

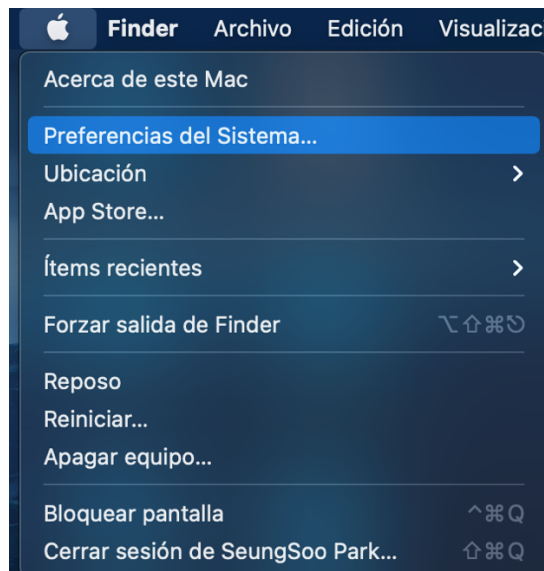
Sistemas Informáticos: Unidad 6 Caso 1

Compartición de carpetas en MacOS

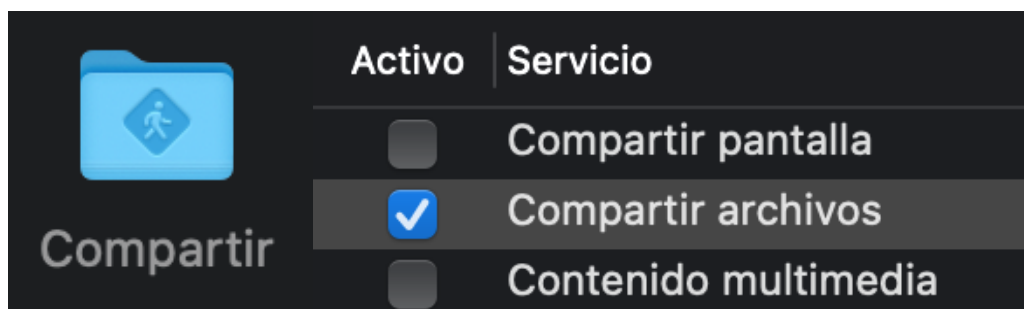
Cualquier sistema operativo ofrece la interfaz de compartimiento de carpetas entre los usuarios de un mismo ordenador, asignándoles los permisos personalizados para cada usuario, entre lectura, lectura y escritura, y sólo escritura (como en MacOS).

Vamos a proceder a gestionar la compartición de carpetas en MacOS:

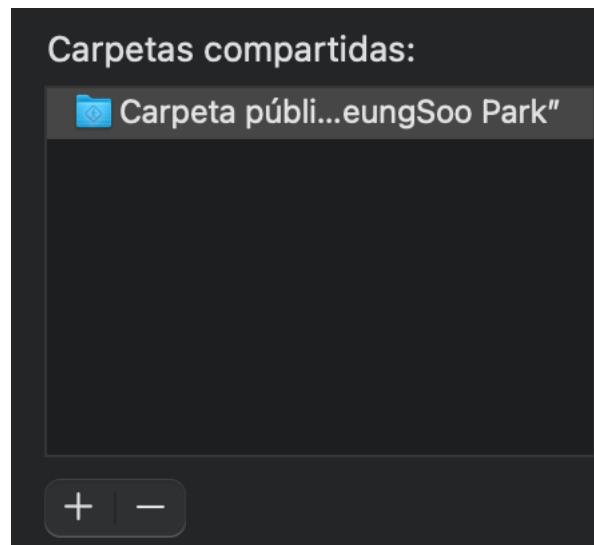
1. Primero le damos al icono de la manzana (icono principal), y accedemos a Preferencias del Sistema.



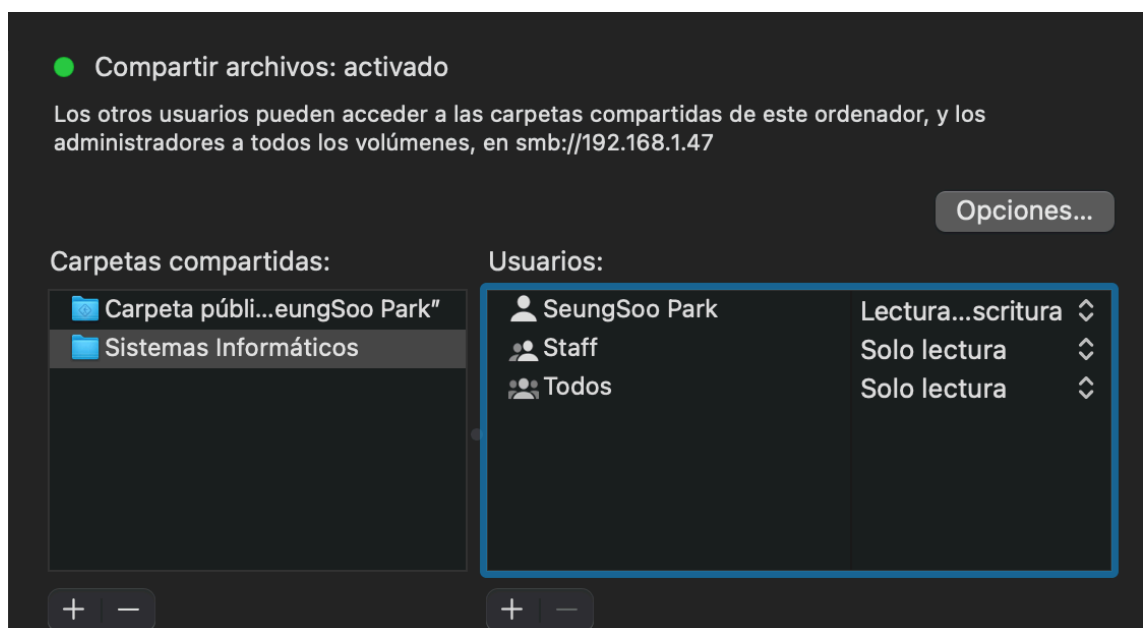
2. Le damos a la opción de gestión Compartir y luego habilitamos Compartir Archivos.



3. Añadimos una nueva carpeta para ser compartida entre los usuarios, en este caso la carpeta Sistemas Informáticos.

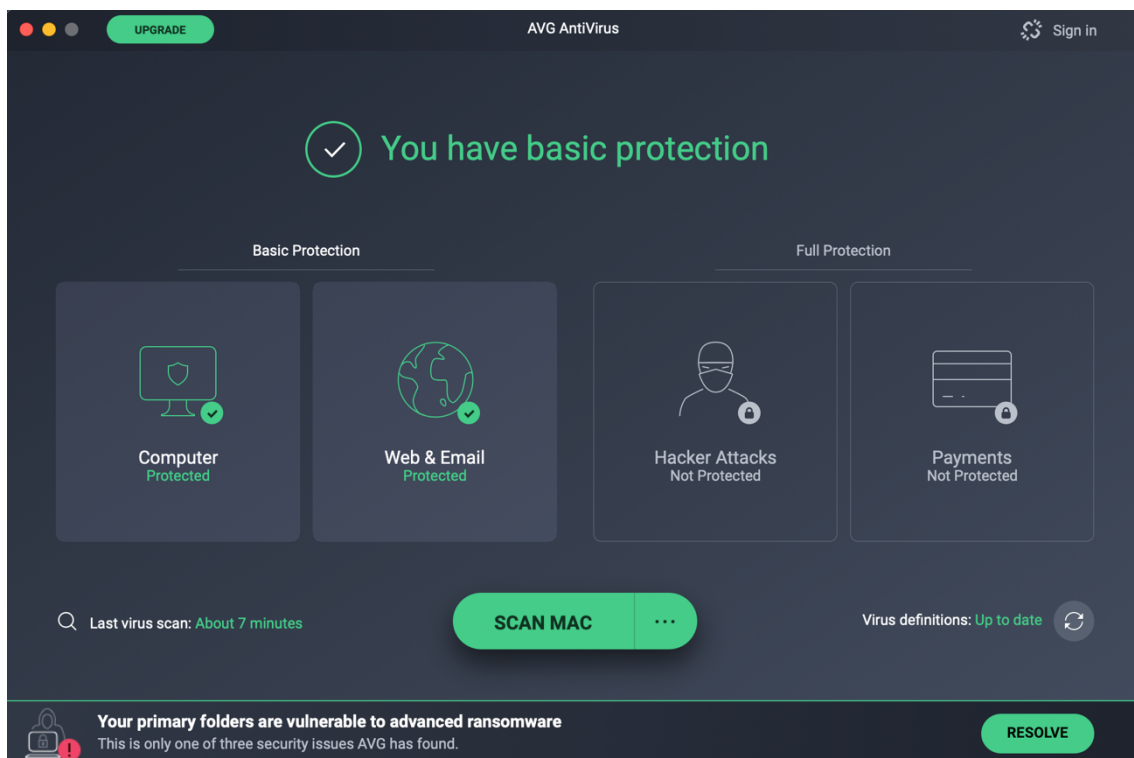


4. Una vez añadido la nueva carpeta, asignamos los permisos a los usuarios, en este caso, solo el permiso de lectura para los usuarios estándares e invitados, mientras que el administrador, en este caso SeungSoo Park, dispondrá de todos los permisos (lectura y escritura).



Antivirus AVG

Una de las buenas opciones en antivirus es el AVG Antivirus, en mi caso, instalado para Mac.



Al ser de la versión gratuita, no dispone de un servicio completo de protección, sino sólo las protecciones básicas como escaneo de archivos del ordenador y protección básico de web y email.

La versión de pago comercial, ofrece una protección completa como protección ante ataques de hacker y protección de pago online.

Como se puede apreciar en la captura de pantalla este antivirus despliega un interfaz legible y simple, fácil de manejar con un botón principal de escaneo.

Orden de Criterio de Seguridad

Ante una descarga de un software bajo un sistema operativo desactualizado puede traer algunos problemas de seguridad ya que presenta más vulnerabilidades a nuevas amenazas digitales actualizados. Por lo que es recomendable seguir el siguiente criterio, ante estos tipos de situaciones:

1. Actualizar sistema operativo. Es fundamental tener el sistema operativo actualizado antes que otras operaciones, ya que el sistema operativo es la fuente principal de un sistema informático. Éste debe estar actualizado periódicamente para soportar nuevos sistemas de redes y sobre todo que el Firewall esté actualizado para identificar nuevas formas de amenazas que puedan colarse en nuestro sistema de red local.
2. Instalar un antivirus. Una vez tenido el sistema operativo actualizado, el equipo cumplirá con todas las condiciones técnicas para soportar el software de antivirus. Éste nos ayudará a protegernos de una gran inmensidad de amenazas maliciosas de los hackers que puede dañar nuestro equipo personal.
3. Actualizar los drivers de los periféricos. Una vez tenido la garantía y la seguridad de un antivirus, ya lo demás se posiciona en un segundo plano por lo que, actualizar los drivers de los periféricos no requiere muchos esfuerzos.
4. Instalar software adicional. A partir de implementar seguridad plena en el equipo, se puede proceder a descargar softwares adicionales de cualquier tipo que no sea maliciosa y que el antivirus esté capacitado de captar cualquier amenaza de virus, gusanos, caballos de Troya, etc.

Conclusiones y Reflexiones

En cualquier sistema de red, es fundamental garantizar la protección y la seguridad en ella para poder gestionar libremente. Para lograr tal estado, es bastante conveniente tener en disposición un buen antivirus, y así poder instalar softwares tranquilamente, estar notificado de cualquier peligro digital y gestionar los permisos de archivos en un sistema de red sin preocuparnos de la seguridad de la misma.