FS/ASSI – CURSO 2019-2020

Giacomo Mossio

– PRÁCTICA 3 –

INFORME ACERCA DE LOS MECANISMOS DE DEFENSA EN NUESTRO ENTORNO DOMÉSTICO

1.- ORDENADOR Y SISTEMA OPERATIVO.

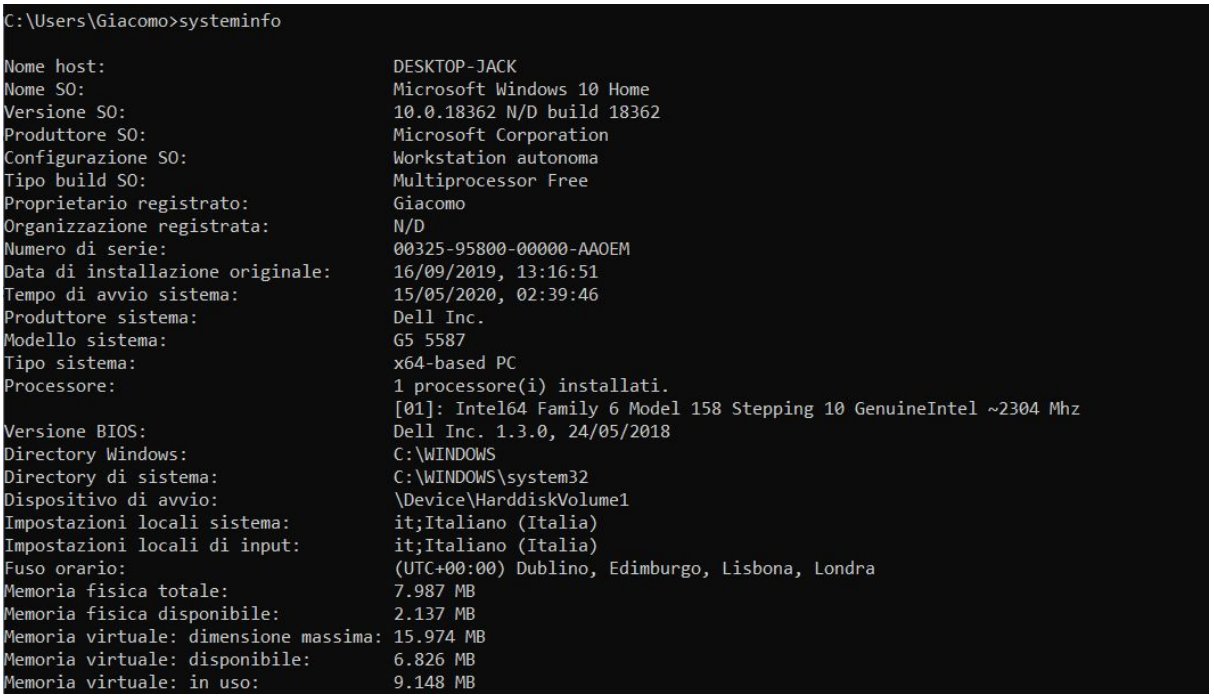
Configuración general de equipo (Fabricante, CPU, RAM, discos, etc.):

Fabricante: Dell Inc.

CPU: Intel(R) Core(TM) i5-8300H CPU @ 2.3OGHZ 2.30 GHZ

RAM: 8,00 GB (7,80 GB utilizable)

discos: 256 GB SSD



Describir fabricante y versión del sistema Operativo:

El fabricante del sistema operativo es Windows, el nombre del SO es Microsoft Windows 10 home, su versión es la 1903 y la build es 18362

Localizar en Internet la fecha límite de actualizaciones mantenimiento y de seguridad de nuestra versión del sistema operativo, especialmente si no es la más actual:

La versión 1903 no es la más actual y su mantenimiento y asistencia es garantida hasta el 8 diciembre 2020 [1].

Número de cuentas de usuario y cuáles de ellas tienen privilegios de administrador:

En este ordenador tengo dos usuarios: uno para mí con permisos de administrador y otro con permisos usuario para cuando mi familia quiere usar mi ordenador.

Política de contraseñas:

Para acceder a mi cuenta personal uso siempre la huella digital y además tengo impostato un PIN y una contraseña en caso no funciona el lector de huellas (ya me pasó). En vez, para acceder a la otra cuenta usuario, dejé elegir una contraseña a mi padre que ha escrito en una agenda para no olvidarla.

Política de copias de seguridad:

Actualmente no tengo copias de seguridad de todos los datos de mi ordenador pero tengo guardados en la nube los documentos más importantes.

Política de actualizaciones:

He puesto mi horario de actividad en las configuraciones de windows Update y dejo que Windows descargue las actualizaciones cuando disponibles.

Descripción de la política de actualizaciones (qué tipo de actualizaciones, cuándo y cómo se instalan, etc.):

La actualización de las funcionalidades es la única que no se instala automáticamente y por eso todavía no he instalado la versión 1909.
Todas las otras se instalan de manera automática cuando no estoy utilizando el ordenador (desde las 02.00 hasta las 08.00)

2.- CONEXIÓN A INTERNET.

Descripción de la conexión a Internet:
Mi conexión es una fibra de 100 MB que comparto con mis 5 compañeros, el ISP es Jazztel [2]. La red de internet es transmitida por la línea eléctrica trámite los cables y después repartida por un router que tengo en mi habitación. El router está utilizado también por un otro mi compañero. Siempre nos conectamos con cualquier dispositivo al router mediante wifi.

Indicar la configuración básica del router:
El router tiene todavía su configuración básica, con la contraseña por defecto para acceder a la pagina de configuracion (user: admin, contraseña: admin) y con el PIN configurado por el instalador. No he modificado nada porque el router no es mio y en futuro será utilizado por otra gente.

Dirección IP pública del router: 188.76.106.158

¿Tiene direcciones privadas? (especificar la dirección IP privada, leer más abajo):
Sí, la direccion de mi ordenador actualmente es 192.168.0.101

¿Tiene filtrado de conexiones entrantes?: (si, siempre que tenga direcciones privadas):
Sí, tengo el NAT activo

¿Tiene alguna configuración especial de conexiones entrantes? (si/no en caso afirmativo, indicar las asignaciones):
Sí, todas las indicadas en el volcado de pantalla

¿El router tiene la contraseña asignada por el instalador o una propia?:
Tiene la contraseña por defecto (admin) porque no quiero modificarla dado que no es mio

En caso de disponer de conexión Wifi:
Nivel de seguridad de la conexión (WEP, WPA, WPA2):
WPA2-PSK

Medidas adicionales (Filtrado de MAC, No anuncio del SSID, desactivación del DHCP, empleo de 802.X etc.):
No

¿La Wifi tiene la contraseña asignada por el instalador o una propia?:
Tiene la contraseña asignada por el instalador que consiste en un PIN de 8 cifras y está escrita debajo del router.

Adjuntar captura(s) de pantalla de opciones básicas de configuración del router:

Status

Firmware Version:	3.19.1 Build 180119 Rel.59618n
Hardware Version:	WR940N v6 00000000

LAN

MAC Address:	98-DA-C4-5C-11-7C
IP Address:	192.168.0.1
Subnet Mask:	255.255.255.0

Wireless

Wireless Radio:	Enable
Name (SSID):	ROB
Mode:	11bgn mixed
Channel Width:	Automatic
Channel:	Auto (Current channel 8)
MAC Address:	98-DA-C4-5C-11-7C
WDS Status:	Disable

WAN

MAC Address:	98-DA-C4-5C-11-7D	
IP Address:	192.168.1.141	Dynamic IP
Subnet Mask:	255.255.255.0	
Default Gateway:	192.168.1.1	Release
DNS Server:	192.168.1.1 , 0.0.0.0	

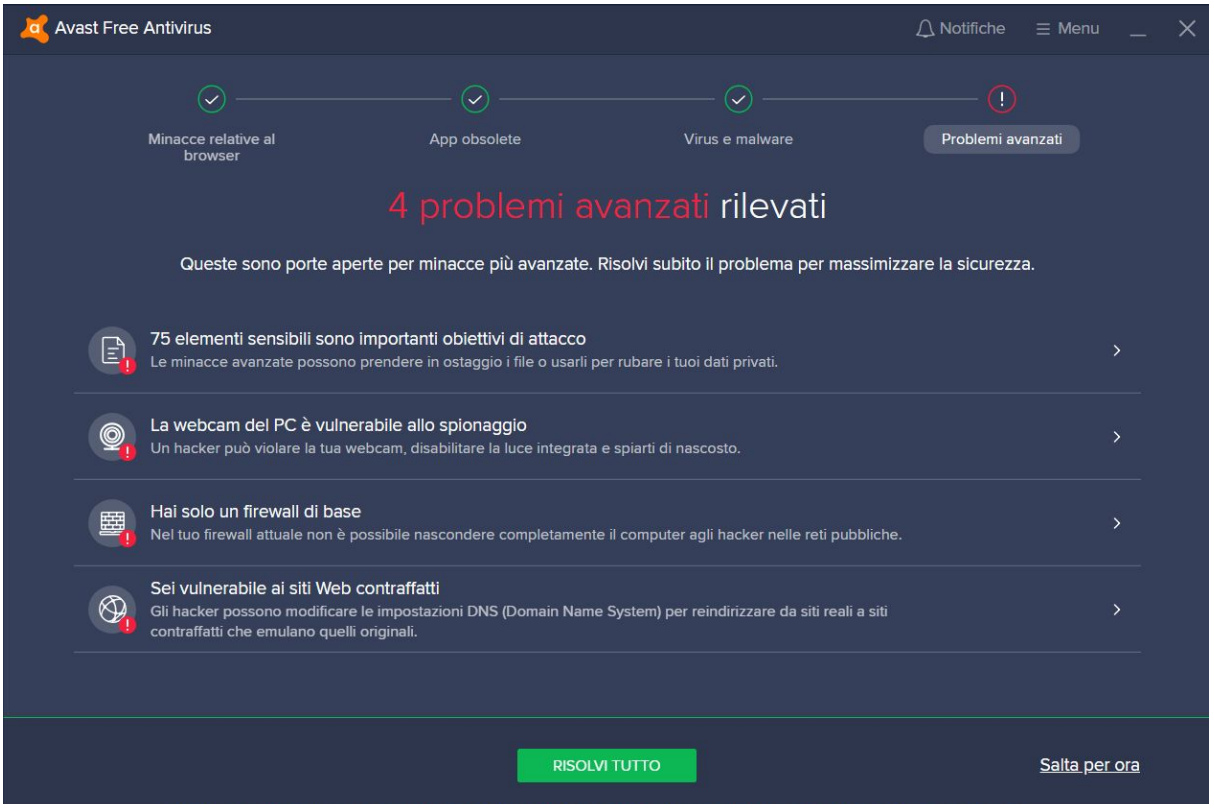
Traffic Statistics

	Received	Sent
Bytes:	916,379,298	3,539,169,073
Packets:	30,896,951	33,009,680

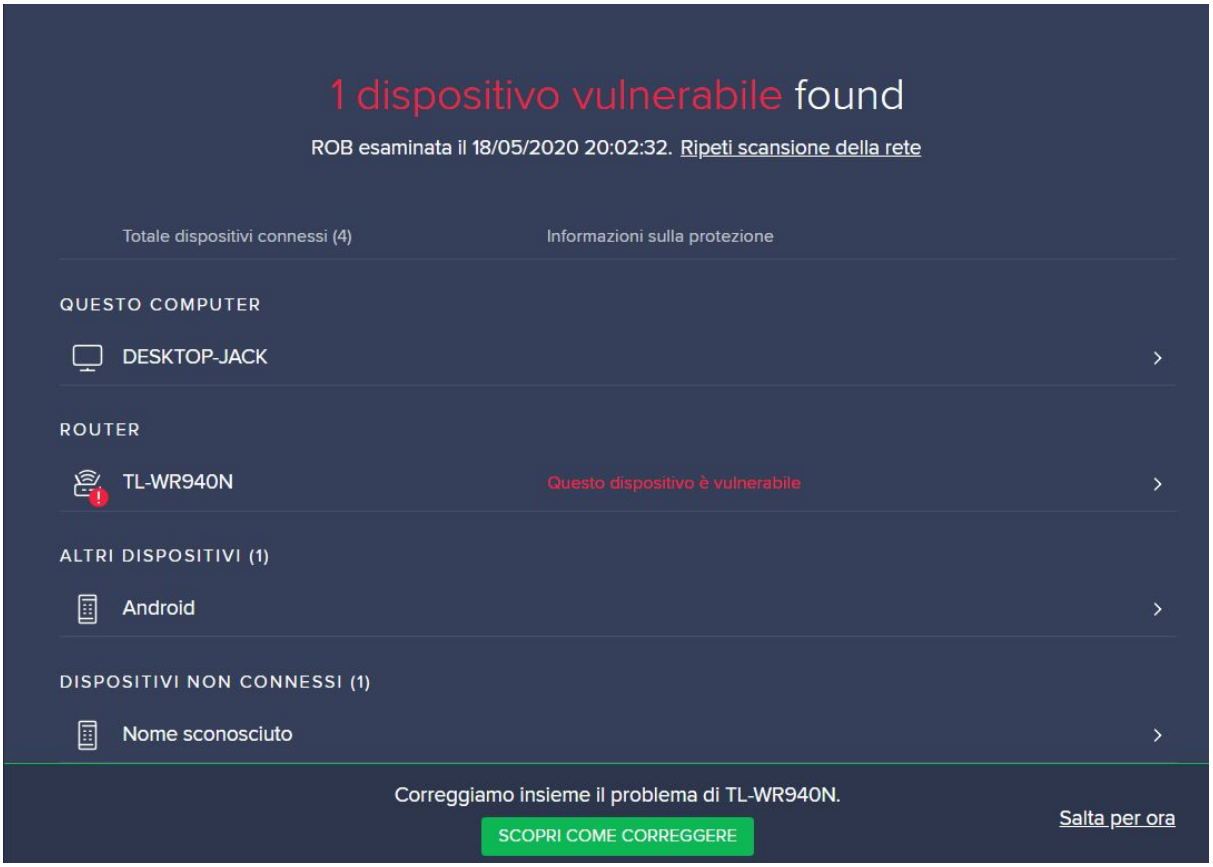
System Up Time:	4 days 19:05:18	Refresh

3.- PROTECCIÓN CONTRA EL MALWARE.

Tengo instalado en mi ordenador la versión gratuita de Avast. Su versión actual es la 20.3.2405 y se actualizo hace dos semanas, tengo la opción de actualización automática activa; los escaneos de los archivos son automáticas cuando los descargo y puedo siempre desactivar el antivirus por archivos individuales. La conexión es también protegida por el antivirus.
Tengo también el firewall de Windows defender activado y todas las otras protecciones; la version de Windows defender es la 4.18.2004.6 .
He efectuado una analisi del ordenador con Avast y los resultados son los siguientes:



Sinceramente no me parecen amenazas graves que necesitan alguna acción y para solucionar los problemas debería comprar la versión premium del programa.
Siguen los resultados de la analisi de la red que encuentra como vulnerabilidad la contraseña por defecto que pero ya expliqué porque no voy a cambiarla.



Hace poco tiempo había también efectuado un escaneo con Windows defender de todos los archivos y no había encontrado problemas.
He descargado Panda y ejecutado un escaneo, siguen los resultados

Los “problemas” señalados se refieren a archivos de cache en los navegadores y poco más.
Pienso que la protección ofrecida de Windows defender junto con Avast free es suficiente para mi ordenador.

4.- BUENAS PRÁCTICAS EN INTERNET

Recomendación 1:
Utiliza **patrones** para crear y recordar tus claves [3]
Ficha de la Guía número: **2**

Recomendación 2:
Si quieres acceder, rectificar,suprimir tus datos o deseas oponerte a que sean tratados con determinada finalidad o deseas limitar su tratamiento tienes que **ejercer tus derechos** ante el titular de la web que aparece en el aviso legal. [3]
Ficha de la Guía número: **7**

Recomendación 3:
Cierra siempre la sesión cuando salgas de una página en la que te hayas autenticado con usuario y contraseña. Con esta acción evitas que si una persona utiliza tu ordenador o tu dispositivo móvil pueda acceder a tu información personal usando la sesión que has dejado abierta. [3]
Ficha de la Guía número: **8**

Recomendación 4:
No conectes **dispositivos extraíbles** cuya procedencia y contenido ignoras. [3]
Ficha de la Guía número: **13**

Recomendación 5:
En primer lugar y si te resulta posible, utiliza ordenadores distintos para el ámbito profesional y para el personal o de ocio. Si no es posible, otra alternativa más sencilla es crear perfiles de **usuario distintos** en función del uso que vayas a hacer del dispositivo. [3]
Ficha de la Guía número: **16**

Recomendación 6:
Cada cosa tiene su tiempo. Ve adaptando las reglas y **límites establecidos** en función de la edad y la confianza que te generan tus hijos. [3]
Ficha de la Guía número: **17**

5.- CONCLUSIONES.

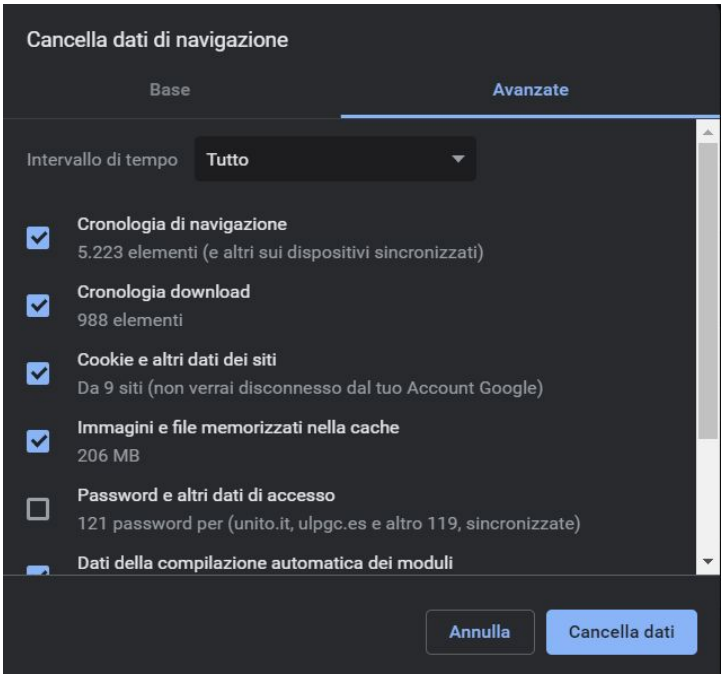
1.- Contrastar nuestras políticas de uso del ordenador y sistema operativo con las recomendaciones efectuadas en la Unidad 4 [4] y en su caso, detectar posibles mejoras:
Antes de esa analisi tampoco sabía que había una actualización de Windows disponible y ahora lo he actualizado a la versión 1909.

Nunca había pensado de utilizar dos cuentas personales para mi ordenador (una cuenta usuario y una administrador) pero puede ser buena idea usarlas.
Otro aspecto que tengo que encargarme son las copias de seguridad porque ahora tengo guardados en Google Drive solamente los documentos fundamentales pero hay muchísimas informaciones importantes que están solamente en mi ordenador y podría perderlas para siempre.

2.- Contrastar nuestras políticas de uso de la conexión a Internet/Wifi con las recomendaciones efectuadas en la Unidad 4 [4] y obligatoriamente, detectar posibles mejoras (ya que hay medidas de seguridad propuestas que seguro no están implantadas):
En mi red de conexión a internet solamente tengo las medidas de seguridad básicas como el NAT pero podría implementar otras como:
-cambiar la contraseña de acceso e impedir la configuración desde Internet
-cambiar la contraseña para las conecciones wifi
-ocultar el identificador de la red
-utilizar la lista de control de acceso (ACL) por MAC
-desactivar el DHCP en el Router y utilizar las IP estáticas
-emplear los protocolos de autenticación 802.1x

Cambiar las contraseñas lo considero importante pero yo soy solamente un residente de esta casa y ya sé que me olvidaría de resetear el router una vez que me haya ido.

3.- Contrastar nuestras políticas de protección contra el malware con las recomendaciones efectuadas en la Unidad 4 [4] y en su caso, detectar posibles mejoras:
La análisis completa de Avast me mostró unas amenazas que pero no considero fundamentales, pues podría cifrar los archivos que contienen datos personales guardados en mi ordenador.
Desde ahora tendré más cuidado con lo que piden los cookies de navegación y los borraré de vez en cuando.



4.- Contrastar nuestras políticas de uso de Internet en general con las recomendaciones indicadas en la Guía de Seguridad y Privacidad [3] en Internet y en su caso, detectar posibles mejoras:
Generalmente uso la herramienta de Google para guardar mis contraseñas de cualquier sitio y ultimamente estoy usando también la herramienta para generar contraseñas seguras. El ordenador lo uso casi solamente yo, y a veces mi padre pero entiendo que cualquiera persona que tenga la contraseña de mi cuenta de Google pueda acceder a un montón de sitios con mis credenciales pero yo soy bastante cuidadoso y confío en la seguridad de Google porque Google depende de ella. Por eso algo que considero de importancia fundamental es cerrar siempre la secciones cuando se usan dispositivos públicos o de los demás.

Por cierto algo que voy a hacer es limpiar mi correo porque me llegan correos de publicidad que no me importan nada (de verdad también desde el correo de la ULPGC recibo demasiado mensajes que no me interesan).

6.- BIBLIOGRAFÍA

[1] "Tu ordenador se actualizará a la última versión de Windows 10 quieras o no", Adsl Zone , 2020. [En línea]. Disponible en: https://www.adslzone.net/2019/07/17/windows-10-actualizar-1803-1903/. [Accedido: 17-may2020]

[2] "¿Cuál es mi dirección IP?", WhatIsMyIpAddress.com, 2020. [En línea]. Disponible en: https://whatismyipaddress.com/es/mi-ip

[3] "PRiVACiDAD Y SEGURiDAD EN iNTERNET", Oficina de Seguridad del Internauta, 2020. [En línea]. Disponible en: https://www.osi.es/sites/default/files/docs/guiaprivacidadseguridadinternet.pdf

[4] Antonio Ocón Carreras, Carlos Rosa Remedios, Apuntes de emergencias tecnológicas. Las Palmas de Gran Canaria : Universidad de Las Palmas de Gran Canaria, Vicerrectorado de Ordenación Académica y EEES, Estructura de Teleformación ULPGC, 2011.