Introducción

Nuestro propósito es cambiar la vida de las personas a nivel profesional, y estamos dispuestos a conseguirlo.

La demanda de profesionales en redes y ciberseguridad sigue en crecimiento. Este programa te prepara para obtener certificaciones altamente valoradas en el sector: CCNA (200-301), CyberOps Associate (200-201) y Fortinet (Fortigate Administrator + FortiAnalyzer).

Tendrás acceso a laboratorios avanzados con tecnología Cisco, Fortinet y herramientas líderes en el sector para garantizar una formación 100% práctica y orientada al empleo.

Curso dirigido a

Lo importante es tu pasión en este sector. Teniendo en cuenta que el objetivo del Máster es profundizar en el desarrollo de redes y la preparación de las certificaciones CISCO 200-301, CyberOps 200-201 y Fortinet Certified Security Operations, es necesario tener conocimientos de informática, especialmente en redes que te capaciten para poder tener las bases para afrontar el Máster con garantías. Puedes haber obtenido dichos conocimientos bien de forma autodidacta, bien a través de una formación como ASIR o STI, Certificados de Profesionalidad en informática o similares.

Aunque no es un requisito imprescindible, es recomendable estar desempleado para tener mas tiempo en su preparación. Se tiene que recordar que la asistencia a las clases son obligatorias por lo que la compatibilidad horaria es importante.

Beneficios de la certificación

Certificado, igual a empleabilidad para los estudiantes.

El número de empleos en la industría de la computación en la nube está creciento tan rapidamente que no hay profesionales cualificados para cubrir los puestos de trabajo disponibles. Obtener la certificación es parte de la solución.

Este programa se desarrolla internacionalmente en más de 150 países del mundo y no sólo busca formar profesionales para que trabajen en su propio país, sino profesionales que sean reconocidos internacionalmente. Por ello, uno de los objetivos del programa es formar nuevos profesionales expertos en redes que obtengan una certificación con reconocimiento internacional llamada Cisco Certified Network Associate – CCNA.

Contratación:

El 86% de los gerentes de contratación indican: las certificaciones TI son una prioridad alta o media durante el proceso de evaluación de candidatos.

Ocho de cada diez directores de recursos humanos verifican la certificación entre los candidatos al puesto de trabajo.

Un 99% de los responsables de RRHH consideran la certificación como parte de sus criterios de contratación.

Progreso: En una encuesta a 700 profesionales de TI, el 60% dijo que la certificación le condujo a un nuevo empleo.

Objetivos

Dos grandes objetivos:

Desarrollarse profesionalmente para ser capaz de:
Diseñar, construir y mantener redes de ordenadores en entornos empresariales
Monitorear, detectar, analizar y dar respuesta a la ciberdelincuencia, el ciberespionaje, las amenazas internas, las amenazas persistentes avanzadas, los requisitos normativos y otros problemas de ciberseguridad a los que se enfrentan las organizaciones a diario
Despliegue de NGFW (Next Generation Firewall) para la detección y bloqueo malware
Configuración de políticas de FW para la protección de la información y los servicios de la red
Acceder con éxito a los exámenes oficiales de Cisco CCNA (200-301), CyberOps Associate (CBROPS) (200-201) y Fortinet Certified Security Operations (Fortigate Administrator + FortiAnalyzer).
Para ello, se ha elaborado un programa formativo que permita al alumnado ser capaz de construir redes LAN simples, realizar configuraciones básicas de routers y switches e implementar esquemas de direccionamiento IPv6, implementar pequeñas redes enrutadas y conmutadas, así como resolver los retos e incidencias habituales en este tipo de redes y habilitar mecanismos traducción de direcciones según el propósito deseado, de establecer comunicaciones seguras mediante VPN sitio-a-sitio en una red compleja, de elegir un método adecuado para la priorización de tráfico (QoS), de diseñar esquemas de red y de establecer líneas de actuación para la administración de la red y la resolución de problemas.

Entre las destrezas adquiridas tras finalizar la formación, destacamos:

Profundización en conceptos y servicios de IPv6
Aplicación de seguridad como política transversal a las implementaciones de red
Orientación al entrenamiento de competencias en configuraciones de red confiables, particularmente, con relación a los protocolos de agregación de enlaces (LACP, PAgP).
Implementaciones de tolerancia a fallos con protocolos de redundancia de primer salto (FHRP).
Mecanismos de priorización de tráfico (QoS).
Tratamiento de los modelos de virtualización y de redes definidas por software (SDN).
Presentación de los elementos y tecnologías necesarios para abordar la gestión, programación y automatización de redes.
Comprender los principios, roles y responsabilidades involucrados en las operaciones de ciberseguridad, así como las tecnologías, herramientas, regulaciones y estándares disponibles.
Describir las vulnerabilidades y amenazas comunes en los dispositivos de usuario y en las infraestructuras de red.
Demostrar habilidades fundamentales aplicadas a la monitorización, detección, investigación, análisis y respuesta a incidentes de seguridad.
Clasificar eventos intrusivos según categorías definidas por modelos de seguridad y establecer acciones defensivas.
Llevar a cabo con éxito las tareas, deberes y responsabilidades de un Analista de Seguridad de nivel asociado en un Centro de Operaciones de Seguridad (SOC).
Comprender los principios, roles y responsabilidades involucrados en las operaciones de ciberseguridad, así como las tecnologías, herramientas, regulaciones y estándares disponibles.
Describir las vulnerabilidades y amenazas comunes en los dispositivos de usuario y en las infraestructuras de red.
Demostrar habilidades fundamentales aplicadas a la monitorización, detección, investigación, análisis y respuesta a incidentes de seguridad.
Clasificar eventos intrusivos según categorías definidas por modelos de seguridad y establecer acciones defensivas.
Explicar cómo investigar las vulnerabilidades y ataques de punto final.
Evaluar alertas de seguridad y analizar los datos de intrusión en la red para identificar vulnerabilidades y hosts comprometidos.
Aplicar modelos de respuesta a incidentes para gestionar incidentes de seguridad de red
Llevar a cabo con éxito las tareas, deberes y responsabilidades de un Analista de Seguridad de nivel asociado en un Centro de Operaciones de Seguridad (SOC)

Contenidos del curso

El curso, en español, se desarrolla sobre la plataforma de formación Cisco NetAcad y Fortinet Training Institute. Se integrará el uso de IA para mejorar y ampliar un perfil ya muy demandado.

Módulo 1: CCNA – Introducción a las Redes y Seguridad Perimetral

Fundamentos de conmutación, enrutamiento y comunicaciones inalámbricas
Redes empresariales, seguridad y programación
Laboratorios prácticos
Preparación para el examen de certificación CISCO CCNA (200-301)
Módulo 2: CyberOps – Centro de Operaciones de Seguridad (SOC)

Ciberseguridad y funcionamiento de un SOC (Centro de Operaciones de Seguridad)
Sistemas Operativos: Windows y Linux en un entorno de seguridad
Protocolos y servicios de red
Laboratorios prácticos
Preparación para el examen de certificación 200-201 CyberOps Associate (CBROPS)
Módulo 3: Fortinet – Seguridad Avanzada y Cloud Security

FCP = FORTIGATE ADMINISTRATOR Y FORTIANALYZER
Preparación para los exámenes de certificación de Fortinetde FCP Security Operations
Módulo 4: Orientación Profesional y Laboral

Simulaciones de entrevistas laborales en ciberseguridad
Desarrollo de CV orientado a ciberseguridad
Análisis de fortalezas y áreas de mejora para aumentar las posibilidades de empleo en el sector
Optimización de perfiles en LinkedIn para mejorar la visibilidad profesional

Metodología

El programa se desarrolla con clases teórico-prácticas, con gran cantidad de laboratorios reales, guiados por profesores expertos en activo. Además, incluye:

Seguimiento con evaluaciones parciales y exámenes finales teóricos y prácticos.
Uso de contenidos multimedia y actividades interactivas para reforzar la comprensión.
Formación en pensamiento crítico, resolución de problemas y aplicación práctica de habilidades, en casos que se acercan a la realidad empresarial.

Modalidades

Clases presenciales (Tajamar. C/ Pío Felipe, 12; 28038 Madrid) o virtuales en streaming
Acceso a laboratorios en la nube para prácticas desde cualquier lugar

Por qué hacer el Máster en ciberseguridad

Nuestro propósito es cambiar la vida de las personas a nivel profesional, y estamos dispuestos a conseguirlo.

La necesidad de profesionales de redes de alto nivel continúa estando presente. La certificación CCNA es reconocida como un paso muy importante para los profesionales de redes en su camino a una carrera exitosa en el campo de redes con tecnología Cisco.

Nuestro objetivo es conseguir que el alumnado adquiera aquellos conocimientos necesarios para la administración de redes informáticas a nivel profesional así como que el alumno acceda con éxito a los exámenes oficiales de Cisco CCNA (200-301), Certificación CyberOps CBROPS (200-201) y Fortinet Certified Security Operations, unas de las certificaciones más importantes y con una implantación más elevada en la industria de las redes informáticas.

Ventajas

Aquí puedes ver las ventajas de estudiar en Tajamar, benefíciate de la mejor experiencia, los mejores profesionales y las mejores instalaciones.

Salidas profesionales

Profesionales altamente cualificados

Las organizaciones de hoy en día dependen cada vez más de Internet y sus complejas redes internas donde transita mucha información. Necesitan profesionales altamente capacitados para mantener sus redes trabajando transparentemente y expandiéndose en forma constante.

Un profesional experto en conectividad y redes es fundamental en las empresas que día a día trabajan con información que viaja por Internet. Todas las empresas de hoy dependen de Internet para conectarse internamente con su personal, como con sus proveedores y clientes. Es el medio de comunicación por excelencia para un exitoso desenvolvimiento de cualquier negocio.

La necesidad de profesionales de redes de alto nivel continúa estando presente. La certificación CCNA es reconocida como un paso muy importante para los profesionales de redes en su camino a una carrera exitosa en el campo de redes con tecnología Cisco.

Contar con esta certificación y con las habilidades suficientes para respaldarla, distinguirán al alumno que la obtenga. El Programa de formación que ofrecemos es precisamente para ayudar a la persona tanto a desarrollar estas habilidades como a aprobar los exámenes de certificación. Con este programa, podrás acceder a roles como:

Operador de Red N1 y N2.
Operador SOC (Centro de Operaciones de Seguridad).
Administrador/analista de seguridad de plataformas Fortinet.
Técnico en redes y seguridad IT.

Proceso de selección

El proceso de selección se basará en los siguientes criterios:

El Currículum Vitae
Entrevista (si se considera necesario tras revisar el CV)
Precio
Nuestro compromiso es que nadie se quede sin un futuro profesional por falta de recursos. Por eso, hemos creado un sistema de pagos flexible que te permite abonar el Máster una vez hayas recibido una oferta laboral. Queremos transformar tu vida profesional, y estamos aquí para ayudarte a lograrlo.

Estamos tan seguros de nuestra propuesta que, si no conseguimos ofrecerte una oportunidad laboral, te reembolsamos el 50% de lo que hayas abonado. Si puedes realizar el pago completo desde el inicio, el precio es de 4.760 euros. Para quienes prefieren un pago aplazado, ofrecemos diversas opciones adaptadas a cada situación. Los pagos comenzarán una vez consigas tu oferta de trabajo.