The DevOps Company

Microsoft Partner

AZ-500T00
Microsoft Azure Security Technologies

Sobre este curso.

Este curso proporciona a los profesionales de seguridad de TI el conocimiento y las habilidades necesarias para implementar controles de seguridad, mantener la postura de seguridad de una organización e identificar y remediar las vulnerabilidades de seguridad. Este curso incluye seguridad para la identidad y el acceso, protección de la plataforma, datos y aplicaciones, y operaciones de seguridad.

Duración.

4 Días.

Perfil del público.

Este curso está dirigido a ingenieros de seguridad de Azure que planean realizar el examen de certificación asociado o que realizan tareas de seguridad en su trabajo diario. Este curso también sería útil para un ingeniero que quiera especializarse en brindar seguridad para plataformas digitales basadas en Azure y desempeñar un papel integral en la protección de los datos de una organización.

Requisitos previos.

Los alumnos que superan la prueba tendrán conocimientos previos y comprensión de:

- Procedimientos recomendados y requisitos de seguridad del sector, como defensa en profundidad, acceso con privilegios mínimos, control de acceso basado en roles, autenticación multifactor, responsabilidad compartida y modelo de confianza cero.
- Protocolos de seguridad, como las redes privadas virtuales (VPN), el protocolo de seguridad de Internet (IPSec), la capa de sockets seguros (SSL), y los métodos de cifrado de discos y datos.
- Tener cierta experiencia en la implementación de cargas de trabajo de Azure En este curso no se cubren los conceptos básicos de la administración de Azure, sino que el contenido se basa en ese conocimiento al agregar información específica de seguridad.
- Tener experiencia con sistemas Windows y Linux, así como lenguajes de scripting.
- Los laboratorios del curso pueden usar PowerShell y la CLI.

Examen.

AZ-500: Microsoft Azure Security Technologies.

Temario.

Módulo 1: Protección de soluciones de Azure con Azure Active Directory.

Explore cómo configurar y administrar su instancia de Azure Active Directory de forma segura.

- Exploración de las características de Azure Active Directory.
- Comparación de Azure AD y Active Directory Domain Services.
- Investigación de roles en Azure AD.

- Implementación de Azure AD Domain Services.
- Creación y administración de usuarios de Azure AD.
- Administración de usuarios con grupos de Azure AD.
- Configuración de unidades administrativas de Azure AD.
- Implementación de la autenticación sin contraseña.
- Laboratorios.

Al final de este módulo, podrá:

- Configuración de Azure AD y Azure AD Domain Services para la seguridad.
- Creación de usuarios y grupos que habilitan el uso seguro del inquilino.
- Uso de MFA para proteger las identidades del usuario.
- Configuración de opciones de seguridad sin contraseña.

Módulo 2: Implementación de la identidad híbrida.

Explore cómo implementar y configurar Azure AD Connect para crear una solución de identidad híbrida para su empresa.

- Implementación de Azure AD Connect.
- Exploración de las opciones de autenticación.
- Configuración de la sincronización de hash de contraseña (PHS).
- Implementación de autenticación transferida (PTS).
- Implementación de la federación con Azure AD.
- Exploración del árbol de decisión de autenticación.
- Configurar la escritura diferida de contraseñas.

Al final de este módulo, podrá:

- Implementación de Azure AD Connect.
- Selección y configuración de la mejor opción de autenticación para sus necesidades de seguridad.
- Configurar la escritura diferida de contraseñas.

Módulo 3: Implementación de Azure AD Identity Protection.

Proteger las identidades de Azure AD mediante el acceso condicional, MFA, las revisiones de acceso y otras funcionalidades.

- Exploración de Azure AD Identity Protection.
- Configuración de detecciones de eventos de riesgo.
- Implementación de la directiva de riesgo de usuario.
- Implementación de la directiva de riesgo de inicio de sesión.
- Implementación de la autenticación multifactor en Azure.
- Exploración de la configuración de la autenticación multifactor.
- Habilitación de la autenticación multifactor.
- Implementación del acceso condicional de Azure AD.
- Configuración de las condiciones de acceso condicional.
- Implementación de revisiones de acceso.
- Laboratorios.

Al final de este módulo, podrá:

- Implementar y configurar Identity Protection.
- Configurar MFA para usuarios, grupos y aplicaciones.
- Crear directivas de acceso condicional para garantizar la seguridad.
- Crear y seguir un proceso de revisión de acceso.

Módulo 4: Configuración de Azure AD Privileged Identity Management.

Asegúrese de que las identidades con privilegios tengan protección adicional y proporcione el mínimo acceso necesario a estas para poder realizar el trabajo.

- Exploración del modelo de confianza cero.
- Revisión de la evolución de la administración de identidades.
- Implementación de Azure AD Privileged Identity Management.
- Configuración del ámbito de Privileged Identity Management.
- Implementación de la incorporación de Privileged Identity Management.
- Exploración de las opciones de configuración de Privileged Identity Management.
- Implementación de un flujo de trabajo de Privileged Identity Management.
- Laboratorios.

Al final de este módulo, sabrá hacer lo siguiente:

- Describir la Confianza cero y cómo afecta a la seguridad.
- Configurar e implementar roles con Privileged Identity Management (PIM).
- Evaluar la utilidad de cada configuración de PIM en relación con los objetivos de seguridad.

Módulo 5: Diseño de una estrategia de gobernanza empresarial.

Aprenda a usar RBAC y Azure Policy para limitar el acceso a las soluciones de Azure y determinar qué método es adecuado para sus objetivos de seguridad.

- Revisión del modelo de responsabilidad compartida.
- Exploración de las ventajas de la seguridad en la nube de Azure.
- Revisión de la jerarquía de sistemas de Azure.
- Configuración de directivas de Azure.
- Habilitación del control de acceso basado en rol (RBAC) de Azure.
- Comparación y contraste de Azure RBAC y directivas de Azure Policy.
- Configuración de roles integrados.
- Habilitación de bloqueos de recursos.
- Implementación de planos técnicos de Azure.
- Diseño de un plan de administración de suscripciones de Azure.
- Laboratorios.

Al final de este módulo, podrá:

- Explicación del modelo de responsabilidad compartida y cómo afecta a la configuración de seguridad.
- Creación de directivas de Azure para proteger las soluciones.
- Configuración e implementación del acceso a servicios mediante RBAC.

Módulo 6: Implementación de la seguridad perimetral.

Evite los ataques antes de que lleguen a las soluciones de Azure. Use los conceptos de Defensa en profundidad y Confianza cero para proteger el perímetro de Azure.

- Definir la defensa en profundidad.
- Exploración de la seguridad de red virtual.
- Habilitar la protección de Denegación de servicio distribuido (DDoS).
- Configuración de una implementación de protección de denegación de servicio distribuido.
- Exploración de las características de Azure Firewall.
- Implementación de Azure Firewall.
- Configuración de la tunelización forzada de VPN.
- Creación de rutas definidas por el usuario y aplicaciones virtuales de red.
- Exploración de una topología en estrella tipo hub-and-spoke
- Laboratorios.

Al final de este módulo, podrá:

- Definir la defensa en profundidad.
- Proteger el entorno de ataque por denegación de servicio.
- Proteger las soluciones con firewalls y VPN.
- Explorar la configuración de la seguridad perimetral de un extremo a otro en función de la posición de seguridad.

Módulo 7: Configuración de la seguridad de red.

Use las funcionalidades de red de Azure para proteger la red y las aplicaciones de ataques externos e internos.

- Exploración de grupos de seguridad de red (NSG).
- Implementación de grupos de seguridad de red.
- Creación de grupos de seguridad de aplicaciones.
- Habilitación de puntos de conexión de servicio.
- Configuración de servicios de punto de conexión de servicio.
- Implementación de vínculos privados.
- Implementación de una puerta de enlace de aplicación de Azure.
- Implementación de un firewall de aplicaciones web.
- Configuración y administración de Azure Front Door.
- Revisión de ExpressRoute.
- Laboratorios.

Al final de este módulo, podrá:

- Implementación y configuración de grupos de seguridad de red para proteger las soluciones de Azure.
- Configuración y bloqueo de puntos de conexión de servicio y vínculos privados.
- Protección de las aplicaciones con Application Gateway, firewall de aplicaciones web y Front Door.
- Configuración de ExpressRoute para ayudar a proteger el tráfico de red.

Módulo 8: Configuración y administración de la seguridad del host.

Aprenda a bloquear los dispositivos, las máquinas virtuales y otros componentes que ejecutan las aplicaciones en Azure.

- Habilitación de Endpoint Protection.
- Definición de una estrategia para dispositivos con privilegios de acceso.
- Implementación de estaciones de trabajo con privilegios de acceso.
- Crear plantillas de máquina virtual.
- Habilitación y protección de la administración de acceso remoto.
- Configurar administración de actualizaciones.
- Implementación del cifrado de disco.
- Implementación y configuración de Windows Defender.
- Exploración de recomendaciones de Microsoft Defender for Cloud.
- Protección de cargas de trabajo de Azure con pruebas comparativas de seguridad de Azure.
- Laboratorios.

Al final de este módulo, podrá:

- Configuración e implementación de Endpoint Protection.
- Implementación de una estrategia de acceso con privilegios para dispositivos y estaciones de trabajo con privilegios.
- Protección de las máquinas virtuales y acceso a ellas.
- Implementación de Windows Defender.
- Práctica de la seguridad por capas mediante la revisión e implementación de Security Center y pruebas comparativas de seguridad.

Módulo 9: Habilitación de la seguridad de contenedores.

Explore cómo proteger las aplicaciones que se ejecutan en contenedores y cómo conectarse a ellas de forma segura.

- Exploración de contenedores.
- Configuración de la seguridad de Azure Container Instances.
- Administración de la seguridad para Azure Container Instances (ACI).
- Exploración de Azure Container Registry (ACR).
- Habilitación de la autenticación de Azure Container Registry.
- Revisión de Azure Kubernetes Service (AKS).
- Implementación de una arquitectura de Azure Kubernetes Service.
- Configuración de redes de Azure Kubernetes Service.
- Implementación del almacenamiento de Azure Container Service.
- Protección de la autenticación en Azure Kubernetes Service con Active Directory.
- Administración del acceso a Azure Kubernetes Service mediante controles de acceso basado en rol de Azure.

Al final de este módulo, podrá:

- Definir las herramientas de seguridad disponibles para contenedores en Azure.
- Configurar la seguridad de contenedores y servicios de Kubernetes.
- Bloquear los recursos de red, almacenamiento e identidad conectados a sus contenedores.
- Implementar RBAC para controlar el acceso a los contenedores

Módulo 10: Implementación y protección de Azure Key Vault.

Proteja sus claves, certificados y secretos en Azure Key Vault. Aprenda a configurar el almacén de claves para la implementación más segura.

- Explorar Azure Key Vault.
- Configuración del acceso a Key Vault.
- Revisión de un ejemplo de Key Vault seguro.
- Implementación y administración de certificados de Key Vault.
- Creación de claves de Key Vault.
- Administración de claves administradas por el cliente.
- Habilitación de secretos de Key Vault.
- Configuración de la rotación de claves.
- Administración de características de seguridad y recuperación de Key Vault.
- Laboratorios.
- Exploración del módulo de seguridad de hardware de Azure.

Al final de este módulo, podrá:

- Definición de lo que es un almacén de claves y cómo protege certificados y secretos.
- Implementar y configurar Azure Key Vault.
- Proteger el acceso y la administración del almacén de claves.
- Almacenar claves y secretos en el almacén de claves.
- Exploración de consideraciones de seguridad clave, como la rotación de claves y la copia de seguridad o recuperación.

Módulo 11: Configuración de las características de seguridad de una aplicación.

Registre las aplicaciones de la empresa y, a continuación, use las características de seguridad de Azure para configurar y supervisar un acceso seguro a la aplicación.

- Revisión de la Plataforma de identidad de Microsoft.
- Exploración de escenarios de aplicación de Azure AD.
- Registro de una aplicación con el registro de aplicaciones.
- Configuración de permisos de Microsoft Graph.
- Habilitar identidades administradas.
- Implementación de certificados de aplicación web.
- Laboratorios.

Al final de este módulo, podrá:

- Registrar una aplicación en Azure mediante el registro de aplicaciones.
- Seleccionar y configurar los usuarios de Azure AD que pueden acceder a cada aplicación.
- Configurar e implementar certificados de aplicación web.

Módulo 12: Implementación de la seguridad de almacenamiento.

Asegúrese de que el almacenamiento y la transferencia de los datos, así como el acceso a los mismos, se realiza de forma segura mediante las características de seguridad de archivos y almacenamiento de Azure.

- Definición de la soberanía de datos.
- Configuración del acceso a Azure Storage.
- Implementación de firmas de acceso compartido.
- Administración de la autenticación de almacenamiento de Azure AD.
- Implementación del cifrado del servicio de almacenamiento.
- Configuración de directivas de retención de datos de blobs.
- Configuración de la autenticación de Azure Files.
- Habilitación de la propiedad obligatoria de transferencia segura.
- Laboratorios.

Al final de este módulo, podrá:

- Definición de la soberanía de datos y cómo se logra en Azure.
- Configuración del acceso de Azure Storage de forma segura y administrada.
- Cifrado de los datos mientras están en reposo y en tránsito.
- Aplicación de reglas para la retención de datos.

Módulo 13: Configuración y administración de la seguridad de bases de datos SQL.

Configure y bloquee la base de datos SQL en Azure para proteger los datos corporativos mientras están almacenados.

- Habilitación de la autenticación de bases de datos SQL.
- Configuración de firewalls de base de datos SQL.
- Habilitación y supervisión de la auditoría de bases de datos.
- Implementar detección y clasificación de datos.
- Explorar la evaluación de vulnerabilidad.
- Habilitación de Defender para SQL (Advanced Threat Protection).
- Configuración del enmascaramiento de datos dinámicos.
- Implementar cifrado de datos transparente.
- Implementar características de Always Encrypted.
- Implementación de Always Encrypted.
- Laboratorios.

Al final de este módulo, podrá:

- Configurar qué usuarios y aplicaciones tienen acceso a las bases de datos SQL.
- Bloquear el acceso a los servidores mediante firewalls.
- Detectar, clasificar y auditar el uso de los datos.
- Cifrar y proteger los datos mientras están almacenados en la base de datos.

Módulo 14: Configuración y administración de Azure Monitor.

Use Azure Monitor, Log Analytics y otras herramientas de Azure para supervisar el funcionamiento seguro de las soluciones de Azure.

- Explorar Azure Monitor.
- Configuración y supervisión de métricas y registros.
- Habilitación de Log Analytics.
- Administración de orígenes conectados para el análisis de registros.
- Habilitación de las alertas de Azure Monitor.
- Configuración de propiedades para el registro de diagnóstico.
- Laboratorios.

Al final de este módulo, podrá:

- Configurar y supervisar Azure Sentinel.
- Definir las métricas y los registros de los que quiera realizar un seguimiento para las aplicaciones de Azure.
- Conectar orígenes de datos a Log Analytics y configurar el servicio.
- Crear y supervisar alertas asociadas a la seguridad de las soluciones.

Módulo 15: Habilitar y administrar Microsoft Defender para la nube.

Use Azure Security Center, Azure Defender y Puntuación de seguridad para realizar un seguimiento de su posición de seguridad en Azure y mejorarlo.

- Revisión de la cadena de eliminación cibernética.
- Implementar Microsoft Defender para la nube.
- Configuración de las directivas del centro de seguridad.
- Administración e implementación de las recomendaciones del centro de seguridad.
- Exploración de la puntuación de seguridad.
- Implementación de Microsoft Defender for Cloud.
- Definición de ataques por fuerza bruta.
- Implementación del acceso a máquinas virtuales Just-In-Time.
- Laboratorios.

Al final de este módulo, podrá:

- Definir los tipos más comunes de ciberataques.
- Configurar Azure Security Center en función de la posición de seguridad.
- Revisar la Puntuación de seguridad y elevarla.
- Bloquear las soluciones mediante Security Center y Defender.
- Habilitar el acceso Just-In-Time y otras características de seguridad.

Módulo 16: Configuración y supervisión de Microsoft Sentinel

Use Azure Sentinel para detectar, realizar un seguimiento y responder a las infracciones de seguridad dentro del entorno de Azure.

- Habilitación de Microsoft Sentinel.
- Configuración de conexiones de datos a Sentinel.
- Creación de libros para explorar datos de Sentinel.
- Habilitación de reglas para crear incidentes.
- Configuración de cuadernos de estrategias.
- Búsqueda e investigación de posibles infracciones.

Al final de este módulo, podrá:

- Explicación de qué es Azure Sentinel y cómo se usa
- Implementación de Azure Sentinel
- Conectar datos a Azure Sentinel, como registros de Azure, Azure AD y otros
- Seguimiento de incidentes mediante libros, cuadernos de estrategias y técnicas de búsqueda