Práctico N° 4 - Seguridad en la nube de AWS

1. ¿Quién es responsable de la seguridad de la nube según el modelo de responsabilidad compartida de AWS?
    a. Cliente
    b. Amazon
    c. Es una responsabilidad compartida
    d. Un tercero contratado por el cliente

2. ¿Cuál es la responsabilidad del cliente en el modelo de responsabilidad compartida de AWS en cuanto a la protección de datos en la nube?
    a. Proteger la infraestructura subyacente, incluyendo servidores, almacenamiento y redes.
    b. Proteger los datos mientras están en tránsito entre los servidores de AWS.
    c. Proteger los datos almacenados en la nube, incluyendo su cifrado y control de acceso.
    d. Ninguna de las anteriores.

3. ¿Cuál de las siguientes es una forma en que AWS puede ayudar a los clientes a proteger sus cuentas?
    a. Proporcionando herramientas de cifrado de datos en tránsito y en reposo.
    b. Ofreciendo servicios de autenticación y autorización, como AWS Identity and Access Management (IAM).
    c. Proporcionando herramientas de monitorización de seguridad, como Amazon GuardDuty.
    d. Todas las anteriores.

4. ¿Cuál de las siguientes opciones describe mejor el propósito de los roles de IAM en AWS?
    a. Los roles de IAM se utilizan para autenticar a los usuarios en AWS.
    b. Los roles de IAM se utilizan para establecer los permisos que los usuarios tienen para acceder a los recursos de AWS.
    c. Los roles de IAM se utilizan para conceder acceso a los recursos de AWS a aplicaciones y servicios que se ejecutan en la nube.
    d. Los roles de IAM se utilizan para otorgar permisos temporales a los usuarios o aplicaciones que necesitan realizar una tarea específica en AWS.

5. ¿Qué es AWS KMS y cómo se puede utilizar para proteger datos en AWS?
    a. AWS KMS es un servicio de gestión de claves que se utiliza para proteger los datos en tránsito en AWS.
    b. AWS KMS es un servicio de gestión de claves que se utiliza para proteger los datos en reposo en AWS.
    c. AWS KMS es un servicio de autenticación que se utiliza para proteger el acceso a los recursos de AWS.
    d. AWS KMS es un servicio de orquestación de eventos que se utiliza para proteger la cuenta de AWS contra ataques.

6. ¿Qué es Amazon Cognito y cómo se puede utilizar para proteger el acceso a las aplicaciones de AWS?
    a. Amazon Cognito es un servicio de gestión de identidades que se utiliza para proteger los datos en tránsito en AWS.
    b. Amazon Cognito es un servicio de gestión de claves que se utiliza para proteger los datos en reposo en AWS.
    c. Amazon Cognito es un servicio de autenticación que se utiliza para proteger el acceso a las aplicaciones web y móviles.
    d. Amazon Cognito es un servicio de orquestación de eventos que se utiliza para proteger la cuenta de AWS contra ataques.

7. ¿Cuál es la diferencia entre las políticas administradas y las políticas insertadas en IAM de AWS?
    a. Las políticas administradas son generalmente proporcionadas por AWS y las políticas insertadas son creadas por los usuarios.
    b. Las políticas administradas son generalmente creadas por los usuarios y las políticas insertadas son proporcionadas por AWS.
    c. Las políticas administradas son políticas globales y las políticas insertadas son políticas locales.

8. ¿Cuál de las siguientes medidas de seguridad tomaría para proteger el acceso a una cuenta de AWS? (Escoger dos)
    a. Habilitar una supervisión mejorada
    b. Otorgar los mínimos privilegios
    c. Habilitar Cloudtrail para monitoreo de performance detallado
    d. Habilitar Multi-Factor Authentication (MFA)
    e. Usar un solo rol para todos los usuarios de IAM

9. ¿Cuál de las siguientes entidades de administración de acceso e identificación (IAM) está asociada con una clave de acceso secreta y un ID de clave de acceso cuando se utiliza la interfaz de línea de comandos (CLI) de AWS?

a. IAM user
b. IAM role
c. IAM policy
d. IAM group