GUÍA DIDÁCTICA

SEGURIDAD INFORMÁTICA

Ciclo Formativo: Sistemas Microinformáticos y Redes (SMR)
Centro: I.E.S. Alto Jarama
Profesor: Antonio Sanz
Curso académico: 2025 – 2026
Módulo: 0226 Seguridad Informática

ÍNDICE

Contenido

1. Introducción y contextualización del módulo

El módulo profesional **Seguridad Informática** pertenece al segundo curso del ciclo formativo de grado medio **Sistemas Microinformáticos y Redes (SMR)**, en la familia profesional de **Informática y Comunicaciones**.

Su finalidad es capacitar al alumnado para **aplicar técnicas y procedimientos que garanticen la seguridad de los equipos, sistemas y redes**, preservando la integridad, disponibilidad y confidencialidad de la información.

Este módulo proporciona los conocimientos y destrezas necesarios para configurar entornos seguros, gestionar copias de seguridad, proteger la información frente a accesos no autorizados y aplicar medidas preventivas frente a vulnerabilidades.

Además, integra las bases de la **aplicada** a entornos empresariales, orientando al alumno a detectar riesgos, implementar soluciones de protección y valorar la importancia de la seguridad digital en la sociedad actual.

Orientación profesional

El contenido de este módulo está directamente relacionado con perfiles laborales emergentes en el ámbito de la seguridad digital. Las salidas profesionales más vinculadas son:

- **Técnico/a en soporte y mantenimiento informático.**
- **Técnico/a de redes locales y servicios de Internet.**
- **Administrador/a de sistemas en entornos seguros.**
- **Técnico/a en seguridad básica.**
- **Auditor/a auxiliar en seguridad de sistemas.**

La formación adquirida sienta las bases para continuar estudios en **ciclos de grado superior** de la misma familia profesional, especialmente en el módulo **Seguridad en entornos de las tecnologías de la información (CE-TI)** del ciclo **ASIR**.

El módulo se desarrolla en el segundo curso, momento en el que el alumnado ya dispone de competencias previas en montaje, mantenimiento de equipos y administración de redes, lo que permite abordar la seguridad informática desde una perspectiva global y aplicada.

2. Resultados de aprendizaje y criterios de evaluación

De acuerdo con el *Real Decreto 1691/2007* y el *Decreto 107/2010*, los resultados de aprendizaje (RA) y criterios de evaluación (CE) del módulo **Seguridad Informática** son los siguientes:

RESULTADOS DE APRENDIZAJE (RA) Y SU PONDERACIÓN EN EL MÓDULO		
		%
RA1	Determina las medidas de seguridad activa y pasiva necesarias en un sistema informático, analizando las posibles vulnerabilidades.	20%
RA2	Aplica procedimientos de protección frente a software malicioso, seleccionando y configurando las herramientas necesarias.	20%
RA3	Configura el sistema para asegurar la protección de datos, aplicando la normativa vigente.	20%
RA4	Realiza procedimientos de copia y restauración, garantizando la integridad y disponibilidad de la información.	20%
RA5	Utiliza herramientas de monitorización para detectar vulnerabilidades y ataque y defensa en entornos de pruebas.	20%
	TOTAL %	100%

RA1. Determina las medidas de seguridad activa y pasiva necesarias en un sistema informático, analizando las posibles vulnerabilidades.

Criterios de evaluación:

1. Se han identificado las amenazas potenciales de seguridad sobre los sistemas informáticos.
2. Se han clasificado las medidas de seguridad activa y pasiva.
3. Se han aplicado herramientas de diagnóstico y detección de vulnerabilidades.
4. Se han propuesto medidas correctoras adecuadas al contexto.
5. Se han documentado los procedimientos y conclusiones del análisis.

RA2. Aplica procedimientos de protección frente a software malicioso, seleccionando y configurando las herramientas necesarias.

Criterios de evaluación:

1. Se han identificado los diferentes tipos de malware y sus efectos.
2. Se han instalado y configurado programas antivirus, antiespía y cortafuegos.
3. Se han actualizado las bases de datos de firmas de virus.
4. Se han realizado análisis periódicos de los sistemas y redes.
5. Se han documentado los resultados de los análisis realizados.

RA3. Configura el sistema para asegurar la protección de datos, aplicando la normativa vigente.

Criterios de evaluación:

1. Se han identificado los tipos de información personal y sensible.
2. Se han aplicado políticas de control de acceso a los datos.
3. Se han gestionado permisos de lectura, escritura y ejecución.
4. Se han implementado procedimientos de cifrado y autenticación.
5. Se han realizado copias de seguridad automáticas y programadas.
6. Se ha documentado la configuración y mantenimiento del sistema seguro.

RA4. Realiza procedimientos de copia y restauración, garantizando la integridad y disponibilidad de la información.

Criterios de evaluación:

1. Se han identificado los distintos tipos de copias de seguridad (completa, incremental, diferencial).
2. Se han programado copias automáticas con herramientas de respaldo.
3. Se han realizado pruebas de restauración verificando su eficacia.
4. Se han documentado las operaciones de copia y recuperación.

RA5. Aplica medidas de seguridad en redes de área local, configurando dispositivos y servicios de comunicación.

Criterios de evaluación:

1. Se han identificado vulnerabilidades en redes cableadas e inalámbricas.
2. Se han configurado cortafuegos (*firewalls*) y listas de control de acceso.
3. Se han implantado protocolos seguros (HTTPS, SSH, VPN).
4. Se ha comprobado la efectividad de las medidas adoptadas mediante pruebas de penetración.
5. Se han documentado las actuaciones realizadas y los resultados obtenidos.

3. Contenidos del módulo

Los contenidos del módulo **Seguridad Informática,** según el currículo del *Decreto 107/2010* de la Comunidad de Madrid, se estructuran en los siguientes bloques temáticos:

Bloque 1. Conceptos básicos 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. Protección frente a software malicioso

- 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. Protección de datos y normativa legal

- 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. Copias de seguridad y recuperación de datos

- 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. Seguridad en redes

- 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. Herramientas de auditoría y pruebas de penetración

- 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 **Seguridad Informática** se organiza en **seis 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. Conceptos básicos y medidas de seguridad en sistemas informáticos

Duración estimada: 15 horas
Competencias relacionadas: C1, C2, C3
Resultado de aprendizaje asociado: RA1

Objetivos específicos:

- Comprender los principios básicos de la seguridad informática.
- Analizar amenazas y vulnerabilidades comunes en sistemas y redes.
- Aplicar medidas de seguridad activa y pasiva en equipos informáticos.

Actividades principales:

- Debate inicial sobre la importancia de la seguridad en la era digital.
- Identificación de vulnerabilidades en sistemas operativos simulados.
- Configuración de medidas básicas de seguridad en Windows y Linux.
- Elaboración de un informe de riesgos inicial del aula/laboratorio.

Instrumentos de evaluación:

- Cuaderno de trabajo.
- Observación directa de prácticas.
- Informe técnico individual.

Criterios de calificación:

- Participación activa y trabajo en equipo (20%)
- Precisión en el análisis de vulnerabilidades (40%)
- Calidad y claridad del informe técnico (40%)

UD2. Protección frente a software malicioso

Duración estimada: 20 horas
Competencias relacionadas: C2, C3, C5
Resultado de aprendizaje asociado: RA2

Objetivos específicos:

- Identificar y clasificar los diferentes tipos de malware.
- Utilizar herramientas antivirus, antiespía y cortafuegos.
- Configurar políticas de actualización y protección del sistema.

Actividades principales:

- Instalación y configuración de software antimalware (Malwarebytes, Windows Defender, ClamAV).
- Simulación de infección controlada en entorno virtualizado.
- Configuración de reglas básicas de cortafuegos en Windows y pfSense.
- Elaboración de una guía práctica de prevención y detección.

Instrumentos de evaluación:

- Prueba práctica individual.
- Documentación técnica del proceso.
- Informe de resultados.

Criterios de calificación:

- Correcta configuración de herramientas de protección (40%)
- Detección y eliminación de amenazas (40%)
- Calidad de la documentación (20%)

UD3. Protección de datos y normativa legal

Duración estimada: 20 horas
Competencias relacionadas: C3, C7, C8
Resultado de aprendizaje asociado: RA3

Objetivos específicos:

- Comprender la legislación vigente en materia de protección de datos.
- Configurar políticas de privacidad y acceso seguro.
- Aplicar técnicas de cifrado y autenticación segura.

Actividades principales:

- Análisis de casos reales de vulneraciones del RGPD.
- Creación de cuentas y políticas de contraseñas seguras.
- Cifrado y descifrado de archivos mediante GPG.
- Configuración de autenticación SSH y uso de certificados digitales.

Instrumentos de evaluación:

- Cuaderno de prácticas.
- Actividades guiadas con entrega.
- Exposición oral sobre un caso de seguridad y privacidad.

Criterios de calificación:

- Comprensión normativa (20%)
- Implementación técnica (50%)
- Comunicación y documentación (30%)

UD4. Copias de seguridad y restauración de datos

Duración estimada: 15 horas
Competencias relacionadas: C4, C8
Resultado de aprendizaje asociado: RA4

Objetivos específicos:

- Identificar los distintos tipos de copias de seguridad.
- Configurar y programar tareas automáticas de respaldo.
- Ejecutar y verificar restauraciones efectivas.

Actividades principales:

- Configuración de copias automáticas con Cobian Backup y rsync.
- Simulación de pérdida de datos y restauración completa.
- Creación de scripts de copia en Linux con cron y bash.
- Elaboración de un plan de contingencia básico.

Instrumentos de evaluación:

- Evaluación práctica de restauración.
- Cuaderno de laboratorio.
- Informe técnico final.

Criterios de calificación:

- Correcta automatización del proceso (40%)
- Verificación funcional de las copias (40%)
- Calidad del informe técnico (20%)

UD5. Seguridad en redes de área local

Duración estimada: 25 horas
Competencias relacionadas: C1, C2, C5
Resultado de aprendizaje asociado: RA5

Objetivos específicos:

- Analizar riesgos en redes cableadas e inalámbricas.
- Configurar dispositivos de red seguros (switches, routers, cortafuegos).
- Implementar protocolos seguros y servicios cifrados.

Actividades principales:

- Escaneo de red y detección de vulnerabilidades con Nmap y Wireshark.
- Configuración de VLAN y listas de control de acceso.
- Instalación y configuración de pfSense como cortafuegos.
- Configuración de túneles VPN y autenticación segura.

Instrumentos de evaluación:

- Pruebas prácticas en laboratorio.
- Informes técnicos de configuración.
- Examen práctico final.

Criterios de calificación:

- Eficacia de la configuración de red segura (50%)
- Análisis e interpretación de resultados (30%)
- Documentación y argumentación técnica (20%)

UD6. Auditoría y proyecto final de Seguridad Informática

Duración estimada: 15 horas
Competencias relacionadas: Todas
Resultado de aprendizaje asociado: Integración de RA1–RA5

Objetivos específicos:

- Integrar los conocimientos adquiridos a lo largo del módulo.
- Planificar y ejecutar una auditoría básica de seguridad.
- Elaborar un informe profesional de vulnerabilidades y propuestas de mejora.

Actividades principales:

- Desarrollo de una auditoría práctica en entorno virtualizado (Metasploit, OpenVAS).
- Redacción del informe final de vulnerabilidades y recomendaciones.
- Presentación y defensa del proyecto en grupo.

Instrumentos de evaluación:

- Proyecto práctico final.
- Presentación oral y defensa técnica.
- Evaluación de la documentación entregada.

Criterios de calificación:

- Calidad técnica del proyecto (40%)
- Análisis crítico y justificación (30%)
- Presentación y defensa (30%)

FASE DE FORMACIÓN EN EMPRESA			
RA5. Monitorización, Detección y Respuesta (Red/Blue Team)		**40% 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	10	a)	Se han identificado vulnerabilidades en redes cableadas e inalámbricas.
Documento de evaluación FFE	5%	b)	Se han configurado cortafuegos (firewalls) y listas de control de acceso.
Documento de evaluación FFE	10	c)	Se han implantado protocolos seguros (HTTPS, SSH, VPN).
Documento de evaluación FFE	5%	d)	Se ha comprobado la efectividad de las medidas adoptadas mediante pruebas de penetración.
Documento de evaluación FFE	10%	f)	Se han documentado las actuaciones realizadas y los resultados obtenidos.
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.			

5. Evaluación del aprendizaje

La evaluación del módulo se ajustará a los principios establecidos por la LOMLOE: **continua, formativa y orientada al desarrollo competencial**.

El proceso de evaluación integrará la observación del trabajo diario, la revisión de evidencias de aprendizaje y la valoración de la autonomía técnica del alumnado.

Instrumentos de evaluación

- Observación directa del trabajo en laboratorio.
- Cuaderno de prácticas y documentación técnica.
- Pruebas teórico-prácticas individuales.
- Informes e investigaciones.
- Proyecto final y exposición.
- Autoevaluación y coevaluación entre iguales.

Ponderaciones globales

Elemento evaluado	Peso (%)
Prácticas de laboratorio	40 %
Proyecto final y auditoría	30 %
Pruebas teóricas	20 %
Participación, actitud y trabajo en equipo	10 %

Criterios de calificación

- Superación de todas las prácticas esenciales con aprovechamiento mínimo del 50 %.
- Presentación de documentación técnica clara, estructurada y verificable.
- Asistencia y participación activa en las actividades del módulo.
- En el caso de evaluación final, se aplicarán pruebas globales teórico-prácticas.

6. Anexo I – Rúbrica ampliada de evaluación por competencias

Criterio de evaluación	Competencia profesional	Excelente (9–10)	Avanzado (7–8)	Básico (5–6)	Insuficiente (<5)
Analiza vulnerabilidades y aplica medidas de seguridad.	C1, C2	Identifica todas las vulnerabilidades y aplica soluciones eficaces y documentadas.	Detecta la mayoría de vulnerabilidades con correcciones adecuadas.	Identifica parcialmente las amenazas.	No detecta ni corrige las vulnerabilidades.
Protege equipos frente a software malicioso.	C2, C3	Configura herramientas de protección completas y eficaces.	Configura parcialmente con errores menores.	Configura con ayuda.	No logra la protección del sistema.
Implementa copias de seguridad y restauración.	C4	Programa copias automáticas verificadas y documentadas.	Realiza copias funcionales sin documentación completa.	Hace copias manuales parciales.	No asegura la restauración.
Aplica medidas de seguridad en redes.	C5	Configura cortafuegos, VPN y servicios cifrados correctamente.	Aplica medidas básicas de seguridad.	Configura de manera incompleta.	No aplica medidas eficaces.
Cumple la normativa de protección de datos.	C7	Aplica la LOPDGDD correctamente y documenta su cumplimiento.	Comprende la normativa y aplica medidas básicas.	Conoce la normativa, pero sin aplicación práctica.	Desconoce o incumple la normativa.

7. Anexo II – Correspondencia entre competencias, resultados y criterios

Competencia profesional	Resultado de aprendizaje	Criterios de evaluación asociados
C1. Instalar y configurar sistemas microinformáticos.	RA1	CE1.1 – CE1.5
C2. Detectar y resolver incidencias de seguridad.	RA1, RA2	CE1.1 – CE2.5
C3. Implementar medidas de seguridad.	RA2, RA3	CE2.1 – CE3.6
C4. Realizar copias de seguridad y restauraciones.	RA4	CE4.1 – CE4.4
C5. Configurar seguridad en redes.	RA5	CE5.1 – CE5.5
C7. Cumplir la normativa legal de protección de datos.	RA3	CE3.1 – CE3.6
C8. Documentar procedimientos y elaborar informes.	Todos	Todos los criterios asociados

8. Anexo III – Proyecto final integrado

El proyecto final consiste en la **planificación, implementación y auditoría de un entorno seguro** en red local, integrando todos los conocimientos adquiridos a lo largo del módulo.

Fases del proyecto:

1. **Análisis de riesgos.** Identificación de amenazas potenciales y vulnerabilidades.
2. **Diseño de medidas de seguridad.** Configuración de sistemas operativos y redes seguras.
3. **Implementación.** Instalación de cortafuegos, antivirus, políticas de acceso y copias automáticas.
4. **Auditoría.** Ejecución de pruebas con herramientas como *Wireshark*, *Nmap* o *OpenVAS*.
5. **Informe técnico.** Documentación detallada del proceso y conclusiones.

Evaluación del proyecto:

- Aplicación de medidas de seguridad: 40 %
- Razonamiento técnico y justificación: 30 %
- Informe y presentación: 30 %