EXTRACTO DE PROGRAMACIÓN DOCENTE

GOBIERNO DEL PRINCIPADO DE ASTURIAS

CONSEJERÍA DE EDUCACIÓN, CULTURA Y DEPORTE

CIFP

Centro Integrado de Formación Profesional

AVILÉS

Principado de Asturias

DEPARTAMENTO DE FAMILIA PROFESIONAL:

INFORMÁTICA Y COMUNICACIONES

CICLO FORMATIVO:

IFC401 – CURSO DE ESPECIALIZACIÓN EN CIBERSEGURIDAD EN ENTORNOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

MÓDULO FORMATIVO:

5022– BASTIONADO DE REDES Y SISTEMAS

DOCENTE:

LUIS MANUEL ALVAREZ MARTINEZ

Índice de contenidos

1. Contenidos 3

Unidad de trabajo 0: Escenario Wargames. 3

Unidad de trabajo 1: Introducción al bastionado de redes y sistemas. Planes de securización. 3

Unidad de trabajo 2: Copias de seguridad 3

Unidad de trabajo 3: Contraseñas 3

Unidad de trabajo 4: Actualizaciones 4

Unidad de trabajo 5: Seguridad de red 4

Unidad de trabajo 6: Bastionado de sistemas 6

Unidad de trabajo 7: Control de acceso 7

Unidad de trabajo 8: Gestión de logs 7

2. Evaluación 7

2.1. Criterios de evaluación 8

2.2. Procedimientos e instrumentos de evaluación 8

Principios generales 8

Métodos específicos 8

2.3. Criterios de calificación y ponderación 9

2.4. Segunda Evaluación final de junio 10

2.5. Ponderación de resultados de aprendizaje 10

2.6. Jerarquía Documental y Condiciones de Realización de las tareas 10

3. Actividades de recuperación 12

3.1. Actividades de recuperación del primer cuatrimestre 12

3.2. Programas de recuperación de módulos no superados 12

4. Mínimos exigibles 13

1. Contenidos

. Los contenidos se desarrollan en base a los dispuestos por el Real Decreto 479/2020. Se enumeran a continuación enmarcados en las unidades didácticas que los comprenden.

Unidad de trabajo 0: Escenario Wargames.

Actividades

Acceso a sistemas del escenario.

Acceso mediante conexión vpn al escenario.

Unidad de trabajo 1: Introducción al bastionado de redes y sistemas. Planes de securización.

Contenidos

Diseño de planes de securización:

- Análisis de riesgos.
- Principios de la Economía Circular en la Industria 4.0.
- Plan de medidas técnicas de seguridad.
- Políticas de securización más habituales.
- Guías de buenas prácticas para la securización de sistemas y redes.
- Estándares de securización de sistemas y redes.
- Caracterización de procedimientos, instrucciones y recomendaciones.
- Niveles, escalados y protocolos de atención a incidencias.

Actividades

Identificación de activos.

Unidad de trabajo 2: Copias de seguridad

Contenidos

Configuración de los sistemas informáticos:

- Sistemas de copias de seguridad.

Actividades

Configuración de servicio de backup con Veeam Backup *

Unidad de trabajo 3: Contraseñas

Contenidos

Configuración de sistemas de control de acceso y autenticación de personas:

- − Mecanismos de autenticación. Tipos de factores.
- − Autenticación basada en distintas técnicas:

Actividades

Gestor de contraseñas*

Investigar directivas de contraseña actuales

Definir e implementar directiva de dominio de contraseñas *

Implementar directiva local de contraseñas en sistemas Linux *

Unidad de trabajo 4: Actualizaciones

Contenidos

Configuración de los sistemas informáticos:

- Configuración de actualizaciones y parches automáticos.

Actividades

Investigar directivas de actualización

Configuración de actualizaciones de sistemas Windows mediante GPO de dominio *

Configuración de actualizaciones del sistema Linux *

Redimensionado de discos de hipervisores

Actualizaciones de hosts esxi

Actualizaciones de vcenter

Actualización de router pfsense

Unidad de trabajo 5: Seguridad de red

Contenidos

Diseño de redes de computadores seguras:

- Segmentación de redes.
- Subnetting.
- Redes virtuales (VLANs).
- Zona desmilitarizada (DMZ).
- Seguridad en redes inalámbricas (WPA2, WPA3, etc.).

- Protocolos de red seguros (IPSec, etc.).

Configuración de dispositivos y sistemas informáticos:

- Seguridad perimetral. Firewalls de Próxima Generación.
- Seguridad de portales y aplicativos web. Soluciones WAF (Web Application Firewall).
- Seguridad del puesto de trabajo y endpoint fijo y móvil. AntiAPT, antimalware.
- Seguridad de entornos cloud. Soluciones CASB.
- Seguridad del correo electrónico
- Soluciones DLP (Data Loss Prevention)
- Herramientas de almacenamiento de logs.
- Protección ante ataques de denegación de servicio distribuido (DDoS).
- Configuración segura de cortafuegos, enrutadores y proxies.
- Redes privadas virtuales (VPNs), y túneles (protocolo IPSec).
- Monitorización de sistemas y dispositivos.
- Herramientas de monitorización (IDS, IPS).
- SIEMs (Gestores de Eventos e Información de Seguridad).
- Soluciones de Centros de Operación de Red, y Centros de Seguridad de Red:
- NOCs y SOCs.

Actividades

Grupos de interfaces y alias. Habilitar tráfico DNS *

Reglas de cortafuegos (1) - aislamiento de DMZ *

Reglas de cortafuegos (2) - eliminar reglas "permit any any" *

Segmentación de red interna. Rediseño de red *

Configuración de servicio dhcp para migraciones *

Migración de máquinas a nuevas redes *

Instalación y configuración básica de pfBlockerNG *

Filtrado IPv4 básico *

Creación de reglas manuales vs reglas automáticas *

Geolocalización de direcciones IP. Bloqueo de determinadas regiones

Geolocalización de direcciones IP. Creación de feeds con formato GeoIP

Creación de feeds con formato whois

Configuración de infraestructura DNS

Configuración de DNSBL

Filtrado por categorías DNSBL

Cierre del escenario DNSBL

Configuración inicial de snort *

Reconocimiento de aplicaciones en snort con OpenAppID

Unidad de trabajo 6: Bastionado de sistemas

Contenidos

Configuración de dispositivos para la instalación de sistemas informáticos:

- Precauciones previas a la instalación de un sistema informático: aislamiento, configuración del control de acceso a la BIOS, bloqueo del orden de arranque de los dispositivos, entre otros.
- Seguridad en el arranque del sistema informático, configuración del arranque seguro.
- Seguridad de los sistemas de ficheros, cifrado, particionado, entre otros.

Configuración de los sistemas informáticos:

- Reducción del número de servicios, Telnet, RSSH, TFTP, entre otros.
- Hardening de procesos (eliminación de información de depuración en caso de errores, aleatorización de la memoria virtual para evitar exploits, etc.).
- Eliminación de protocolos de red innecesarios (ICMP, entre otros).
- Securización de los sistemas de administración remota.
- Sistemas de prevención y protección frente a virus e intrusiones (antivirus, HIDS, etc.).
- Configuración de actualizaciones y parches automáticos.
- Sistemas de copias de seguridad.
- Shadow IT y políticas de seguridad en entornos SaaS.

Actividades

Configuración de arranque seguro en Linux *

Cortafuegos Linux (host-based firewall) *

Configuración de red segura en Linux

Configuración de servicio ssh

Bastionado AD mediante GPO *

Implementación del ENS en dominio Active Directory

Unidad de trabajo 7: Control de acceso

Contenidos

Administración de credenciales de acceso a sistemas informáticos:

- Gestión de credenciales.
- Infraestructuras de Clave Pública (PKI).
- Acceso por medio de Firma electrónica.
- Gestión de accesos. Sistemas NAC (Network Access Control, Sistemas de Gestión de Acceso a la Red).
- Gestión de cuentas privilegiadas.
- Protocolos RADIUS y TACACS, servicio KERBEROS, entre otros.

Actividades

Acceso restringido a equipos mediante GPO *

Configuración de estación de trabajo para administración

Servicio vpn para acceso a red interna-Conexión a servicio LDAP *

Unidad de trabajo 8: Gestión de logs

Contenidos

Configuración de dispositivos y sistemas informáticos:

- Herramientas de almacenamiento de logs.
- SIEMs (Gestores de Eventos e Información de Seguridad).

Actividades

Registros DNS para configuración de hora por NTP

Sincronizar sistemas Linux mediante NTP *

Sincronizar sistemas Windows mediante NTP *

Sincronizar hipervisores y vcenter

Servicio horario local en router pfsense

Reglas de cortafuegos para servicio NTP

2. Evaluación

Los siguientes apartados recogen los distintos aspectos de la evaluación.

2.1. Criterios de evaluación

Son criterios de evaluación a tener en consideración todos los detallados previamente. Las capacidades personales y sociales podrán ser evaluadas como parte de otras actividades que integren los mencionados criterios.

2.2. Procedimientos e instrumentos de evaluación

Principios generales

El proceso de evaluación del aprendizaje programado debe atender a los siguientes puntos:

- En el desarrollo de las unidades de trabajo en que se divide el módulo, se realizará un proceso de **evaluación continua**.
- La evaluación continua, dentro de cada unidad de trabajo, se realiza valorando la participación del alumno en la clase, los trabajos y actividades, tanto individuales como en grupo, y la resolución de ejercicios y cuestionarios que en cada caso se realicen.
- Los criterios de evaluación específicos de cada unidad de trabajo han sido mostrados previamente junto con la descripción de sus contenidos.

Métodos específicos

En cada una de las unidades de trabajo enumeradas en la programación se realizan las siguientes actividades de evaluación:

- **Exámenes**: Cuestionario tipo **test**: Se realiza un **cuestionario en cada evaluación**. La nota mínima para superar el cuestionario es de 5.

- Trabajos prácticos:

  Se plantean principalmente **tareas de tres tipos**:

  - **DOC**: Elaboración de documentación.
  - **LAB**: Laboratorios, trabajo sobre los sistemas del escenario sobre aspectos puntuales.
  - **PRJ**: Proyectos, trabajos de mayor entidad que los laboratorios que no solamente se centran en un aspecto concreto, sino que intervendrán en ellos distintos aspectos tratados en diversas unidades de trabajo.

  Estas tareas se evaluarán de la siguiente manera:

  DOC: Se entregará la documentación elaborada.

  LAB: Se solicitará una evidencia de que se ha realizado el trabajo planteado en el laboratorio. Normalmente consistirá en una o varias imágenes, o uno o varios archivos de configuración.

PRJ: Entregables especificados en el proyecto.

2.3. Criterios de calificación y ponderación

Siguiendo el proceso de evaluación descrito, la calificación de los alumnos para cada evaluación puede concretarse a través de la suma de dos componentes, ambas pruebas objetivas: **exámenes (20%) y trabajos prácticos (80%)**.

a) Exámenes: Resolución de cuestionarios de tipo test. Cada una de estas pruebas se valorará de 0 a 10 considerándose aprobada si el alumno obtiene una valoración igual o superior a 5, **descontando las preguntas contestadas incorrectamente en proporción de -1/3 de la puntuación otorgada a las preguntas contestadas correctamente.**

b) **Trabajos prácticos**: Existen dos formas de calificación:

- Para tareas de documentación o laboratorios sencillos, se utilizará la forma de calificación consistente en tres niveles de corrección: **no satisfactorio, satisfactorio y supera lo esperado**. Al término de la evaluación se totalizarán el número de trabajos realizados de forma satisfactoria.

  El nivel «no satisfactorio» indica que no se alcanzan los criterios evaluados; «satisfactorio», que se alcanzan en grado suficiente; y «supera lo esperado», que se alcanzan con mayor autonomía, calidad técnica y capacidad de justificación.

- Para documentaciones y laboratorios más complejos, y siempre en el caso de los **proyectos**, cada prueba se valorará de 0 a 10 en función de la:
  - Calidad de los trabajos.
  - Autonomía en la realización.

Si a lo largo del periodo de evaluación se hubieran realizado varias de estas pruebas se calculará la media aritmética entre ellas, siempre y cuando el alumno haya superado los contenidos mínimos exigibles para aprobar cada una de ellas. Esta media aritmética será ponderada en función de la importancia dada a cada ejercicio.

En cualquier caso, tener en cuenta los siguientes criterios:

- La entrega de los trabajos individuales es imprescindible para la superación del módulo.

- Dicha entrega ha de realizarse en el plazo marcado por el profesor para ello.

- **Originalidad de los trabajos**: se evaluará negativamente todo trabajo que haya sido total o parcialmente copiado entre alumnos. La evaluación negativa afectará a todos los alumnos implicados.

- Sobre los exámenes: se realizarán uno por evaluación. En la segunda evaluación final de junio se repetirán los exámenes de ambas evaluaciones.

2.4. Segunda Evaluación final de junio

Para el alumnado que no supere el módulo profesional en la primera evaluación final se realizará una **segunda evaluación final (finales de junio)**. Durante el periodo comprendido entre ambas evaluaciones finales se desarrollarán las actividades de refuerzo destinadas a superar el módulo en la segunda evaluación final. La docencia impartida entre la primera evaluación final y la segunda estará dedicada a que el alumnado que no haya superado el módulo en la primera evaluación final pueda afianzar sus conocimientos y afrontar con garantías de éxito la segunda evaluación final.

2.5. Ponderación de resultados de aprendizaje

Es necesario alcanzar todos los Resultados de Aprendizaje para poder superar el módulo profesional. Los diferentes RAs tendrán una ponderación diferente a la hora de conformar las calificaciones de las diferentes evaluaciones y de la calificación final del módulo.

En la siguiente tabla, se indica que todos los RA son exigidos para poder superar el módulo profesional y su ponderación para la nota final.

R.A.	Mínimo	Peso R.A. en la nota final
RA1	SI	15%
RA2	SI	10%
RA3	SI	10%
RA4	SI	15%
RA5	SI	20%
RA6	SI	10%
RA7	SI	20%

Los exámenes y trabajos prácticos constituyen instrumentos para obtener evidencias de los criterios de evaluación vinculados a cada resultado de aprendizaje. El reparto del 20 % correspondiente a cuestionarios y del 80 % correspondiente a trabajos prácticos se aplicará sobre las evidencias disponibles para cada RA. La calificación final se obtendrá aplicando la ponderación de los resultados de aprendizaje establecida en esta programación, siempre que todos hayan sido alcanzados.

Cuando un RA no disponga de prueba escrita específica, su calificación procederá íntegramente de las evidencias prácticas vinculadas a sus criterios de evaluación.

2.6. Jerarquía Documental y Condiciones de Realización de las tareas

Los **requisitos** que debe cumplir la implementación de las tareas prácticas son los **indicados en el enunciado de cada tarea**. Esta es la fuente primaria que debemos usar para determinar qué **parámetros o configuraciones específicas** se deben aplicar. Esto implica también determinar si las configuraciones realizadas se consideran correctas y, por lo tanto, evaluadas positivamente.

En este sentido, el enunciado funciona exactamente como el **contrato** (o "**pliego de condiciones**") que establece un cliente con un proveedor de servicios de TI, ya que es el

documento de referencia al que hay que acudir en caso de discrepancia entre ambas partes sobre lo que el proveedor tiene o no tiene que hacer.

Además de este documento, se facilitarán al alumno diversas **ayudas** sobre aspectos concretos de configuración de cada tarea. Estas ayudas pueden ajustarse en mayor o menor medida a los requisitos específicos expuestos en el enunciado, pudiendo mostrar configuraciones de ejemplo (nombres de host, direcciones IP, tamaños de disco, etc.) que no son exactamente los indicados en los requisitos del enunciado, a pesar de que el proceso general mostrado en la ayuda sí sea perfectamente útil para lograr la configuración requerida. Por lo tanto, debemos adaptar siempre los procedimientos de las guías a los requisitos específicos de nuestra tarea.

Tanto el **enunciado** principalmente como los archivos de ayuda proporcionados constituyen la **fuente de información esencial para la realización de cada tarea.** Deben ser leídos con calma, analizados y entendidos, y ser consultados de continuo durante todo el desarrollo para asegurar el cumplimiento estricto de los requisitos.

Teniendo en cuenta la **prevalencia de esta documentación específica**, podemos usar herramientas complementarias, incluidas **herramientas de Inteligencia Artificial (IA)**, que nos ayuden en el desarrollo de las tareas, atendiendo siempre a las directrices y normas específicas que el profesor establezca sobre su uso. No obstante, es fundamental entender que cualquier contenido, solución o código generado mediante IA debe ser asimilado, comprendido y totalmente "hecho propio" por el alumno. Si se emplea IA para escribir scripts o configuraciones, el alumno debe estar preparado para explicar, justificar y defender detalladamente dicho trabajo ante el profesor. Esta comprobación servirá para certificar que se ha investigado y entendido la solución implementada, garantizando que no se trata de un mero proceso de "copiar y pegar" sin criterio.

3. Actividades de recuperación

Los siguientes apartados detallan los distintos tipos de actividades de recuperación.

3.1. Actividades de recuperación del primer cuatrimestre

Este punto se refiere a las actividades que realizarán los alumnos que obtengan calificación negativa en la evaluación parcial intermedia de febrero.

Al tratarse de un sistema de evaluación totalmente continua, en el cual al final del curso se emplean todos los contenidos que se han ido desarrollando durante el curso en el desarrollo de la práctica final, no es necesaria la realización de actividades específicas de recuperación tras el primer cuatrimestre. El alumno tendrá la oportunidad de recuperar en el segundo cuatrimestre todas las evaluaciones con calificación negativa por medio de:

- Repetición de todos los exámenes de tipo test con calificación negativa
- Realización de los proyectos propuestos durante el curso, y su documentación asociada.

En el caso de los **cuestionarios de tipo test**, se podrán **repetir** en la segunda evaluación final de junio.

3.2. Programas de recuperación de módulos no superados

El alumnado que no haya superado el módulo en la evaluación ordinaria podrá recuperarlo de cara a la sesión de segunda evaluación final (típicamente, a finales del mes de junio).

Tras la evaluación ordinaria se le proporcionará al alumno un **programa de recuperación del módulo no superado**.

.

4. Mínimos exigibles

Son mínimos exigibles todos los criterios de evaluación detallados en esta programación.

Se consideran contenidos mínimos los indicados con un asterisco (*) en esta programación.