de convertir el sistema de ficheros de forma automática. En caso de no seleccionarse esa opción durante la actualización, es posible migrar posteriormente a APFS desde el menú "Edición - Convertir a APFS" de la app "Utilidad de discos" del modo de recuperación:

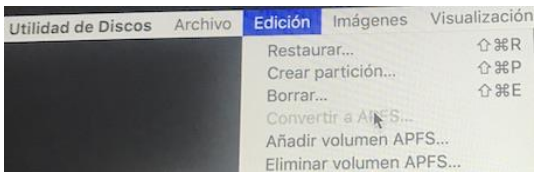


Figura 234 - Conversión de formato HFS+ a APFS del disco de sistema

Antes de proceder a la conversión, se recomienda realizar una copia de seguridad completa de los datos, para minimizar las consecuencias en caso de que el proceso aborte por causas desconocidas.

16. COPIAS DE SEGURIDAD Y RESTAURACIÓN

Un elemento fundamental para la protección del equipo y sus datos es mantener una política de copias de seguridad (*backups*) adecuada, especialmente antes de proceder a la actualización del sistema operativo y antes de instalar nuevas apps, especialmente si éstas provienen de mercados o fuentes no oficiales.

En macOS se distinguen dos tipos de copia de seguridad:

- Orientadas a los datos de usuario: las dos alternativas integradas de fábrica en macOS para la gestión de este tipo de copias de seguridad son Time Machine y el *backup* de iCloud.
- Orientadas a los datos del sistema, de forma que sea posible restaurar sus componentes en caso de fallo (ver apartado "16.3. Creación de un instalador de arranque en una unidad USB o un disco externo").

16.1 TIME MACHINE

La app Time Machine (en adelante, TM) permite salvar los contenidos completos del sistema de almacenamiento del equipo en un dispositivo de almacenamiento

externo (entre otros, una unidad USB externa, un sistema de almacenamiento NAS conectado a la red por SMB, o un Mac configurado como destino de la copia).

La configuración de las copias de seguridad con TM se detalla en la [Ref.- 124]. ***Se recomienda cifrar la unidad destino de las copias de seguridad***, de forma que solo sea posible acceder a los datos si se conoce la clave [Ref.- 125], especialmente si el destino de la copia es un NAS compartido con otros usuarios. Es importante reseñar que, a pesar de que el menú de TM indica "Encriptar copias de seguridad", no son las copias de seguridad propiamente las que se cifran, sino el disco en el que se albergan.

TM emplea por defecto un modelo de *backup* incremental: la primera copia será completa, pero, en las copias posteriores, solo se salvan los archivos que han sido modificados desde el anterior *backup*. Todas las versiones de esos ficheros son guardadas, permitiendo su posterior restauración. Las copias se realizan "en caliente", no requiriéndose que los usuarios interrumpan su trabajo.

Complementariamente, el usuario puede forzar un *backup* completo cuando lo considere oportuno. Se aconseja realizar copias de seguridad completas antes de cualquier actualización de sistema operativo y de apps del sistema.

Cuando se conecta una unidad de disco externa, el sistema, al detectarla, preguntará al usuario si desea utilizarla como destino de las copias de TM, debiendo indicar en ese momento si desea que las copias estén cifradas. Si no se opta por ese modelo, para pasar a copias cifradas se deberá seguir las instrucciones de la [Ref.- 127]:

Figura 235 - Selección de la unidad para las copias de seguridad de Time Machine

Una vez formateado el disco por parte de TM, se abrirá el menú de configuración (disponible en "Preferencias del sistema - Time Machine"); si se selecciona la opción "Mostrar Time Machine en barra de menús", el icono "" aparecerá en dicha barra, desde el que se puede iniciar una copia de seguridad.

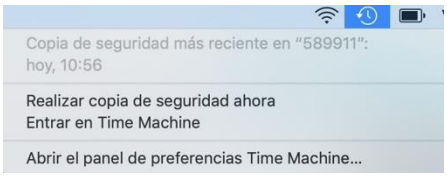


Figura 236 - Menú de TM en la barra de menús de estado

El menú "Opciones..." permite seleccionar qué elementos se excluirán de la copia de seguridad, tanto ficheros y directorios como otras ubicaciones (por ejemplo, unidades externas adicionales), para lo cual se requiere de acceso privilegiado. Por defecto, el propio disco está excluido. ***Se recomienda no excluir ningún elemento del***

disco de sistema en la primera copia de seguridad, para disponer de al menos un *backup* completo.

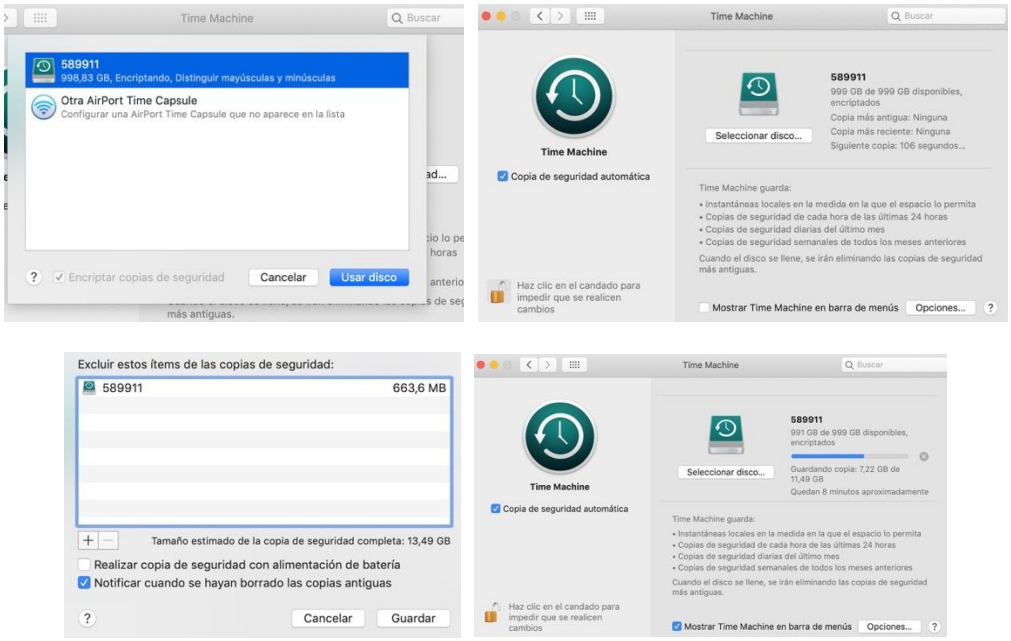


Figura 237 - Realización de una copia de seguridad con Time Machine

Mientras la unidad permanezca conectada al equipo, TM mantendrá un modelo de copia de seguridad fijo descrito en la cuarta imagen de la <Figura 237>. Para que esta planificación no se lleve a cabo, se debe desactivar la opción "Copia de seguridad automática", pero no es posible definir otras opciones de planificación.

Time Machine dispone de una utilidad de línea de comandos denominada "`tmutil`", lo cual permite incluir las copias en tareas planificadas. Por ejemplo, la opción "`listbackups`" muestra la lista de *backups* realizados en el sistema.

16.1.1 CONFIGURACIÓN DE OTRO MAC COMO DESTINO DE COPIAS DE SEGURIDAD DE TIME MACHINE

A través de la opción "Preferencias del sistema - Compartir - Compartir archivos" es posible configurar otro ordenador Mac como destino de las copias de seguridad. En el menú "Carpetas compartidas" se dará de alta la carpeta del Mac compartida para este propósito y, mediante el menú "Opciones avanzadas" disponible al pinchar sobre ella con el botón derecho, se seleccionará la opción "Compartir como destino de la copia de seguridad de Time Machine". La compartición debe incluir SMB como protocolo:

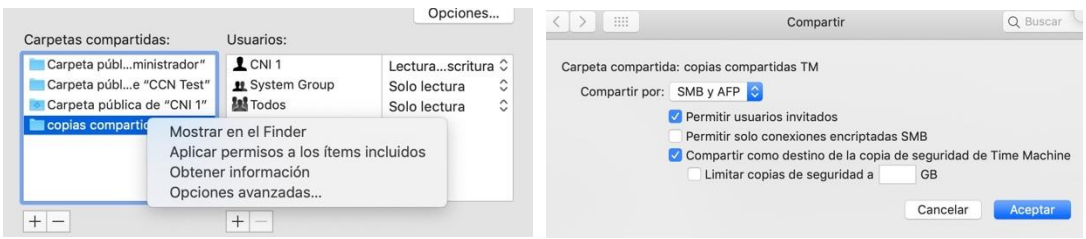


Figura 238 - Configuración de un Mac como destino de copias de Time Machine

En el Mac que será origen de las copias, se deberá:

- Mapear desde el Finder el equipo destino de las copias mediante SMB (`smb://<equipo_destino_de_las_copias>`). Desde ese momento, el equipo remoto aparecerá en la sección "Ubicaciones" del Mac origen.
- Acceder desde el Finder a "Ubicaciones" y al recurso compartido del Mac remoto.
- Entrar en las opciones de TM y, desde el menú "Seleccionar disco", elegir el recurso compartido.

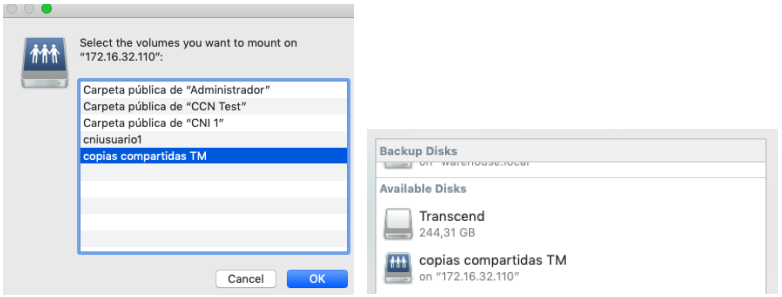


Figura 239 - Uso de un Mac accesible por la red como destino de las copias de TM

16.2 COPIA DE SEGURIDAD EN LA NUBE

El proceso de *backup* en la nube permite realizar las copias de seguridad en la nube de Apple, empleando las capacidades de almacenamiento de iCloud Drive. En la actualidad, Apple proporciona 5GB de espacio de almacenamiento gratuito en iCloud, pudiendo ampliarse dicha capacidad mediante varias opciones de pago.

El análisis de este tipo de *backup* queda fuera del alcance de la presente guía, y será analizado en la "Guía CCN-STIC-459 - Cuenta de usuario, servicios y aplicaciones de Apple" [Ref.- 404].

Es posible verificar qué información está siendo sincronizada o copiada en la cuenta de iCloud del usuario desde "Preferencias del Sistema - iCloud" y comprobando las categorías habilitadas en el panel de la derecha.

Las copias de seguridad de iCloud no deben confundirse con el servicio de iCloud Drive, un servicio de almacenamiento de ficheros y documentos "en la nube", integrado en el sistema operativo, en el que las aplicaciones pueden guardar los documentos de la misma manera que se almacenan en el disco duro local.

Desde el punto de vista de seguridad, ***se recomienda evitar el uso de servicios de terceros para tareas críticas asociadas a la seguridad***, por lo que ***se desaconseja hacer uso de las capacidades de sincronización, copias de seguridad (o backups)*** y/o almacenamiento de información, datos y ficheros ***de iCloud***.

16.3 CREACIÓN DE UN INSTALADOR DE ARRANQUE EN UNA UNIDAD USB O UN DISCO EXTERNO

La creación de un disco externo que actúe como instalador de arranque permite restaurar en el equipo la versión de fábrica de macOS existente en el ordenador, pero que conservará el Apple ID vigente en el equipo. Los pasos a seguir son [Ref.- 33]:

1. Descargar el paquete de instalación de macOS Mojave en un equipo que disponga de macOS Sierra 10.12.5 o posterior, o El Capitán 10.11.6.
2. Formatear la unidad USB o el disco externo seleccionándolo en la app "Utilidad de Discos", pestaña "Borrar", y eligiendo el formato "Mac OS Plus (con registro)". Será necesario confirmar la operación mediante la opción "Borrar".
3. Lanzar el comando "`createinstallmedia`" desde una ventana de terminal (se solicitará la contraseña del usuario autorizado para invocar el comando mediante la utilidad "`sudo`"):

```
$ sudo /Applications/Install\ macOS\
Mojave.app/Contents/Resources/createinstallmedia --volume /Volumes/<Nombre
dado a la unidad durante la operación de formateo>
Password:
Ready to start.
To continue we need to erase the volume at /Volumes/USB_arranque.
If you wish to continue type (Y) then press return: Y
Erasing disk: 0%... 10%... 20%... 30%... 40%... 50%... 60%... 70%... 80%...
90%... 100%
Making disk bootable…
Copying boot files…
Install media now available at "/Volumes/Instalar macOS Mojave"[65]
```

Figura 240 - Comando para crear un instalador de arranque

La creación de un instalador de arranque es recomendable tras haberse completado la actualización/instalación de macOS, pues permite reinstalar el sistema en caso de fallo irreversible en el disco de sistema sin necesidad de disponer de conexión a Internet.

16.4 RESTAURACIÓN

Al igual que para el proceso de realización de copias de seguridad, se distinguen dos tipos de restauración:

- De datos de usuario.
- De sistema: para reemplazar la actual imagen de macOS con otra diferente.

16.4.1 RESTAURACIÓN DE DATOS DE USUARIO MEDIANTE TIME MACHINE

Este tipo de restauración está condicionado por el mecanismo utilizado para las copias de seguridad. El presente apartado describe la restauración de datos salvados mediante la utilidad Time Machine.

[65] El volumen será renombrado, y tendrá el mismo nombre que el instalador utilizado para la creación.

Para proceder a la restauración, se seleccionará el menú de Time Machine disponible en la barra de menús de estado o, en su defecto, lanzando la app Time Machine desde el Launcher.

NOTA: queda fuera del alcance de la presente guía la restauración de copias de seguridad realizadas mediante iCloud, que se abordará en la "Guía CCN-STIC-459 - Cuenta de usuario, servicios y aplicaciones de Apple" [Ref.- 404].

El interfaz de Time Machine ofrece un interfaz tipo Finder desde el que se puede navegar hasta el elemento concreto. En la sección de la derecha, se dispone de una barra temporal, por la que el usuario se puede desplazar hasta llegar a la fecha con la copia desde la que se desea restaurar. Si TM detecta que ya existe un elemento con igual nombre en la misma ubicación, solicitará confirmación sobre si conservar (opción recomendada) o no el fichero original o actual.

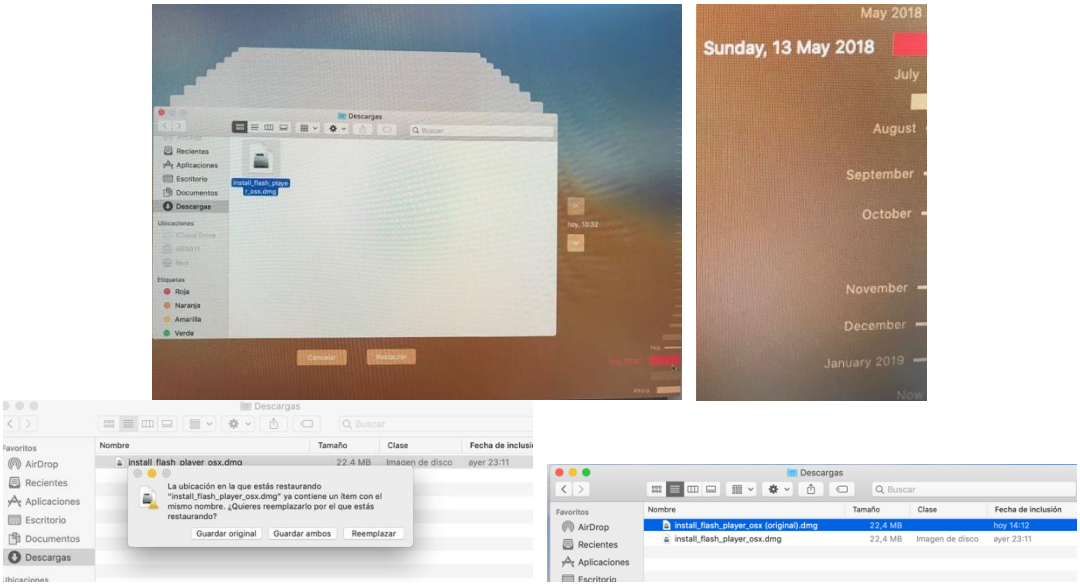


Figura 241 - Restauración de datos de usuario desde Time Machine

16.4.2 RESTAURACIÓN DE SISTEMA

Para restaurar el volumen de sistema desde una copia realizada por el usuario mediante Time Machine, es preciso arrancar en modo de recuperación, según se describe en el apartado "18.2. Modo "Recuperación" (Recovery)", y seleccionar la opción "Restaurar desde una copia de seguridad de Time Machine". El proceso es completamente guiado, por lo que el usuario únicamente debe seleccionar la imagen correcta.

Si la copia de seguridad se realizó sobre un disco cifrado, se solicitará la correspondiente contraseña. También se requerirá la introducción de las credenciales de un usuario (no necesariamente con perfil de administrador) que pueda descifrar el disco de destino (en caso de que este disco se encuentre también cifrado con FileVault, que es lo recomendado), es decir, que forme parte de la cadena de *Secure Token*.

Este proceso de restauración elimina todos los datos existentes en el disco de destino, por lo que se debe llevar a cabo minuciosamente.

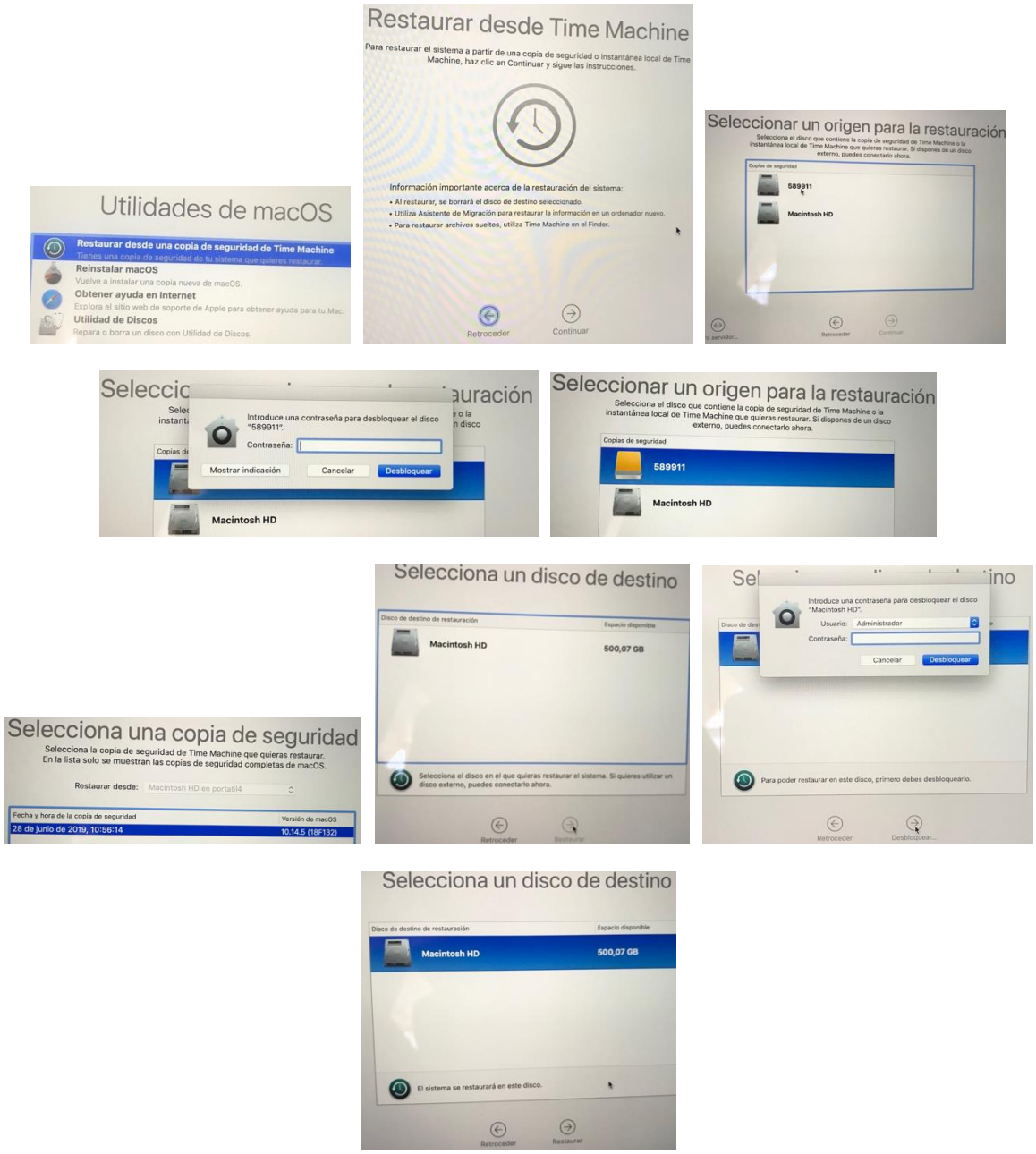


Figura 242 - Proceso de restauración de un volumen de sistema mediante Time Machine

Complementariamente a la restauración desde Time Machine, se puede reinstalar macOS desde el menú de recuperación, tal como se describe en el apartado "5.3. Reinstalación de macOS".

17.ELIMINACIÓN DE LOS DATOS DEL ORDENADOR

Para eliminar completamente todos los datos residentes en un disco hay que llevar a cabo una operación de formateo.

Si el motivo de la eliminación de los datos es que el equipo va a cambiar de usuario, se aconseja llevar a cabo previamente el proceso descrito en el apartado "17.3. Acciones de borrado por cambio de usuario".

IMPORTANTE: antes de proceder a eliminar los datos, se recomienda realizar una copia de seguridad completa que garantice poder recuperarlos en caso necesario (ver apartado "16. Copias de seguridad y restauración"), ya que este proceso es irreversible.

17.1 BORRADO DEL DISCO DE SISTEMA

El formateo del disco en el que reside la imagen del sistema operativo equivale a eliminar todos los datos de usuario y sistema, incluyendo:

- El Apple ID y cualquier otra cuenta de usuario que hubiese sido dada de alta.
- La configuración y datos de las apps y del sistema.
- Las apps de terceros descargadas e instaladas.

Esto permite restaurar el ordenador a los ajustes de fábrica (especialmente necesario de cara a transferir el equipo a otro usuario), y requiere reiniciar el equipo en modo Recuperación (ver apartado "18.2. Modo "Recuperación" (Recovery)") y seleccionar "Utilidad de Discos" en la ventana del menú "Utilidades de macOS".

Una vez dentro de "Utilidad de Discos", se debe:

1. Marcar la unidad en la barra lateral izquierda (el nombre por defecto del disco de sistema es "Macintosh HD").
2. Seleccionar la pestaña "Borrar".
3. Proporcionar el nombre deseado al disco (puede ser el mismo que tuviera) y elegir "APFS" en el campo "Formato". En caso de que se vaya a reinstalar Mojave en este disco, aunque se seleccionase "Mac OS Plus (con registro)", el proceso de instalación procedería a reformatearlo como "APFS".
4. Confirmar la operación mediante el botón "Borrar".
5. Al finalizar el borrado, cerrar el menú "Utilidad de Discos" y, si procede, instalar de nuevo el sistema operativo o restaurar una copia de seguridad a través de las opciones de "Utilidades de macOS".

17.2 BORRADO DE UN DISCO DIFERENTE AL DE ARRANQUE

La eliminación de datos de un disco diferente al de arranque también se lleva a cabo mediante la aplicación "Utilidad de Discos". La pestaña "Borrar" permitirá seleccionar el disco o volumen a borrar desde la barra lateral, y, una vez elegido, mostrará las opciones para el formateo:

- "Nombre": se usará para su identificación dentro del equipo.
- "Formato": solo mostrará los formatos compatibles. Se recomienda la selección de APFS si está disponible.
- "Esquema": opcional.

17.3 ACCIONES DE BORRADO POR CAMBIO DE USUARIO

Aunque el formateo del disco de sistema elimina del mismo las cuentas de usuario y el vínculo con el Apple ID, cuando el equipo va a ser traspasado a otra persona se recomienda realizar una serie de acciones previas al borrado del disco. En

la [Ref.- 115] se dispone del documento oficial de Apple con todos los detalles. Adicionalmente, de cara a evitar inconsistencias relativas a la gestión remota de los servicios existentes en el dispositivo, se recomienda:

- Eliminar el dispositivo del servicio "Buscar mi Mac" de iCloud: para ello, se recomienda desconectar temporalmente el equipo de su conexión a Internet y acceder a "https://icloud.com#find". Una vez seleccionado el dispositivo, pinchar en el símbolo "X" (ver <Figura 158>).
- Eliminar todas las cuentas dadas de alta en el ordenador a través del menú "Preferencias del sistema - Cuentas de Internet - "–"".
- Verificar que no quedan ajustes en NVRAM asociados a la funcionalidad "Buscar mi Mac" (ver apartado "11.3. Buscar mi Mac (Find my Mac)"): para ello, se debe ejecutar el comando "`nvram -p -x | grep -i fmm`". Si la salida no es vacía, eliminar las variables que aparezcan mediante el comando "`nvram -d <variable>`" (ver ejemplo de la <Figura 243>):

```
$ nvram -p -x | grep -i fmm
fmm-mobileme-token-FMM bplist0 ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ
fmm-mobileme-token-FMM-BridgeHasAccount   BridgeHasAccountValue
fmm-computer-name                        portatil 4

$ sudo nvram -d fmm-computer-name
$ sudo nvram -d fmm-mobileme-token-FMM
$ sudo nvram -d fmm-mobileme-token-FMM-BridgeHasAccount
```

Figura 243 - Comprobación de las variables asociadas a "Buscar mi Mac" en NVRAM

18.MODOS DE ARRANQUE DE MACOS 10.14 MOJAVE

La EFI (*Extensible Firmware Interface*) es un estándar cuyo propósito es ofrecer el interfaz entre el *firmware* y el sistema operativo, que surgió como alternativa a la BIOS de los chips Intel. Proporciona servicios tanto al gestor de arranque como al sistema operativo, y en los equipos Mac reside en una partición independiente. Uno de los componentes de la EFI es la tabla de particiones GUID (GPT, *GUID Partition Table*), que reemplaza al MBR (*Master Boot Record*) utilizado por las BIOS.

macOS proporciona diferentes opciones de arranque para los equipos Mac basados en plataforma Intel, determinadas por las *snag-keys* o *startup keys* (teclas que el usuario pulsa para condicionar el modo de arranque deseado).

El proceso de arranque se detalla en el apartado "20. Anexo A. Proceso de arranque de macOS".

Cada modo de arranque lleva asociada una funcionalidad específica, junto a sus herramientas necesarias. Los modos existentes a fecha de elaboración de la presente guía se describen en la [Ref.- 5], y, como se indica en la misma, están influenciados por la existencia de una contraseña de *firmware* (ver apartado "18.1. Contraseña de firmware"):

- **Recuperación de macOS** (ver apartado "18.2. Modo "Recuperación" (Recovery)").

- **Gestor de arranque**: permite seleccionar el disco o volumen desde el que se iniciará el sistema (ver apartado "18.3. Gestor de arranque").
- **Modo seguro**: (ver apartado "18.4. Modo seguro").
- "**Apple hardware test**": realiza un diagnóstico a nivel del hardware del equipo (se lanza pulsando la tecla "D" durante el arranque del ordenador), que presenta un informe de los elementos que no han pasado la comprobación y permite arrancar en modo de recuperación, desde el que se lanza por defecto el navegador web Safari con las opciones necesarias para solicitar soporte técnico a Apple *on-line*.
- **Modo de restablecimiento de la NVRAM**: ver apartado "18.5. Modo de restablecimiento de la NVRAM".
- **Modo "Disco de destino"**: ver apartado "18.6. Modo "Target Disk".

18.1 CONTRASEÑA DE FIRMWARE

Se recomienda establecer una contraseña de **firmware** para evitar que el ordenador pueda arrancar desde cualquier dispositivo externo o interno diferente al definido como "disco de arranque".

Para ello, el ordenador debe iniciarse en modo de recuperación (ver apartado "18.2. Modo "Recuperación" (Recovery)") y ejecutar "Utilidades - Utilidad de Seguridad de Arranque":

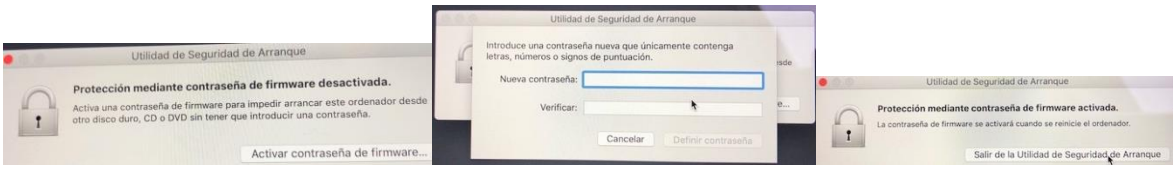


Figura 244 - Establecimiento de una contraseña de firmware

Cuando la contraseña de *firmware* está activa (indicado por el mensaje "Protección mediante contraseña de firmware activada") y se intenta arrancar el equipo en un modo que la requiera, como el modo de recuperación, se solicitará su introducción mediante el menú de la imagen izquierda de la <Figura 245>:

Figura 245 - Introducción de la contraseña de firmware

Para desactivar esta contraseña, se debe nuevamente entrar en el menú de recuperación y elegir la opción "Utilidades - Utilidad de Seguridad de Arranque - Desactivar contraseña de firmware" (se solicitará introducir la contraseña vigente) (ver imagen central y derecha de la <Figura 245>).

NOTA: es importante diferenciar entre la contraseña de *firmware* establecida desde el menú de recuperación y la contraseña de *firmware* de un solo uso que se puede establecer desde el menú "Bloquear mi Mac" disponible como parte del servicio "Buscar mi Mac" (ver apartado "11.1.2. Cuenta de iCloud").

Se recomienda que el valor de la contraseña de** firmware **sea diferente a cualquier otra contraseña utilizada en el equipo, tanto de las cuentas de usuario existentes en macOS, como las cuentas asociadas a los servicios de Apple (Apple IDs).

En la [Ref.- 39] se ofrece un estudio de ingeniería inversa en el que ilustra que la contraseña de *firmware* se almacena en la variable CBF2CC32 de la NVRAM.

18.1.1 UTILIDAD *FIRMWAREPASSWD*

Desde macOS Yosemite, se dispone de la utilidad "`firmwarepasswd`" (bajo "`/usr/sbin`"), que permite gestionar la contraseña de *firmware* desde el sistema operativo, incluyendo el poder establecerla, consultar si existe una vigente, o suprimirla.

Los modos de seguridad del *firmware* disponibles en macOS son:

- "`none`": no se ha establecido una contraseña en el *firmware*.
- "`command`": la contraseña del *firmware* se solicitará en los modos de arranque especiales (modo de seguridad por defecto).
- "`full`": la contraseña del *firmware* se solicitará en todos los modos de arranque, incluyendo el modo de arranque normal. Éste es el modo más restrictivo, pero el más seguro.

```
$ sudo firmwarepasswd -mode
Password:
Mode: none
Option roms allowed

$ 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:
Password Enabled: Yes

$ sudo firmwarepasswd -mode
Mode: command
Option roms not allowed

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

Figura 246 - Establecimiento de la contraseña de firmware mediante la utilidad "firmwarepasswd"

La opción "`-verify`" permite comprobar si la contraseña introducida es la vigente o no. Esta opción (que debe ser ejecutada por un usuario administrador) permite ataques de fuerza bruta, ya que se puede invocar indefinidamente:

```
$ sudo firmwarepasswd -verify
Verifying Firmware Password
Enter password:
Incorrect
ERROR | main | Exiting with error: 4

$ sudo firmwarepasswd -verify
Verifying Firmware Password
Enter password:
Correct
```

Figura 247 - Comando "firmwarepasswd -verify"

Por otra parte, la opción "`unlockseed`" permite obtener el código de 33 caracteres para la eliminación de la contraseña del *firmware* por parte del soporte técnico de Apple en caso de olvido de dicha contraseña (ver apartado "18.1.2. Eliminación de la contraseña del firmware por parte de Apple"). Los 17 primeros 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 propia contraseña y del modo de seguridad. Estos 16 caracteres cambian cuando cambia la contraseña de *firmware*, y también (tras reiniciar el equipo) si se modifica el modo de seguridad mediante "`firmwarepasswd -setmode`".

```
$ sudo firmwarepasswd -unlockseed
C027AF...21F9F5
```

Figura 248 - Visualización de la clave de recuperación de la contraseña de firmware

Este código también se obtiene pulsando la combinación de teclas "^ + ⌥ + ⌘ + ⇧ + S" (`Control + Opción + Comando + Cambio + S`) simultáneamente[66] en la pantalla de arranque que solicita la contraseña de *firmware*:

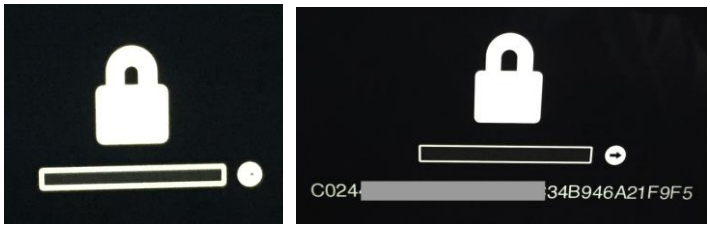


Figura 249 - Obtención de la semilla de desbloqueo durante la solicitud de contraseña de firmware

18.1.2 ELIMINACIÓN DE LA CONTRASEÑA DEL FIRMWARE POR PARTE DE APPLE

No existe ninguna forma soportada para deshabilitar una contraseña de *firmware* olvidada, salvo a través de un servicio técnico autorizado Apple[67], aportando un comprobante de compra del ordenador y la semilla de la contraseña de *firmware* ilustrada en la <Figura 249>.

En base a esta semilla, Apple generará un código de respuesta en forma de fichero (*keyfile*) firmado digitalmente, denominado "SCBO", único para ese equipo y

[66] La pulsación sobre este conjunto de teclas puede iniciarse en cualquier orden, salvo la tecla "S" que debe ser pulsada en último lugar.

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

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.

Aunque históricamente han existido servicios de terceros en Internet que ofrecen este servicio, en la [Ref.- 39] se incluye una investigación en la que se demuestra que, a menos que se disponga de las claves privadas de Apple, no es posible implementar un generador de SCBO. En este estudio, se ilustra que la contraseña de *firmware* se almacena en una variable de la NVRAM, que se pone a cero a través del fichero SCBO firmado por Apple.

18.2 MODO "RECUPERACIÓN" (RECOVERY)

En este modo el sistema arranca desde la partición de recuperación (*Recovery HD*), que es una porción del disco o unidad de almacenamiento con un sistema operativo y unas herramientas de kernel propios. Desde este menú se pueden realizar tareas de diagnóstico y reparación del sistema, y ciertas acciones de configuración de bajo nivel (como habilitar/deshabilitar SIP, ver apartado "9.10. SIP: System Integrity Protection").

El acceso en modo de recuperación requiere reiniciar el equipo a la vez que se pulsan las teclas descritas posteriormente hasta que aparezca el logotipo de Apple®, momento en que se lanza el proceso de arranque de la partición de recuperación, que concluyen con la presentación del menú "Utilidades de macOS". Si el sistema tiene configurada una contraseña de *firmware* (***opción recomendada***), ésta será solicitada para proseguir con el arranque.

La combinación de teclas elegida durante el reinicio condiciona el comportamiento de la opción "Reinstalar macOS":

- "⌘+ R" (`Comando + R`): para recargar la última versión instalada en el sistema.
- "⌥ + ⌘ + R" (`Opción + Comando + R`): para cargar la última versión disponible compatible con el Mac.
- "⇧ + ⌥ + ⌘+ R" (`Cambio + Opción + Comando + R`)": para cargar la versión que el Mac trajese de fábrica, o la última más próxima que esté disponible. Este escenario se utiliza típicamente si se llevó a cabo una actualización de macOS y el sistema presenta problemas de inestabilidad o bajo rendimiento.

Independientemente de la opción de arranque escogida, el resto de opciones del menú "Utilidades de macOS" no varía.

IMPORTANTE: el proceso de reinstalación de macOS mantiene los archivos y ajustes del usuario. Si se desea realizar una instalación desde cero, es preciso reformatear el volumen previamente.

Cuando se arranca de la partición de recuperación, el sistema de ficheros del disco no está accesible por defecto, ya que está encapsulado en una imagen

denominada "`BaseSystem.dmg`"[68]. Sí se comparten los parámetros definidos en la NVRAM.

El modo de arranque de recuperación está asimismo influenciado por el valor de la variable NVRAM "`recovery-boot-mode`" (por defecto, sin asignar). El valor de esta variable se puede fijar a través del comando "`sudo nvram "recovery-boot-mode=<VALOR>"`". Por ejemplo:

- "`recovery-boot-mode=unused`": hará que el equipo se reinicie en modo de recuperación de forma automática[69] la próxima vez que tenga lugar el proceso de rearranque (la variable se restablecerá y quedará sin valor cuando se salga del modo de recuperación):
- "`recovery-boot-mode=locked`": impide que aparezca el menú de recuperación de macOS, de modo que, aunque se pulse cualquiera de las combinaciones de teclas para arranque en modo *Recovery*, la operación no tenga éxito (este mecanismo se usa por parte de la función "Bloquear" de "Buscar mi Mac", ver apartado "11.3. Buscar mi Mac (Find my Mac)").

IMPORTANTE: este valor **no debe fijarse nunca manualmente**, ya que puede llevar el sistema a un estado inconsistente desde el que sea imposible arrancar.

El menú "Utilidades de macOS" ofrece las siguientes opciones:

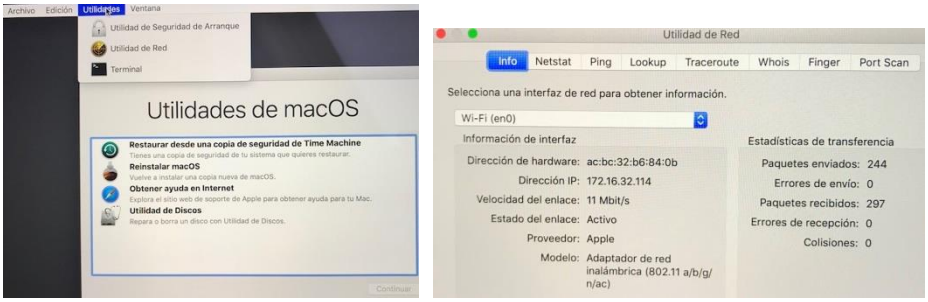


Figura 250 - Utilidades del menú de recuperación de macOS

- **Restaurar desde una copia de seguridad de Time Machine**: ver apartado "16.1. Time Machine".
- **Reinstalar macOS**: permite restaurar la versión de macOS en función del modo de arranque seleccionado. Esta opción no elimina los ajustes correspondientes al Apple ID de la cuenta de iCloud configuradas en el ordenador (ver apartado "11. Servicios de Apple").
- **Obtener ayuda en Internet**: arranca una instancia del navegador web Safari que incluye enlaces al sitio web de soporte técnico de Apple.
- **Utilidad de Discos**: descrita en el apartado "18.2.1. Utilidad de Discos".
- Menú "**Utilidades**": dispone de las opciones:

[68] https://www.ghostlyhaks.com/forum/macbook/65-icloud-wipeout-and-admin-access-on-efi-locked-mac

[69] https://anandmpandit.blogspot.com/2017/09/how-to-boot-into-recovery-mode-on-mac.html

- Terminal: arranca una consola, o terminal, desde la que se pueden ejecutar comandos.
- Utilidad de Seguridad de Arranque: permite establecer una contraseña de *firmware* (ver apartado "18.1. Contraseña de firmware").
- Utilidad de red: incorpora diversas utilidades que pueden utilizarse para identificar problemas de conectividad.

18.2.1 UTILIDAD DE DISCOS

Esta utilidad permite realizar operaciones de diagnóstico, reparación, montado, particionado, formateo y restauración en los discos instalados en el ordenador.

En macOS Mojave no se dispone de la opción "`DUDebugMenuEnabled`" para la "Utilidad de discos" que permitía iniciar dicha app en modo de depuración y obtener detalles de todos los volúmenes existentes en un disco. Sí es posible lanzar el comando "`diskutil list`" desde un terminal en modo de recuperación para este fin:

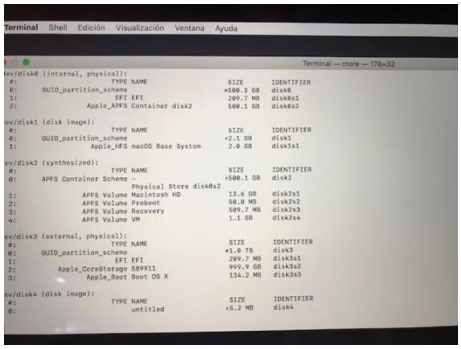


Figura 251 - Salida de "diskutil list" en modo de recuperación

- **Primera ayuda**: escanea el volumen para detectar fallos y, si los encuentra, proceder a repararlos.
- **Crear partición**: el sistema de ficheros APFS (ver apartado "15.5. APFS (Apple File System)") utiliza volúmenes en lugar de particiones, por lo que este menú sugiere su utilización frente a un esquema de particionado tradicional (si bien permite también recurrir a él mediante la opción "Crear particiones siempre").

Para poder montar el volumen asociado al disco de arranque y acceder a él si está cifrado con FileVault, se requerirá introducir las credenciales de un usuario que tenga el *Secure Token* habilitado (ver apartado "15.1.3. Secure Token"). En macOS Mojave ya no se dispone del menú "⌥ + Archivo - Desactivar encriptación" (`Opción + Archivo - Desactivar encriptación`) que permitía deshabilitar FileVault en el disco de arranque.

18.2.2 MENÚ "DISCO DE ARRANQUE"

Desde el menú "" del modo de recuperación es posible establecer el arranque desde otro volumen de sistema conectado al Mac.

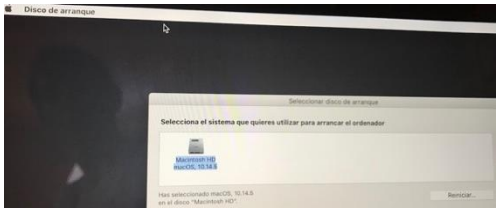


Figura 252 - Utilidad "Disco de arranque" del modo de recuperación

18.3 GESTOR DE ARRANQUE

Para iniciar el ordenador desde un instalador de arranque contenido en una unidad USB, debe reiniciarse el equipo y pulsar la tecla "⌥" (`Opción`) hasta que se muestren el selector de volúmenes de arranque. Si existe una contraseña de *firmware* vigente, será necesario introducirla.

Una vez identificada la unidad, pulsar sobre el botón "⇧" (`Cambio`).

18.4 MODO SEGURO

Accesible desde la tecla "⇧" (`mayúsculas`), este modo se utiliza en caso de que el ordenador no pueda iniciarse desde el disco de arranque. En este modo únicamente se cargan determinadas extensiones del kernel [Ref.- 36].

Cuando se arranca en este modo, la ventana de inicio de sesión (*login*) del ordenador mostrará en su esquina superior izquierda el texto "Safe Boot". Una vez iniciado, la opción "" - Acerca de este Mac - Informe del sistema - [Software] Modo de arranque" también permite ver si se el equipo se ha iniciado en este modo.

Información del software de sistema:	
Versión del sistema:	macOS 10.14.4 (18E226)
Versión del kernel:	Darwin 18.5.0
Volumen de arranque:	Macintosh HD
Modo de arranque:	**Seguro**
Nombre del ordenador:	MacBook Pro de Administrador
Nombre de usuario:	Administrador (admin)
Memoria virtual segura:	Activado
Protección de la integridad del sistema:	Activado
Tiempo desde el arranque:	2 minutos

Figura 253 - Arranque en modo seguro

NOTA: en la página oficial de Apple [Ref.- 36] se indica que, para el caso de los equipos que no disponen de un teclado, el modo de arranque seguro puede iniciarse mediante una conexión remota por SSH desde otro equipo y ejecutando el comando "`sudo nvram boot-args="-x"`". Sin embargo, durante las pruebas realizadas durante la elaboración de la presente guía, se ha constatado que este comando "`nvram`" falla en Mojave con el error "`nvram: Error setting`

`variable - 'boot-args': (iokit/common) not permitted`", siendo posible ejecutarlo solo en modo de arranque de recuperación.

18.5 MODO DE RESTABLECIMIENTO DE LA NVRAM

Para restablecer la NVRAM, descrita a continuación, se debe pulsar "⌥ + ⌘ + P + R" (`Opción + Comando + P + R`) durante unos 20 segundos y soltar dichas teclas después de escuchar dos veces el sonido de arranque.

IMPORTANTE: este modo no puede invocarse si existe una contraseña de *firmware* (***opción recomendada desde el punto de vista de seguridad***) vigente en el equipo, por lo que, si se requiere invocarlo, habrá que proceder a desactivar dicha contraseña previamente.

Entre las situaciones que pueden requerir restablecer la NVRAM está que el equipo se esté iniciando desde un disco diferente al seleccionado como disco de arranque.

18.5.1 NVRAM

La NVRAM (*Non-Volatile Random Access Memory*, o memoria de acceso aleatorio no volátil) es una pequeña memoria del ordenador que almacena algunos ajustes de configuración de macOS que deben persistir entre reinicios [Ref.- 37], incluida la contraseña de *firmware*, si ésta se ha configurado [Ref.- 39].

Los ajustes de configuración almacenados en la NVRAM dependen del modelo de ordenador Mac utilizado, del *firmware* EFI y de los dispositivos o periféricos conectados. Durante el arranque, tanto el gestor de arranque como varios *drivers* consultan las variables de la NVRAM para determinar cómo inicializar los distintos componentes del sistema.

El formato de una variable NVRAM (seguido de un ejemplo)[70] es:

```
GUID (Globally Unique Identifier) del propietario de la variable + nombre + valor

8BE4DF61-93CA-11D2-AA0D-00E098032B8C (EFI) + BootOrder + <entero de 16 bits>
```

Entre otros ajustes, la NVRAM mantiene la selección del disco de arranque (impidiendo así que el disco de arranque se fije de manera programática), la zona horaria, el estado de activación de la localización o el volumen del equipo. El comando "`nvram -p`" informa de los ajustes vigentes de la NVRAM[71] [72]:

```
$ nvram -p
bluetoothInternalControllerInfo %90%82%ac%05%00%000%14%ac%bc2%b6%84%0c
fmm-computer-name    portatil2
bluetoothActiveControllerInfo  %90%82%ac%05%00%00%00%000%14%ac%bc2%b6%84%0c
SystemAudioVolumeDB  %f4
ALS_Data   ^%0d%8a%8a%00%00%00%00
SystemAudioVolume    _
LocationServicesEnabled   %01
```

[70] https://wikileaks.org/ciav7p1/cms/page_26968084.html

[71] https://eclecticlight.co/2018/08/24/whats-stored-in-nvram/

[72] https://eclecticlight.co/2017/09/19/self-starting-macs-startup-chimes-and-other-secrets-of-nvram/

```
csr-active-config    %10%00%00%00
backlight-level i%05
BootCampProcessorPstates   %0c%00
```

Figura 254 - Salida del comando "nvram -p"

Estos valores también están disponibles en el menú "🍎 - Acerca de este Mac - [Visión general] - Informe del sistema - [Software] Registros - Contenido de NVRAM".

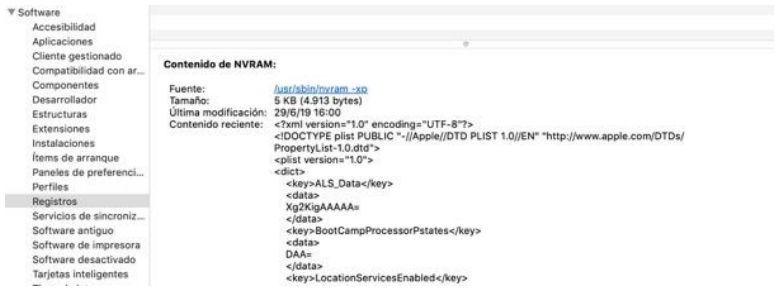


Figura 255 - Información de parámetros NVRAM desde la app "Informe del sistema"

Tras el arranque del sistema, los ajustes de los parámetros NVRAM se cargan en la memoria principal. Cuando se invoca un reinicio o apagado del equipo de forma ortodoxa, los ajustes presentes en memoria se vuelcan a la NVRAM.

18.6 MODO "TARGET DISK"

Este modo, accesible pulsando la tecla de encendido seguida de la tecla "T" durante el arranque en el ordenador destino, permite conectar dos ordenadores Mac a través de los puertos definidos en la [Ref.- 38], lo cual tiene utilidad para:

- Transferir archivos entre los equipos.
- Realizar un proceso de migración a un nuevo equipo Mac mediante el "Asistente de migración de macOS".
- Acceder a los discos del equipo que se haya indicado como "Modalidad de disco de destino" (*target*) desde el otro equipo (denominado *host*). Esto permite resolver problemas si un equipo no arranca de forma correcta.

Alternativamente, es posible establecer esta modalidad para el disco de arranque mediante el menú "🍎 - Preferencias del Sistema - Disco de arranque - [Selección del disco] - Modalidad de disco de destino" (previamente se habrá desbloqueado el menú pulsando en el candado e introduciendo la contraseña de administrador).

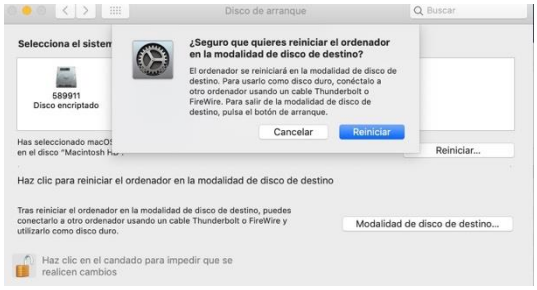


Figura 256 - Modo de arranque "Target Disk"

Desde el menú del Finder del equipo *host* se dispondrá de acceso al disco de destino (*target*), permitiéndose:

- Operaciones de copia, borrado, etc. hasta que se expulse la unidad (pinchando sobre ella con el botón derecho) o arrastrándola a la papelera.
  El Mac actuando como *target* no estará disponible para interactuar con él mientras dure esta conexión.
- Ejecutar en el *host* el sistema operativo del destino: reiniciando el *host* con la tecla "⌥" (`Opción`) pulsada, que mostrará el menú "Administrador de inicio", desde el que se puede seleccionar como unidad de arranque el disco de destino.

En cualquiera de los dos casos, si el disco de destino está cifrado con FileVault (opción recomendada), el sistema solicitará las credenciales de un usuario que tenga activo el Secure Token (ver apartado "15.1.3. Secure Token").

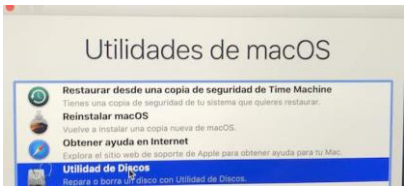
18.7 MODO MONOUSUARIO

El modo monousuario (*single user mode*, o SUM, o modo de un solo usuario) es un modo especial de arranque en el que "`launchd`" no establece una sesión gráfica, aunque sí arranca demonios del sistema, como se puede comprobar a través del comando "`launchctl list`". En versiones anteriores de macOS, este modo se iniciaba pulsando "⌘ + S" (`Comando + S`) durante el arranque, pero en los equipos actuales el procedimiento a seguir para arrancar en este modo es el descrito en la [Ref.- 13], que requiere iniciar el sistema desde el menú de recuperación.

- Si se está usando una contraseña de *firmware* (opción recomendada desde el punto de vista de seguridad), el usuario deberá introducirla.
- Si el disco está cifrado con FileVault (ver apartado "15.1. FileVault"), opción recomendada desde el punto de vista de seguridad, será necesario introducir las credenciales de un usuario activo en el sistema (no necesariamente con permisos de administración) para poder descifrar los contenidos del disco.

El terminal que se obtiene al arrancar en este modo tiene el *prompt* "`bash-3.2#`" en macOS Mojave, y privilegios de administrador.

La partición "`/`" se montará en modo lectura, por lo que, si se precisase modificar alguno de sus contenidos, sería necesario remontarla en modo escritura mediante los comandos: "`/sbin/fsck -fy`" seguido de "`/sbin/mount -uw /`".



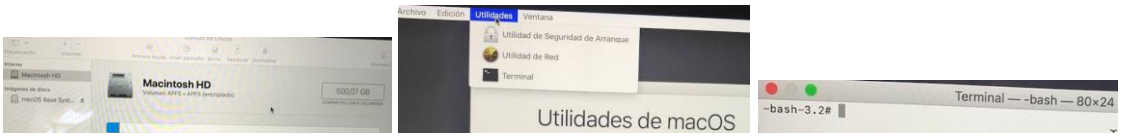


Figura 257 - Arranque en "modo monousuario"

En versiones anteriores de macOS, el procedimiento de arranque en modo monousuario se llevaba a cabo para modificar contraseñas de usuarios, incluido el administrador, en caso de olvido. Sin embargo, en Mojave este método, basado en la utilidad "`dscl`", ya no está vigente, y falla con el error "`<dscl_cmd> DS Error: -14009 (eDSUnknownNodeName)`".

Tampoco sigue vigente en Mojave el método de creación de un usuario administrador basado en borrar el fichero "`/var/db/.AppleSetupDone`". La existencia de este fichero en versiones anteriores hacía creer al sistema operativo que debía llevarse a cabo un proceso de instalación inicial, durante el cual se permitía dar de alta una nueva cuenta de administrador.

Si FileVault está activado, la utilidad "`resetpassword`", invocada desde el terminal del modo de recuperación, arranca el asistente para restablecer la contraseña, tal como se describe en la [Ref.- 6].

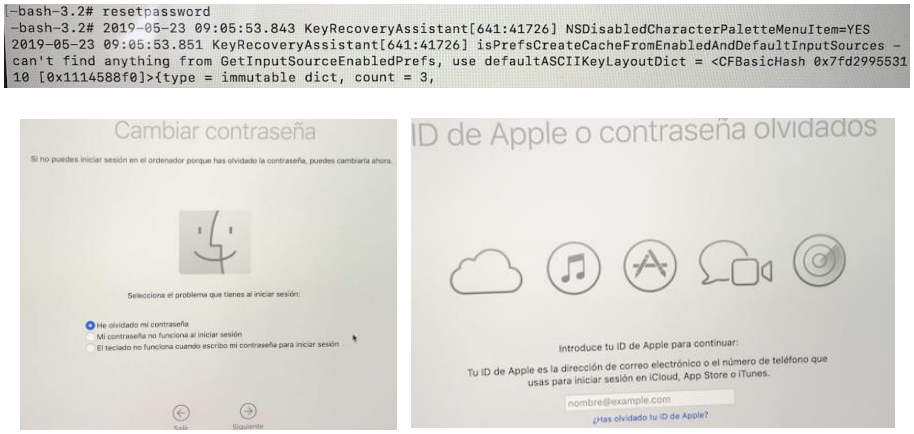


Figura 258 - Utilidad "resetpassword"

Para salir del modo monousuario es suficiente con rearrancar el equipo mediante el comando "`reboot`". En versiones anteriores de macOS, el modo monousuario llevaba implícito el arranque en modo detallado (ver apartado "18.8. Modo detallado"), pero ya no es así en Mojave. Si se sale del terminal mediante el comando "`exit`", el equipo volverá al menú de Recuperación.

Desde el modo de monousuario solo ciertos comandos están disponibles: el contenido de los directorios "`/usr/bin`" y "`/usr/sbin`" es muy limitado, por lo que no todas las tareas de administración pueden realizarse.

18.8 MODO DETALLADO

El modo de arranque detallado ("*Verbose mode*") [Ref.- 13] proporciona detalles sobre los diferentes pasos y acciones llevadas a cabo por macOS durante el proceso de arranque, mostrando los mensajes de los diferentes subsistemas y servicios que están siendo arrancados. Este modo, que se inicia pulsando "⌘ + V" (`Comando + V`), puede ser empleado en modo de arranque normal, en modo seguro y en modo de monousuario, pero no si se está usando una contraseña de *firmware* (ver apartado "18.1. Contraseña de firmware") por lo que, de ser así, habrá que desactivarla previamente.

Al salir de una sesión en modo detallado, también se mostrará una pantalla con la información asociada al proceso de cierre.

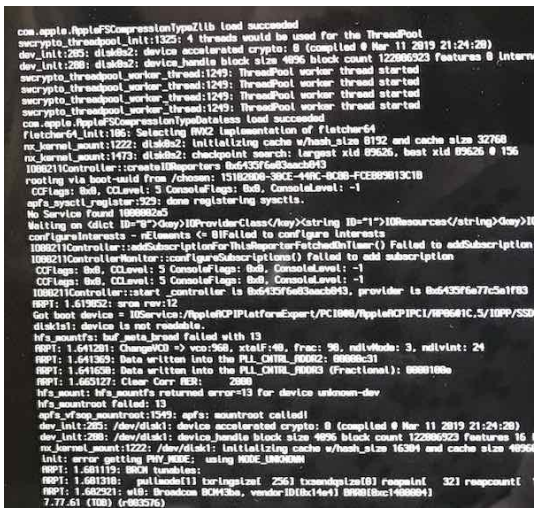


Figura 259 - Arranque en "modo detallado"

18.9 SECURE BOOT PARA CHIP T2

Los equipos Mac equipados con el chip T2 [Ref.- 42] disponen de la funcionalidad "*Secure Boot*", encargada de comprobar la firma criptográfica de todos los componentes del proceso de arranque de macOS. Cada componente verificado entra en la cadena de confianza cuyo anclaje está en la ROM de arranque (*Boot*ROM), que contiene la clave pública de la CA de Apple empleada para establecer la cadena de confianza (ver página 8 de la [Ref.- 43] y la sección "*Startup Security Utility*" de la [Ref.- 4]).

Secure Boot también protege los modos de arranque de recuperación (*Recovery*), de diagnóstico y de recuperación desde Internet.

Secure Boot permite alterar la política de verificación, incluyendo deshabilitarla por completo, a través de la "Utilidad de seguridad de arranque" ("*Startup Security Utility*") disponible en el modo de arranque de recuperación.

Desde el punto de vista de seguridad, ***se recomienda mantener el Secure Boot en modo "Full Security"***.

19.RESUMEN DE LAS RECOMENDACIONES DE SEGURIDAD DE MACOS 10.14

	Decálogo Básico de Seguridad
1	Establecer una política de inicio de sesión que minimice el riesgo de acceso no autorizado al sistema, empleando políticas de creación de contraseñas robustas y controlando los perfiles de usuario existentes en el equipo y sus opciones de inicio de sesión. Las credenciales de acceso deben solicitarse inmediatamente tras apagarse la pantalla de forma automática, lo cual debe suceder a la mayor brevedad posible si el usuario deja de interactuar con el equipo.
2	Comprobar el estado de cifrado del volumen de arranque y, en caso de no encontrarse cifrado, proceder a cifrarlo mediante FileVault.
3	Mantener la versión de macOS actualizada, así como la versión de todas las apps, preferiblemente de forma manual, y realizando previamente una copia de seguridad antes de la actualización. La copia de seguridad debe realizarse sobre una unidad de almacenamiento cifrada, y, preferiblemente, a través de Time Machine en un soporte físico (frente al uso de iCloud).
4	Evaluar la utilización del llavero como gestor de contraseñas, tratando de no incluir en él las contraseñas más sensibles y críticas, junto a las capacidades de autorrellenar contraseñas y códigos de seguridad de Safari, y al servicio de comprobación de reutilización de contraseñas.
5	Configurar el segundo factor de autentificación (2FA) en la cuenta de usuario de iCloud asociada al ID de Apple vinculado al equipo. Evitar que la dirección de correo electrónico del Apple ID sea similar al nombre de usuario de sistema operativo, a fin de minimizar la relación que un posible atacante pueda inferir del uno conociendo el otro.
6	Evitar en lo posible el uso de servicios que impliquen envío de información a Apple, como Siri y Spotlight. Analizar las necesidades de uso de las comunicaciones propietarias de Apple y sus opciones de configuración para evitar exponer elementos del sistema (como el interfaz Wi-Fi y/o Bluetooth) de forma innecesaria.
7	Evitar el uso de servicios compartidos (descritos en la sección "10.1. Servicios compartidos"), especialmente los de carácter menos seguro. En caso de ser necesarios de forma puntual, proceder a desactivarlos una vez finalice el motivo para su uso
8	Configurar adecuadamente el cortafuegos de macOS, de forma que bloquee todas las conexiones innecesarias para el correcto funcionamiento del equipo.
9	Revisar los elementos de la sección "Privacidad", concretamente los asociados a la funcionalidad "TCC: Transparency, Consent and Control", y establecer las máximas restricciones posibles, especialmente para los elementos más críticos.
10	Inhabilitar los demonios y agentes que no se requieran para la correcta operativa del equipo. Dado que la inhabilitación de demonios requiere deshabilitar SIP, se debe recordar proceder a reactivar SIP tan pronto se haya completado la operación.

20.ANEXO A. PROCESO DE ARRANQUE DE MACOS

A continuación se proporciona una breve y simplificada introducción al proceso de arranque de los ordenadores Mac y del sistema operativo macOS.

La última documentación sobre el proceso de arranque inicial (denominado *Early Boot Process*) publicada oficialmente por Apple en la [Ref.- 40] data de 2013, por lo que existe cierta incertidumbre sobre la vigencia y exactitud de parte de dicha información; para usuarios interesados en la materia, se recomienda la lectura de la [Ref.- 128], de 2018. En dicha referencia se proporciona el siguiente diagrama, que incorpora los pasos de arranque (incluso para ordenadores Mac equipados con chip T2, correspondiente a las burbujas rodeadas por una línea negra más intensa):

- A la izquierda (en color verde) se muestran las fases en las que hay interacción por parte del usuario.
- A la derecha (en color morado) se referencia al estado de la pantalla que corresponde a cada fase.
- En rosa se muestra las fases llevadas a cabo por los componentes del sistema de arranque.
- En azul se señalan acciones adicionales que pueden resultar de las salidas de las distintas fases.

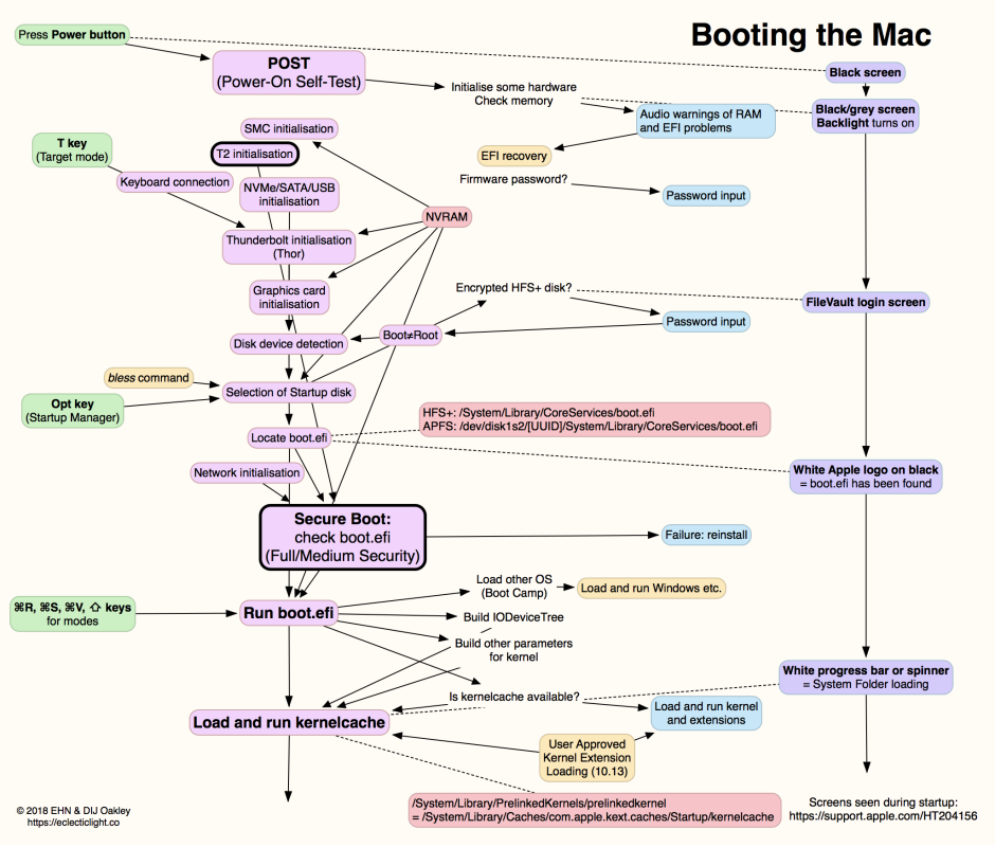


Figura 260 - Diagrama del proceso de arranque de macOS.
© 2018 EHN & DU Oakley. https://eclecticlight.com.

1. Al encender un equipo Mac, la BootROM del *firmware* se activa y realiza dos tareas:

   - Inicializa algunos componentes *hardware* (como la memoria) y verifica su estado a través del POST (*Power-On Self Test*). En los Mac basados en Intel anteriores a 2016 la salida de esta fase se indicaba con una señal acústica, que varía según el resultado del POST (la salida normal es un sonido único que dura alrededor de un segundo). El resultado del POST está disponible en el menú "" - Acerca de este Mac - [Visión general] - Informe del sistema", en la sección "Hardware - Diagnóstico":

Figura 261 - Informe de resultados del Power-On Self Test

   - Inicializa otros componentes *hardware* (como el SMC - *System Management Controller*, los *chipset* Bluetooth, Wi-Fi y de gráficos, y el chip T2 para aquellos equipos que disponen de él), y selecciona el sistema operativo a arrancar del volumen especificado como disco de arranque predeterminado en la EFI.

2. Una vez el BootROM finaliza sus tareas y selecciona el sistema operativo a arrancar, pasa el control al *boot loader* (en equipos sin chip T2, residente en "`/System/Library/CoreServices/boot.efi`"[73]) cuyo principal objetivo es cargar el entorno de ejecución del *kernel*. En equipos equipados con chip T2, tiene lugar el proceso explicado en el apartado "18.9. Secure Boot para chip T2". El gestor de arranque se conoce como "OS X *Booter*".

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

   Las acciones de arranque del *boot loader* son dependientes de ciertas variables definidas en la NVRAM, y también de las *snag-keys* o *startup keys* (teclas que el usuario haya pulsado para condicionar el tipo de arranque deseado - ver apartado "18. Modos de arranque de macOS 10.14 Mojave"). En el pasado, el fichero "`/Library/Preferences/SystemConfiguration/com.apple.Boot.plist`" albergaba los parámetros de "`boot.efi`", pero en la actualidad, aunque sigue existiendo por compatibilidad hacia atrás, apenas tiene contenido.

[73] En versiones antiguas de macOS la EFI residía en la BootROM, pero en los equipos más modernos se ubica en disco.

El "`boot.efi`" elabora el árbol de dispositivos (`IODeviceTree`), que incorpora todos los dispositivos disponibles en el ordenador Mac (este árbol se puede consultar en la salida del comando "`ioreg`"), que conforma el IOKit.

3. Tras los pasos 1 y 2, y la ejecución de "`boot.efi`", el sistema está preparado para ejecutar el *kernel*[74] y sus extensiones. En base a ellos, y para agilizar el arranque, macOS construye una versión pre-enlazada (*prelinked*) que almacena en una caché del kernel (*kernelcache*), bajo "`/System/Library/PrelinkedKernels/prelinkedkernel`" (a la que apunta "`/System/Library/Caches/com.apple.kext.caches/Startup/kernelcache`").
4. Si no es posible utilizar esta caché, el *boot loader* buscará en "`/System/Library/Extensions/*.kext`" y en "`/Library/Extensions/*.kext`" las extensiones de *kernel* a cargar según el tipo de arranque; este proceso, más lento que el de la caché, consulta los ficheros "`./Contents/Info.plist`" de cada extensión y ejecuta el *linker* (enlazador).
5. Una vez cargado el *kernel* y todas las extensiones necesarias para el arranque, el *boot loader* ejecutará el procedimiento de inicialización del *kernel*, que se localiza en la partición raíz, y se inicializa el IOKit, encargado de enlazar los drivers de los diferentes componentes *hardware* en el *kernel*.
6. A partir de ese momento, el *kernel* arranca el sistema operativo macOS (basado en FreeBSD) desde el disco de arranque, e invoca "`launchd`", el primer proceso que es ejecutado en el sistema.
7. "`launchd`" inicializa el sistema, se encarga de ejecutar los servicios de sistema[75] y establece parte del entorno de usuario. "`launchd`" también tiene la capacidad de ejecutar servicios bajo demanda, desactivarlos en periodos de inactividad, y activarlos de nuevo cuando sea necesario.
8. Por último, "`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.

En base al proceso de arranque, se evidencia que 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. Por tanto, ***se recomienda analizar el contenido de los directorios donde residen estas extensiones***, "`/System/Library/Extensions/*.kext`" ***y*** "`/Library/Extensions/*.kext`", ***para confirmar que no existe ninguna extensión de kernel sospechosa o desconocida***, analizando el propósito de cada uno de los elementos no habituales en macOS. Se aconseja salvar el listado de contenidos estos directorios tras instalar el sistema

[74] *Unified prelinked kernel.*

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

operativo macOS, de modo que sirva como referencia (*base line*) para futuras comparaciones.

21.ANEXO B. REFERENCIAS

Referencia	Título, autor y ubicación
[Ref.- 1]	Cómo actualizar a macOS Mojave. Apple. URL: https://support.apple.com/es-es/HT201475
[Ref.- 2]	Kernel Architecture Overview. URL:https://developer.apple.com/library/archive/documentation/Darwin/Conceptual/KernelProgramming/Architecture/Architecture.html
[Ref.- 3]	Apple security updates. Apple. URL: https://support.apple.com/en-us/HT201222 (EN) URL: https://support.apple.com/es-es/HT201222 (ES)
[Ref.- 4]	Guía de referencia sobre la implementación de macOS. Apple. URL: https://help.apple.com/deployment/macos/?lang=es
[Ref.- 5]	Combinaciones de teclas de arranque en el Mac. Apple. URL: https://support.apple.com/es-es/HT201255
[Ref.- 6]	Cambiar o restablecer la contraseña de una cuenta de usuario de macOS. Apple. URL: https://support.apple.com/en-us/HT202860
[Ref.- 7]	Ocultar una cuenta de usuario de macOS. Apple. URL: https://support.apple.com/es-es/HT203998
[Ref.- 8]	Cómo configurar tiras de política en macOS. Apple. URL: https://support.apple.com/es-es/HT202277
[Ref.- 9]	Utilizar FileVault para encriptar el disco de arranque del Mac. Apple. URL: https://support.apple.com/es-es/HT204837
[Ref.- 10]	Downloads Mac notebooks. Apple. URL: https://support.apple.com/downloads/macnotebooks
[Ref.- 11]	Downloads Peripherals. Apple. URL: https://support.apple.com/downloads/peripherals
[Ref.- 12]	Cómo actualizar a macOS Mojave - Comprueba la compatibilidad. Soporte de Apple. URL: https://support.apple.com/es-es/HT201475
[Ref.- 13]	Arrancar el Mac en modo de usuario único o en modo detallado. Apple. URL: https://support.apple.com/es-es/HT201573
[Ref.- 14]	Xcode 10. Apple. URL: https://developer.apple.com/xcode/
[Ref.- 15]	AppleScript. The language of automation. Macosxautomation.com. URL: https://macosxautomation.com/applescript/firsttutorial/index.html Introduction to AppleScript: Overview & Language Guide. Apple. URL:https://developer.apple.com/library/mac/documentation/AppleScript/Conceptual/AppleScriptX/AppleScriptX.html
[Ref.- 16]	Mac macOS: Creating a login hook. Apple. URL: https://support.apple.com/es-es/HT2420
[Ref.- 17]	Customizing Login and Logout. Daemons and Services Programming Guide. Apple. URL:https://developer.apple.com/library/archive/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CustomLogin.html
[Ref.- 18]	Scheduling Timed Jobs. Daemons and Services Programming Guide. Apple. URL:https://developer.apple.com/library/archive/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/ScheduledJobs.html
[Ref.- 19]	Cambiar o restablecer la contraseña de una cuenta de usuario de macOS. Apple. URL: https://support.apple.com/es-es/HT202860
[Ref.- 20]	Security and Your Apps. Apple WWDC. 2015. URL: https://developer.apple.com/videos/wwdc/2015/?id=706

Referencia	Título, autor y ubicación
[Ref.- 21]	About the security content of macOS Sierra 10.12. Apple. URL: https://support.apple.com/en-us/HT207170
[Ref.- 22]	About the security content of macOS High Sierra 10.13. Apple. URL: https://support.apple.com/en-us/HT208144
[Ref.- 23]	macOS Mojave 10.14.5, Security Update 2019-003 High Sierra, Security Update 2019-003 Sierra. Apple. URL: https://support.apple.com/en-us/HT210119
[Ref.- 24]	Cómo configurar tiras de política en macOS. Apple. URL: https://support.apple.com/es-es/HT202277
[Ref.- 25]	Configurar macOS para la autenticación exclusiva con tarjeta inteligente. Apple. URL: https://support.apple.com/es-es/HT208372
[Ref.- 26]	Using Your YubiKey as a Smart Card in macOS. Apple. URL: https://support.yubico.com/support/solutions/articles/15000006468-using-your-yubikey-as-a-smart-card-in-macos
[Ref.- 27]	If you see authentication server errors when turning FileVault on in macOS High Sierra . Apple. URL: https://support.apple.com/en-ie/HT208171
[Ref.- 28]	Use of SecureToken. macOS Deployment Reference. Apple. URL: https://help.apple.com/deployment/macos/?lang=en#/apd8faa99948
[Ref.- 29]	FileVault. macOS Deployment Reference. Apple. URL: https://help.apple.com/deployment/macos/?lang=en#/iore5b074158
[Ref.- 30]	Best Practices for Deploying FileVault 2. Apple Technical White Paper. URL: https://kryptera.se/assets/uploads/2014/10/WP_FileVault2.pdf
[Ref.- 31]	Bonjour Overview. Apple Developers. URL:https://developer.apple.com/library/archive/documentation/Cocoa/Conceptual/NetServices/Articles/domainnames.html#//apple_ref/doc/uid/TP40002460-SW1
[Ref.- 32]	Zero Configuration Networking. URL: http://www.zeroconf.org
[Ref.- 33]	Cómo crear un instalador de arranque para macOS. Soporte de Apple. URL: https://support.apple.com/es-es/HT201372
[Ref.- 34]	Cómo borrar los discos del Mac. Soporte de Apple. URL: https://support.apple.com/es-es/HT208496
[Ref.- 35]	Utilizar una contraseña de firmware en el Mac. Apple. URL: https://support.apple.com/es-es/HT204455.
[Ref.- 36]	Utilizar el modo seguro para aislar los problemas en el Mac. Apple. URL: https://support.apple.com/es-es/HT201262
[Ref.- 37]	Restablecer la NVRAM o la PRAM del Mac. Apple. URL: https://support.apple.com/es-es/HT204063
[Ref.- 38]	Usar la modalidad de disco de destino para mover archivos a otro ordenador. Apple. URL: https://support.apple.com/es-es/HT201462
[Ref.- 39]	Apple EFI firmware passwords and the SCBO myth. @Mac Reversing. Junio 2016. URL: https://reverse.put.as/2016/06/25/apple-efi-firmware-passwords-and-the-scbo-myth/
[Ref.- 40]	The Early Boot Process - Kernel Programming Guide. Apple. Agosto 2013. URL:https://developer.apple.com/library/archive/documentation/Darwin/Conceptual/KernelProgramming/booting/booting.html
[Ref.- 41]	How to report a security or privacy vulnerability. Apple. E-mail: product-security@apple.com
[Ref.- 42]	Acerca del chip de seguridad T2 de Apple. Apple. URL: https://support.apple.com/es-es/HT208862
[Ref.- 43]	Apple T2 Security Chip Security Overview. Apple. URL: https://www.apple.com/mac/docs/Apple_T2_Security_Chip_Overview.pdf
[Ref.- 44]	Security. Built in. Apple. URL: https://www.apple.com/in/macos/security/
[Ref.- 45]	Abrir apps de forma segura en el Mac. Apple. URL: https://support.apple.com/es-es/HT202491

Referencia	Título, autor y ubicación
[Ref.- 46]	Technical Note TN2206: macOS Code Signing In Depth. Mac Developer Library. Apple. URL: https://developer.apple.com/library/mac/technotes/tn2206/_index.html
[Ref.- 47]	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.- 48]	Malware Persistence on macOS 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.- 49]	Acerca del mensaje de alerta "¿Seguro que desea abrirlo?" (cuarentena de archivos / detección de software malicioso conocido) en macOS. Apple. URL: https://support.apple.com/es-es/HT201940
[Ref.- 50]	Your Apps and the Future of macOS Security. Apple WWDC 2018. URL: https://developer.apple.com/videos/play/wwdc2018/702/
[Ref.- 51]	macOS Mojave gets new APIs around AppleEvent sandboxing – but AEpocalypse still looms. Felix Schwarz. URL: https://www.felix-schwarz.org/blog/2018/08/new-apple-event-apis-in-macos-mojave Apple Event sandboxing in macOS Mojave lacks essential APIs. Felix Schwarz. URL: https://www.felix-schwarz.org/blog/2018/06/apple-event-sandboxing-in-macos-mojave
[Ref.- 52]	Managing Mojave's privacy protection: Privacy controls. The Eclectic Light Company. URL: https://eclecticlight.co/2018/09/17/managing-mojaves-privacy-protection-privacy-controls/
[Ref.- 53]	Signing Your Apps for Gatekeeper. Apple developers. URL: https://developer.apple.com/developer-id/
[Ref.- 54]	Notarizing Your App Before Distribution. Apple. URL: https://developer.apple.com/documentation/security/notarizing_your_app_before_distribution
[Ref.- 55]	Hardened Runtime Entitlements. Apple Developers. URL: https://developer.apple.com/documentation/security/hardened_runtime_entitlements
[Ref.- 56]	App Sandbox Entitlements. Apple Developers. URL: https://developer.apple.com/documentation/security/app_sandbox_entitlements
[Ref.- 57]	Code Signing Services. Apple Developers. URL: https://developer.apple.com/documentation/security/code_signing_services
[Ref.- 58]	Guía de referencia sobre la implementación de macOS. Apple. URL: https://help.apple.com/deployment/macos/?lang=es#/
[Ref.- 59]	Technical Note TN2459: User-Approved Kernel Extension Loading. Apple. URL:https://developer.apple.com/library/archive/technotes/tn2459/_index.html#//apple_ref/doc/uid/DTS40017658
[Ref.- 60]	Tarjeta inteligente. Ajustes del servicio de gestión de dispositivos móviles. Apple. URL: https://support.apple.com/es-es/guide/mdm/mdm731e6a3c4/web
[Ref.- 61]	Si el Mac no deja de pedirte la contraseña del llavero. Apple. URL: https://support.apple.com/es-es/guide/keychain-access/kyca1242/10.5/mac/10.14
[Ref.- 62]	Manual del usuario de Acceso a Llaveros. Apple. URL: https://support.apple.com/es-es/guide/keychain-access/welcome/mac
[Ref.- 63]	Recovering Evidence from SSD Drives in 2014: Understanding TRIM, Garbage Collection and Exclusions. Apple. URL: https://articles.forensicfocus.com/2014/09/23/recovering-evidence-from-ssd-drives-in-2014-understanding-trim-garbage-collection-and-exclusions/
[Ref.- 64]	Authorisation Rights. DssW. URL: http://www.dssw.co.uk/reference/authorization-rights/index.html
[Ref.- 65]	About System Integrity Protection on your Mac. Apple. https://support.apple.com/en-gb/HT204899
[Ref.- 66]	Logging. Apple. URL: https://developer.apple.com/documentation/os/logging
[Ref.- 67]	Measuring Performance Using Logging. WWDC 2018. Apple. URL: https://developer.apple.com/videos/play/wwdc2018/405/

Referencia	Título, autor y ubicación
[Ref.- 68]	How Mojave changes the unified log. The Eclectic Light Company. Sept 2018. URL: https://eclecticlight.co/2018/09/25/how-mojave-changes-the-unified-log/
[Ref.- 69]	Keychain Services. Apple Developers. URL: https://developer.apple.com/documentation/security/keychain_services
[Ref.- 70]	Usar Touch ID en el Mac. Apple. URL: https://support.apple.com/es-es/HT207054
[Ref.- 71]	Cómo usar la Touch Bar de tu MacBook Pro. Apple. URL: https://support.apple.com/es-es/HT207055
[Ref.- 72]	Usar Mission Control en el Mac. Apple. URL: https://support.apple.com/es-es/HT204100
[Ref.- 73]	Conocer el escritorio del Mac. Apple. URL: https://support.apple.com/es-es/guide/mac-help/mh40612/10.14/mac/10.14
[Ref.- 74]	Qué contiene la barra de menús del Mac. Apple. URL: https://support.apple.com/es-es/guide/mac-help/mchlp1446/10.14/mac/10.14
[Ref.- 75]	How to Add, Remove, and Rearrange Menu Bar Icons in macOS Mojave. MacRumors. October 2018. URL: https://www.macrumors.com/how-to/rearrange-macos-menu-bar-icons/
[Ref.- 76]	Usar el Dock en el Mac. Apple. URL: https://support.apple.com/es-es/guide/mac-help/mh35859/10.14/mac/10.14
[Ref.- 77]	Organizar los archivos en pilas en el Mac. Apple. URL: https://support.apple.com/es-es/guide/mac-help/mh35846/mac
[Ref.- 78]	Usar Notificaciones en el Mac. Apple. URL: https://support.apple.com/es-es/HT204079
[Ref.- 79]	Cómo usar Night Shift en el Mac. Apple. URL: https://support.apple.com/es-es/HT207513
[Ref.- 80]	How To Manage Plist Files With PlistBuddy. Marco Santa Developer. URL: https://marcosantadev.com/manage-plist-files-plistbuddy/
[Ref.- 81]	Launchd Info. URL: https://www.launchd.info
[Ref.- 82]	Creating Launch Daemons and Agents. Apple. URL:https://developer.apple.com/library/mac/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/CreatingLaunchdJobs.html
[Ref.- 83]	Types of Background Processes. Daemons and Services Programming Guide. Apple developers. URL:https://developer.apple.com/library/archive/documentation/MacOSX/Conceptual/BPSystemStartup/Chapters/DesigningDaemons.html#//apple_ref/doc/uid/10000172i-SW4-SW9
[Ref.- 84]	Sierra's System Integrity Protection (SIP): beyond root. The Eclectic Company. Abril 2017. URL: https://eclecticlight.co/2017/04/28/sierras-system-integrity-protection-sip-beyond-root/
[Ref.- 85]	OS X: Acerca del firewall de aplicación. Apple. URL: https://support.apple.com/es-es/HT201642
[Ref.- 86]	PF - Anchors. Openbsd.org. URL: https://www.openbsd.org/faq/pf/anchors.html
[Ref.- 87]	Launchctl 2.0 Syntax. Babo D's corner. April 2016. URL: https://babodee.wordpress.com/2016/04/09/launchctl-2-0-syntax/
[Ref.- 88]	Configurar controles parentales en el Mac. Apple. URL: https://support.apple.com/es-es/guide/mac-help/mtusr004/10.14/mac/10.14
[Ref.- 89]	MacOS and *OS Internals. Books. Jonathan Levin. URL: http://newosxbook.com
[Ref.- 90]	Configurar el uso compartido de archivos en Mac. Apple. URL: https://support.apple.com/es-es/guide/mac-help/mh17131/mac
[Ref.- 91]	macOS Sierra: Configure usuarios, invitados y grupos en su Mac. Apple. URL: https://support.apple.com/kb/PH25796?viewlocale=es_ES&locale=pt_BR
[Ref.- 92]	Share the screen of another Mac. Apple. URL: https://support.apple.com/guide/mac-help/share-the-screen-of-another-mac-mh14066/10.14/mac/10.14

Referencia	Título, autor y ubicación
[Ref.- 93]	Apple Remote Desktop. Apple. URL: https://www.apple.com/es/remotedesktop/
[Ref.- 94]	SMB3: Overview. Anton Kolomyeytsev. URL: https://www.starwindsoftware.com/blog/smb-3-0-in-a-nutshell
[Ref.- 95]	Compartir tu impresora en el Mac. Apple. URL: https://support.apple.com/es-es/guide/mac-help/mchlp2424/10.14/mac/10.14
[Ref.- 96]	macOS Sierra: Compartir la conexión a Internet de su Mac. Apple. URL: https://support.apple.com/kb/PH25327?locale=es_ES
[Ref.- 97]	If Personal Hotspot is not working on your iPhone or iPad (Wi-Fi + Cellular). Apple. URL: https://support.apple.com/en-us/HT203302
[Ref.- 98]	Manual del usuario de macOS. Apple. URL: https://support.apple.com/es-es/guide/mac-help/welcome/mac
[Ref.- 99]	How to use Mac content caching to save bandwidth, speed up iCloud access & more. Christian Zibreg. Julio 2018. URL: https://www.idownloadblog.com/2018/07/17/howto-mac-content-caching/
[Ref.- 100]	Configurar ajustes avanzados del almacenamiento en caché de contenido en el Mac. Apple. URL: https://support.apple.com/es-es/guide/mac-help/mchl91e7141a/mac
[Ref.- 101]	Conocer el número de ciclos de la batería de los portátiles Mac. Apple. URL: https://support.apple.com/es-es/HT201585
[Ref.- 102]	Monitor OS X LaunchAgents folders to help prevent malware attacks. Topher Kessler. Abril 2012. URL: https://www.cnet.com/news/monitor-os-x-launchagents-folders-to-help-prevent-malware-attacks/
[Ref.- 103]	Usar dispositivos Bluetooth con el Mac. Apple. URL: https://support.apple.com/es-es/guide/mac-help/blth8111/mac
[Ref.- 104]	Bonjour. Apple Developers. URL: https://developer.apple.com/bonjour/
[Ref.- 105]	Usar AirDrop en el Mac. Apple. URL: https://support.apple.com/es-es/HT203106
[Ref.- 106]	AirDrop Security (Página 45). iOS Security. Apple. Mayo 2019. URL: https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf
[Ref.- 107]	Configurar una conexión VPN en el Mac. Apple. URL: https://support.apple.com/es-es/guide/mac-help/mchlp2963/10.14/mac/10.14
[Ref.- 108]	Puertos TCP y UDP usados por los productos de software de Apple. Apple. URL: https://support.apple.com/es-es/HT202944
[Ref.- 109]	Introducir los ajustes del servidor proxy en el Mac. Apple. URL: https://support.apple.com/guide/mac-help/enter-proxy-server-settings-on-mac-mchlp2591/mac
[Ref.- 110]	macOS Security. Overview for IT. Apple. URL: https://www.apple.com/business/resources/docs/macOS_Security_Overview.pdf
[Ref.- 111]	Autenticación de doble factor para el ID de Apple. Apple. URL: https://support.apple.com/es-es/HT204915
[Ref.- 112]	Gestionar y usar el ID de Apple. Apple. URL: https://support.apple.com/es-es/HT203993
[Ref.- 113]	Utilizar "Buscar mi Mac" para localizar un Mac perdido. Apple. URL: https://support.apple.com/es-es/guide/mac-help/mh36811/10.14/mac/10.14
[Ref.- 114]	iCloud: Erase your device with Find My iPhone. Apple. URL. https://support.apple.com/kb/ph2701?locale=en_US
[Ref.- 115]	Qué hacer antes de vender, regalar o renovar tu Mac. Apple. URL: https://support.apple.com/es-es/HT201065
[Ref.- 116]	Usar Continuidad para conectar tu Mac, iPhone, iPad, iPod touch y Apple Watch. Apple. URL: https://support.apple.com/es-es/HT204681
[Ref.- 117]	Requisitos de sistema de Mac, iPhone, iPad, iPod touch y Apple Watch para el uso de las funciones de Continuidad. Apple. URL: https://support.apple.com/es-es/HT204689

Referencia	Título, autor y ubicación
[Ref.- 118]	Configurar un llavero de iCloud. Apple. URL: https://support.apple.com/es-es/HT204085
[Ref.- 119]	Lista de certificados raíz de confianza disponibles en iOS 12, macOS 10.14, watchOS 5 y tvOS 12. Apple. URL: https://support.apple.com/es-es/HT209144
[Ref.- 120]	Deprecation of Legacy TLS 1.0 and 1.1 Versions. Christopher Wood. Webkit.org. URL: https://webkit.org/blog/8462/deprecation-of-legacy-tls-1-0-and-1-1-versions/
[Ref.- 121]	Java and Apple Safari Browser. Oracle. URL: https://www.java.com/en/download/faq/safari.xml
[Ref.- 122]	What does the TCC Compatibility database do? The Eclectic Light Company. URL: https://eclecticlight.co/2018/11/20/what-does-the-tcc-compatibility-database-do/
[Ref.- 123]	Cómo bloquear elementos emergentes en Safari. Apple. URL: https://support.apple.com/es-es/HT203987
[Ref.- 124]	Realizar una copia de seguridad de tu Mac con Time Machine. Apple. URL: https://support.apple.com/es-es/HT201250
[Ref.- 125]	Garantizar la seguridad del disco de copia de seguridad de Time Machine del Mac. Apple. URL: https://support.apple.com/es-es/guide/mac-help/mh21241/mac
[Ref.- 126]	About Apple File System. Apple developers. URL: https://developer.apple.com/documentation/foundation/file_system/about_apple_file_system
[Ref.- 127]	Seleccionar un disco de copia de seguridad y configurar las opciones de encriptación en el Mac. Apple. URL: https://support.apple.com/es-es/guide/mac-help/mh11421/10.14/mac/10.14
[Ref.- 128]	Booting the Mac: Visual Summary. Howard Oakley. The Eclectic Light Company. Agosto 2018. URL: https://eclecticlight.co/2018/08/25/booting-the-mac-visual-summary/
[Ref.- 129]	Bypassing Apple's System Integrity Protection. Objective-See. 2016. URL: https://objective-see.com/blog/blog_0x14.html
[Ref.- 130]	Cambia el nombre de la carpeta de inicio y de tu cuenta de usuario de macOS. Apple. URL: https://support.apple.com/es-es/HT201548
[Ref.- 131]	Aprender a utilizar el Finder del Mac. Apple. URL: https://support.apple.com/es-es/HT201732
[Ref.- 132]	Information Property List. Apple Developers. URL: https://developer.apple.com/documentation/bundleresources/information_property_list
[Ref.- 133]	Authorization Services. Apple Developers. URL: https://developer.apple.com/documentation/security/authorization_services
[Ref.- 134]	" Compatibilidad de las apps de 32 bits con macOS High Sierra 10.13.4 y versiones posteriores". Apple. URL: https://support.apple.com/es-es/HT208436

Referencia	Título, autor y ubicación
[Ref.- 400]	"Guía CCN-STIC-454 - Seguridad en iPad". CCN-CERT. Agosto 2014. URL: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/12-ccn-stic-454-seguridad-en-ipad.html
[Ref.- 401]	"Guía CCN-STIC-455 - Seguridad en iPhone". CCN-CERT. Agosto 2014. URL: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/13-ccn-stic-455-seguridad-en-iphone.html
[Ref.- 402]	"Guía CCN-STIC-455C - Guía Práctica de Seguridad en Dispositivos Móviles iPhone (iOS 11.x)". URL: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3161-ccn-stic-455c-guia-practica-de-seguridad-en-dispositivos-moviles-iphone-ios-11x-1/file.html
[Ref.- 403]	"Guía CCN-STIC-455D - Guía Práctica de Seguridad en Dispositivos Móviles iPhone (iOS 12.x)". URL: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3158-ccn-stic-455d-guia-practica-de-seguridad-en-dispostivos-moviles-iphone-ios-12/file.html
[Ref.- 404]	"Guía CCN-STIC-459 - Cuenta de usuario, servicios y aplicaciones de Apple". *(Prevista su publicación para finales de 2019).*

22.ANEXO C. ÍNDICE DE FIGURAS