

Cuaderno de prácticas: SEGURIDAD

Apellidos y nombre	

Tiempo Empleado	En aula	Fuera del aula	Total
Horas/minutos			

Usuario:	Fecha	
----------	-------	--

### Entorno Windows

En la dirección <http://www.cdlibre.org/consultar/catalogo/index.html> en el apartado de utilidades, podéis encontrar software libre relacionado con la seguridad.

#### 1 Crear un punto de restauración

E.1 Antes de instalar un nuevo programa, o realizar cualquier operación que pueda afectar al registro, debemos crear un punto de restauración. Haz un punto de restauración. (Inicio, todos los programas, accesorios, herramientas del sistema, restaurar sistema)

R:

#### 2 Arrancar en modo seguro

E.2 Para reparar problemas de seguridad ha que arrancar en modo seguro, para ello en el momento de arrancar el ordenador hay que pulsar la tecla F8 y elegir la opción de arranque en modo seguros. Indica que otras opciones aparecen en el menú.

R:

#### 3 Crearse un usuario que no sea del grupo “administradores”

E.3 Para mejorar la seguridad de nuestro sistema debemos trabajar cotidianamente con un usuario que **No** sea del grupo administradores. Créate un usuario que se llame “Usuario” que no sea del grupo administradores (panel de control, cuentas de usuario) Indica el tipo de cuenta seleccionado.

R:

#### 4 Antivirus

E.4 Busca un antivirus gratuito en <http://alerta-antivirus.inteco.es/> (útiles gratuitos). No te lo bajes, simplemente indica cuál has elegido y la dirección de descarga. Los antivirus gratuitos que recomendamos son: Avast (Alwil software ), Avira y AVG

R:

E.5 ¿Conoce los antivirus en línea?(R1) ¿Qué diferencia hay con los antivirus convencionales?(R2). Indica 2 direcciones más de antivirus en línea distintas de las indicadas en la cuestión siguiente (R3). (pista: <http://alerta-antivirus.inteco.es/> -> útiles gratuitos)

R1:

R2:

R3:

E.6 Pasa uno de estos dos antivirus en línea al ordenador. Indica si hay algún “incidente” y cual.

•<http://www.pandasecurity.com/spain/> (análisis on-line gratuito con active-scan)

•<http://housecall.trendmicro.com/es/> (housecall)

R:

E.7 Existen herramientas de desinfección específica diseñada para la eliminación de un determinado “malware”. Indica dos .Mira en la dirección:

•<http://alerta-antivirus.red.es/utiles/ver.php?tema=U&articulo=8&pagina=0>

Cuaderno de prácticas: SEGURIDAD

•<http://www.microsoft.com/spain/seguridad/malwareremove/default.msp>

R:

## 5 Detector de espías (spyware)

E.8 Busca un detector de programas espías en <http://alerta-antivirus.inteco.es/>. Indica la dirección web de donde te puedes bajar los tres antiespías siguientes:

- Ad-aware-spyware : <http://>
- spybot: <http://>
- Windows defender: <http://>

### Sitio para ver si el antiespía es un espía

- <http://www.infospyware.com/rogue-software>
- <http://www.forospyware.com/t5.html>
- [http://www.spywarewarrior.com/rogue\\_anti-spyware.htm#online](http://www.spywarewarrior.com/rogue_anti-spyware.htm#online)

Otro anti-espías

- <http://www.sin-espías.com/>
- <http://www.emsisoft.org/es/>.
- <http://www.spychecker.com/> Lista de muchos anti-*malware*

E.9 Intálale el anti espías Ad-aware. Indica la versión que te has instalado.

R:

E.10 Instálale el programa audiogalaxy <http://www.audiogalaxy.com/>. O kaZaA (<http://www.kazaa.com/us/index.htm> ). Indica cual te has instalado y que versión.

R:

E.11 Ejecuta el detector de espías. Indica si ha encontrado algún espía.

R:

E.12 Desinstala el programa Kazaa o audiogalaxy.(hecho; no hecho)

E.13 Mira los programa de inicio. Comprueba si alguno es un espía. En <http://www.sin-espias.com/items/>. Indica si hay alguno. Puedes mirar los programas de inicio en Inicio-> ejecutar y teclear "msconfig".

En estas direcciones puedes consultar si un programa es un *malware* o no.

- <http://www.sin-espias.com/items/>
- [www.what-process.com](http://www.what-process.com)
- <http://www.whatsrunning.net/whatsrunning/processinfocentral.aspx>

R:

## 6 Escaneador de puertos

- *Lee primero la información sobre los puertos que aparece en esta dirección:*

○ <http://www.seguridadenlared.org/es/index7esp.html>

Leelo y encontrarás información interesante como esta: "Detectar que puertos de comunicaciones es una medida básica de seguridad para nuestros equipos. Existen tres formas básicas para detectarlos:

• **Usando las herramientas proporcionadas por el sistema operativo:** Tanto Windows como Linux o Mac OS X nos ofrecen una herramienta que nos va a mostrar que conexiones de red tenemos en cada momento. Esa herramienta es el programa netstat, y para ejecutarla, en ambos casos, necesitamos abrir una Consola.

• **Usando un escaner de puertos:** Una herramienta para detectar puertos abiertos es el escaner de puertos. Sirve para controlar el estado de los puertos de cualquier PC conectado a la Red.

Cuaderno de prácticas: SEGURIDAD

•**Usando un escaner de puertos online:** Estas herramientas detectan que puertos son accesibles desde el exterior de nuestra red, ya que aunque tengamos un puerto abierto en nuestro PC, tal vez un firewall, o más comúnmente un router que este en nuestra red, impida su acceso” (Asociación de Internautas).

- En <http://www.internautas.org/w-scanonline.php> hay un detector de puertos.
- En <http://seguridad.internautas.org/> hay mas información.

E.14 Pasa ahora un escaneador proporcionado por el sistema operativo: Desde el interfaz de comandos, usando la orden: **netstat -an** .. Anota algunos de los puertos que aparecen o pega la ventana.

R:

E.15 Instala el escaneador de puertos local como el **portscan**. Puedes encontrarlo en <http://www.seguridadenlared.org/35.html> mira [portscan.zip](#). Escanea los puertos del ordenador de tu compañero (indicando la dirección IP de su ordenador). Indica el resultado. (pega la ventana).

R:

E.16 Mira en: <http://alerta-antivirus.red.es/utiles/ver.php?tema=U&articulo=3> los programas de escaneo de puertos en línea.(upeseros). Utiliza uno. indica cual has utilizado y un resumen del resultado (tal está abierto, todos cerrados, etc)

R:

## 7 Cortafuegos

E.17 Pasar un detector de puertos en línea. (<http://alerta-antivirus.red.es/utiles/ver.php?tema=U&articulo=3> ). Indica el que has usado (repartíselos, no usar todos el mismo). Anota los puertos que tienes abierto.

- <http://www.upseros.com/portscan.php>
- <http://scan.sygate.com/>
- <http://www.internautas.org/w-scanonline.php>
- <https://www.grc.com/x/ne.dll?bh0bkyd2>

R:

E.18 Busca un cortafuego gratuito en <http://alerta-antivirus.inteco.es/>. Indica otros distintos a los relacionados a continuación.

- ZoneAlarm
- Comodo versión 2.4
  - [http://www.personalfirewall.comodo.com/license\\_registration.html](http://www.personalfirewall.comodo.com/license_registration.html)

R:

E.19 Instala el cortafuego zonealarm o comodo 2.4. Indica cual has instalado.

R:

Cuaderno de prácticas: SEGURIDAD

E.20 Pasar un detector de puertos en línea, como antes. Indica si hay algún puerto que ya no aparece.

R:

## **8 Limpiador de registro de Windows**

E.21 Buscar un limpiador de registros de Windows. Indica la dirección del sitio oficial de dos de los indicados.

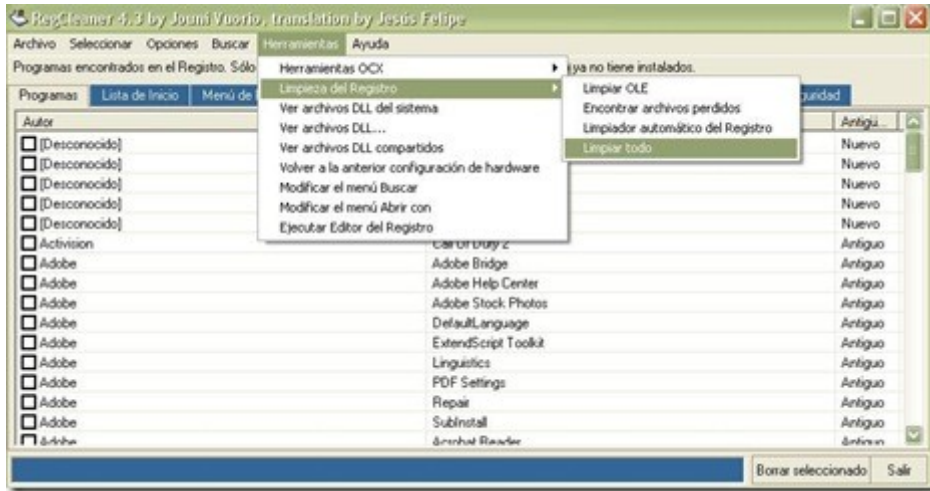
- Regcleaner
- RegistryRobot
- ccleaner
- Easycleaner

E.22 Instalar el programa Regcleaner y ponerlo en español. Indica como lo has hecho.

R:

## Redes de datos

### Cuaderno de prácticas: SEGURIDAD



E.23 Limpiar el registro de Windows (usando la opción correspondiente de regcleaner. El que busca encuentra). Indica incidencias. (no ha encontrado ninguna incidencia, pocas, muchas etc.)

R:

## 9 Otras herramientas de seguridad

### Microsoft

Dirección de seguridad de Microsoft en España

- <http://www.microsoft.com/spain/seguridad/default.mspx>

E.24 Entra en esta dirección: <http://www.microsoft.com/spain/protect/default.mspx> Consejos de seguridad de Microsoft. Indica tres consejos de distintas secciones, que se recomienden en esta página.

R:

Mira en esta dirección: [Microsoft Baseline Security Analyzer Version 2.0](http://www.microsoft.com/baselinesecurityanalyzer/) . Es un programa que



Cuaderno de prácticas: SEGURIDAD

analiza la seguridad de tu ordenador según Microsoft.

E.25 Instala el MBSA, y ejecútalo. Indica las incidencias.

R:

### Un software integrado Advance Systemcare

E.26 El programa "Advance Systemcare", es un programa que analiza el ordenador limpiando en una sola operación varios aspectos de los comentados en la práctica, como son el registro, ficheros no necesarios y el malware.. Lo puedes descargar de <http://www.iobit.com/advancedwindowscareper.html> . Instálalo y pásaselo al ordenador. Tiene varias opciones: limpieza, prevención, utilidades. Prueba las opciones. Indica las incidencias detectadas.

R:

### AOL Active Security Monitor

Es un programa que te da una nota sobre la seguridad de tu ordenador

Puedes descargarlo desde esta dirección

- <http://aol-active-security-monitor.softonic.com/>
- <http://daol.aol.com/security/active-security-monitor>

Otro escaner

- <http://www.eset.com/esibeta/>

### 10 Navegación segura

A continuación hay distintos *plug-ing* que se pueden instalar en nuestro navegador para aumentar la seguridad de la navegación. Indican si el sitio es sospechoso

- [http://www.trendsecure.com/portal/en-US/tools/security\\_tools/trendprotect/overview](http://www.trendsecure.com/portal/en-US/tools/security_tools/trendprotect/overview)

Netcraft

- <http://toolbar.netcraft.com/install>

Mcafe

- <http://www.siteadvisor.com/>

E.27 Instálate uno de ellos. Indica cómo advierte sobre un peligro.

Cuaderno de prácticas: SEGURIDAD

R:

E.28 Configura en navegador para que no acceda las galletitas (pedir datos de *cookies* de origen y bloquear los *cookies* de terceros). Indica como lo has hecho.

R:

E.29 Desinstala todos los programas que hayas instalado en la práctica. Indica si lo has hecho.

R:

## 11 Enlaces

- <http://seguridad.internautas.org/>

Seguridad de las tarjetas de coordenadas

- <http://seguridad.internautas.org/html/901.html>

Guía para detectar web falsas

- <http://seguridad.internautas.org/html/863.html>

Generador de claves WEP

- <http://seguridad.internautas.org/html/4165.html>

Guía de nuevos fraudes

- <http://seguridad.internautas.org/html/816.html>

Curso de certificados digital

- <https://ws024.juntadeandalucia.es/cursoCertificados/inicio.htm>

Utilidades Internal Microsoft

- <http://technet.microsoft.com/es-es/sysinternals/default.aspx>