1) ¿Cuál es el primer paso que realiza un usuario en el proceso de solicitud de un certificado?

a) Generar una petición de certificado.

**b) Crear un par de claves.**

c) Firmar la solicitud.

d) Enviar la solicitud a la autoridad de certificación.

2) ¿En qué consiste la fase de saludo de SSL/TLS?

a) En intercambiar los nombres de las aplicaciones que se conectan.

b) En la presentación de los participantes en la comunicación.

**c) En el intercambio de claves públicas y la negociación del algoritmo de cifrado.**

d) En cifrar el tráfico con las claves intercambiadas previamente.

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

a) PIN.

b) Cifrado de los datos del chip.

**c) Relieves.**

d) Ninguna de las anteriores.

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

a) RSA.

**b) Diffie-Hellman.**

c) DSA.

d) ElGamal.

5) Bitlocker es un ejemplo de...

a) Cortafuegos.

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

c) Antivirus.

d) Sistema de firma digital.

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

a) Autenticación.

**b) Integridad.**

c) No repudio.

d) Confidencialidad.

7) ¿Qué permite el mecanismo timestamping?

a) Saber la hora que es.

**b) Conocer el momento exacto en que se realizó la firma.**

c) Conocer el momento exacto en que se comprobó la firma.

d) Ninguna de las respuestas es correcta.

8) ¿Qué tipo de firma digital permite detectar cualquier cambio posterior de los datos firmados?

**a) Avanzada.**

b) Ordinaria.

c) Con árbitro.

d) Ninguna de las anteriores.

9) ¿Qué contiene un certificado digital?

a) El nombre del suscriptor.

b) El nombre de la autoridad de certificación que emite el certificado.

c) El método de firma.

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

10) ¿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.

11) ¿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.**

12) 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.

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) Al recibir un correo de un amigo nos llama la atención que el asunto del correo esté en inglés (ya que este amigo nunca nos escribe en este idioma). Además el correo solo contiene un enlace para visitar una página web. ¿Qué debemos hacer?

**a) Avisar a nuestro amigo de que es posible que haya sido víctima de una técnica de suplantación y es probable que tenga que cambiar la contraseña.**

b) Visitar la página web que nos proporciona el correo.

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

d) Eliminar el correo sin avisar a nuestro amigo.

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) Si en un equipo aparecen muchas ventanas de publicidad, ¿por qué variedad de software malicioso podemos deducir que se encuentra infectado?

a) Virus.

b) Gusano.

**c) Adware.**

d) Keylogger.

17) ¿Cuál de las siguientes opciones es cierta?

**a) El adware es un tipo de software malicioso que suele considerarse no dañino.**

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

c) La finalidad del spyware siempre es conseguir información del usuario para hacerle daño, por lo que se le considera un tipo de software malicioso dañino.

d) Un ransomware es un programa que muestra al usuario un mensaje indicándole que se va a formatear el disco duro sin que esto llegue a producirse.

18) ¿Qué es un troyano?

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 que ocasiona daños cuando se ejecuta.**

19) ¿Cuál de las siguientes afirmaciones sobre el correo electrónico basura o spam es cierta?

a) Nunca tiene una intención comercial.

**b) Es un tipo de correo electrónico no deseado.**

c) Un correo electrónico que contiene una foto de un perrito jugando al futbol y que es enviado por un desconocido no se considera correo basura o spam, sin embargo sí se considera tal si se envía a 1000 personas.

d) Todas las opciones son ciertas.

20) ¿Cuál de las siguientes opciones es falsa?

a) Un rootkit es un tipo de software malicioso que utiliza técnicas para permanecer oculto respecto al sistema.

**b) El hecho de descargar un programa de la página web oficial garantiza que este no es software malicioso.**

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

d) Algunas variedades de malware utilizan el correo electrónico para propagarse.

21) ¿Cuál de las siguientes afirmaciones es cierta?

a) Las copias de seguridad permiten evitar infecciones de virus y malware.

b) Las copias de seguridad permiten evitar que nuestro equipo se infecte al navegar por Internet.

**c) Las copias de seguridad permiten minimizar el impacto ocasionado por el malware.**

d) Las copias de seguridad contribuyen a la desinfección de malware del equipo.

22) ¿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.

23) ¿Por qué se dice que no existe una solución mágica ante una infección o incidente de seguridad?

a) Porque no existe ninguna herramienta antimalware que elimine todas las variedades de malware.

**b) Porque las medidas que se adoptan para desinfectar un equipo difieren según las diversas variantes y especímenes de malware de que se trate y, además, lo más común no siempre resulta efectivo.**

c) Porque debemos utilizar una herramienta distinta para eliminar correctamente cada infección o incidente de seguridad.

d) Porque conviene instalar muchas herramientas de detección y corrección de malware diferentes para tener un equipo seguro.

24) ¿Qué herramienta utilizarías para bloquear accesos no autorizados a tu equipo?

**a) Cortafuegos.**

b) Copias de seguridad.

c) Software congelador.

d) Antispyware.

25) ¿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.**

26) ¿Cuál de los siguientes servicios no se ofrecen en un centro de protección y respuesta ante amenazas?

a) Propagación de herramientas para eliminar malware.

b) Análisis de vulnerabilidades detectadas y de incidentes de seguridad.

c) Avisos de seguridad.

**d) Ninguno de los anteriores.**

27) ¿Qué tipo de cortafuegos permite bloquear y permitir el tráfico que llega a un equipo informático?

a) Cortafuegos perimetral.

b) Cortafuegos de red.

**c) Cortafuegos de host.**

d) Cortafuegos individual.

28) ¿Cuál de las siguientes medidas contribuye a protegernos contra el malware en correos electrónicos?

a) Configurar el correo para que compruebe los mensajes.

b) No reenviar mensajes que formen parte de cadenas.

c) No hacer clic en los enlaces que aparecen en un correo electrónico que procede de una fuente que no es de confianza.

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

29) ¿Qué nombre recibe el conjunto de herramientas que contribuye a prevenir las infecciones por malware y a desinfectar los equipos infectados?

**a) Suite de seguridad.**

b) Programas de control parental.

c) Cortafuegos.

d) Copias de seguridad.

30) ¿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.

31) 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**

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

**a) Clonezilla.**

b) Rsync.

c) GetDataBack.

d) Los puntos de restauración.

33) ¿Cuál de las siguientes afirmaciones sobre los puntos de restauración creados con Windows es correcta?

a) Se utilizan para restaurar el equipo cuando el sistema operativo no arranca.

**b) Uno de los inconvenientes que presenta su uso es la cantidad de espacio que se necesita para almacenar los puntos.**

c) Se deben crear puntos de restauración diariamente para su óptima utilización.

d) Ninguna de las afirmaciones es correcta.

34) ¿Cuál de las siguientes afirmaciones sobre RAID 5 es correcta?

a) Necesita dos discos, por tanto la información almacenada se duplica de un disco al otro.

**b) Se puede implementar con tres discos, entre los cuales se reparte en bandas la información.**

c) Su funcionamiento es similar al de RAID 1.

d) Recibe también el nombre de disk mirroring.

35) ¿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.

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

**a) Tener unas normas redactadas que indiquen cómo preservar la información.**

b) Conocer y detallar qué técnica de seguridad activa es la más adecuada para preservar la información.

c) Conocer y detallar qué técnica de seguridad pasiva es la más adecuada para preservar la información.

d) Tan solo mantener la información almacenada de forma segura ante fallos físicos.

37) Si un amigo te comenta que posee mucha información y que le gustaría disponer de un sistema que le permitiera, en caso de fallo del disco, recuperar la información de manera rápida y en cualquier situación, ¿qué le recomendarías en primer lugar?

**a) Que se compre otro disco y configure un sistema RAID 1.**

b) Que cree una imagen al instalar el sistema operativo.

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

d) Que cree un punto de restauración.

38) ¿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.**

39) ¿Cuál de los siguientes métodos no se corresponde con un método de recuperación de datos?

a) Gestión de imágenes.

b) Copia de seguridad.

**c) Tecnología NAS.**

d) Utilización de puntos de restauración.

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.**