

# Prueba de conocimientos

10 minutos

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

## Comprobación de conocimientos

1. Los auditores de cumplimiento quieren asegurarse de que, a medida que los empleados cambian de trabajo o dejan la empresa, también se cambian o revocan sus privilegios. Les preocupa especialmente el grupo Administrador. Para abordar sus problemas, ¿cuál de las siguientes opciones implementaría?

☒ Revisiones de acceso

✓ **Revisiones de acceso.** Las revisiones de acceso permiten a las organizaciones administrar de forma eficiente la pertenencia a grupos, el acceso a las aplicaciones empresariales y la asignación de roles. El acceso de los usuarios se puede revisar de forma periódica para asegurarse de que solo las personas adecuadas tengan acceso continuado.

☐ Directivas basadas en tiempo de Azure

☐ Acceso a la máquina virtual de JIT

2. Identity Protection ha informado de que se han filtrado las credenciales de un usuario. Según la directiva, se debe restablecer la contraseña del usuario. ¿Qué rol de Azure AD puede restablecer la contraseña?

☒ Administrador global

✓ **Administrador global.** Para usar Identity Protection, un usuario debe estar en uno de estos roles. Cada rol tiene privilegios diferentes, pero solo el administrador global puede restablecer la contraseña de un usuario.

☐ Administrador de seguridad

- ☐ Operador de seguridad

3. ¿En cuál de las siguientes clasificaciones identifica Identity Protection los riesgos?

- ☐ Dirección IP específica

- ☒ Viaje atípico

✓ Identity Protection puede reconocer inicios de sesión desde ubicaciones y horas inesperadas.

- ☐ Dispositivo no registrado

4. Ha implementado Identity Protection y está revisando el informe Usuarios de riesgo. Para cada evento notificado, ¿puede elegir cualquiera de las siguientes acciones?

- ☒ Confirmar el peligro del usuario

✓ Confirmar que un usuario se ha visto comprometido es una opción válida al revisar los informes de proyección de identidad.

- ☐ Eliminación del evento de riesgo

- ☐ Descartar la cuenta de usuario

5. ¿Para habilitar cuál de las acciones enumeradas a continuación puede usarse el acceso condicional?

- ☐ Bloquear o conceder acceso desde una hora específica del día.

- ☐ Designar cuentas de usuario con privilegios.

- ☒ Requerir autenticación multifactor.

✓ Es posible forzar a un usuario, a un grupo de usuarios o a todos los usuarios a utilizar MFA con una directiva de acceso condicional.

6. ¿Qué plan de licencias es compatible con Identity Protection?

- ☐ Azure Active Directory Free

- ☐ Azure Active Directory Premium P1

- ☒ Azure Active Directory Premium P2

✓ Identity Protection facilita la configuración del acceso condicional en

función del riesgo de las aplicaciones para protegerlas de riesgos basados en identidades.

---

## Siguiente unidad: Resumen

Continuar >