1) ¿De qué tipo es el sistema que permite el intercambio de claves en SSL/TLS?

**a) Híbrido.**

b) Simétrico.

c) Asimétrico.

d) Ninguna de las respuestas anteriores es correcta.

2) ¿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.

3) En el proceso de firma digital de un documento, obtener el resumen del documento es...

a) El último paso.

b) El segundo paso.

**c) El primer paso.**

d) Un paso opcional.

4) ¿Qué medidas físicas de seguridad incluye el DNIe?

a) PIN.

b) Cifrado de los datos del chip.

**c) Relieves.**

d) Ninguna de las anteriores.

5) ¿Qué se recomienda a la hora de usar cifrado en una unidad de disco USB?

a) Utilizar siempre Linux.

**b) Crear un volumen o contenedor dentro del dispositivo.**

c) Que esté formateado en NTFS.

d) Que tenga un tamaño menor de 16 GB.

6) ¿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.**

7) ¿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.

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

a) VeriSign.

**b) FNMT.**

c) Comodo.

d) Thawte.

9) ¿Qué servicios proporciona la firma digital?

a) De autenticación.

b) De integridad.

c) De no repudio.

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

10) ¿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.**

11) 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.

12) ¿Cuál de las siguientes opciones contribuye a evitar los fraudes informáticos derivados de las cadenas de correos?

a) Desconfiar de los correos electrónicos de desconocidos.

b) Al reenviar masivamente un correo electrónico, eliminar las direcciones de correo a las que este se ha enviado previamente.

c) Al reenviar un correo a mucha gente, utilizar el campo de correo en copia oculta (campo CCO) en lugar del destinatario (campo Para).

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

13) ¿Qué es un gusano informático?

**a) Un tipo de software malicioso que se propaga automáticamente sin la intervención de los usuarios.**

b) Un tipo de software malicioso que necesita intervención humana para propagarse.

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 ocasiona daños al ser ejecutado.

14) ¿Cuál de las siguientes opciones es verdadera?

a) Un keylogger es un tipo de software malicioso que captura las pulsaciones de las teclas.

b) El hecho de descargar un programa de su página web oficial no garantiza que este no sea software malicioso.

c) Conviene desconfiar del software que circula por las redes P2P porque desconocemos su procedencia.

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

15) ¿Cuál de las siguientes afirmaciones sobre la denegación de servicio es verdadera?

a) Se produce solo en servidores web y servicios accesibles por la red.

**b) El hecho de que el personal de limpieza desconecte accidentalmente un equipo informático que está funcionando puede ser un ejemplo de denegación de servicio.**

c) Los ataques de denegación de servicio siempre provienen de una entidad ajena a la organización.

d) Todos los ataques de denegación de servicio se realizan mediante redes informáticas.

16) La página de inicio de nuestro equipo ha cambiado automáticamente. ¿Por qué variedad de software malicioso es probable que esté infectado?

a) Virus.

b) Gusano.

**c) Browser hijacker.**

d) Keylogger.

17) ¿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.**

18) ¿Cuál de las siguientes opciones constituye un ejemplo de ingeniería social aplicada a la informática?

a) La creación de una página web que imita el funcionamiento de la web de otro portal web para obtener las claves de acceso de los clientes.

b) El envío de un correo electrónico suplantando la identidad del banco y en el que se indica que se ha detectado un problema y que se debe llamar a un número de teléfono que aparece en el correo para solucionarlo con la mayor brevedad posible.

c) El envío de un correo electrónico en el que se indica que se ha ganado un premio (sin haber participado en ningún sorteo) y que tenemos que visitar un enlace que se nos facilita en el correo para recoger dicho premio.

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

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

a) Ambos son lo mismo.

b) Un correo electrónico que contiene publicidad de una empresa y que es enviado por un desconocido se considera correo no deseado, sin embargo si quien lo envía es un conocido que nos cae mal se considera correo basura o spam.

**c) El correo basura o spam es un tipo concreto de correo electrónico no deseado cuyos fines son publicitarios o económicos.**

d) El correo electrónico no deseado es un tipo concreto de correo basura o spam cuyos fines son publicitarios o económicos.

20) ¿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.

21) 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.

22) ¿Cuál de las siguientes medidas no contribuye a protegernos contra el malware en correos electrónicos?

a) Denunciar el correo abusivo o fraudulento informando al emisor del mensaje.

**b) Configurar el antivirus para que inspeccione el correo electrónico, ya que así estaremos seguros de que no hay ningún tipo de malware y podremos confiar en el contenido de los correos.**

c) Cuando reenviemos correos de forma masiva, borrar la lista de direcciones proveniente de reenvíos anteriores.

d) Utilizar la copia oculta al reenviar correos.

23) ¿Qué inconveniente puede presentar la utilización de software congelador para restaurar un equipo al mismo punto?

**a) Si el sistema se restaura al mismo punto, no se actualiza el sistema, por lo que será vulnerable a futuras amenazas.**

b) Este tipo de herramienta no es adecuado si se permite la utilización de dispositivos de almacenamiento externos.

c) Un usuario malintencionado no puede acceder a información previa a la sesión actual.

d) Se protege de las infecciones por software malicioso.

24) ¿Qué tipo de suite de seguridad será más adecuada en un entorno compuesto por 10 equipos?

a) Suite de seguridad personal.

**b) Suite de seguridad corporativa.**

c) Suite de seguridad compleja.

d) Suite de seguridad.

25) ¿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.

26) ¿De qué modo se puede estar informado de las últimas amenazas de malware y conocer las últimas incidencias de seguridad detectadas?

a) Activando las actualizaciones de la herramienta antimalware.

**b) Visitando los centros de protección y respuesta ante amenazas.**

c) Activando las actualizaciones del sistema operativo y el navegador web.

d) Todas las respuestas son correctas.

27) ¿Cuál de las siguientes medidas contribuye a protegerse del malware?

a) Diseñar políticas de contraseñas que incluyan contraseñas complejas.

b) No navegar por páginas web inseguras, sospechosas o que ofrezcan regalos o promociones dudosos.

c) Utilizar cuentas de usuario con privilegios limitados para el uso diario del equipo.

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

28) ¿Cuál de las siguientes afirmaciones sobre antivirus y suites de seguridad es cierta?

a) Se utilizan para denominar el mismo tipo de herramientas de seguridad.

**b) El término suite de seguridad engloba un conjunto de herramientas que protegen frente a diversos tipos de malware, como antivirus, antirootkits o antispyware, entre otros.**

c) Los antivirus ofrecen soluciones contra los virus y las suites de seguridad contra el resto de software malicioso.

d) Es mejor instalar un antivirus, ya que ofrece protección contra el tipo de malware más extendido: los virus.

29) ¿Cuál de las siguientes afirmaciones sobre los cortafuegos es cierta?

a) Los cortafuegos permiten o deniegan el tráfico en función de las reglas que deben cumplir los mensajes que pasan por ellos.

b) Los cortafuegos suelen definir una política por defecto que se aplica a aquellos mensajes que no cumplen las condiciones de ninguna regla.

c) Un cortafuegos correctamente configurado añade protección a la red o al equipo, pero debe combinarse con otras herramientas de protección.

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

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 aplicaciones utilizaremos para crear una imagen?

**a) Clonezilla.**

b) Rsync.

c) GetDataBack.

d) Los puntos de restauración.

32) ¿En cuál de las siguientes situaciones es interesante utilizar la gestión de imágenes?

**a) Cuando, tras instalar algún programa o actualización, el sistema empieza a funcionar de forma no deseada.**

b) Cuando es necesario recuperar los datos de un disco externo formateado.

c) Cuando, por culpa de un virus, se han borrado los datos del dispositivo de almacenamiento USB.

d) Ninguna de las respuestas es correcta.

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) Si alguien te comenta que teme perder las fotos de su familia que tiene almacenadas en un disco externo, ¿qué le recomendarías para mantener la integridad de la información?

**a) Que haga copias de seguridad periódicamente.**

b) Que se haga una imagen del disco y la guarde en un lugar seguro.

c) Que cree un punto de restauración mensualmente.

d) Ninguna de las respuestas es válida.

35) ¿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.**

36) ¿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.

37) ¿Se puede garantizar una buena gestión del almacenamiento de la información?

**a) Sí, siempre que se cumplan las normas de la política de almacenamiento.**

b) Sí, siempre que se mantenga la información alejada de accesos no autorizados.

c) Sí, siempre que se garantice una seguridad activa de la información.

d) Ninguna de las respuestas es correcta.

38) ¿Cuál de los siguientes niveles de RAID sería el más adecuado para un entorno doméstico en el que se necesita principalmente tolerancia a fallos?

a) RAID 0.

**b) RAID 1.**

c) RAID 5.

d) Las respuestas a y b son adecuadas.

39) ¿Qué hay que tener en cuenta para llevar a cabo un buen control sobre el amacenamiento de la información?:

a) Que se garantice una seguridad física

b) Que se garantice una seguridad lógica

c) Que se permite mantener la disponible, la integridad y la autenticidad de la información

**d) Todas las afirmaciones anteriores son correctas**

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

a) Las copias normales copian los archivos creados en el día.

b) Para datos muy cambiantes es recomendable hacer una copia de los mismos trimestralmente.

**c) La política de retención indica cuánto tiempo se va a conservar cada copia de seguridad.**

d) Podrá utilizarse el mismo tipo de copia tanto si se van a copiar bases de datos completas como ficheros ordinarios.