1) ¿Qué se creó para solucionar el problema de la confianza en la clave pública de un usuario?

a) Las funciones hash.

b) Las listas blancas.

**c) Los certificados digitales y las autoridades de certificación.**

d) Ninguna de las respuestas es correcta.

2) ¿Qué propiedad de la firma digital no permite que el emisor pueda negar la autoría de un mensaje?

a) Autenticación.

b) Integridad.

**c) No repudio.**

d) Confidencialidad.

3) ¿Para qué se utiliza Diffie-Hellman?

a) Para cifrar sesiones SSL/TLS.

b) Para informar al usuario de que el certificado del servidor no es válido.

c) Para verificar el certificado del servidor.

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

4) ¿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.

5) ¿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.

6) ¿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.

7) ¿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.**

8) ¿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.

9) ¿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.**

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

a) PIN.

b) Cifrado de los datos del chip.

**c) Relieves.**

d) Ninguna de las anteriores.

11) ¿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.

12) ¿Qué es el ransomware?

a) Un tipo de software malicioso considerado no dañino.

b) Un tipo de software malicioso que utiliza técnicas especiales para permanecer oculto respecto al sistema.

c) Un tipo de software malicioso que muestra al usuario un mensaje indicándole que se va a formatear el disco duro sin que esto llegue a producirse.

**d) Ninguna de las opciones anteriores es cierta.**

13) ¿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.

14) ¿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.**

15) ¿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.

16) ¿Cuál de las siguientes afirmaciones relacionadas con la suplantación de identidad es cierta?

a) El phishing es un tipo de estafa informática que emplea técnicas de ingeniería social para suplantar la identidad de otra persona o entidad haciéndose pasar por ella mediante el protocolo de voz sobre IP.

b) El SMiShing es un tipo de estafa informática que hace creer a la víctima, sin que sea realmente así, que se ha comprometido su seguridad.

c) El SMiShing es un tipo de estafa informática que utiliza mensajes de correo basura o spam para embaucar a las víctimas.

**d) Ninguna de las opciones anteriores es cierta.**

17) ¿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.**

18) ¿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.**

19) ¿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.

20) 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.

21) ¿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.

22) ¿Qué opción de las siguientes adoptarías para evitar infecciones al navegar por Internet?

a) Instalar una suite de seguridad que ofrezca inspección de tráfico en tiempo real.

**b) Hacer una copia de seguridad de todos los archivos importantes del sistema.**

c) Configurar el cortafuegos para rechazar todo el tráfico entrante.

d) Instalar un software congelador.

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 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) ¿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.**

26) ¿Por qué motivo son las suites de seguridad adecuadas para entornos empresariales?

a) Porque permiten intervenir remotamente en un equipo donde se ha detectado una infección que no se ha podido eliminar.

b) Porque permiten minimizar el consumo de ancho de banda.

c) Porque facilitan la gestión al tener centralizadas todas las actualizaciones.

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

27) ¿Qué ventajas presenta la utilización de software congelador?

a) El equipo que utiliza este tipo de herramientas estará libre de virus de forma garantizada.

**b) Cuando se produce la restauración, se eliminan las infecciones previas originadas por software malicioso.**

c) La información generada por un usuario en cada sesión no será modificada al restaurar el equipo.

d) Ninguna de las respuestas es correcta.

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) Nuestro equipo parece infectado por algún tipo de malware que nuestra herramienta antimalware es incapaz de eliminar, ya que continuamente aparece una ventana que indica que se ha detectado una actividad ilegal procedente de este equipo y que debemos pagar una multa a una cuenta de correo. ¿Qué deberíamos hacer?

a) Formatear el equipo para eliminarlo, aunque perdamos información importante de la que no tengamos copia de seguridad.

b) Si nuestro antivirus no lo puede detectar, desinstalarlo y probar otro antivirus mejor.

c) Pagar la multa.

**d) Visitar las páginas web de los centros de protección y respuesta ante amenazas para estudiar si nos encontramos ante algún tipo de estafa.**

30) ¿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.

31) ¿Qué se puede utilizar para realizar una recuperación de datos en un disco externo?

a) Clonezilla.

b) Rsync.

**c) GetDataBack.**

d) Los puntos de restauración.

32) 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**

33) ¿Cuál de las siguientes afirmaciones es verdadera?

a) La tecnología NAS ofrece alojamiento en la nube.

**b) Los servicios de almacenamiento remoto ofrecen las modalidades de cloud público y cloud privado.**

c) Dentro de la clasificación de dispositivos locales encontramos los remotos y los de almacenamiento en la nube.

d) La tecnología SAN también es conocida como almacenamiento en la nube.

34) ¿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.

35) ¿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.

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) Los puntos de restauración utilizados en Windows...

a) Permiten recuperar datos borrados de cualquier dispositivo de almacenamiento.

b) También son conocidos como modo a prueba de fallos.

c) Son similares a la aplicación de recuperación de datos GetDataBack.

**d) Permiten pasar a un estado anterior del sistema.**

38) ¿Cuál de las siguientes afirmaciones sobre los soportes o dispositivos para las copias de seguridad es cierta?

a) Para una correcta elección hay que tener en cuenta el tiempo de acceso a los datos.

b) Para una correcta elección hay que tener en cuenta la velocidad a la que se realizará la copia.

c) Para una correcta elección hay que tener en cuenta el tipo de datos.

**d) Las respuestas a y b son ciertas.**

39) 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.

40) ¿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.