	PROGRAMACIÓN DIDÁCTICA **DEPARTAMENTO DE INFORMÁTICA**	**Curso:** **2022/2023** **Revisión:** **1**
Módulo: Bastionado de Redes y Sistemas **Ciclo: Curso de Especialización en Ciberseguridad**		

Índice

1. Resultados de Aprendizaje y Criterios de Evaluación 1
2. CRITERIOS DE EVALUACIÓN Y CALIFICACIÓN DEL MÓDULO 3
   1) Evaluación inicial 4
3. PROCEDIMIENTOS E INSTRUMENTOS DE EVALUACIÓN 4
   1) Instrumentos de evaluación 4
   2) Pruebas escritas 5
   3) Ejercicios prácticos 5
   4) Convocatoria ordinaria de mayo 5
   5) Convocatoria extraordinaria de junio 5
   6) Pérdida del derecho a la evaluación continua 5

Realizado por:	**Revisado por:**	**Aprobado por:**
Marta Ribas Corvinos	Equipo docente	Departamento de informática
Fecha: 7/10/2022	Fecha:	Fecha: (*La del acta de probación en el Dpto.*)

1. Resultados de Aprendizaje y Criterios de Evaluación

1. Diseña planes de securización incorporando buenas prácticas para el bastionado de sistemas y redes.
   a) Se han identificado los activos, las amenazas y vulnerabilidades de la organización.
   b) Se ha evaluado las medidas de seguridad actuales.
   c) Se ha elaborado un análisis de riesgo de la situación actual en ciberseguridad de la organización
   d) Se ha priorizado las medidas técnicas de seguridad a implantar en la organización teniendo también en cuenta los principios de la Economía Circular.

e) Se ha diseñado y elaborado un plan de medidas técnicas de seguridad a implantar en la organización, apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos de la organización.
f) Se han identificado las mejores prácticas en base a estándares, guías y políticas de securización adecuadas para el bastionado de los sistemas y redes de la organización.

2. Configura sistemas de control de acceso y autenticación de personas preservando la confidencialidad y privacidad de los datos.
   a) Se han definido los mecanismos de autenticación en base a distintos / múltiples factores (físicos, inherentes y basados en el conocimiento), existentes.
   b) Se han definido protocolos y políticas de autenticación basados en contraseñas y frases de paso, en base a las principales vulnerabilidades y tipos de ataques.
   c) Se han definido protocolos y políticas de autenticación basados en certificados digitales y tarjetas inteligentes, en base a las principales vulnerabilidades y tipos de ataques. d) Se han definido protocolos y políticas de autenticación basados en tokens, OTPs, etc., en base a las principales vulnerabilidades y tipos de ataques.
   d) Se han definido protocolos y políticas de autenticación basados en características biométricas, según las principales vulnerabilidades y tipos de ataques.

3. Administra credenciales de acceso a sistemas informáticos aplicando los requisitos de funcionamiento y seguridad establecidos.
   a) Se han identificado los tipos de credenciales más utilizados.
   b) Se han generado y utilizado diferentes certificados digitales como medio de acceso a un servidor remoto.
   c) Se ha comprobado la validez y la autenticidad de un certificado digital de un servicio web.
   d) Se han comparado certificados digitales válidos e inválidos por diferentes motivos.
   e) Se ha instalado y configurado un servidor seguro para la administración de credenciales (tipo RADIUS - Remote Access Dial In User Service)

4. Diseña redes de computadores contemplando los requisitos de seguridad.
   a) Se ha incrementado el nivel de seguridad de una red local plana segmentándola físicamente y utilizando técnicas y dispositivos de enrutamiento.
   b) Se ha optimizado una red local plana utilizando técnicas de segmentación lógica (VLANs).
   c) Se ha adaptado un segmento de una red local ya operativa utilizando técnicas de subnetting para incrementar su segmentación respetando los direccionamientos existentes.
   d) Se han configurado las medidas de seguridad adecuadas en los dispositivos que dan acceso a una red inalámbrica (routers, puntos de acceso, etc.).
   e) Se ha establecido un túnel seguro de comunicaciones entre dos sedes geográficamente separadas.

5. Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad.
   a) Se han configurado dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad.

b) Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.
c) Se han identificado comportamientos no deseados en una red a través del análisis de los registros (Logs), de un cortafuego.
d) Se han implementado contramedidas frente a comportamientos no deseados en una red.
e) Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.

6. Configura dispositivos para la instalación de sistemas informáticos minimizando las probabilidades de exposición a ataques.
   a) Se ha configurado la BIOS para incrementar la seguridad del dispositivo y su contenido minimizando las probabilidades de exposición a ataques.
   b) Se ha preparado un sistema informático para su primera instalación teniendo en cuenta las medidas de seguridad necesarias.
   c) Se ha configurado un sistema informático para que un actor malicioso no pueda alterar la secuencia de arranque con fines de acceso ilegítimo.
   d) Se ha instalado un sistema informático utilizando sus capacidades de cifrado del sistema de ficheros para evitar la extracción física de datos.
   e) Se ha particionado el sistema de ficheros del sistema informático para minimizar riesgos de seguridad.

7. Configura sistemas informáticos minimizando las probabilidades de exposición a ataques.
   a) Se han enumerado y eliminado los programas, servicios y protocolos innecesarios que hayan sido instalados por defecto en el sistema.
   b) Se han configurado las características propias del sistema informático para imposibilitar el acceso ilegítimo mediante técnicas de explotación de procesos.
   c) Se ha incrementado la seguridad del sistema de administración remoto SSH y otros.
   d) Se ha instalado y configurado un Sistema de detección de intrusos en un Host (HIDS) en el sistema informático.
   e) Se han instalado y configurado sistemas de copias de seguridad.

2. CRITERIOS DE EVALUACIÓN Y CALIFICACIÓN DEL MÓDULO

RESULTADOS DE APRENDIZAJE	CALIFICACIÓN
RA1. Diseña planes de securización incorporando buenas prácticas para el bastionado de sistemas y redes	9,09 %
RA2. Configura sistemas de control de acceso y autenticación de personas preservando la confidencialidad y privacidad de los datos	9,09 %
RA3. Administra credenciales de acceso a sistemas informáticos aplicando los requisitos de funcionamiento y seguridad establecidos	9,09 %
RA4. Diseña redes de computadores contemplando los requisitos de seguridad	18,18 %
RA5. Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad	18,18 %

RA6. Configura dispositivos para la instalación de sistemas informáticos minimizando las probabilidades de exposición a ataques	18,18 %
RA7. Configura sistemas informáticos minimizando las probabilidades de exposición a ataques	18,18 %

1) Evaluación inicial

En la primera sesión del curso se realizará un test de evaluación inicial basado en los conocimientos de sistemas operativos y redes básicos para iniciar el curso.

Debido a la procedencia del alumnado de grados superiores de programación (Desarrollo de Aplicaciones Multimedia y Desarrollo de Aplicaciones Web) o de administración de sistemas informáticos en red, se deberá realizar un repaso de conocimientos básicos para equiparar el nivel entre ambos grupos de procedencia.

Los resultados obtenidos en la evaluación inicial se tendrán en cuenta para el desarrollo del curso.

3. PROCEDIMIENTOS E INSTRUMENTOS DE EVALUACIÓN

En el procedimiento de evaluación se tendrá en cuenta tanto el grado de conocimientos adquiridos sobre los contenidos, como el grado de consecución de las actividades propuestas, valorando en todo momento el esfuerzo realizado por el alumno/a así como los razonamientos empleados.

Cuando un profesor tenga evidencias claras de que un alumno ha realizado de forma fraudulenta una actividad, calificará la citada actividad con un 0.

Adicionalmente se podrán interponer las sanciones disciplinarias que se estimen oportunas.

Si aun no existiendo evidencias, el profesor tuviera sospechas por cualquier tipo de motivo de que un alumno ha realizado cualquier actividad con métodos fraudulentos, podrá realizar -previa consulta con el departamento- una nueva prueba de contraste al efecto de comprobar que el alumno realmente es competente para realizar esa tarea. Dicha prueba de competencia podrá realizarse por cualquier medio, incluyendo la entrevista oral. En los casos en que no quede registro del resultado de la prueba, se requerirá la presencia de otro profesor habilitado para la impartición del módulo. Si se comprueba que el alumno no es competente para realizar la tarea, la evaluación de la misma será un 0.

1) Instrumentos de evaluación

Como quiera que se pretende dar una formación integral de nuestros alumnos, en las calificaciones de la nota de **exámenes** y la nota de **prácticas** se tendrá en cuenta la expresión precisa y correcta haciendo especial mención en la limpieza, orden, sintaxis y semántica de informes, proyectos y cuántos documentos sean requeridos al alumno, no obstante si el profesor considera un trabajo de una pésima presentación, éste no será evaluado.

La evaluación se realizará mediante examen teórico/práctico y actividades de entrega obligatoria a través de la plataforma Moodle.

La calificación obtenida por cada alumno en cada trimestre resultará de la ponderación las dos siguientes notas:

- **Nota de conocimientos:** proviene de las pruebas objetivas de contenidos y cualquier otro tipo de actividad evaluable realizada en el trimestre no englobada en la nota de prácticas.
- **Nota de prácticas:** proviene de las tareas evaluables realizadas en el trimestre.

En cada una de las evaluaciones se informará al alumno del peso de la nota de prácticas, pudiendo incluso especificar la ponderación individual de cada una de las actividades en función de los criterios de evaluación que abarque.

Si en alguna de las evaluaciones finalmente no se realizasen prácticas, la nota de la evaluación podría corresponder en su totalidad a la nota de conocimientos

2) Pruebas escritas

En la primera evaluación habrá un examen teórico / práctico calificado sobre 10 puntos.

En la segunda evaluación habrá un examen teórico / práctico calificado sobre 10 puntos.

En la tercera evaluación habrá un examen teórico / práctico calificado sobre 10 puntos.

No habrá examen de recuperación de cada una de las evaluaciones hasta la convocatoria ordinaria de mayo.

3) Ejercicios prácticos

A lo largo del curso se podrán desarrollar prácticas de refuerzo de los contenidos expuestos en clase.

4) Convocatoria ordinaria de mayo

En esta convocatoria el alumno tendrá la oportunidad de recuperar criterios de evaluación no superados. En caso de tener mínimos no superados deberá hacer un examen que comprenderá todos los contenidos del curso.

5) Convocatoria extraordinaria de junio

El alumno que haya suspendido la convocatoria ordinaria de marzo podrá presentarse a este examen para superar el módulo. En ningún caso se guardarán contenidos superados para quitar materia del examen de convocatoria extraordinaria.

El examen teórico / práctico versará sobre los contenidos de todo el curso y deberá obtener una calificación de 5 puntos para superar el módulo

6) Pérdida del derecho a la evaluación continua

El número de horas cuya falta conlleva la pérdida del derecho a evaluación continua está establecido en el 15% de las horas del módulo. Es decir, 26 horas.

La forma de calificación con pérdida de evaluación continua consistirá en una prueba teórico / práctica en la convocatoria ordinaria de marzo en el que se evaluarán todos los criterios de evaluación del módulo. Para superar el módulo deberá obtener una calificación igual o superior a 5.