ExecuTrain

Impulsamos tu talento tecnológico

MICROSOFT	RED HAT	VIRTUALIZACIÓN
CIBERSEGURIDAD	DESARROLLO	OFFICE
BIG DATA	BLOCK CHAIN	BASES DE DATOS
GESTIÓN DE SERVICIOS IT	CLOUD COMPUTING	METODOLOGÍAS EN PROYECTOS
SISTEMAS OPERATIVOS	Y MÁS...	

www.executrain.com.mx

¿Por qué ExecuTrain?

ExecuTrain es un proveedor de entrenamiento corporativo a nivel internacional y líder mundial en la capacitación empresarial. Contamos con más de 30 años de Experiencia y con más de 75 mil personas capacitadas a nivel Nacional.

Te guiamos en la definición de tus requerimientos de capacitación, en las diferentes etapas:

- ✓ Detección de necesidades, evaluación de conocimientos, plan de capacitación y seguimiento posterior para elegir el plan de capacitación como tú lo necesitas.
- ✓ El **más amplio catálogo de cursos**, desde un nivel básico hasta los niveles de conocimientos más especializados.
- ✓ En ExecuTrain el material y la **metodología están diseñados por expertos en aprendizaje humano**. Lo que te garantiza un mejor conocimiento en menor tiempo.
- ✓ Tú puedes confiar y estar seguro del aprendizaje porque nuestro **staff de instructores es de primer nivel**, algunos de los cuales son consultores en reconocidas empresas.
- ✓ No pierdas tu tiempo, los cursos están diseñados para un aprendizaje práctico.

Nuestro compromiso es que tú aprendas, si no quedas satisfecho con los resultados del programa, podrás volver a tomar los cursos hasta tu entera satisfacción o la devolución de tu dinero.

Modalidad de Servicio

Cursos en Fecha Calendario

Súmate a nuestros grupos en fechas públicas.

Cursos Privados

On site, en nuestras instalaciones o en línea con instructor en vivo.

Autoestudio con soporte de instructor

Cursos en modalidad autoestudio, con acceso 24/7 a la plataforma de estudio, con soporte de instructor y foros de ayuda

ExecuTrain
Impulsamos tu talento tecnológico

Duración: 28 horas

AZ-500 / Secure cloud resources with Microsoft security technologies

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.

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.

Rol de trabajo: Ingeniero de Seguridad
Preparación para el examen: AZ-500

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..

Módulos

Administración de controles de seguridad para la identidad y el acceso

Este módulo se centra en administrar eficazmente los controles de seguridad en el identificador de Microsoft Entra mediante la protección de identidades, autenticación y autorización para proteger usuarios, grupos e identidades externas frente a amenazas, a la vez que garantiza un acceso seguro y sin problemas a los recursos.

- Introducción
- Prueba comparativa de seguridad en la nube de Microsoft: Administración de identidades y acceso con privilegios
- ¿Qué es Microsoft Entra ID?
- Proteger a los usuarios de Microsoft Entra

- Creación de un nuevo usuario en microsoft Entra ID
- Protección de grupos de Microsoft Entra
- Se recomienda cuándo usar identidades externas
- Protección de identidades externas
- Implementación de Microsoft Entra Identity Protection
- Microsoft Entra Connect
- Microsoft Entra Cloud Sync
- Opciones de autenticación
- Sincronización de hash de contraseñas con el identificador de Microsoft Entra
- Autenticación de tránsito de Microsoft Entra
- Federación con el identificador de Entra de Microsoft
- ¿Qué es la autenticación de Microsoft Entra?
- Implementación de la autenticación multifactor (MFA)
- Autenticación Kerberos
- Administrador de Redes de Área Local de Nueva Tecnología (NTLM)
- Opciones de autenticación sin contraseña para Microsoft Entra ID
- Implementación de la autenticación sin contraseña
- Implementación de la protección con contraseña
- Inicio de sesión único de Microsoft Entra ID
- Implementación del inicio de sesión único (SSO)
- Integrar el inicio de sesión único (SSO) y los proveedores de identidad
- Introducción al identificador comprobado de Microsoft Entra
- Configuración del identificador comprobado de Microsoft Entra
- Recomendar y aplicar protocolos de autenticación modernos
- Grupos de administración de Azure
- Configuración de permisos de rol de Azure para grupos de administración, suscripciones, grupos de recursos y recursos
- Control de acceso basado en rol de Azure
- Roles integrados de Azure
- Asignación de permisos de rol de Azure para grupos de administración, suscripciones, grupos de recursos y recursos
- Roles integrados de Microsoft Entra
- Asignar roles integrados en Microsoft Entra ID
- Control de acceso basado en rol de Microsoft Entra
- Creación y asignación de un rol personalizado en el identificador de Microsoft Entra
- Seguridad de confianza cero
- Microsoft Entra Privileged Identity Management
- Configuración de Privileged Identity Management
- Gobierno de Microsoft Entra ID
- Administración del ciclo de vida de la identidad
- Flujos de trabajo de ciclo de vida
- Administración de derechos
- Delegación y roles en la administración de derechos
- Revisiones de acceso
- Configure la administración de roles y las revisiones de acceso mediante el Gobierno de Microsoft Entra ID
- Implementación de directivas de acceso condicional para recursos en la nube en Azure
- Introducción a Azure Lighthouse
- Evaluación del módulo
- Resumen

Administración del acceso a aplicaciones en Microsoft Entra

En este módulo se explica cómo administrar el acceso a las aplicaciones en el identificador de Microsoft Entra, incluido el control del acceso a aplicaciones empresariales, la administración de registros y permisos de aplicaciones, el uso de entidades de servicio y la configuración del proxy de aplicación de Microsoft Entra para el acceso seguro.

- Introducción
- Administrar el acceso a las aplicaciones empresariales en el identificador de Microsoft Entra, incluidas las concesiones de permisos de OAuth
- Administración de registros de aplicaciones en Microsoft Entra ID
- Configurar ámbitos del permiso de registro de aplicaciones
- Gestión del consentimiento de permisos para el registro de aplicaciones
- Administrar y usar entidades de servicio
- Administración de identidades administradas para recursos de Azure
- Recomendación sobre cuándo usar y configurar una instancia de Microsoft Entra Application Proxy, incluida la autenticación
- Evaluación del módulo
- Resumen

Planeamiento e implementación de la seguridad de las redes virtuales

Este módulo está diseñado para proporcionar a los administradores los conocimientos y aptitudes necesarios para planear e implementar medidas de seguridad sólidas para redes virtuales de Azure, lo que garantiza la confidencialidad, integridad y disponibilidad de los recursos de red.

- Introducción
- Prueba comparativa de seguridad en la nube de Microsoft: protección de datos, registro y detección de amenazas y seguridad de red
- ¿Qué es una Azure Virtual Network?
- Azure Virtual Network Manager
- Planear e implementar grupos de seguridad de red (NSG) y grupos de seguridad de aplicaciones (ASG)
- Planeamiento e implementación de las rutas definidas por el usuario
- Planeamiento e implementación del emparejamiento de Red Virtual o puerta de enlace de Red Virtual
- Planifique e implemente una Red de Área Amplia Virtual, incluido el concentrador virtual protegido.
- Conectividad VPN segura, incluyendo de punto a sitio y de sitio a sitio
- Cifrado de Azure
- ¿Qué es el cifrado de Azure Virtual Network?
- Azure ExpressRoute
- Implementación del cifrado a través de ExpressRoute
- Configuración del firewall en recursos de Azure
- Supervisión de la seguridad de red con Network Watcher
- Resumen

Planeamiento e implementación de la seguridad para el acceso privado a los recursos de Azure

Este módulo se centra en equipar a los administradores con los conocimientos y aptitudes necesarios para planear e implementar medidas de seguridad sólidas para el acceso privado a los recursos de Azure, proteger los datos confidenciales y mejorar la integridad de la red.

- Introducción
- Planeamiento e implementación de puntos de conexión de servicio de red virtual
- Planificar e implementar puntos de conexión privados
- Planeamiento e implementación de servicios de Private Link
- Planeamiento e implementación de la integración de red de Azure App Service y Azure Functions
- Planificar e implementar configuraciones de seguridad de red de una instancia de App Service Environment (ASE)
- Planeamiento e implementación de configuraciones de seguridad de red de una instancia de Azure SQL Managed Instance
- Evaluación de módulos
- Resumen

Planeamiento e implementación de la seguridad para el acceso público a los recursos de Azure

Este módulo permite a los administradores planear e implementar una seguridad sólida para los recursos de Azure, lo que garantiza la confidencialidad, la integridad y la disponibilidad de las aplicaciones o servicios.

- Introducción
- Planee e implemente la seguridad de la capa de transporte (TLS) en las aplicaciones, incluido Azure App Service y API Management.
- Planificación, implementación y administrará una instancia de Azure Firewall, las directivas de firewall y de Azure Firewall Manager
- Planeamiento e implementación de una instancia de Azure Application Gateway
- Planear e implementar un firewall de aplicaciones web (WAF)
- Planee e implemente una instancia de Azure Front Door, incluida Content Delivery Network (CDN)
- Se recomienda cuándo usar Azure DDoS Protection Standard
- Evaluación de módulos
- Resumen

Planear e implementar la seguridad avanzada para la computación

Este módulo está diseñado para proporcionar a los administradores los conocimientos y aptitudes necesarios para planear e implementar medidas de seguridad avanzadas para los recursos de proceso de Azure, proteger las aplicaciones y los datos frente a las amenazas de seguridad en constante evolución.

- Introducción
- Planee e implemente el acceso remoto a puntos de conexión públicos, Azure Bastion y el acceso a una máquina virtual (VM) cuando sea necesario (JIT)
- ¿Qué es Azure Kubernetes Service?
- Configuración del aislamiento de red para Azure Kubernetes Service (AKS)
- Protección y supervisión de Azure Kubernetes Service
- Configuración de la autenticación para Azure Kubernetes Service
- Configure la seguridad para Azure Container Instances (ACI)
- Configure la seguridad de Azure Container Apps (ACA)
- Administración del acceso a Azure Container Registry (ACR)
- Configuración del cifrado de disco, Azure Disk Encryption (ADE), cifrado como host y cifrado de disco confidencial
- Recomendaciones de configuraciones de seguridad para Azure API Management
- Evaluación de módulos
- Resumen

Planeamiento e implementación de la seguridad para el almacenamiento

Este módulo está diseñado para proporcionar a los administradores los conocimientos y aptitudes necesarios para planear e implementar medidas de seguridad completas para los recursos de almacenamiento de Azure, proteger la integridad de los datos, la confidencialidad y la disponibilidad.

- Introducción
- Azure Storage
- Configuración del control de acceso para cuentas de almacenamiento
- Administrar el ciclo de vida de las claves de acceso de la cuenta de almacenamiento
- Selección y configuración de un método adecuado para el acceso a Azure Files
- Selección y configuración de un método adecuado para el acceso a blobs de Azure
- Selección y configuración de un método adecuado para el acceso a Tablas de Azure
- Selección y configuración de un método adecuado para el acceso a las colas de Azure

- Seleccionar y configurar los métodos adecuados para proteger de amenazas de seguridad de datos, incluidas las eliminaciones temporales, las copias de seguridad, el control de versiones y el almacenamiento inmutable
- Configuración de Bring Your Own Key (BYOK)
- Habilitación del cifrado doble en el nivel de infraestructura de Azure Storage
- Evaluación de módulos
- Resumen

Planeamiento e implementación de la seguridad de Azure SQL Database e Instancia administrada de Azure SQL

Este módulo está diseñado para capacitar a los administradores con los conocimientos y aptitudes necesarios para planear e implementar medidas de seguridad sólidas para Azure SQL Database e Instancia administrada de Azure SQL, lo que garantiza la protección de datos y el cumplimiento normativo.

- Introducción
- Seguridad de Azure SQL Database y de SQL Managed Instance
- Habilitación de la autenticación de bases de datos en Microsoft Entra
- Habilitación y supervisión de la auditoría de bases de datos
- Identificar casos de uso del Portal de gobernanza de Microsoft Purview
- Implementar la clasificación de datos de información confidencial con el Portal de gobernanza de Microsoft Purview
- Planeamiento e implementación de enmascaramiento dinámico
- Implementar cifrado de datos transparente
- Se recomienda cuándo usar Always Encrypted de Azure SQL Database
- Implementación de un firewall de Azure SQL Database
- Evaluación de módulos
- Resumen

Implementación y administración del cumplimiento de las directivas de gobernanza en la nube

Este módulo se centra en permitir que los administradores planeen, implementen y administren de forma eficaz la gobernanza de la seguridad en Azure, lo que garantiza el cumplimiento de las directivas organizativas y los procedimientos recomendados.

- Introducción
- Referencia de seguridad en la nube de Microsoft: acceso, datos, identidad, red, punto de conexión, gobernanza, recuperación, incidentes y administración de vulnerabilidades
- Gobernanza en Azure
- Creación, asignación e interpretación de directivas e iniciativas de seguridad en Azure Policy
- Implementación de infraestructuras seguras mediante una zona de aterrizaje
- Azure Key Vault
- Seguridad de Azure Key Vault
- Autenticación de Azure Key Vault
- Creación y configuración de una instancia de Azure Key Vault
- Recomienda cuándo usar un módulo de seguridad de hardware dedicado (HSM)
- Configurar el acceso a Key Vault, incluidas las directivas de acceso de almacén y el control de acceso basado en roles de Azure
- Administración de certificados, secretos y claves
- Configura la rotación de claves
- Configuración de la copia de seguridad y recuperación de certificados, secretos y claves
- Implementación de controles de seguridad para proteger las copias de seguridad
- Implementar controles de seguridad para la gestión de activos
- Evaluación del módulo
- Resumen

Administración de la posición de seguridad mediante Microsoft Defender for Cloud

En este módulo se enseña a los administradores a administrar y mejorar la seguridad en la nube mediante Microsoft Defender for Cloud, centrándose en la identificación y corrección proactivas de riesgos.

- Introducción
- Implementar Microsoft Defender para la nube
- Identificar y corregir riesgos de seguridad mediante el inventario y la puntuación de seguridad de Microsoft Defender for Cloud
- Evaluación del cumplimiento con marcos de seguridad y Microsoft Defender for Cloud
- Agregar estándares regulatorios y del sector a Microsoft Defender for Cloud
- Incorporación de iniciativas personalizadas a Microsoft Defender for Cloud
- Conexión de entornos de nube híbrida y multinube a Microsoft Defender for Cloud
- Implementar y utilizar la Administración de superficie expuesta a ataques externos de Microsoft Defender
- Evaluación de módulos
- Resumen

Configuración y administración de la protección contra amenazas mediante Microsoft Defender for Cloud

Este módulo se centra en las técnicas esenciales para configurar y administrar la protección contra amenazas exclusivamente con Microsoft Defender for Cloud, lo que permite a los especialistas en ciberseguridad reforzar la posición de seguridad de sus entornos en la nube.

- Introducción
- Habilitación de los servicios de protección de cargas de trabajo en Microsoft Defender for Cloud
- Defender para servidores
- Defender para Storage
- Examen de malware en Defender para Storage
- Detección de amenazas a datos confidenciales
- Implementar Microsoft Defender para Storage
- Habilitación de la configuración de la directiva integrada de Azure
- Configurar planes de Microsoft Defender para servidores, bases de datos y almacenamiento
- Implementación y administración de la administración de vulnerabilidades de Microsoft Defender
- Área de trabajo de Log Analytics
- Administrar la retención de datos en un área de trabajo de Log Analytics
- Implementación del agente de Azure Monitor
- Recopilación de datos con el Agente de Azure Monitor
- Reglas de recopilación de datos (DCR) en Azure Monitor
- Transformaciones en reglas de recopilación de datos (DCR)
- Supervisión de eventos de seguridad de red y datos de rendimiento mediante la configuración de reglas de recopilación de datos (DCR) en Azure Monitor
- Conectar las suscripciones de Azure
- Acceso a la máquina Just-In-Time
- Habilitar acceso Just-In-Time
- Seguridad de contenedores en Microsoft Defender para contenedores
- Factores de amenaza de Kubernetes administrados
- Arquitectura de Defender for Containers
- Configuración de los componentes de Microsoft Defender para contenedores
- Microsoft Defender para la seguridad de DevOps en la nube
- Soporte y requisitos previos de DevOps Security
- Posición de seguridad del entorno de DevOps
- Conexión del entorno de laboratorio de GitHub a Microsoft Defender for Cloud

- Configuración de la acción de GitHub de DevOps de seguridad de Microsoft
- Protección contra amenazas de IA en Defender for Cloud
- Habilitación de la protección contra amenazas para cargas de trabajo de IA en Defender for Cloud
- Obtención del contexto de la aplicación y el usuario final para alertas de IA
- Ejercicio: Configuración de Microsoft Defender for Cloud para la protección mejorada
- Comprobación de conocimientos
- Resumen

Configuración y administración de soluciones de automatización y supervisión de seguridad

En este módulo se enseña a configurar y administrar herramientas de seguridad con Azure Monitor y Microsoft Sentinel. Ayuda a las organizaciones a encontrar y tratar rápidamente problemas de seguridad en su configuración en la nube.

- Introducción
- Administración de alertas de seguridad y respuesta a ellas en Microsoft Defender for Cloud
- Configuración de la automatización de flujos de trabajo con Microsoft Defender para la nube
- Planes de retención de registros en Microsoft Sentinel
- Alertas e incidentes de Microsoft Sentinel
- Configuración de conectores de datos en Microsoft Sentinel
- Habilitar reglas de análisis en Microsoft Sentinel
- Configuración de la automatización en Microsoft Sentinel
- Automatización de la respuesta a amenazas con Microsoft Sentinel
- Evaluación de módulos
- Resumen