200 XP

# Prueba de conocimientos

5 minutos

Elija la respuesta más adecuada para cada una de las preguntas siguientes. Después, seleccione **Comprobar las respuestas**.

## Comprobación de conocimientos

**1.** Un administrador de base de datos SQL ha leído recientemente sobre ataques por inyección de código SQL. Pregunta qué se puede hacer para minimizar el riesgo de este tipo de ataque. ¿Cuál de las siguientes características ayudará a proteger la base de datos?

- (●) Advanced Threat Protection

  ✔ **Protección contra amenazas avanzada. Advanced Threat Protection es una característica de Advanced Data Security para bases de datos. La característica proporciona alertas cuando se produce un posible ataque, como inyección de código SQL.**

- ( ) Detección y clasificación de datos
- ( ) Enmascaramiento dinámico de datos

**2.** Una organización proporciona un servicio de soporte para sus clientes. Los representantes de servicio deben identificar a las personas que llaman mediante los cuatro últimos números de su tarjeta de crédito. Es necesario asegurarse de que el número completo de la tarjeta de crédito no esté totalmente expuesto a los representantes de servicio. ¿Cuál de las siguientes opciones debe implementar?

- ( ) Always Encrypted
- ( ) Clasificación de datos
- (●) Enmascaramiento dinámico de datos

  ✔ **Enmascaramiento dinámico de datos. El enmascaramiento dinámico de datos limita la exposición de información confidencial ocultándolos a**

los usuarios sin privilegios. Esta característica permite a los clientes designar la cantidad de datos confidenciales que se revelarán.

**3.** Los auditores deben estar seguros de que los datos confidenciales de la base de datos siempre permanecen cifrados en reposo, en tránsito y en uso. Para garantizar a los auditores que esto se está haciendo, ¿cuál de las siguientes características está configurada?

- (●) Always Encrypted

  ✔ **Always Encrypted. Always Encrypted ayuda a proteger la información confidencial en reposo en el servidor, durante el movimiento entre el cliente y el servidor, y mientras los datos están en uso. Always Encrypted garantiza que los datos confidenciales nunca van a aparecer como texto no cifrado dentro del sistema de base de datos. Después de configurar el cifrado de datos, solo las aplicaciones cliente o los servidores de aplicaciones que tienen acceso a las claves pueden acceder a los datos de texto no cifrado. Always Encrypted utiliza el algoritmo AEAD_AES_256_CBC_HMAC_SHA_256 para cifrar los datos de la base de datos.**

- ( ) Disk Encryption
- ( ) Enmascaramiento dinámico de datos

**4.** Una aplicación web de App Service usa una base de datos SQL. Los usuarios deben autenticarse en la base de datos con sus credenciales de Azure AD. ¿Cuál de las siguientes tareas de configuración habilitaría esto?

- ( ) Creación de un administrador de base de datos SQL
- ( ) Creación de un administrador de base de datos de Azure AD
- (●) Creación de usuarios en cada base de datos

  ✔ **No cree usuarios en la base de datos maestra. En su lugar, se deben crear usuarios contenidos en cada base de datos.**

**5.** ¿Qué tipo de reglas de firewall se pueden configurar para una base de datos de Azure SQL?

- ( ) Reglas de firewall de nivel de centro de datos
- (●) Reglas de firewall de nivel de servidor

  ✔ **Se pueden crear reglas de firewall de nivel de servidor y reglas de**

firewall de nivel de base de datos. Las reglas de firewall de IP de nivel de servidor permiten a los clientes acceder a toda la base de Azure SQL Database, es decir, todas las bases de datos dentro del mismo servidor de base de datos SQL. Estas reglas se almacenan en la base de datos maestra. Las reglas de firewall de IP de nivel de base de datos permiten a los clientes acceder a determinadas bases de datos seguras dentro del mismo servidor de base de datos SQL. Puede crear estas reglas para cada base de datos (incluida la base de datos maestra) y se almacenan en las bases de datos individuales.

- ○ Reglas de firewall de nivel de tabla

## Siguiente unidad: Resumen

Continuar >

¿Cómo lo estamos haciendo? ☆ ☆ ☆ ☆ ☆