CONVOCATORIA DE PRUEBAS SELECTIVAS PARA CUBRIR UNA PLAZA DE PERSONAL LABORAL EN LA COMISIÓN NACIONAL DEL MERCADO DE VALORES. SUBDIRECTOR DE CIBERSEGURIDAD INTERNA PARA EL DEPARTAMENTO DE SISTEMAS DE INFORMACIÓN. 06/21.
FASE DE OPOSICIÓN. TERCERA PARTE

Coloque aquí la etiqueta con el código de barras

EJERCICIO ESCRITO – RESOLUCIÓN DE EJERCICIOS.

1) Desarrolle el siguiente tema (puntuación máxima 10 puntos)

Explique en detalle, al menos, cinco (5) medidas de seguridad de cualquier tipo que debe implantar una organización para defenderse de un ataque por ransomware, relacionando dichas medidas de seguridad con los dominios del framework de ciberseguridad del NIST (Identify, Protect, Detect, Respond, Recover). Adicionalmente, describa, con el detalle que considere oportuno, un caso real de ransomware conocido que conozca.

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

Su Entidad es un actor clave en el sistema financiero español. La Alta Dirección de su Entidad acaba de comunicarle que un objetivo prioritario de negocio para el año 2024 será cumplir con el Esquema Nacional de Seguridad (Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad) y lograr la certificación correspondiente al nivel medio.

Para ello, cuenta con un tiempo de 8 meses desde ahora hasta el inicio de la auditoría correspondiente. Dispone de recursos internos limitados que ascienden a un total 5 FTEs y un presupuesto total de 1.100.000,00 €.

El Departamento de Ciberseguridad se encuentra dentro del Departamento de Tecnología. En la actualidad, el Departamento de Tecnología se encuentra en un proceso de transformación dimensionado para 5 años, siendo este el segundo año del plan. La estrategia del Departamento de Tecnología es apostar por el entorno cloud y realizar una migración total de sus sistemas.

Relativo a capacidades de ciberseguridad, actualmente su Entidad cuenta con las siguientes:

- En términos de monitorización, se cuenta con un SOC delegado en un tercero.
- En términos de seguridad de dispositivos de usuario final, se encuentra en fase de análisis el despliegue de Endpoint Detection and Response (EDR). Se están priorizando medidas de seguridad en la totalidad de endpoints.
- En cuanto al cifrado de datos, se han focalizado esfuerzos en reforzar las comunicaciones con terceras partes, aplicando algoritmos como TLS.
- En términos de control de accesos y gestión de usuarios, la Entidad gestiona a día de hoy las cuentas privilegiadas manualmente y de manera ad-hoc.
- En cuanto a control de redes y dispositivos, la Entidad está desarrollando un proyecto de mejora de la segmentación y segregación de la red.
- La administración del CPD está externalizada en un tercero.
- Los dispositivos de mesa de empleados cuentan con sistema operativo Windows, principalmente, y Linux. En cuanto a servidores, el 25% del parque de los servidores se encuentran en cloud y el 75% on-premise.
- En relación a la gobernanza del dato y gestión de la confidencialidad de la información, la Entidad se encuentra en fase de revisión de las reglas de clasificación de información y la configuración inicial de una nueva herramienta DLP.
- En términos de desarrollo de código, el proceso de desarrollo de código cuenta con dos entornos separados: entorno de desarrollo y entorno de producción. Solo se

realiza desarrollo de código de forma segura para contadas aplicaciones desarrolladas en la Entidad y para casos muy concretos. Por ejemplo, la aplicación web y móvil de la Entidad no están bajo directrices de S-SDLC.

- En relación a la gestión de terceras partes, en los contratos con terceros se incluyen SLAs y algunas pocas cláusulas de seguridad. Sin embargo, esto lleva muchos años sin ser revisado por nadie.

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

A. Explique qué acciones llevaría a cabo para liderar y ejecutar convenientemente una adaptación al Esquema Nacional de Seguridad y su posterior auditoría, entendiendo que el objetivo debe ser obtener la certificación del ENS del nivel medio.
B. Diseñe un protocolo a alto nivel de gestión de incidentes que incluya todas las fases necesarias para una correcta gestión del ciclo de vida de los incidentes según criticidad. Para la elaboración, debe tener en cuenta los requisitos del Esquema Nacional de Seguridad a este respecto, así como todo el contexto previamente descrito. Incluya dentro del Protocolo un apartado concreto relativo a la notificación de incidentes a las Autoridades Competentes.
C. Durante la ejecución normal de los proyectos, se ha dado cuenta que la relación con el resto del Departamento de Tecnología del que depende no ve con buenos ojos las exigencias y proyectos que ha puesto encima de la mesa. Explique de qué forma llegaría a un acuerdo para poder posicionar la ciberseguridad como un elemento clave dentro de los procesos de la Entidad y defina un Modelo de Colaboración con el Departamento de Tecnología en proyectos e iniciativas donde deban estar involucrados.
D. Diseñe un Política que cubra el ciclo de vida de parches y vulnerabilidades teniendo en cuenta el contexto previamente dado. Deberá hacer hincapié en los puestos de usuario, servidores y la gestión del CPD.
E. Describa qué procesos llevaría a cabo para adecuar las acciones de cara a la adaptación del ENS, los procesos y el gobierno de su equipo de Ciberseguridad bajo el Sistema de Gestión de Calidad de la Entidad, recientemente certificada en la ISO 9001.