1) ¿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.**

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

a) VeriSign.

**b) FNMT.**

c) Comodo.

d) Thawte.

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) ¿Qué tipo de certificado es el más extendido?

a) PEM.

**b) X.509.**

c) X.506.

d) DER.

5) Los certificados digitales se crearon para solucionar el problema de...

**a) Confianza en la clave pública de un usuario.**

b) Gestión del anillo de claves públicas.

c) Pérdida de la clave privada.

d) Confianza en la clave simétrica de un usuario.

6) ¿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.

7) ¿Qué servicios proporciona la firma digital?

a) De autenticación.

b) De integridad.

c) De no repudio.

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

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

a) RSA.

**b) Diffie-Hellman.**

c) DSA.

d) ElGamal.

9) Bitlocker es un ejemplo de...

a) Cortafuegos.

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

c) Antivirus.

d) Sistema de firma digital.

10) ¿En qué consiste la fase de comunicación 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 cifrado simétrico.**

11) ¿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.

12) ¿Cuál de las siguientes afirmaciones relacionadas con la suplantación de la identidad es falsa?

a) El pharming es una técnica de suplantación de identidad que consiste en redireccionar peticiones a una página web falsa.

b) El correo electrónico es una herramienta muy utilizada por los estafadores para embaucar a las víctimas.

c) En la mayoría de los casos las víctimas no son conscientes del engaño, por lo que no dudan en introducir su contraseña en una página web que no es legítima pensando que sí lo es.

**d) El vishing consiste en el envío de mensajes de texto a la víctima para procurar que visite una página web o llame a un número de teléfono.**

13) ¿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.**

14) ¿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.**

15) 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.

16) ¿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.**

17) ¿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.

18) ¿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.

19) ¿De qué modo se produce con más frecuencia la infección de los troyanos?

a) De forma automática, al navegar por Internet.

**b) Al ejecutar un archivo infectado.**

c) Al borrar un archivo infectado.

d) Todas las respuestas son correctas.

20) ¿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.

21) 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.

22) ¿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.

23) ¿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.**

24) ¿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.

25) ¿Cuál de las siguientes afirmaciones sobre las políticas de los cortafuegos es verdadera?

a) Un cortafuegos con una política de entrada muy restrictiva es más seguro.

b) Un cortafuegos con una política de salida muy restrictiva es más seguro.

c) Un cortafuegos con políticas de entrada y salida muy restrictivas siempre es más conveniente.

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

26) ¿Cuál de las siguientes afirmaciones sobre los tipos de cortafuegos es verdadera?

a) Un cortafuegos de filtrado de paquetes tiene en cuenta la colocación individual de cada uno dentro de una serie de paquetes.

**b) Los cortafuegos de aplicación permiten que los programas y aplicaciones accedan o no a la red.**

c) Un cortafuegos de estado filtra el tráfico atendiendo únicamente a las direcciones IP, el protocolo y el número de puerto utilizado.

d) Todas las respuestas son verdaderas.

27) ¿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.

28) ¿Qué herramienta utilizarías para proteger los datos importantes frente a pérdidas de información ocasionadas por malware?

**a) Copias de seguridad.**

b) Antivirus.

c) Cortafuegos.

d) Software congelador.

29) ¿Qué es un congelador?

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.**

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) La clonación de una partición a otra...

a) Consiste en copiar la partición en un archivo.

b) Copia todo el contenido de la partición en un disco.

c) No es posible con Clonezilla.

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

33) ¿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.

34) ¿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.

35) 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.

36) 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**

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) ¿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 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.