Networking Academy

Introducción a la Ciberseguridad

Alcance y la secuencia

Versión 3.0

Contenido

Público Objetivo

El curso Introducción a la seguridad cibernética 3.0 está diseñado para estudiantes que están considerando una carrera en seguridad cibernética. Este curso exploratorio brinda a los alumnos una introducción a la seguridad cibernética, explorando formas de estar seguro en línea, los diferentes tipos de malware y ataques, las medidas utilizadas por las organizaciones para mitigar los ataques e investigando oportunidades profesionales. El curso en línea es apropiado para estudiantes en muchos niveles educativos y tipos de instituciones, incluidas escuelas secundarias, universidades, colegios, escuelas técnicas y profesionales, capacitación laboral y centros comunitarios.

Prerequisitos

No hay prerequisitos para este curso

Descripción del curso

Introducción a la Ciberseguridad incluye:

- Cinco módulos compuestos por temas clave.
- Los módulos enfatizan el pensamiento crítico, la resolución de problemas, la colaboración y la aplicación práctica de las habilidades.

Las actividades de nivel de tema están diseñadas para indicar el dominio de un alumno de las habilidades del curso, lo que permite a los alumnos evaluar la comprensión antes de realizar un cuestionario o examen calificado.
El lenguaje que describe los conceptos está diseñado para que los estudiantes de todos los niveles lo entiendan fácilmente.

- Las evaluaciones y las actividades de práctica enfocadas en competencias específicas están diseñadas para aumentar la retención y proporcionar flexibilidad en el camino del aprendizaje.
- Las herramientas de aprendizaje multimedia, que incluyen laboratorios, videos y cuestionarios, abordan una variedad de estilos de aprendizaje, estimulan el aprendizaje y promueven la retención de conocimientos.
- Las actividades basadas en simulación de Labs y Packet Tracer ayudan a los estudiantes a desarrollar el pensamiento crítico y habilidades para resolver problemas complejos.
- Las evaluaciones innovadoras brindan retroalimentación inmediata para respaldar la evaluación del conocimiento y las habilidades.
- Los alumnos exploran los aspectos básicos de la seguridad en línea.
- Los alumnos conocen diferentes tipos de malware y ataques, y cómo las organizaciones se protegen contra estos ataques.
- Los estudiantes exploran opciones de carrera en seguridad cibernética.

Objetivos del Curso

El material del curso ayudará a desarrollar las habilidades de los alumnos, que incluyen:

- Explicar los conceptos básicos para estar seguro en línea, incluido qué es la ciberseguridad y su impacto potencial.
- Explicar las ciberamenazas, ataques y vulnerabilidades más comunes.
- Explicar cómo protegerse mientras está en línea.
- Explicar cómo las organizaciones pueden proteger sus operaciones contra estos ataques

- Acceder a una variedad de información y recursos para explorar las diferentes opciones de carrera en seguridad cibernética.

Requerimiento de equipamento

Cualquier dispositivo con acceso a Internet (Smartphones/Tablets/Chromebooks/ Laptops/Desktops).

Esquema del curso

La Tabla 1 a continuación detalla los módulos y sus competencias asociadas. Cada módulo es una unidad integrada de aprendizaje que consta de contenido, actividades y evaluaciones que apuntan a un conjunto específico de competencias. El tamaño del módulo depende de la profundidad del conocimiento y la habilidad necesarios para dominar la competencia.

Tabla 1: Título y objetivo del módulo

Título del módulo/Título del tema	Objetivo
Módulo 1: Introducción a la Ciberseguridad	
1.0: Introducción a la Ciberseguridad	Explicar los conceptos básicos para estar seguro en línea, incluido qué es la ciberseguridad y su impacto potencial.
1.1 The World of Cybersecurity	1.1 El mundo de la ciberseguridad
1.2 Datos de la organización	Identificar los tipos de información confidencial que los piratas informáticos pueden usar para invadir su privacidad o dañar su reputación, dónde pueden acceder a esta información y por qué es de interés para los ciberdelincuentes.
1.3 ¿Qué se llevó?	Explicar qué son los datos organizacionales y por qué deben protegerse.
1.4 Atacantes cibernéticos	Describir quiénes son los atacantes cibernéticos y qué quieren.
1.5 Ciberguerra	Explicar qué es la guerra cibernética y por qué las naciones y los gobiernos necesitan profesionales de ciberseguridad para ayudar a proteger a sus ciudadanos e infraestructura.
Módulo 2: Ataques, Conceptos y Técnicas	
2.0: Ataques, Conceptos y Técnicas	Explicar las ciberamenazas, ataques y vulnerabilidades más comunes.
2.1 Análisis de un ciberataque	Identificar los diferentes tipos de malware y sus síntomas.
2.2 Métodos de infiltración	Describir los diferentes métodos de infiltración.
2.3 Exploits y vulnerabilidad de seguridad	Explicar cómo encontrar vulnerabilidades de seguridad.
2.4 El panorama de la ciberseguridad	Explicar cómo categorizar las vulnerabilidades de seguridad.

Módulo 3: Explicar cómo categorizar las vulnerabilidades de seguridad	
3.0 Explicar cómo categorizar las vulnerabilidades de seguridad.	Explicar cómo protegerse mientras está en línea.
3.1 Protección de sus dispositivos y red	Identificar formas de proteger sus dispositivos informáticos.
3.2 Mantenimiento de datos	Identificar formas de proteger sus dispositivos informáticos.
3.3 ¿Quién es el propietario de sus datos?	Crear contraseñas seguras.
3.4 Protección de su privacidad en línea	Implementar técnicas para mantener los datos de forma segura.
3.5 Descubra su propio comportamiento arriesgado en línea	Explicar formas de mejorar la seguridad de los datos en línea.
Módulo 4: Protección de la Organización	
4.0 Protección de la Organización	Explicar cómo las organizaciones pueden proteger sus operaciones contra estos ataques.
4.1 Dispositivos y tecnologías de ciberseguridad	Explicar los diferentes firewalls, dispositivos de seguridad y software que utilizan los profesionales de ciberseguridad para proteger la red, los datos y el equipo de una organización.
4.2 Enfoque conductual de la ciberseguridad	Explicar cómo detectar una ciberamenaza a través de enfoques de seguridad basados en el comportamiento.
4.3 Enfoque de Cisco para la ciberseguridad	Explicar el enfoque de Cisco con respecto a la seguridad cibernética, incluido el equipo CSIRT y el Manual de estrategias de seguridad.
4.4 Enfoque de Cisco para la ciberseguridad	Explicar el enfoque de Cisco con respecto a la seguridad cibernética, incluido el equipo CSIRT y el Manual de estrategias de seguridad.
Módulo 5: ¿Su futuro estará en la ciberseguridad?	
5.0 ¿Su futuro estará en la ciberseguridad?	Acceder a una variedad de información y recursos para explorar las diferentes opciones de carrera en ciberseguridad.
5.1 Cuestiones legales y éticas	Identificar algunos de los problemas legales personales y corporativos que pueden surgir al trabajar en ciberseguridad.
5.2 Educación y carreras	Identificar qué certificaciones profesionales y los próximos pasos que deben tomar para seguir una carrera en ciberseguridad.