PROGRAMACIÓN DIDÁCTICA F.P.

TÉCNICO EN SISTEMAS MICROINFORMÁTICOS Y REDES (SMR)

SEGURIDAD INFORMÁTICA

BARTOLOMÉ JESÚS CHOZA MEDINA

CURSO 2026/2027

1. Contextualización y relación con el Plan de Centro

1.1. Ubicación de la enseñanza

El módulo profesional de Seguridad Informática (código 0226) se imparte en el segundo curso del Ciclo Formativo de Grado Medio en Sistemas Microinformáticos y Redes (SMR), perteneciente a la familia profesional de Informática y Comunicaciones. Con la nueva ordenación del sistema de Formación Profesional Dual en Andalucía, este módulo cuenta con una asignación de 84 horas totales distribuidas a razón de 4 horas semanales durante el periodo lectivo del centro educativo.

1.2. Cualificaciones Profesionales de Referencia y Unidades de Competencia (CNCP)

Este módulo profesional responde de forma directa a los requerimientos de la siguiente Cualificación Profesional del Catálogo Nacional de Cualificaciones Profesionales (CNCP):

- **Cualificación Profesional de Referencia:** Montaje y reparación de sistemas microinformáticos (Código: IFC300_2), que comprende las siguientes Unidades de Competencia:
- • UC0957_2: Mantener el rendimiento de los sistemas informáticos mediante el seguimiento de las recomendaciones de seguridad y uso.
- • UC0958_2: Aplicar técnicas de recuperación de datos e integridad del sistema ante incidencias informáticas.
- • UC0959_2: Realizar las operaciones de verificación y prueba de los elementos de seguridad y protección de datos.

1.3. Descripción del centro, contexto Socioeconómico y entorno Productivo

El IES Jándula se ubica en la localidad de Andújar (Jaén), prestando servicio a una amplia comarca con un tejido empresarial compuesto por pymes, empresas de servicios informáticos, entidades agroindustriales y sector público. La seguridad informática constituye un pilar estratégico transversal en todas las organizaciones del entorno para salvaguardar la confidencialidad de los datos, prevenir incidentes de ciberseguridad y cumplir con el Reglamento General de Protección de Datos (RGPD). El perfil profesional formado en el IES Jándula aporta valor directo garantizando entornos microinformáticos seguros y resilientes.

1.4. Integración con los planes y proyectos del centro

La programación de Seguridad Informática se alinea e integra estrechamente con las líneas estratégicas del Plan de Centro del IES Jándula:

- **Plan de Transformación Digital Educativa (TDE) y Competencia Digital:** Fomento del uso ético, responsable y seguro de las infraestructuras de red y equipos informáticos del centro.

- **Proyecto de Innovación Educativa:** Incorporación de metodologías activas y colaborativas para el diagnóstico de vulnerabilidades mediante simulación y entornos virtuales seguros.
- **Plan de Convivencia y Coeducación:** Concienciación sobre ciberseguridad, gestión ética de credenciales, derechos digitales y erradicación del ciberacoso.
- **Plan de Sostenibilidad y Ecoescuela:** Protocolos de gestión ambiental para el tratamiento de residuos de equipamiento de seguridad y sistemas de alimentación ininterrumpida (RAEE).

2. Marco legal

2.1. Normativa estatal de formación profesional

- Ley Orgánica 3/2022, de 31 de marzo, de ordenación e integración de la Formación Profesional.
- Real Decreto 659/2023, de 18 de julio, por el que se desarrolla la ordenación general del Sistema de Formación Profesional.
- Real Decreto 1691/2007, de 14 de diciembre, por el que se establece el título de Técnico en Sistemas Microinformáticos y Redes y sus enseñanzas mínimas.
- Real Decreto 499/2024, de 21 de mayo, por el que se modifican determinados Reales Decretos de títulos de Formación Profesional para la actualización de sus contenidos.

2.2. Normativa autonómica de formación profesional

- Decreto 147/2025, de 17 de septiembre, por el que se establece la ordenación de las enseñanzas de los Grados D y E del Sistema de Formación Profesional en la Comunidad Autónoma de Andalucía.
- Orden de 18 de septiembre de 2025, por la que se regula la evaluación, certificación, acreditación y titulación académica del alumnado que cursa enseñanzas de los grados D y E en la Comunidad Autónoma de Andalucía.
- Orden de 26 de septiembre de 2025, por la que se regula la fase de formación en empresa u organismo equiparado en la Comunidad Autónoma de Andalucía.
- Orden de 7 de julio de 2009, por la que se desarrolla el currículo correspondiente al título de Técnico en Sistemas Microinformáticos y Redes en Andalucía.
- Decreto 483/2026 y Orden de 31 de agosto de 2026, de medidas de simplificación administrativa y agilización en la gestión de las programaciones didácticas.

3. Objetivos Generales del Ciclo Formativo

3.1. Objetivos Generales

La enseñanza del módulo profesional de Seguridad Informática contribuye a alcanzar los siguientes Objetivos Generales del título de Técnico en Sistemas Microinformáticos y Redes:

a) Seleccionar y desplegar mecanismos de protección física, pasiva y lógica en sistemas informáticos para prevenir accesos no autorizados y pérdidas de información.

b) Aplicar técnicas de duplicación, copias de seguridad e integridad de datos garantizando la continuidad operativa del sistema.
c) Configurar cortafuegos, redes privadas virtuales y elementos de seguridad perimetral para proteger las comunicaciones de la red local.
d) Diagnosticar e intervenir ante la presencia de software malicioso ejecutando protocolos de desinfección y restauración.
e) Verificar el cumplimiento de la normativa legal sobre protección de datos de carácter personal y propiedad intelectual.

3.2. Competencias Profesionales, Personales y Sociales del Título

a) Desplegar sistemas de protección pasiva y física en los equipos y centros de proceso de datos.
b) Mantener la seguridad lógica en sistemas microinformáticos verificando los derechos de acceso y autenticación.
c) Ejecutar planes de respaldo y recuperación asegurando la disponibilidad de la información ante fallos de hardware o desastres.
d) Implementar conexiones seguras y redes privadas virtuales (VPN) para el tráfico cifrado de datos.

3.3. Resultados de aprendizaje del módulo

A continuación se presentan los 5 Resultados de Aprendizaje (RA) oficializados para el módulo de Seguridad Informática, junto con su ponderación dentro de la nota global del módulo:

Resultado de Aprendizaje (RA)	Descripción del RA	Ponderación (%)
RA1	Aplica medidas de seguridad pasiva en sistemas informáticos describiendo sus características y relacionándolas con las necesidades de protección.	**25 %**
RA2	Adopta medidas de seguridad activa y aseguramiento de la información configurando herramientas de copia de seguridad y almacenamiento redundante.	**25 %**
RA3	Asegura la confidencialidad e integridad de la información aplicando técnicas criptográficas y de autenticación de usuarios.	**25 %**
RA4	Configura la seguridad en redes locales e inalámbricas identificando vulnerabilidades y aplicando mecanismos de protección perimetral.	**20 %**

RA5	Cumple las normas sobre protección de datos personales y propiedad intelectual analizando la legislación vigente y las políticas de seguridad.	**5 %**

4. Organización, secuenciación y temporalización de los contenidos

4.1. Contenidos

Los contenidos del módulo se organizan en los siguientes bloques temáticos de conocimiento práctico y aplicado: seguridad pasiva y física en CPDs; copias de seguridad y sistemas redundantes RAID; criptografía y certificados digitales; seguridad perimetral, cortafuegos y VPNs; seguridad en redes Wi-Fi; software malicioso e incidentes de seguridad; y legislación sobre protección de datos (RGPD/LOPDGDD) y gestión ambiental de equipos.

4.2. Secuenciación de los contenidos

Con la carga lectiva de 84 horas anuales (4 horas semanales en 2º curso), las Unidades Didácticas se distribuyen de forma proporcional entre los trimestres lectivos del centro educativo:

Unidad Didáctica	Denominación de la Unidad	Horas Lectivas	RAs Implicados
UD 1	Seguridad informática e identificación de amenazas	**8 h**	RA1
UD 2	Seguridad pasiva, CPD, SAI y control de accesos	**8 h**	RA1
UD 3	Criptografía, firma electrónica y certificados digitales	**8 h**	RA3
UD 4	Seguridad perimetral, cortafuegos, VPN y redes	**28 h**	RA4
UD 5	Almacenamiento seguro, redundancia RAID y respaldos	**14 h**	RA2
UD 6	Seguridad activa, malware y protección de escritorio	**16 h**	RA3, RA2
UD 7	Legislación, LOPDGDD/RGPD y normas ISO 27001	**2 h**	RA5

4.3. Unidades Didácticas

A continuación se detalla la secuenciación y la carga horaria adaptada proporcionalmente para cada Unidad Didáctica:

4.3.1. Unidad 1: Seguridad informática e identificación de amenazas (8 h)

Conceptos de confidencialidad, integridad, disponibilidad y no repudio. Tipos de amenazas y análisis de riesgos.

4.3.2. Unidad 2: Seguridad pasiva, CPD, SAI y control de accesos (8 h)

Ubicación del CPD, control de acceso físico, climatización, dimensionamiento e instalación de SAIs.

4.3.3. Unidad 3: Criptografía, firma electrónica y certificados digitales (8 h)

Cifrado simétrico y asimétrico, funciones Hash, PKI, certificados X.509 y firma digital.

4.3.4. Unidad 4: Seguridad perimetral, cortafuegos, VPN y redes (28 h)

Configuración de cortafuegos (UFW/pfSense), filtrado de paquetes, zonas DMZ, VPNs (OpenVPN/WireGuard) y seguridad Wi-Fi (WPA3).

4.3.5. Unidad 5: Almacenamiento seguro, redundancia RAID y respaldos (14 h)

Configuración de volúmenes RAID informáticos, estrategias de copia de seguridad (completas, incrementales, diferenciales) y restauración.

4.3.6. Unidad 6: Seguridad activa, malware y protección de escritorio (16 h)

Análisis de malware (virus, ransomware, phishing), antivirus corporativos, bastionado de sistemas operacionales (hardening) y parches de seguridad.

4.3.7. Unidad 7: Legislación, LOPDGDD/RGPD y normas ISO 27001 (2 h)

Reglamento General de Protección de Datos (RGPD), LOPDGDD, derechos ARCO+, propiedad intelectual y principios del SGSI (ISO/IEC 27001).

4.4. Interdisciplinariedad

Seguridad Informática se coordina horizontalmente con los módulos de Servicios en Red (configuración de servidores DNS/HTTP seguros y cortafuegos), Sistemas Operativos en Red (permisos de acceso, directivas de grupo y bastionado) y Aplicaciones Web (seguridad en CMS y comercio electrónico).

4.5. Elementos transversales

- **Trabajo en equipo y comportamiento ético:** Sensibilización sobre el uso responsable de la información, protección de datos personales e identidad digital.
- **Sostenibilidad y cultura ambiental:** Gestión sostenible de residuos electrónicos (RAEE), baterías de SAI obsoletas y eficiencia energética en servidores.
- **Innovación tecnológica y cultura emprendedora:** Adopción de marcos de ciberseguridad corporativos y buenas prácticas operativas de concienciación.

5. Fase de Formación en empresa. Período, RAs dualizado/s

Conforme al Decreto 147/2025 y la Orden de 26 de septiembre de 2025, la Fase de Formación en Empresa (FFE) del módulo de Seguridad Informática se articula mediante actividades formativas coordinadas entre el centro docente y las empresas colaboradoras. Se potencian especialmente en la empresa los siguientes Criterios de Evaluación vinculados a los entornos de producción reales:

RA3 y RA4 (Seguridad Lógica y Redes): Instalación de agentes antivirus corporativos, despliegue de actualizaciones críticas de seguridad y soporte en la implantación de VPNs corporativas.

Evaluación integradora: El tutor o tutora laboral emitirá un informe cualitativo sobre el desempeño del alumnado en la empresa. Este informe será considerado de forma integradora por el profesorado del módulo para valorar la consecución práctica de los Criterios de Evaluación asociados a la FFE.

6. Principios metodológicos y pedagógicos

6.1. Orientaciones metodológicas

Se adopta una metodología activa, práctica y competencial orientada al Aprendizaje Basado en Retos (ABR) y la resolución de incidentes de seguridad simulados. Las actividades integran el análisis de casos reales de vulnerabilidades, auditorías sencillas de sistemas y el despliegue defensivo de herramientas informáticas de protección.

6.2. Actividades de enseñanza-aprendizaje

- **Laboratorio de Seguridad Pasiva:** Montaje simulado y configuración de SAIs, calculando tiempos de autonomía y respuesta ante fallos de suministro eléctrico.
- **Taller de Criptografía:** Generación de pares de claves RSA/ECC, cifrado de archivos con OpenSSL/GPG y firma/verificación de documentos digitales.
- **Laboratorio de Seguridad Perimetral:** Despliegue y configuración de reglas de cortafuegos en entornos Linux/Windows y establecimiento de túneles VPN punto a punto.
- **Prácticas de Diagnóstico:** Análisis e identificación de patrones de tráfico sospechosos con Wireshark y configuración de herramientas de restauración ante desastres.

6.3. Materiales y recursos didácticos

- **Equipamiento de Aula:** Equipos PC con soporte de virtualización (VirtualBox/VMware), distribuciones Linux (Ubuntu/Debian) y sistemas Windows Server.
- **Software Específico:** Wireshark, OpenSSL, VeraCrypt, UFW, pfSense, Clonezilla, VeraCrypt y suites antivirus corporativas de evaluación.
- **Recursos Documentales:** Documentación técnica del INCIBE, CCN-CERT, Guías de seguridad AEPD y estándares ISO/IEC 27001.

7. Evaluación

7.1. Instrumentos de evaluación

La evaluación es continua, formativa, integradora y criterial (Orden de 18 de septiembre de 2025). Los instrumentos de evaluación son exclusivamente herramientas y medios para la recogida de evidencias del aprendizaje, sin asignación directa de porcentajes fijos a los instrumentos. Se utilizan los siguientes medios:

- **Pruebas Teórico-Prácticas (PTP):** Pruebas escritas y supuestos prácticos individuales de resolución de incidencias, configuración de cortafuegos y ejercicios criptográficos.
- **Actividades Prácticas de Desarrollo (ATP):** Entregas obligatorias de memorias técnicas de prácticas, scripts de respaldo, configuraciones de VPN y pruebas en entornos virtualizados.
- **Trabajo de Clase y Observación (TCC):** Observación del desempeño diario en el aula-taller, rigor técnico, cumplimiento de protocolos de seguridad y actitud profesional.

7.2. Ponderación de resultados de aprendizaje y criterios de evaluación

De acuerdo con los estándares aprobados en el departamento, la calificación del módulo se determina de forma estricta según la ponderación porcentual asignada a cada Resultado de Aprendizaje (RA). Los Criterios de Evaluación (CE) actúan como descriptores de logro sin peso porcentual individualizado:

- RA1 (Seguridad Pasiva y Física): 20 % de la nota final.
- RA2 (Seguridad Activa, RAID y Respaldos): 20 % de la nota final.
- RA3 (Criptografía y Autenticación): 30 % de la nota final.
- RA4 (Seguridad en Redes y Perimetral): 20 % de la nota final.
- RA5 (Legislación y Protección de Datos): 10 % de la nota final.

7.3. Matriz de ponderación criterios de evaluación y unidades didácticas

Matriz de correspondencia y evaluación de los Resultados de Aprendizaje en las Unidades Didácticas y en la empresa:

RA	Peso RA	UD1	UD2	UD3	UD4	UD5	UD6	UD7
RA1	**25 %**	**X**	**X**					
RA2	**25 %**					**X**	**X**	
RA3	**25 %**			**X**			**X**	
RA4	**20 %**				**X**			
RA5	**5 %**							**X**

7.4. Sistema de recuperación, subida de nota y evaluaciones Final1ª y Final2ª

Regla del 80 % de Asistencia Obligatoria (PEC IES Jándula / Orden de 18 de septiembre de 2025): La asistencia a las actividades lectivas es obligatoria. Al contar el módulo con una carga de 84 horas lectivas, acumular más del 20 % de ausencias no justificadas (17 horas o más) supondrá la pérdida del derecho a la evaluación continua en la convocatoria ordinaria. El alumnado en esta situación conservará el derecho a ser evaluado mediante una prueba presencial global extraordinaria y la entrega completa de los supuestos prácticos de laboratorio programados.

Mecanismos de Recuperación y Mejora: Durante el periodo ordinario se realizarán pruebas de recuperación por cada RA no superado. En la sesión de evaluación ordinaria de junio se habilitará una prueba específica de recuperación y de mejora de calificación para el alumnado que desee elevar su nota final.

8. Atención a la diversidad

En cumplimiento con los principios del Diseño Universal para el Aprendizaje (DUA), la programación garantiza la accesibilidad a los contenidos mediante múltiples formas de representación, expresión y compromiso. Se aplican adaptaciones metodológicas, tiempos adicionales en las pruebas evaluativas y el uso de herramientas asistivas sin minorar los Criterios de Evaluación necesarios para obtener el título profesional.

- **Medidas de refuerzo:** Enunciados guiados paso a paso para laboratorios de virtualización, repositorios de comandos y tutorías de refuerzo.
- **Medidas de ampliación:** Auditorías avanzadas de seguridad perimetral, análisis de firmas de malware y despliegue de cortafuegos empresariales.

9. Bibliografía del módulo

- **Recursos Oficiales INCIBE:** Guías de buenas prácticas y alertas del Instituto Nacional de Ciberseguridad (INCIBE — www.incibe.es).
- **Documentación CCN-CERT:** Series de Guías STIC del Centro Criptológico Nacional (CCN-CERT — www.ccn-cert.cni.es).
- **Portal AEPD:** Materiales pedagógicos y guías sobre el RGPD de la Agencia Española de Protección de Datos (AEPD — www.aepd.es).