

# Microsoft Entra ID Protection

Microsoft Entra ID (anteriormente conocida como Azure Active Directory) es una herramienta que gestiona la seguridad de las identidades en la nube. Nos ayuda a **detectar, investigar y corregir riesgos basados en identidad**. Estos riesgos basados en identidad pueden incorporarse a herramientas como el acceso condicional para tomar decisiones de acceso a nuestros recursos.

---

## Objetivos Didácticos

El objetivo del curso se focaliza en que los estudiantes adquieran los conocimientos necesarios para **ayudar a las organizaciones a identificar, investigar y solucionar riesgos relacionados con la identidad** utilizando las herramientas que proporciona Microsoft Entra ID.

Aprenderás a **configurar y personalizar políticas de seguridad** en Azure AD Identity Protection para adaptarse a las necesidades de una organización.

---

## Audiencia

- Personal de IT responsable de la gestión de identidades y la seguridad de las cuentas de usuario en Azure AD.
- Administradores de seguridad de IT que desean aprender a proteger mejor las identidades y los datos de los usuarios en sus organizaciones.
- Analistas de seguridad que necesitan aprender a detectar y responder a incidentes relacionados con la seguridad de la identidad.

---

## Metodología

Aula virtual en directo.

---

## Duración

18 horas

---

## Temario del curso

1. **¿QUÉ ES LA PROTECCIÓN DE IDENTIDADES?**
  - 1.1. ¿Qué es el Riesgo?
  - 1.2. ¿Cómo investigar el Riesgo?
  - 1.3. Roles requeridos para poder trabajar con Microsoft Entra.
  - 1.4. Licenciamiento Requerido.
2. **MICROSOFT ENTRA ID PROTECTION DASHBOARD**
  - 2.1. Métricas.
  - 2.2. Gráficos de ataque.

- 2.2.1. Interpretar el gráfico de ataque.
  - 2.3. Filtros.
  - 2.4. Mapas.
  - 2.5. Recomendaciones.
- 3. TIPOS DE RIESGOS**
  - 3.1. Riesgos de Sign-in y sus tipos.
  - 3.2. Riesgos de Usuarios y sus tipos.
- 4. POLITICAS DE ACCESO BASADAS EN RIESGOS**
  - 4.1. Política de acceso condicional basada en riesgos de inicio de sesión.
  - 4.2. Política de acceso condicional basada en el riesgo del usuario.
  - 4.3. Políticas de protección de identidad.
  - 4.4. Política de registro de autenticación MFA de Microsoft Entra.
- 5. EXPERIENCIA DE LOS USUARIOS**
  - 5.1. Registro de autenticación MFA.
  - 5.2. Corrección de inicio de sesión en riesgo.
  - 5.3. Remediación de usuarios en riesgo.
- 6. PROTECCIÓN DE IDENTIDADES Y USUARIOS B2B**
  - 6.1. Desbloquear tu cuenta.
  - 6.2. Restablecer la contraseña del usuario.
  - 6.3. Descartar manualmente los riesgos de usuario.
- 7. SIMULACIÓN DE DETECCIONES DE RIESGO**