1) ¿Cuál de las siguientes opciones se considera una vulnerabilidad?

a) No utilizar antivirus.

b) No utilizar mecanismos de protección frente a fallos eléctricos.

c) No tener actualizado el sistema operativo.

**d) Todas las anteriores.**

2) ¿Cuál de las siguientes opciones es un activo para una empresa?

a) Los estudios de mercado.

b) El sistema operativo.

c) La sala de servidores.

**d) Todas las anteriores.**

3) La autenticación...

a) Garantiza que la información solo sea accesible e interpretada por personas o sistemas autorizados.

b) Asegura que la información solo sea accesible para los usuarios legítimos cuando la necesiten.

c) Garantiza que la información solo pueda ser alterada por las personas autorizadas o los usuarios legítimos.

**d) Garantiza la identidad de los participantes en una comunicación.**

4) Elaborar las reglas y procedimientos para los servicios críticos de una organización es un aspecto a tener en cuenta...

a) En el plan de contingencia.

**b) En la política de seguridad.**

c) Tanto en el plan de contingencia como en la política de seguridad.

d) En el análisis de riesgos.

5) En función de lo que se quiere proteger...

a) La seguridad de la información ofrece la seguridad física y la seguridad lógica.

b) La seguridad informática ofrece la seguridad activa y la seguridad pasiva.

c) La seguridad de la información ofrece la seguridad activa y la seguridad pasiva.

**d) La seguridad informática ofrece la seguridad física y la seguridad lógica.**

6) ¿Cuál de las siguientes afirmaciones es falsa?

**a) En función de las acciones realizadas, se distingue entre ataques de tipo pasivo y de tipo activo.**

b) Un tipo de ataque es hacerse pasar por el administrador.

c) Una de las fases del ataque informático es el reconocimiento.

d) Los ataques orientados a la explotación de las debilidades humanas son imposibles de detectar por las actuales herramientas de seguridad.

7) ¿Cuál de las siguientes afirmaciones sobre la seguridad de la información es cierta?

**a) Se trata del conjunto de medidas y procedimientos que permiten proteger la integridad, la confidencialidad y la disponibilidad de la información.**

b) Contiene medidas detalladas para conseguir la recuperación del sistema.

c) Se trata del conjunto de medidas de seguridad que afectan a la información independientemente de ella.

d) Es el conjunto de datos con los que trabaja una empresa y que si caen en manos inadecuadas pueden llegar a perjudicarla seriamente.

8) ¿Cuál de las siguientes afirmaciones es cierta?

a) El impacto es la estimación del grado de exposición que existe a que una amenaza se materialice.

**b) El robo de información se considera un riesgo de alto nivel.**

c) Un desastre informático tiene lugar cuando se produce una situación que atenta contra el sistema.

d) El impacto cero no existe.

9) Las comunicaciones no cifradas se pueden considerar...

a) Un ataque.

b) Una amenaza.

c) Un riesgo.

**d) Una vulnerabilidad.**

10) ¿Qué principio de la seguridad informática se incumple si tiene lugar un robo a través de la red del número de tarjeta de crédito?

**a) La confidencialidad.**

b) La integridad.

c) La disponibilidad.

d) La autenticación.

11) ¿Cuáles son los riesgos externos a los que están sujetos los sistemas informáticos?

a) El humo y la humedad.

b) Los fenómenos naturales.

c) Los riesgos humanos.

**d) Las respuestas b y c son correctas.**

12) ¿Qué es la autonomía de un SAI?

a) El tiempo que transcurre desde que se produce el fallo de la corriente eléctrica hasta que el SAI se pone en funcionamiento.

**b) El tiempo que el SAI puede seguir alimentando a un equipo en caso de producirse un fallo eléctrico.**

c) El número de elementos que se pueden conectar como carga al SAI.

d) El número de SAI necesarios para tener en marcha un CPD en caso de que falle el suministro eléctrico.

13) ¿Cuál es el objetivo de las tomas de tierra?

a) Desviar la tensión eléctrica a tierra.

b) Aislar los equipos de las vibraciones de la tierra.

**c) Desviar la corriente eléctrica a tierra si falla el aislamiento de los conductores.**

d) Obtener la corriente eléctrica de tierra si se produce un fallo eléctrico.

14) ¿Qué es la seguridad física?

**a) El conjunto de medidas destinadas a evitar daños físicos en los sistemas informáticos.**

b) El conjunto de medidas destinadas a proteger solo los programas informáticos.

c) El conjunto de medidas destinadas a proteger solo los datos de usuario.

d) El conjunto de medidas destinadas a proteger los equipos de los virus informáticos.

15) ¿Cuál de las siguientes afirmaciones es verdadera?

**a) Al configurar un CPD hay que tener en cuenta el tipo de datos que se van a manejar.**

b) Al configurar un CPD hay que tener en cuenta el número de equipos y personas que va a contener.

c) Las empresas dimensionan su CPD en base a su capital.

d) Las empresas dimensionan su CPD en base al espacio físico disponible.

16) ¿Para qué es importante la elección del sistema de refrigeración de un CPD?

a) Para evitar una refrigeración excesiva de los equipos del CPD.

b) Para evitar un sobrecalentamiento excesivo de los equipos informáticos del CPD.

**c) Para lograr una mayor eficiencia energética y ahorrar en el consumo eléctrico.**

d) Para evitar que los equipos de refrigeración ocupen mucho espacio dentro del CPD.

17) ¿En qué tipos de SAI tiene lugar un pequeño corte de energía desde que se produce un fallo de suministro eléctrico hasta que se pone en marcha el SAI?

a) En los SAI offline interactivos.

b) En los SAI online.

**c) En los SAI offline pasivos.**

d) En ninguno, ya que siempre hay suministro.

18) ¿Qué función tiene un SAI?

a) Proporcionar corriente estabilizada.

b) Proporcionar tensión eléctrica sin fluctuaciones.

c) Sustituir el uso de energía eléctrica en los ordenadores.

**d) Permitir un apagado ordenado de los equipos.**

19) ¿Cuál de las siguientes afirmaciones sobre los centros de proceso de datos es verdadera?

**a) Un CPD es un conjunto de instalaciones físicas y de requerimientos hardware específicos que albergan sistemas informáticos centralizados.**

b) Un CPD es un conjunto de instalaciones físicas y de requerimientos software específicos que utilizan los sistemas informáticos centralizados.

c) Un CPD es un conjunto de instalaciones físicas con sistemas informáticos centralizados.

d) Un CPD es un conjunto de instalaciones físicas con sistemas informáticos no centralizados.

20) ¿Cuál es la finalidad de los centros de respaldo?

a) Sustituir al CPD principal cuando quede obsoleto.

**b) Tomar el control del sistema si falla el CPD principal.**

c) Replicar la información del CPD principal.

d) Trabajar en paralelo con el CPD principal para mejorar su eficiencia.

21) Para implementar un sistema de ACL en Windows...

**a) Es necesario utilizar el sistema de archivos NTFS.**

b) Es recomendable, aunque no necesario, utilizar el sistema de archivos NTFS.

c) La implementación de ACL en Windows no depende del sistema de archivos.

d) Hace falta utilizar un sistema operativo de servidor.

22) ¿De qué se componen las ACL en GNU/Linux?

a) De categoría.

b) De identificador de usuario o grupo.

c) De cadena de permisos.

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

23) ¿Cuál de las siguientes no es una medida o un mecanismo establecido en una política de seguridad?

a) Autenticación de usuarios.

b) Certificados digitales.

**c) Ubicación física de los usuarios.**

d) Listas de control de acceso.

24) ¿Qué es security token?

a) Un dispositivo biométrico de identificación.

b) Un mensaje de confirmación que se envía al teléfono móvil o al correo electrónico.

c) El acuse de recibo de los mensajes de correo.

**d) Un dispositivo hardware que sirve para autenticar al usuario.**

25) ¿En qué consiste el ataque por fuerza bruta?

**a) En probar distintas claves hasta dar con la correcta.**

b) En atacar un sistema mediante virus.

c) En instalar un virus que provoque el calentamiento del procesador.

d) En abrir un ordenador para robar el disco duro.

26) Como administradores, ¿qué medida podemos aplicar para generar una buena política de contraseñas?

a) Forzar a usar contraseñas de menos de 8 caracteres.

**b) Establecer un número máximo de intentos para acceder al sistema.**

c) Permitir al usuario utilizar las mismas contraseñas anteriores.

d) Dejar que el usuario no cambie la contraseña durante un largo periodo de tiempo.

27) ¿Qué permiten las listas de control de acceso?

**a) Controlar qué usuarios pueden acceder a las distintas aplicaciones, sistemas, recursos, etc.**

b) Controlar únicamente el uso del sistema que hace un usuario.

c) Controlar únicamente a qué páginas web accede el usuario.

d) Controlar a qué hora entran los usuarios en el ordenador.

28) ¿Qué es el phising?

a) El robo de las claves de un usuario.

b) Un virus que calienta el procesador.

**c) La suplantación de la identidad de una persona a través de Internet.**

d) El robo de los contactos de correo.

29) ¿Qué tipo de sistema de autenticación es Kerberos?

**a) SSO.**

b) Web SSO.

c) OTP.

d) Identidad federada.

30) ¿Qué consideración se le da a un mensaje de correo falso que indica que enviemos las claves del banco?

a) Ataque por fuerza bruta.

b) Sniffer.

**c) Ataque por ingeniería social.**

d) Ataque por diccionario.

1) ¿Cuál de las siguientes afirmaciones sobre la seguridad informática es cierta?

a) Se trata del conjunto de medidas y procedimientos que permiten proteger la integridad, la confidencialidad y la disponibilidad de la información.

**b) Trata de proteger la información que utiliza una infraestructura informática y de telecomunicaciones para ser transmitida o almacenada.**

c) Contiene medidas detalladas para lograr la recuperación del sistema.

d) Es el conjunto de datos con los que trabaja una empresa y que si caen en manos inadecuadas pueden llegar a perjudicarla seriamente.

2) ¿Qué es un ataque informático?

**a) Una acción que trata de aprovechar una debilidad del sistema informático.**

b) Son acciones únicamente intencionadas que pueden llegar a poner el sistema en peligro.

c) Una circunstancia que atenta contra el buen funcionamiento del sistema, como por ejemplo un error de configuración.

d) Todas las respuestas son correctas.

3) ¿Qué son las vulnerabilidades?

a) Los recursos que necesitan las empresas para poder alcanzar sus objetivos.

**b) Las debilidades que pueden encontrarse en los activos y que pueden alterar el funcionamiento del sistema.**

c) El conjunto de medidas y procedimientos que permiten proteger la integridad, la confidencialidad y la disponibilidad de la información.

d) Ninguna de las respuestas es correcta.

4) En función de lo que se quiere proteger...

a) La seguridad de la información ofrece la seguridad física y la seguridad lógica.

b) La seguridad informática ofrece la seguridad activa y la seguridad pasiva.

c) La seguridad de la información ofrece la seguridad activa y la seguridad pasiva.

**d) La seguridad informática ofrece la seguridad física y la seguridad lógica.**

5) Las comunicaciones no cifradas se pueden considerar...

a) Un ataque.

b) Una amenaza.

c) Un riesgo.

**d) Una vulnerabilidad.**

6) ¿Qué principio de la seguridad informática se incumple si tiene lugar un robo a través de la red del número de tarjeta de crédito?

**a) La confidencialidad.**

b) La integridad.

c) La disponibilidad.

d) La autenticación.

7) ¿Cuál de las siguientes opciones es un activo para una empresa?

a) Los estudios de mercado.

b) El sistema operativo.

c) La sala de servidores.

**d) Todas las anteriores.**

8) ¿Cuál de las siguientes afirmaciones es falsa?

a) El riesgo cero no existe.

b) Un impacto prácticamente no afecta al funcionamiento de una empresa que tiene establecido un buen método de actuación ante las amenazas.

c) Las organizaciones han de estar preparadas para cualquier tipo de desastre.

**d) El impacto es el daño producido en caso de que un riesgo se materialice.**

9) Elaborar las reglas y procedimientos para los servicios críticos de una organización es un aspecto a tener en cuenta...

a) En el plan de contingencia.

**b) En la política de seguridad.**

c) Tanto en el plan de contingencia como en la política de seguridad.

d) En el análisis de riesgos.

10) La integridad...

a) Garantiza que la información solo sea accesible e interpretada por personas o sistemas autorizados.

b) Asegura que la información solo sea accesible para los usuarios legítimos cuando la necesiten.

**c) Garantiza que la información solo pueda ser alterada por las personas autorizadas o los usuarios legítimos.**

d) Garantiza la identidad de los participantes en una comunicación.

11) ¿Qué es un cold site o sala fría?

**a) Un CPD externo a la organización que posee toda la infraestructura necesaria en cuanto a instalaciones para poner en marcha un CPD similar al principal.**

b) Un CPD externo a la organización que posee la infraestructura necesaria en cuanto a instalaciones y equipos para poner en marcha un CPD similar al principal.

c) Un CPD interno a la organización que posee toda la infraestructura necesaria en cuanto a instalaciones y equipos para poner en marcha un CPD similar al principal.

d) Una sala en el CPD de otra organización con los datos de nuestra organización replicados.

12) ¿Qué aspectos no contempla el concepto de seguridad física?

a) Las medidas de prevención destinadas a evitar daños físicos en los sistemas informáticos.

b) Las medidas de detección destinadas a evitar daños físicos en los sistemas informáticos.

**c) Las medidas de prevención y detección destinadas a preservar únicamente los datos de los sistemas físicos.**

d) Las medidas destinadas a proteger los equipos y los datos que contienen.

13) ¿Por qué es importante el entorno físico de los equipos informáticos?

a) Por la seguridad de las personas que trabajan en él.

**b) Porque minimiza los diversos factores de riesgo a los que puedan estar expuestos los equipos.**

c) Porque evita accidentes laborales y que los empleados causen baja.

d) Porque evita los cortocircuitos que estropean los equipos.

14) ¿En qué consume más energía un CPD?

a) En la iluminación.

b) En la alimentación de los equipos.

c) En la alimentación de los SAI.

**d) En la climatización.**

15) ¿Cuál de las siguientes afirmaciones es verdadera?

**a) Al configurar un CPD hay que tener en cuenta el tipo de datos que se van a manejar.**

b) Al configurar un CPD hay que tener en cuenta el número de equipos y personas que va a contener.

c) Las empresas dimensionan su CPD en base a su capital.

d) Las empresas dimensionan su CPD en base al espacio físico disponible.

16) ¿Cómo se puede realizar la gestión de un SAI?

a) Por control remoto instalando una antena en el SAI.

b) Por correo electrónico.

c) Conectando el equipo al SAI mediante un USB o cable de red.

**d) Desde cualquier equipo al que esté conectado, mediante programas específicos.**

17) ¿Qué es un centro de proceso de datos?

**a) Un conjunto de instalaciones físicas y de requerimientos hardware específicos que albergan sistemas informáticos centralizados.**

b) Un conjunto de instalaciones físicas y de requerimientos software específicos que utilizan los sistemas informáticos centralizados.

c) Un conjunto de instalaciones físicas con sistemas informáticos centralizados.

d) Un conjunto de instalaciones físicas con sistemas informáticos no centralizados.

18) ¿Se podría seguir trabajando con normalidad en una oficina si se produce un corte de suministro eléctrico y empiezan a funcionar los SAI?

a) Sí, porque los SAI continuarían suministrando energía eléctrica.

b) Sí, siempre que los SAI fueran de tipo online, ya que continuarían suministrando energía eléctrica.

**c) No, porque los SAI solo están pensados para realizar cierres ordenados en los servidores disponiendo de unos minutos.**

d) No, porque solo podrían seguir trabajando los servidores.

19) ¿Qué es la autonomía de un SAI?

a) El tiempo que transcurre desde que se produce el fallo de la corriente eléctrica hasta que el SAI se pone en funcionamiento.

**b) El tiempo que el SAI puede seguir alimentando a un equipo en caso de producirse un fallo eléctrico.**

c) El número de elementos que se pueden conectar como carga al SAI.

d) El número de SAI necesarios para tener en marcha un CPD en caso de que falle el suministro eléctrico.

20) ¿Qué factores de riesgo afectan a los equipos informáticos?

**a) Espacio, humedad, luz solar, temperatura, polvo y campos magnéticos.**

b) Humedad, luz solar, temperatura, polvo y electricidad.

c) Espacio, instalación eléctrica defectuosa y malas condiciones del edificio.

d) Radiación electromagnética y rayos de sol.

21) Para implementar un sistema de ACL en Windows...

**a) Es necesario utilizar el sistema de archivos NTFS.**

b) Es recomendable, aunque no necesario, utilizar el sistema de archivos NTFS.

c) La implementación de ACL en Windows no depende del sistema de archivos.

d) Hace falta utilizar un sistema operativo de servidor.

22) ¿Cómo se denomina el fraude que consiste en suplantar la identidad de las personas a través de Internet?

**a) Phising.**

b) Bulling.

c) Sniffing.

d) Snorkeling.

23) ¿Cuál de las siguientes no es una medida o un mecanismo establecido en una política de seguridad?

a) Autenticación de usuarios.

b) Certificados digitales.

**c) Ubicación física de los usuarios.**

d) Listas de control de acceso.

24) ¿Cómo se llaman los programas que permiten capturar las pulsaciones del teclado?

a) Troyanos.

b) KeyCaptchas.

**c) Keyloggers.**

d) Sniffers.

25) ¿Qué es security token?

a) Un dispositivo biométrico de identificación.

b) Un mensaje de confirmación que se envía al teléfono móvil o al correo electrónico.

c) El acuse de recibo de los mensajes de correo.

**d) Un dispositivo hardware que sirve para autenticar al usuario.**

26) ¿Qué tipo de contraseña se considera segura?

a) Una contraseña larga con números romanos.

b) Una contraseña larga con letras mayúsculas y minúsculas.

c) Una contraseña de más de 8 caracteres que incluya iniciales y fechas.

**d) Una contraseña suficientemente larga que incluya números, letras (mayúsculas y minúsculas ) y caracteres no alfanuméricos.**

27) ¿De qué se componen las ACL en GNU/Linux?

a) De categoría.

b) De identificador de usuario o grupo.

c) De cadena de permisos.

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

28) ¿Qué se recomienda en relación a la comunicación de contraseñas?

a) Enviarlas por correo electrónico.

**b) Transmitirlas por un canal seguro cifrado.**

c) Comunicarlas por un medio seguro como el teléfono.

d) Ninguna de las anteriores.

29) ¿Cómo se llama el sistema de autorización que permite, mediante un usuario y contraseña únicos, validarse en varias aplicaciones?

**a) Sistema Single Sign-On (SSO).**

b) Sistema monousuario.

c) OpenID.

d) Kerberos.

30) ¿Cómo se llama la herramienta que permite controlar qué usuarios pueden acceder a las distintas aplicaciones, recursos, etc.?

**a) Listas de control de acceso.**

b) Uso de contraseñas.

c) Firewall.

d) Proxy.

1) ¿Qué es una vulnerabilidad del sistema informático?

a) Una acción que trata de aprovechar una debilidad para provocar un impacto.

b) Una acción intencionada que puede poner en riesgo al sistema.

c) Cualquier circunstancia que atente contra el buen funcionamiento del sistema operativo.

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

2) ¿Cuál de las siguientes afirmaciones es cierta?

a) El impacto es la estimación del grado de exposición que existe a que una amenaza se materialice.

**b) El robo de información se considera un riesgo de alto nivel.**

c) Un desastre informático tiene lugar cuando se produce una situación que atenta contra el sistema.

d) El impacto cero no existe.

3) Las comunicaciones no cifradas se pueden considerar...

a) Un ataque.

b) Una amenaza.

c) Un riesgo.

**d) Una vulnerabilidad.**

4) ¿Qué principio de la seguridad informática viola el hecho de modificar la información que se transmite a través de la red?

a) La confidencialidad.

**b) La integridad.**

c) La disponibilidad.

d) La autenticación.

5) ¿Cuál de las siguientes opciones se considera un ataque?

a) No tener actualizado el sistema operativo.

b) Los errores de configuración.

**c) El uso de la ingeniería social.**

d) La manipulación de la configuración del sistema.

6) La autenticación...

a) Garantiza que la información solo sea accesible e interpretada por personas o sistemas autorizados.

b) Asegura que la información solo sea accesible para los usuarios legítimos cuando la necesiten.

c) Garantiza que la información solo pueda ser alterada por las personas autorizadas o los usuarios legítimos.

**d) Garantiza la identidad de los participantes en una comunicación.**

7) Un plan de recuperación es una medida...

**a) Del plan de contingencia.**

b) De la política de seguridad.

c) Tanto del plan de contingencia como de la política de seguridad.

d) Del análisis de riesgos.

8) ¿Qué es un activo para una organización?

**a) Todo aquel recurso necesario para que la organización alcance los objetivos marcados.**

b) El resultado de aplicar medidas preventivas en los recursos informáticos.

c) Todo aquello relacionado con la seguridad activa y la pasiva.

d) Todas las respuestas son correctas.

9) ¿Es lo mismo seguridad informática que seguridad de la información?

a) Sí, las dos protegen la integridad y confidencialidad de la información para que no llegue a manos indebidas.

b) No, la seguridad informática protege la integridad y el no repudio de la información.

**c) No, la seguridad de la información protege la integridad, la confidencialidad y la disponibilidad de la información.**

d) Sí, ambas tienen como objetivo principal proteger las vulnerabilidades de la información.

10) En función de lo que se quiere proteger...

a) La seguridad de la información ofrece la seguridad física y la seguridad lógica.

b) La seguridad informática ofrece la seguridad activa y la seguridad pasiva.

c) La seguridad de la información ofrece la seguridad activa y la seguridad pasiva.

**d) La seguridad informática ofrece la seguridad física y la seguridad lógica.**

11) ¿Cómo se puede realizar la gestión de un SAI?

a) Por control remoto instalando una antena en el SAI.

b) Por correo electrónico.

c) Conectando el equipo al SAI mediante un USB o cable de red.

**d) Desde cualquier equipo al que esté conectado, mediante programas específicos.**

12) ¿Cómo se llama el material que aísla del fuego?

**a) Ignífugo.**

b) Fireprotected.

c) Antifuego.

d) Firewall.

13) ¿Qué es el factor de potencia de un SAI?

a) El resultado de multiplicar la potencia real por la potencia aparente del SAI.

**b) La relación entre la potencia aparente y la potencia real consumida por el SAI.**

c) El factor por el que hay que multiplicar la potencia para obtener la tensión del SAI.

d) El número de elementos que se pueden conectar como carga al SAI.

14) ¿Por qué es tan importante la seguridad física?

**a) Porque preserva los equipos y dispositivos que contienen los datos de las empresas.**

b) Porque protege los equipos informáticos, que tienen un gran valor.

c) Porque protege la seguridad de las personas.

d) Porque protege los datos de las empresas, que tienen un gran valor.

15) ¿Cuál es la finalidad de los centros de respaldo?

a) Sustituir al CPD principal cuando quede obsoleto.

**b) Tomar el control del sistema si falla el CPD principal.**

c) Replicar la información del CPD principal.

d) Trabajar en paralelo con el CPD principal para mejorar su eficiencia.

16) ¿Se podría seguir trabajando con normalidad en una oficina si se produce un corte de suministro eléctrico y empiezan a funcionar los SAI?

a) Sí, porque los SAI continuarían suministrando energía eléctrica.

b) Sí, siempre que los SAI fueran de tipo online, ya que continuarían suministrando energía eléctrica.

**c) No, porque los SAI solo están pensados para realizar cierres ordenados en los servidores disponiendo de unos minutos.**

d) No, porque solo podrían seguir trabajando los servidores.

17) ¿Cuál de las siguientes afirmaciones es verdadera?

a) La climatización de un CPD se basa únicamente en la instalación de equipos de aire acondicionado.

**b) Los pasillos fríos son las zonas interiores del CPD por las que circula el aire procedente de los equipos de refrigeración.**

c) Los pasillos calientes son las zonas exteriores del CPD por las que circula el aire procedente de los equipos informáticos.

d) El aire de los pasillos fríos se extrae para su posterior refrigeración y filtrado.

18) ¿Qué características deben cumplir las instalaciones que van a albergar equipos informáticos?

**a) Instalación eléctrica y de red adecuadas, control de acceso y protección frente a incendios.**

b) Protecciones sísmicas, SAI y sistemas detectores de incendios.

c) Sistemas antihumedad, protección frente a incendios, protección sísmica y protección eléctrica.

d) Sistemas de control de presencia y SAI.

19) ¿Por qué es importante el entorno físico de los equipos informáticos?

a) Por la seguridad de las personas que trabajan en él.

**b) Porque minimiza los diversos factores de riesgo a los que puedan estar expuestos los equipos.**

c) Porque evita accidentes laborales y que los empleados causen baja.

d) Porque evita los cortocircuitos que estropean los equipos.

20) ¿Cuál de las siguientes afirmaciones sobre los centros de proceso de datos es verdadera?

**a) Un CPD es un conjunto de instalaciones físicas y de requerimientos hardware específicos que albergan sistemas informáticos centralizados.**

b) Un CPD es un conjunto de instalaciones físicas y de requerimientos software específicos que utilizan los sistemas informáticos centralizados.

c) Un CPD es un conjunto de instalaciones físicas con sistemas informáticos centralizados.

d) Un CPD es un conjunto de instalaciones físicas con sistemas informáticos no centralizados.

21) ¿Cómo se denomina el sistema de autenticación que utiliza una contraseña de un solo uso?

a) Security token.

b) UTP.

c) SSO.

**d) Ninguna de las anteriores.**

22) ¿Qué es la seguridad lógica?

a) El conjunto de medidas destinadas a evitar daños físicos en los sistemas informáticos.

**b) El conjunto de medidas destinadas a proteger los datos y las aplicaciones informáticas.**

c) El conjunto de medidas destinadas a proteger los equipos informáticos de accesos no autorizados.

d) El conjunto de medidas destinadas a proteger los sistemas físicos, los datos lógicos y a las personas que trabajan con ellos.

23) ¿Qué consideración se le da a un mensaje de correo falso que indica que enviemos las claves del banco?

a) Ataque por fuerza bruta.

b) Sniffer.

**c) Ataque por ingeniería social.**

d) Ataque por diccionario.

24) ¿Qué tipo de contraseña se considera segura?

a) Una contraseña larga con números romanos.

b) Una contraseña larga con letras mayúsculas y minúsculas.

c) Una contraseña de más de 8 caracteres que incluya iniciales y fechas.

**d) Una contraseña suficientemente larga que incluya números, letras (mayúsculas y minúsculas ) y caracteres no alfanuméricos.**

25) ¿Cuál es el comando de Linux que permite establecer y asignar las ACL?

a) chacl.

b) setacl.

**c) setfacl.**

d) getacl.

26) ¿En qué consiste un ataque por diccionario?

a) En atacar un sistema mediante virus.

**b) En averiguar la contraseña de un usuario probando con un listado predefinido de palabras.**

c) En instalar un programa para capturar las pulsaciones del teclado.

d) En interceptar las comunicaciones de un ordenador.

27) En los routers podemos establecer listas de control de acceso...

a) En los routers no se pueden establecer listas de control de acceso, solo en los sistemas operativos.

b) Por IP y por puerto.

c) Por las direcciones IP.

**d) Por protocolo, por interfaz y por IP.**

28) ¿Qué permiten las listas de control de acceso?

**a) Controlar qué usuarios pueden acceder a las distintas aplicaciones, sistemas, recursos, etc.**

b) Controlar únicamente el uso del sistema que hace un usuario.

c) Controlar únicamente a qué páginas web accede el usuario.

d) Controlar a qué hora entran los usuarios en el ordenador.

29) ¿Qué es el phising?

a) El robo de las claves de un usuario.

b) Un virus que calienta el procesador.

**c) La suplantación de la identidad de una persona a través de Internet.**

d) El robo de los contactos de correo.

30) ¿Qué permiten los sistemas SSO (Single Sign-On)?

**a) Tener centralizadas las credenciales de usuario para que sean usadas por distintas aplicaciones.**

b) Identificar de forma única a un usuario.

c) Trabajar con sistemas gestores de contraseñas.

d) Entrar a distintas aplicaciones por Internet mediante el correo electrónico.

1) ¿Cuál de las siguientes afirmaciones es verdadera?

a) Las políticas de seguridad contienen medidas detalladas para conseguir la recuperación del sistema.

b) Los planes de contiengencia contemplan la prevención del sistema.

**c) Un aspecto a tener en cuenta en la elaboración de las políticas de seguridad es sensibilizar al personal de los posibles problemas de seguridad.**

d) Un aspecto a tener en cuenta en la elaboración de los planes de contingencia es establecer una clasificación de los archivos con menor importancia.

2) Las seguridades activa y pasiva pertenecen a...

**a) La seguridad informática.**

b) La seguridad de la información.

c) La seguridad informática y la seguridad de la información.

d) Ninguna de las respuestas es correcta.

3) ¿Qué es un activo para una organización?

**a) Todo aquel recurso necesario para que la organización alcance los objetivos marcados.**

b) El resultado de aplicar medidas preventivas en los recursos informáticos.

c) Todo aquello relacionado con la seguridad activa y la pasiva.

d) Todas las respuestas son correctas.

4) La confidencialidad...

**a) Garantiza que la información solo sea accesible e interpretada por personas o sistemas autorizados.**

b) Asegura que la información solo sea accesible para los usuarios legítimos cuando la necesiten.

c) Garantiza que la información solo pueda ser alterada por las personas autorizadas o los usuarios legítimos.

d) Garantiza la identidad de los participantes en una comunicación.

5) ¿Cuál de las siguientes afirmaciones sobre la seguridad informática es cierta?

a) Se trata del conjunto de medidas y procedimientos que permiten proteger la integridad, la confidencialidad y la disponibilidad de la información.

**b) Trata de proteger la información que utiliza una infraestructura informática y de telecomunicaciones para ser transmitida o almacenada.**

c) Contiene medidas detalladas para lograr la recuperación del sistema.

d) Es el conjunto de datos con los que trabaja una empresa y que si caen en manos inadecuadas pueden llegar a perjudicarla seriamente.

6) ¿Vulnerabilidad y agujero de seguridad son lo mismo?

a) No, los agujeros de seguridad se asocian a las amenazas.

**b) Sí, ya que pueden estar asociados, por ejemplo, a fallos en la implementación de las aplicaciones.**

c) No, las vulnerabilidades se asocian a los recursos del sistema.

d) Sí, pero en el caso de la seguridad lógica.

7) Las comunicaciones no cifradas se pueden considerar...

a) Un ataque.

b) Una amenaza.

c) Un riesgo.

**d) Una vulnerabilidad.**

8) ¿Qué principio de la seguridad informática viola el hecho de modificar la información que se transmite a través de la red?

a) La confidencialidad.

**b) La integridad.**

c) La disponibilidad.

d) La autenticación.

9) ¿Cuál de las siguientes opciones se considera un ataque?

a) No tener actualizado el sistema operativo.

b) Los errores de configuración.

**c) El uso de la ingeniería social.**

d) La manipulación de la configuración del sistema.

10) ¿Cuál de las siguientes afirmaciones es falsa?

a) El riesgo cero no existe.

b) Un impacto prácticamente no afecta al funcionamiento de una empresa que tiene establecido un buen método de actuación ante las amenazas.

c) Las organizaciones han de estar preparadas para cualquier tipo de desastre.

**d) El impacto es el daño producido en caso de que un riesgo se materialice.**

11) ¿Cuáles son los riesgos externos a los que están sujetos los sistemas informáticos?

a) El humo y la humedad.

b) Los fenómenos naturales.

c) Los riesgos humanos.

**d) Las respuestas b y c son correctas.**

12) ¿Se podría seguir trabajando con normalidad en una oficina si se produce un corte de suministro eléctrico y empiezan a funcionar los SAI?

a) Sí, porque los SAI continuarían suministrando energía eléctrica.

b) Sí, siempre que los SAI fueran de tipo online, ya que continuarían suministrando energía eléctrica.

**c) No, porque los SAI solo están pensados para realizar cierres ordenados en los servidores disponiendo de unos minutos.**

d) No, porque solo podrían seguir trabajando los servidores.

13) ¿Qué tipo de conexiones podemos encontrar en un SAI?

a) Conexiones eléctricas diversas y de telefonía.

b) Conexiones eléctricas diversas y de almacenamiento masivo.

**c) Conexiones eléctrica y de datos.**

d) Conexiones de corriente continua y alterna.

14) ¿Cómo se denomina el conjunto de medidas de prevención y detección destinadas a evitar los daños físicos en los sistemas informáticos y a proteger los datos almacenados en ellos?

a) Seguridad informática.

b) Seguridad pasiva.

c) Seguridad lógica.

**d) Seguridad física.**

15) ¿Cuál es la finalidad de los centros de respaldo?

a) Sustituir al CPD principal cuando quede obsoleto.

**b) Tomar el control del sistema si falla el CPD principal.**

c) Replicar la información del CPD principal.

d) Trabajar en paralelo con el CPD principal para mejorar su eficiencia.

16) ¿Cuál de las siguientes afirmaciones es verdadera?

a) La climatización de un CPD se basa únicamente en la instalación de equipos de aire acondicionado.

**b) Los pasillos fríos son las zonas interiores del CPD por las que circula el aire procedente de los equipos de refrigeración.**

c) Los pasillos calientes son las zonas exteriores del CPD por las que circula el aire procedente de los equipos informáticos.

d) El aire de los pasillos fríos se extrae para su posterior refrigeración y filtrado.

17) ¿Cómo se llama el dispositivo que permite, mediante un teclado, un ratón y una pantalla, acceder a varios equipos?

a) Router KVM.

**b) Concentrador KVM.**

c) Switch TPR.

d) Concentrador TPR.

18) ¿Qué es un SAI?

a) Un dispositivo destinado a proporcionar corriente estabilizada.

b) Un dispositivo destinado a proporcionar tensión eléctrica sin fluctuaciones.

c) Un dispositivo que sustituye el uso de la energía eléctrica en los ordenadores.

**d) Un dispositivo destinado a proporcionar electricidad en caso de que esta falle.**

19) ¿Cuál de las siguientes afirmaciones es verdadera?

**a) Al configurar un CPD hay que tener en cuenta el tipo de datos que se van a manejar.**

b) Al configurar un CPD hay que tener en cuenta el número de equipos y personas que va a contener.

c) Las empresas dimensionan su CPD en base a su capital.

d) Las empresas dimensionan su CPD en base al espacio físico disponible.

20) ¿Qué factores de riesgo afectan a los equipos informáticos?

**a) Espacio, humedad, luz solar, temperatura, polvo y campos magnéticos.**

b) Humedad, luz solar, temperatura, polvo y electricidad.

c) Espacio, instalación eléctrica defectuosa y malas condiciones del edificio.

d) Radiación electromagnética y rayos de sol.

21) ¿Cuál de las siguientes afirmaciones sobre políticas de seguridad corporativa no es cierta?

a) Definen las pautas a seguir para garantizar la seguridad de la información.

b) Configuran el marco de actuación de todos los usuarios.

**c) Son definidas únicamente por la dirección de la organización.**

d) Recogen normas aplicables a toda la empresa.

22) ¿Qué permiten los sistemas SSO (Single Sign-On)?

**a) Tener centralizadas las credenciales de usuario para que sean usadas por distintas aplicaciones.**

b) Identificar de forma única a un usuario.

c) Trabajar con sistemas gestores de contraseñas.

d) Entrar a distintas aplicaciones por Internet mediante el correo electrónico.

23) ¿De qué se componen las ACL en GNU/Linux?

a) De categoría.

b) De identificador de usuario o grupo.

c) De cadena de permisos.

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

24) ¿Cuál de las siguientes opciones es una ventaja de usar ACL en redes?

a) Facilitan las tareas de administración.

b) Aumentan el rendimiento de la red al eliminar el tráfico deseado.

**c) Aumentan la seguridad en la red.**

d) Permiten la ejecución de determinados comandos con fines malintencionados.

25) ¿Qué tipo de contraseña se considera segura?

a) Una contraseña larga con números romanos.

b) Una contraseña larga con letras mayúsculas y minúsculas.

c) Una contraseña de más de 8 caracteres que incluya iniciales y fechas.

**d) Una contraseña suficientemente larga que incluya números, letras (mayúsculas y minúsculas ) y caracteres no alfanuméricos.**

26) ¿Qué se recomienda en relación a la comunicación de contraseñas?

a) Enviarlas por correo electrónico.

**b) Transmitirlas por un canal seguro cifrado.**

c) Comunicarlas por un medio seguro como el teléfono.

d) Ninguna de las anteriores.

27) ¿Cuál de las siguientes opciones no es una amenaza para las contraseñas?

a) Los keyloggers.

**b) Los gusanos.**

c) La ingeniería social.

d) Los sniffers.

28) ¿Cómo se llaman los sistemas de identificación basados en rasgos de la persona?

a) Sistemas de identificación personales.

b) Sistemas de identificación fisiológicos.

c) Sistemas de identificación biológicos.

**d) Sistemas de identificación biométricos.**

29) Los administradores establecen los derechos y privilegios de los usuarios utilizando...

a) El registro de Windows.

b) El visor de sucesos.

**c) Las directivas de seguridad local.**

d) El panel de control de conexiones de red.

30) ¿Cómo se denomina el fraude que consiste en suplantar la identidad de las personas a través de Internet?

**a) Phising.**

b) Bulling.

c) Sniffing.

d) Snorkeling.

1) En función de lo que se quiere proteger...

a) La seguridad de la información ofrece la seguridad física y la seguridad lógica.

b) La seguridad informática ofrece la seguridad activa y la seguridad pasiva.

c) La seguridad de la información ofrece la seguridad activa y la seguridad pasiva.

**d) La seguridad informática ofrece la seguridad física y la seguridad lógica.**

2) ¿Cuál de las siguientes afirmaciones es falsa?

a) La caída de un servidor puede considerarse un desastre.

b) Los resultados del análisis de riesgos permiten valorar las medidas que se deberían tomar para reducir los posibles daños.

c) El riesgo cero no existe.

**d) Uno de los objetivos del análisis de riesgos es identificar los posibles desastres en caso de que se produzcan amenazas en la organización.**

3) ¿Cuál de las siguientes opciones se considera una vulnerabilidad?

a) No utilizar antivirus.

b) No utilizar mecanismos de protección frente a fallos eléctricos.

c) No tener actualizado el sistema operativo.

**d) Todas las anteriores.**

4) ¿Qué principio de la seguridad informática se incumple si tiene lugar un robo a través de la red del número de tarjeta de crédito?

**a) La confidencialidad.**

b) La integridad.

c) La disponibilidad.

d) La autenticación.

5) ¿Cuál de las siguientes opciones es un activo para una empresa?

a) Los estudios de mercado.

b) El sistema operativo.

c) La sala de servidores.

**d) Todas las anteriores.**

6) ¿Cuál de las siguientes afirmaciones sobre la seguridad informática es cierta?

a) Se trata del conjunto de medidas y procedimientos que permiten proteger la integridad, la confidencialidad y la disponibilidad de la información.

**b) Trata de proteger la información que utiliza una infraestructura informática y de telecomunicaciones para ser transmitida o almacenada.**

c) Contiene medidas detalladas para lograr la recuperación del sistema.

d) Es el conjunto de datos con los que trabaja una empresa y que si caen en manos inadecuadas pueden llegar a perjudicarla seriamente.

7) El uso de contraseñas débiles se considera...

a) Una amenaza.

**b) Una vulnerabilidad.**

c) Un ataque.

d) Un riesgo.

8) Elaborar las reglas y procedimientos para los servicios críticos de una organización es un aspecto a tener en cuenta...

a) En el plan de contingencia.

**b) En la política de seguridad.**

c) Tanto en el plan de contingencia como en la política de seguridad.

d) En el análisis de riesgos.

9) ¿Qué es un ataque informático?

**a) Una acción que trata de aprovechar una debilidad del sistema informático.**

b) Son acciones únicamente intencionadas que pueden llegar a poner el sistema en peligro.

c) Una circunstancia que atenta contra el buen funcionamiento del sistema, como por ejemplo un error de configuración.

d) Todas las respuestas son correctas.

10) La confidencialidad...

**a) Garantiza que la información solo sea accesible e interpretada por personas o sistemas autorizados.**

b) Asegura que la información solo sea accesible para los usuarios legítimos cuando la necesiten.

c) Garantiza que la información solo pueda ser alterada por las personas autorizadas o los usuarios legítimos.

d) Garantiza la identidad de los participantes en una comunicación.

11) ¿Cuáles son los riesgos externos a los que están sujetos los sistemas informáticos?

a) El humo y la humedad.

b) Los fenómenos naturales.

c) Los riesgos humanos.

**d) Las respuestas b y c son correctas.**

12) ¿Qué permite un concentrador KVM?

**a) Acceder a diversos ordenadores con un teclado, un ratón y una pantalla.**

b) Concentrar varios SAI para multiplicar su acción.

c) Acceder a los interfaces GVA de varios ordenadores.

d) Reunir varios puntos de suministro de energía en un solo punto.

13) ¿Qué es la seguridad física?

**a) El conjunto de medidas destinadas a evitar daños físicos en los sistemas informáticos.**

b) El conjunto de medidas destinadas a proteger solo los programas informáticos.

c) El conjunto de medidas destinadas a proteger solo los datos de usuario.

d) El conjunto de medidas destinadas a proteger los equipos de los virus informáticos.

14) ¿Cuál es el objetivo de las tomas de tierra?

a) Desviar la tensión eléctrica a tierra.

b) Aislar los equipos de las vibraciones de la tierra.

**c) Desviar la corriente eléctrica a tierra si falla el aislamiento de los conductores.**

d) Obtener la corriente eléctrica de tierra si se produce un fallo eléctrico.

15) ¿Qué es un SAI?

a) Un dispositivo destinado a proporcionar corriente estabilizada.

b) Un dispositivo destinado a proporcionar tensión eléctrica sin fluctuaciones.

c) Un dispositivo que sustituye el uso de la energía eléctrica en los ordenadores.

**d) Un dispositivo destinado a proporcionar electricidad en caso de que esta falle.**

16) ¿Cuál de las siguientes afirmaciones es verdadera?

**a) Al configurar un CPD hay que tener en cuenta el tipo de datos que se van a manejar.**

b) Al configurar un CPD hay que tener en cuenta el número de equipos y personas que va a contener.

c) Las empresas dimensionan su CPD en base a su capital.

d) Las empresas dimensionan su CPD en base al espacio físico disponible.

17) ¿Qué tipo de conexiones podemos encontrar en un SAI?

a) Conexiones eléctricas diversas y de telefonía.

b) Conexiones eléctricas diversas y de almacenamiento masivo.

**c) Conexiones eléctrica y de datos.**

d) Conexiones de corriente continua y alterna.

18) ¿Qué material se utiliza para extinguir los incendios con equipos eléctricos?

a) Agua oxigenada.

**b) Agua nebulizada.**

c) Agua salada.

d) Polvo.

19) ¿Cuál es la finalidad de los centros de respaldo?

a) Sustituir al CPD principal cuando quede obsoleto.

**b) Tomar el control del sistema si falla el CPD principal.**

c) Replicar la información del CPD principal.

d) Trabajar en paralelo con el CPD principal para mejorar su eficiencia.

20) ¿En qué consume más energía un CPD?

a) En la iluminación.

b) En la alimentación de los equipos.

c) En la alimentación de los SAI.

**d) En la climatización.**

21) ¿Para qué se utiliza un keylogger?

a) Para copiar los logs del sistema

**b) Para capturar las pulsaciones del teclado**

c) Para capturar los movimientos del ratón

d) Para cifrar los datos del disco duro

22) ¿Cómo se denomina el fraude que consiste en suplantar la identidad de las personas a través de Internet?

**a) Phising.**

b) Bulling.

c) Sniffing.

d) Snorkeling.

23) Como administradores, ¿qué medida podemos aplicar para generar una buena política de contraseñas?

a) Forzar a usar contraseñas de menos de 8 caracteres.

**b) Establecer un número máximo de intentos para acceder al sistema.**

c) Permitir al usuario utilizar las mismas contraseñas anteriores.

d) Dejar que el usuario no cambie la contraseña durante un largo periodo de tiempo.

24) ¿En qué consiste un ataque por diccionario?

a) En atacar un sistema mediante virus.

**b) En averiguar la contraseña de un usuario probando con un listado predefinido de palabras.**

c) En instalar un programa para capturar las pulsaciones del teclado.

d) En interceptar las comunicaciones de un ordenador.

25) ¿Cómo se llama el sistema de autorización que permite, mediante un usuario y contraseña únicos, validarse en varias aplicaciones?

**a) Sistema Single Sign-On (SSO).**

b) Sistema monousuario.

c) OpenID.

d) Kerberos.

26) ¿Qué permiten las listas de control de acceso?

**a) Controlar qué usuarios pueden acceder a las distintas aplicaciones, sistemas, recursos, etc.**

b) Controlar únicamente el uso del sistema que hace un usuario.

c) Controlar únicamente a qué páginas web accede el usuario.

d) Controlar a qué hora entran los usuarios en el ordenador.

27) ¿Cuál de las siguientes opciones es una ventaja de usar ACL en redes?

a) Facilitan las tareas de administración.

b) Aumentan el rendimiento de la red al eliminar el tráfico deseado.

**c) Aumentan la seguridad en la red.**

d) Permiten la ejecución de determinados comandos con fines malintencionados.

28) ¿Cuál de las siguientes no es una medida o un mecanismo establecido en una política de seguridad?

a) Autenticación de usuarios.

b) Certificados digitales.

**c) Ubicación física de los usuarios.**

d) Listas de control de acceso.

29) ¿Qué es security token?

a) Un dispositivo biométrico de identificación.

b) Un mensaje de confirmación que se envía al teléfono móvil o al correo electrónico.

c) El acuse de recibo de los mensajes de correo.

**d) Un dispositivo hardware que sirve para autenticar al usuario.**

30) Una aplicación exhaustiva del nivel de control mediante ACL...

**a) Complica las tareas de administración de la seguridad del sistema.**

b) Hace imposible que los sistemas sean accedidos por personas no autorizadas.

c) Facilita las tareas de administración de la seguridad del sistema.

d) Hace imposible que los sistemas sean atacados por virus y troyanos.