



ADEIT | **FUNDACIÓ
UNIVERSITAT EMPRESA**
UNIVERSITAT DE VALÈNCIA

PROCESO DE SELECCIÓN DEL PUESTO DE DIRECCIÓN DE ESTRATEGIA DIGITAL

RESPUESTAS AL EXAMEN TIPO TEST

FECHA DE CELEBRACIÓN: 30-06-2021

HORA DE CELEBRACIÓN: 15:00

INFORMACIÓN DEL CANDIDATO/A	
Nombre	
Apellidos	
DNI	

INSTRUCCIONES

- 1- El examen contará con **20 preguntas tipo test**, con cuatro opciones de respuesta cada una, y con **una sola respuesta válida**.

- 2- La **puntuación** de las mismas, se realizará conforme a las siguientes reglas:
 - Cada **pregunta correctamente** contestada, sumará **un (1) punto**.
 - Las **preguntas incorrectamente** contestadas, o las preguntas **en blanco**, tendrán una valoración de **cero (0) puntos**.

- 3- **Para aprobar** el examen, la puntuación final del mismo debe ser igual o superior a **10 puntos**.

- 4- La respuesta correcta debe **marcarse rodeando** con un **círculo la letra** de la opción elegida.

- 5- Si hubiera **varias opciones marcadas**, o hubiera dudas sobre cuál es realmente la elección marcada por el candidato, la pregunta **se considerará no contestada**, y se obtendrán **cero puntos** en la misma.

- 6- El tiempo para la realización de la prueba es de **30 minutos**.

- 7- **No** está permitido **consultar libros, manuales** o cualquier **dispositivo electrónico**.

- 8.- Los **móviles** deben permanecer en **“modo avión”** a efectos de no perturbar la concentración del resto de candidatos.

- 9- El **incumplimiento** de las normas anteriores determinará la **expulsión del candidato** del examen, y su **eliminación del proceso selectivo**.

CUESTIONARIO

- 1- **¿Qué es lo primero que haría para definir el plan de contingencias de ADEIT?**
- a) **Identificar los procesos críticos de la organización**
 - b) Revisar y actualizar el inventario de activos TIC
 - c) Revisar y mejorar las condiciones de seguridad del CPD
 - d) Revisar y actualizar la relación de personas que deberían ser avisadas en una contingencia y sus datos y teléfonos de contacto
- 2- **En el método TOPSIS de decisión entre alternativas...**
- a) **La alternativa seleccionada debe ser aquella que esté lo más cerca posible de la solución ideal positiva y lo más lejos posible de la solución ideal negativa.**
 - b) La idea es comparar cada permutación posible de alternativas con la información ordinal de evaluaciones que aporta para cada criterio la matriz de decisión.
 - c) En cada comparación se asocia: índice de concordancia (mide argumentos a favor de la alternativa) e índice de discordancia (mide argumentos en contra).
 - d) Se ignora la cuantía de la diferencia entre alternativas para cada criterio, sólo señala si existe o no, y considera la importancia del criterio para el decisor.
- 3- **¿Qué medida no aportaría una mejora en el nivel de madurez en seguridad en ADEIT?**
- a) Implantar un doble factor de autenticación
 - b) Hacer una campaña de phishing simulado en ADEIT
 - c) **Dar permisos de administrador de sus equipos a los usuarios, para que puedan protegerlos bien**
 - d) Ninguna de las anteriores



- 4- **Según el Esquema Nacional de Seguridad, en lo relativo a la auditoría:**
- a) Los sistemas de información de categoría BÁSICA, o inferior, no necesitarán realizar una auditoría. Bastará una autoevaluación realizada por el mismo personal que administra el sistema de información, o en quien este delegue.
 - b) Los sistemas de información de categoría MEDIA no necesitarán realizar una auditoría. Bastará una autoevaluación realizada por el mismo personal que administra el sistema de información, o en quien éste delegue.
 - c) **Los sistemas de información de categoría BÁSICA, o inferior, no necesitarán realizar una auditoría. Bastará una autoevaluación realizada en cualquier caso por personal de seguridad ajeno al que administra el sistema de información.**
 - d) El ENS no considera suficiente una autoevaluación en ningún sistema de información de categoría BÁSICA, MEDIA o ALTA.
- 5- **Las dimensiones de seguridad de la información pueden resumirse en:**
- a) **Disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad**
 - b) Integridad, autenticación, confidencialidad, precisión, portabilidad
 - c) Disponibilidad, confidencialidad, autenticación, portabilidad, integración
 - d) Autenticación, disponibilidad, integridad, escalabilidad, portabilidad
- 6- **¿Cuál es el objetivo de un ataque "eavesdropping"?**
- a) Es un ataque que tiene por objeto colapsar los recursos del sistema.
 - b) Es un ataque que tiene por objeto suplantar la identidad de otro usuario.
 - c) **Es un ataque que tiene por objeto obtener información sin modificarla.**
 - d) Es un ataque que tiene por objeto comprometer la identidad de la información.



- 7- **¿Cuándo deber determinarse un Acuerdo de Nivel de Servicio según Métrica v3?**
- a) Antes de implementar el sistema en el entorno de operación.
 - b) Una vez que el sistema se encuentra en su entorno de operación y antes de aceptarlo.
 - c) Una vez que el sistema se encuentra en su entorno de operación y una vez aceptado.**
 - d) Ninguna de la anteriores es correcta.
- 8- **Respecto a los tipos de licencias de software libre, con la licencia GNU GPL:**
- a) Los usuarios o compañías que distribuyen sus trabajos pueden cobrar o distribuirlos gratuitamente.
 - b) Los usuarios o compañías que distribuyen sus trabajos bajo las GNU GPL no pueden cobrar y sólo pueden distribuirlos gratuitamente.
 - c) Todo el software con licencia GNU GPL es copyleft.**
 - d) La licencia BSD original es compatible con la GNU GPL.
- 9- **¿Cuál de estas acciones dañinas se basa en la ingeniería social?**
- a) Business e-mail compromise (BEC).**
 - b) Ransomware.
 - c) Eavesdropping.
 - d) Todas las anteriores.
- 10- **¿Qué serie de guías CCN-STIC establece las políticas y procedimientos adecuados para la implementación de las medidas contempladas en el Esquema Nacional de Seguridad?**
- a) CCN-STIC-400.
 - b) CCN-STIC-600.
 - c) CCN-STIC-800.**
 - d) CCN-STIC-500.

11- Considerando la importancia de la Protección de Datos en el uso de herramientas TIC, de acuerdo con la normativa vigente en materia de protección de datos personales algunos de los principios que rigen el tratamiento de los datos personales son:

- a) El principio de eficacia, jerarquía, desconcentración y coordinación.
- b) Licitud, lealtad, publicidad y limitación de la finalidad.
- c) Licitud, lealtad, transparencia y limitación de la finalidad.**
- d) Licitud, coordinación, transparencia y limitación de la finalidad.

12- ¿Cuál de las siguientes afirmaciones es cierta?

- a) La caza activa de amenazas tiene por objetivo detectar situaciones que no han sido identificadas por las herramientas de seguridad habituales.
- b) La correlación de eventos es clave en el funcionamiento de un Centro de Operaciones de Seguridad.
- c) Al proceso de configurar de forma segura sistemas y aplicaciones se le denomina bastionado.
- d) Todas las anteriores son ciertas.**

13- ¿Cuál de las siguientes afirmaciones es cierta?

- a) El doble factor de autenticación consiste en utilizar algo que tengo y algo que soy.
- b) El doble factor de autenticación consiste en utilizar algo que tengo y algo que sé.
- c) El doble factor de autenticación consiste en utilizar algo que sé y algo que soy.
- d) Todas las anteriores son ciertas.**



- 14- Indicar la respuesta verdadera respecto al concepto de un sistema de información:**
- a) Es el conjunto de procedimientos, manuales y automatizados dirigidos a la recogida, elaboración, evaluación, almacenamiento, recuperación y distribución de informaciones dentro de una organización
 - b) Es el conjunto de procedimientos, manuales y automatizados dirigidos a la recogida, elaboración, almacenamiento, recuperación, condensación y distribución de informaciones dentro de una organización
 - c) Es el conjunto de procedimientos, manuales y automatizados y de funciones dirigidas a la recogida, elaboración, almacenamiento, recuperación y distribución de informaciones dentro de una organización
 - d) Es el conjunto de procedimientos, manuales y automatizados y de funciones dirigidas a la recogida, elaboración, evaluación, almacenamiento, recuperación, condensación y distribución de informaciones dentro de una organización**
- 15- A un sistema de información definido como "Sistemas orientados a la ayuda en la toma de decisiones esporádicas u ocasionales" corresponde al tipo de sistema de información:**
- a) Sistemas orientados a la gestión de empresa o Management Information Systems (MIS)
 - b) Sistemas orientados al proceso de transacciones o Transaction Processing Systems
 - c) Sistemas de apoyo a la toma de decisiones o Decision Support Systems (DSS)**
 - d) Sistemas de apoyo a la dirección o Executive Support Systems (ESS)
- 16- La gestión inteligente de los Datos (Smart Data) permite a empresas y organizaciones obtener numerosos beneficios, pero ¿cuál de los siguientes consideras que tiene una mayor importancia estratégica en su proceso de transformación digital?:**
- a) Incrementar de forma significativa la capacidad de almacenamiento de los datos de sus clientes.
 - b) Disponer de una visión integral y completa (360º) de sus clientes actuales y potenciales para ofrecerles productos y servicios personalizados y diferenciados.**

- c) Utilizar los datos para hacer un análisis histórico de sus resultados anuales.
- d) Cumplir de forma adecuada las exigencias legales del Reglamento de Protección de Datos de Carácter Personal (RGPD)

17- ¿Cuál de las siguientes palancas o vectores de transformación digital consideras que es el más importante para que una empresa u organización aborde con éxito su proceso de transformación digital?

- a) Personas (cultura corporativa, liderazgo, modelo organizativo y talento).
- b) Datos (Big Data – Smart Data & Analytics).
- c) Tecnologías (Cloud; Movilidad; Inteligencia Artificial y Robótica; Realidad Aumentada y Virtual; Internet de las Cosas; Internet, Social Media y Comunidades; Blockchain; Biometría, etc.).
- d) Todas las respuestas anteriores son correctas.**

18- Según el RD 806/2014, ¿Qué son medios y servicios en referencia a los medios y servicios compartidos?

- a) Todas las actividades, infraestructuras técnicas, instalaciones, aplicaciones, equipos, inmuebles, redes, ficheros electrónicos, licencias y demás activos que dan soporte a los sistemas de información.**
- b) Todas las infraestructuras técnicas, instalaciones, aplicaciones, equipos, inmuebles, redes, ficheros electrónicos, licencias y demás activos que dan soporte a los sistemas de información.
- c) Todas las infraestructuras técnicas, instalaciones, aplicaciones, equipos, inmuebles, redes, licencias y demás activos que dan soporte a los sistemas de información.
- d) Todas las actividades, infraestructuras técnicas, aplicaciones, equipos, inmuebles, redes, ficheros electrónicos, licencias y demás activos que dan soporte a los sistemas de información.

19- Según la guía CCN-STIC-827 Gestión y uso de dispositivos móviles, señale la INCORRECTA:

- a) La autenticación del usuario se realizará con una contraseña/pin del dispositivo y/u otro tipo de autenticación antes de acceder a los recursos del organismo.
- b) Los dispositivos deben bloquearse automáticamente después de un determinado periodo de inactividad.
- c) El uso de un modelo BYOD (Bring Your Own Device) está intensamente desaconsejado.**
- d) Bajo la potestad del administrador de seguridad, podrá bloquearse de forma remota el dispositivo si se sospecha que ha podido ser dejado en un estado no seguro o en una ubicación no segura.

20- Indique la opción INCORRECTA en relación con el Esquema Nacional de Seguridad (ENS):

- a) Los sistemas de información a los que se refiere el ENS serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos expuestos en el ENS.
- b) Gestión de riesgos, función diferenciada y reevaluación periódica son 3 de los principios básicos que deberán tenerse en cuenta en las decisiones en materia de seguridad.
- c) El Instituto Nacional de las Tecnologías de la Información (INTECO), en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de la seguridad de las tecnologías de la información y las comunicaciones.**
- d) Si a los 12 meses de la entrada en vigor del ENS hubiera circunstancias que impidan la plena aplicación de lo exigido en el mismo, se dispondrá de un plan de adecuación que marque los plazos de ejecución, los cuales, en ningún caso, serán superiores a 48 meses desde la entrada en vigor.