

A continuación se detalla el contenido del Curso IPv6 Forum Security Engineer (Gold), de una semana de duración y una carga de unas 40 horas, incluidos dos intentos de examen de certificación.

Curso	Día	Contenido
IPv6 Certified Security Engineer (Gold)	<b>Día 1</b>	1 Repaso de IPv6 1.1 Cabecera básica y de extensión 1.2 Direccionamiento IPv6 1.3 ICMPv6 1.4 Autoconfiguración: SLAAC vs. DHCPv6 1.5 Mecanismos de Transición IPv6  2 Introducción Seguridad TIC 2.1 Introducción 2.2 Seguridad Perimetral vs. Nodo 2.3 Clasificación de técnicas y amenazas 2.4 Prácticas y Herramientas de Seguridad 2.5 Capa Física 2.6 Capa de Enlace 2.7 Capa de Red 2.8 Capa de Transporte 2.9 Capa de Aplicación 2.10 Ingeniería Social  P1 - Laboratorio I P1.1 Preparación y herramientas básicas P1.2 Captura de paquetes P1.3 Identificación de parámetros P1.4 Generación de amenazas (I)
	<b>Día 2</b>	3 Amenazas de Seguridad con IPv6 3.1 Introducción: Mitos y Realidades 3.2 Clasificación Amenazas 3.3 Comparativa IPv4 vs. IPv6 3.4 Aspectos de seguridad con IPv6 3.5 First Hop Security (FHS) 3.6 Implicaciones de seguridad de IPv6 en redes solo-IPv4  4 Soluciones de Seguridad IPv6 4.1 Extensiones de Privacidad 4.2 IPsec 4.3 SEND 4.4 RA-GUARD 4.5 Especificaciones de Seguridad  5 IPv6 y la Seguridad de Capa 2 5.1 802.1x 5.2 Controles de capa 2  P2 - Ataques de Capa 2  6 Formato de Paquete IPv6 6.1 Cabecera básica IPv6 6.2 Cabeceras de extensión IPv6 6.3 Opciones IPv6

		<p>7 Arquitectura Direccionamiento IPv6</p> <p>7.1 Tamaño de prefijos y direcciones</p> <p>7.2 Ámbito de las direcciones</p> <p>7.3 Identificadores de interfaz</p> <p>7.4 Direcciones especiales o reservadas</p> <p>7.5 Exploración de redes IPv6</p> <p>7.6 Información Pública de la Red</p> <p>7.7 Direccionamiento Global</p> <p>P3 - Ataques Relacionados con Direccionamiento IPv6</p>
	<b>Día 3</b>	<p>8 ICMPv6</p> <p>8.1 Introducción</p> <p>8.2 Path MTU Discovery</p> <p>8.3 Fragmentación IPv6</p> <p>9 Neighbor Discovery Protocol (NDP)</p> <p>9.1 Amenazas a NDP</p> <p>9.2 DAD</p> <p>9.3 NUD</p> <p>9.4 Address Resolution</p> <p>10 SLAAC</p> <p>P4 - Ataques ICMPv6/NDP/SLAAC</p> <p>11 DHCPv6</p> <p>P5 - Ataques DHCP</p> <p>12 Multicast Listener Discovery (MLD)</p>
	<b>Día 4</b>	<p>13 DNS</p> <p>13.1 DNS con IPv6</p> <p>13.2 Ataques al DNS</p> <p>P6 - Ataques DNS</p> <p>14 Mecanismos de Transición</p> <p>15 Seguridad en Protocolos de Routing IPv6</p> <p>16 Filtrado con IPv6</p> <p>16.1 Filtrado de prefijos</p> <p>16.2 Filtrado de paquetes</p> <p>P7 - Filtrado de paquetes</p> <p>P7.1 Filtrando ICMPv6</p> <p>P7.2 Filtrando protocolos</p>
	<b>Día 5</b>	<p>17 Certificación IPv6 Forum</p> <p>17.1 Introducción certificaciones IPv6 Forum</p> <p>17.2 Preguntas preparatorias</p> <p>17.3 Simulacro examen</p> <p>17.4 Examen certificación IPv6 Forum Certified Security Engineer (Gold). Dos intentos con instructor</p>