1) ¿Qué propiedad de la firma digital garantiza que el mensaje no ha sido modificado?

a) Autenticación.

**b) Integridad.**

c) No repudio.

d) Confidencialidad.

2) ¿Cómo se llama la fase inicial en la que se negocia el algoritmo de cifrado a usar en una conexión SSL/TLS?

a) Fase de despedida.

b) Fase de negociación.

c) Fase de intercambio de claves.

**d) Fase de saludo.**

3) ¿Qué tipo de firma digital permite detectar cualquier cambio posterior de los datos firmados y se genera mediante un dispositivo seguro de creación de firma?

a) Avanzada.

b) Ordinaria.

c) Con árbitro.

**d) Reconocida.**

4) ¿Cómo se denomina el mecanismo que permite consignar el momento exacto en que se ha realizado la firma?

a) Sincronismo de tiempo.

b) Estampado de hora.

**c) Sellado de tiempo.**

d) Ninguna de las respuestas es correcta.

5) ¿Cuál de las siguientes es una autoridad de certificación española?

a) VeriSign.

**b) FNMT.**

c) Comodo.

d) Thawte.

6) ¿Qué acción debe realizarse para comprobar la validez de un certificado?

a) Validarlo en la web de la autoridad de certificación que lo ha firmado.

b) Mirar si la fecha actual es mayor que la de caducidad del certificado.

**c) Verificar la firma de la autoridad que ha firmado el certificado.**

d) No ha de realizarse ninguna acción.

7) ¿Cómo se llama el sistema que permite el intercambio de claves en SSL/TLS?

a) RSA.

**b) Diffie-Hellman.**

c) DSA.

d) ElGamal.

8) ¿Qué requisito es necesario para poder comprobar la autenticidad de un certificado?

a) Tener actualizado el navegador.

b) Usar Mozilla Firefox.

**c) Tener instalado el certificado de la AC raíz en el navegador.**

d) Ninguna de las respuestas es correcta.

9) ¿Cuál de los siguientes es un elemento hardware necesario para usar el DNIe?

a) Teclado QWERTY.

**b) Lector de tarjetas inteligentes.**

c) Ratón.

d) Lector de CD-ROM.

10) Bitlocker es un ejemplo de...

a) Cortafuegos.

**b) Tecnología de cifrado de disco para Windows.**

c) Antivirus.

d) Sistema de firma digital.

11) ¿Cuál de las siguientes opciones constituye un ejemplo de denegación de servicio?

a) Un empleado instala a propósito en un equipo de la empresa un programa que genera tráfico basura y consume mucho ancho de banda, impidiendo que el resto de usuarios de la red ejerza un uso normal de la misma.

b) Juan ejecuta un archivo adjunto en un correo que, sin saberlo, instala un programa malicioso que afecta al funcionamiento del servidor de correo de ese equipo.

c) Un atacante que controla un gran número de equipos informáticos realiza un ataque coordinado contra un servidor web para detener su funcionamiento.

**d) Todas las opciones anteriores son ejemplos de denegación de servicio.**

12) ¿Cuál de las siguientes opciones es cierta?

a) Un espécimen de software malicioso puede realizar más de una acción dañina, como capturar las pulsaciones del teclado y utilizar técnicas para permanecer oculto respecto al sistema.

b) Ransomware es un tipo de software malicioso que cifra archivos del disco duro para exigir el pago de dinero.

c) Una bomba lógica es un tipo de software malicioso que se pone en funcionamiento cuando se cumple alguna condición.

**d) Todas las respuestas son ciertas.**

13) ¿Qué es un virus?

a) Un tipo de software malicioso que puede duplicarse por sí mismo sin necesidad de infectar otros archivos.

**b) Un tipo de software malicioso que se propaga infectando otros ficheros.**

c) Un tipo de software malicioso que muestra a los usuarios publicidad de forma intrusiva.

d) Un tipo de software malicioso que parece un programa inofensivo pero que ocasiona daños cuando se ejecuta.

14) ¿Cómo se denomina un programa que parece inofensivo pero que permite a otro usuario controlar nuestro equipo de forma remota?

a) Gusano.

**b) Troyano.**

c) Rogueware.

d) Rootkit.

15) Si recibimos un mensaje de texto en nuestro teléfono que indica que se ha bloqueado nuestra tarjeta de crédito y que tenemos que visitar una página web para desbloquearla, es probable que estemos siendo víctimas de una técnica de suplantación de identidad conocida como...

a) Pharming.

b) Vishing.

**c) SMiShing.**

d) Grooming.

16) Nuestro equipo será más vulnerable si...

a) El sistema operativo no se actualiza periódicamente.

b) El navegador y los plugins que utiliza no están actualizados.

c) No actualizamos los programas que instalamos en él.

**d) Todas las respuestas son correctas.**

17) ¿Cuál de las siguientes opciones es verdadera?

a) Todo software malicioso realiza acciones consideradas dañinas o perjudiciales.

b) Según el impacto producido en la víctima diferenciamos entre especímenes que se instalan de forma automática y especímenes que necesitan la intervención del usuario.

c) Según las acciones que realiza un virus distinguimos entre virus automático y virus residente.

**d) Algunas variedades de software malicioso pueden realizar más de una acción.**

18) ¿Cómo se podrían disminuir los fraudes informáticos derivados de las cadenas de correos electrónicos?

a) Evitando reenviar el correo en cualquier caso.

b) Reenviando el correo íntegramente solo a algunos amigos.

**c) Utilizando, en caso de que se decida reenviar el correo, la copia oculta (campo CCO) y eliminando la lista de remitentes anteriores.**

d) Reenviando el correo recibido a todos los contactos conocidos.

19) ¿Cuál de las siguientes afirmaciones sobre el correo electrónico no deseado y el correo basura o spam es cierta?

a) Es más fácil detectar el correo electrónico no deseado que el correo basura o spam.

**b) Es más fácil detectar el correo basura o spam que el correo electrónico no deseado.**

c) Un correo electrónico que anuncia un producto para prevenir el envejecimiento de la piel enviado a personas que no han solicitado recibir ese tipo de información se considera correo electrónico no deseado.

d) Ninguna de las respuestas es cierta.

20) ¿Cuál de las siguientes afirmaciones acerca de la ingeniería social aplicada a la informática es cierta?

a) El correo electrónico es tal vez el medio más utilizado por los estafadores, aunque no el único.

b) Los piratas informáticos suelen utilizar técnicas de ingeniería social para suplantar la identidad de las víctimas.

c) Los correos electrónicos masivos son considerados otra técnica de ingeniería social.

**d) Todas las opciones anteriores son ciertas.**

21) ¿Cuál de las siguientes afirmaciones sobre suites de seguridad corporativas es cierta?

a) Permiten que un equipo se descargue la última versión del motor y la base de firmas y que el resto de equipos se la descarguen de aquel, pero no permiten analizar otro equipo de la red.

b) Constituyen la solución más adecuada para todas las situaciones, incluso para un solo equipo.

**c) Permiten obtener información relativa a software malicioso detectado o eliminado en los clientes de la red.**

d) Todas las respuestas son ciertas.

22) Si recibimos un correo electrónico de un desconocido con un archivo adjunto que forma parte de una cadena de correos, ¿qué deberíamos hacer?

a) Pasar el antivirus al archivo adjunto para estar seguros de que no es peligroso y poder así ver su contenido.

**b) Ignorar el correo electrónico.**

c) Reenviar el correo a todos nuestros conocidos utilizando la copia oculta.

d) Reenviar el correo a todos nuestros conocidos utilizando la copia oculta y borrando la lista de correos originada por reenvíos previos.

23) ¿Cuál de las siguientes medidas no contribuye a protegerse contra el malware?

**a) Facilitar datos personales, como claves, por correo electrónico.**

b) Desactivar la interpretación de Visual Basic Script.

c) Actualizar periódicamente el sistema operativo y las aplicaciones críticas.

d) Mantenerse actualizado visitando periódicamente páginas web de información o suscribiéndose a boletines de seguridad.

24) ¿Qué es una copia de seguridad?

**a) Una medida de seguridad paliativa que consiste en guardar una parte o toda la información del sistema con la intención de poder recuperarla en caso de pérdida de información.**

b) Un dispositivo software o hardware que forma parte de un equipo y está diseñado para protegerlo mediante el bloqueo de accesos no autorizados.

c) Un conjunto de programas de seguridad que contribuyen a la detección de software malicioso y, en muchos casos, a su desinfección.

d) Un tipo de software que permite guardar el estado del equipo en un momento determinado, para que, al volver a iniciarse el equipo, el estado se restaure automáticamente.

25) ¿Qué herramienta recomendarías emplear en un aula de informática donde se permite la utilización de USB y la instalación de programas, lo que puede ocasionar muchas infecciones por malware?

a) Un navegador actualizado.

b) Un cortafuegos muy restrictivo.

c) Un cortafuegos permisivo.

**d) Un software congelador.**

26) ¿Qué servicios ofrecen los centros de protección y respuesta ante amenazas?

a) Propagación de información relacionada con la seguridad.

b) Auditorías de seguridad.

c) Gestión de vulnerabilidades.

**d) Todas las respuestas son correctas.**

27) ¿Qué es una suite de seguridad?

a) Una medida de seguridad paliativa que consiste en guardar una parte o toda la información del sistema con la intención de poder recuperarla en caso de pérdida de información.

b) Un dispositivo software o hardware que forma parte de un equipo y está diseñado para protegerlo mediante el bloqueo de accesos no autorizados.

**c) Un conjunto de programas de seguridad que contribuyen a la detección de software malicioso y, en muchos casos, a su desinfección.**

d) Un tipo de software que permite guardar el estado del equipo en un momento determinado para que, al volver a iniciarse el equipo, el estado se restaure automáticamente.

28) ¿Qué es un cortafuegos?

a) Una medida de seguridad paliativa que consiste en guardar una parte o toda la información del sistema con la intención de poder recuperarla en caso de pérdida de información.

**b) Un dispositivo software o hardware que forma parte de un equipo y está diseñado para protegerlo mediante el bloqueo de accesos no autorizados.**

c) Un conjunto de programas de seguridad que contribuyen a la detección de software malicioso y, en muchos casos, a su desinfección.

d) Un tipo de software que permite guardar el estado del equipo en un momento determinado, para que, al volver a iniciarse el equipo, el estado se restaure automáticamente.

29) Tenemos un programa que requiere acceso a Internet y que utiliza un puerto TCP diferente cada vez que se ejecuta. ¿Cuál de los siguientes tipos de cortafuegos sería más adecuado utilizar y cómo lo configurarías?

a) Cortafuegos de filtrado de paquetes, permitiendo la entrada de paquetes que lleguen a cualquier puerto TCP.

b) Cortafuegos de filtrado de paquetes, permitiendo la salida de paquetes procedentes de cualquier puerto TCP.

**c) Cortafuegos de aplicación, permitiendo el acceso a esa aplicación.**

d) Ninguno de los anteriores.

30) ¿Qué debo hacer si sospecho que mi equipo está infectado por algún tipo de malware?

a) Escanear el equipo en busca de virus.

b) Restaurar el sistema a un estado anterior para eliminarlo.

c) Hacer copias de seguridad para evitar que ese malware elimine mis archivos importantes.

**d) Antes de realizar nada, identificar de qué tipo de malware se trata y cuál es su alcance.**

31) ¿Cuál de las siguientes afirmaciones sobre la tecnología RAID es cierta?

**a) No es apta para la recuperación de datos.**

b) Se considera una medida preventiva.

c) En caso de pérdida de datos en un disco, para recuperar los datos es suficiente con transferir la estructura y el contenido del disco.

d) Permite volver a un estado anterior del sistema para proceder a la recuperación.

32) ¿Cuál de las siguientes afirmaciones es falsa?

a) Para solucionar la necesidad de espacio de almacenamiento no siempre es recomendable ampliar el número de discos duros.

b) Existen distribuciones software que permiten transformar un equipo en servidor NAS.

c) La tecnología SAN es una red de área de almacenamiento.

**d) El almacenamiento en la nube ofrece balanceo de carga y tolerancia a fallos.**

33) ¿Qué se puede utilizar para recuperar los datos de un disco duro formateado por error?

**a) La herramienta GetDataBack.**

b) La restauración de la imagen del equipo que viene de fábrica.

c) Los puntos de restauración creados en Windows para recuperar cualquier sistema operativo que esté instalado.

d) Todas las respuestas con correctas.

34) El concepto de seguridad en sistemas de almacenamiento engloba:

a) Todas aquellas medidas que permitan mantener la información segura frente a fallos físicos

b) Todas aquellas medidas que permitan mantener la información segura frente a fallos lógicos

c) Protegerla de de accesos no autorizados

**d) Todas las anteriores son correctas**

35) ¿Qué implica una correcta gestión del almacenamiento de la información?

a) Saber cuánta capacidad se va a necesitar.

b) Conocer con qué frecuencia se va a utilizar.

c) Estudiar qué tecnología de almacenamiento será la más adecuada.

**d) Todas las respuestas son correctas.**

36) ¿Cuál de las siguientes aplicaciones utilizaremos para crear una imagen?

**a) Clonezilla.**

b) Rsync.

c) GetDataBack.

d) Los puntos de restauración.

37) ¿Cuál de las siguientes afirmaciones sobre la gestión de imágenes es verdadera?

a) El tipo de imagen que más se suele utilizar es el de tipo incremental.

b) La clonación en equipos solo puede realizarse si se trata de una clonación de disco a disco y estos son iguales en características.

**c) Si el equipo no arranca, su restauración a partir de una imagen es una solución.**

d) Si el equipo ni siquiera arranca, la restauración mediante una imagen no es una buena solución.

38) Si un amigo te comenta que quiere instalar drivers nuevos para la tarjeta gráfica, pero que teme que luego el equipo no funcione correctamente, ¿qué le recomendarías para que el equipo pueda volver a funcionar en caso de que la instalación no resulte como debería?

a) Que se instale y configure un NAS.

b) Que copie los datos en un almacenamiento en la nube.

**c) Que cree un punto de restauración, si está utilizando Windows como sistema.**

d) Ninguna de las respuestas es válida.

39) ¿Cuál de los siguientes niveles de RAID sería el más apropiado para un sistema que necesite un rendimiento alto y en el que no son muy importantes las pérdidas de datos?

**a) RAID 0.**

b) RAID 1.

c) RAID 5.

d) RAID 6.

40) ¿Cuál de las siguientes afirmaciones sobre copias de seguridad es cierta?

a) Las copias de seguridad en frío son aquellas que se hacen sobre ficheros abiertos y bases de datos sobre las que se está trabajando.

b) Las copias de seguridad en caliente son aquellas que se hacen sobre ficheros y bases de datos sobre las que no hay accesos.

c) No se permite realizar copias en caliente si se utilizan dispositivos de almacenamiento locales.

**d) Ninguna de las respuestas es cierta.**