



CRITERIOS DE EVALUACIÓN Y CALIFICACIÓN

CURSO 2017-2018

DEPARTAMENTO: [DPTO. INFORMÁTICA Y COMUNICACIONES]

CURSO: 2º CFGM SISTEMAS MICROINFORMÁTICOS Y REDES

MATERIA: [Seguridad Informática]

CRITERIOS DE EVALUACIÓN:

1. Aplicar medidas de seguridad pasiva en sistemas informáticos, describir características de entornos y relacionarlas con sus necesidades:

Se ha valorado la importancia de mantener la información segura.

Se han descrito las diferencias entre seguridad física y lógica.

Se han definido las características de la ubicación física y las condiciones ambientales de los equipos y servidores.

Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.

Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.

Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida.

Se han indicado las características de una política de seguridad basada en listas de control de acceso.

Se ha valorado la importancia de establecer una política de contraseñas.

Se han valorado las ventajas que supone la utilización de sistemas biométricos.

2. Gestionar dispositivos de almacenamiento, describir los procedimientos efectuados y aplicar técnicas para asegurar la integridad de la información:

Se ha interpretado la documentación técnica relativa a la política de almacenamiento.

Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad entre otros).

Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red.

Se han descrito las tecnologías de almacenamiento redundante y distribuido.



Se han seleccionado estrategias para la realización de copias de seguridad.

Se ha tenido en cuenta la frecuencia y el esquema de rotación.

Se han realizado copias de seguridad con distintas estrategias.

Se han identificado las características de los medios de almacenamiento remotos y extraíbles.

Se han utilizado medios de almacenamiento remotos y extraíbles.

Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento.

3. Aplicar mecanismos de seguridad activa, describir sus características y relacionarlas con las necesidades de uso del sistema informático:

Se han seguido planes de contingencia para actuar ante fallos de seguridad.

Se han clasificado los principales tipos de software malicioso.

Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades.

Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas.

Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso.

Se han aplicado técnicas de recuperación de datos.

4. Asegurar la privacidad de la información transmitida en redes inalámbricas, describir las vulnerabilidades e instalar software específico:

Se ha identificado la necesidad de inventariar y controlar los servicios de red.

Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.

Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado.

Se han aplicado medidas para evitar la monitorización de redes cableadas.

Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas.

Se han descrito y utilizado sistemas de identificación como la firma electrónica o certificado digital, entre otros.

Se ha instalado y configurado un cortafuegos en un equipo o servidor.



5. Reconocer la legislación y normativa sobre seguridad y protección de datos, y analizar las repercusiones de su incumplimiento:

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 la obligación 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.

INSTRUMENTOS DE CALIFICACIÓN:

Pruebas Objetivas

Ejercicios Prácticos y Actividades

CRITERIOS DE CALIFICACIÓN:

La valoración asignada a cada uno de los procedimientos de evaluación será la siguiente para cada evaluación:

Pruebas Objetivas: 60%

Ejercicios Prácticos y Actividades:40%

Para poder realizar la media ponderada de cada evaluación tanto Pruebas Objetivas como los ejercicios prácticos deben tener una calificación igual o superior a 4.

La calificación final del módulo será calculada como la media aritmética (sin decimales) de la obtenida en las 2 evaluaciones siempre que cada evaluación tenga una nota igual o superior a 5, en caso contrario el alumno deberá examinarse en la convocatoria extraordinaria de Junio.

PROCEDIMIENTOS PARA RECUPERAR EN LA EVALUACIÓN ORDINARIA:



Se realizará una única prueba de recuperación al finalizar las dos evaluaciones. En esta prueba el alumno tendrá que realizar la parte correspondiente a la evaluación o evaluaciones que tenga pendientes.

Consistirá en una prueba objetiva y/o la entrega de tareas no superadas de cada evaluación suspensa.

PROCEDIMIENTOS PARA RECUPERAR EN LA EVALUACIÓN EXTRAORDINARIA:

Se realizará una prueba en junio que incluirá preguntas teóricas y/o ejercicios prácticos de todos los contenidos impartidos durante el curso. Debido a la amplitud de los contenidos la duración de esta prueba podrá estar entre 2 y 6 horas.

Si el profesor así lo estima oportuno, pedirá la presentación de un boletín de actividades prácticas que se pondrá a disposición del alumno. Junto con la prueba objetiva se le entregará al alumno un pequeño cuestionario acerca de la resolución de los ejercicios del boletín, o bien se le realizará una entrevista oral, de tal forma que el profesor pueda comprobar que el autor de las soluciones es el alumno en cuestión. No se corregirá el boletín si el cuestionario no es contestado o es contestado de forma incorrecta, o bien no se supere dicha entrevista.

Para aprobar dicha convocatoria se deberán superar positivamente ambas partes por separado.

Por tanto la calificación final del módulo (en la Ev. ordinaria) si sólo consta de prueba objetiva será la nota de la dicha prueba. En el caso de que el profesor haya establecido actividades prácticas de recuperación, la calificación vendrá dada por la media ponderada de la calificación del examen final y la nota de prácticas de recuperación.

PROCEDIMIENTOS PARA MEJORAR LA CALIFICACIÓN DE LA MATERIA:

[
]

PROCEDIMIENTOS DE EVALUACIÓN EN CASO DE PÉRDIDA DE LA EVALUACIÓN CONTINUA:

[



Para aquellos alumnos que, como consecuencia de faltas de asistencia, pierdan ese derecho se les aplicará una evaluación extraordinaria por pérdida de evaluación continua para cada evaluación.

Se les evaluará mediante una prueba objetiva, que podrá ser distinta a la aplicada al alumnado que no ha perdido la posibilidad de evaluación continua, y cuya nota constituirá el 100% de la nota de la evaluación correspondiente

]