PSP07.- Aplicaciones con comunicaciones seguras.

Orientaciones para el alumnado

En esta última unidad de trabajo del módulo, verás los conceptos relacionados con la criptografía, encriptación de la información y protocolos criptográficos, así como sus principales aplicaciones.

También verás las clases Java de los paquetes **`java.security`** y **`javax.crypto`**, que permiten encriptar información mediante clave pública y privada, realizar resúmenes de mensajes y firmas digitales.

Por último verás ve la biblioteca JSSE, en particular las clases **`SSLSocket`** y **`SSLServerSocket`** para programar aplicaciones cliente/servidor seguras.

Datos generales de la Unidad de Trabajo

Nombre completo del MP	Programación de servicos y procesos.	**Siglas MP**	PSP
Nº y título de la UT	07.- Aplicaciones con comunicaciones seguras.		
Índice o tabla de contenidos	La unidad de trabajo contiene los siguientes bloques de contenidos: 1.- Introducción. 2.- Criptografía. 2.1.- Encriptación de la información. 2.2.- Principios criptográficos. 2.3.- Criptografía de clave privada o simétrica. 2.4.- Criptografía de clave pública o asimétrica. 2.5.- Resumen de mensajes, firma digital y certificados digitales. 2.6.- Principales aplicaciones de la criptografía. 3.- Protocolos seguros de comunicaciones. 3.1.- Protocolo criptográfico SSL/TLS. 3.2.- Otros protocolos seguros. 4.- Criptografía en Java. 4.1.- Arquitectura criptográfica de Java. 4.2.- Proveedores y motores criptográficos. 4.3.- Gestión de claves con el paquete `java.security`. 4.4.- Resúmenes de mensajes con la clase `MessageDigest`. 4.5.- Firma digital con la clase `Signature` de `java.security`. 4.6.- Encriptación con la clase `Cipher` del paquete `javax.crypto`. 4.7.- Ejemplos de encriptación simétrica y asímetrica con `Cipher`. 5.- Sockets seguros en Java (JSSE). 5.1.- Programar un socket seguro de servidor. 5.2.- Programar un socket seguro cliente. 5.3.- Ejemplos de aplicaciones con comunicaciones seguras.		
Objetivos	✔ Proteger las aplicaciones y los datos definiendo y aplicando criterios de seguridad en el acceso, almacenamiento y transmisión de la información. ✔ Conocer las principales técnicas y aplicaciones de la criptografía. ✔ Utilizar el API criptográfico que incorpora Java para el desarrollo de aplicaciones con comunicaciones seguras y almacenamiento seguro de datos.		
Temporalización (estimación)	**Tiempo necesario para estudiar los contenidos (h)**		10
	Tiempo necesario para completar la tarea (h)		3

	Tiempo necesario para completar el examen (h)	1
	Nº de días que se recomienda dedicar a esta unidad	27
	La temporalización anterior no deja de ser una estimación media, ya que el tiempo a invertir va a depender mucho de las circunstancias personales de cada cual.	
Consejos y recomendaciones	Te ofrecemos una serie de pautas que pueden ayudarte y facilitar la tarea de aprendizaje: - Es muy importante que entiendas bien los conceptos de la unidad, básicos para este módulo. - Para ello es conveniente que dispongas de Internet para consultar dudas. - Organízate, elaborando un calendario y planificando un horario de estudio para evitar la acumulación de tareas. - Haz una primera lectura de los contenidos del tema y continúa con una lectura detallada de cada apartado realizando los ejercicios de autoevaluación y anotando todas las dudas para consultarlas con tu tutora o tutor. - Para completar conocimientos puedes consultar los enlaces que encontrarás bajo el epígrafe "Para Saber Más". - Recuerda que con este tipo de enseñanza tienes flexibilidad de horario y tú marcas el ritmo de estudio que más te interese, aunque te aconsejamos que te ajustes al calendario de aparición de las unidades didácticas y participes activamente en los foros de las respectivas unidades. - En la medida de tus posibilidades reserva un tiempo semanal para el estudio y procura respetarlo, la constancia y el esfuerzo son la clave del éxito en este tipo de enseñanzas. - Realiza las prácticas que están relacionadas con los contenidos que se vayan abordando. Ten en cuenta que en este tipo de formación a distancia tú eres quien tiene que determinar las prácticas que debes realizar. - Realiza la tarea correspondiente a la unidad, pero primero lee atentamente el enunciado y asegúrate de haber entendido lo que has de hacer. Envíasela a tu tutor o tutora a través del sistema establecido en la plataforma. - Haz el examen on-line de la unidad. - Internet es un gran recurso y una gran fuente de información, pero es recomendable contrastar las informaciones con fuentes fiables. - No dudes en comentarle a tu tutor o tutora cualquier duda que te pueda surgir.	