Boletín Oficial

DE LA

AGRUPACIÓN TÉCNICA PROFESIONAL DE MEDIADORES FINANCIEROS TITULADOS DE ESPAÑA

MEDFIN

MEDIADORES FINANCIEROS

- Mediación en Finanzas, Préstamos, Valores.- EAFI -

AÑO 15 NÚMERO 91 Julio/Agosto 2025

Boletín Oficial

Julio/Agosto 2025

AÑO 15 NÚMERO 91

SUMARIO

Ejemplar: Gratuito
Recepción: Periódica
Edición: MEDFIN
Imprime: Gráficas Alhorí
Pablo Vallecillos Carrillo
D.L.: V-3256-2011

Boletín Oficial
DE LA
AGRUPACIÓN TÉCNICA PROFESIONAL
DE
MEDIADORES FINANCIEROS TITULADOS DE ESPAÑA

Redacción y Administración
C./ Covarrubias, nº 22-1º-Derecha
28010-MADRID
Telf. Corp: 91 457 29 29

E-mail: medfin@atp-guiainmobiliaria.com
Web: www.atp-medfin.com

ACTUALIDAD Corporativa

El Gobierno amplía el parque público de vivienda asequible

Inmuebles procedentes del rescate bancario se incorporarán a la nueva empresa estatal de vivienda. Además, el Ejecutivo ha impulsado la Ley de Consumo Sostenible, que fomenta la reparabilidad de los productos, veta la publicidad de combustibles fósiles y regula la reventa de entradas.

El Consejo de Ministros ha adoptado recientemente nuevas medidas para facilitar el acceso a la vivienda, la "principal preocupación" del Ejecutivo, según ha señalado la ministra de Vivienda y Agenda Urbana.

El objetivo, es ampliar el parque público de vivienda asequible y permanente ante una crisis que sufre todo el entorno europeo, pero que en España se agrava por la ausencia de un parque de esas características. La ministra ha apuntado que en los últimos años el porcentaje del parque público de vivienda ha pasado del 2,5% al 3,4%, aún lejos del 9% que es la media europea. Para aumentar y blindar ese parque, el Gobierno ha creado instrumentos como la Ley de Vivienda y la Empresa Pública de Vivienda y Suelo, que va a garantizar que todos los recursos del Estado que puedan convertirse en un hogar tengan esa finalidad y no otra.

Más viviendas y suelo para alquiler asequible

La ministra ha agregado que, mientras se desarrollan las promociones que resuelvan "esta emergencia habitacional", son necesarias medidas extraordinarias para disponer en el menor tiempo posible de esas viviendas. Con ese objetivo, el Consejo de Ministros ha aprobado transmitir los activos de la SAREB, la sociedad que se creó en el año 2012 para gestionar los activos problemáticos de entidades de depósito afectadas por la crisis financiera e inmobiliaria, a la entidad pública empresarial SEPES, en vías de convertirse en la Empresa Estatal de Vivienda y Suelo de la Administración General del Estado.

De esta manera, se incorporan viviendas para alquiler asequible al parque público y se reparan "las secuelas derivadas de la anterior crisis financiera, del uso de estas viviendas procedentes de los desahucios de las familias para pagar el rescate financiero", en palabras de la titular de Vivienda. Se trata de uno de los anuncios realizados por el presidente del Gobierno a comienzos de este año: ofrecer a la ciudadanía esas viviendas en forma de alquiler asequible, es decir, que se sitúen por debajo del precio del mercado y, en ningún caso, superen el 30% de los ingresos de las familias. "En definitiva, se trata de destinar aquello que un día sirvió para rescatar a los bancos a rescatar a las familias".

Vivienda y Agenda Urbana ha evaluado todos los suelos e inmuebles propiedad de la SAREB para determinar cuáles podían ponerse a disposición de los ciudadanos lo antes posible. En total, son unas 40.000 viviendas y unos 2.400 suelos donde podrían construirse otras 55.000. El valor estimado de la operación es de 5.900 millones de euros.

Los criterios empleados han sido, en primer lugar, geográficos: aquellos lugares donde más se precisa vivienda en alquiler y a precios asequibles; también se han priorizado las zonas declaradas tensionadas y las afectadas por la DANA. Se ha tenido en cuenta, igualmente, la dimensión de las viviendas y las condiciones técnicas y de habitabilidad en que se encuentran los inmuebles.

La titular de Vivienda ha recordado que la tarea de construir un parque de viviendas asequibles comenzó con terrenos de titularidad del Ministerio de Defensa, para lo que se estableció una consignación presupuestaria importante. Un segundo acuerdo del Consejo de Ministros de hoy ha consistido, precisamente, en habilitar a la empresa pública para que pueda usar esos recursos, que suman 593 millones de euros.

También en el ámbito de la vivienda, se ha subrayado que comienza a aplicarse el registro único de alquileres de corta duración, necesario para la comercialización de los alojamientos turísticos o los contratos temporales o de habitaciones. El fin es ofrecer garantías a la ciudadanía y, sobre todo, impedir el fraude y poner coto a los alojamientos turísticos ilegales que están impidiendo el acceso de tantas familias a la vivienda, que ha reiterado la necesidad de que todas las administraciones se impliquen en las políticas públicas de vivienda.

Futura Ley de Consumo Sostenible

El Consejo de Ministros ha abordado el Anteproyecto de Ley de Consumo Sostenible, presentado por el ministro de Derechos Sociales, Consumo y Agenda 2030, como una norma "ambiciosa" que entronca con los Objetivos de Desarrollo Sostenible y el Pacto Verde Europeo; además, concreta los preceptos constitucionales sobre la protección de la salud y los consumidores y el derecho a disfrutar de un medio ambiente adecuado.

El primer pilar de la ley tiene que ver con el 'ecopostureo', la construcción de imágenes de marca referentes a la sostenibilidad de los bienes o servicios que se ofertan que no están basadas en datos contrastables o en prácticas reales. En transposición de una directiva europea, el texto establece un sistema para certificar de manera objetiva ese tipo de valoraciones sobre las cualidades o virtudes de un producto.

La lucha contra la obsolescencia programada, la reducción intencional de la vida útil de productos como los electrodomésticos, constituye el segundo pilar de la norma. Se prohíbe, por ejemplo, inducir a la sustitución de elementos de un bien antes de que sea necesario y afirmar que el uso de recambios que no sean proporcionados por el productor puede afectar al funcionamiento de un bien cuando esto no es verdad. Igualmente, se regulan las actualizaciones de software; por ejemplo, se obliga a informar de que una actualización impedirá abrir ciertos programas o perjudicará al funcionamiento de un equipo.

La promoción de la sostenibilidad constituye el tercer elemento central del texto. "Intervenir sobre el etiquetado de los bienes y productos para poder identificar aquellos que tengan una garantía superior a dos años".

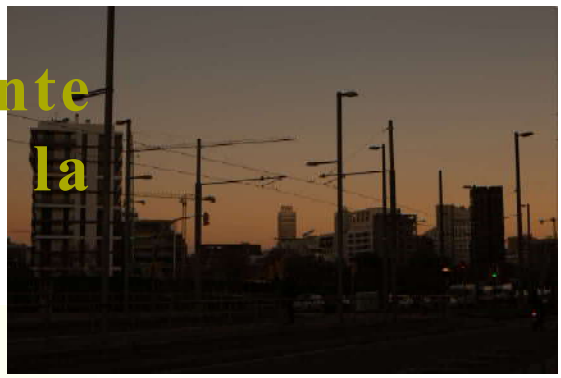
Derecho a reparar y transición hacia modelos más sostenibles

El cuarto pilar de la ley consagra el derecho a reparar. Los repuestos para un producto tendrán que estar disponibles hasta diez años después de que deje de fabricarse, se amplía el plazo de garantía de un bien cuando este se repare, y los productores asumirán una parte del coste de las reparaciones.

La norma, por último, fortalece la garantía de los derechos de los consumidores y fomenta la transición hacia modelos productivos más sostenibles. Entre otros muchos aspectos, se regula la publicidad que explota el miedo como emoción principal; se obliga a indicar de manera clara que se ha alterado el peso del contenido o el número de envases de un producto sin modificar su precio; se prohíbe la reventa de entradas para espectáculos por un precio que sea superior al de la venta original más el IPC, y se veta la publicidad de los vuelos cortos, los combustibles sólidos y los vehículos más contaminantes.

Se ha remarcado que la filosofía que inspira el texto es "reconocer que la transición ecológica e industrial no puede recaer sobre una suma de responsabilidades individuales", sino que hay que "responsabilizar al sistema económico en su conjunto y transformar los modos de producción, de distribución y de consumo". El ministro ha abogado por asegurar que el acceso a un consumo sostenible y al bienestar en tiempos de cambio climático "no sea una cuestión de clase social o de capacidad de renta, sino un derecho universalmente garantizado".

España lidera el repunte de la construcción en la UE en el último año



La producción de la construcción en España creció un 14,7% en abril de 2025 en términos interanuales, frente al 2,5% de la UE o al 3% de la eurozona.

España vuelve a colocarse al frente de la producción del sector de la construcción.

Según los datos de Eurostat, la oficina de estadísticas comunitaria, la actividad de la construcción en la eurozona subió un 1,7% en abril de 2025, tras dejarse un 0,2% en marzo, mientras que en el conjunto de la Unión Europea creció un 1,4%, frente al descenso del 0,3% registrado el mes anterior.

Entre los países sobre los que se disponen cifras, los mayores aumentos mensuales se registraron en Hungría (5,3%), España (4,3%) y Eslovenia (4%), al tiempo que los principales descensos se observaron en República Checa (-5%), Dinamarca (-0,9%) y Polonia (-0,8%).

Abril 2025 | Producción de la construcción en la UE

Variación mensual e interanual de los países con datos disponibles

País	Variación mensual (%)	Variación interanual (%)
UE-27	1.4	2.5
Eurozona	1.7	3.0
Bélgica	1.8	6.6
Bulgaria	-0.6	7.0
R. Checa	-5	1.9
Dinamarca	-0.9	0.4
Alemania	1.4	0.3
Irlanda	nd	nd
España	4.3	14.7
Francia	0.7	-0.5
Croacia	nd	nd
Italia	nd	nd
Luxemburgo	nd	nd
Hungría	5.3	-0.5
Países Bajos	1.2	-0.6
Austria	1.2	2.3
Polonia	-0.8	-4.3
Portugal	3.5	0.3
Rumania	2	-0.4
Eslovenia	4	-5.9
Eslovaquia	-0.4	-2.1
Finlandia	-0.1	5.8
Suecia	-0.4	1,0
Noruega	0.1	-2.3

En comparación con abril del año pasado, la actividad actual de la construcción en la zona euro fue tres puntos superior, mientras que, en los Veintisiete, la lectura estuvo un 2,5% por encima de los niveles de entonces.

En concreto, la construcción se anotó las mejoras interanuales más destacadas en España (14,7%), Bulgaria (7%) y Bélgica (6,6%). De su lado, las disminuciones más abultadas se dieron en Eslovenia (-5,9%), Polonia (-4,3%) y Eslovaquia (-2,1%).

INFORMACIÓN *de Actualidad*

Cómo afecta la nueva clasificación CNAE-2025 a tu empresa

El Real Decreto 10/2025, publicado en el BOE, aprobó hace meses la nueva Clasificación Nacional de Actividades Económicas 2025 (CNAE-2025).

Esta actualización, que no se realizaba desde el año 2009, responde a la necesidad de **incorporar nuevos códigos** para sectores cada vez más relevantes, especialmente aquellos relacionados con la digitalización.

Sin embargo, hay una cuestión que desde su publicación ha tomado por sorpresa a muchas asesorías y despachos profesionales: es **obligatorio comunicar** los nuevos códigos a los sujetos responsables de la obligación de ingresos de cuotas.

Empresas y autónomos debían actualizar los **códigos CNAE antes del 30 de junio de 2025.**

¿Qué son los códigos CNAE?

Los códigos CNAE son un sistema utilizado en España para clasificar las actividades económicas que realizan las empresas y los autónomos.

Este sistema **facilita la organización y clasificación de las actividades,** lo que permite a las administraciones públicas y organismos gestionar y controlar de manera más eficiente las actividades económicas del país.

Una de las funciones más importantes de los códigos CNAE es su uso por parte de la Seguridad Social, ya que estos códigos permiten determinar las bases de cotización y las tarifas de primas por accidentes de trabajo y enfermedades profesionales, según el nivel de riesgo asociado a cada actividad económica.

Además, el sistema CNAE facilita la gestión y actualización de los registros administrativos de la TGSS garantizando la precisión y la organización de los datos.

Los códigos CNAE constan de la siguiente estructura:

Sección: se trata del nivel más general y está representado por una letra.
División: es un nivel un poquito más específico y se compone de dos dígitos.
Grupo: supone un tercer dígito.
Clase: se compone de cuatro dígitos.

¿Por qué se actualizan los códigos CNAE?

Los códigos CNAE se han actualizado **para reflejar los avances científicos, tecnológicos y estructurales que están impactando en el mercado laboral.**

A medida que surgen nuevas actividades económicas, especialmente aquellas relacionadas con la transformación digital y el medio ambiente, se ha considerado necesario crear nuevos puestos de trabajo que necesitan ser clasificados adecuadamente.

Por ello, la actualización de los códigos CNAE tiene como **objetivo adaptarse a estas nuevas realidades del mercado permitiendo una mejor organización y gestión de las actividades económicas.**

De esta forma, se facilita la afiliación a la Seguridad Social y se asegura que todos los sectores emergentes y en crecimiento estén correctamente representados en el sistema.

¿Cómo es el CNAE-2025?

El CNAE-2025 mantiene la **estructura de 99 grupos** en los que se clasifican las actividades económicas, pero con una serie de novedades que permiten una mayor precisión y adaptación a las realidades actuales del mercado.

Entre las principales actualizaciones se incluyen nuevas actividades económicas y modificaciones en los grupos existentes.

Algunos de los cambios más destacados son:

Nuevas clases profesionales: se han incorporado actividades específicas como las relaciones públicas y la comunicación, que reflejan el auge de los sectores relacionados con la digitalización.

Incorporación de nuevos sectores: También se han añadido nuevas actividades, por ejemplo, de promoción inmobiliaria, adaptándose a las necesidades de un mercado inmobiliario más dinámico y enfocado en nuevas formas de inversión y comercialización.

¿Cuándo se deben actualizar los códigos CNAE?

La actualización de los códigos CNAE se debe realizar en función de cuándo se haya registrado la actividad:

Registros comunicados antes del 16 de enero de 2025: los sujetos responsables tenían hasta, 30 de junio de 2025, para actualizar sus códigos al formato CNAE-2025.

Registros comunicados a partir del 16 de enero de 2025: las nuevas incorporaciones deberán incluir la nueva codificación CNAE-2025 en el momento de su registro.

Así viene recogido en la Disposición adicional única sobre la obligación de comunicación de la codificación de la actividad económica, que señala también que:

Los sujetos responsables indicados en los párrafos anteriores deberán comunicar, igualmente, la codificación de la variable actividad económica según la CNAE-2009 para el periodo de tiempo que transcurra entre la entrada en vigor de este real

decreto y la entrada en vigor de la legislación de la Seguridad Social que establezca la tarifa de primas para la cotización al sistema de la Seguridad Social por accidentes de trabajo y enfermedades profesionales adaptada a la CNAE-2025.

Por tanto, es importante que las asesorías estén al tanto de esta modificación para asegurar que las actividades de sus clientes estén correctamente registradas según las nuevas disposiciones.

¿Deben todas las empresas comunicar el nuevo código CNAE 2025?

Según el Boletín RED 2/2025 las empresas deberán comunicar el código CNAE-2025 correspondiente a cada Código de Cuenta de Cotización (CCC) afectado.

Para facilitar este proceso en el mes de marzo se habilitó una nueva funcionalidad en el Sistema RED que permite:

- Consultar los posibles códigos CNAE-2025 aplicables a cada CCC, según su actual CNAE-2009.

- Seleccionar el código CNAE-2025 correcto dentro de las opciones disponibles.

Casos en los que SÍ es obligatorio comunicar el CNAE-2025

En estos casos es obligatorio comunicarlo:

. CCC en alta a 3 de marzo de 2025: se habilitó la funcionalidad para elegir el código CNAE-2025 aplicable.
. CCC asignados o que reinicien actividad a partir del 4 de marzo de 2025: es obligatorio comunicar tanto el código CNAE-2009 como el CNAE-2025.
. CCC con un código CNAE-2009 que se desglosa en varios CNAE-2025: la empresa debe informar a la TGSS del código CNAE-2025 correspondiente.

Casos en los que NO es necesario comunicar el CNAE-2025

Si el código CNAE-2009 de un CCC se corresponde con un único CNAE-2025 la TGSS lo asignará automáticamente, sin necesidad de comunicación por parte de la empresa.

¿Cómo puedo conocer el código CNAE de mi empresa?

Existen varias formas de averiguarlo:

1. Consultando en la Agencia Tributaria.

En este caso, será necesario acceder a la web de la Agencia Tributaria y seleccionar «Informaciones y gestiones» para poder ver el código CNAE según la actividad declarada.

2. A través del buscador de códigos CNAE.

También es posible usar buscadores en línea para introducir una descripción de la actividad de tu empresa y obtener el código correspondiente.

3. Mediante CodIA del INE.

El INE ha creado una herramienta específica llamada CodIA en la que es necesario introducir la descripción de la actividad para que la herramienta sugiera el código CNAE más adecuado.

¿La TGSS informa sobre los CCC que requieren la comunicación del nuevo código CNAE 2025?

Sí, en las ultimas semanas de febrero la TGSS envió un correo electrónico a cada Autorización RED con un enlace para acceder a una base de datos en formato Excel.

¿Qué información incluía?

Para los CCC cuya CNAE 2009 correspondiera con un único valor en la CNAE 2025:
Se envió un Excel con la relación de estos CCC.
No es necesario realizar ninguna comunicación, ya que la TGSS asigna automáticamente el nuevo código CNAE 2025.

Para los CCC cuya CNAE 2009 se desglosa en varios códigos CNAE 2025:
Se envió un Excel con la relación de estos CCC.
Se incluye la información de los posibles valores CNAE 2025 para que la empresa realice la comunicación obligatoria antes del 30 de junio de 2025.

Es muy importante que las empresas y las asesorías revisen estos emails y realicen las gestiones necesarias.

¿Cuáles son las ventajas de la actualización de los códigos CNAE?

Las ventajas son las siguientes:

Mayor claridad y precisión: Antes era complicado determinar qué códigos CNAE correspondían a ciertos sectores, lo que generaba incertidumbre. Con la nueva actualización se incluyen nuevas actividades económicas, lo que facilita la clasificación de sectores emergentes, especialmente los relacionados con la digitalización y el medioambiente.

Adaptación a la realidad económica: El nuevo CNAE refleja mejor los avances científicos y tecnológicos y los cambios en el mercado laboral, permitiendo a las empresas y autónomos mantenerse actualizados con las tendencias y necesidades actuales.

¿Cuáles son las desventajas de la actualización de los códigos CNAE?

En cuanto a las desventajas destacan:

Plazo limitado para actualizar: Aunque se ha tenido hasta el 30 de junio de 2025, para realizar la actualización, el proceso sigue siendo manual. Este tiempo ha podido resultar escaso para empresas que necesitasen realizar ajustes en varios registros.

Falta de automatización: Actualmente, todo el proceso de actualización se debe realizar manualmente, lo que puede ser tedioso y propenso a errores. Sería ideal poder automatizar este proceso para facilitar la gestión de los cambios.

Dudas sobre la coincidencia con el IAE: Un tema importante que está generando confusión es si los nuevos códigos CNAE coincidirán con los códigos del Impuesto de Actividades Económicas (IAE). Si no coinciden, esto podría implicar la necesidad de modificar las escrituras sociales de las empresas, lo que podría ser un proceso complejo. Por el momento, debemos esperar más instrucciones de la TGSS para resolver esta cuestión.

¿Cuál es la diferencia entre CNAE e IAE?

La CNAE es un sistema de clasificación que categoriza las actividades económicas desarrolladas en España con fines estadísticos y cuyo uso es obligatorio.

Por su parte, el IAE o Impuesto de Actividades Económicas es un tributo que grava el desarrollo de actividades económicas y afecta a las empresas cuyo importe neto de la cifra de negocios sea igual o superior a 1 millón de euros.

FORMACIÓN CONTINUADA DEL
~ MEDFIN ~
~ MEDIADOR FINANCIERO ~

El ciberriesgo se puede definir como la combinación de la probabilidad de ocurrencia de ciberincidentes, esto es, eventos que comprometan la confidencialidad, la integridad o la disponibilidad de la información y/o los sistemas de información, sean producto de actividad maliciosa o no, con su impacto[1].

Estos eventos son cada vez más relevantes para el conjunto del sistema financiero y para otros sectores productivos, debido al avance en el proceso de digitalización de la economía y la sociedad[2].

Además, debido a las interconexiones financieras y tecnológicas, los ciberincidentes pueden propagarse rápidamente entre bancos, entidades no bancarias e infraestructuras del mercado financiero, con potenciales implicaciones para la estabilidad financiera. La dependencia de servicios críticos proporcionados por terceros supone nuevas vulnerabilidades y riesgos de concentración dentro del sistema financiero.

En este contexto, los reguladores y supervisores prudenciales están prestando una atención prioritaria a estos riesgos e impulsando distintas iniciativas para aumentar la resiliencia de las entidades financieras frente a los mismos, esto es, para reforzar su ciberresiliencia. La iniciativa de las autoridades refuerza los incentivos, ya de por sí, elevados de las entidades financieras para invertir en recursos tecnológicos, no sólo para proteger sus datos, sino también la integridad de la provisión de servicios a sus clientes.

Entre las iniciativas de las autoridades europeas destacan la aprobación reciente del Reglamento DORA (Digital Operational Resilience Act, por sus siglas en inglés)[3], la Directiva NIS2 sobre ciberseguridad[4], los trabajos en curso para responder a la recomendación de la Junta Europea de Riesgo Sistémico (JERS) sobre la coordinación en caso de ciberincidentes sistémicos y las pruebas de resistencia con fines de supervisión de la resiliencia de los bancos frente a los ciberataques por parte del Mecanismo Único de Supervisión en 2024.

El resto del capítulo se organiza de la siguiente forma. El epígrafe T1 analiza los conceptos de ciberriesgo y de ciberresiliencia en el contexto de digitalización del sistema financiero. El epígrafe T2 describe la frecuencia e impacto creciente de los ciberriesgos. Ambas secciones recogen datos públicos sobre los ciberriesgos, sujetos a múltiples limitaciones. El epígrafe T3 recoge las distintas iniciativas de las propias entidades financieras y de las autoridades micro- y macroprudenciales, y de otros ámbitos, para reforzar la ciberresiliencia. El epígrafe T4 concluye con posibles perspectivas de evolución de los ciberriesgos, por ejemplo, en relación con el efecto del desarrollo de la inteligencia artificial, y de las herramientas de las entidades y las autoridades para contenerlos, que tendrán que poner el énfasis en la disposición de los recursos tecnológicos adecuados, además de los recursos financieros utilizados para absorber pérdidas operacionales.

1 Véase el Cyber-Lexicon del Financial Stability Board (FSB, por sus siglas en inglés) para una definición de terminología de relevancia para los ciberriesgos.

2 Véase el Informe de la Comisión Europea del 24 de enero de 2024.

3 Véase el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 y (UE) 2016/1011.

4 Directiva UE 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

Los ciberriesgos y el sistema financiero

El sistema financiero como ecosistema

El sistema financiero constituye un sistema muy complejo, formado por numerosos participantes intensamente interconectados y dependientes entre sí. Este sistema incluye las infraestructuras de mercado, los distintos tipos de entidades financieras (bancarias y no bancarias) y sus principales proveedores de servicios tecnológicos, y el conjunto de las autoridades supervisoras de todos ellos. Las entidades financieras presentan tanto interconexiones directas a través de sus activos y pasivos, como indirectas, al invertir o financiarse con el mismo tipo de instrumentos (véase el epígrafe 2 del capítulo 2 de este IEF).

Adicionalmente, existen numerosas interconexiones operativas entre los participantes del sector, a través de las infraestructuras de mercado, los proveedores de servicios comunes e incluso la prestación de servicios entre entidades financieras.

Estas interconexiones entre entidades y otras características del sistema financiero hacen que el impacto de los ciberriesgos pueda llegar a poner en peligro la estabilidad financiera[5].

La materialización de ciberincidentes puede así afectar no solamente a cada participante individual, sino también extenderse y amplificarse con implicaciones sistémicas para el conjunto del sector. Además de las interconexiones, otras características relevantes del sistema financiero para valorar los ciberriesgos incluyen su fuerte dependencia de la tecnología, su atractivo para atacantes con distintas motivaciones (por ejemplo, económicas y políticas) y una gran sensibilidad a la pérdida de la confianza de sus participantes[6].

Las entidades financieras complementan sus capacidades tecnológicas mediante distintas relaciones con otros agentes. Estas incluyen la contratación de servicios de proveedores, la participación en consorcios, inversiones en start-ups o adquisiciones de productos de terceros.

En muchos casos, la oferta de servicios tecnológicos está fuertemente concentrada en un número relativamente pequeño de proveedores, en particular en el caso de los relacionados con la computación en la nube[7]. De hecho, algunos de estos proveedores han pasado a ser elementos vertebradores para el sistema financiero, a un nivel comparable al de las infraestructuras de mercado. Por ejemplo, en el segmento de computación en la nube, tres empresas representan más del 60% de cuota de mercado[8] y su fallo simultáneo podría tener consecuencias operativas adversas a nivel sistémico. Constituyen, por tanto, puntos únicos de fallo, dado que los incidentes que les afectan, incluso los no intencionados, tienen impacto en el conjunto del sector. Más aún, muchos de estos proveedores prestan sus servicios también a compañías de otros sectores, pudiendo llegar a ser críticos para la economía de un país en su conjunto o incluso de un grupo de países.

Identificar todas las interdependencias existentes en el sector es un reto complejo. Las entidades financieras tradicionales se conectan entre ellas y a las infraestructuras de mercado, existen nuevos actores que ofrecen servicios financieros (por ejemplo, fintech)[9] y hay una creciente dependencia de los proveedores tecnológicos directos. Pero, además, existen otras dependencias de terceros no debidamente identificadas, producidas por las subcontrataciones sucesivas a lo largo de las cadenas de contratación de productos y servicios tecnológicos, sobre las que las entidades financieras tienen escaso o ningún control. Esto ha llevado a que iniciativas como el toolkit del FSB[10] sobre gestión de riesgos de terceros o el Reglamento DORA de la Unión Europea (UE), analizado en más detalle en el epígrafe T3, hayan puesto el foco en estas dependencias.

8 Ting Yang Koh and Jermy Prenio (2023). Managing cloud risk – some considerations for the oversight of critical cloud service providers in the financial sector. FSI Insights on policy implementation No 53.

9 El FSB define fintech como «innovación financiera facilitada por la tecnología que podría resultar en nuevos modelos de negocio, aplicaciones, procesos o productos con un efecto material asociado sobre los mercados financieros y las instituciones, y la provisión de servicios financieros». Las empresas que hacen uso de estas innovaciones tecnológicas son comúnmente designadas también por el mismo término.

10 Véase el informe del FSB Enhancing third-party risk management and oversight – a toolkit for financial institutions and financial authorities, del 4 de diciembre de 2023.

Transformación digital y exposición al ciberriesgo

El sistema financiero está fuertemente digitalizado y las entidades financieras dependen de su tecnología no solo para desarrollar el negocio, sino como un factor diferencial y competitivo. En los últimos años, el proceso de transformación digital se ha acelerado extraordinariamente[11], tanto para mejorar la eficiencia de los procesos internos de las entidades financieras como para ofrecer a sus clientes servicios flexibles, personalizados y accesibles de forma inmediata, desde cualquier lugar y con distintos tipos de dispositivos[12]. Este fenómeno se ha visto reforzado por la aparición de nuevos competidores para las entidades financieras tradicionales, como son las bigtech[13] o las fintech, que pueden ofrecer soluciones muy atractivas de forma muy ágil e innovadora.

El elevado nivel de digitalización del sistema financiero incrementa su exposición al ciberriesgo. La mayor parte de las entidades financieras tienen entornos tecnológicos extraordinariamente complejos, donde conviven aplicaciones antiguas con otras que se apoyan en tecnologías más innovadoras, fruto no solo de los procesos de transformación, sino también, en algunos casos, de sucesivas fusiones y adquisiciones[14]. Esta complejidad supone un reto para las entidades a la hora de mantener un entorno de control adecuado y, por tanto, las hace más vulnerables, tanto a fallos en los sistemas como a ciberataques.

En este contexto, la pandemia del COVID-19 ha actuado como un acelerador, introduciendo cambios en el funcionamiento de las entidades financieras y en su relación con los clientes. Por ejemplo, el teletrabajo, que se mantiene estable en niveles superiores a los previos a la pandemia, ha traído consigo riesgos adicionales para las entidades y sus empleados, entre los que podemos citar los originados por los accesos a sistemas corporativos desde dispositivos personales y redes domésticas, y el manejo de datos confidenciales en los domicilios de los empleados. El acceso electrónico de los clientes a distintos servicios financieros se vio impulsado como consecuencia de las restricciones a la movilidad durante las fases iniciales de la pandemia, y parte de este impulso se ha conservado en el período posterior de normalización de relaciones sociales.

La ampliación de la oferta de servicios financieros a distancia ha aumentado la exposición de los clientes que los utilizan a ciberataques y fraudes. Se han observado crecimientos muy significativos en los casos de fraudes que utilizan ingeniería social, como el phishing[15], el smishing[16], y el vishing[17], acompañados de suplantación de sitios web y aplicaciones móviles, entre otros. A pesar de los esfuerzos de las entidades para mejorar la educación en ciberseguridad de sus clientes, algunos continúan siendo altamente vulnerables, especialmente aquellos que antes de la pandemia no hacían uso de los canales digitales.

Aunque algunos estudios sugieren que el financiero es uno de los sectores críticos mejor preparados frente a los ciberriesgos, existe una cierta heterogeneidad a nivel de entidades individuales. Si bien la mejor posición relativa del sector se debe en parte a su elevado grado de regulación y supervisión, en algunos casos las medidas de seguridad y los controles implementados por las entidades, especialmente en el caso de las más pequeñas, deben todavía mejorarse para gestionar adecuadamente los ciberriesgos.

11 Según el informe del Observatorio de la Digitalización Financiera FUNCAS – KPMG La digitalización como eje de transformación bancaria, la penetración de la banca digital en España pasó del 54,9% en 2019 al 69,6% en 2022, superando en casi 10 puntos porcentuales la media europea de 2022 de 59,7%. Asimismo, el informe destaca que el avance en la transformación digital fue una prioridad estratégica en 2022 para el 58% de las entidades, por delante de la mitigación de los efectos de la inflación que fue prioridad para el 53%.

12 Véase José Ramón Martínez Resano. (2022). Regulating for Competition with Bigtechs: Banking-As-A-Service and 'Beyond Banking'.

13 El FSB define bigtech como «grandes compañías tecnológicas con amplias redes de clientes establecidas».

14 Véase "Evolución de los principales grupos bancarios españoles (2009-2021)", del Banco de España.

15 Los ataques de phishing son aquellos en los que un atacante trata de conseguir información confidencial (contraseñas, datos bancarios, etc.) de usuarios legítimos de forma fraudulenta, recurriendo a la suplantación de la identidad digital de una entidad de confianza.

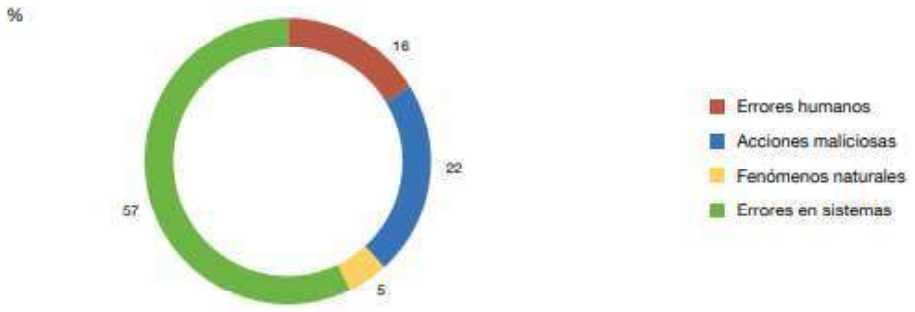
16 El smishing es una técnica que consiste en el envío de un SMS por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima con el objetivo de robarle información privada o realizarle un cargo económico.

17 El vishing es un tipo de estafa de ingeniería social por teléfono; a través de una llamada, se suplanta la identidad de una empresa, organización o persona de confianza, con el fin de obtener información personal y sensible de la víctima.

Gráfico T.1

Pese a ser responsables de los mayores impactos, los ciberincidentes con origen malicioso representan un porcentaje reducido del total de ciberincidentes reportados

T.1.a Causas de los ciberincidentes reportados a ENISA en Europa entre 2013 y 2023



Eventos no maliciosos y ciberataques

El concepto de ciberincidente va más allá de los ciberataques. Conviene destacar que la propia definición de ciberincidente del Cyber Lexicon del FSB (véase nota al pie 1) remite tanto a los de naturaleza maliciosa, causados por ciberataques, como a los no maliciosos.

Estos últimos, que incluyen eventos provocados por desastres naturales (por ejemplo, terremotos), errores humanos o fallos accidentales en los sistemas, también pueden afectar a la capacidad de las entidades y del sector en su conjunto para seguir operando con normalidad, por lo que la resiliencia frente a estos ciberincidentes es igualmente relevante.

Es importante destacar las diferencias en términos de la frecuencia e impacto de los distintos tipos de ciberincidentes. Analizando las principales causas de los ciberincidentes de todos los sectores que se reportan anualmente a la Agencia de la Unión Europea para la Ciberseguridad (ENISA, por sus siglas en inglés), se observa que los no maliciosos, como fallos en los sistemas o errores humanos, son los más comunes18 (véase gráfico T.1). A pesar de su prevalencia, estos incidentes no tienen, en la mayoría de las ocasiones, un

impacto relevante ni a nivel individual ni a nivel sistémico. Son los ciberincidentes maliciosos, que representan en torno al 22% del total, los que tienen un mayor impacto.

La propia naturaleza de los ciberincidentes maliciosos y su intencionalidad explican su mayor impacto a pesar de su menor frecuencia. En la mayoría de los casos se trata de ataques diseñados para causar el mayor impacto posible en sus víctimas; por ejemplo, paralizando sus operaciones o robando datos confidenciales. A esto hay que sumar la posibilidad de aumentar el alcance y el impacto que, en algunos casos, tienen los atacantes: de un único usuario a un grupo más amplio de una o más entidades. También contribuyen al mayor impacto los efectos a largo plazo de este tipo de incidentes, como el daño reputacional.

18 En este gráfico y en el resto incluidos en el capítulo temático, se ha utilizado la mejor aproximación basada en información pública para ilustrar distintos hechos estilizados relevantes relacionados con los ciberriesgos. Estas aproximaciones afrontan importantes limitaciones en cuanto a la cantidad y calidad de datos disponibles. Los supervisores disponen de datos confidenciales muy superiores. La elevada prioridad del ciberriesgo en la agenda regulatoria y supervisora hace esperar una mayor disponibilidad futura de datos agregados publicables.

De la ciberseguridad a la ciberresiliencia

El concepto de ciberseguridad tiene un alcance bien delimitado. El Cyber Lexicon del FSB define la ciberseguridad como la preservación de la confidencialidad, integridad y disponibilidad de la información y/o los sistemas de información en un medio interconectado.

Estamos, por tanto, ante un concepto fundamentalmente preventivo y de protección. Sin embargo, la evolución hacia un mundo completamente digital en el que las ciberamenazas son cada vez más frecuentes y sofisticadas hace necesario un cambio de paradigma, asumiendo como hipótesis de trabajo que en algún momento se producirá un ciberincidente con impacto.

El concepto de ciberresiliencia surge como evolución del concepto de ciberseguridad.

El Cyber Lexicon del FSB define la ciberresiliencia como la capacidad de una organización para continuar llevando a cabo su misión, anticipándose y adaptándose a las ciberamenazas y a otros cambios relevantes en su entorno, resistiendo, conteniendo y recuperándose rápidamente ante ciberincidentes.

A su vez, la ciberresiliencia se puede generalizar como resiliencia operacional u operativa. El Comité de Supervisión Bancaria de Basilea (BCBS, por sus siglas en inglés), en sus Principles for Operational Resilience[19], definió la resiliencia operacional como la capacidad de un banco para mantener sus operaciones críticas en situaciones adversas, definición que podría aplicarse no solo a bancos, sino también a todo tipo de compañías privadas e instituciones públicas dentro y fuera del sistema financiero. Este es un enfoque más holístico, que no se centra exclusivamente en gestionar la tecnología, sino que concede la misma importancia a las personas y a los procesos de las organizaciones y enlaza con disciplinas ya existentes, como la continuidad de negocio.

19 Véase el informe del BCBS Principles for Operational Resilience de marzo de 2021.

La relación entre el ciberriesgo y los riesgos económico-financieros

Nivel individual

Los eventos de ciberriesgo pueden tener un impacto individual significativo en el ámbito operativo, pero también más allá de este. En un entorno fuertemente digitalizado, la tecnología se convierte en un factor transversal a toda la actividad del negocio, por lo que el ciberriesgo puede tener impacto en otros riesgos, como el legal, el reputacional o los riesgos financieros clásicos.

Los ciberincidentes pueden llegar a generar un impacto importante sobre la reputación de una entidad. La indisponibilidad de los servicios o las vulneraciones de la confidencialidad o la integridad de la información en poder de las entidades financieras pueden tener un impacto en la confianza de los clientes y del mercado en general, tanto si son eventos maliciosos como si son accidentales. Estos impactos reputacionales pueden verse agravados si no hay una gestión adecuada de la comunicación pública cuando se producen los ciberincidentes.

Estimado/a Lector/a:

En esta sección de nuestro Boletín Oficial, denominada **«Formación»** desarrollamos aquellos temas que consideremos de interés profesional para la actualización y formación continuada de nuestros Colegiados. El desarrollo de los temas expuestos en esta sección variará según su extensión y contenido, por lo cual algunos de ellos serán expuestos durante varias ediciones del Boletín, mientras que otros comenzarán y finalizarán en una misma edición.

En este número de nuestra publicación, correspondiente a los meses de Julio/Agosto de 2025, comenzamos con el desarrollo del tema **«Ciberriesgos»**. Continuaremos con el desarrollo de este nuevo tema en la próxima edición de nuestro Boletín correspondiente a los meses de Septiembre/Octubre de 2025. Esperamos que el tema desarrollado haya sido de su interés y agrado.

Cuestionario Formativo

A continuación facilitamos algunas preguntas básicas en referencia al «Área de Formación Continuada».

La contestación de las mismas le permitirá saber si ha fijado los conceptos básicos formativos en esta materia. Para la comprobación de las respuestas correctas puede consultar la página 23 de nuestro Boletín Oficial.

1.- Se define el ciberriesgo como:

a) la combinación de probabilidad de ocurrencia de ciberincidentes, es decir, hechos que comprometan la confidencialidad, la integridad o la disponibilidad de la información o de los sistemas informativos, sena o no producto de actividad maliciosa con su impacto.
b) las numerosas interconexiones operativas entre los participantes del sector, a través de las infraestructuras de mercado, los proveedores de servicios comunes e incluso la presatación de servicios entre entidades financieras.
c) las capacidades tecnológicas como la contratación de servicios de proveedores, la participación de consorcios, las inversiones en start-ups o las adquisiciones de productos de terceros.

2.- El sistema financiero está altamente digitalizado, por lo que las entidades financieras dependen de su tecnología para:

a) prestar sus servicios a compañías de otros sectores .
b) desarrollar el negocio, así como un factor diferencial y competitivo.
c) comparar las infraestructuras de mercado.

3.- La ciberseguridad tiene un alcance delimitado. Se define como:

a) la capacidad de una organización para seguir llevando a cabo su misión, anticipándose y adaptándose a las ciberamenazas y a otros cambios relevante de su entorno.
b) la capacidad de una entidad financiera para mantener sus operaciones críticas en situaciones adversas.
c) la preservación de la confidencialidad, integridad y disponibilidad de la información o los sistemas de información en un medio interconectado.

Consultorio Formativo

Sección dedicada a responder desde un punto de vista formativo y práctico, cuestiones variadas de actualidad, surgidas por dudas y consultas planteadas en el ejercicio de la actividad de nuestros profesionales.

Pregunta

¿Qué son los productos híbridos?

Respuesta

Se trata de productos que, por su naturaleza, no pueden clasificarse como renta fija, ni tampoco como renta variable, de ahí su carácter híbrido.

Tienen algunos aspectos asimilables a la renta fija y otras características propias de la renta variable. Los principales productos de este tipo son las participaciones preferentes y las obligaciones y bonos convertibles.

Pregunta

¿Qué son los productos derivados?

Respuesta

Los productos derivados son instrumentos financieros cuyo valor deriva de la evolución de los precios de otro activo, denominado activo subyacente. El activo subyacente puede ser muy

variado: una acción, una cesta de acciones, un valor de renta fija, una divisa, un tipo de interés, un índice bursátil, una materia prima y productos más sofisticados o incluso la inflación o los riesgos de crédito. Un derivado es una contratación a plazo en la que se establecen todos los detalles en el momento del acuerdo, mientras que el intercambio efectivo se produce, en su caso, en un momento futuro.

Pregunta

¿Qué son los productos estructurados?

Respuesta

Los productos estructurados consisten en la unión de dos o más productos financieros en una sola estructura. Normalmente, lo más común suele ser un producto de renta fija junto con uno o más derivados. Estos productos son de carácter complejo y de elevado riesgo.

Pregunta

¿Qué es "fintech"?.

Respuesta

El término fintech procede de las palabras en inglés Finance and Technology y hace referencia a todas aquellas actividades que impliquen el empleo de la innovación y los desarrollos tecnológicos para el diseño, oferta y prestación de productos y servicios financieros.

Desarrollan actividades fintech tanto entidades financieras ya establecidas como nuevas empresas que actúan en algún punto de la cadena de valor del servicio financiero.

Pregunta

¿Qué tipo de servicios y productos "fintech" existen?.

Respuesta

Entre los servicios y productos fintech se encuentran el asesoramiento y la gestión patrimonial automatizados, los servicios que ayudan a mejorar la gestión de las finanzas personales, la financiación participativa, los servicios de pago mediante dispositivos móviles o electrónicos, o la tokenización de activos, entre otros.

Respuestas correctas al cuestionario del Área de Formación Continuada

1.- a
2.- b
3.- c

Pregunta

¿Qué es el "blockchain"?

Respuesta

Blockchain o cadena de bloques, es una base de datos distribuida en la que pueden registrarse todo tipo de transacciones directamente entre las partes (sin necesidad de intermediarios), permitiendo su trazabilidad. Al tener todos los participantes la misma información, no es posible alterarla sin el consenso de la red, por lo que se puede considerar como fiable. Blockchain tiene múltiples aplicaciones en diversos ámbitos y, en particular, en el ámbito financiero parece que permitiría transacciones inmediatas, gestionar la identidad y una mayor accesibilidad a productos y servicios financieros.

Pregunta

¿Qué es un "sandbox"?.

Respuesta

En el ámbito fintech, un sandbox es un espacio controlado de pruebas, cuya finalidad es que los promotores prueben, bajo el control de los supervisores financieros, nuevos modelos de negocio que aporten beneficios en el entorno financiero. Con ello se pretende acompasar el cumplimiento de la regulación financiera al crecimiento de las empresas fintech, de forma que no se impida su desarrollo con una regulación excesivamente restrictiva ni se disminuya la protección de los derechos de los consumidores.

AGRUPACIÓN TÉCNICA PROFESIONAL

DE

MEDIADORES FINANCIEROS TITULADOS

DE ESPAÑA

Miembro Colectivo de la
AGRUPACIÓN TÉCNICA PROFESIONAL

C./ Covarrubias, nº 22-1º-Derecha.- 28010 MADRID.- Telf. Corp.: 91 457 29 29
E-mail: medfin@atp-guiainmobiliaria.com
Web: www.atp-medfin.com