



1. La confidencialidad es una propiedad de la seguridad de la información que evita
- A) la modificación no autorizada de la información.
 - B) la eliminación no autorizada de la información.
 - C) la divulgación no autorizada de la información. *
 - D) ajustar los dispositivos de red para mejorar su rendimiento y eficiencia.

Referencia bibliográfica: <https://www.studocu.com/>

2. Marque la alternativa que corresponda con el modelo de control de acceso a los objetos (conceder o denegar) en función a una lista de condiciones.
- A) RBAC
 - B) DAC
 - C) MAC
 - D) ACL *

Referencia bibliográfica: <https://www.studocu.com/>

3. Marque el parámetro de clasificación de la información que corresponda a esta definición: «Es la información obsoleta debido a nueva información, o debido a cambios substanciales en la empresa».
- A) Antigüedad
 - B) Asociación legal
 - C) Valor
 - D) Vida útil *

Referencia bibliográfica: <https://www.studocu.com/>

4. Señale el parámetro de clasificación de la información que asocia las garantías de la privacidad a través de las leyes.
- A) Asociación legal *
 - B) Valor
 - C) Antigüedad
 - D) Vida útil

Referencia bibliográfica: <https://www.studocu.com/>

5. Marque los momentos en los cuales se pueden aplicar técnicas de mitigación de riesgos contra posibles ataques.
- A) Antes de transferir el riesgo
 - B) Después de un ataque *
 - C) Durante la aceptación del riesgo
 - D) Antes de eliminar el riesgo

Referencia bibliográfica: <https://www.studocu.com/>



6. Marque la fase de un ataque en donde se prueba que es posible explotar una vulnerabilidad previamente identificada.
- A) Cubriendo rastros
 - B) Reconocimiento
 - C) Consiguiendo accesos *
 - D) Escaneo

Referencia bibliográfica: <https://www.studocu.com/>

7. Señale la alternativa CORRECTA sobre la evolución de las herramientas de ataque versus el conocimiento técnico.
- A) Las herramientas de ataques en el transcurso del tiempo se han vuelto menos automatizadas, por lo cual, requieren de un mayor nivel de conocimientos técnicos.
 - B) Las herramientas de ataques en el transcurso del tiempo se han vuelto escasas, pero más automatizadas y sofisticadas, por lo cual, requieren de un menor nivel de conocimientos técnicos.
 - C) Las herramientas de ataques en el transcurso del tiempo no se han vuelto más automatizadas ni sofisticadas, por lo que es indiferente el conocimiento técnico.
 - D) Las herramientas de ataque en el transcurso del tiempo se han vuelto más automatizadas y sofisticadas, por lo cual, requieren de un menor nivel de conocimientos técnicos. *

Referencia bibliográfica: <https://www.studocu.com/>

8. Debido a la sobrecarga de las capacidades del usuario validado, marque el tipo de ataque que impide el uso normal de una computadora o red.
- A) DoS *
 - B) Swarm-as-a-service
 - C) Fuzzing de inteligencia artificial
 - D) Man-in-the-Middle

Referencia bibliográfica: <https://www.studocu.com/>

9. Marque el tipo de ataque basada en herramientas de tecnología de inteligencia artificial y de enjambres que permiten la automatización de *botnets* gigantes, las cuales pueden ser adquiridas mediante medios ilegales sin necesidad de conocimiento técnico, haciendo más sencillo que un delincuente interrumpa las operaciones de cualquier negocio.
- A) Swarm-as-a-service *
 - B) Envenenamiento del Machine Learning
 - C) Fuzzing de inteligencia artificial
 - D) Man-in-the-Middle

Referencia bibliográfica: <https://www.studocu.com/>



10. Marque la alternativa que contenga una de las principales fuentes de vulnerabilidad que afectan a la seguridad lógica.

- A) Troyanos
- B) Virus
- C) Actualización *
- D) Gusanos

Referencia bibliográfica: <https://www.studocu.com/>

11. Señale el tipo de atacante que represente a un *hacker* de sombrero negro.

- A) Hacktivistas
- B) Craker *
- C) Script kiddies
- D) Jailbreak

Referencia bibliográfica: <https://www.studocu.com/>

12. Marque la alternativa que hace referencia a dos problemas de seguridad sobre la infraestructura tecnológica que pueden ocasionar amenazas lógicas.

- A) Modificación, robo o pérdida de información no autorizada *
- B) Manipulación del procesamiento y distorsión de resultados
- C) Pérdida de confianza e ingresos no autorizados
- D) Afectación de la imagen corporativa y distorsión de resultados

Referencia bibliográfica: <https://www.studocu.com/>

13. Señale la alternativa que corresponda con la siguiente definición: «Error, fallo o problema dentro de un programa o *software* que desencadena un resultado indeseado o no previsto».

- A) Debug
- B) Malware
- C) Bug *
- D) Gusano

Referencia bibliográfica: <https://www.studocu.com/>

14. De acuerdo con el marco de ITIL, ¿cuál es el objetivo de la gestión de acceso?

- A) Gestionar el acceso al Service Desk del usuario
- B) Gestionar el acceso a los centros de cómputo, datacenters y demás instalaciones restringidas
- C) Gestionar el derecho al uso de los servicios de TI *
- D) Proveer sistemas de seguridad que apliquen restricciones a las aplicaciones

Referencia bibliográfica: ITIL (<https://www.globalsuitesolutions.com/es/que-es-til-y-para-que-sirve/>)



15. Marque la alternativa que NO es una característica del Estado moderno, según la Secretaría de Gestión Pública.

- A) Orientado al ciudadano
- B) Inclusivo
- C) Abierto
- D) Célere *

Referencia bibliográfica:

<https://sgp.pcm.gob.pe/politica-nacional-de-modernizacion-de-la-gestion-publica-al-2021/>

16. ¿Qué tipo de *malware* es una pieza de código (programa, script, etc.) que se activa en un momento predeterminado o bajo condiciones predefinidas, para ejecutar acciones dañinas sobre la información o servicios informáticos?

- A) Bomba lógica *
- B) Spyrware
- C) Ransomware
- D) Backdoor

Referencia bibliográfica: <https://www.studocu.com/>

17. ¿Qué tipo de *malware* secuestra el acceso al ordenador, unidades de almacenamiento o archivos, y utiliza técnicas criptográficas con el objetivo de solicitar un rescate?

- A) Rootkit
- B) Backdoor
- C) Botnet
- D) Rasomware *

Referencia bibliográfica: <https://www.studocu.com/>

18. Los cinco pilares centrales de la política de modernización de la gestión pública son

- A) políticas públicas, planes estratégicos y operativos; gobierno abierto; gestión por procesos; servicio civil meritocrático; sistema de información, seguimiento, monitoreo, evaluación; gestión del conocimiento.
- B) gobierno electrónico; gobierno abierto; gestión por procesos; servicio civil meritocrático; sistema de información, seguimiento, monitoreo, evaluación y gestión del conocimiento.
- C) políticas públicas, planes estratégicos y operativos; presupuesto para resultados; gestión por procesos; servicio civil meritocrático; sistema de información, seguimiento, monitoreo, evaluación y gestión del conocimiento.
*
- D) gobierno electrónico; gobierno abierto; gestión por procesos; servicio civil meritocrático; presupuesto para resultados.



Referencia bibliográfica:

<https://sgp.pcm.gob.pe/politica-nacional-de-modernizacion-de-la-gestion-publica-al-2021/>

- 19.** Marque la alternativa que corresponda con la siguiente definición: «Es una infraestructura tecnológica administrada por la Secretaría de Gobierno y Transformación Digital, que permite la implementación de servicios públicos en línea por medios electrónicos, y el intercambio electrónico de información entre entidades del Estado a través de internet, telefonía móvil y otros medios tecnológicos disponibles, de manera segura».
- A) Sistema nacional de gobierno y transformación digital
 - B) Plataforma nacional de interoperabilidad *
 - C) Plataforma nacional de gobierno digital
 - D) Sistema integrado de interoperabilidad

Referencia bibliográfica: <https://www.gob.pe/741-plataforma-de-interoperabilidad-del-estado>

- 20.** Marque los ocho dominios de desempeño del proyecto.
- A) Interesados; equipo; enfoque de desarrollo y del ciclo de vida; planificación; trabajo del proyecto; entrega; medición e incertidumbre *
 - B) Interesados, equipo; enfoque de desarrollo y del ciclo de vida; planificación; trabajo del proyecto; entrega; medición y priorización.
 - C) Interesados; equipo; enfoque de desarrollo y del ciclo de vida; planificación; trabajo del proyecto; entrega, medición y liderazgo
 - D) Interesados; equipo; enfoque de desarrollo y del ciclo de vida; planificación; trabajo del proyecto; entrega; medición y despliegue

Referencia bibliográfica: PMBOK Edición 7 - Los 8 Performance Domain de PMBOK®7