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: Supervisión de Riesgo Tecnológico

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.

CASO PRÁCTICO 1 (35 puntos)

Durante la supervisión del riesgo tecnológico de una entidad financiera de tamaño grande, tomando como referencia el Reglamento DORA, se han documentado los siguientes hallazgos:

ID	
1	El marco de gestión de riesgos de la entidad lo gestionan y controlan técnicos del área de informática y lo aprueba su director. El órgano de dirección recibe un informe técnico para estar informado, aunque dada su falta de conocimiento, confía en el director de dicha área de informática.
2	En una muestra de riesgo, han valorado que el riesgo inherente de infección en un puesto de usuario mediante un correo de phishing es medio: media probabilidad y medio impacto. Si bien, dado que tienen antivirus y anti-spam se considera que el riesgo residual resulta bajo: baja probabilidad y bajo impacto.
3	La entidad tiene un cortafuegos perimetral. Sólo permite determinado tráfico de entrada y registra dicha actividad (conexiones permitidas y bloqueadas). Para el tráfico de salida está todo permitido sin guardar registros de actividad. La red interna está separada en dos segmentos: la red de usuario y la de servidores. Un dispositivo registra todos los accesos entre ambas redes, para alertar si la IP de un puesto de usuario no administrador accede a la consola de un servidor (por RDP o SSH).
4	Los equipos de trabajo de los usuarios están protegidos por el antivirus y su correo por un sistema anti-spam. Los usuarios no son administradores de su puesto de trabajo. Tienen un sistema antivirus avanzado, pero no registra la actividad en una consola central. En una muestra se detecta que 2 de 10 dispositivos no tenían el software de antivirus actualizado en los últimos 5 meses.
5	Se ha contratado un servicio de escaneo automático semanal de vulnerabilidades sobre los servicios publicados en Internet. Para la red interna se lanza cada dos años un escaneo de puertos para detectar si hay dispositivos no identificados y qué puertos exponen. Para ambos servicios se generan informes sobre las vulnerabilidades encontradas, mensuales en el primer caso y bianuales en el segundo. Este informe lo gestiona el área de informática para subsanar las vulnerabilidades encontradas en función de la gravedad. Se encuentra que hay algunas vulnerabilidades críticas que no se han corregido en los últimos seis meses.
6	Ha ocurrido un incidente grave de un ransomware hace seis meses. En algunos sistemas esenciales tuvieron que recuperar los datos de 15 días antes del incidente, dado que, aunque hacen copia de seguridad diaria, el sistema de backup llevaba 13 días fallando sin que se dieran cuenta del problema. En ese incidente se informó del problema al órgano de dirección al inicio y cuando ya se restableció el servicio. Como no tenían un procedimiento de gestión de incidentes, en el momento de detección se reunieron el responsable de ciberseguridad y el director del área de informática para resolver el problema y asignar funciones. Después del restablecimiento del servicio no se observa ningún informe o acción relacionada posterior.
7	Un sistema que realiza una función esencial de la entidad está externalizado. Para dicho servicio externalizado, a nivel contractual, se indica la descripción de servicio, la fecha de finalización, la obligación de notificación de incidentes graves que ocurran y el aviso con tiempo de un cambio en los términos y condiciones del contrato. Se observa ausencia de otras cláusulas relevantes relacionadas con la ciberresiliencia.

8	El acceso VPN requiere un usuario y contraseña propio para cada empleado de la entidad. Adicionalmente, necesitan otro usuario y contraseña para acceder a los servicios internos: aplicaciones, carpetas compartidas y correo electrónico. Los administradores han publicado un acceso a un servidor por RDP (Remote Desktop Protocol), autenticándose mediante certificado electrónico, para que en el caso de que el servicio de VPN falle, poder arreglarlo con urgencia desde su domicilio.
9	La política de gestión de cambios de la entidad indica que antes de poner en producción un cambio se pruebe primero en el entorno de desarrollo/preproducción. Se observa que eso se cumple para los sistemas esenciales. Para sistemas no esenciales no hay dichos entornos, aunque cuentan con copias de seguridad previas. A veces se necesita hacer un cambio urgente (por un fallo en el comportamiento o una nueva actualización de seguridad importante), y se pide autorización al director del área de informática para hacer el cambio directamente en producción.
10	A los empleados se les entrega la Política de Seguridad de la entidad al incorporarse. El personal de informática recibe formación sobre los productos con los que trabajan, incluyendo aspectos de ciberseguridad. Para los demás empleados no se observa ningún comunicado o formación sobre la ciberseguridad. Si tienen dudas pueden contactar con soporte informático. Aunque la política de la entidad requiere cambios de contraseña periódicos y uso de contraseñas robustas no reutilizables, su sistema de autenticación de usuarios no obliga a hacerlo.

1.1 Organice en la tabla de las hojas de respuesta la relación de deficiencias que considera que la entidad financiera debería subsanar, indicando: **(20 puntos)**

- Valoración de la gravedad (por ejemplo: muy grave, grave, media, baja).
- Identificación de los riesgos para cada hallazgo (referenciar el Reglamento DORA en la medida de lo posible) y recomendaciones para subsanarlos.
- Plazo esperado de subsanación (por ejemplo: corto, medio, largo).

Indique aparte de la tabla los criterios empleados para considerar la clasificación de la gravedad de las deficiencias y para estimar los plazos de subsanación.

1.2 Haga un informe ejecutivo (resumen para la alta dirección, sin información muy técnica) sobre el resultado de la supervisión y las principales recomendaciones. No debe superar la cara de un folio. **(10 puntos)**

1.3 Indique de forma razonada dos hallazgos de la tabla, donde aplicaría otro criterio en el caso de que la entidad financiera fuera de tamaño pequeño. **(5 puntos)**

PREGUNTAS CORTAS (5 puntos cada una)

2.- Indique en qué consiste una prueba de penetración basada en amenazas (Threat-Led Penetration Test, TLPT) o del marco TIBER-ES y su tratamiento en el Reglamento DORA. Además, indicar en qué se diferencian de otras pruebas de pentesting.

3.- Detalle las obligaciones de comunicación de incidentes relacionados con las TIC de una entidad financiera (cómo, a quién, cuando y bajo qué criterios) según el Reglamento DORA.

4.- Describa las principales fases del ciclo de vida que debe tener en cuenta una entidad en la contratación de proveedores de nube (cloud) para soportar servicios esenciales o importantes. Indique las implicaciones en el Reglamento DORA en este proceso de contratación.

ID	Gravedad	Identificación de riesgos y recomendaciones.	Plazo de subsanac.

ID	Gravedad	Identificación de riesgos y recomendaciones.	Plazo de subsanac.