PROGRAMACIÓN DIDÁCTICA

GOBIERNO DEL PRINCIPADO DE ASTURIAS

CONSEJERÍA DE EDUCACIÓN, CULTURA Y DEPORTE

CIFP

Centro Integrado de Formación Profesional

AVILÉS

Principado de Asturias

DEPARTAMENTO DE FAMILIA PROFESIONAL

INFORMÁTICA Y COMUNICACIONES

CICLO FORMATIVO:

IFC301 CFGS ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS EN RED

MÓDULO:

0378 SEGURIDAD Y ALTA DISPONIBILIDAD

PROFESOR:

MANUEL CARLOS VARO CUBERO

ÍNDICE

1. RESULTADOS DE APRENDIZAJE Y CRITERIOS DE EVALUACIÓN
2. CONTENIDOS Y UNIDADES DE TRABAJO
3. EVALUACIÓN, CALIFICACIÓN Y GARANTÍAS DE OBJETIVIDAD
4. PROGRAMA DE RECUPERACIÓN

1. RESULTADOS DE APRENDIZAJE Y CRITERIOS DE EVALUACIÓN

Los siguientes resultados de aprendizaje y criterios de evaluación proceden del currículo y constituyen el referente directo de la evaluación.

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

Ponderación del RA: 20 % · Carga curricular orientativa: 23 h

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.

Ponderación del RA: 15 % · Carga curricular orientativa: 19 h

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 han 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.

Ponderación del RA: 15 % · Carga curricular orientativa: 19 h

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. Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.

Ponderación del RA: 15 % · Carga curricular orientativa: 19 h

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

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

Ponderación del RA: 5 % · Carga curricular orientativa: 11 h

a) Se han identificado los tipos de «proxy», sus características y funciones principales.
b) Se ha instalado y configurado un servidor «proxy-cache».
c) Se han configurado los métodos de autenticación en el «proxy».
d) Se ha configurado un «proxy» en modo transparente.
e) Se ha utilizado el servidor «proxy» para establecer restricciones de acceso Web.
f) Se han solucionado problemas de acceso desde los clientes al «proxy».
g) Se han realizado pruebas de funcionamiento del «proxy», monitorizando su actividad con herramientas gráficas.
h) Se ha configurado un servidor «proxy» en modo inverso.
i) 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.

Ponderación del RA: 20 % · Carga curricular orientativa: 23 h

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

Ponderación del RA: 10 % · Carga curricular orientativa: 14 h

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.

2. CONTENIDOS Y UNIDADES DE TRABAJO

Los contenidos básicos se organizan en siete unidades de trabajo, con una distribución horaria orientativa que suma las 128 horas curriculares del módulo. La correspondencia es deliberadamente directa entre unidad y RA para facilitar la trazabilidad de actividades, pruebas y recuperación.

UT	Unidad	RA	Horas	Momento de evaluación
UT1	Pautas y prácticas de seguridad informática	RA1	23	1.ª evaluación parcial
UT2	Implantación de mecanismos de seguridad activa	RA2	19	1.ª evaluación parcial
UT3	Legislación y normas sobre seguridad	RA7	14	1.ª evaluación parcial
UT4	Acceso remoto seguro y seguridad perimetral	RA3	19	2.ª evaluación parcial
UT5	Instalación y configuración de cortafuegos	RA4	19	2.ª evaluación parcial
UT6	Instalación y configuración de proxy	RA5	11	2.ª evaluación parcial
UT7	Implantación de soluciones de alta disponibilidad	RA6	23	2.ª evaluación parcial

UT1. Pautas y prácticas de seguridad informática

RA1 · 23 h orientativas · 1.ª evaluación parcial Fiabilidad, confidencialidad, integridad y disponibilidad; vulnerabilidades; seguridad física y lógica; contraseñas; biometría; criptografía; copias y almacenamiento; análisis forense.

UT2. Implantación de mecanismos de seguridad activa

RA2 · 19 h orientativas · 1.ª evaluación parcial

Amenazas lógicas; malware; actualización; herramientas preventivas y paliativas; cifrado, firmas y certificados; redes inalámbricas; servicios de red; IDS.

UT3. Legislación y normas sobre seguridad

RA7 · 14 h orientativas · 1.ª evaluación parcial

Protección de datos; control de acceso a datos personales; figuras legales; derechos; servicios de la sociedad de la información; normas de gestión de seguridad.

UT4. Acceso remoto seguro y seguridad perimetral

RA3 · 19 h orientativas · 2.ª evaluación parcial Perímetros y zonas de riesgo; protocolos seguros; VPN; pasarelas de acceso; autenticación remota y servidores de autenticación.

UT5. Instalación y configuración de cortafuegos

RA4 · 19 h orientativas · 2.ª evaluación parcial Tipos y funciones; filtrado; ubicación; reglas; registros; pruebas; diagnóstico y documentación.

UT6. Instalación y configuración de proxy

RA5 · 11 h orientativas · 2.ª evaluación parcial Tipos de proxy; proxy-cache; autenticación; transparente; restricciones; resolución de incidencias; monitorización; inverso; documentación.

UT7. Implantación de soluciones de alta disponibilidad

RA6 · 23 h orientativas · 2.ª evaluación parcial

Continuidad; redundancia; virtualización; servidores redundantes; balanceadores; almacenamiento redundante; clústeres; escalabilidad y documentación.

2.1. Operativización didáctica de las unidades

Las actividades descritas son orientativas y podrán adaptarse al grupo y a los recursos disponibles. No sustituyen la publicación previa de RA, CE, peso y plazos de cada actividad

evaluable.

UT / RA	Objetivo y actividades principales	Evidencia / producto esperado	Recursos y seguridad	CE / apoyo y ampliación
UT1 · RA1	Analizar riesgos y adoptar pautas seguras. Casos de vulnerabilidades, contraseñas, cifrado, copias y análisis forense básico.	Informe técnico, configuración o resolución razonada de casos.	Máquinas virtuales y datos ficticios; no se realizarán acciones sobre sistemas ajenos o redes públicas.	a-i. Guías paso a paso; ampliación sobre hardening y forense.
UT2 · RA2	Analizar amenazas y contramedidas. Laboratorio controlado de malware, actualización, certificados, Wi-Fi e IDS.	Evidencias de detección, análisis y aplicación de medidas preventivas/paliativas.	Entornos aislados, snapshots y muestras seguras/simuladas.	a-i. Listas de comprobación; ampliación con monitorización y reglas IDS.
UT3 · RA7	Interpretar normativa y trasladarla a decisiones de administración y seguridad.	Resolución de supuesto legal y matriz de obligaciones/medidas.	Textos normativos y casos anonimizados.	a-g. Plantillas de análisis; ampliación sobre SGSI/ISO 27001.
UT4 · RA3	Diseñar e implantar acceso remoto seguro, zonas de riesgo, VPN, pasarela y autenticación.	Topología, configuración funcional, pruebas y documentación.	Laboratorio virtual aislado con restauración rápida.	a-g. Configuraciones base; ampliación con autenticación centralizada.
UT5 · RA4	Planificar, configurar y diagnosticar cortafuegos y reglas de filtrado.	Política de filtrado, configuración, registros, pruebas y memoria técnica.	Red de laboratorio segmentada; pruebas solo contra equipos autorizados.	a-h. Plantillas de reglas; ampliación con alta disponibilidad de firewall.
UT6 · RA5	Implantar y comprobar proxy directo/inverso, autenticación, filtros y monitorización.	Proxy funcional con pruebas, restricciones y documentación.	Máquina virtual preconfigurada cuando sea necesario para optimizar el tiempo.	a-i. Guía base; ampliación con TLS/reverse proxy y cabeceras.
UT7 · RA6	Diseñar e implantar continuidad, redundancia, balanceo, almacenamiento y virtualización.	Arquitectura de alta disponibilidad, pruebas de fallo y documentación.	VM, balanceadores y almacenamiento simulado; snapshots para recuperación.	a-i. Escenarios progresivos; ampliación con automatización y escalado.

3. EVALUACIÓN, CALIFICACIÓN Y GARANTÍAS DE OBJETIVIDAD

Regla esencial de SADIS. Cada RA se supera mediante un bloque de actividades evaluables (50 %) y una prueba presencial (50 %). Para superar el bloque de actividades deberá haberse entregado al menos el 75 % de las actividades publicadas y obtener una calificación ponderada mínima de 5,00/10. Las actividades no entregadas computarán con 0 puntos. No se exige aprobar individualmente cada actividad. El examen del RA deberá alcanzar al menos 5,00/10. No existe compensación entre el bloque de actividades y el examen.

3.1. Referentes e instrumentos

La evaluación se realiza por resultados de aprendizaje a partir de sus criterios de evaluación. Los instrumentos ordinarios con incidencia en la calificación serán las actividades evaluables publicadas en el Aula Virtual y las pruebas presenciales. Cuando

proceda, las evidencias obtenidas en la Formación en Empresa se integrarán en la valoración de los CE correspondientes a través de los instrumentos previstos y conforme al Plan de formación individual, sin constituir un tercer bloque de calificación. Otras tareas, ejercicios, preguntas de clase o prácticas de entrenamiento tendrán carácter formativo salvo que se identifiquen expresamente como actividad evaluable.

3.2. Actividades evaluables en Aula Virtual

Cada RA podrá incluir un número variable de actividades. Se publicarán su peso en el bloque, RA y CE, condiciones de realización y plazo de entrega.

- Los pesos de las actividades de cada RA sumarán el 100 % del bloque. Las no entregadas computarán con 0 en su media ponderada.
- Para superar el bloque habrá que entregar al menos el 75 % de las actividades ordinarias y alcanzar una media ponderada mínima de 5,00/10. No se exige un 5 en cada actividad.
- Realización y seguimiento en el aula: salvo autorización expresa del profesorado, las actividades evaluables se realizarán en clase, durante las sesiones lectivas establecidas. El alumnado deberá informar al profesor del trabajo que está desarrollando y mostrar y explicar sus avances, procedimientos y resultados cuando se le requiera. La entrega final no sustituye la acreditación del proceso y de los aprendizajes exigidos.
- **Identificación de capturas de máquinas virtuales:** cuando una actividad exija capturas de pantalla de una máquina virtual, deberá aparecer de forma visible y legible el nombre de la máquina virtual, el nombre de usuario o del equipo, o una anotación o identificador personal establecido por el profesorado que permita relacionar la evidencia con el alumno o alumna. La identificación deberá formar parte del entorno capturado y no añadirse posteriormente mediante la edición de la imagen. Las capturas sin identificación suficiente no acreditarán por sí solas el trabajo realizado; el profesorado podrá solicitar su subsanación o una demostración equivalente. Si no se aporta la evidencia requerida, no se puntuará el apartado cuya realización no pueda verificarse.
- Verificación y valoración de evidencias: cuando no se haya podido comprobar suficientemente el proceso de realización de una actividad, el profesorado podrá solicitar una explicación individual, una demostración práctica, la reproducción de procedimientos o una comprobación equivalente vinculada a los RA y CE evaluados. Antes de cerrar la calificación se ofrecerá la posibilidad de acreditar los aspectos pendientes de verificación. La nota se establecerá según las evidencias de aprendizaje efectivamente demostradas y la puntuación prevista para cada apartado; los aspectos no acreditados no obtendrán puntuación. No se aplicará ninguna reducción fija por falta de seguimiento. Una actividad entregada computará para el mínimo del 75 %, salvo invalidación de autoría conforme al apartado 7.9. Se documentarán las comprobaciones relevantes y se contemplarán medidas equivalentes ante situaciones justificadas o adaptaciones autorizadas.
- Una entrega invalidada por falta de autoría personal debidamente comprobada recibirá 0 y no contará como realizada a efectos del 75 %, según el procedimiento del apartado 7.9.
- Las calificaciones válidas se conservarán durante el curso, salvo sustitución en recuperación. El cierre ordinario fija el número de actividades para el 75 %; las de recuperación no lo alterarán retroactivamente.

3.3. Pruebas presenciales

Las pruebas serán individuales y podrán incluir cuestiones teóricas, supuestos, interpretación de configuraciones, resolución de incidencias, tareas prácticas o combinaciones de estos formatos. Cuando una prueba abarque varios RA, estará dividida en bloques independientes y se obtendrá una calificación de examen diferenciada para cada RA.

Antes de cada prueba se comunicarán los RA y CE evaluados, estructura, puntuación, materiales o software permitidos. La prueba de cada RA deberá alcanzar al menos 5,00/10.

3.4. Calificación de cada RA

Solo cuando el bloque de actividades del RA esté superado -al menos el 75 % de las actividades entregadas y una calificación ponderada mínima de 5,00/10- y la prueba presencial alcance al menos 5,00/10 se calculará la calificación del resultado de aprendizaje mediante:

Calificación RA = 0,50 × bloque de actividades + 0,50 × examen presencial

Si no se alcanza el 75 % mínimo de entregas, si el bloque de actividades obtiene menos de 5,00/10 o si el examen no alcanza 5,00/10, el RA queda pendiente, aunque la media matemática resultante pudiera ser igual o superior a 5. El bloque ya superado se conservará durante el curso. Cuando quede pendiente el bloque de actividades, la recuperación se centrará en las actividades necesarias para alcanzar el mínimo de entrega y/o la calificación requerida.

Cuando un RA no pueda considerarse superado por incumplimiento de alguno de los mínimos establecidos, aunque el resultado matemático de la ponderación sea igual o superior a 5, la calificación que se consigne a efectos de registro se ajustará al procedimiento previsto en la concreción curricular, los acuerdos departamentales y las normas de evaluación del centro.

3.5. Ponderación de RA y calificación final

RA	Descripción abreviada	Peso
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.	15
RA3	Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.	15
RA4	Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.	15
RA5	Implanta servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.	5
RA6	Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.	20
RA7	Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.	10

La calificación numérica final se obtendrá mediante la media ponderada de los siete RA con los pesos anteriores, siempre que todos estén superados. No existe compensación entre RA: un resultado de aprendizaje pendiente impide la evaluación positiva del módulo.

3.6. Trazabilidad RA-CE-evidencias

No se fija de antemano una asignación permanente de cada criterio de evaluación (CE) a una actividad o examen concretos, ni una ponderación porcentual individual de los CE. La programación establece los resultados de aprendizaje (RA), sus CE y los instrumentos ordinarios de calificación: actividades evaluables y prueba presencial. Según la naturaleza del aprendizaje, podrán emplearse prácticas y configuraciones de laboratorio, pruebas de funcionamiento, informes, documentación técnica, resolución de supuestos, cuestiones teóricas, observación y demostraciones integradas en esos instrumentos.

Al diseñar cada actividad o examen, el profesorado concretará los CE que se evaluarán, las evidencias requeridas y la puntuación, y lo comunicará al alumnado antes de su realización. Mantendrá un registro docente de la correspondencia RA-CE-instrumento-evidencia y, antes de cerrar cada RA, comprobará que todos sus CE hayan sido evaluados, completando las evidencias pendientes cuando sea necesario. Un CE podrá evaluarse mediante varios instrumentos sin duplicar la valoración de una misma evidencia.

3.7. Integración de evidencias de Formación en Empresa

Las evidencias obtenidas durante la Formación en Empresa se asociarán únicamente a los RA y CE que figuren en el Plan de formación individual de cada estudiante. Su utilización no implica una asignación genérica de RA o CE a la empresa ni modifica el sistema común de calificación del módulo.

La información y valoración de la persona tutora de empresa se integrarán, cuando corresponda, con las evidencias obtenidas en el centro. No se duplicará la valoración de un mismo CE y la responsabilidad de la evaluación y calificación académica corresponderá al profesorado responsable del módulo. El sistema 50% bloque de actividades y 50 % examen se mantiene sin crear una ponderación independiente para la Formación en Empresa.

3.8. Evaluaciones parciales y finales

Primera evaluación parcial

Permite la superación acumulable de RA1, RA2 y RA7. Los RA o partes superadas se conservan durante el curso.

Segunda evaluación parcial

Permite la superación acumulable de RA3, RA4, RA5 y RA6. Se conserva cualquier RA o parte ya superada.

Primera Evaluación Final

Coincide con la tercera evaluación del curso y se destina a la evaluación de los RA o partes que permanezcan pendientes tras las evaluaciones parciales, integrando, cuando corresponda, las evidencias válidas obtenidas durante la Formación en Empresa. No se repiten RA ni bloques ya superados.

Segunda Evaluación Final

El alumnado se evalúa únicamente de los RA y, dentro de ellos, de las actividades o examen que continúen pendientes.

3.9. Autoría, uso de IA e incidencias

Las actividades deben acreditar el trabajo y dominio personal del alumnado. Podrán solicitarse archivos fuente, historial de elaboración, capturas, configuraciones, demostraciones o una breve defensa técnica. El uso de IA generativa solo será admisible en los términos expresamente autorizados y, en ese caso, deberá declararse; el alumnado responderá de comprender y justificar el resultado.

Capturas de máquinas virtuales y autoría. Cuando se soliciten evidencias mediante capturas de máquinas virtuales, estas deberán incluir una identificación visible que permita vincularlas al alumnado, conforme a lo establecido en el apartado 7.2. Esta identificación es un elemento de trazabilidad, pero no sustituye las verificaciones de autoría que el profesorado pueda considerar necesarias.

Procedimiento de verificación ante indicios de uso indebido de IA. Los programas detectores de IA podrán aportar indicios complementarios, incluido el porcentaje que señalen. Cuando existan indicios relevantes de sustitución del trabajo personal exigido, se seguirá este procedimiento:

- 1. Informe de indicios. El profesorado dejará constancia escrita de la actividad afectada, fecha, hechos observables e indicios concretos. Cuando utilice un detector de IA, identificará la herramienta y conservará el resultado, haciendo constar su valor meramente orientativo y contrastándolo con otras evidencias.
- 2. Comunicación al alumnado. Se comunicará individualmente al alumno o alumna, por los canales del centro, qué aspectos requieren aclaración y qué evidencias se pretenden comprobar. Se ofrecerá la oportunidad de aportar explicaciones, borradores, historial de trabajo u otros elementos pertinentes antes de decidir.
- 3. Comprobación de autoría. Se podrán solicitar archivos fuente, configuraciones, historial de elaboración, explicación técnica individual o demostración práctica vinculada a los RA y CE de la actividad. La comprobación será proporcionada a la tarea y tendrá en cuenta las adaptaciones o circunstancias justificadas.
- 4. Registro y decisión. El profesorado documentará las comprobaciones realizadas, las explicaciones recibidas, las evidencias valoradas y la decisión motivada. Si no queda acreditada una sustitución indebida del trabajo personal, no se aplicará la consecuencia prevista por falta de autoría y se calificarán las evidencias de aprendizaje que resulten verificables.
- 5. Comunicación de la decisión y revisión. Se notificará la decisión al alumnado por los cauces institucionales y se le informará de la posibilidad de solicitar aclaraciones, revisión y, en su caso, reclamación conforme a los procedimientos y plazos establecidos por el centro.

Solo cuando la comprobación docente motivada y documentada acredite suficientemente una sustitución indebida del trabajo personal exigido, la actividad se calificará con 0/10 y no computará como realizada a efectos del mínimo de entrega del 75 %, conforme al procedimiento del centro. Se custodiarán las evidencias y registros según las instrucciones institucionales. Las incidencias técnicas o causas justificadas podrán dar lugar a una evidencia equivalente; las irregularidades en exámenes se tramitarán conforme a las normas del centro.

3.10. Revisión y objetividad

Los criterios de evaluación y calificación serán públicos. El alumnado podrá solicitar aclaraciones y revisar actividades, pruebas y calificaciones conforme al procedimiento institucional. Las evidencias y pautas de corrección se custodiarán según las instrucciones del centro.

3.11. Comunicación al alumnado y publicidad de criterios

Al inicio del curso se facilitará en el Aula Virtual una guía con RA, CE, ponderaciones, sistema 50 % actividades/50 % examen, mínimos y 75 % de entregas, obligación general de realizar las actividades en clase y permitir su seguimiento, comprobaciones complementarias de los aprendizajes no acreditados, recuperación, revisión, procedimiento de autoría y uso de IA y seguridad de laboratorio. La calificación se basará en evidencias de aprendizaje verificadas, sin penalizaciones fijas por la falta de seguimiento.

En cada actividad o examen se comunicarán los RA y CE, evidencia esperada, peso o puntuación, materiales permitidos, plazo y procedimiento de incidencias. En las actividades se indicará expresamente cualquier excepción a la regla general de realización y seguimiento en clase y, cuando se exijan capturas de máquinas virtuales, las condiciones de identificación de dichas evidencias. No será necesario adjuntar la rúbrica íntegra, aunque el profesorado podrá utilizarla como instrumento de evaluación para justificar la calificación.

4. PROGRAMA DE RECUPERACIÓN

La recuperación se organiza por RA y por bloques. El alumnado recuperará el bloque de actividades cuando no haya alcanzado el 75 % mínimo de entregas y/o su calificación ponderada sea inferior a 5,00/10, y recuperará la prueba presencial cuando esta permanezca pendiente. Los bloques ya superados se conservan durante el curso 2026/2027.

4.1. Recuperación de actividades

La recuperación podrá consistir en entrega, subsanación o sustitución por evidencias equivalentes sobre los mismos CE, con exigencia comparable, para alcanzar el 75 % de actividades válidas y el mínimo ponderado de 5,00/10. Antes de cerrar una actividad ordinaria podrán realizarse comprobaciones complementarias sobre los aspectos cuyo aprendizaje no se haya acreditado; si estos continúan pendientes, se incluirán en el procedimiento de recuperación que corresponda. Las actividades invalidadas tras comprobar una falta de autoría no contarán como realizadas y deberán recuperarse mediante una nueva evidencia personal verificable, cuando proceda. Las actividades de recuperación se realizarán y supervisarán en clase, salvo que se autorice expresamente otra modalidad o se establezcan medidas equivalentes justificadas. Se mantendrán las notas válidas salvo sustitución expresa. Pesos, plazos y criterios se comunicarán en el Aula Virtual.

4.2. Tras las evaluaciones parciales

Los RA no superados en las evaluaciones parciales quedan pendientes para la 1.ª Evaluación Final. Se conservará cualquier bloque de actividades o examen ya superado y se recuperará exclusivamente el bloque que permanezca pendiente.

4.3. Tras la 1.ª Evaluación Final

El alumnado que mantenga aprendizajes pendientes recibirá un Plan Individual de Recuperación que identificará RA, CE y bloque o bloques pendientes. Cuando el bloque de actividades esté pendiente, se concretarán las actividades que deban entregarse, subsanarse o sustituirse para alcanzar el requisito mínimo de entrega y la calificación exigida. El plan indicará asimismo procedimiento, plazos, criterios de evaluación y recursos de apoyo. La 2.ª Evaluación Final se centrará exclusivamente en dichas evidencias pendientes.

4.4. Aprendizajes vinculados a la Formación en Empresa

Cuando algún RA o CE previsto en el Plan de formación individual no haya podido desarrollarse u observarse suficientemente en la empresa, se reajustará el plan y las evidencias necesarias se obtendrán en el centro o mediante otras actividades previstas. La recuperación se organizará conforme a los mismos criterios de evaluación y al sistema general de actividades y examen, sin atribuir a la empresa evidencias no producidas realmente.