CUADERNO DE EVALUACIÓN

INTERNET SEGURO

CUADERNO DE EVALUACIÓN

INTERNET SEGURO

Nombre y Apellidos: DNI:	Firma:

Instrucciones: Cumplimente la prueba de evaluación, sin olvidar incluir sus datos personales y firma, a la finalización del curso. Señale la respuesta correcta rellenando o coloreando la casilla. ¡Suerte!

Ejemplo: ~~a~~ | b | c | d

1.	a	b	c	d
2.	a	b	c	d
3.	a	b	c	d
4.	a	b	c	d
5.	a	b	c	d
6.	a	b	c	d
7.	a	b	c	d
8.	a	b	c	d
9.	a	b	c	d
10.	a	b	c	d
11.	a	b	c	d
12.	a	b	c	d
13.	a	b	c	d
14.	a	b	c	d
15.	a	b	c	d
16.	a	b	c	d
17.	a	b	c	d
18.	a	b	c	d
19.	a	b	c	d
20.	a	b	c	d
21.	a	b	c	d
22.	a	b	c	d
23.	a	b	c	d
24.	a	b	c	d
25.	a	b	c	d
26.	a	b	c	d
27.	a	b	c	d
28.	a	b	c	d
29.	a	b	c	d
30.	a	b	c	d
31.	a	b	c	d
32.	a	b	c	d
33.	a	b	c	d
34.	a	b	c	d
35.	a	b	c	d
36.	a	b	c	d

37.	a	b	c	d
38.	a	b	c	d
39.	a	b	c	d
40.	a	b	c	d

1. Los programas antivirus:

a) Representan un sistema de seguridad completo.

b) Son muy eficaces detectando y eliminando virus, pero deben ser complementados con otras herramientas.

c) Solo son necesarios cuando el equipo en cuestión es infectado.

d) No son necesarios, puesto que los virus son cosas del pasado.

2. Un equipo con una instalación “limpia” del sistema operativo:

a) Puede infectarse una vez que es conectado a la red.

b) Puede infectarse al conectar una memoria externa, aun sin estar conectado a la red.

c) No incluye antivirus por defecto.

d) Las opciones a y b son correctas.

3. Un equipo puede estar infectado por un virus informático si presenta el siguiente síntoma:

a) El equipo no puede ejecutar programas que requieren muchos recursos.

b) El equipo no se enciende.

c) Emergen ventanas con publicidad pornográfica.

d) El navegador se queda “colgado”.

4. Respecto a Windows Defender para Windows 10:

a) Ofrece protección a tiempo parcial.

b) Ofrece protección en tiempo real.

c) Ofrece protección en tiempo completo.

d) Ofrece protección en tiempo diferido.

5. Indica cuál es la principal característica de los virus de tipo troyano:

a) Ofrecer servicios al usuario.
b) Replicarse masivamente.
c) Engañar al usuario.
d) Eliminar otro tipo de virus.

6. El virus SASSER aprovechaba una vulnerabilidad que desbordaba el buffer del componente:

a) LASSS.
b) SSASL.
c) SASSL.
d) LSASS.

7. Los cortafuegos pueden estar conectados a:

a) Una VPN.
b) Una DMZ.
c) Un servidor proxy.
d) Todas las opciones son incorrectas.

8. Indica a qué puerto se realizan las peticiones del protocolo HTTP:

a) 20.
b) 23.
c) 443.
d) 80.

9. Señala cuál de las siguientes es una de las limitaciones de un cortafuegos:

a) Filtrar el tráfico de la red.
b) Prevenir ataques en la red externa.
c) Permitir o bloquear el tráfico en determinados puertos lógicos.
d) Prevenir ataques en la red interna.

10. Podemos habilitar el cortafuegos del sistema mediante el siguiente comando en consola del sistema:

a) netsh advfirewall set currentprofile state on.
b) netsh advfirewall set currentprofile state off.
c) netsh advfirewall reset.
d) Ipconfig.

11. Indica cuál de las siguientes afirmaciones sobre las cookies de navegación no es correcta:

a) Son introducidas por usuarios maliciosos.
b) Permiten agilizar la navegación.
c) Cada servidor web puede contar con sus propias cookies.
d) Pueden ser eliminadas del equipo cuando el usuario lo desee.

12. Respecto a Antimalware Bytes:

a) Es una potente herramienta de seguridad.
b) Es un peligroso virus.
c) Es un peligroso espía.
d) Es un potente cortafuegos.

13. Indica cuál es la táctica que seguía Evidence Eliminator para convencer a los usuarios:

a) Intimidarlos.
b) Convencerlos.
c) Ofrecer una versión gratuita permanente.
d) Amenazarlos.

14. Antimalware Bytes ofrece los siguientes tipos de análisis:

a) Rápido.
b) Personalizado.
c) Completo.
d) Todas las opciones son correctas.

15. ¿Cuál de los siguientes antiespías es recomendable usar?

a) Ad-Aware.
b) Super Terminator.
c) Spyware Aware.
d) Super Aware.

16. Indica cuál no es una ventaja del marketing tradicional:

a) Ideal para las grandes compañías.
b) Ideal para las pequeñas compañías.
c) Llega a casi todo tipo de público.
d) Mueve masas.

17. Indica en qué año redactó Bill Gates un memorándum en el que Microsoft se comprometía a mejorar la seguridad en sus sistemas operativos:

a) 2000.
b) 2001.
c) 2002.
d) 2003.

18. ¿Cuál de las siguientes opciones no está disponible en Windows Update?

a) Buscar actualizaciones.
b) Eliminar actualizaciones.
c) Cambiar horas activas.
d) Ver historial de actualizaciones.

19. Mantener constantemente actualizado el sistema operativo y Windows Defender sirve, entre otras cosas, para:

a) Contar con mejoras de interfaz.
b) Contar con las últimas actualizaciones de seguridad.
c) Poder instalar nuevas aplicaciones.
d) Ralentizar el sistema.

20. ¿Cuál de los siguientes navegadores web no es un navegador alternativo a Microsof Edge?

a) Google Chrome.
b) Mozilla Firefox.
c) TunnelBear.
d) Opera.

21. Para facilitar a los usuarios una navegación segura y prevenirlos de amenazas, los desarrolladores de navegadores web incluyen en sus navegadores:

a) Funciones de reproducción de vídeo.
b) Funciones de reducción de consumición de recursos.
c) Funciones para las redes sociales.
d) Funciones de seguridad.

22. Indica cuál de los siguientes tipos de certificados digitales no ha sido visto en el temario:

a) Certificado de persona física.
b) Certificado de representante.
c) Certificado de administración pública.
d) Certificado de persona virtual.

23. Cuando hablamos de un dispositivo que nos permite almacenar certificados digitales y cifrar claves públicas y privadas sin necesidad de componentes hardware adicionales, nos referimos a:

a) Tarjeta criptográfica.
b) DNI electrónico.
c) Token USB.
d) Firma digital.

24. Un ataque que, de forma distribuida, pretende consumir los recursos de un servidor y/o saturar la red a la que está conectado es un ataque de tipo:

a) DoS.
b) DDoS.
c) DoSS.
d) DDoSS.

25. Indica cuál de los siguientes es un método de certificación de correo:

a) HTTP y HTTPS.
b) SSL y TLS.
c) SLS y TSL.
d) SFTP y MLP.

26. Cuando nos encontramos en un entorno de trabajo seguro y necesitamos enviar un correo electrónico de forma anónima, se recomienda usar:

a) Una cuenta de correo anónima.
b) Una red VPN.
c) Una cuenta de correo temporal.
d) Un servidor proxy.

27. Cuando nos encontramos en un entorno de trabajo NO seguro y necesitamos enviar un correo electrónico de forma anónima, se recomienda usar:

a) Una red VPN.
b) Una cuenta de correo temporal.
c) Una cuenta de correo anónima.
d) Un servidor proxy.

28. Una de las principales características de Hushmail es:

a) Ser versión gratuita.
b) Ofrecer cuentas de correo temporales.
c) La mensajería instantánea.
d) El uso de cifrado PGP.

29. Las redes que permiten a sus usuarios intercambiar información a una velocidad potencialmente superior a la que ofrecen los prestadores de servicio de alojamiento son redes:

a) VPN.
b) P2D.
c) De intercambio.
d) P2P.

30. En las redes de pares es crucial, por encima de otros aspectos, contar con un:

a) Antivirus propiamente configurado.
b) Cortafuegos propiamente configurado.
c) Antiespía propiamente configurado.
d) Todas las opciones son correctas.

31. Debido a que en ocasiones es posible rastrear la información de los usuarios de las redes de pares, estos prefieren:

a) Velocidad sobre anonimato.
b) Anonimato y velocidad.
c) Anonimato sobre velocidad.
d) No utilizar este tipo de redes.

32. Indica cuál de las siguientes opciones no corresponde a un tipo de clasificación según la topología de las redes P2P:

a) Descentralizadas.
b) Puras.
c) Híbridas.
d) Centralizadas.

33. La última versión disponible en la actualidad de Microsoft Baseline Security Analyzer es:

a) 2.1.
b) 2.1.1.
c) 2.2.
d) 2.3.

34. Indica cuál de las siguientes no es una herramienta de análisis de archivos online o basado en la nube:

a) MetaDefender.
b) VirusTotal.
c) CCleaner.
d) Panda Cloud Cleaner.

35. Los sistemas operativos, en esencia, son programas y como tal…

a) … no se encuentran exentos de bugs y/o exploits.
b) … se encuentran exentos de bugs y/o exploits.
c) … no necesita ser ejecutado.
d) … no consume recursos.

36. Indica cuál de las siguientes no es un tipo de copia de seguridad:

a) … no están conectados a internet.
b) … el sistema operativo no está correctamente actualizado.
c) … se configuran de forma específica.
d) … el sistema operativo no es Windows.

37. Según las pautas de seguridad a la hora de establecer contraseñas estudiadas, indica cuál de las siguientes contraseñas es más segura:

a) Creciente.
b) Completa.
c) Parcial.
d) Incremental.

38. Entre otros motivos, Linux se considera de los sistemas operativos más seguros debido a que…

a) “123456789”.
b) “Antonio90@”.
c) “Antonio90@Lopez&Baloncesto!”.
d) “AntonioLopezGarcia90@”.

39. Cuando hablamos de seguridad en redes inalámbricas (wifi) una consideración muy importante a tener en cuenta, tanto en redes domésticas como empresariales, es…

a) … nadie usa Linux y por lo tanto no es un objetivo para los hackers.
b) … es solo para usuarios avanzados.
c) … cuenta con el respaldo de Microsoft.
d) … es de código abierto y sus usuarios contribuyen a mejorarlo.

40. Cuando hablamos de seguridad en redes inalámbricas (wifi) una consideración muy importante a tener en cuenta, tanto en redes domésticas como empresariales, es…

a) … cambiar las contraseñas que vienen establecidas por defecto.
b) … cambiar el nombre de la red wifi para poder identificarla fácilmente.
c) … mantener las contraseñas establecidas por defecto, puesto que son las más seguras.
d) … dejar claro a los vecinos que no pueden conectarse a nuestra red wifi.