PPF: PRUEBA PRÁCTICA FINAL			
Denominación del curso	IFCT0109. Seguridad Informática	**Código curso:**	23-38/002065
Denominación del MF/ UF	MF0486_3– Seguridad en equipos informáticos	**Fecha:**	07/08/2024
		Duración:	180 minutos
Nombre Docente Examinador	Benito Manuel González Rodríguez	**Firma Docente**	
Nombre y apellido del alumno/a **DNI**		**Firma Alumno**	
		Nota Obtenida	

INTRUCCIONES PARA EL/LA ALUMNO/A

⇨ **DESCRIPCIÓN GENERAL DE LA PRÁCTICA:**

Esta actividad evaluable consiste en cuatro apartados. En el primero se trabaja con las amenazas y riesgos. En la segunda se trabaja con contramedidas. En la tercera se trata con sistemas de autenticación segura y en la cuarta se utilizarán reglas de filtrado de un firewall.

⇨ **INSTRUCCIONES ESPECÍFICAS:**

La actividad consta de 4 apartados.

1. Una empresa proporciona alojamiento de páginas web, con un sistema de información valorado en 250.000 €. Un análisis de riesgos revela que hay dos amenazas:
   1. Un fallo del suministro eléctrico, caracterizado por:
      - Impacto o daño = 10.000 €
      - Probabilidad de ocurrencia de la amenaza= 0. 1
   2. Un ataque dirigido desde internet, caracterizado por:
      Impacto o daño =500.000 €
      Probabilidad de ocurrencia de la amenaza= 0.005

   El modelo de seguridad de la empresa tiene el criterio de *optimizar la inversión concentrando los recursos en eliminar la mayor amenaza, y asumir el riesgo de las amenazas menores*.

   Se pide que:
   a. **Se cuantifique el riesgo de cada amenaza.**
   b. **Se calcule el presupuesto en seguridad que resultaría justificado invertir.**
   c. **Se calcule el riesgo que asume la empresa tras la inversión.**

2. En una empresa ocurren muchos incidentes de seguridad; algunos son de pequeña importancia, como las frecuentes interrupciones en la conexión a internet, y otros son más críticos, como las paradas del sistema durante jornadas completas, debido a errores en los servidores.

   También se producen fugas de información, pequeños hurtos de periféricos, y otros accesorios. La empresa también es consciente del incumplimiento de alguna ley referente a la información.

La Dirección expone la situación, y pide que se proponga un plan de acción para corregir todos esos problemas.

Se pide:

Resumir brevemente las acciones a realizar, dando al menos una justificación de las mismas.

3. La empresa dispone de una cantidad elevada de personal que trabaja fuera de la empresa, en las instalaciones del cliente, por amplios periodos de tiempo.
   Los trabajadores usan un portátil con lector de huella para conectarse a la red de la empresa. Cuando los trabajadores cambian de cliente, se tienen que intercambiar los portátiles, para poder usar las aplicaciones apropiadas, y es práctica común decir a otros la contraseña propia, de manera que unos usuarios acceden con las credenciales de otros.

   Se pide:

   Describe un sistema de autenticación fuerte que mejore la seguridad del sistema.

4. Una empresa dispone de un servidor web y de un servidor de correo electrónico, y ambos comparten la IP pública 15.15.15.15.
   El servidor web debe ser accesible desde el exterior, empleando el protocolo HTTPS.
   El servidor de correo debe poder recibir el correo que le envían otros servidores externos, así como enviar correo (tiene la dirección IP privada 192.168.100.20).
   Además, se permite que los usuarios de la red privada (con rango de red 192.168.100.0/24) puedan navegar libremente por internet.

   Se pide:

   Configure las reglas de acceso en el firewall perimetral.

Protocolo (TCP/UDP)	Puerto	IP Origen	IP Destino	Acción

Nota. Los servicios, puertos y protocolos a utilizar son los siguientes:

Servicio	Protocolo	Puerto
Navegación web	HTTP	80 (TCP)
Navegación web segura	HTTPS	443 (TCP)
Envío de correo	SMTP	25 (TCP)

Elaborar un documento con la respuesta a los mismos

⇨ **EQUIPO Y MATERIAL:**

En el aula homologada Ordenador con conexión a Internet, navegador y procesador de textos.

⇨ **DURACIÓN DE LA PRUEBA:**

El tiempo estimado de la prueba es de 180 minutos