CONTESTACION DEL COMITÉ CONSULTIVO DE LA CNMV AL CONSULTATION PAPER DE LA COMISIÓN EUROPEA SOBRE "UN MARCO DE RESILIENCIA OPERATIVA DIGITAL PARA LOS SERVICIOS FINANCIEROS: HACIENDO EL SECTOR FINANCIERO DE LA UE MÁS SEGURO"

1.- Introducción.

El Comité Consultivo agradece la oportunidad de realizar comentarios sobre un tema tan relevante como la seguridad en los ámbitos de utilización de tecnologías por las entidades que prestan servicios de inversión y la prevención de ciber ataques, que pueden tener consecuencias desde el punto de vista de la estabilidad financiera –en caso de entidades de gran tamaño- así como crear un potencial perjuicio tanto al desarrollo de la actividad de las entidades, como a los inversores, clientes de estas entidades.

Por la propia naturaleza del Comité Consultivo, la contestación a este documento a consulta se circunscribe al siguiente marco:

- Las medidas de prevención en materia de seguridad tecnológica pertenecen, como señala el documento de la Comisión Europea, al ámbito prudencial de las entidades. Esto hace que la presente contestación del Comité Consultivo de la CNMV, se realice teniendo en cuenta el ámbito propio de actuación que, en esta materia, tiene la CNMV.

- Son numerosas las preguntas dirigidas a ser contestadas por cada entidad y referidas a circunstancias específicas de cada una de ellas. Por razones obvias, las contestaciones del Comité Consultivo no se centrarán en estas preguntas, sino en las que, siendo de carácter más general, permitan una posición del Comité.

2.- Comentarios generales.

-El Comité Consultivo considera la seguridad tecnológica y la prevención de ciber ataques algo de gran importancia en el ámbito de los mercados de valores.

Las implicaciones que ello puede tener para el mercado en su conjunto y/o para inversores en particular (por mucho que sistemas de indemnización puedan cubrir parcialmente algunos de ellos) hacen de esta cuestión una cuestión muy relevante.

Por ello, como primera consideración, el Comité valora muy positivamente que la Comisión Europea dedique su atención de forma específica- como muestra este documento a consulta- a

esta materia.

Asimismo el Comité toma nota de la preocupación que este tema despierta en el ámbito de la propia CNMV, que ha introducido la elaboración de una Guía Técnica sobre esta materia en su plan de Actuación para el año 2020.

-El Comité quiere enfatizar que es este un ámbito donde la proporcionalidad debe ser un elemento presente en todo momento, como se apreciará a lo largo de la presente contestación. La naturaleza y volumen de actividades de las entidades determinan el alcance del riesgo que un ciber ataque, o una brecha de seguridad informática, pueden plantear al mercado en su conjunto o a inversores en concreto.

Tratándose de prevenir estos riesgos, es especialmente importante ajustar las medidas específicas a las circunstancias concurrentes en cada caso, diferenciando claramente entidades con capacidad de movilizar riesgos significativos de aquellas que no la tienen.

3.- Contestación al documento a consulta.

El documento a consulta se centra en una serie de preguntas alrededor de las siguientes temáticas:

- *Mejoras específicas de los requisitos de gestión de los riesgos de seguridad y de las TIC en las diferentes piezas de la legislación sobre servicios financieros de la UE.*
- *Armonización de la notificación de incidentes de TIC*.
- *La elaboración de un marco de pruebas de resiliencia operacional digital en todos los sectores financieros.*
- *Normas específicas que permitan una mejor supervisión de determinados proveedores terceros de TIC.*
- *Otras áreas de atención, tales como:*
    - *el intercambio eficaz de información sobre las TIC y las amenazas a la seguridad entre los participantes en los mercados financieros y una mejor cooperación entre las autoridades públicas.*
    - *la promoción de los seguros u otra fórmula de transferencia de riesgo.*
    - *La interacción de esta potencial nueva regulación con la Directiva NIS.*
    - *evaluación del potencial impacto.*

Respecto de cada uno de estos apartados, el Comité realiza las siguientes consideraciones:

ICT and security requirements

1. Taking into account the deep interconnectedness of the financial sector, its extensive reliance on ICT systems and the level of trust needed among financial actors, do you agree that all financial entities should have in place an ICT and security risk management framework based on key common principles?

- ☐ *Yes*
- ☐ *No*
- X *Don't know/no opinion*

To the extent you deem it necessary, please explain your reasoning.

La seguridad informática es clave es un mercado global y muy automatizado. En un contexto de normalización y estandarización de las rutinas, procesos y prácticas de mercado a través de una intensa regulación, es relevante establecer unos principios comunes que garanticen un nivel mínimo de seguridad informática y den confort a los inversores.

Pero ello no puede suponer que no se tengan en cuenta los específicos ámbitos operativos y formas de actuación- más o menos informatizadas- de cada entidad, así como la naturaleza de las actividades que cada una desarrolla. Como se ha señalado más arriba, la proporcionalidad es en este ámbito, esencial.

Por ello, en tanto los "principios comunes" no perjudiquen esta proporcionalidad en modo alguno, serán adecuados. Pero debe cuidarse que no vayan más allá y perjudiquen un tratamiento específico para cada perfil de riesgo.

En este sentido, es relevante también prestar atención a la realidad de ciber ataques ya que, por ejemplo, respecto de entidades de más reducido tamaño, la experiencia no muestra precedentes preocupantes.

ICT and security incident reporting requirements

21. ***Do you agree that a comprehensive and harmonised EU-wide system of ICT and security incident reporting should be designed for all financial entities?***

- ☐ *Yes*
- ☐ *No*
- x *Don't know*

To the extent you deem it necessary, please explain your reasoning.

De nuevo, es importante resaltar que el avance a nivel de la UE en esta materia no debe ser similar para todo tipo de entidades y todo tipo de perfiles de actividad, volumen, etc.

Por tanto, en tanto el sistema de reporte tenga en cuenta una vez más este principio y aplique la proporcionalidad, será adecuado. Por ello, deben adoptarse umbrales y formatos diferentes en los principios y normas a adoptar.

Adicionalmente, el Comité considera positivo que la UE esté atenta a los principios que se fijen a

nivel internacional en estas materias, para poder estar coordinada con ellos.

22. ***If the answer to the previous question (no. 21) is yes, please explain which of the following elements should be harmonised?***

Elements to be harmonised in the EU-wide system of ICT incident reporting	*Yes*	*No*	*Don't know/not applicable*
Taxonomy of reportable incidents	x		
Reporting templates	x		
Reporting timeframe	x		
Materiality thresholds	x		
Other (please specify)			

To the extent you deem it necessary, please explain your reasoning.

Aunque la contestación a la pregunta anterior no es "si" por las razones expuestas, el Comité aprecia positivamente que se pueda establecer un mecanismo de reporte de incidencias que responda a los principios allí mencionados. En ese proceso, deberían ser armonizados los apartados señalados en el cuadro.

23. ***What level of detail would be required for the ICT and security incident reporting? Please elaborate on the information you find useful to report on, and what may be considered as unnecessary.***
To the extent you deem it necessary, please explain your reasoning.

El reporte debe simplificarse lo más posible para hacerlo sencillo y rápido y para ofrecer la información mínima necesaria, también para el sector.

Es más relevante, en este sentido, centrar el reporte en el tipo de vulnerabilidad que en el impacto concreto en una entidad.

24. ***Should all incidents be within the scope of reporting, or should materiality thresholds be considered, whereby minor incidents would have to be logged and addressed by the entity but still remain unreported to the competent authority?***

- ☐ *Yes*
- X *No*
- ☐ *Don't know*

To the extent you deem it necessary, please explain your reasoning.

Es importante fijar umbrales de materialidad. La finalidad no es abarcar cuestiones individuales complejas, sino dar a conocer incidentes susceptibles de afectar al mercado o a inversores, por su naturaleza o por su incidencia.

25. ***Which governance elements around ICT and security incident reporting would be needed? To which national competent authorities should ICT and security incidents be reported or should there be one single authority acting as an EU central hub/database?***

To the extent you deem it necessary, please explain your reasoning.

Las comunicaciones deberían hacerse en primer lugar a la autoridad nacional, dentro de un procedimiento armonizado a nivel europeo. Es la autoridad que tiene más cercana y conoce mejor a la entidad y sus circunstancias, y el potencial de contagio, o afectación a inversores.

También se considera adecuado que, a nivel de la UE, se establezca algún tipo de coordinación o autoridad a la que a su vez se remitan estas comunicaciones para general conocimiento y evaluación a nivel de la UE.

26. ***Should a standing mechanism to exchange incident reports among national competent authorities be set up?***

x *Yes*

☐ *No*

☐ *Don't know*

To the extent you deem it necessary, please explain your reasoning.

Aparte de la coordinación a nivel de la UE, parece enteramente adecuado que existan intercambios de información y cooperación entre supervisores de diferentes estados cuando un incidente pueda afectar en varios de ellos.

2.2 Digital operational resilience testing framework

29. ***Should all financial entities be required to perform a baseline testing/assessment of their ICT systems and tools? What could its different elements be?***

Different elements of a baseline testing/assessment framework	*Yes*	*No*	*Don't know/ not applicable*
Gap analyses?	x		
Compliance reviews?	x		
Vulnerability scans?	x		
Physical security reviews?	x		
Source code reviews?		x	
Others (please specify)			

To the extent you deem it necessary, please explain your reasoning*.*

La aproximación a este tema puede ser diferente en entidades con sistemas propios y entidades que utilizan sistemas de terceros.

En particular, en entidades de tamaño más reducido, el nivel de outsourcing es significativo, por lo que no debería establecerse obligaciones de comprobación sobre esas entidades de tamaño reducido. Sin embargo, sí podría plantearse algún tipo de certificación o similar respecto de estas terceras entidades de outsourcing.

Por otro lado, aquí, una vez más, la proporcionalidad vinculada al perfil de actividad de la entidad, es esencial. No es lo mismo una entidad que se dedica al asesoramiento que una entidad que

gestiona un *robo advisor* o utiliza tecnología de forma intensiva en el desarrollo de su actividad.

30. ***For the purpose of being subject to more advanced testing (e.g. threat led penetration testing, TLPT), should financial entities be identified at EU level (or should they be designated by competent authorities) as "significant" on the basis of a combination of criteria such as:***

Criteria	*Yes*	*No*	*Don't know/ not applicable*
Proportionality–related factors (i.e. size, type, profile, business model)?	x		
Impact – related factor (criticality of services provided)?	x		
Financial stability concerns (Systemic importance for the EU)?	x		
Other appropriate qualitative or quantitative criteria and thresholds (please specify)?			

To the extent you deem it necessary, please explain your reasoning.

Realmente, una vez más es la proporcionalidad en sus diferentes vertientes (tipo de actividad, tamaño, entidad sistémica o no), la que debe aplicarse.

32. What would be the most efficient frequency of running such more advanced testing given their time and resource implications?

- *Every six months*
- *X* *Every year*
- *Once every three years*
- *Other*

To the extent you deem it necessary, please explain your reasoning.

Para entidades sometidas a un análisis avanzado por sus características, un año puede ser un plazo razonable. Adicionalmente, debería establecerse la obligación de revisión cuando existan cambios relevantes en la infraestructura o en las aplicaciones utilizadas por la entidad.

2.3 Addressing third party risk: Oversight of third party providers (including outsourcing)

37.- ***What is your view on the possibility to introduce an oversight framework for ICT third party providers?***

	Yes	*No*	*Don't know/ not applicable*
Should an oversight framework be established?			

Should it focus on critical ICT third party providers?			
Should "criticality" be based on a set of both qualitative and quantitative thresholds (e.g. concentration, number of customers, size, interconnectedness, substitutability, etc.)?			
Should proportionality play a role in the identification of critical ICT third party providers?	x		
Should other related aspects (e.g. data portability, exit strategies and related market practices, fair contractual practices, environmental performance, etc.) be included in the oversight framework?			
Should EU and national competent authorities responsible for the prudential or organisational supervision of financial entities carry out the oversight?			
Should a collaboration mechanism be established (e.g. within colleges of supervisors where one national competent authority assumes the lead in overseeing a relevant ICT service provider to an entity under its supervision - see			
Should the oversight tools be limited to non-binding tools (e.g. recommendations, cross-border cooperation via joint inspections and exchanges of information, onsite reviews, etc.)?			
Should it also include binding tools (such as sanctions or other enforcement actions)?			

To the extent you deem it necessary, please explain your reasoning.

Como en ocasiones anteriores, la proporcionalidad es muy relevante en este caso. Los proveedores son diferentes en tamaño, tipo de servicios prestados, capacidad de afectación al mercado, etc.

El Comité es consciente de que la externalización de los servicios informáticos, o de parte de éstos, es una práctica habitual en las entidades que prestan servicios de inversión. Y es consciente de la aproximación que a esta materia han realizado algunas autoridades, como es el caso del Informe Final de la Autoridad Bancaria Europea sobre las Guías en materia de acuerdos de externalización del 25 de febrero de 2019.

Por tanto, este es un tema relevante al que prestar atención.

Sin embargo, en cuanto a si debe establecerse un marco supervisor o no para estas entidades, caben diferentes aproximaciones. Una de ellas es establecer algún tipo de supervisión directa sobre este tipo de terceros proveedores de ICT y otra es mantener el punto de supervisión con

cada entidad financiera, de forma que sea a través de ella como puedan supervisarse y comprobarse los aspectos que se consideren más adecuados.

Sin perjuicio de lo señalado en la contestación a la pregunta 29, esta segunda aproximación se considera más coherente con el ámbito de la supervisión financiera.

38. What solutions do you consider most appropriate and effective to address concentration risk among ICT third party service providers?

	Yes	*No*	*Don't know/ not applicable*
Diversification strategies, including a potential mandatory or voluntary rotation mechanism with associated rules to ensure portability (e.g. auditing model)			
Mandatory multi-provider approach		X	
Should limits be set by the legislator or supervisors to tackle the excessive exposure of a financial institution to one or more ICT third party providers?		X	
Other (please specify)			

To the extent you deem it necessary, please explain your reasoning.

La concentración puede no tener efectos negativos, sino positivos, en algunos ámbitos. La armonización de procedimientos, formatos, etc entre entidades de menor tamaño, utilizando para ello algún proveedor, puede ser algo positivo, y sin embargo, podría considerarse como concentración.

En caso que se trate de proveedores cuyo tamaño y perfil de actividad pueda ocasionar riesgos relevantes, sí estaríamos en una situación donde la concentración puede convertirse en un riesgo.

Sin embargo, el principio general no debe ser limitativo o prohibitivo- de ahí las contestaciones en el cuadro superior- sino de supervisión prudencial sobre las entidades financieras concretas.

Tomar medidas de carácter limitativo o prohibitivo debe tener una base sólida de evidencias de ser necesaria.

2.4 Other areas where EU Action may be needed

Information sharing.

39.Do you agree that the EU should have a role in supporting and promoting the voluntary exchanges of such information between financial institutions?

- ☐ *Yes*
- ☐ *No*
- X *Don't know/no opinion*

To the extent you deem it necessary, please explain your reasoning.

No se discute la utilidad de un intercambio de información de este tipo. De hecho, las entidades

pueden ser libres de hacerlo.

Sin embargo, este intercambio puede producirse bien directamente, bien a través de alguna autoridad competente, que filtre la información, identifique su alcance y pueda confirmar la utilidad de su comunicación o difusión.

El Comité considera que esta segunda opción puede ser más adecuada, ya que, en ocasiones, este tipo de intercambio de información directamente entre entidades, puede generar desconcierto entre las mismas, ser incompleta, afectar a temas sensibles, etc

41. ***Do you see any particular challenges associated with the sharing of information on cyber threats and incidents with your peer financial institutions?***

X Yes

☐ *No*

☐ *Don't know/no opinion*

To the extent you deem it necessary, please explain your reasoning. If you answered yes, please explain which are the challenges and why, by giving concrete examples.

El intercambio de información sobre ataques o amenazas puede perjudicar la posición de una entidad frente a sus competidores, que pueden utilizarla en su propio interés, y frente a sus clientes. Esto último es especialmente relevante en un mercado basado en la confianza.

Sin embargo, esto no es así en todos los casos, ya que tratándose de entidades que tengan perfiles de negocio diferentes esta preocupación no estaría presente.

<u>Promotion of cyber insurance and other risk transfer schemes:</u>

45.- ***Where do you see challenges in the development of an EU cyber insurance/risk transfer market, if any?***

Issues	*Yes*	*No*	*Don't know/ not applicable*
Lack of a common taxonomy on cyber incidents	X		
Lack of available data on cyber incidents	X		
Lack of awareness on the importance of cyber/ICT security	X		
Difficulties in estimating pricing or risk exposures	X		
Legal uncertainties around the contractual terms and coverage	X		

Other (please specify)			

To the extent you deem it necessary, please explain your reasoning, by also specifying to the extent possible how such issues or lacks could be addressed.

46. Should the EU provide any kind of support to develop EU or national initiatives to promote developments in this area? If so, please provide examples.

X Yes

☐ *No*

☐ *Don't know/no opinion*

To the extent you deem it necessary, please explain your reasoning.

El principio en esta materia debe ser la voluntariedad y el margen de actuación de cada entidad al respecto.

Sin embargo, al tratarse de un ámbito en el que hay recorrido para avanzar en la aproximación general a los aspectos señalados en la respuesta a la pregunta anterior, el rol de la UE en su armonización puede ser útil

3. POTENTIAL IMPACTS

57. ***To the extent possible and based on the information provided for in the different building blocks above, which possible impacts and effects (i.e. economic, social, corporate, business development perspective etc.) could you foresee, both in the short and the long term? Please provide details.***

Una vez más, la proporcionalidad es esencial a la hora de limitar el impacto en las entidades, sus costes, la obligatoria contratación de expertos externos, etc,

Es importante que las medidas regulatorias estén adecuadamente aquilatadas a lo necesario, teniendo en cuenta el perfil de las actividades de cada entidad y los potenciales riesgos, muy limitados en ocasiones.

Si este principio no se aplicase adecuadamente, el impacto en entidades más pequeñas y medianas puede ser muy negativo.

Por otro lado, desde una perspectiva más global de mercado, algunas de las medidas pueden favorecer el incremento de la seguridad y la estabilidad, también para los inversores; el fortalecimiento de los elementos de persuasión para evitar en origen o reducir el impacto de ciberataques; la potenciación de la industria de ICT y su concentración, ya que hoy es un sector disperso; y favorecer mayores inversiones en este sector.

61. ***Which administrative formalities or requirements in respect to the ICT risks are today the most burdensome, human-resource intensive or cost-inefficient from an economic perspective? And how would you suggest they should be addressed?***

Please provide details.

El avance en tecnologías y protocolos más comunes se vería como una ventaja en esta materia,

donde el panorama actual presenta dispersión, lo que afecta a la hora de buscar eficiencia y reducción de costes.