Convocatoria 06/24 – CONVOCATORIA DE PRUEBAS SELECTIVAS PARA CUBRIR 2 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

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)

En el marco de la estrategia supervisora de la CNMV para verificar el grado de preparación de las entidades financieras frente al Reglamento (UE) 2022/2554 sobre resiliencia operativa digital (DORA), se ha realizado una supervisión in situ en la entidad DUERO S.V (tamaño grande) durante el segundo trimestre de 2025.

Como resultado de la supervisión, se ha elaborado un informe preliminar en el que se recogen deficiencias e indicadores de riesgo en relación con los cinco pilares de DORA.

ID	Indicador	Valor reportado	Objetivo (2025)	Observaciones
1	Porcentaje de incidentes clasificados según materialidad DORA.	22%	100%	35 incidentes totales; solo 8 han sido clasificados formalmente.
2	Número de informes remitidos al Consejo de Administración.	0	2 (semestrales)	El Consejo no ha recibido información formal sobre riesgos TIC en 2025.
3	Porcentaje de procesos críticos probados en escenarios adversos.	50%	100%	El proceso de compraventa de valores no fue sometido a prueba.
4	Porcentaje de proveedores TIC en funciones esenciales o críticas con contratos alineados a DORA.	50%	100%	El proveedor tecnológico de la plataforma de trading no tiene cláusulas de portabilidad ni auditoría.
5	Porcentaje de proveedores TIC en funciones esenciales o críticas con pruebas de continuidad realizadas.	60%	100%	El proveedor *cloud* y el *call center* no participaron en pruebas.
6	Tiempo medio de notificación interna de incidentes relevantes.	72h	≤4h	La notificación a nivel de dirección operativa se retrasa sistemáticamente.
7	Grado de avance en plan de pruebas tipo Red-Team.	15%	≥70%	No se han contratado proveedores externos ni definido el alcance.
8	Tasa de rotación personal interno.	27%	<10%	Falta de plan de retención y escasez de personal cualificado.
9	Porcentaje de auditorías TIC ejecutadas respecto al plan anual.	50%	100%	Auditorías de gestión de accesos y resiliencia están pendientes.

Observaciones adicionales

- El CISO (*Chief Information Security Officer*) reporta al COO (*Chief Operating Officer*), no directamente al Consejo de administración, ni al Comité de Riesgos TIC.
- No existe política formal de clasificación de incidentes según DORA; la entidad usa criterios internos heterogéneos.
- El Comité de riesgos TIC no se reúne desde hace un año.
- Se detectó el uso de datos reales de clientes en entornos de pruebas sin medidas de seguridad equivalentes.

Preguntas

1.1 Identificación de riesgos y evaluación de criticidad. (15 puntos)

- Detecta y describe los riesgos más relevantes para la entidad en relación con el reglamento DORA.
- Clasifica los riesgos en alto, medio o bajo, justificando la evaluación con los requisitos DORA.
- Prioriza de manera justificada qué riesgos deberían abordarse con carácter inmediato de acuerdo con lo establecido en DORA.

1.2 Acciones supervisoras. (15 puntos)

Elabora un plan de remediación dirigido a DUERO S.V con medidas concretas para su ejecución:

- Acciones correctoras.
- Responsable dentro de la entidad de cada acción correctora.
- Plazo (corto ≤3 meses, medio ≤12 meses, largo >12 meses).

Si en la próxima revisión (Q4 2025) la entidad no presenta avances significativos en la ejecución de dicho plan, ¿qué medidas adicionales podría adoptar la CNMV en el marco de sus competencias?

1.3 Consecuencias estratégicas. (5 puntos)

Analiza las consecuencias para DUERO S.V en caso de no alcanzar un grado suficiente de madurez DORA antes de enero 2026.

¿Qué riesgos regulatorios, reputacionales y operativos podría enfrentar?

PREGUNTAS CORTAS (5 puntos cada una)

1. Indica en qué consiste una prueba de penetración basada en amenazas (Threat-Led Penetration Test, TLPT) del marco TIBER-ES y su tratamiento en el Reglamento DORA. ¿Qué características debería tener una entidad para ser candidata a un TLPT?

2. Detalla los criterios utilizados para que un incidente de seguridad sea catalogado como grave y, por tanto, susceptible de ser reportado a la autoridad competente, según el Reglamento DORA, incluyendo dos ejemplos.

3. Indica en detalle los requisitos que impone DORA en materia de gestión de proveedores TIC que sustentan funciones esenciales o importantes. ¿Qué mecanismos de supervisión, auditoría y resiliencia contractual introduce y de qué forma? ¿Qué impacto consideras que suponen estos requerimientos en las entidades financieras?