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

SC-100 / Microsoft Cybersecurity Architect

Se trata de un curso avanzado de nivel de experto. Aunque no es necesario asistir, se recomienda encarecidamente que los alumnos hayan aprobado otra certificación de nivel de técnico auxiliar en la cartera seguridad, cumplimiento e identidad (como AZ-500, SC-200 o SC-300) antes de asistir a esta clase. Este curso prepara a los alumnos con la experiencia para diseñar y evaluar estrategias de ciberseguridad en las siguientes áreas: Confianza cero; gobernanza, riesgo y cumplimiento (GRC), operaciones de seguridad (SecOps) y datos y aplicaciones. Los alumnos también aprenderán a diseñar soluciones siguiendo los principios de confianza cero y a especificar los requisitos de seguridad para la infraestructura en la nube en diferentes modelos de servicio (SaaS, PaaS, IaaS).

Perfil del Público

Este curso es para ingenieros de seguridad en la nube con experiencia que han aprobado una certificación anterior en la cartera seguridad, cumplimiento e identidad. Concretamente, los alumnos deben tener experiencia y conocimientos avanzados en una amplia gama de áreas de ingeniería de seguridad, como la identidad y el acceso, la protección de plataformas, las operaciones de seguridad, la protección de datos y la protección de aplicaciones. También deben tener experiencia con implementaciones híbridas y en la nube. En su lugar, los alumnos principiantes deben realizar el curso SC-900: Conceptos básicos de seguridad, cumplimiento e identidad de Microsoft.

Rol de trabajo: Arquitecto de soluciones
Preparación para el examen: SC-100

Requisitos Previos

Antes de asistir a este curso, los estudiantes deben tener:

- ✓ Se recomienda encarecidamente haber asistido y superado una de las certificaciones de nivel asociado en la cartera de seguridad, cumplimiento e identidad (como AZ-500, SC-200 o SC-300)
- ✓ Experiencia avanzada y conocimientos sobre la identidad y el acceso, la protección de plataformas, las operaciones de seguridad, la protección de datos y la protección de aplicaciones.
- ✓ Experiencia en implementaciones híbridas y en la nube.

Módulos

Introducción a la Confianza cero y los marcos de Mejores Prácticas

Obtendrá información sobre las prácticas recomendadas de seguridad y antipatrones, el concepto de Zero Trust y sus principios rectores, y los marcos clave de mejores prácticas, como CAF, WAF, MCRA y MCSB. También obtendrá información sobre el marco de adopción de Confianza cero y cómo se relacionan los marcos entre sí.

- Introducción
- Describir antipatrones y procedimientos recomendados
- Descripción del concepto de Confianza cero
- Describir los marcos
- Describir el marco de adopción de Confianza cero
- Describir cómo se relacionan los marcos entre sí
- Evaluación del módulo
- Resumen

Diseñar soluciones de seguridad que se alineen con Cloud Adoption Framework (CAF) y Well-Architected Framework (WAF)

Obtendrá información sobre Cloud Adoption Framework (CAF) y el Marco de buena arquitectura (WAF) y cómo puede usarlos para diseñar soluciones más seguras.

- Introducción
- Comprender el Cloud Adoption Framework
- Descripción de la metodología segura de Cloud Adoption Framework
- Descripción de las zonas de aterrizaje de Azure
- Diseño de la seguridad con zonas de aterrizaje de Azure
- Descripción del Marco de buena arquitectura
- Comprender el pilar de seguridad de Well-Architected Framework
- Evaluación de una estrategia de seguridad
- Definición de una estrategia de seguridad
- Recomendar soluciones para la seguridad y la gobernanza
- Diseño de procesos de DevSecOps seguros
- Diseño de una estrategia para la adopción segura de la inteligencia artificial
- Evaluación del módulo
- Resumen

Diseño de soluciones que se alineen con la Arquitectura de referencia de ciberseguridad de Microsoft (MCRA) y Microsoft Cloud Security Benchmark (MCSB)

Obtendrá información sobre los marcos de seguridad de Microsoft (el marco de adopción de seguridad (SAF), la arquitectura de referencia de ciberseguridad de Microsoft (MCRA) y Microsoft Cloud Security Benchmark (MCSB) y cómo usarlos para diseñar soluciones seguras que protejan contra amenazas internas, ataques externos, riesgos en la cadena de suministro y riesgos específicos de la inteligencia artificial.

- Introducción
- Describir la arquitectura de referencia de ciberseguridad de Microsoft
- Descripción de Microsoft Cloud Security Benchmark
- Diseñar soluciones con procedimientos recomendados para funcionalidades y controles
- Diseño de soluciones con procedimientos recomendados para proteger contra ataques internos, externos y de cadena de suministro.
- Diseño de soluciones de inteligencia artificial que se alinean con Microsoft Cloud Security Benchmark
- Diseño de soluciones que se alinean con el marco de adopción de Confianza cero
- Evaluación del módulo
- Resumen

Diseño de una estrategia de resistencia para ransomware y otros ataques en función de los procedimientos recomendados de seguridad de Microsoft

Obtendrá información sobre ciberamenazas comunes, como el ransomware, y para qué tipos de patrones de ataque se debe preparar una organización.

- Introducción
- Patrones comunes de ciberamenazas y ataques
- Compatibilidad con la resistencia empresarial
- Diseñar soluciones para mitigar ataques de ransomware, incluida la priorización de BCDR y el acceso con privilegios
- Diseño de soluciones para continuidad empresarial y recuperación ante desastres (BCDR), incluida la copia de seguridad y restauración seguras
- Evaluación de soluciones para actualizaciones de seguridad
- Evaluación del módulo
- Resumen

Diseño de soluciones para el cumplimiento normativo

Aprenda a diseñar soluciones de seguridad que aborden los requisitos de cumplimiento normativo en entornos multinube. Aprenderá a traducir los requisitos de cumplimiento en controles de seguridad, usar el Administrador de cumplimiento de Microsoft Purview para el cumplimiento multinube, incluida la gobernanza de inteligencia artificial, abordar los requisitos de privacidad con Microsoft Priva, diseñar soluciones de Azure Policy y evaluar el cumplimiento mediante Microsoft Defender for Cloud.

- Introducción
- Traducción de los requisitos de cumplimiento en controles de seguridad
- Consideraciones de cumplimiento de inteligencia artificial
- Diseñar una solución para abordar los requisitos de cumplimiento mediante Microsoft Purview
- Abordar los requisitos de privacidad con Microsoft Priva
- Abordar los requisitos de seguridad y cumplimiento con Azure Policy
- Evaluar y validar la alineación con estándares normativos y pruebas comparativas mediante Microsoft Defender for Cloud
- Evaluación del módulo
- Resumen

Diseño de soluciones para la administración de identidades y acceso

Diseñe soluciones de administración de identidades y acceso que protejan los recursos de la organización al tiempo que permiten la productividad. Obtenga información sobre cómo diseñar estrategias de acceso para diferentes modelos de implementación, habilitar la colaboración externa segura, implementar la autenticación moderna y proteger la infraestructura de identidad.

- Presentación
- Diseño de una solución para el acceso a recursos SaaS, PaaS, IaaS, híbridos y multinube
- Diseñar una solución para microsoft Entra ID, incluidos entornos híbridos y multinube
- Diseñar una solución para identidades externas
- Diseñar estrategias modernas de autenticación y autorización
- Diseño de una solución para identidades de agente mediante Microsoft Entra Agent ID
- Diseño de directivas de acceso condicional para agentes de IA
- Validación de la alineación de las directivas de acceso condicional con una estrategia de Zero Trust
- Especificación de los requisitos para proteger Active Directory Domain Services
- Diseñar una solución para administrar secretos, claves y certificados.
- Prueba de conocimientos
- Resumen

Diseño de soluciones para proteger el acceso con privilegios

Aprenderá técnicas avanzadas para diseñar soluciones que protejan el acceso con privilegios

mediante los principios de confianza cero, el modelo de acceso empresarial y las funcionalidades de gobernanza de id. de Microsoft Entra, incluidas las consideraciones para las cargas de trabajo de inteligencia artificial y los entornos multinube.

- Introducción
- Asegurar acceso privilegiado
- Diseño de la asignación de roles con privilegios mediante enterprise Access Model
- Evaluación de la seguridad y la gobernanza con soluciones de Microsoft Entra ID
- Diseño de una solución para proteger la administración de inquilinos
- Diseño de una solución para la administración de derechos de infraestructura en la nube
- Diseño de una solución para estaciones de trabajo de acceso con privilegios y acceso remoto
- Evaluación de una solución de administración de revisiones de acceso
- Evaluación del módulo
- Resumen

Diseño de soluciones para operaciones de seguridad

Aprenderá técnicas para diseñar capacidades de operaciones de seguridad, como el registro, la auditoría, la Administración de eventos e información de seguridad (SIEM), la Orquestación de la seguridad y la respuesta automatizada (SOAR) y los flujos de trabajo de seguridad.

- Introducción
- Describir la función de las operaciones de seguridad (SecOps)
- Supervisión de diseño para admitir entornos híbridos y multinube
- Soluciones de diseño para admitir el registro y la auditoría centralizados
- Soluciones de diseño para la detección y respuesta que incluyen detección y respuesta ampliadas (XDR) y administración de información y eventos de seguridad (SIEM)
- Diseño de una solución para la orquestación de seguridad, automatización y respuesta (SOAR)
- Diseñar y evaluar flujos de trabajo de seguridad, incluida la respuesta a incidentes, la búsqueda de amenazas y la administración de incidentes
- Diseñar y evaluar la cobertura de detección de amenazas mediante matrices de MITRE ATT&CK, como Cloud, Enterprise, Mobile e ICS
- Evaluación del módulo
- Resumen

Caso práctico interactivo: Modernización de la identidad y la seguridad de los datos

Aplique sus aptitudes de arquitecto de ciberseguridad en un escenario empresarial real centrado en la seguridad de identidades y datos. Analice los requisitos de diseño, responda a preguntas conceptuales y técnicas y diseñe una solución para satisfacer las necesidades empresariales.

- Introducción
- Caso práctico interactivo
- Aspectos destacados del caso práctico interactivo
- Comprobación de conocimientos
- Resumen

Caso práctico interactivo: Modernización del control de acceso de los usuarios y la resistencia a amenazas

Aplique sus aptitudes de arquitecto de ciberseguridad en un escenario empresarial real centrado en el control de acceso de los usuarios y la resistencia a amenazas. Analice los requisitos de diseño, responda a preguntas conceptuales y técnicas y diseñe una solución para satisfacer las necesidades empresariales.

- Introducción
- Caso práctico interactivo
- Aspectos destacados del caso práctico interactivo
- Comprobación de conocimientos
- Resumen

Evaluar soluciones para proteger Microsoft 365

Aprenderá a evaluar las soluciones de seguridad para proteger Microsoft 365.

- Introducción
- Evaluación de la posición de seguridad de las cargas de trabajo de productividad y colaboración mediante métricas
- Evaluar cómo Microsoft Defender para Office 365 y Microsoft Defender for Cloud Apps proteger las cargas de trabajo de productividad
- Evaluar cómo Microsoft Intune protege y administra los puntos de conexión
- Evaluación de soluciones para proteger datos en Microsoft 365 mediante Microsoft Purview
- Evaluar cómo los controles de seguridad y cumplimiento de datos protegen los datos de la organización utilizados por Microsoft 365 Copilot
- Evaluación del módulo
- Resumen

Diseño de soluciones para proteger aplicaciones

Aprenderá a proteger las aplicaciones, las API y el proceso de desarrollo mediante técnicas como la administración de posiciones, el modelado de amenazas y el acceso seguro para las identidades de carga de trabajo.

- Introducción
- Diseñar e implementar estándares para proteger el desarrollo de aplicaciones
- 9 min
- Diseño de una estrategia de ciclo de vida completo para la seguridad de las aplicaciones
- Evaluación de la posición de seguridad de las carteras de aplicaciones existentes
- Evaluación de amenazas de aplicación con modelado de amenazas
- Acceso seguro para identidades de carga de trabajo
- Diseño de una solución para la administración y seguridad de API
- Diseño de una solución para el acceso seguro a las aplicaciones
- Asignación de tecnologías a los requisitos de seguridad de las aplicaciones
- Evaluación del módulo
- Resumen

Diseño de soluciones para proteger los datos de una organización

Obtenga información sobre cómo diseñar soluciones que protejan los datos de una organización mediante funcionalidades como Microsoft Purview, Defender para SQL y Defender para Storage.

- Introducción
- Principios y marcos de diseño de seguridad de datos
- Evaluación de soluciones para la detección y clasificación de datos
- Especificación de prioridades para mitigar las amenazas a los datos
- Evaluación de soluciones para el cifrado de datos en reposo y en tránsito, incluido Azure KeyVault y el cifrado de infraestructura
- Diseño de la seguridad de datos para cargas de trabajo de Azure
- Diseño de la seguridad de los datos usados en las cargas de trabajo de IA
- Diseño de la seguridad para Azure Storage
- Diseño de una solución de seguridad con Microsoft Defender para SQL y Microsoft Defender para Storage
- Evaluación del módulo
- Resumen

Caso práctico interactivo: Protección de aplicaciones y datos

Aplique sus aptitudes de arquitecto de ciberseguridad en un escenario empresarial real centrado en proteger las aplicaciones y los datos. Analice los requisitos de diseño, responda a preguntas conceptuales y técnicas y diseñe una solución para satisfacer las necesidades empresariales.

- Introducción
- Caso práctico interactivo
- Aspectos destacados del caso práctico interactivo
- Comprobación de conocimientos
- Resumen

Especificación de los requisitos para proteger los servicios SaaS, PaaS e IaaS

Aprenderá a analizar los requisitos de seguridad para diferentes ofertas en la nube (SaaS, PaaS e IaaS), cargas de trabajo de IoT, cargas de trabajo web, contenedores y cargas de trabajo de IA.

- Introducción
- Especificación de las líneas de base de seguridad para los servicios SaaS, PaaS e IaaS
- Especificación de los requisitos de seguridad para cargas de trabajo de IoT
- Especificación de los requisitos de seguridad para cargas de trabajo web
- Especificar los requisitos de seguridad para contenedores y la orquestación de contenedores.
- Especificación de los requisitos de seguridad para cargas de trabajo de IA
- Evaluación de la seguridad de las cargas de trabajo de Microsoft Foundry
- Evaluación del módulo
- Resumen

Diseño de soluciones para la administración de la posición de seguridad en entornos híbridos y multinube

Aprenderá a diseñar soluciones de administración de posturas de seguridad que se integran en escenarios híbridos y multinube mediante funcionalidades en Microsoft Defender for Cloud, Azure Arc y Microsoft Cloud Security Benchmark (MCSB).

- Introducción
- Evaluación de la posición de seguridad mediante Microsoft Defender for Cloud, incluido el banco de pruebas de seguridad en la nube de Microsoft
- Evaluación de la posición de seguridad mediante Puntuación de seguridad de Microsoft
- Diseñar soluciones de administración de posturas integradas que incluyen Microsoft Defender for Cloud en entornos híbridos y multinube
- Seleccionar soluciones de protección de cargas de trabajo en la nube en Microsoft Defender for Cloud
- Diseño de una solución para integrar entornos híbridos y multinube mediante Azure Arc
- Diseño de una solución para Administración de superficie expuesta a ataques externos de Microsoft Defender
- Especificar los requisitos y las prioridades para un proceso de gestión de posturas que utiliza rutas de ataque de Microsoft Security Exposure Management
- Evaluación del módulo
- Resumen

Diseño de soluciones para proteger los puntos de conexión de cliente y servidor

Aprenderá a analizar los requisitos de seguridad para distintos tipos de puntos de conexión, incluidos servidores, clientes, IoT, OT, dispositivos móviles y dispositivos insertados. Estos requisitos tienen en cuenta diferentes plataformas y sistemas operativos y establecerán estándares para la protección de puntos de conexión, el refuerzo de la seguridad y la configuración.

- Introducción a la seguridad de los puntos de conexión
- Especificar los requisitos de seguridad para los servidores
- Especificación de los requisitos de seguridad para dispositivos móviles y clientes
- Especificación de los requisitos de seguridad para dispositivos IoT y sistemas insertados
- Evaluar soluciones para proteger la tecnología operativa (OT) y los sistemas de control industrial (ICS) mediante Microsoft Defender para IoT
- Especificar las líneas base de seguridad para los puntos de conexión de servidor y de cliente
- Diseño de una solución para el acceso remoto seguro
- Evaluación de las soluciones de Solución de contraseñas de administrador local (LAPS) de Windows
- Evaluación del módulo
- Resumen

Diseño de soluciones para la seguridad de red

Aprenderá a diseñar soluciones de red seguras mediante técnicas como la segmentación de red, el filtrado de tráfico, la supervisión de red y la administración de posturas.

- Presentación
- Evaluar los diseños de red para alinearse con los requisitos de seguridad y los procedimientos recomendados
- Diseñar soluciones para la segmentación de la red
- Diseñar soluciones para el filtrado del tráfico con grupos de seguridad de red
- Soluciones de diseño para la administración de la posición de red
- Diseño de soluciones para la supervisión de la red
- Evaluación de soluciones que usan Acceso a Internet de Microsoft Entra
- Evaluar soluciones que usan Acceso privado de Microsoft Entra
- Evaluación del módulo
- Resumen

Caso práctico interactivo: Protección de puntos de conexión e infraestructura

Aplique sus aptitudes de arquitecto de ciberseguridad en un escenario empresarial real centrado en la seguridad de la infraestructura y los puntos de conexión. Analice los requisitos de diseño, responda a preguntas conceptuales y técnicas y diseñe una solución para satisfacer las necesidades empresariales.

- Introducción
- Caso práctico interactivo
- Aspectos destacados del caso práctico interactivo
- Comprobación de conocimientos
- Resumen