SUPUESTO 2 (60 puntos)

La puntuación máxima de este ejercicio será de 60 puntos. De ellos, hasta 10 puntos se asignarán a la valoración de la capacidad del aspirante para aplicar los conocimientos en la materia, la coherencia y sistemática de la exposición, la capacidad de análisis y la calidad de la expresión escrita.

Durante una mañana laboral, el Servicio de Informática del Ayuntamiento de Aldaia recibe varias alertas del sistema de monitorización y del firewall perimetral:

1. Tres cuentas de usuario muestran múltiples intentos fallidos de autenticación en un intervalo de pocos minutos, desde direcciones IP externas.
2. El firewall registra intentos de conexión entrante hacia el puerto 3389/TCP (RDP) dirigidos a dos servidores internos.
3. Varios empleados de distintas áreas municipales informan de haber recibido un correo sospechoso con asunto "Actualización urgente de su certificado digital" que incluye un enlace externo acortado.
4. Uno de los equipos de urbanismo presenta un comportamiento anómalo:
    - alto consumo de CPU,
    - lentitud extrema,
    - y conexiones salientes hacia dominios no habituales.
5. El CPD mantiene todos los servicios críticos en funcionamiento, pero se sospecha que podría estar iniciándose un intento coordinado de intrusión.

Se pide:

1. Describir el procedimiento técnico inmediato de contención y análisis ante este escenario. (8 puntos)
2. Indicar las medidas para verificar, aislar y analizar el equipo afectado (8 puntos)
3. Exponer las acciones en el firewall, monitorización y directorio activo para mitigar accesos no autorizados. (8 puntos)
4. Detallar el protocolo ante correos sospechosos y riesgo de phishing. (8 puntos)
5. Clasificar el incidente según ENS/CCN-STIC y justificar si se considera un ciberincidente. (5 puntos)
6. Especificar cuándo y cómo debe notificarse. (5 puntos)
7. Proponer medidas adicionales de refuerzo y prevención a medio plazo. (8 puntos)

Plaça de la Constitució, 10 46960 Aldaia València
Tel. 961 50 15 00 Fax 961 51 06 93
C.I.F. P-4602100-B Reg.Entitats Locals 01460214