GUÍA DIDÁCTICA

CIBERSEGURIDAD

Ciclo Formativo: Sistemas Microinformáticos y Redes (SMR)
Centro: I.E.S. Alto Jarama
Profesor: Antonio Sanz
Curso académico: 2025 – 2026
Módulo: CMO-314 Ciberseguridad

ÍNDICE

Contenido

1. Competencias del título vinculadas al módulo

El módulo profesional **Ciberseguridad** contribuye al desarrollo de las **competencias profesionales, personales y sociales** del título de *Técnico en Sistemas Microinformáticos y Redes*, entre las que destacan:

- **C1.** Instalar, configurar y mantener sistemas microinformáticos, garantizando su funcionalidad y seguridad.
- **C2.** Detectar y resolver incidencias de seguridad en equipos y redes locales.
- **C3.** Implementar políticas de seguridad activa y pasiva.
- **C4.** Realizar copias de seguridad y restauración de datos.
- **C5.** Configurar mecanismos de protección frente a software malicioso y ataques externos.
- **C6.** Aplicar medidas preventivas de protección ambiental y personal en el mantenimiento de equipos.
- **C7.** Cumplir la normativa legal relacionada con la protección de datos, la privacidad y la propiedad intelectual.
- **C8.** Documentar procedimientos de seguridad y elaborar informes técnicos.

Estas competencias se alinean con las **competencias clave europeas**:

- Competencia digital.
- Competencia matemática y en ciencia, tecnología e ingeniería.
- Aprender a aprender.
- Competencias personales, sociales y de aprender a convivir.
- Competencia ciudadana y en conciencia y expresión cultural.

De este modo, el módulo fomenta no solo las capacidades técnicas, sino también la **responsabilidad ética, la prevención, la gestión de riesgos** y el **uso responsable de las tecnologías de la información**.

2. Resultados de aprendizaje y criterios de evaluación

De acuerdo con la **Orden 3536/2025, de 12 de agosto, de la Consejería de Educación, Ciencia y Universidades** *del 27 de agosto sobre el Currículo de los módulos profesionales que integran el catálogo de optatividad en los ciclos formativos de grado medio*, los RA's para este módulo son los siguientes:

RESULTADOS DE APRENDIZAJE (RA) Y SU PONDERACIÓN EN EL MÓDULO		
		%
RA1	Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.	20%
RA2	Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.	20%
RA3	Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.	20%
RA4	Diseña planes de securización de sistemas e implanta sistemas de control de acceso y autenticación de personas.	20%
RA5	Utiliza herramientas de monitorización para detectar vulnerabilidades y ataque y defensa en entornos de pruebas.	10%
RA6	Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia..	10%
	TOTAL %	100%

RA1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.

Criterios de evaluación:

a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos.
b) Se han descrito las diferencias entre seguridad física y lógica.
c) Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen.
d) Se ha contrastado la incidencia de las técnicas de ingeniería social en los

fraudes informáticos.

e) Se han adoptado políticas de contraseñas
f) Se han valorado las ventajas que supone la utilización de sistemas biométricos.
g) Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información.
h) Se ha reconocido la necesidad de establecer un plan integral de protección perimetral, especialmente en sistemas conectados a redes públicas.
i) Se han identificado las fases del análisis forense ante ataques a un sistema.

RA2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.

Criterios de evaluación:

a) Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático.
b) Se ha verificado el origen y la autenticidad de las aplicaciones instaladas en un equipo, así como el estado de actualización del sistema operativo.
c) Se ha identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles
d) Se han analizado diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados.
e) Se han implantado aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso.
f) Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas.
g) Se han evaluado las medidas de seguridad de los protocolos usados en redes inalámbricas.
h) Se ha reconocido la necesidad de inventariar y controlar los servicios de red que se ejecutan en un sistema.
i) Se han descrito los tipos y características de los sistemas de detección de Intrusiones.

RA3. Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.

Criterios de evaluación:

a) Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red interna.
b) Se han clasificado las zonas de riesgo de un sistema, según criterios de seguridad perimetral.
c) Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización.
d) Se han configurado redes privadas virtuales mediante protocolos seguros a distintos niveles.
e) Se ha implantado un servidor como pasarela de acceso a la red interna desde ubicaciones remotas.
f) Se han identificado y configurado los posibles métodos de autenticación en el acceso de usuarios remotos a través de la pasarela.
g) Se ha instalado, configurado e integrado en la pasarela un servidor remoto de autenticación.

RA4. Diseña planes de securización de sistemas e implanta sistemas de control de acceso y autenticación de personas.

Criterios de evaluación:

a) Se han identificado los distintos tipos de copias de seguridad (completa, incremental, diferencial).
b) Se han identificado los activos, las amenazas y vulnerabilidades de la organización.
c) Se han evaluado las medidas de seguridad actuales.
d) Se ha elaborado un análisis de riesgo de la situación actual en ciberseguridad de la organización
e) Se han definido los mecanismos de autenticación en base a distintos / múltiples factores (físicos, inherentes y basados en el conocimiento) existentes.
f) Se han definido protocolos y políticas de autenticación basados en contraseñas y frases de paso, en base a las principales vulnerabilidades y tipos de ataques.

RA5. Utiliza herramientas de monitorización para detectar vulnerabilidades y ataque y defensa en entornos de pruebas.

Criterios de evaluación:

a) Se ha definido la terminología esencial del hacking ético.
b) Se ha definido el alcance y condiciones de un test de intrusión.
c) Se han analizado y definido los tipos vulnerabilidades.
d) Se han analizado y definido los tipos de ataque.
e) Se han determinado y caracterizado las diferentes vulnerabilidades existentes.
f) Se han determinado las herramientas de monitorización disponibles en el mercado adecuadas en función del tipo de organización.
g) Se han utilizado técnicas de "Equipo Rojo y Azul".
h) Se han realizado informes sobre las vulnerabilidades detectadas

RA6. Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.

Criterios de evaluación:

a) Se ha descrito la legislación sobre protección de datos de carácter personal.
b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.
c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.
d) Se ha contrastado el deber de poner a disposición de las personas los datos personales que les conciernen.
e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.
f) Se han contrastado las normas sobre gestión de seguridad de la información.
g) Se ha comprendido la necesidad de conocer y respetar la normativa legal aplicable.

3. Contenidos del módulo

Los contenidos del módulo **Ciberseguridad,** según la **Orden 3536/2025, de 12 de agosto, de la Consejería de Educación, Ciencia y Universidades** *del 27 de agosto sobre el Currículo de los módulos profesionales que integran el catálogo de optatividad en los ciclos formativos de grado medio*

Bloque 1. Adopción de pautas de seguridad informática.

- Principios de seguridad: confidencialidad, integridad, disponibilidad.
- Tipos de amenazas y vulnerabilidades.
- Políticas y normas de seguridad.
- Medidas de seguridad activa y pasiva.
- Ética profesional y responsabilidad en la gestión de la seguridad.

Bloque 2. Seguridad física y ambiental.

- Tipos de malware: virus, troyanos, gusanos, ransomware, spyware, rootkits.
- Análisis y detección de malware.
- Herramientas antivirus, antimalware y cortafuegos.
- Seguridad en el arranque del sistema.
- Procedimientos de desinfección y recuperación.

Bloque 3. Seguridad lógica.

- Ley Orgánica 3/2018 (LOPDGDD) y Reglamento General de Protección de Datos (RGPD).
- Políticas de privacidad y seguridad de la información.
- Gestión de permisos de acceso y auditoría de usuarios.
- Cifrado simétrico y asimétrico: GPG, certificados digitales.
- Control de acceso mediante contraseñas seguras y autenticación multifactor.

Bloque 4. Análisis forense en sistemas informáticos.

- Estrategias de backup: completo, diferencial, incremental.
- Herramientas de copia de seguridad: Cobian Backup, Veeam, *rsync*, *tar*.
- Automatización de copias mediante tareas programadas.
- Procedimientos de restauración y verificación de datos.
- Almacenamiento externo y en la nube (Google Drive, NAS).

Bloque 5. Implantación de mecanismos de seguridad activa.

- Conceptos de red segura.
- Vulnerabilidades de red y ataques comunes (sniffing, spoofing, DoS).
- Configuración de cortafuegos (Windows, Linux, pfSense).
- Protocolos seguros: SSL/TLS, HTTPS, SSH, VPN.
- Seguridad en redes inalámbricas: WPA3, autenticación 802.1X.
- Monitorización de tráfico con Wireshark y Nmap.

Bloque 6. Seguridad en la red corporativa.

- Fases de una auditoría de seguridad.
- Herramientas básicas: Nmap, Nessus, Metasploit, Nikto, OpenVAS.
- Análisis de vulnerabilidades en entornos virtualizados.
- Elaboración de informes técnicos de auditoría.
- Buenas prácticas éticas y legales en las pruebas de seguridad.

Bloque 7. Implantación de técnicas de acceso remoto. Seguridad perimetral.

- Fases de una auditoría de seguridad.
- Herramientas básicas: Nmap, Nessus, Metasploit, Nikto, OpenVAS.
- Análisis de vulnerabilidades en entornos virtualizados.
- Elaboración de informes técnicos de auditoría.
- Buenas prácticas éticas y legales en las pruebas de seguridad.

Bloque 8. Bastionado de redes y sistemas.

- Fases de una auditoría de seguridad.
- Herramientas básicas: Nmap, Nessus, Metasploit, Nikto, OpenVAS.
- Análisis de vulnerabilidades en entornos virtualizados.

- Elaboración de informes técnicos de auditoría.
- Buenas prácticas éticas y legales en las pruebas de seguridad.

Bloque 9. Hacking ético.

- Fases de una auditoría de seguridad.
- Herramientas básicas: Nmap, Nessus, Metasploit, Nikto, OpenVAS.
- Análisis de vulnerabilidades en entornos virtualizados.
- Elaboración de informes técnicos de auditoría.
- Buenas prácticas éticas y legales en las pruebas de seguridad.

Bloque 10. Normativa de ciberseguridad.

- Fases de una auditoría de seguridad.
- Herramientas básicas: Nmap, Nessus, Metasploit, Nikto, OpenVAS.
- Análisis de vulnerabilidades en entornos virtualizados.
- Elaboración de informes técnicos de auditoría.
- Buenas prácticas éticas y legales en las pruebas de seguridad.

4. Desarrollo de las Unidades Didácticas

El módulo profesional **Ciberseguridad** se organiza en **nueve unidades didácticas**, que integran los contenidos, las competencias y los resultados de aprendizaje descritos en el currículo oficial.

Cada unidad combina la enseñanza teórica con prácticas de laboratorio, simulaciones y actividades de aplicación real, orientadas a desarrollar las competencias técnicas y transversales del alumnado.

UD1. Fundamentos de la Ciberseguridad (incluye seguridad física y ambiental) y tratamiento seguro de la información.

Duración estimada: 13 horas

Resultado de aprendizaje asociado: RA1

Competencias relacionadas

- CP1: Instalar y mantener sistemas informáticos seguros.
- CP2: Analizar vulnerabilidades y riesgos.
- CP3: Aplicar medidas de protección.
- CP4: Cumplir normativa de protección de datos.
- CP5: Actuar con responsabilidad y ética digital.

Objetivos específicos:

- Reconocerá la importancia de la confidencialidad, integridad y disponibilidad (CIA) en los sistemas.
- Clasificará vulnerabilidades según su origen, tipología e impacto.
- Diferenciará entre seguridad física y seguridad lógica.
- Identificará técnicas de ingeniería social y su relación con el fraude informático.
- Aplicará políticas seguras de contraseñas y autenticación.
- Valorará el uso de sistemas biométricos como método de autenticación.
- Utilizará técnicas criptográficas básicas para proteger la información.
- Comprenderá la necesidad de un plan perimetral de seguridad.
- Identificará las fases del análisis forense ante incidentes.
- Conocerá la legislación vigente sobre protección de datos y servicios digitales.
- Reconocerá derechos, obligaciones y roles legales en el tratamiento de datos.

Actividades principales:

- Presentación interactiva.
- Identificación de riesgos físicos.
- Análisis de casos reales.
- Mini cuestionario inicial.
- Práctica: contraseñas seguras.
- Mapa básico de vulnerabilidades.

Instrumentos de evaluación:

- Observación directa.
- Preguntas orales.
- Cuestionario tipo test.
- Lista de cotejo.
- Ficha de análisis.

Criterios de calificación:

- Participación: 20%
- Prácticas: 40%
- Cuestionarios: 30%
- Actitud y ética digital: 10%

UD2. Seguridad Activa, Malware y Contramedidas

Duración estimada: 16 sesiones
Resultado de aprendizaje asociado: RA2:

Competencias relacionadas

- CP1: Instalar y mantener sistemas informáticos seguros.
- CP2: Analizar vulnerabilidades y riesgos.
- CP3: Aplicar medidas de protección.

Objetivos específicos:

- Clasificar amenazas lógicas.
- Analizar malware en entorno controlado.
- Implantar herramientas antimalware.
- Aplicar cifrado y certificados.
- Reconocer IDS/IPS.

Actividades principales:

- Análisis de malware controlado.
- Uso de antivirus y antimalware.
- Creación de reglas básicas firewall.
- Laboratorio Wi-Fi segura.

Instrumentos de evaluación:

- Observación directa.
- Prácticas evaluables.
- Prueba objetiva.

Criterios de calificación:

- Prácticas: 50%
- Prueba escrita: 30%
- Actitud: 20%

UD3. Redes Seguras, Perímetro y Acceso Remoto (VPN)

Duración estimada: 13 sesiones
Resultado de aprendizaje asociado: RA3

Competencias relacionadas

- CP1: Instalar y mantener sistemas informáticos seguros.
- CP3: Aplicar medidas de protección.

Objetivos específicos:

- Reconocer zonas de riesgo.
- Configurar VPN.
- Implantar pasarela de acceso remoto.
- Configurar autenticación remota.

Actividades principales:

- Configuración OpenVPN.
- Montaje de pasarela remota.
- Prueba de protocolos seguros.
- Práctica SSH + Firewall.

Instrumentos de evaluación:

- Prácticas
- Test
- Observación

Criterios de calificación:

- Prácticas: 50%
- Prueba escrita: 30%
- Actitud: 20%

UD4. Plan de Securización y Control de Acceso

Duración estimada: 16 sesiones
Resultado de aprendizaje asociado: RA4

Competencias relacionadas

- CP1: Instalar y mantener sistemas informáticos seguros.
- CP2: Analizar vulnerabilidades y riesgos.
- CP3: Aplicar medidas de protección.

Objetivos específicos:

- Identificar activos, amenazas y vulnerabilidades.
- Realizar análisis de riesgos.
- Configurar MFA.
- Establecer políticas de autenticación.

Actividades principales:

- Análisis de riesgos.
- Configuración MFA.
- Práctica de copias de seguridad.

Instrumentos de evaluación:

- Prácticas
- Informe
- Test

Criterios de calificación:

- Prácticas: 40%
- Prueba escrita: 40%
- Actitud: 20%

UD5. Monitorización, Detección y Respuesta (Red/Blue Team)

Duración estimada: 15 sesiones

Resultado de aprendizaje asociado: RA5

Competencias relacionadas

- CP1: Instalar y mantener sistemas informáticos seguros.
- CP2: Analizar vulnerabilidades y riesgos.
- CP3: Aplicar medidas de protección.

Objetivos específicos:

- Comprender hacking ético.
- Detectar vulnerabilidades.
- Aplicar técnicas Red Team y Blue Team.

Actividades principales:

- Simulación ataque-defensa.
- Uso de herramientas de monitorización.
- Informe técnico.

Instrumentos de evaluación:

- Informe
- Observación
- Test

Criterios de calificación:

- Prácticas: 50%
- Prueba escrita: 40%
- Actitud: 10%

UD6. Integración Normativa y Proyecto Final

Duración estimada: 12 sesiones

Resultado de aprendizaje asociado: RA6

Competencias relacionadas

- CP1
- CP2
- CP3
- CP4
- CP5

Objetivos específicos:

- Integrar conocimientos del módulo.
- Elaborar un proyecto de securización.
- Aplicar normativa en un caso real.

Actividades principales:

- Proyecto final.
- Revisión normativa.
- Presentación oral.

Instrumentos de evaluación:

- Informe final
- Presentación
- Rúbrica

Criterios de calificación:

- Prácticas: 50%
- Prueba escrita: 30%
- Actitud: 20%

Fase de formación en empresa

FASE DE FORMACIÓN EN EMPRESA			
RA5. Monitorización, Detección y Respuesta (Red/Blue Team)		**30% de RA5**	**%**
ACTIVIDADES PROPUESTAS		**ACTIVIDADES DE EVALUACIÓN**	
Actividades en la empresa relacionadas con el RA esperado		A acordar con le empresa con convenio	
INSTRUMENTOS DE EVALUACIÓN		**INSTRUMENTOS DE CALIFICACIÓN**	
Documento de evaluación FFE		Escala numérica	
CRITERIOS DE CALIFICACIÓN			
Instrumento de Evaluación	**%**	**Criterio de Evaluación**	
Documento de evaluación FFE	5%	e)	Se han determinado y caracterizado las diferentes vulnerabilidades existentes.
Documento de evaluación FFE	5%	f)	Se han determinado las herramientas de monitorización disponibles en el mercado adecuadas en función del tipo de organización.
Documento de evaluación FFE	7,5%	e)	Se han analizado y definido los tipos vulnerabilidades.
Documento de evaluación FFE	5%	g)	Se han utilizado técnicas de "Equipo Rojo y Azul".
Documento de evaluación FFE	7,5%	h)	Se han realizado informes sobre las vulnerabilidades detectadas
CONSIDERACIONES SOBRE LOS INSTRUMENTOS DE EVALUACIÓN Y DE CALIFICACIÓN			
Evaluación de FFEs: El profesor tendrá en cuenta la valoración realizada por el tutor de la empresa sobre los RA que los calificará como "superados o no superados" (evaluación cualitativa). El tutor de la empresa valorará el grado de consecución de los RA en una escala del 0 al 10 para ayudar al profesor del módulo a aplicar los criterios de calificación asociados a estos RA. Esta valoración se incluirá en el informe del tutor de empresa en el campo de observaciones. - Si no se hace así, se aplicará un **10** a cada criterio de evaluación superado y un **4** a cada criterio de evaluación en caso de No Superado. Con estas calificaciones se calculará la media final del RA o Ras incluido en la FFE. - Si un alumno contraviene las normas básicas, podrá determinarse la finalización anticipada de la FFE y será calificado con un 0 en cada criterio de calificación del RA asociado a la FFE.			