

Guía de Laboratorio - Tarea 18

Gobernanza, Cumplimiento y Protección de Datos

AZURE GOVERNANCE
BLUEPRINTS & SECURITY

1. Marco Conceptual

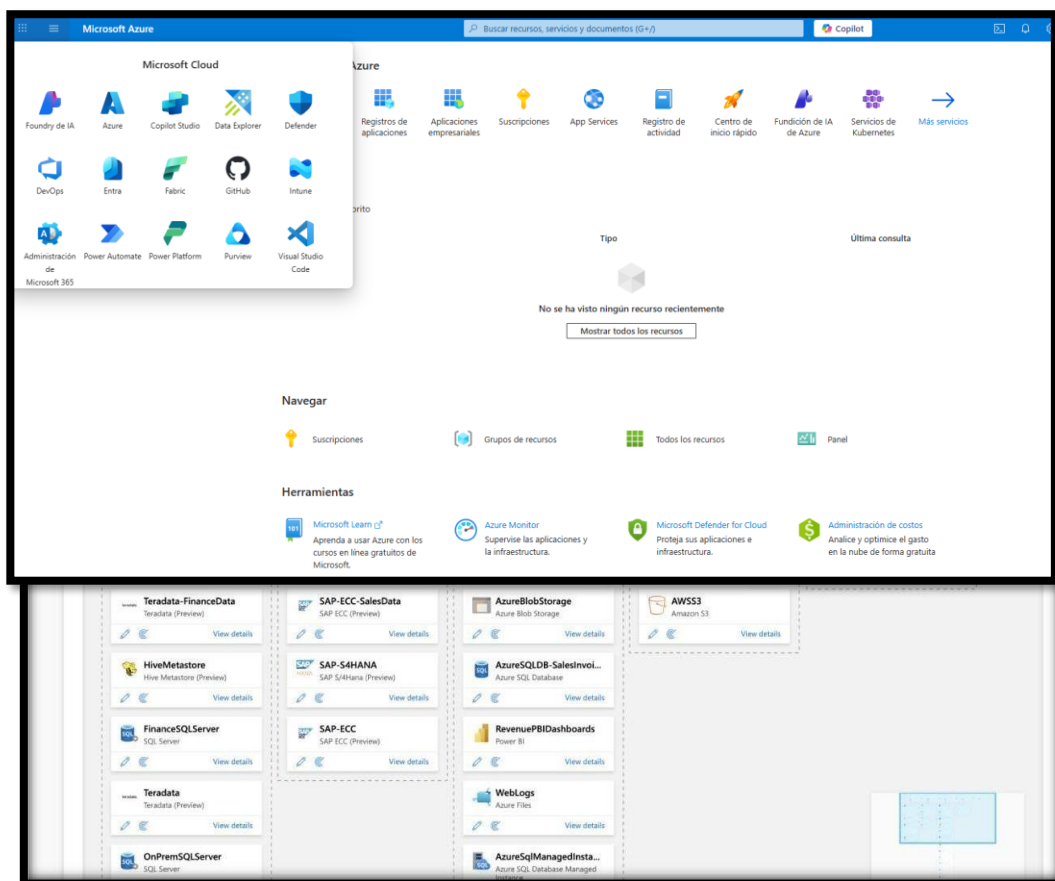
Control y Protección

La gobernanza establece las reglas para que la nube sea segura y manejable. Implementaremos Blueprints para estandarizar entornos y RBAC para controlar quién toca qué.

Referencia: [Protección de datos en entornos Big Data \(Hiberus\)](#)

Integrante Campana Gutierrez Erickson

1. Acceso y Verificación del Entorno El proceso inició ingresando al portal de Microsoft Purview mediante las credenciales institucionales y el enlace proporcionado en la guía. Se realizó una comprobación visual del tablero principal para asegurar que los módulos críticos (Gobernanza, Catálogos y Mapa de Datos) estuvieran operativos, confirmando así el acceso al entorno de trabajo correcto.

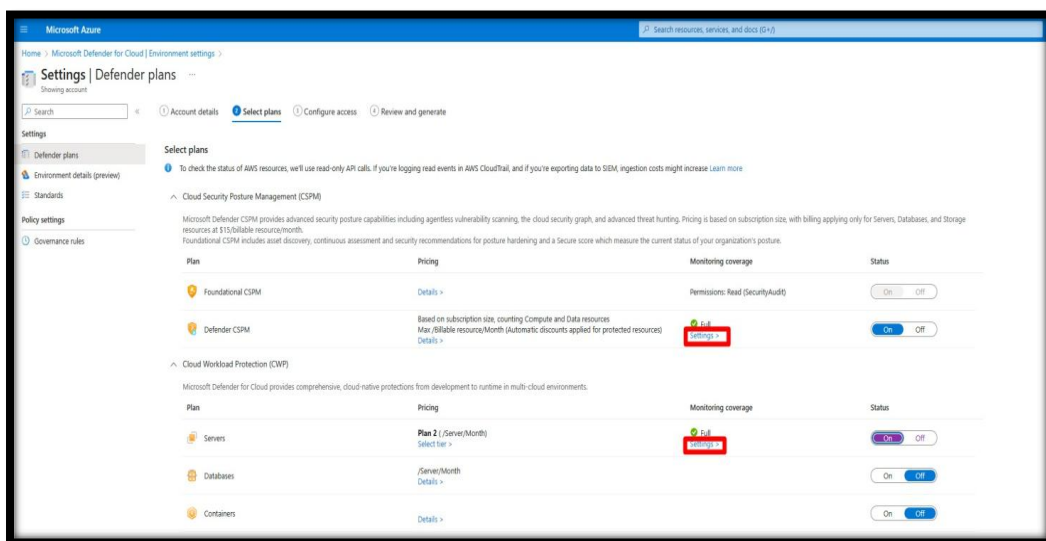


3. Integración de Fuentes en el Data Map Dentro de la sección de Mapa de Datos (*Data Map*), se procedió a dar de alta una nueva fuente siguiendo estos pasos:

- Selección de la tipología del recurso (ej. Azure SQL, Storage, etc.).
- Asignación de identificadores (nombre, ruta de acceso y suscripción).
- Finalización del registro y corroboración de que el nuevo recurso apareciera visible en la topología del mapa.

4. Ejecución del Análisis de Datos (Scanning) Sobre la fuente recién integrada, se programó una tarea de exploración:

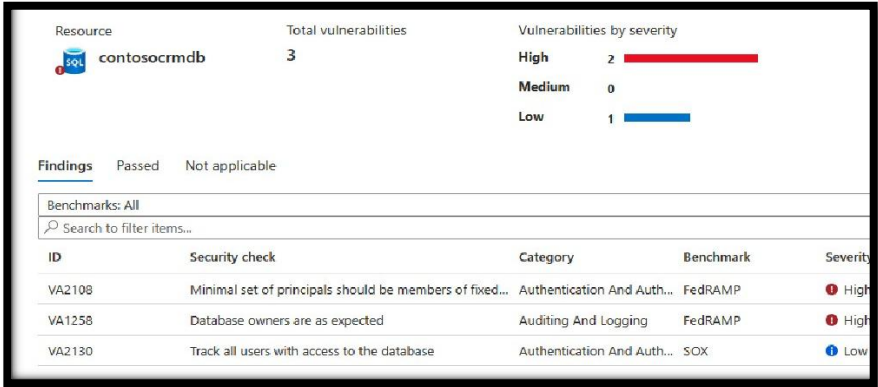
- Parametrización: Se establecieron las credenciales de acceso, se definió el alcance del escaneo (*scope*) y se fijó la frecuencia de ejecución.
- Lanzamiento: Se activó el proceso y se monitoreó el estado hasta confirmar que pasara a "En progreso", asegurando que la extracción de metadatos estaba en marcha.



5. Resultados y Catalogación Al concluir el análisis, se inspeccionó el reporte generado por Purview para validar:

- El volumen y naturaleza de los activos detectados.
- La precisión de los metadatos y las clasificaciones automáticas sugeridas.
- La correcta indexación de estos elementos dentro del Catálogo de Purview para su consulta.

6. Etiquetado y Clasificación Manual Se accedió al inventario de activos descubiertos. Tras revisar los detalles de un elemento específico, se le asignó una etiqueta de sensibilidad (como "Confidencial" o "Uso Interno") acorde a la normativa de la guía, guardando los cambios para reflejarlos en el sistema.



7. Validación Final en el Catálogo Para cerrar la práctica, se utilizó el motor de búsqueda de Purview. Se localizó el activo trabajado y se auditó su ficha técnica, verificando el linaje de los datos, la exactitud de la descripción y la presencia de las nuevas etiquetas de clasificación.

1. Actividades para el Estudiante

Azure AD Connect es una herramienta de Microsoft diseñada para cumplir y lograr sus objetivos de identidad híbrida. Permite sincronizar las identidades de su Active Directory (AD) local a Azure Active Directory (Azure AD).

Pasos Clave para Configurar Azure AD Connect:

1. Preparar los Requisitos Previos:

- Tener una suscripción de Azure y un inquilino de Azure AD.
- Tener un dominio AD local con al menos un controlador de dominio.
- Designar un servidor miembro del dominio (o el propio controlador de dominio, aunque no es la mejor práctica) para instalar Azure AD Connect.
- Disponer de credenciales de **Administrador de Empresa** (Enterprise Admin) en el AD local y de **Administrador Global** en Azure AD.
- Asegurar la conectividad de red (puertos necesarios, sin *firewalls* que bloqueen el tráfico hacia Azure AD).

2. Descargar e Instalar Azure AD Connect:

- Descargue la última versión del *software* desde el Centro de descarga de Microsoft.
- Ejecute el asistente de instalación en el servidor designado.

3. Selección del Método de Instalación:

Seleccione la **configuración rápida (*Express Settings*)** para la topología de un solo bosque de AD local o la **configuración personalizada (*Customize*)** para más opciones (por ejemplo, varios bosques, sincronización opcional, o el uso de una base de datos SQL Server existente).

4. Conexión a Azure AD:

- Introduzca las credenciales del **Administrador Global** de Azure AD para autenticar y establecer la conexión.

5. Conexión a Active Directory Local:

- Introduzca las credenciales de un administrador del dominio de AD local (o la cuenta de servicio de sincronización de Azure AD Connect que se creará, si se eligió la configuración rápida).

1. Explica cómo configurar políticas de seguridad en Azure Security Center y por qué son importantes.

Para configurar políticas de seguridad en lo que hoy conocemos como **Microsoft Defender for Cloud** (anteriormente Azure Security Center) y comprender su valor estratégico, puedes seguir esta guía detallada:

Cómo configurar las Políticas de Seguridad

El proceso se realiza directamente desde el portal de Azure y se centra en definir qué reglas deben cumplir tus recursos.

1. **Acceso a la Herramienta:** Ingresa al portal de Azure y busca **Microsoft Defender for Cloud**.
2. **Selección del Entorno:** En el menú lateral, dirígete a **"Configuración del entorno" (Environment settings)**. Aquí verás una lista de tus suscripciones o grupos de administración; selecciona aquella sobre la que deseas aplicar las reglas.
3. **Navegación a Políticas:** Dentro de la configuración de la suscripción, busca la sección **"Política de seguridad" (Security policy)**.
4. **Gestión de Estándares:** Verás que, por defecto, se aplica el *Azure Security Benchmark* (el estándar base de Microsoft).
 - **Para activar/desactivar reglas:** Puedes entrar en el estándar y modificar el estado de recomendaciones específicas si no aplican a tu negocio (para evitar "falsos positivos" en tus alertas).
 - **Para agregar normativas:** Utiliza la opción de **"Agregar más estándares"** si tu empresa necesita cumplir con regulaciones específicas de la industria como **ISO 27001**, **PCI DSS** (pagos), o **NIST**.

¿Por qué son importantes?

Las políticas de seguridad no son solo una lista de verificación; son el motor de la gobernanza en la nube por tres razones principales:

1. **Evaluación Continua y Automatizada:** Azure no descansa. Las políticas permiten que Defender for Cloud escanee constantemente tus recursos (servidores, bases de datos, redes) comparando su configuración real contra las reglas definidas. Si alguien deja un puerto abierto o una base de datos sin cifrar, el sistema lo detecta al instante.
2. **Visibilidad a través del "Secure Score":** Traducen el estado técnico de tu seguridad a un número comprensible: la **Puntuación de Seguridad**. Esto permite a los directivos y administradores saber rápidamente qué tan "sano" es su entorno. Si cumples con las políticas, la puntuación sube.
3. **Estandarización y Cumplimiento:** Garantizan que todos los recursos, sin importar quién los haya creado, cumplan con los mismos requisitos mínimos de seguridad. Esto es vital para pasar auditorías y mantener la integridad de los datos corporativos.

2. ¿Qué es Azure Policy y cómo se puede utilizar para asegurar la gobernanza en Azure? Proporcione un ejemplo.

¿Qué es Azure Policy?

Azure Policy es el servicio de Azure diseñado para hacer cumplir estándares organizacionales y evaluar el cumplimiento a escala. Imagínalo como un conjunto de "guardarraíles" o reglas automáticas que controlan las propiedades de los recursos que se crean o modifican en tu nube.

A diferencia de un sistema de monitoreo pasivo, Azure Policy actúa activamente: puede auditar recursos que no cumplen las reglas, modificar configuraciones automáticamente o impedir (denegar) la creación de recursos que violen tus normativas.

¿Cómo asegura la gobernanza?

La gobernanza en la nube se trata de mantener el control sobre costos, seguridad, coherencia y cumplimiento legal. Azure Policy es la herramienta principal para ejecutar esta estrategia mediante tres pilares:

Cumplimiento en Tiempo Real: Evalúa los recursos en el momento en que se intentan crear. Si una solicitud no cumple con la política (por ejemplo, intentar crear una máquina virtual gigante y costosa), Azure Policy puede bloquearla antes de que genere gastos.

Estandarización: Asegura que todos los equipos de desarrollo sigan las mismas reglas (por ejemplo, que todos los recursos tengan las etiquetas o "tags" correctas para facturación).

Remediación: Si ya existen recursos que incumplen una nueva norma, Azure Policy puede marcarse como "no conformes" o, en algunos casos, ejecutar tareas para corregirlos automáticamente.

Ejemplo Práctico

Escenario: Soberanía de Datos y Control de Regiones.

Imagina que tu empresa, por regulaciones legales (como el GDPR en Europa), tiene estrictamente prohibido almacenar datos o procesar información fuera de Europa Occidental.

La Política: Utilizas una definición de política integrada llamada "Allowed locations" (Ubicaciones permitidas).

La Configuración: Al asignar esta política a tu suscripción, seleccionas únicamente la región West Europe como parámetro permitido.

El Resultado (Efecto Deny): Si un administrador intenta crear una base de datos SQL o una máquina virtual en la región East US o Brazil South, Azure Policy interceptará la solicitud y la bloqueará, mostrando un mensaje de error indicando que la acción fue prohibida por la política de gobernanza de la empresa.

De esta forma, garantizas técnicamente que ningún error humano viole la normativa legal de la organización.

3. Detalla el proceso de configuración de Azure Compliance Manager para cumplir con los estándares de la empresa.

1. Prerrequisitos y Roles

Antes de iniciar, asegura tener los permisos adecuados. No todos los administradores tienen acceso por defecto.

- **Roles necesarios:** Necesitas ser *Administrador de cumplimiento (Compliance Administrator)*, *Administrador global* o *Administrador de datos de cumplimiento* para configurar evaluaciones.
- **Licenciamiento:** Las evaluaciones básicas (como Microsoft Cloud Security Benchmark) suelen ser gratuitas. Las plantillas premium (ISO 27001, NIST, GDPR, etc.) pueden requerir licencias E5 o complementos de cumplimiento.

2. Acceso y Configuración Inicial

1. Ingresa al **Portal de cumplimiento de Microsoft Purview** (<https://www.google.com/search?q=compliance.microsoft.com>).
2. En el menú de navegación izquierdo, selecciona **Compliance Manager (Administrador de cumplimiento)**.
3. **Configuración de pruebas automatizadas:**
 - Ve a *Configuración (Settings)* dentro del Administrador de cumplimiento.
 - Asegúrate de activar la **prueba automatizada de acciones de mejora**. Esto permite que Azure detecte automáticamente si has configurado algo correctamente (ej. si activaste MFA, el sistema lo detecta y sube tu puntuación sin que tengas que marcarlo manualmente).

3. Selección de Estándares (Plantillas de Evaluación)

Este es el paso crítico para alinear la herramienta con los "estándares de la empresa".

A. Usar Estándares de la Industria (Predefinidos)

Si tu empresa debe cumplir con normas internacionales:

1. Ve a la pestaña **Evaluaciones (Assessments) > Plantillas de evaluación**.
2. Busca la norma requerida (ej. *ISO 27001:2013*, *NIST 800-53*, *GDPR*).
3. Selecciona la plantilla y crea una evaluación.

B. Crear Estándares Personalizados (Internos)

Si tu empresa tiene políticas únicas que no están en una norma estándar:

1. Ve a **Plantillas de evaluación > Crear nueva plantilla**.
2. Puedes:
 - **Extender una plantilla existente:** Copiar una norma (como ISO) y agregarle controles extra de tu empresa.
 - **Importar desde Excel:** Crear una plantilla desde cero subiendo un archivo Excel con tus propios controles y acciones de mejora.

4. Creación de la Evaluación (Assessment)

Una vez elegida la plantilla, debes aplicarla a un ámbito específico.

1. Asigna un nombre (ej. "Auditoría ISO 27001 - Q4 2025").
2. **Seleccionar grupo:** Elige si aplica a toda la organización o a grupos específicos de recursos/usuarios.
3. Esto generará una **Puntuación de Cumplimiento** inicial basada en tu configuración actual.

5. Gestión de Acciones de Mejora (El trabajo operativo)

Aquí es donde se realiza el trabajo real de cumplimiento. Azure divide las responsabilidades en dos:

- **Acciones de Microsoft (Managed by Microsoft):** Controles que Microsoft gestiona por ti en la nube (seguridad física de datacenters, parcheo del host). Revisa estos para entender qué cubre tu proveedor.
- **Acciones del Cliente (Managed by Customer):** Lo que tu equipo debe hacer.
 1. Entra a tu evaluación y ve a la pestaña **Acciones de mejora**.
 2. Filtra por estado "No implementado".
 3. **Asignación:** Puedes asignar una acción técnica a un usuario específico (ej. "Configurar Firewall") y enviarle un correo desde la herramienta.

6. Documentación y Pruebas

Para cada control, debes evidenciar el cumplimiento:

1. Haz clic en una Acción de Mejora.
2. **Estado de implementación:** Cambia de "No implementado" a "Implementado" o "Implementación alternativa".
3. **Estado de prueba:** Indica si ha sido validado (Pasó, Falló, Fuera de alcance).
4. **Evidencia:** Sube documentos, capturas de pantalla o enlaces a políticas internas en la sección de notas/evidencia para auditorías futuras.

7. Monitoreo y Reportes

- **Puntuación:** Monitorea el *Compliance Score*. Una puntuación más alta indica menor riesgo.
- **Alertas:** Configura alertas para cambios críticos en la configuración que reduzcan tu puntuación.
- **Informes:** Utiliza el botón **Exportar** para generar un Excel con el estado de todos los controles. Esto es lo que generalmente se entrega a los auditores externos o a la gerencia.

Resumen de Mejores Prácticas

Fase	Acción Clave
Inicio	Activa las pruebas automatizadas para no trabajar doble.
Alcance	No apliques todas las normas a todo el tenant; segmenta por necesidad.
Operación	Asigna propietarios a los controles; no dejes todo al Oficial de Cumplimiento.
Mantenimiento	Revisa las actualizaciones de las plantillas (Azure actualiza las normas periódicamente).

4. ¿Cuáles son las mejores prácticas para implementar la encriptación de datos en Azure? Explique cómo asegurar tanto datos en reposo como en tránsito.

1. Gestión de Claves: La Base de Todo

Antes de cifrar datos, debes decidir quién tiene las llaves. La práctica fundamental es centralizar el control.

- **Azure Key Vault (AKV):** Es el servicio obligatorio para almacenar claves criptográficas, certificados y secretos. Nunca almacenes claves en código o archivos de configuración.
 - **Claves Administradas por el Cliente (CMK) vs. Plataforma (PMK):**
 - *PMK (Por defecto):* Microsoft gestiona y rota las claves. Es seguro y fácil, pero tú no tienes el control total.
 - *CMK (Recomendado para cumplimiento):* Tú generas y controlas las claves en tu Key Vault. Si revocas el acceso a la clave, los datos se vuelven inaccesibles inmediatamente (Kill Switch).
-

2. Asegurando Datos en Reposo (Data at Rest)

Esto protege los datos almacenados físicamente (discos, bases de datos, blobs) contra el robo físico del hardware o accesos no autorizados al almacenamiento.

A. Almacenamiento (Azure Storage)

Todos los datos en Azure Storage (Blob, Queue, Table, Files) se cifran automáticamente mediante **SSE (Server-Side Encryption)** usando AES de 256 bits.

- **Mejor práctica:** Habilita **CMK (Customer-Managed Keys)** para cuentas de almacenamiento que

contengan datos altamente confidenciales. Esto asegura que ni siquiera Microsoft pueda descifrar los datos sin tu permiso explícito en Key Vault.

B. Máquinas Virtuales (Compute)

Hay dos niveles de cifrado para VMs:

1. **Azure Disk Encryption (ADE):** Utiliza las características nativas del SO (*BitLocker* para Windows y *DM-Crypt* para Linux) para cifrar el disco desde dentro del sistema operativo.
 2. **Encryption at Host (Cifrado en el host):** Cifra los datos en el servidor físico de Azure antes de que fluyan al servicio de almacenamiento.
- **Mejor práctica:** Usa **ADE** si necesitas cumplimiento estricto que exige cifrado a nivel de SO. Usa **Encryption at Host** para un mejor rendimiento, ya que no consume CPU de la VM.

C. Bases de Datos (SQL y Cosmos DB)

- **Transparent Data Encryption (TDE):** Es el estándar para Azure SQL Database y SQL Managed Instance. Cifra los archivos de la base de datos, registros y copias de seguridad en tiempo real.
- **Always Encrypted:** Una función más avanzada donde los datos permanecen cifrados incluso en la memoria de la base de datos; solo la aplicación cliente tiene la clave para verlos. Úsalo para columnas con datos muy sensibles (ej. tarjetas de crédito, SSN).

3. Asegurando Datos en Tránsito (Data in Transit)

Esto protege los datos mientras se mueven entre el usuario y la nube, o entre servicios dentro de la nube, evitando ataques de "Man-in-the-middle".

A. Tráfico Externo (Usuario a Aplicación)

- **TLS 1.2 o superior:** Configura todos los servicios web (App Service, Front Door, Application Gateway) para rechazar conexiones TLS 1.0 o 1.1 (versiones obsoletas).
- **Certificados:** Gestiona la rotación automática de certificados SSL/TLS mediante Key Vault para evitar expiraciones que dejen el tráfico expuesto.

B. Tráfico Híbrido (On-Premises a Azure)

- **VPN IPsec:** Utiliza VPN Site-to-Site para cifrar el tráfico a través de internet público.
- **ExpressRoute con MACsec:** Si usas ExpressRoute (conexión privada dedicada), habilita **MACsec** (Media Access Control Security). Esto cifra los datos a nivel de capa física (Capa 2) entre tus routers y los de Microsoft, ofreciendo una seguridad superior a IPsec.

C. Tráfico Interno (VM a VM)

- **VNet Encryption:** Habilita esta función para cifrar el tráfico entre máquinas virtuales dentro de la misma red virtual (VNet) o redes emparejadas. Esto evita que un atacante que haya vulnerado una VM pueda "olfatear" el tráfico de la red interna.

Ámbito	Tecnología Clave	Práctica Recomendada
Claves	Azure Key Vault	Usar Managed HSM para claves críticas y rotarlas periódicamente.
Discos VM	ADE / Host Encryption	Cifrar discos OS y de datos; no dejar discos "crudos".
Bases de Datos	TDE / Always Encrypted	Mantener TDE activo y usar Always Encrypted para columnas PII.
Red	TLS / VPN / MACsec	Deshabilitar cifrados débiles (SSL 3.0, TLS 1.0/1.1) y forzar HTTPS .
Archivos	Storage Encryption	Usar CMK (claves propias) en lugar de las claves predeterminadas de Microsoft.