



## Curso: Security + (SY-401)

### Descripción General:

En este curso, los estudiantes aplicarán, supervisarán y solucionarán problemas de infraestructura, la aplicación, la información y la seguridad operacional. Los estudiantes se prepararán para el CompTIA Security + examen de certificación (SY0-401).

### Al finalizar el curso:

#### Al término de este curso, el alumno será capaz de:

- » Identificar los conceptos fundamentales de la seguridad informática.
- » Identificar las amenazas y vulnerabilidades de seguridad.
- » Gestión de datos, aplicaciones y seguridad del host.
- » Implementar la seguridad de la red.
- » Identificar y aplicar el control de acceso y las medidas de seguridad de gestión de cuentas.
- » Administrar certificados.
- » Identificar y aplicar el cumplimiento y las medidas de seguridad operacional.
- » Gestión de riesgos.
- » Resolución de problemas y gestión de incidentes de seguridad.
- » Plan para la continuidad del negocio y recuperación de desastres.

### Audiencia:

Este curso está dirigido a los profesionales de tecnología de la información (IT) que tiene como responsabilidad la creación de redes y las habilidades administrativas en las redes (TCP / IP) basados en Windows® de control de transmisión / Protocolo de Internet Protocolo; familiaridad con otros sistemas operativos, como Mac OS X®, Unix o Linux; y que quiere seguir una carrera en TI mediante la adquisición de conocimientos básicos de temas de seguridad; prepararse para el examen de certificación CompTIA Security +; o utilizar Security + como la base para las certificaciones de seguridad avanzadas o roles profesionales.

### Duración:

40 horas

**Para más información:** [www.newhorizons.com.pa](http://www.newhorizons.com.pa)

### Observación:

EL manual y Examen del curso N+ SY0-401 están en idioma Inglés

<b>1</b>	<p><b>Lección 1: Aspectos básicos de seguridad</b></p> <ul style="list-style-type: none"> <li>» El ciclo de Seguridad de la Información</li> <li>» Controles de Seguridad de la Información</li> <li>» Métodos de autenticación</li> <li>» Fundamentos de Criptografía</li> <li>» Fundamentos Política de Seguridad</li> </ul>
<b>2</b>	<p><b>Lección 2: Identificación de Amenazas de Seguridad y Vulnerabilidades</b></p> <ul style="list-style-type: none"> <li>» Ingeniería Social</li> <li>» Malware</li> <li>» Amenazas de software basada en</li> <li>» Amenazas basadas en red</li> <li>» Amenazas y Vulnerabilidades inalámbricos</li> <li>» Amenazas físicas y vulnerabilidades</li> </ul>

<b>3</b>	<p><b>Lección 3: Gestión de datos, aplicaciones y seguridad de host</b></p> <ul style="list-style-type: none"> <li>» Manejo de Seguridad de Datos</li> <li>» Manejo de Seguridad de Aplicaciones</li> <li>» Administrar dispositivos y Seguridad del Host</li> <li>» Administrar Mobile Security</li> </ul>
<b>4</b>	<p><b>Lección 4: Implementación de seguridad de red</b></p> <ul style="list-style-type: none"> <li>» Parámetros de seguridad Configurar en dispositivos y tecnologías de red</li> <li>» Elementos de red Diseño y Componentes</li> <li>» Implementar protocolos y servicios de red</li> <li>» Aplicar los principios de administración de red segura</li> <li>» Secure tráfico inalámbrico</li> </ul>
<b>5</b>	<p><b>Lección 5: Implementación de control de acceso, autenticación y administración de cuentas</b></p> <ul style="list-style-type: none"> <li>» Control de acceso y servicios de autenticación</li> <li>» Implementar controles de cuentas de seguridad Gestión</li> </ul>
<b>6</b>	<p><b>Lección 6: Administración de certificados</b></p> <ul style="list-style-type: none"> <li>» Instale una jerarquía CA</li> <li>» Certificados Enroll</li> <li>» Asegure el tráfico de red mediante el uso de certificados</li> <li>» renovar los certificados</li> <li>» Copia de seguridad y restauración de certificados y claves privadas</li> <li>» Certificados Revocar</li> </ul>
<b>7</b>	<p><b>Lección 7: Cumplimiento Implementación y Seguridad Operacional</b></p> <ul style="list-style-type: none"> <li>» Seguridad Física</li> <li>» Cumplimiento Legal</li> <li>» Conciencia de Seguridad y Formación</li> <li>» Integrar los sistemas y datos con terceros</li> </ul>
<b>8</b>	<p><b>Lección 8: Gestión de Riesgos</b></p> <ul style="list-style-type: none"> <li>» Análisis de Riesgos</li> <li>» Implementar vulnerabilidad Herramientas de Evaluación y Técnicas</li> <li>» Analizar en busca de vulnerabilidades</li> <li>» Técnicas de mitigación y disuasión</li> </ul>
<b>9</b>	<p><b>Lección 9: Resolución de problemas y gestión de incidentes de seguridad</b></p> <ul style="list-style-type: none"> <li>» Responder a Incidentes de Seguridad</li> <li>» Recuperarse de un Incidente de Seguridad</li> </ul>
<b>10</b>	<p><b>Lección 10: Continuidad del negocio y recuperación de desastres Planificación</b></p> <ul style="list-style-type: none"> <li>» Continuidad del Negocio</li> <li>» Plan de Recuperación de Desastres</li> <li>» Ejecutar PRM y Procedimientos</li> </ul>