

SUPUESTO PRÁCTICO - 1

Usted trabaja como responsable de Seguridad de la Información en una universidad. Dicha universidad cuenta con copias de seguridad para sus sistemas críticos siguiendo un esquema 3-2-1-1, siendo esta última una copia inmutable. La universidad tiene su infraestructura en modo onpremise, si bien tiene algunos servicios en nube, tales como el Directorio Activo sincronizado en Azure. Además, tiene una estrategia de recuperación anti desastres basado en dos infraestructuras:

- Los sistemas críticos tales como la web, el aula virtual, la sede electrónica, la web y el ERP están sincronizados en almacenamiento y máquinas virtuales en un proveedor Cloud. Dicho contrato cubre exclusivamente el almacenamiento y el cómputo necesario para realizar las pruebas de restauración, pero no para la operación en contingencia.
- En local, en el CPD secundario, hay cierta capacidad excedente a modo de respaldo.

Son las 22h de un domingo y recibe una llamada telefónica del Director de Informática de la universidad y del responsable de sistemas comunicándole que la universidad ha sufrido un ciberataque por ransomware y que debe procederse a dar respuesta a dicho incidente.

Tras montar rápidamente una reunión de inicial de crisis, se identifica la necesidad de tomar medidas inmediatas destinadas a detener el ataque y comenzar a las 7am del día siguiente con las acciones de respuesta y recuperación.

En base a ello, responda a las siguientes preguntas:

1. Explique qué acciones propondría llevar a cabo como medidas inmediatas y justifíquelas brevemente.

2. Explique de manera resumida qué acciones recomendaría como respuesta al incidente.

3. Explique de manera resumida qué acciones post-incidentes recomendaría, una vez recuperado el incidente.

NOTA: En todo lo no definido explícitamente en este supuesto, podrá realizar las suposiciones que se estime oportunas, debiendo hacerlas constar en su propuesta de solución acompañadas de la justificación correspondiente.

SUPUESTO PRÁCTICO - 2

La Universidad Rey Juan Carlos es la responsable de realizar la cotización de la Seguridad Social de las prácticas en empresa de sus estudiantes de prácticas. Para poder cumplir con este precepto la universidad debe desarrollar un sistema integrado con la Seguridad Social y los sistemas de gestión de la universidad para poder informar de manera automatizada de las prácticas de los estudiantes, sus periodos, su asistencia y en base a ello realizar la cotización correspondiente.

La información de los estudiantes de prácticas reside en una aplicación de desarrollo propio en PHP y base de datos relacional Oracle. La información académica de los estudiantes reside en el ERP Universitas XXI, cuyos datos están también en una base de datos relacional Oracle. Estos sistemas se ubican en el CPD local de la universidad, bastionado dentro de una VLAN privada y detrás de un firewall y un balanceador de tráfico de red.

La Seguridad Social dispone de *web services* con sus especificaciones correspondientes para la integración. Dichos servicios son accesibles a través de la Red SARA.

Usted se integrará dentro de un grupo de trabajo multidisciplinar con el objetivo de aconsejar sobre la arquitectura tecnológica propuesta para el proyecto.

En base a ello, responda a las siguientes preguntas:

- 1. Aconseje sobre la pertinencia o no de realizar un desarrollo propio o una subcontratación del desarrollo, analizando pros y contras. Asimismo, aconseje sobre los procedimientos de contratación que recomendaría utilizar.**
- 2. Describa y dibuje la arquitectura tecnológica que plantearía.**
- 3. Proponga un modelo de desarrollo ágil o un modelo de desarrollo en cascada justificando pros y contras. Realice una planificación del proyecto, especificando de manera resumida cada una de las actividades**

NOTA: En todo lo no definido explícitamente en este supuesto, podrá realizar las suposiciones que se estime oportunas, debiendo hacerlas constar en su propuesta de solución acompañadas de la justificación correspondiente.

SUPUESTO PRÁCTICO 3

La Universidad Rey Juan Carlos, ofrece servicios a 40.000 alumnos matriculados entre Grados, Máster y Títulos Propios. Alrededor de 3000 PDI y 1700 PTGAS. Los servicios que se ofrecen desde el Area de IT son muy diversos, abordando las necesidades de todo el colectivo que forman la URJC.

Como uno de los pilares importantes e imprescindibles que se ofrece para dar servicio al PDI, PTGAS y al estudiante, es la plataforma de e-Learning implementada con Moodle, la plataforma de escritorios virtuales como vWorkspace. Todas y cada una de las plataformas que ofrecen servicio a la comunidad universitaria, son pilares de la institución.

Usando una de las dos plataformas descritas que se ofrece desde el servicio de IT, se requiere describir que elementos de seguridad y componentes son necesarios para proteger los servicios, englobándolos dentro del ENS, cumplimiento de normas ISO, Guías CCN/CERT.

Elemento que se valorarán positivamente a la hora de realizar la exposición:

- 1.- Diseño gráfico del hardware de la plataforma que se ha elegido para describir**
- 2.- Descripción del software que se implementa para dar soporte**
- 3.-Diseño lógico de infraestructura**
- 4.- Basado en el ENS describir:**
 - Políticas de seguridad y requisitos mínimos de seguridad**
 - Seguridad de sistemas: auditoría, informe e incidentes de seguridad.**
 - Normas de conformidad**
- 5.- En función de los sistemas operativos a implantar, explicar las guías del CCN/cert que se aplicarían y detallar la funcionalidad de dichas guías.**

SUPUESTO PRÁCTICO 4

La Universidad ha comunicado que un objetivo prioritario para el año 2024 será cumplir con el Esquema Nacional de Seguridad (ENS) (Real Decreto 311/2022, de 3 de mayo) y lograr la certificación correspondiente al nivel medio. Para ello, se cuenta con un plazo de 12 meses hasta el inicio de la auditoría correspondiente.

El Departamento de Ciberseguridad forma parte del área de TI. Actualmente, el área de TI se encuentra en un proceso de transformación apostando por el entorno cloud y la migración total de sus sistemas en los próximos cinco años.

Relativo a capacidades de ciberseguridad, actualmente la Universidad cuenta con las siguientes:

- Monitorización: SOC (Centro de Operaciones de Seguridad) delegado en un tercero.
- Seguridad de dispositivos de usuario final: En fase de análisis el despliegue de Endpoint Detection and Response (EDR), priorizando medidas de seguridad en la totalidad de endpoints.
- Cifrado de datos: Se han reforzado las comunicaciones con terceras partes, aplicando algoritmos como TLS.
- Control de accesos y gestión de usuarios: Gestión manual y ad-hoc de cuentas privilegiadas.
- Control de redes y dispositivos: Proyecto de mejora de la segmentación y segregación de la red.
- Dispositivos clientes sistemas operativos Windows; servidores 25% en cloud y 75% on-premise.
- Gobernanza del dato y gestión de la confidencialidad de la información: En fase de revisión de reglas de clasificación y configuración inicial de una nueva herramienta DLP.
- Gestión de terceras partes: Contratos con SLAs y algunas cláusulas de seguridad, sin revisiones recientes.

Preguntas:

1. 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.

2. Diseñe un protocolo de gestión de incidentes que incluya 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. Incluya dentro del Protocolo un apartado concreto relativo a la notificación de incidentes a las Autoridades Competentes.

3. Diseñe una 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.