Criterios de Evaluación

SEGURIDAD INFORMÁTICA

Sistemas Microinformáticos y Redes – 2º SMR

1) Resultados de aprendizaje

1. Aplicar medidas de seguridad pasiva en sistemas informáticos, describir características de entornos y relacionarlas con sus necesidades.
2. Gestionar dispositivos de almacenamiento, describir los procedimientos efectuados y aplicar técnicas para asegurar la integridad de la información.
3. Aplicar mecanismos de seguridad activa, describir sus características y relacionarlas con las necesidades de uso del sistema informático.
4. Asegurar la privacidad de la información transmitida en redes inalámbricas, describir las vulnerabilidades e instalar software específico.
5. Reconocer la legislación y normativa sobre seguridad y protección de datos, y analizarlas repercusiones de su incumplimiento.

A. Criterios de evaluación del resultado de aprendizaje 1:

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 las condiciones ambientales delos 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 indicado 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.

B. Criterios de evaluación del resultado de aprendizaje 2:

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.

C. Criterios de evaluación del resultado de aprendizaje 3:

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.

D. Criterios de evaluación del resultado de aprendizaje 4:

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

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

E. Criterios de evaluación del resultado de aprendizaje 5:

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.

2) CALIFICACIÓN

La nota final del trimestre se obtendrá de las siguientes ponderaciones:

1) 10% Comportamiento, actitud, participación.
2) 20 % Entrega de Boletines.
3) 70% Nota Media de los exámenes.

Nota trimestre = 0,2*Boletines + 0,7*Exámenes + 0,1*Actitud

La ponderación solo se realizará cuando:

1) La nota media de los exámenes teóricos haya superado el 5.
2) Todas las actividades, boletines y exámenes prácticos sean APTOS.

La **Nota Final** de la asignatura será la media ponderada de todas y cada una de las unidades didácticas que la componen.

3) Observaciones

1) La asistencia a clase es obligatoria, aconsejable y necesaria para la superación del módulo
2) Para superar todos los resultados de aprendizaje será necesario entregar todas las actividades y realizar todos los exámenes relativos al mismo.
3) Para aprobar el módulo es necesario superar todos los resultados de aprendizaje descritos anteriormente.

4) Se calificará al alumno mediante notación numérica de 0 a 10. Una calificación por debajo de 5 indicará que no ha superado las pruebas de esa/s unidad/es didácticas.

La evaluación será continua, teniendo en cuenta la asistencia y actitud en clase, valorándose la participación en las clases que se impartan en el aula, el nivel de destreza demostrado en la realización de los ejercicios y trabajos, las aportaciones que realice y el trabajo en casa.

Para mayor información se realizarán trabajos individuales o en pequeños grupos, exposiciones, controles o pruebas individuales durante el trimestre. Estos controles o pruebas podrán realizarse sin previo aviso, para ver el nivel de trabajo diario, y serán tanto de carácter práctico como pruebas objetivas para evaluación de conceptos. El número de controles o pruebas y sus contenidos serán determinados por el profesorado. Al final de cada trimestre, se realizará un examen trimestral que abarcará todos los contenidos del mismo.

El alumno o alumna que quede demostrado que ha copiado en algún control o examen, la nota será 0 en el examen que haya copiado y el profesorado puede poner un examen especial para ese alumno o alumna en la siguiente convocatoria. Además, si hay sospecha de que el alumnado ha copiado en un control o examen, el profesorado puede realizar otro examen sin previo aviso, a parte o a todo el grupo, para determinar cuáles son los conocimientos reales del alumnado.

La materia de la asignatura es acumulativa, es decir, cada

conocimiento nuevo que se introduce se apoya o complementa a los anteriores, lo que implica que es necesario repasar continuamente conceptos ya aprendidos, lo que hace que el alumno o alumna los tenga siempre frescos y los llegue a dominar realmente. Por tanto, aunque un alumno tenga superada la materia de una parte necesitará aplicar dichos conocimientos para superar los siguientes.

El profesor podrá proponer pruebas para la recuperación de cada trimestre según el interés que demuestre el alumnado en el desarrollo de las clases.

Además, se realizará un examen de la evaluación final, al que asistirán los alumnos y alumnas que no hayan superado algún resultado de aprendizaje. En este examen el alumnado tendrá que superar todos los contenidos del módulo.

A todos los alumnos se les proporcionará información sobre su derecho a reclamar cualquier calificación obtenida, así como de los cauces y plazos que se deben seguir.

Horas de libre configuración adscritas al módulo de Seguridad Informática

Las horas de libre configuración, a efectos de evaluación, quedan adscritas al módulo de Seguridad Informática. Esto quiere decir que las horas de libre configuración y Seguridad Informática se evaluarán de forma independiente, como si fueran bloques independientes que forman parte de un único módulo, pero con una única nota. Para alcanzar la calificación positiva se habrá de superar cada uno de ellos de forma independiente. La calificación final en el módulo de Seguridad Informática será una media ponderada de ambos bloques:

- **Seguridad Informática, 60%.**
- **Las horas de libre configuración 40%.**