



## FICHA DE ACCIÓN FORMATIVA

TÍTULO DEL CURSO	INTRODUCCIÓN A LA CIBERSEGURIDAD: PRINCIPIOS Y BUENAS PRÁCTICAS
DURACIÓN (HORAS)	120 h
PROGRAMA/S AL QUE ESTÁ VINCULADO	<ul style="list-style-type: none"> <li>• Talento Joven</li> <li>• Talento 45+</li> </ul>
PÚBLICO OBJETIVO DEL CURSO	A jóvenes desempleados inscritos en el Sistema Nacional de Garantía Juvenil en búsqueda de empleo y personas entre 45 y 60 años de edad en situación de desempleo o inactividad laboral.
OBJETIVOS DE APRENDIZAJE	Capacitar al alumnado para: aprender los principios básicos de seguridad y el marco legal aplicable, para inventariar activos, gestionar datos y diseñar métricas de rendimiento, aprendiendo a configurar sistemas de monitorización, controlar accesos y aplicar buenas prácticas en redes y dispositivos, y abordar la creación y verificación de planes de continuidad y copias de seguridad, esenciales para la protección empresarial.
INDICACIÓN DE ALINEACIÓN CON CdP	<p>CÓDIGO CERTIFICADO: <b>IFCT0109</b></p> <p>VINCULADO A MÓDULO: <b>MF0490_3 – Gestión de servicios en el sistema informático 90 h convalidable directo</b></p>
MÓDULOS O BLOQUES TEMÁTICOS DEL CURSO	<ol style="list-style-type: none"> <li>1. Fundamentos de ciberseguridad, ética y marco legal</li> <li>2. Gestión de la seguridad y normativas</li> <li>3. Análisis de los procesos de sistemas</li> <li>4. Sistemas de almacenamiento</li> <li>5. Métricas e indicadores de rendimiento</li> <li>6. Monitorización de sistemas y comunicaciones</li> <li>7. Sistema de registro (logs) según requerimientos</li> <li>8. Control de accesos e identidades</li> <li>9. Redes seguras y Wi-Fi de laboratorio</li> <li>10. Backup, continuidad y recuperación</li> <li>11. Concienciación y buenas prácticas de usuario y endpoint</li> </ol>
OBSERVACIONES	