Cloud & Network Security

Reactivos

Pregunta 1

Según la definición proporcionada por la OCDE, ¿cuál de las siguientes afirmaciones describe mejor la naturaleza de la identidad digital?

Opciones:

a. La identidad digital es directa y siempre se verifica en la realidad física.
b. La identidad digital solo se compone de datos personales en internet.
c. La identidad digital es estática y no cambia con el tiempo.
d. La identidad digital es contextual y dinámica, siempre está cambiando.

Pregunta 2

Completa la siguiente afirmación: Según la Real Academia Española (2022), la identidad se define como todos aquellos rasgos que pertenecen a un individuo, es decir, los rasgos que hacen única a una persona frente a los demás. En el ámbito digital, para reforzar la seguridad de la identidad, las organizaciones implementan sistemas de *IAM*, que se refieren a la Gestión de Identidad y Acceso. En estos sistemas, cada cliente cuenta con un __________ único y una ____________, además de una capa adicional de seguridad mediante el registro de una huella biométrica.

Opciones:

a. identificador, *PIN*
b. código, firma digital
c. nombre, número de teléfono
d. usuario, contraseña

Pregunta 3

¿Cómo podría una organización mejorar la seguridad de la identidad digital más allá de la implementación de usuarios y contraseñas en un sistema *IAM*?

Opciones:

a. Utilizar métodos de autenticación multifactorial, como la verificación de huellas biométricas.
b. Solicitar a los usuarios que compartan su contraseña periódicamente.
c. Eliminar por completo la necesidad de contraseñas.
d. Permitir a los usuarios elegir contraseñas simples para facilitar el recuerdo.

Pregunta 4

Según la información proporcionada, ¿cuál de las siguientes acciones NO es una característica de la identidad digital según la OCDE?

Opciones:

a. La identidad digital es estática.
b. La identidad digital es subjetiva.
c. La identidad digital es real.
d. La identidad digital es contextual y dinámica.

Pregunta 5

Coloca en orden cronológico los siguientes pasos que una organización podría seguir para fortalecer la seguridad de la identidad digital en un entorno empresarial:

1. Implementar autenticación multifactorial.
2. Realizar auditorías de seguridad periódicas.
3. Educar a los empleados sobre prácticas seguras en línea.
4. Establecer políticas de contraseñas robustas.

Opciones:

a. 4, 3, 1, 2
b. 3, 4, 2, 1
c. 1, 2, 3, 4
d. 2, 1, 4, 3

Pregunta 6

De acuerdo con la información proporcionada sobre *networking* en la nube, ¿cuál es una ventaja específica que ofrece la infraestructura en la nube en comparación con la infraestructura local?

Opciones:

a. Limitada capacidad de gestión
b. Menor flexibilidad
c. Escalabilidad sencilla y rápida
d. Mayor seguridad

Pregunta 7

Completa la siguiente afirmación: "El *NAT* (*Network Address Translation*) es un proceso que traduce una dirección *IP* privada a una dirección *IP* pública, permitiendo que los *local hosts* se conecten a internet. Además, también se encarga de la traducción de los números de puertos y sus ________."

Opciones:

a. sistemas operativos
b. máscaras
c. contraseñas
d. protocolos

Pregunta 8

Selecciona la afirmación correcta sobre la función de un *switch* en una red.

Opciones:

a. Un *switch* se utiliza exclusivamente para establecer conexiones seguras mediante *VPN*.
b. Un *switch* permite la conexión inalámbrica de dispositivos a la red.
c. Un *switch* facilita la comunicación entre dispositivos en la misma red y puede instalarse localmente o en la nube.
d. Un *switch* conecta diferentes redes y facilita la conexión a internet.

Pregunta 9

¿Cuál es el principal objetivo de *NAT* (*Network Address Translation*) en una red?

Opciones:

a. Crear tablas de ruteo para el tráfico de red.
b. Gestionar direcciones *IP* en servidores *DNS*.
c. Traducir direcciones *IP* privadas a direcciones *IP* públicas.
d. Establecer conexiones inalámbricas en una red.

Pregunta 10

El *NAT* (*Network Address Translation*) es un proceso en el cual se traduce una dirección *IP* privada a una dirección *IP* pública para permitir que los *hosts* locales se conecten a internet. Indica dos tipos de *NAT* comúnmente utilizados: *NAT* estático y *NAT* ____________.

Opciones:

a. dinámico
b. estático
c. privado
d. dinámico-estático

Pregunta 11

Selecciona la opción que describe correctamente una característica del servicio *Amazon S3*.

Opciones:

a. La replicación por lotes en *S3* se aplica automáticamente y sincroniza los *buckets* en diferentes regiones.
b. *S3 Object Lambda* te permite transferir datos en línea de manera eficiente.
c. *S3 Storage Lens* es una herramienta que te permite monitorear la consistencia de *Amazon S3* en tiempo real.
d. *Amazon S3* cifra cada objeto con una clave única, encriptada mediante otra clave que se encuentra rota.

Pregunta 12

¿Cuál es la principal función de *Amazon S3* en el almacenamiento de datos?

Opciones:

a. Proporcionar servicios de transferencia de datos.
b. Realizar análisis de *big data*.
c. Administrar y monitorear el almacenamiento de objetos.
d. Almacenar datos de forma segura en la nube.

Pregunta 13

¿Cuál es la herramienta de *Amazon* que permite monitorear el uso del almacenamiento de objetos en *S3* y proporciona recomendaciones para mejorar la rentabilidad y configurar la protección de datos?

Opciones:

a. *Amazon CloudTrail*
b. *S3 Storage Lens*
c. *Amazon CloudWatch*
d. *S3 Object Lambda*

Pregunta 14

Coloca en orden los siguientes elementos de *S3* según su capacidad de acceso:

1. *Buckets* de *S3*
2. Objetos
3. Etiquetas de objetos de *S3*
4. Prefijos

Opciones:

a. 1, 4, 3, 2
b. 1, 2, 3, 4
c. 4, 2, 3, 1
d. 2, 1, 4, 3

Pregunta 15

El servicio de *Amazon S3* almacena los datos como ________ y organiza estos datos en ________.

Opciones:

a. fragmentos, directorios
b. bloques, contenedores
c. objetos, *buckets*
d. registros, categorías

Pregunta 16

¿Cuál es el propósito principal de *AWS CloudTrail* según la información proporcionada?

Opciones:

a. Monitorizar y registrar la actividad de los usuarios en la infraestructura de *AWS*.
b. Almacenar datos operativos y métricas en la nube.
c. Monitorear y observar aplicaciones mediante la recopilación de datos operativos.
d. Evaluar continuamente las configuraciones de recursos de *AWS*.

Pregunta 17

¿Cuál de las siguientes herramientas de monitoreo en *AWS* se destaca por ofrecer la capacidad de evaluar continuamente las configuraciones de los recursos y enviar alertas en caso de cambios?

Opciones:

a. *VPC Flow Logs*
b. *AWS Config*
c. *CloudTrail*
d. *CloudWatch*

Pregunta 18

Relaciona cada herramienta de monitoreo y seguridad de *AWS* con su función principal.

Herramientas	Funciones Principales
1. *CloudWatch*	A. Monitoreo y observación de aplicaciones mediante la recopilación de datos operativos.
2. *CloudTrail*	B. Registro y monitoreo de la actividad de los usuarios en la infraestructura de *AWS*.
3. *AWS Config*	C. Monitoreo constante y registro de configuraciones de recursos.
4. *VPC Flow Logs*	D. Registro de tráfico de *IP* para diagnosticar reglas de grupo de seguridad.
5. *AWS Trusted Advisor*	E. Inspección del entorno de *AWS* y recomendaciones para ahorro de dinero, mejora de rendimiento, disponibilidad y seguridad.

Opciones:

a. 1-B, 2-A, 3-C, 4-D, 5-E
b. 1-A, 2-D, 3-B, 4-C, 5-E
c. 1-A, 2-B, 3-C, 4-D, 5-E
d. 1-D, 2-A, 3-C, 4-B, 5-E

Pregunta 19

Completa la siguiente afirmación: "*AWS CloudTrail* almacena dos tipos de eventos: eventos de administración, que identifican...".

Opciones:

a. la monitorización y observación de aplicaciones.
b. la visibilidad y datos operativos en *CloudWatch*.
c. la recopilación de datos operativos en la nube.
d. la creación o eliminación de recursos dentro de la infraestructura.

Pregunta 20

¿Cuál de las siguientes herramientas de *AWS* es más adecuada para evaluar y auditar la configuración de los recursos en busca de posibles problemas operativos?

Opciones:

a. *AWS Config*
b. *CloudWatch*
c. *VPC Flow Logs*
d. *AWS Trusted Advisor*

Pregunta 21

¿Cuál es una característica fundamental de las bases de datos relacionales?

Opciones:

a. Cada fila de la tabla tiene una clave única para relacionar datos.
b. Los datos lógicos y físicos están siempre integrados.
c. No es posible realizar operaciones lógicas en los datos.
d. Las bases de datos relacionales no permiten el uso de *SQL*.

Pregunta 22

El propósito principal de *Amazon Aurora* es ofrecer un motor de bases de datos relacionales que _______________.

Opciones:

a. reduzca la compatibilidad con *MySQL* y *PostgreSQL*
b. proporcione seguridad y disponibilidad para aplicaciones de alto rendimiento
c. ofrezca servicios de infraestructura sin administración de bases de datos
d. elimine la necesidad de migraciones entre bases de datos

Pregunta 23

Coloca en orden los siguientes elementos según los pasos que se deben seguir para desarrollar bases de datos relacionales:

1. Crear una base de datos llamada "paquetería".
2. Crear una tabla llamada "clientes" con campos: *ID* del cliente (clave única), nombre, dirección, teléfono, correo electrónico.
3. Crear una tabla llamada "paquetes" con un campo llamado "*ID* del cliente" para relacionar las tablas y colocar la información de los paquetes.

Opciones:

a. 2, 3, 1
b. 2, 1, 3
c. 1, 2, 3
d. 3, 2, 1

Pregunta 24

Según la información proporcionada, ¿cuál de las siguientes características es una ventaja específica de las bases de datos relacionales?

Opciones:

a. Uso de entidades subordinadas en las tablas.
b. Organización jerárquica de las tablas.
c. Manejo eficiente de datos gráficos y multimedia.
d. Claves únicas para evitar duplicidad de registros.

Pregunta 25

Completa la frase: *SQL* es el lenguaje que te permite _________________.

Opciones:

a. mejorar la productividad y disminuir el costo de la base de datos
b. ejecutar transacciones como un todo o un objeto
c. configurar la estructura de almacenamiento físico de las bases de datos
d. establecer una conexión con las bases de datos y realizar operaciones como consultar, modificar, agregar o eliminar datos

Pregunta 26

¿Cuál es uno de los beneficios clave de la integración continua?

Opciones:

a. Mejora la productividad de los desarrolladores al reducir tareas manuales y errores.
b. Permite la ejecución automática de código sin intervención humana.

c. Proporciona un servicio *Lambda* sin necesidad de servidor
d. Facilita la creación de sitios altamente potentes con *AWS Amplify*.

Pregunta 27

Relaciona los tipos de ataques cibernéticos mencionados con sus descripciones correspondientes.

Tipos de ataques	Descripciones
1. Inyección *SQL*	A. Ataque encubierto donde un *hacker* inserta un código para acceder a datos protegidos.
2. *Phishing*	B. Delito que engaña a las personas para compartir información confidencial.
3. Denegación de servicio en los sitios web	C. Intento de hacer que un recurso informático no esté disponible inundando con solicitudes.
4. *Ransomware*	D. Tipo de *malware* que impide el acceso a archivos y exige un rescate para recuperarlos.

Opciones:

a. 1-B, 2-A, 3-C, 4-D
b. 1-D, 2-A, 3-B, 4-C
c. 1-C, 2-D, 3-B, 4-A
d. 1-A, 2-B, 3-C, 4-D

Pregunta 28

Los siguientes eventos pueden desencadenar la ejecución automática de código en *AWS Lambda*, excepto:

Opciones:

a. Modificaciones de objetos en *Amazon S3*
b. Modificaciones de objetos en *MySQL*
c. Actualizaciones de tablas en *Amazon DynamoDB*
d. Solicitudes *HTTP* a través de *Amazon API Gateway*

Pregunta 29

Coloca en orden de prioridad las siguientes medidas para proteger *AWS Lambda*.

1. Utilizar *Multi-Factor Authentication* (*MFA*).
2. Configurar la *API* y el registro de actividad del usuario con *AWS CloudTrail*.
3. Utilizar *SSL/TLS* para comunicarse con los recursos de *AWS*.

Opciones:

a. 2,3,1
b. 3,2,1
c. 1, 3, 2
d. 1,2,3

Pregunta 30

En el contexto de la seguridad de la infraestructura en la nube, ¿cuál de las siguientes medidas es esencial para proteger los datos en *AWS Lambda*?

Opciones:

a. Configurar la *API* y el registro de actividad del usuario con *AWS CloudTrail.*
b. Ejecutar automáticamente el código en respuesta a eventos.
c. Utilizar *Multi-Factor Authentication* (*MFA*) con cada cuenta.
d. Ejecutar automáticamente el código en respuesta a eventos.

Pregunta 31

¿Cuál es una desventaja de la criptografía simétrica?

Opciones:

a. Proporciona integridad y autenticidad.
b. Necesitas compartir la clave.
c. Es fácil de usar.
d. Se enfoca en el algoritmo.

Pregunta 32

¿Cuál es uno de los beneficios clave de la criptografía asimétrica?

Opciones:

a. Utiliza una única clave para cifrar y descifrar.

b. Proporciona integridad, autenticidad y no repudio.
c. Es fácil de programar.
d. Requiere compartir la clave privada.

Pregunta 33

El ataque que más afecta a la criptografía simétrica es de fuerza bruta, el cual consiste en la ejecución de un programa que va cambiando un carácter de la posible clave hasta que consigue la correcta. Este ataque se caracteriza por su ________________.

Opciones:

a. enfoque en la criptografía asimétrica
b. utilización de múltiples claves
c. método sistemático y exhaustivo
d. rapidez en descifrar información

Pregunta 34

¿Cuál de las siguientes afirmaciones describe adecuadamente la criptografía asimétrica?

Opciones:

a. Es más vulnerable a los ataques de fuerza bruta.
b. Utiliza una única clave para cifrar y descifrar la información.
c. Implica el uso de un par de claves relacionadas: pública y privada.
d. Se basa en algoritmos rápidos y fáciles de implementar.

Pregunta 35

Relaciona los tipos de algoritmos de cifrado simétrico con sus descripciones correspondientes.

AES (*Advanced Encryption Estandar*)	A. Crea una matriz 4x4 y realiza rondas de cifrado para generar la clave.
2. *ChaCha20*	B. Cifrado de flujo de alta velocidad utilizado en conexiones *HTTPS*.
3. Cifrado *TwoFish*	C. Se utiliza en unidades de procesamiento de 32 bits y es más lento.

Opciones:

a. 1-A, 2-B, 3-C
b. 1-C, 2-A, 3-B
c. 1-B, 2-C, 3-A
d. 1-A, 2-C, 3-B

Pregunta 36

Según la información proporcionada, ¿cuál es el propósito principal de la prueba de penetración (*pentest*)?

Opciones:

a. Verificar la calidad del servicio en la nube.
b. Analizar la configuración de red y los mecanismos de seguridad.
c. Evaluar la eficiencia operativa de los sistemas.
d. Encontrar y remediar vulnerabilidades mediante ataques simulados.

Pregunta 37

En la fase de modelado de amenazas de un *pentest*, el *pentester* realiza la captura, organización y análisis de los datos desde el punto de vista de seguridad. Este proceso implica examinar detalladamente la información recopilada para identificar posibles riesgos y amenazas. Además, la información recopilada se organiza de manera que sea útil para la posterior elaboración de informes.

Completa la siguiente afirmación:
En esta fase, el *pentester* evalúa la información desde una perspectiva de seguridad para ________________ y proporcionar una base sólida para la ________________.

Opciones:

a. minimizar los impactos; monitorización continua
b. asegurar la confidencialidad; implementación de medidas preventivas
c. descartar amenazas; implementación de medidas correctivas
d. identificar riesgos y amenazas; elaboración de informes ejecutivos

---

Pregunta 38

Organiza las siguientes fases de un *pentest* en orden cronológico, comenzando por la primera:

1. Elaboración de informes
2. Análisis de vulnerabilidades
3. Reconocimiento
4. Modelado de amenazas

5. Explotación

Opciones:

a. 3, 2, 4 ,5 ,1
b. 1, 3, 4, 2, 5
c. 3, 1, 4, 2, 5
d. 3, 4, 2, 5, 1

Pregunta 39

Asocia cada fase de un *pentest* con su descripción correspondiente:

1. Reconocimiento	A. Fase donde se define el alcance y los objetivos de la prueba, incluyendo la recopilación de información sobre la empresa.
2. Análisis de vulnerabilidades	B. Fase en la que se analiza la respuesta del sistema a los ataques, mediante análisis estáticos y dinámicos.
3. Modelado de amenazas	C. Fase que implica la captura, organización y análisis de datos desde el punto de vista de seguridad.
4. Explotación	D. Momento de llevar a cabo la prueba para identificar todas las vulnerabilidades del sistema.
5. Elaboración de informes	E. Fase de documentación de todas las vulnerabilidades detectadas, con informes técnico y ejecutivo.

Opciones:

a. 1-B, 2-D, 3-C, 4-A, 5-E
b. 1-A,2-B,3-C,4-D,5-E
c. 1-A, 2-C, 3-D, 4-E, 5-B
d. 1-C, 2-A, 3-E, 4-B, 5-D

Pregunta 40

¿Cuál es la principal diferencia entre un *pentest* de caja blanca y unode caja negra?

Opciones:

a. En el *pentest* de caja blanca, el *pentester* busca archivos públicos para determinar vulnerabilidades, mientras que en el *pentest* de caja negra se revisa el código del sistema en tiempo real.
b. El *pentest* de caja blanca se realiza sin conocimiento previo de la empresa, mientras que en el *pentest* de caja negra se utiliza información técnica proporcionada por el personal de la empresa.
c. En el *pentest* de caja negra, el *pentester* tiene una visión parcial de los sistemas, mientras que en el *pentest* de caja blanca se tiene acceso total a la información técnica.
d. La fase de recopilación de información es crucial en el *pentest* de caja blanca, pero no es relevante en el *pentest* de caja negra.