Certificación en Desarrollo de Software, Ciberseguridad o Computación en la nube

El programa de Especialista en Tecnología de la Información es una forma para que los estudiantes validen las habilidades de TI.

Las certificaciones de especialista en TI son una excelente manera de aumentar la confianza de sus estudiantes brindándoles la sensación de logro que viene con la obtención de una credencial reconocida por la industria.

Dirigido a: Personas a partir de los 15 años

Material: Contenido digital, material multimedia (audios y/o videos)
Plataforma de práctica y simulación

Duración: 50 horas

Desarrollo de Software

1. Conceptos básicos de programación

1.1 Describir el almacenamiento informático y los tipos de datos

- Cómo una computadora almacena programas e instrucciones en la memoria de la computadora, pilas y montones de memoria, requisitos de tamaño de memoria para varios tipos de almacenamiento de datos, datos numéricos y datos textuales, recolección de basura

1.2 Construya y analice algoritmos y diagramas de flujo para resolver problemas de programación

- Estructuras de decisión utilizadas en todos los lenguajes de programación de computadoras; estructuras de decisión; múltiples estructuras de decisión, como if...else y switch; leer y construir diagramas de flujo; tablas de decisión; evaluar expresiones; bucles for, bucles while, bucles do...while; recursión

1.3 Incorporar manejo de errores en aplicaciones o módulos

- Manejo estructurado de excepciones (try-catch-finally), pruebas unitarias, lanzamiento de excepciones, lectura de la pila, codificación defensiva, comprensión del alcance en el manejo de excepciones

1.4 Construir y analizar código basado en patrones de programación funcional

- Evento, delegado, promesas, programación sincrónica frente a asincrónica (AJAX, XHR), inmutabilidad

2. Principios de desarrollo de software

2.1 Describir la gestión del ciclo de vida del desarrollo de software (SDLC)

- Análisis de requisitos, planificación y diseño, implementación, pruebas, despliegue, mantenimiento; Conceptos ágiles

2.2 Interpretar las especificaciones de la aplicación

- Leer las especificaciones de la aplicación y traducirlas en prototipos y código, seleccionando el tipo de aplicación y los componentes apropiados

2.3 Construir y analizar código que utiliza algoritmos y estructuras de datos

- Matrices, pilas, colas, listas vinculadas, diccionarios (pares clave-valor), algoritmos de clasificación (clasificación por selección, clasificación por burbuja, clasificación rápida, clasificación por fusión), algoritmos de búsqueda (búsqueda lineal, búsqueda binaria), implicaciones de rendimiento de diversas estructuras de datos , eligiendo la estructura de datos correcta, FIFO, LIFO

2.4 Describir el propósito de los sistemas de control de versiones

- GitHub, check-in, check-out, fusionar, bifurcar, revertir, clonar, resolver conflictos

2.5 Describir conceptos de codificación segura

- Cifrado, hashing y firmas digitales; claves públicas, privadas y compartidas; mitigar la falsificación de solicitudes entre sitios (csrf); Inyección SQL; riesgos de usar iframes

3. Programación Orientada a Objetos

3.1 Construir, analizar y usar clases

- Propiedades, métodos, eventos, campos y constructores; cómo crear clases; cómo usar clases en código; modificadores de acceso; instanciación; estático frente a instancia; encapsulación; composición

3.2 Construir y analizar código que usa herencia

- Heredar la funcionalidad de una clase base en una clase derivada, clases genéricas, clases abstractas

3.3 Construir y analizar código que usa polimorfismo

- Extender la funcionalidad de una clase después de heredar de una clase base, anular métodos en la clase derivada, interfaces, sobrecarga

4. Aplicaciones web

4.1 Construir y analizar aplicaciones web

- HTML5, CSS3 y JavaScript ES6; herramientas de desarrollo de navegadores; solicitud o respuesta HTTP; administración del Estado; cookies, almacenamiento local y de sesión; ciclo de vida de la página; modelo de evento; programación del lado del cliente vs. del lado del servidor

4.2 Describir y configurar el alojamiento web

- Creación de directorios y sitios web virtuales, publicación de aplicaciones web, función del servidor web

4.3 Describir y configurar servicios web

- Servicios web que son consumidos por aplicaciones cliente, accediendo a servicios web desde aplicaciones cliente, JSON, REST API, oAuth, XML

4.4 Describir e identificar patrones arquitectónicos

- Modelo-vista-controlador (MVC), modelo-vista-modelo de vista (MVVM), aplicación de página única (SPA)

5. Bases de datos

5.1 Diseñar y normalizar una base de datos

- Características y capacidades de los productos de bases de datos, diseño de bases de datos, diagramas de relación de entidades (ERD), conceptos de normalización (a 3NF), índices, restricciones, clave principal, claves externas, relaciones

5.2 Construir, analizar y optimizar consultas ANSI SQL

- Creación y acceso a procedimientos almacenados, actualización y selección de datos, DML frente a DDL, funciones, disparadores, cursores, uniones, índices

5.3 Administrar transacciones

- Confirmar, revertir, guardar, concurrencia, niveles de aislamiento, bloqueo

5.4 Describir los métodos de acceso a la base de datos

- Entity Framework (Código primero, Base de datos primero), grupos de conexiones, LINQ

5.5 Describir tipos de bases de datos NoSQL

- Bases de datos de documentos, bases de datos de valores clave

Ciberseguridad

Objetivos de Dominio

1. Principios esenciales de seguridad

1.1 Definir los principios esenciales de seguridad

- Vulnerabilidades, amenazas, exploits y riesgos; vectores de ataque; endurecimiento; defensa en profundidad; confidencialidad, integridad y disponibilidad (CIA); tipos de atacantes; motivos de los ataques; código ético

1.2 Explicar las amenazas y vulnerabilidades comunes

- Malware, ransomware, denegación de servicio, botnets, ataques de ingeniería social (tailgating, spear phishing, phishing, vishing, smishing, etc.), ataques físicos, intermediarios, vulnerabilidades de IoT, amenazas internas, amenazas persistentes avanzadas (APT)

1.3 Explicar los principios de gestión de acceso

- Autenticación, autorización y contabilidad (AAA); RADIO; autenticación multifactor (MFA); políticas de contraseña

1.4 Explicar los métodos y aplicaciones de encriptación

- Tipos de cifrado, hashing, certificados, infraestructura de clave pública (PKI); algoritmos de cifrado fuertes frente a débiles; estados de los datos y encriptación adecuada (datos en tránsito, datos en reposo, datos en uso); protocolos que usan cifrado

2. Conceptos básicos de seguridad de la red

2.1 Describir las vulnerabilidades del protocolo TCP/IP

- TCP, UDP, HTTP, ARP, ICMP, DHCP, DNS

2.2 Explicar cómo las direcciones de red afectan la seguridad de la red

- Direcciones IPv4 e IPv6, direcciones MAC, segmentación de red, notación CIDR, NAT, redes públicas frente a privadas

2.3 Describir la infraestructura y las tecnologías de la red

- Arquitectura de seguridad de red, DMZ, virtualización, nube, honeypot, servidor proxy, IDS, IPS

2.4 Configurar una red SoHo inalámbrica segura

- Filtrado de direcciones MAC, estándares y protocolos de encriptación, SSID

2.5 Implementar tecnologías de acceso seguro

- ACL, firewall, VPN, NAC

3. Conceptos de seguridad de terminales

3.1 Describir los conceptos de seguridad del sistema operativo

- Windows, macOS y Linux; funciones de seguridad, incluidos Windows Defender y firewalls basados en host; CLI y PowerShell; permisos de archivos y directorios; escalada de privilegios

3.2 Demostrar familiaridad con las herramientas de punto final adecuadas que recopilan información de evaluación de seguridad

- Netstat, nslookup, tcpdump

3.3 Verificar que los sistemas de terminales cumplan con las políticas y estándares de seguridad

- Inventario de hardware (gestión de activos), inventario de software, implementación de programas, copias de seguridad de datos, cumplimiento normativo (PCI DSS, HIPAA, RGPD), BYOD (gestión de dispositivos, cifrado de datos, distribución de aplicaciones, gestión de configuración)

3.4 Implementar actualizaciones de software y hardware

- Windows Update, actualizaciones de aplicaciones, controladores de dispositivos, firmware, parches

3.5 Interpretar los registros del sistema

- Visor de eventos, registros de auditoría, registros del sistema y de la aplicación, syslog, identificación de anomalías

3.6 Demostrar familiaridad con la eliminación de malware

- Escaneo de sistemas, revisión de registros de escaneo, remediación de malware

4. Evaluación de vulnerabilidades y gestión de riesgos

4.1 Explicar la gestión de vulnerabilidades

- Identificación, gestión y mitigación de vulnerabilidades; reconocimiento activo y pasivo; pruebas (escaneo de puertos, automatización)

4.2 Usar técnicas de inteligencia de amenazas para identificar posibles vulnerabilidades de la red

- Usos y limitaciones de las bases de datos de vulnerabilidad; herramientas estándar de la industria utilizadas para evaluar vulnerabilidades y hacer recomendaciones, políticas e informes; Vulnerabilidades y exposiciones comunes (CVE), informes de ciberseguridad, noticias de ciberseguridad, servicios de suscripción e inteligencia colectiva; inteligencia de amenazas ad hoc y automatizada; la importancia de actualizar la documentación y otras formas de comunicación de manera proactiva antes, durante y después de los incidentes de ciberseguridad; cómo proteger, compartir y actualizar la documentación

4.3 Explicar la gestión de riesgo

- Vulnerabilidad versus riesgo, clasificación de riesgos, enfoques para la gestión de riesgos, estrategias de mitigación de riesgos, niveles de riesgo (bajo, medio, alto, extremadamente alto), riesgos asociados con tipos específicos de datos y clasificaciones de datos, evaluaciones de seguridad de sistemas de TI (información seguridad, gestión de cambios, operaciones informáticas, aseguramiento de la información)

4.4 Explicar la importancia de la recuperación ante desastres y la planificación de la continuidad del negocio

- Desastres naturales y provocados por el hombre, características de los planes de recuperación ante desastres (DRP) y planes de continuidad del negocio (BCP), respaldo, controles de recuperación ante desastres (detective, preventivo y correctivo)

5. Manejo de incidentes

5.1 Supervise los eventos de seguridad y sepa cuándo se requiere escalar

- RRol de SIEM y SOAR, monitoreo de datos de red para identificar incidentes de seguridad (capturas de paquetes, varias entradas de archivos de registro, etc.), identificación de eventos sospechosos a medida que ocurren

5.2 Explicar el análisis forense digital y los procesos de atribución de ataques

- Cyber Kill Chain, MITRE ATT&CK Matrix y Diamond Model; Tácticas, Técnicas y Procedimientos (TTP); fuentes de evidencia (artefactos); manejo de evidencia (preservación de evidencia digital, cadena de custodia)

Computación en la nube

Computación en la nube

1. Determinar si la solución en la nube es adecuada
   1.1. Explicar las ventajas que brinda la nube a las partes interesadas
   - Describir la infraestructura de la nube
   - Distinguir entre IaaS, PaaS y SaaS
   - Mostrar cómo la nube permite construir aplicaciones más económicas que con los modelos tradicionales
   - Mostrar cómo la nube permite construir aplicaciones más rápido que con los modelos tradicionales

   1.2 Explicar el costo a las partes interesadas
   - Identificar el caso de uso (nuevo desarrollo o transición de un producto o servicio existente)
   - Identifique los recursos que se requerirán para construir el servicio o producto usando componentes alojados en la nube (incluya costos de cómputo, datos y red)
   - Identificar el plan de soporte que se requerirá para cumplir con los criterios de rendimiento, disponibilidad, escalabilidad y confiabilidad (PASR)
   - Considere los factores que intervienen en el retorno de la inversión

   1.3 Explicar el desempeño a las partes interesadas
   - Identificar los criterios de desempeño
   - Considere qué soluciones cumplen con los criterios
   - Evaluar el costo y la disponibilidad de experiencia técnica

   1.4 Explicar la confiabilidad a las partes interesadas
   - Identificar los criterios de confiabilidad, incluidas las velocidades de la red
   - Considere qué soluciones cumplen con los criterios
   - Comprender el acuerdo de nivel de servicio (SLA) con el proveedor de la nube
   - Considere planes de respaldo y recuperación ante desastres (incluida la redundancia de respaldo o el factor de replicación)

   1.5 Explicar la disponibilidad a las partes interesadas
   - Identificar el caso de uso (nuevo desarrollo o transición de un producto o servicio existente)
   - Identificar cualquier SLA ascendente o descendente que regirá los requisitos de disponibilidad
   - Establecer métricas de disponibilidad
   - Evaluar el SLA ofrecido por la solución alojada en la nube

   1.6 Explicar la escalabilidad a las partes interesadas
   - Identificar el caso de uso (nuevo desarrollo o transición de un producto o servicio existente)
   - Comprender que se pueden establecer reglas para ajustar los recursos en función de las necesidades

   1.7 Recomendar soluciones listas para usar (OTS) o personalizadas según sea necesario

- Identificar el caso de uso (nuevo desarrollo o transición de un producto o servicio existente)
- Evaluar si la oferta existente de OTS cumple con las necesidades de rendimiento, disponibilidad, escalabilidad y confiabilidad
- Evaluar el esfuerzo técnico necesario para una solución personalizada
- Evaluar si la solución personalizada puede superar OTS en los criterios PASR

2. Desarrollo de arquitectura en la nube

2.1 Elija entre implementaciones de nube pública, privada e híbrida

- Identificar los requisitos de seguridad y privacidad para la solución (centrándose en las opciones de red que ofrece cada uno)
- Considere los límites impuestos por la tenencia en varias implementaciones en la nube

2.2 Dibujar un diagrama arquitectónico (mostrar flujos de datos)

- Desglosar la solución propuesta en componentes de cómputo, datos y redes
- Producir agrupaciones lógicas para los componentes
- Marcar flujos de datos entre componentes (incluido el protocolo)
- Identificar los límites del sistema y los componentes (incluido el modelo de responsabilidad)

2.3 Definir requisitos

- Decidir si virtualizar el servidor, la red, el almacenamiento y el escritorio
- Sea consciente de los patrones de diseño como los microservicios y sin servidor
- Considere la infraestructura de red, los dispositivos de almacenamiento, la memoria y los dispositivos de usuario final requeridos

2.4 Identificar cómo se comunican los servicios a través de la aplicacióninterfaces de programación (API)

- Identificación de servicios con los que la aplicación necesita integrarse
- Interactuar usando una API

2.5 Crear máquinas virtuales

- Determinar el sistema operativo para las máquinas virtuales
- Elija el tamaño adecuado para las máquinas virtuales
- Decidir la configuración geográfica de las máquinas virtuales (latencia, requisitos legales)
- Configurar opciones (p. ej., limitaciones de tiempo, escalado, copias de seguridad) para las máquinas virtuales

2.6 Identificar los requisitos de almacenamiento de datos

- Distinguir entre datos estructurados y no estructurados
- Determinar la cantidad de almacenamiento necesaria
- Considere la ubicación del almacenamiento
- Considere la seguridad del almacenamiento

3. Implementación del ciclo de vida de desarrollo de la nube

3.1 Crear contenido en entornos virtuales

- Comprender que es necesario configurar un sistema de gestión de código fuente
- Instalar y configurar los paquetes de requisitos previos en el entorno virtual
- Guarde los cambios y realice un seguimiento de los códigos en un sistema de administración de código fuente (como Github)

3.2 Realizar pruebas

- Proporcionar diferentes casos de prueba, escenarios de prueba y guiones de prueba
- Ejecute las pruebas e informe los errores de forma iterativa

3.3 Estructurar la solución global basada en la nube
- Integrar sistemas y aplicaciones dentro del entorno seleccionado
- Integrar sistemas y aplicaciones con sistemas heredados
- Integrar sistemas y aplicaciones con aplicaciones de terceros
- Distinguir entre contenedores y máquinas virtuales
- Saber cuándo elegir contenedores en lugar de máquinas virtuales

3.4 Implementar la aplicación en el servidor
- Decidir sobre la estrategia para implementar una nueva aplicación, reemplazando una anterior
- Comprender el control de versiones
- Identificar soluciones alojadas en la nube para crear canalizaciones de código y datos (p. ej., ofertas de CI/CD nativas de la nube y automatización de flujos de trabajo como GitHub Actions)
- Identificar las prácticas existentes de CI/CD

4. Gestión de operaciones en la nube

4.1 Administrar los costos operativos
- Comprender los precios basados en el uso
- Escalar hacia arriba y hacia abajo para satisfacer la demanda de manera rentable

4.2 Desarrollar una política de continuidad del negocio y recuperación ante desastres
- Identificar riesgos potenciales y escenarios de desastre
- Establecimiento de una estrategia de copia de seguridad local frente a externa

4.3 Brindar soporte a los usuarios
- Identificar políticas de protección y seguridad para usuarios externos e internos
- Proporcionar soporte de aplicaciones y hardware para usuarios internos
- Proporcionar herramientas de formación para usuarios internos y externos

4.4 Supervisión de sistemas en la nube
- Registrar eventos
- Monitorear hardware y software (p. ej., interpretar gráficos y tableros)
- Comprender las notificaciones o alertas para el aprovisionamiento de copias de seguridad

5. Comprender la gobernanza de la nube

5.1 Cumplir con los requisitos reglamentarios y de privacidad
- Identificar los requisitos de privacidad relevantes en función de las restricciones geográficas y de dominio (por ejemplo, BIPA, HIPAA, PDP, FERPA, COPPA, GDPR, CCPA, etc.), así como las políticas específicas de la organización.
- Identificar el cumplimiento del proveedor de la nube con estas normas de privacidad
- Evaluar los tipos de datos gestionados en el entorno
- Evaluar la ubicación y el almacenamiento de datos
- Estar al tanto de los marcos y estándares NIST e ISO

5.2 Cumplir con las pautas éticas
- Considere el impacto del sesgo, la falta de transparencia y la falta de rendición de cuentas
- Explicar los posibles problemas de sesgo y transparencia con servicios prediseñados

5.3 Gestión de la seguridad en la nube
- Comprender las opciones y los conceptos para la verificación y autenticación de la identidad, incluida la identidad digital y la autenticación multifactor

- Comprender las políticas y autorizaciones de acceso (p. ej., opciones de acceso, funciones proporcionadas por el proveedor frente a funciones y permisos personalizados, e higiene del acceso, incluido el acceso con privilegios mínimos, la eliminación del acceso cuando no es necesario, la desactivación de cuentas)
- Comprender la importancia de la seguridad y el cifrado de datos
- Comprender las opciones para protegerse contra el acceso no autorizado en entornos de nube (incluida la detección y prevención de intrusiones, firewalls)