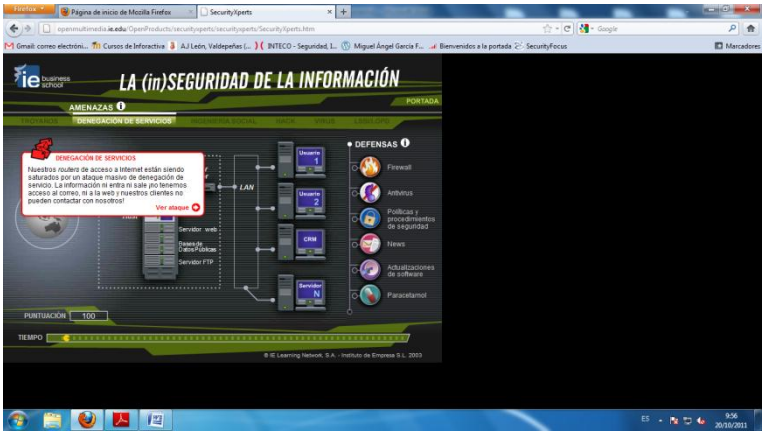
TEMA 1 PRÁCTICA 5: AMENAZAS

A)

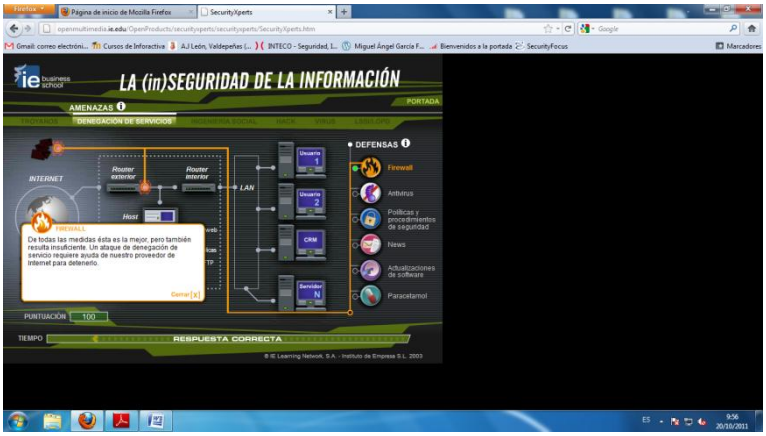
Juego de seguridad

A continuación veremos este pequeño juego a fondo.

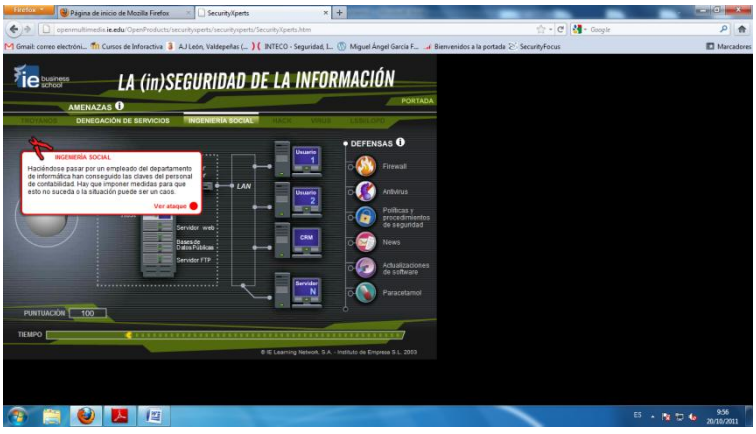
Problema de delegación de servicios.



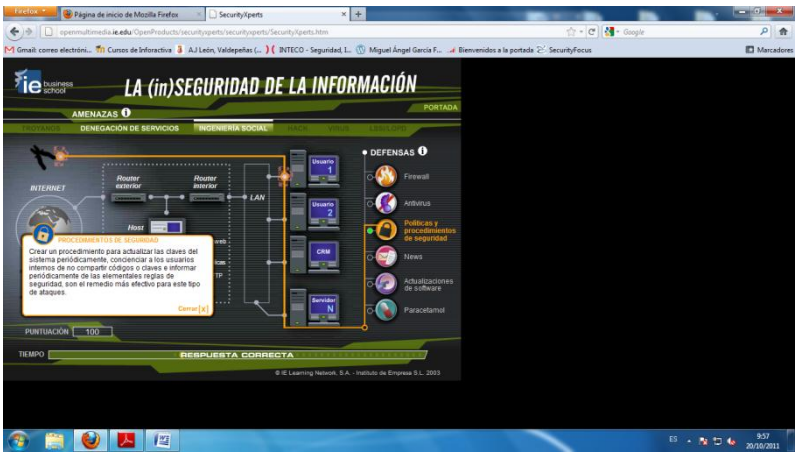
Solución usar un firewall.



Problema Ingeniería social

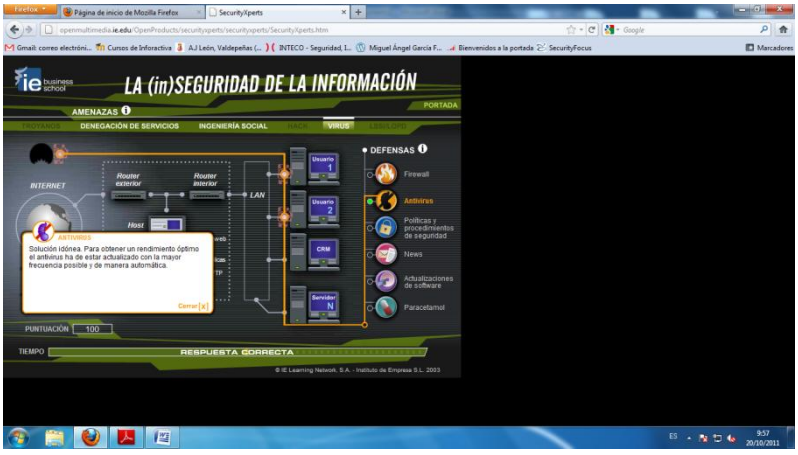


Solución aplicar políticas de seguridad



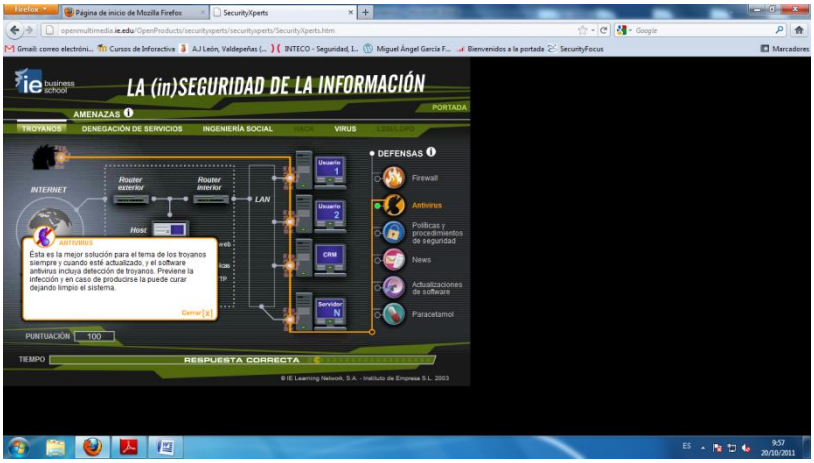
Problema con un virus.

Solución aplicar un antivirus.



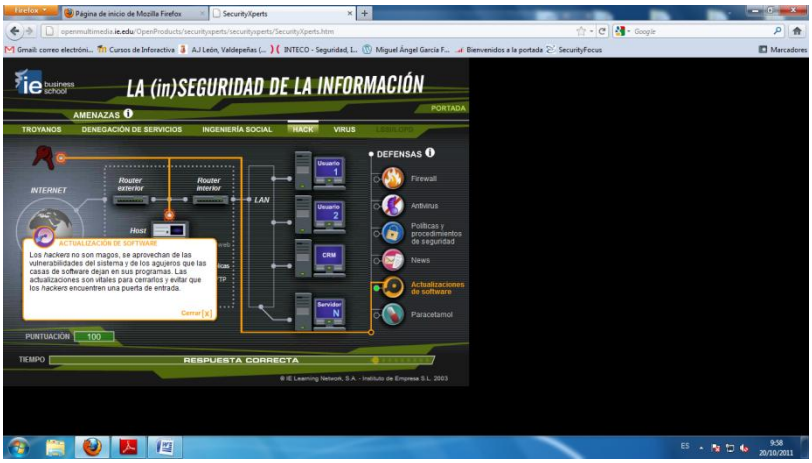
Problema intrusión de un troyano

Solución aplicar un antivirus

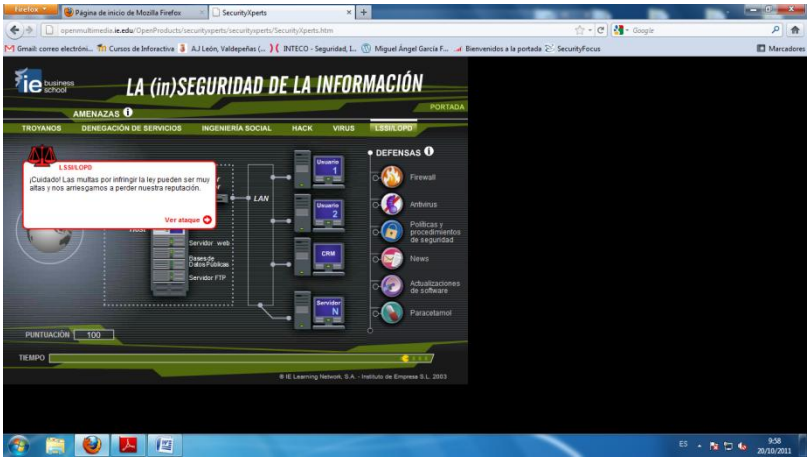


Problema intrusión de un hack.

Solución actualizar nuestro software



Problema con la LSSI/LOPD, solución aplicar todas las técnicas anteriores. El paracetamol es opcional dependiendo, de la capacidad del informático a soportar grandes presiones.



Resumen del ataque al servidor IRC Hispano (caso Ronnie)

Ataque a IRC Hispano: Caso “Ronnie”

Dos años de prisión y una indemnización civil de 1.332.500 euros. Ésta es la condena que ha recibido **Santiago Garrido, alias 'Ronnie'**, autor confeso del mayor ataque DDos (Denegación de Servicio Distribuidos) en España realizado en 2003. **Se trata de un acuerdo** entre la acusación y la defensa.

La indemnización civil se desglosa de la siguiente manera: 474.500 euros en daños a Lleida.net, 570.716 euros en daños a Wanadoo, 120.000 euros en daños a ONO y 218.000 euros en daños a IRC Hispano.

Finalmente la sentencia es firme por haberse aceptado por ambas partes y en el plazo de una semana el juez publicará dicha sentencia. En el juicio, Santiago Garrido **ha reconocido todos los hechos y los daños causados**.

Garrido, vecino de A Coruña, se conectaba a IRC-Hispano utilizando los psuedónimos 'ronne', 'ronnie', 'san71ag0', 'schenker', 'hairyman', 'ddd', 'stokosky' o 'teppenwolf', y fue **detenido en agosto de 2003** por la Unidad de Delitos Telemáticos de la Guardia Civil como presunto autor de los hechos.

El acusado había sido expulsado de IRC-Hispano por saltarse algunas de las normas de la empresa, como utilizar la identidad de otros usuarios en 'chats' del servidor.

Tras su ataque de denegación de servicio contra IRC-Hispano, la Unidad de Delitos Informáticos de la Guardia Civil inició una operación que contó con la colaboración de la empresa antivirus Panda Software y que concluyó con la detención de 'Ronnie'.

"Ronnie" se vengó de la expulsión bombardeando con paquetes de bits la red de chats, en lo que se llama un ataque de Denegación de Servicio. Hasta aquí, era uno más de los bombardeos que suele recibir el IRC-Hispano por parte de usuarios enfadados con sus polémicos operadores. Pero, el día de Navidad, el "cracker" les envió un mensaje de correo, haciéndose responsable del ataque y amenazando con volver.

"La amenaza fue echarles todo abajo, como efectivamente ocurrió. Me irritó que me echaran por una nimiedad", explica el joven. Según la sentencia, "los ataques se fueron sucediendo de forma continuada y periódica hasta mayo de 2003". Santi se dedicó a infectar, con un gusano llamado "Deloder", miles de ordenadores en Europa y Asia que convertía en "zombies" a sus órdenes, lanzados como un ejército contra el IRC-Hispano. A medida que crecía el número de "zombies", el bombardeo se transformaba en una temible Denegación Distribuida de Servicio (el ataque no viene de un frente, fácil de atajar, sinó de múltiples).

Entre abril y mayo, arremetió también contra los proveedores que dan soporte a la red de chats, como Wanadoo, Ono y LleidaNet, que lo denunciaron. Sisco Sapena, presidente de IRC-Hispano, explica: "Fueron nueve meses, a veces cuatro y cinco ataques diarios. Recuerdo el primero, en Navidad, estuve 24 horas encerrado en una habitación para atajarlo. No era la primera vez que nos atacaban, pero nunca había sido tan sistemático. Llegó a peligrar mi empresa, LleidaNet". Bajo un bombardeo, se colapsan las máquinas y todo deja de funcionar: el correo, la web, etc.

La Unidad de Delitos Telemáticos de la Guardia Civil detuvo a Santi Garrido en julio de 2003, pocos días antes de su cumpleaños. Vivía con sus padres, una familia humilde de A Coruña. Se le acusaba del mayor ataque de Denegación Distribuida de Servicio ocurrido en España. El IRC-Hispano, que colaboró activamente en su identificación, junto con Panda Sofware, pedía siete años de cárcel.

B)

Noticia relacionada con amenazas físicas.

Quirós denuncia en la Junta "amenazas físicas" a su equipo por la reforma sanitaria

Defendió la «legitimidad» de cambios y advirtió de que «cuando no hay acuerdo, la responsabilidad de los poderes públicos es indelegable»

La aplicación de la 'reforma Quirós' suma nuevos escollos. A los numerosos frentes abiertos -apertura de los centros de salud por las tardes, eventuales, urgencias...- se añade ahora el de las «amenazas físicas» y las «fuertes presiones» que están sufriendo algunos equipos directivos de la Consejería de Salud. La denuncia llegaba ayer al Parlamento asturiano de boca del máximo responsable sanitario y principal promotor de la renovación. José Ramón Quirós respondía en la Junta General a una interpelación del Grupo Parlamentario Popular sobre política sanitaria en materia de Atención Primaria. Allí defendió la necesidad y «legitimidad» de unos «cambios estructurales profundos» que permitan un servicio «más equitativo en todas las áreas de Asturias y estén centrados en los intereses de los ciudadanos». Y allí advirtió de que «cuando no hay acuerdo la responsabilidad de los poderes públicos es indelegable». Dicho esto, Quirós endureció el gesto para rechazar gran parte de las críticas vertidas contra el proceso procedente en su mayor parte, dijo, del Sindicato Médico (Simpa). Unos mensajes negativos que el consejero resumió con la frase: «Marean al paciente y joden al sistema». Fue entonces cuando denunció ante los diputados regionales las «amenazas físicas» recibidas por dirigentes del sector sanitario y las «insoportables tensiones» y «fuertes presiones» que están sufriendo y que alcanzan incluso, según sus palabras, a sus familias.

C)

Noticia relacionada con amenazas lógicas.

Detenido un joven por fraude de más de 80.000 euros a través Internet

La Policía Nacional ha detenido en Toledo a un joven a quien se atribuye un fraude de más de 80.000 euros cometido mediante ventas fraudulentas a través de Internet. **Al parecer, ofrecía teléfonos móviles de alta gama que luego no enviaba a sus compradores.**

J.M.G., de 24 años de edad, comenzó insertando anuncios en webs de compraventa de artículos entre particulares en los que ofrecía teléfonos de gama alta a bajo precio. En ellos **facilitaba su identidad real y realizaba las transacciones mediante giros postales**. La Brigada Provincial de Policía Judicial de Toledo comprobó que este estafador había recibido numerosos pagos desde distintas provincias con lo que la investigación se extendió a otros puntos de la geografía española. Poco después, J.M.G cambió su modo de actuar y, para perpetrar nuevas estafas, **comenzó a facilitar cuentas bancarias en las que sus víctimas debían realizar los ingresos**. De hecho, aumentó sus actividades ilícitas, ofreciendo ahora todo tipo de teléfonos, consolas y artículos electrónicos. Los agentes detectaron decenas de ingresos fraudulentos, de cantidades que oscilaban entre los 120 y los 200 euros, procedentes de afectados situados en diferentes localidades del país que creían haber encontrado una ganga en la Red.

Intentando evitar la actuación de los agentes, **el arrestado comenzó a utilizar nombres supuestos, aunque el teléfono de contacto que facilitaba a los compradores era el mismo** que en anteriores ocasiones. La información obtenida tras el minucioso análisis de las nuevas cuentas bancarias en las que sus víctimas realizaron los ingresos y las diversas gestiones policiales permitieron capturarle esta semana y acusarle de un delito continuado de estafa.

El detenido **ha pasado ya a disposición judicial**. Los investigadores le atribuyen un fraude superior a los 80.000 euros, cometido a través de Internet en un periodo de un año. Además, estiman que sus víctimas podrían ser más de 400.

D)

Análisis de dos antivirus online

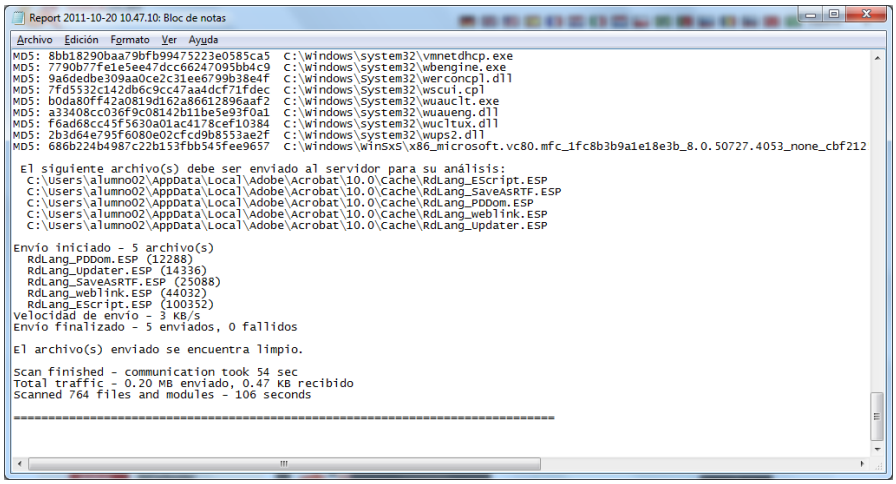
A continuación vamos a proceder a la muestra de cómo analizar en red nuestro equipo con los siguientes antivirus.

Bit Defender

En la página oficial de este antivirus, pulsamos el botón de iniciar el antivirus, si no tenemos los plugins necesarios los instalamos. Seguidamente le damos a iniciar para comenzar el análisis.

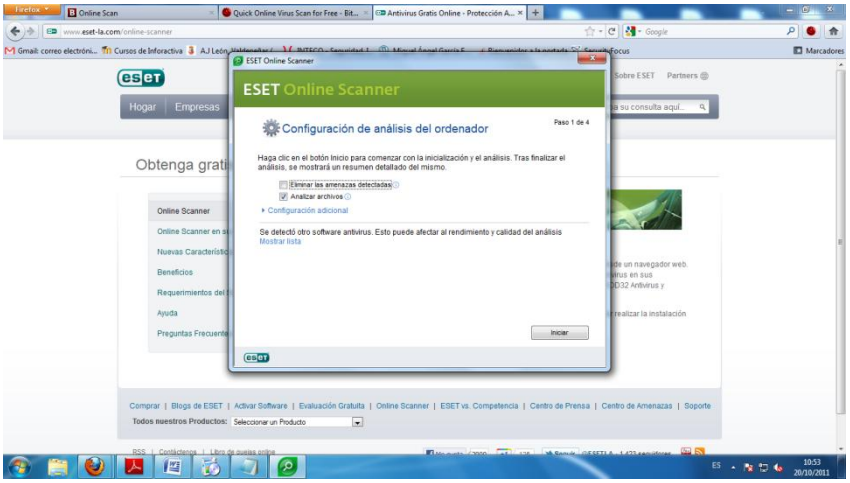
El antivirus analizará nuestro sistema.

Una vez finalizado el análisis nos ejecutara el siguiente informe con los resultados.

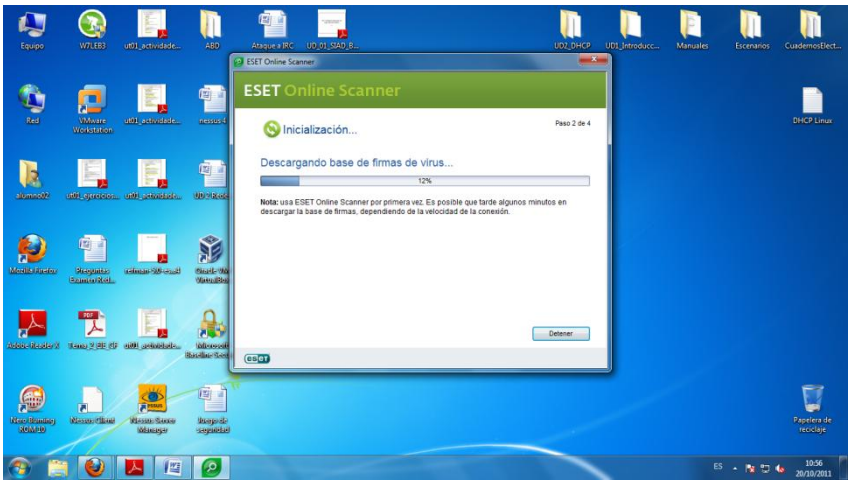


NOD 32 Online

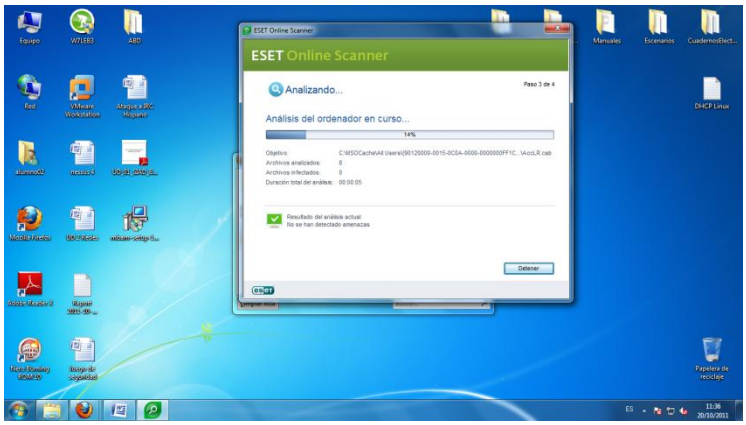
Nos situamos en la página oficial de ESET para probar el antivirus online. Aplicamos la opción de analizar archivos.



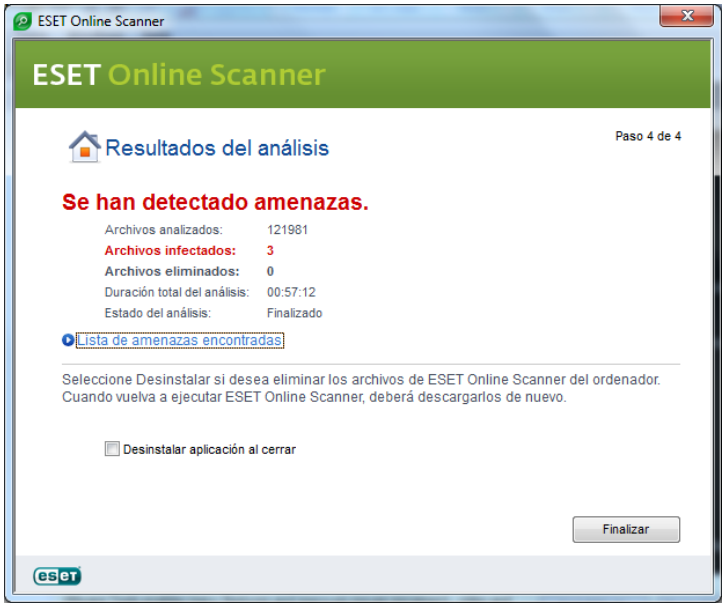
Antes del análisis se necesita descargar la base de firmas.



Se procede al análisis del sistema.



Una vez finalizado el análisis nos da los siguientes resultados.



Si pulsamos a la opción de ver las amenazas encontradas…

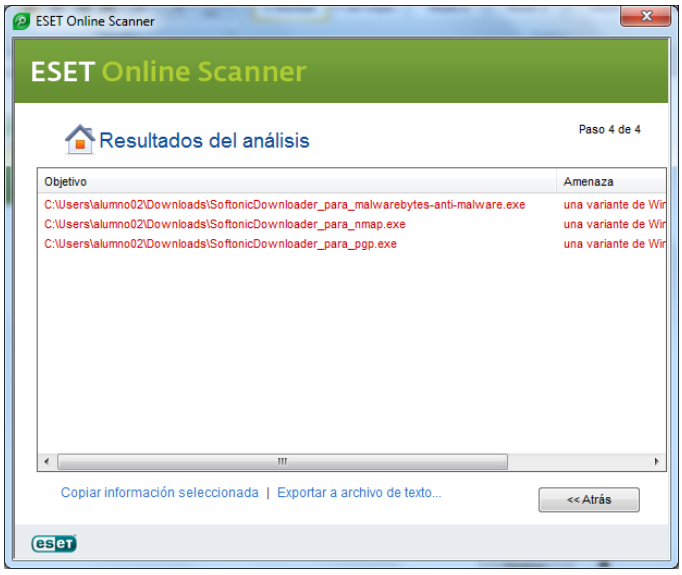


Tabla de resultados

Antivirus:	Nº archivos analizados.	CPU en ejecución.	Opciones avanzadas de escaneo.	Tiempo de escaneo.	vulnerabilidades	virus encontrados	desinfectados
Nod 32 online	121981	45 %	Estándar	57:12 min	3	3	0
Bit defender	164	40 %	Estándar	106 seg	0	0	0

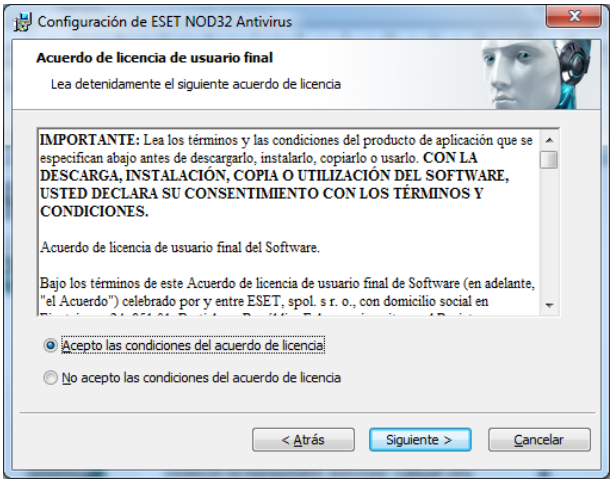
E)

Análisis de dos antivirus locales

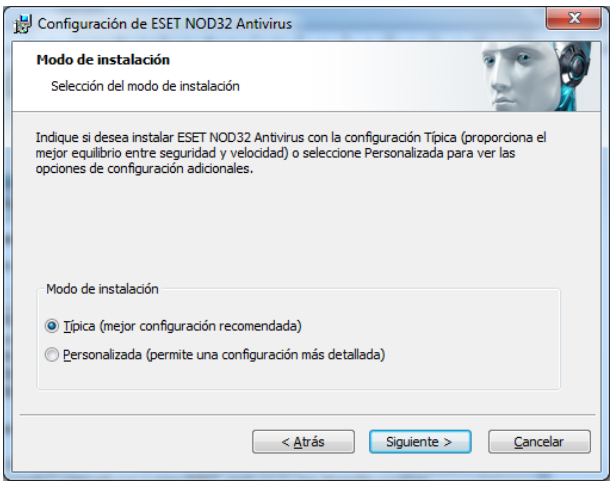
NOD 32 local

Instalamos el antivirus mediante el asistente.

Aceptamos los términos de la licencia.

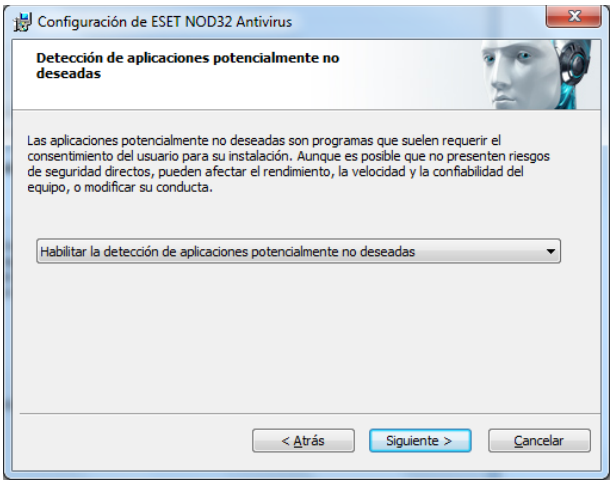


Pulsamos la opción de siguiente

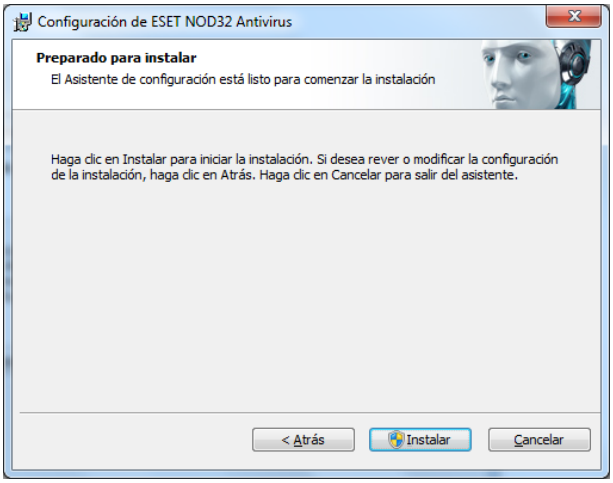


Desmarcamos esta opción.

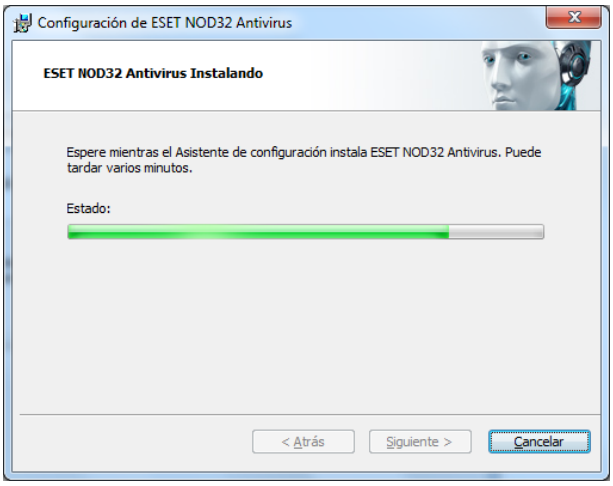
Habilitamos la detección de aplicaciones potencialmente no deseadas.



Una vez seleccionadas las opciones anteriores pulsamos instalar.

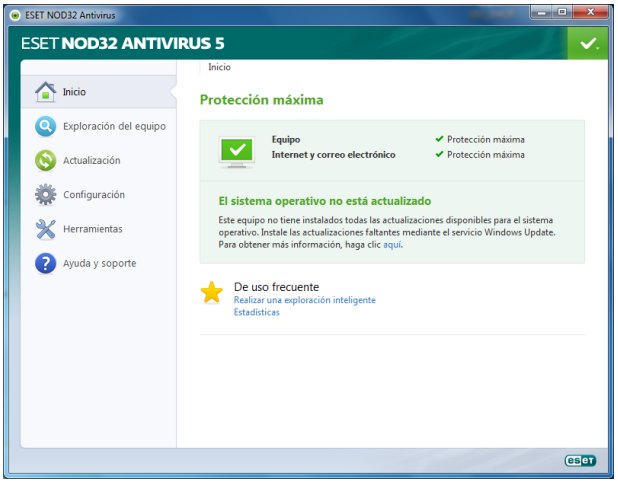


Esperamos a la finalización de la instalación.

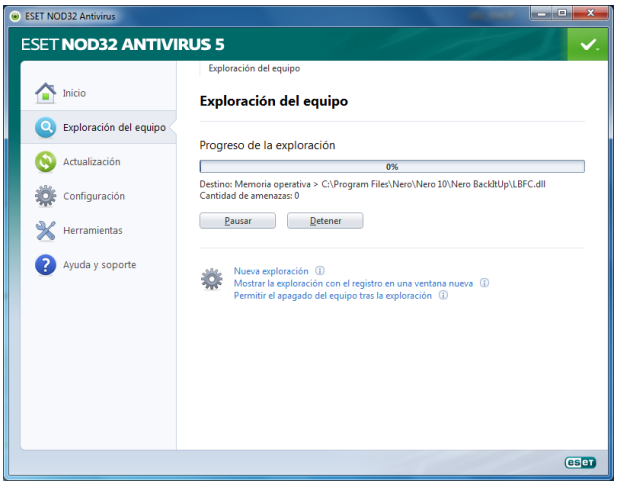


Finalizamos la instalación, (deberemos reiniciar).

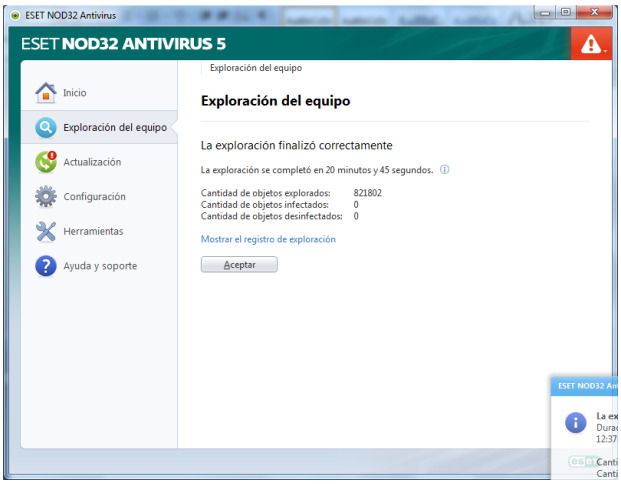
Arrancamos el antivirus y hacemos un análisis completo.



Comenzará el análisis del sistema.



Una vez terminado el análisis nos dará el siguiente resultado.



Avast

Una vez instalado este antivirus, vamos a hacer un análisis rápido del sistema, pulsamos dicha opción y esperamos a que termine la comprobación.

Una vez finalizado el análisis nos dará el siguiente resultado.

Tabla de resultados

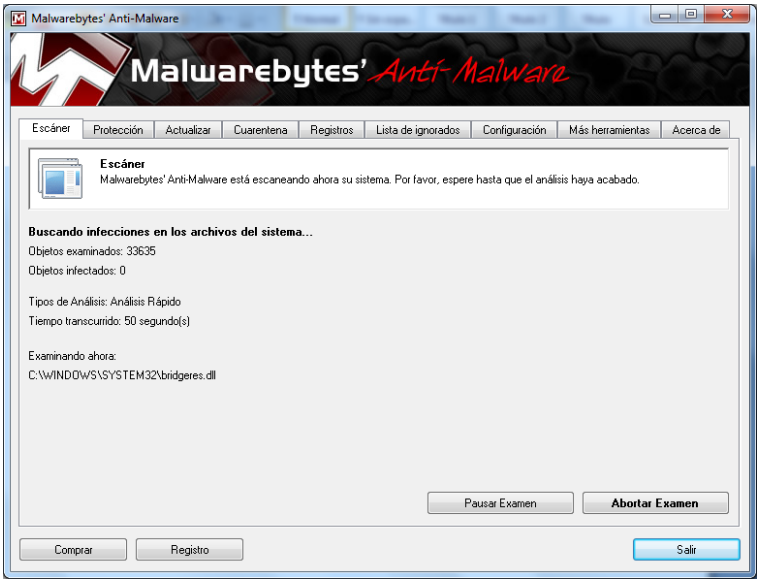
Antivirus:	Nº archivos analizados.	CPU en ejecución.	Opciones avanzadas de escaneo.	Tiempo de escaneo.	vulnerabilidades	virus encontrados	desinfectados
Nod 32	821802	50 %	Completo	20:45 min	0	0	0
Avast	25452	45 %	Rápido	5:05 min	0	0	0

F)

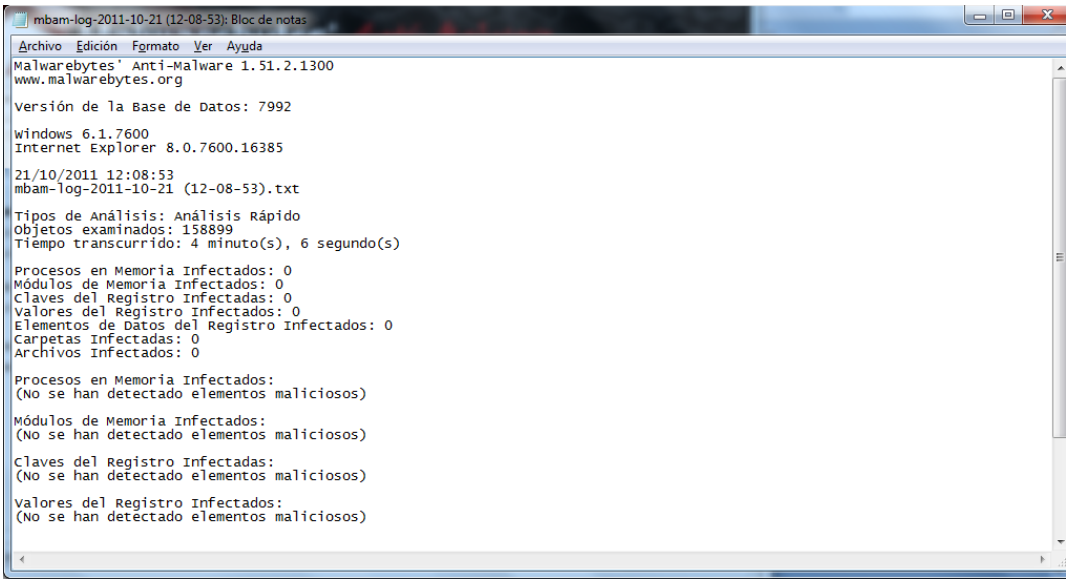
Análisis de dos antimalware locales

Antimalware

Una vez instalada esta aplicación, vamos a hacer un escáner rápido, para comprobar las amenazas de nuestro sistema.



Una vez finalizada la operación, nos mostrará el siguiente informe.



Una vez instalada la aplicación adware, vamos a hacer un análisis completo. Esperamos a que concluya la operación.

Una vez finalizada la comprobación nos dará el siguiente resultado.

Tabla de resultados

Antivirus:	Nº archivos analizados.	CPU en ejecución.	Opciones avanzadas de escaneo.	Tiempo de escaneo.	vulnerabilidades	virus encontrados	desinfectados
Malware	158899	40 %	Rápido	4:06 min	0	0	0
Adware	139886	45 %	Completo	18:54 min	0	0	0

TEMA 1 PRÁCTICA 6: SEGURIDAD FÍSICA Y AMBIENTAL

A)

Estudio de la ubicación y protección física de los equipos y servidores de la clase.

Para obtener una mayor protección y seguridad de la clase podemos instalar o promover los siguientes elementos de seguridad:

a) Acondicionamiento físico.

Debemos estar preparados para cualquier situación que afecte al acondicionamiento físico de la clase, como por ejemplo, estar preparados ante un incendio, que puede dañar seriamente la integridad de nuestros equipos y servidores.

Para poder eliminar efectivamente un pequeño incendio en la clase, podemos usar un extintor de CO_2 o de nieve carbónica.

Los EXTINTORES DE CO2 son apropiados para incendios en equipos delicados ya que los estropean menos que otros agentes extintores, pero son menos eficaces que los extintores de polvo.

Además de protegernos contra incendios, debemos controlar la temperatura o clima de la clase, para que el rendimiento y mantenimiento de nuestros equipos sean los adecuados. Para que esto sea posible, podemos utilizar el siguiente aparato acondicionador.

Big es el climatizador pensado para locales pequeños. Ideal para locales comerciales y aulas, pero también para la instalación en grandes ambientes residenciales, Big responde a todos los criterios de la climatización moderna: potente, eficiente, sencillo y de aspecto lineal.

Debemos tener un generador eléctrico autónomo para casos de cortes de luz repentinos, que impidan la realización normal de las tareas o incluso produzcan pérdidas de datos o daños en los sistemas, para esta situación utilizaremos el siguiente generador eléctrico.

-Motores Distribucion OHV y OHC 4 tiempos.

-Gran depósito para mayor autonomía.

- Chasis completo para mayor protección del equipo.

-Alternador AVR para mejor calidad de corriente.

-Gran escape para reducir nivel sonoro.

-Alarma de aceite en el motor.

-Doble chasis para reducir las vibraciones.

-Panel de control con: 2 tomas de corriente, salida DC 12 V, voltímetro digital, disyuntor diferencial, cuenta horas digital, arranque automático.

-Refrigeración por aire forzado.

Y como no debemos disponer de un armario Rack para evitar el contacto físico con los routers y switches de las personas no deseadas, podemos usar el siguiente armario rack.

Esto permite, además de proteger físicamente los routers y switch, permite refrigerarlos y reducir el ruido producido por tales elementos.

b) Robo o Sabotaje

Este es un punto muy importante a tener en cuenta, ya que supone la protección del robo de nuestros datos, o incluso de nuestras máquinas físicas. Algunos tipos de protección que podemos sugerir son los siguientes:

Debemos controlar quién entra a nuestro complejo y quien no, haciendo referencia las horas que dichos usuarios hacen entrada al centro y a qué departamento pertenecen.

Para hacer un control exhaustivo podemos utilizar un control mediante tarjetas de seguridad como el siguiente.

Son elemento caros, pero eficaces a la hora de proteger información importante.

También podemos utilizar un sistema de acceso biométrico para comprobar las huellas dactilares que permiten el acceso al medio, de forma rápida y eficaz.

Ésta técnica evita el uso de contraseñas complejas. Podemos usar un dispositivo de escáner facial en sustitución de esta técnica.

Podemos contratar a personal para la vigilancia del centro, realizando diversos turnos, en las horas adecuadas de no uso o inclusive para proteger el lugar.

Por último debemos disponer de diferentes cámaras de seguridad para controlar, las distintas zonas a proteger. Que puede estar controlada, por vigilantes, o por empresas encargadas de la seguridad de los complejos.

c) Condiciones atmosféricas y naturales adversas

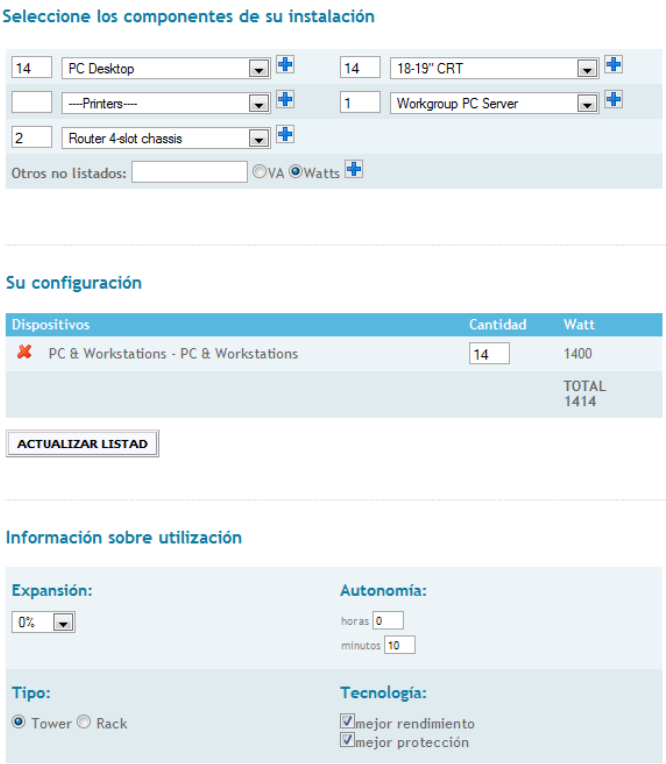
Para evitar estas amenazas o por lo menos reducir el daño, debemos hacer en todo momento copias de seguridad o copias de respaldo para no perder información de nuestros sistemas, podemos instalar también elementos preventivos, a la hora de suceder alguna anomalía, por ejemplo, un detector de incendios.

Para poder acabar con un incendio inesperado antes de que los daños sean irreparables.

B)

Busca un único SAI para todos los sistemas informáticos del aula.

Para comprobar el SAI adecuado a nuestro escenario vamos a hacer el siguiente cálculo:



El resultado con el SAI recomendado es el siguiente:

Mejor inversión

Sentinel Dual (High Power) - SDL

SDL 8000

Tecnología:
Puissance: 6400W / 8000VA

Autonomía: 40 min

% máximo de utilización: **22%**

Características

• posibilidad de instalación en suelo (versión torre) o en armario (versión rack) simplemente extrayendo y rotando el sinóptico (con la llave suministrada)
• tensión filtrada, estabilizada y fiable (tecnología On Line a doble conversión (VFI según normativa EN50091-3) con filtros para la supresión de las perturbaciones atmosféricas
• Nivel de ruido audible muy reducido (<40dBA): permite la instalación sobre cualquier ambiente gracias al control digital PWM del sistema de ventilación dependiendo de la carga aplicada y del uso de la tecnología de alta frecuencia de conmutación en el inversor (>20kHz, valor superior al umbral audible)
• posibilidad de conexión a by-pass externo de mantenimiento con conmutación sin interrupciones (modelos DLD500-600)
• El usuario puede seleccionar los siguientes modos de funcionamiento:
–Active Mode para aumentar el rendimiento (hasta el 98%)
– Economy Mode: permite seleccionar la tecnología Line Interactive (VI), solo se trabaja con el inversor en caso de fluctuaciones de la red, alimentar la carga directamente, para cargas poco sensibles. La función es programable mediante software o planteada manualmente desde el SAI
– Smart Active: El SAI decide de manera autónoma la modalidad de funcionamiento (VI ó VFI) en base a la calidad de la red
– Relevador: El SAI puede ser seleccionado para funcionar solo con la red ausente (modalidad aconsejada para luces de emergencia)
• conversión de frecuencia 50 o 60 Hz
• tensión de salida seleccionable (220-230-240V) monofase o (380-400-415) trifase

• auto encendido al retorno de la red, programable desde el panel manual o mediante software PowerShield³
• auto apagado cuando no hay presencia de cargas conectadas
• by-pass activado, cuando se apaga el SAI se predispone automáticamente el funcionamiento a través de by-pass
• pre-alarma de fin de descarga de batería
• permite la programación de un tiempo de demora (delay), tras el encendido
• tensión filtrada, estabilizada y segura (tecnología On Line doble conversión (VFI según normativa EN50091-3) con filtros EMI para la supresión de las perturbaciones atmosféricas
• en los modelos de 5 y 6 kVA además es posible programar dos tomas de salida de 10A (función Power-Share) en casos de ausencia de la alimentación de red

Si por el contrario si queremos tener un control de SAI independiente en vez de uno unitario, podemos optar por la siguiente opción:

Su configuración

Potencia total: **101 WATT**
Expansión : **0** %
Tipo : **TOWER**
Autonomía : **0h 10min**

Mejor precio

iDialog - IDG

IDG 1200

Tecnología: ONLINE
Puissance: 660W / 1100VA

Autonomía: 29 min

% máximo de utilización: **15%** 

Características

Máxima fiabilidad en la protección de ordenadores gracias también al software de supervisión y shutdown PS3, que se puede descargar gratuitamente desde la página web www.riello-ups.com.
Se puede instalar en PCs con sistema operativo Windows 7, 2003, Xp, 2000, Me, 98; Linux, Mac OSX y Sun Solaris.

Gracias a sus reducidas dimensiones, iDialog con su forma compacta puede colocarse en cualquier lugar del escritorio o del entorno doméstico.

La mejor opción en mi opinión es la primera, ya que es mucho más barato a la hora de comprar máquinas, optimización de espacio y cables y en la optimada duración de alimentación.