**Programación didáctica del módulo: Bastionado de Redes y Sistemas**

**Ciclo formativo: *Curso de especialización de formación profesional en ciberseguridad en entornos de las tecnologías de la información***

**Curso: 2023/2024**

**Profesora: *Marta Hernández Corral***

**Índice**

1. Criterios de evaluación 3

2. Criterios de calificación 5

3. Recuperación 6

# 

## Criterios de evaluación

Resultados de aprendizaje y criterios de evaluación.

**1. Diseña planes de securización incorporando buenas prácticas para el bastionado de sistemas y redes.**

Criterios de evaluación:

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.**

Criterios de evaluación:

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.

e) 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.**

Criterios de evaluación:

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.**

Criterios de evaluación:

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.**

Criterios de evaluación:

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.**

Criterios de evaluación:

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.**

Criterios de evaluación:

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.

## Criterios de calificación

Dado el carácter práctico de la Formación Profesional, se establece una calificación mixta entre los contenidos evaluados en proyectos y en los exámenes.

En cada una de las evaluaciones se calificarán los siguientes conceptos:

* Las **actividades, prácticas o proyectos** de enseñanza-aprendizaje: **40% de la nota**.
* Un **examen escrito** con contenido práctico: **60% de la nota**.

Sin embargo, para superar cada evaluación es necesario:

* Haber obtenido **al menos un 5** en cada uno los **exámenes** escritos.
* Haber obtenido un **5 de media** en las diferentes **actividades** de enseñanza-aprendizaje.
* No haber perdido el derecho a la evaluación continua.
* Que la actitud hacia el profesor y los compañeros sea correcta.

**No se considera la evaluación superada si no se cumplen los dos criterios anteriores.**

|  |
| --- |
| **El alumno deberá superar cada una de las evaluaciones del curso. La nota final del módulo corresponde a la media aritmética de la nota obtenida en las evaluaciones, en el caso de que todas ellas estén aprobadas.**  **Si el alumno no supera una o varias evaluaciones, la nota final será de suspenso.** |

Los alumnos que, después de la primera convocatoria tengan el módulo no superado, accederán a la segunda convocatoria de cada curso académico y tendrán que realizar una prueba evaluación del módulo en las mismas condiciones que en la primera convocatoria. No obstante, si el alumno no se presenta a la prueba de evaluación, no superará el módulo, y se entenderá que el alumno renuncia a la convocatoria, sin necesidad de haberlo solicitado previamente.

## Recuperación

Si un alumno no supera una o varias evaluaciones, deberá recuperar las evaluaciones no superadas en el examen final de recuperación que se realizará en la primera convocatoria ordinaria.

En el examen final de la primera convocatoria ordinaria, el alumno deberá recuperar **únicamente** aquellas evaluaciones no superadas. En el caso de no recuperar las evaluaciones suspensas, la calificación final será de suspenso.

Para poder realizar este examen es necesario haber presentado todos los trabajos prácticos solicitados por el profesor a lo largo de todo el curso y tener una calificación de 5 en estos.

**Acceso a la segunda convocatoria ordinaria**

Los alumnos que, después de la primera convocatoria tengan módulos no superados, accederán a la segunda convocatoria de cada curso académico. No obstante, si el alumno no se presenta a la prueba de evaluación preparada por los profesores para la segunda convocatoria, se entenderá que el alumno renuncia a la misma, sin necesidad de haberlo solicitado previamente.

El acceso a la segunda convocatoria ordinaria se realizará independientemente del tipo de matrícula del alumno (ordinaria o modular).

Antes de la realización de la segunda convocatoria ordinaria si el profesor lo considera oportuno se programarán ejercicios de recuperación que se deberán de entregar en la fecha establecida por cada profesor.

El examen de la segunda convocatoria ordinaria incluirá solo aquellos contenidos que no se hayan conseguido superar en la primera.

La segunda convocatoria ordinaria se realizará en el mes de junio.

* + 1. Planificación de las actividades de recuperación de los módulos no superados

Dado que se utiliza la plataforma Moodle a lo largo del módulo/asignatura, los alumnos tienen a su disposición el conjunto de ejercicios que les pueden servir de refuerzo para superar el examen de la segunda convocatoria ordinaria

En el caso de aquellos alumnos que hayan promocionado a 2º y tengan este módulo no superado, se creará un curso en la plataforma Moodle de la junta, donde el profesor proporciona materiales, así como ejercicios y tareas que deberán realizar los alumnos. La resolución de dudas se realizará utilizando el correo electrónico.

Se realizará una prueba final por cada una de las convocatorias ordinarias, esta prueba supondrá el 100% de la calificación, estado está comprendida entre 1-10. El alumno deberá obtener una calificación final igual o superior a 5 sobre 10 para superar el módulo.