Convocatoria 08/23 – CONVOCATORIA DE PRUEBAS SELECTIVAS PARA CUBRIR 6 PLAZAS DE PERSONAL LABORAL TÉCNICO EN LA CNMV. TÉCNICOS ESPECIALISTAS EN CIBERSEGURIDAD Y SUPERVISIÓN DE RIESGO TECNOLÓGICO

Tercera parte: ejercicio escrito – Resolución de ejercicios

Especialidad: Ciberseguridad

Pegue una etiqueta de código de barras en el siguiente recuadro

Consideraciones generales:

a) Se pueden hacer las suposiciones que se consideren necesarias describiéndolas convenientemente.

b) No se admitirán preguntas relacionadas con el contenido del ejercicio.

Resuelva el siguiente caso práctico (**puntuación máxima 50 puntos**):

Su organización es una entidad clave dentro de la administración pública española, relacionado con el sector financiero. Uno de los objetivos prioritarios para final de año es la adecuación al Esquema Nacional de Seguridad (Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad).

Actualmente su organización cuenta con las siguientes capacidades de ciberseguridad:

1. La organización cuenta con la prestación de servicios de diferentes proveedores para dar soporte a sus operaciones habituales. Actualmente, existen unas cláusulas contractuales, pero no se especifican medidas de seguridad.

Proveedor	Descripción	Datos de interés
TechNet Solutions	Proveedor de servicios en la nube para el almacenamiento de datos de la organización.	El proveedor utiliza un protocolo FTP para la transmisión de la información. En el último año han sufrido, al menos, un ataque de Ransomware.
DataGuard Ltd.	Empresa de soporte y mantenimiento de software de seguridad en puestos de usuarios de la organización.	El proveedor solicita acceso a los sistemas bajo diferentes mecanismos, incluyendo el uso de software vulnerable para el acceso remoto. Desde la organización se desconocen los controles de seguridad que emplean, los permisos utilizados y si se están compartiendo cuentas entre los empleados del proveedor.
SecureLink	Proveedor de soporte de red y comunicación de la organización, incluyendo VPN y firewall.	La solución de VPN utilizada no está actualizada desde hace más de un año. La autenticación utilizada es poco robusta y los algoritmos empleados no cumplen la normativa.
InfoServ	Consultora que gestiona el análisis de datos financieros en los sistemas de la organización.	La API que utilizan para el intercambio de información presenta ciertas vulnerabilidades. La exposición de endpoints (URLs de acceso) hacia Internet no tiene restricción a ningún nivel.

Tabla 1 – Listado de proveedores.

2. La monitorización está delegada en un SOC gestionado por un tercero.
3. La mayoría de las comunicaciones internas están cifradas por algoritmos criptográficos aprobados dentro del catálogo publicado por el CCN-CERT.

4. La organización dispone de un volumen elevado de desarrolladores internos. Las herramientas dentro del pipeline de desarrollo están basadas en repositorios git, únicamente integradas en los IDEs de desarrollo. Actualmente, no se están aplicando metodologías de S-SDLC. La organización utiliza separación de entornos para las diferentes etapas del ciclo de vida del desarrollo.
5. Se dispone de una solución Endpoint Detection and Response (EDR) sobre puestos de usuario y servidores.
6. Existe un inventario de vulnerabilidades con las principales afectaciones que sufre la organización sin mayor nivel de detalle:

Exposición de puertos críticos
Inyección SQL en el Portal Web
Configuración débil TLS
Protocolo de autenticación inseguro
Divulgación de Información en Logs
Aplicaciones con versiones fuera de soporte

Tabla 2 – Inventario de vulnerabilidades.

7. La organización no dispone de una herramienta para la gestión de vulnerabilidades, se están valorando diferentes herramientas a través de pruebas de concepto (PoC).
8. La organización está en proceso de reestructuración de la arquitectura según las buenas prácticas del mercado. Se ha planteado un proceso de segmentación de red.

Debe tener en cuenta las capacidades de ciberseguridad descritas a alto nivel y el contexto previamente definido para responder a las preguntas que se le plantean a continuación:

A. Especifique y describa en detalle las fases del proceso de adecuación al Esquema Nacional de Seguridad (ENS), en todo su ciclo de vida, para cualquier tipo de administración pública. Además, si la categorización del sistema para la organización del supuesto es de nivel medio, indique las principales diferencias en comparación con el nivel básico e indique los factores que han llevado a esta categorización. (**10 puntos**).

B. Describa las fases del proceso de gestión de incidentes. Proponga, al menos, dos acciones concretas para cada fase del proceso en caso de un incidente de Ransomware, originado en uno de los proveedores contratados por la organización. (**10 puntos**).

C. Siguiendo los principios básicos de diseño seguro, enumere y explique en detalle las capacidades y características clave sobre el escenario planteado. Además, describa las ventajas de aplicar procesos de hardening sobre los sistemas operativos de los activos, detallando los pasos clave de dicho proceso. **(10 puntos).**

D. Según el escenario proporcionado, defina a alto nivel los aspectos que debería incluir la normativa interna de gestión de terceros de su organización. Identifique los principales riesgos asociados y proponga controles para dichos riesgos, especificando el tipo de control a implementar (Tabla 1 **–** Listado de proveedores). **(8 puntos).**

E. Dado el inventario de vulnerabilidades citado previamente (Tabla 2 – Inventario de vulnerabilidades) y considerando que ya están identificadas, ¿qué proceso seguiría para gestionar su clasificación, priorización y respuesta? Razone su respuesta. (**8 puntos**).

F. Explique los principios fundamentales de la metodología DevSecOps e indique los tipos de herramientas que pueden utilizarse para fortalecer el ciclo de vida de desarrollo, aplicando esta metodología al supuesto. (**4 puntos**).