Instrumentos y Procedimientos de Evaluación, y Criterios de Calificación

(FORMACIÓN PROFESIONAL)

Curso: 2º SMR **Módulo**: Seguridad Informática **Departamento de**: Informática y Comunicaciones

Para valorar el proceso de aprendizaje del alumnado se realizarán varias sesiones de evaluación parciales a lo largo del curso, además de la evaluación inicial y la evaluación final (dos en el caso de la Formación Profesional Básica).

Se tendrán en consideración los criterios y procedimientos de evaluación, así como los resultados de aprendizaje incluidos en las programaciones didácticas.

A- INSTRUMENTOS Y PROCEDIMIENTOS DE EVALUACIÓN:

Los procedimientos de evaluación que vamos a utilizar son los siguientes:

- **Pruebas**: escritas y orales, tanto teóricas como prácticas.
- **Actividades, prácticas y/o trabajos**: diarias en clase y en casa. Cuestionarios, formularios y tests. Supuestos teóricos y prácticos y resolución de problemas.
- **Proyectos**: trabajos personales o grupales, edición de documentos, elaboraciones multimedia, presentaciones y exposiciones orales.

Los instrumentos de evaluación que vamos a utilizar para los procedimientos de evaluación anteriores son los siguientes:

- Plantillas de corrección.
- Rúbricas.
- Guías de evaluación, escalas de evaluación y listas de control.
- Observación directa del trabajo diario y hojas de registro.

B- CRITERIOS DE CALIFICACIÓN:

La composición y aplicación de estos criterios de calificación tendrá como objetivo la concreción de cada uno de los resultados de aprendizaje establecidos en la programación.

B-1 Criterios de calificación de las evaluaciones parciales.

La calificación para las evaluaciones parciales será informativa e informará sobre los resultados de aprendizajes y los criterios de evaluación siguientes trabajados en la correspondiente evaluación..

RA1. Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.
a) Se ha valorado la importancia de mantener la información segura.
b) Se han descrito las diferencias entre seguridad física y lógica.
c) Se han definido las características de la ubicación física y condiciones ambientales de los equipos y servidores.
d) Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.
e) Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.
f) Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida.
g) Se han esquematizado las características de una política de seguridad basada en listas de control de acceso.
h) Se ha valorado la importancia de establecer una política de contraseñas.
i) Se han valorado las ventajas que supone la utilización de sistemas biométricos.
RA2. Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información.

a) Se ha interpretado la documentación técnica relativa a la política de almacenamiento.
b) Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad, entre otros).
c) Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red.
d) Se han descrito las tecnologías de almacenamiento redundante y distribuido.
e) Se han seleccionado estrategias para la realización de copias de seguridad.
f) Se ha tenido en cuenta la frecuencia y el esquema de rotación.
g) Se han realizado copias de seguridad con distintas estrategias.
h) Se han identificado las características de los medios de almacenamiento remotos y extraíbles.
i) Se han utilizado medios de almacenamiento remotos y extraíbles.
j) Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento.
RA3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.
a) Se han seguido planes de contingencia para actuar ante fallos de seguridad.
b) Se han clasificado los principales tipos de software malicioso.
c) Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades.
d) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas.
e) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso.

f) Se han aplicado técnicas de recuperación de datos.
RA4. Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.
a) Se ha identificado la necesidad de inventariar y controlar los servicios de red.
b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.
c) Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado.
d) Se han aplicado medidas para evitar la monitorización de redes cableadas.
e) Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas.
f) Se han descrito sistemas de identificación como la firma electrónica, certificado digital, entre otros.
g) Se han utilizado sistemas de identificación como la firma electrónica, certificado digital, entre otros.
h) Se ha instalado y configurado un cortafuegos en un equipo o servidor.
RA5. Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.
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 la obligación 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.

B-2 Criterios de calificación para la evaluación final.

El alumnado que no haya superado el módulo profesional en las evaluaciones parciales, podrá recuperar aquellos resultados de aprendizaje con calificación inferior a 5.00 que componen el módulo profesional. Igualmente, el alumnado que así lo desee podrá mejorar su calificación. Para ello, desde la última evaluación parcial hasta la evaluación final se llevarán a cabo los Programas de Refuerzo para la Recuperación de Aprendizajes no Adquiridos y/o Programas de Mejora de las Competencias del Módulo, según proceda.

La calificación para la evaluación final es calculada a partir de los resultados de aprendizajes mencionados en las tabla anterior.