# [FORT] Seguridad en ambientes de computación híbrida y remota

# Desafíos de seguridad

- Acceso seguro: Solo los usuarios autorizados pueden acceder a los recursos corporativos
- Protección de datos: Los datos deben estar protegidos tanto en tránsito como en reposo.
- Gestión de dispositivos: Monitorizar y gestionar los dipositivos remotos revisando que cumplen las políticas de seguridad
- Amenazas emergentes: Adaptarse a las nuevas amenazas que usan vulnerabilidades en conexiones remotas y servicios en la nube

## Estrategias de seguridad

- Autenticación multifactor (MFA)
- Redes privadas virtuales (VPN)
- Zero Trust Architecture(ZTA)

## Herramientas y tecnologías de seguridad

- Azure Active Directory
- Microsoft Endpoint Manager
- Microsoft Defender for Endpoint

## Protección de datos

- Cifrado de datos
- Data prevention Loss

## Gestión de accesos e identidades

- Políticas de acceso condicional
- Sigle Sing-On

## Buenas políticas para la seguridad en el trabajo remoto

- Políticas de seguridad para trabajadores remotos.
- Monitoreo y respuesta a incidentes
- Seguridad del endpoing

# Inteligencia artificial y seguridad en Windows 11

- Detección y respuesta de amenazas:
  - Microsoft defender for endpoint: Usa IA y Machine Learning para analizar los datos de seguridad en tiempo real para detectar comportamientos anomalos y responder a amenazas avanzadas.