



CRITERIOS DE EVALUACIÓN  
SEGURIDAD Y ALTA DISPONIBILIDAD  
0378 – SAD

**CFGS ADMINISTRACIÓN DE SISTEMAS  
INFORMÁTICOS Y REDES**

Familia profesional de Informática y comunicaciones

IES Mutxamel - Curso 2025/26

David Alcaraz Pérez

[dm.alcarazperez@edu.gva.es](mailto:dm.alcarazperez@edu.gva.es)



Fondos Europeos



Financiado por  
la Unión Europea



**GENERALITAT  
VALENCIANA**

Conselleria de Educació, Cultura,  
Universitats y Empleo



**IES MUTXAMEL**  
Carrer Mondúber s/n  
03110 MUTXAMEL (ALACANT)  
03014551@edu.gva.es  
Tel: 965936475|Fax: 965936476  
portal.edu.gva.es/iesmutxamel



Formació Professional  
Comunitat Valenciana

## ÍNDICE

Seguridad y Alta Disponibilidad (0378 – SAD) .....	3
Criterios de evaluación .....	4
Evaluación del aprendizaje .....	6
Instrumentos de evaluación .....	6
Criterios de calificación .....	6
Criterios de recuperación .....	7

## Seguridad y Alta Disponibilidad (0378 – SAD)

### Criterios de evaluación

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

- Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos.
- Se han descrito las diferencias entre seguridad física y lógica.
- Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen.
- Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos.
- Se han adoptado políticas de contraseñas.
- Se han valorado las ventajas que supone la utilización de sistemas biométricos.
- Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información.
- Se ha reconocido la necesidad de establecer un plan integral de protección perimetral, especialmente en sistemas conectados a redes públicas.
- 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.**

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

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

### **RA4. Instala cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.**

- Se han descrito las características, tipos y funciones de los cortafuegos.
- Se han clasificado los niveles en los que se realiza el filtrado de tráfico.
- Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red.
- Se han configurado filtros en un cortafuegos a partir de un listado de reglas de filtrado.
- Se han revisado los registros de sucesos de cortafuegos, para verificar que las reglas se aplican correctamente.
- Se han probado distintas opciones para implementar cortafuegos, tanto software como hardware.
- Se han diagnosticado problemas de conectividad en los clientes provocados por los cortafuegos.
- Se ha elaborado documentación relativa a la instalación, configuración y uso de cortafuegos.

### **RA5. Instala servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.**

- Se han identificado los tipos de «proxy», sus características y funciones principales.
- Se ha instalado y configurado un servidor «proxy-cache».
- Se han configurado los métodos de autenticación en el «proxy».
- Se ha configurado un «proxy» en modo transparente.
- Se ha utilizado el servidor «proxy» para establecer restricciones de acceso Web.
- Se han solucionado problemas de acceso desde los clientes al «proxy».
- Se han realizado pruebas de funcionamiento del «proxy», monitorizando su actividad con herramientas gráficas.
- Se ha configurado un servidor «proxy» en modo inverso.
- Se ha elaborado documentación relativa a la instalación, configuración y uso de servidores «proxy».

## RA6. Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba

- Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad.
- Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema.
- Se han evaluado las posibilidades de la virtualización de sistemas para implementar soluciones de alta disponibilidad.
- Se ha implantado un servidor redundante que garantice la continuidad de servicios en casos de caída del servidor principal.
- Se ha implantado un balanceador de carga a la entrada de la red interna.
- Se han implantado sistemas de almacenamiento redundante sobre servidores y dispositivos específicos.
- Se ha evaluado la utilidad de los sistemas de «clusters» para aumentar la fiabilidad y productividad del sistema.
- Se han analizado soluciones de futuro para un sistema con demanda creciente.
- Se han esquematizado y documentado soluciones para diferentes supuestos con necesidades de alta disponibilidad.

## RA7. Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.

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

## Evaluación del aprendizaje

### Instrumentos de evaluación

Los instrumentos de evaluación son una herramienta pedagógica que detecta tanto el grado de adquisición de objetivos y competencias en los alumnos (aprendizaje) como la consecución de objetivos docentes (enseñanza), con el fin de mejorar el proceso educativo.

Para evaluar el desempeño del alumnado durante todo el curso, se utilizarán las siguientes herramientas:

- **Observación diaria.** Se tendrá en cuenta el trabajo diario que realice el alumno en el aula.
- **Exámenes de carácter teórico/práctico,** pruebas de carácter teórico, generalmente de tipo test además de exámenes prácticos en ordenador donde se llevarán a cabo tareas similares a las realizadas en clase.

### Criterios de calificación

Se evaluará el grado de aprendizaje individual respecto a los resultados de aprendizaje (RA) especificados para el módulo profesional. En cada unidad de programación se trabajará un resultado de aprendizaje. Cada RA tendrá una ponderación sobre el total del módulo, finalmente, la calificación se obtendrá de la siguiente forma:

Exámenes prácticos	Exámenes teóricos	Trabajo en clase, actitud/comportamiento
60%	30%	10%

### Criterios de recuperación

Antes de la **convocatoria ordinaria** se notificará a aquellos alumnos/as que no hayan alcanzado uno o varios de los resultados de aprendizaje establecidos y deberán realizar la recuperación de éstos en dicha convocatoria. La calificación máxima de los resultados de aprendizaje recuperados será de 5.

Si en la convocatoria ordinaria un alumno/a no obtiene una calificación positiva en todos los resultados de aprendizaje, se le convocará a una prueba en la **convocatoria extraordinaria**. Se comunicará con suficiente antelación cuáles son los resultados de aprendizaje que debe recuperar. El alumno/a podrá solicitar materiales adicionales, tareas de repaso o tutorías individuales para la preparación de la prueba de recuperación de la convocatoria extraordinaria. Del mismo modo que en la convocatoria ordinaria, la calificación máxima de los resultados de aprendizaje recuperados será de 5.