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

Diseño de soluciones que se alineen con los procedimientos recomendados de seguridad y las prioridades

Aprenderá a usar procedimientos recomendados de seguridad críticos de Microsoft, como Cloud Adoption Framework (CAF), el Marco de buena arquitectura (WAF) y la Arquitectura de referencia de ciberseguridad de Microsoft (MCRA) para mejorar la posición de seguridad de una organización, aplicar principios de la Confianza cero y minimizar el riesgo de ataques emergentes.

- **Introducción a los marcos de procedimientos recomendados y la Confianza cero**

Conozca qué son los procedimientos recomendados y cómo los usan los arquitectos de ciberseguridad, así como algunos marcos clave de procedimientos recomendados para las funcionalidades de ciberseguridad de Microsoft. También obtendrá información sobre el concepto de Confianza cero y cómo empezar a trabajar con la Confianza cero en una organización.

  - Introducción a los procedimientos recomendados
  - Introducción a la Confianza cero
  - Iniciativas de Confianza cero
  - Pilares tecnológicos de la Confianza cero, parte
  - Pilares tecnológicos de la Confianza cero, parte
  - Prueba de conocimientos: Introducción a los marcos de procedimientos recomendados y la Confianza cero
  - Resumen: introducción a los marcos de procedimientos recomendados y la Confianza cero

- **Diseño de soluciones que se alineen con Cloud Adoption Framework (CAF) y el Marco de buena arquitectura (WAF)**

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

  - Definición de una estrategia de seguridad
  - Introducción a Cloud Adoption Framework
  - Metodología de seguridad de Cloud Adoption Framework
  - Introducción a las zonas de aterrizaje de Azure
  - Diseño de la seguridad con zonas de aterrizaje de Azure
  - Introducción al Marco de buena arquitectura
  - Pilar de seguridad del Marco de buena arquitectura
  - Prueba de conocimientos: Cloud Adoption Framework (CAF) y Marco de buena arquitectura (WAF)
  - Resumen: Diseño de soluciones alineadas con Cloud Adoption Framework (CAF) y el marco de buena arquitectura (WAF)

- **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 la Arquitectura de referencia de ciberseguridad de Microsoft (MCRA) y Microsoft Cloud Security Benchmark (MCSB) y cómo puede utilizarlos para diseñar soluciones más seguras.

  - Introducción a la Arquitectura de referencia de ciberseguridad de Microsoft y Cloud Security Benchmark
  - Diseñar soluciones con procedimientos recomendados para funcionalidades y controles

- Diseño de soluciones con procedimientos recomendados para la protección contra ataques
- Prueba de conocimientos: diseño de una solución con la Arquitectura de referencia de ciberseguridad de Microsoft y Microsoft Cloud Security Benchmark
- Resumen: diseño de una solución con la Arquitectura de referencia de ciberseguridad de Microsoft y Microsoft Cloud Security Benchmark

- **Diseño de una estrategia de resistencia para ciberamenazas comunes, como el ransomware**

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

- Patrones comunes de ciberamenazas y ataques
- Compatibilidad con la resistencia empresarial
- Protección contra ransomware
- Configuraciones de seguridad para las copias de seguridad y la restauración
- Actualizaciones de seguridad
- Prueba de conocimientos: Diseño de una estrategia de resistencia para ciberamenazas comunes
- Resumen: Diseño de una estrategia de resistencia para ciberamenazas comunes como el Ransomware

- **Caso práctico: Diseño de funcionalidades de operaciones de seguridad, identidad y cumplimiento**

Aplique sus aptitudes de arquitecto de ciberseguridad en un escenario empresarial real en el área de operaciones de seguridad, identidad y cumplimiento. Analizará los requisitos de diseño, responderá a preguntas conceptuales y técnicas y diseñará una solución para satisfacer las necesidades empresariales.

- Introducción
- Descripción del caso práctico
- Respuestas de casos prácticos
- Tutorial conceptual
- Tutorial técnico
- Prueba de conocimientos
- Resumen

Diseño de funcionalidades de operaciones de seguridad, identidad y cumplimiento

Aprenderá a diseñar soluciones para operaciones de seguridad (SecOps), administración de identidades y acceso, acceso con privilegios y cumplimiento normativo.

- **Diseño de soluciones para el cumplimiento normativo**

Aprenderá a interpretar y traducir los requisitos normativos en soluciones técnicas. También aprenderá a usar las funcionalidades que se encuentran en Microsoft Purview, Microsoft Priva y Defender for Cloud para el cumplimiento.

- Introducción al cumplimiento normativo
- Traducción de los requisitos de cumplimiento en una solución de seguridad
- Abordar los requisitos de cumplimiento con Microsoft Purview
- Abordar los requisitos de privacidad con Microsoft Priva
- Abordar los requisitos de seguridad y cumplimiento con Azure Policy
- Evaluación del cumplimiento de la infraestructura con Defender for Cloud
- Prueba de conocimientos
- Resumen: diseño de soluciones para requisitos normativos

- **Diseño de soluciones para la administración de identidades y acceso**

Obtendrá información sobre varias estrategias para administrar identidades y el acceso a los recursos, incluidos escenarios híbridos y multinube, identidades externas y acceso condicional.

- Introducción a la administración de identidades y acceso
- Diseño de estrategias de acceso en entornos de nube, híbridos y multinube (incluido Microsoft Entra ID)
- Diseño de una solución para identidades externas
- Diseño de estrategias modernas de autenticación y autorización
- Alineación del acceso condicional y la Confianza cero
- Especificación de requisitos para proteger los Servicios de dominio de Active Directory (AD DS)
- Diseñar una solución para administrar secretos, claves y certificados.
- Prueba de conocimientos: Diseño de soluciones para la administración de identidades y acceso
- Resumen: Diseño de soluciones para la administración de identidades y acceso

- **Diseño de soluciones para proteger el acceso con privilegios**

Aprenderá técnicas avanzadas para diseñar soluciones que administren el acceso con privilegios de forma eficaz.

- Introducción al acceso con privilegios
- Modelo de acceso empresarial
- Diseño de soluciones de gobernanza de identidad
- Diseño de una solución para proteger la administración de inquilinos
- Diseño de una solución para la administración de derechos de infraestructura en la nube (CIEM)
- Diseño de una solución para estaciones de trabajo de acceso con privilegios y servicios bastión
- Prueba de conocimientos: diseño de soluciones para proteger la administración de acceso con privilegios
- Resumen: diseño de soluciones para proteger el acceso con privilegios

- **Diseño de soluciones para operaciones de seguridad**

Aprenderá técnicas para diseñar funcionalidades 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 a las operaciones de seguridad (SecOps)
- Diseño de funcionalidades de operaciones de seguridad en entornos híbridos y multinube
- Diseño del registro y la auditoría centralizados
- Diseño de soluciones de administración de eventos e información de seguridad (SIEM)
- Diseño de soluciones para detección y respuesta
- Diseño de una solución para la orquestación de seguridad, automatización y respuesta (SOAR)
- Diseño de flujos de trabajo de seguridad
- Diseño de la cobertura de detección de amenazas
- Prueba de conocimientos: diseño de soluciones para operaciones de seguridad
- Resumen: diseño de soluciones para operaciones de seguridad

- **Caso práctico: diseño de soluciones de seguridad para aplicaciones y datos**

Aplique sus aptitudes de arquitecto de ciberseguridad en un escenario empresarial real en el área de protección de aplicaciones y datos. Analizará los requisitos de diseño, responderá a preguntas conceptuales y técnicas y diseñará una solución para satisfacer las necesidades empresariales.

- Introducción
- Descripción del caso práctico
- Respuestas de casos prácticos
- Tutorial conceptual
- Tutorial técnico
- Prueba de conocimientos
- Resumen

Diseño de soluciones de seguridad para aplicaciones y datos

Obtenga información sobre cómo diseñar soluciones para proteger datos y aplicaciones, que incluyen: Microsoft 365, desarrollo de aplicaciones, carteras de aplicaciones existentes, detección y clasificación de datos con Microsoft Purview y seguridad de datos para cargas de trabajo de Azure.

- **Especificación de los requisitos para proteger los servicios SaaS, PaaS e IaaS**
  - Introducción a la seguridad de SaaS, PaaS e IaaS
  - 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.
  - Evaluación de la seguridad de los Servicios de IA
  - Evaluación del módulo
  - Resumen: Especificación de los requisitos para proteger los servicios SaaS, PaaS e IaaS

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

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

  - Introducción a la administración de la posición en entornos híbridos y multinube
  - Evaluación de la posición de seguridad mediante Microsoft Cloud Security Benchmark
  - Diseño de la administración de la posición integrada y la protección de la carga de trabajo
  - Evaluación de la posición de seguridad mediante Microsoft Defender for Cloud
  - Evaluación de la posición con la puntuación de seguridad de Microsoft Defender for Cloud
  - Diseño de las protecciones de las cargas de trabajo en la nube con Microsoft Defender for Cloud
  - Integración de entornos híbridos y multinube con Azure Arc
  - Diseño de una solución para administrar la superficie expuesta a ataques externos
  - Administración de posturas mediante rutas de ataque de administración de la exposición
  - Evaluación del módulo
  - Resumen: diseño de soluciones para la administración de la posición de seguridad en entornos híbridos y multinube

- **Diseñar soluciones para proteger Microsoft 365**

Aprenderá a diseñar soluciones de seguridad para Exchange, Sharepoint, OneDrive y Teams.

  - Introducción a la seguridad de Exchange, SharePoint, OneDrive y Teams
  - Evaluación de la posición de seguridad para las cargas de trabajo de colaboración y productividad
  - Diseño de una solución de Microsoft Defender XDR

- Diseño de configuraciones y prácticas operativas para Microsoft 365
- Prueba de conocimientos: Diseño de soluciones para proteger Microsoft 365
- Resumen: diseño de soluciones para proteger Microsoft 365

- **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 a la seguridad de las aplicaciones
- Diseño e implementación de estándares para proteger el desarrollo de aplicaciones
- Evaluación de la posición de seguridad de las carteras de aplicaciones existentes
- Evaluación de amenazas de aplicación con modelado de amenazas
- Diseño de la estrategia de ciclo de vida de seguridad para aplicaciones
- 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
- Prueba de conocimientos: diseño de soluciones para proteger aplicaciones
- Resumen: diseño de soluciones para proteger aplicaciones

- **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 a la seguridad de los datos
- Diseño de una solución para la detección y clasificación de datos mediante Microsoft Purview
- Diseño de una solución para la protección de los datos
- Diseño de la seguridad de datos para cargas de trabajo de Azure
- Diseño de la seguridad para Azure Storage
- Diseño de una solución de seguridad con Microsoft Defender para SQL y Microsoft Defender para Storage
- Prueba de conocimientos: diseño de soluciones para proteger los datos de una organización
- Resumen: diseño de soluciones para proteger los datos de una organización

- **Caso práctico: diseño de soluciones de seguridad para aplicaciones y datos**

Aplique sus aptitudes de arquitecto de ciberseguridad en un escenario empresarial real en el área de protección de aplicaciones y datos. Analizará los requisitos de diseño, responderá a preguntas conceptuales y técnicas y diseñará una solución para satisfacer las necesidades empresariales.

- Introducción
- Descripción del caso práctico
- Respuestas de casos prácticos
- Tutorial conceptual
- Tutorial técnico
- Prueba de conocimientos
- Resumen

Diseño de soluciones de seguridad para infraestructura

Aprenderá a diseñar para la seguridad de la infraestructura, incluida la especificación de requisitos para diferentes modelos en la nube, el diseño de soluciones para la administración de posiciones en entornos híbridos y multinube y la protección de puntos de conexión.

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

Obtenga información sobre cómo analizar los requisitos de seguridad para diferentes ofertas en la nube (SaaS, PaaS e IaaS), cargas de trabajo de IoT, cargas de trabajo web y contenedores.

  - Introducción a la seguridad de SaaS, PaaS e IaaS
  - Especificación de las líneas de base de seguridad para los servicios SaaS, PaaS e IaaS
  - Especificación de requisitos de seguridad para cargas de trabajo web
  - Especificar los requisitos de seguridad para contenedores y la orquestación de contenedores.
  - Prueba de conocimientos: especificación de los requisitos para proteger los servicios SaaS, PaaS e IaaS
  - Resumen: Especificación de los requisitos para proteger los servicios SaaS, PaaS e IaaS

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

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

  - Introducción a la administración de la posición en entornos híbridos y multinube
  - Evaluación de la posición de seguridad mediante Microsoft Cloud Security Benchmark
  - Diseño de la administración de la posición integrada y la protección de la carga de trabajo
  - Evaluación de la posición de seguridad mediante Microsoft Defender for Cloud
  - Evaluación de la posición con la puntuación de seguridad de Microsoft Defender for Cloud
  - Diseño de las protecciones de las cargas de trabajo en la nube con Microsoft Defender for Cloud
  - Integración de entornos híbridos y multinube con Azure Arc
  - Diseño de una solución para administrar la superficie expuesta a ataques externos
  - Administración de posturas mediante rutas de ataque de administración de la exposición
  - Evaluación del módulo
  - Resumen: diseño de soluciones para la administración de la posición de seguridad en entornos híbridos y multinube

- **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
  - Especificación de los requisitos de seguridad del servidor
  - Especificación de los requisitos para dispositivos móviles y clientes
  - Especificación de los requisitos de seguridad de Internet de las cosas (IoT) y los dispositivos insertados
  - Tecnología operativa segura (OT) y sistemas de control industrial (ICS) con Microsoft Defender para IoT

- Especificación de líneas de base de seguridad para 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 proteger los puntos de conexión de cliente y servidor

- **Diseño de soluciones para la seguridad de red**

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

- Introducción
- Diseñar soluciones para la segmentación de la red
- Diseño de 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: Diseño de soluciones de seguridad de red

- **Caso práctico: Diseño de soluciones de seguridad para la infraestructura**

Aplique sus aptitudes de arquitecto de ciberseguridad en un escenario empresarial real en el área de seguridad de la infraestructura. Analizará los requisitos de diseño, responderá a preguntas conceptuales y técnicas y diseñará una solución para satisfacer las necesidades empresariales.

- Introducción
- Descripción del caso práctico
- Respuestas de caso práctico
- Tutorial conceptual
- Tutorial técnico
- Comprobación de conocimientos
- Resumen