

Boletín Oficial



DE LA
AGRUPACIÓN TÉCNICA PROFESIONAL
DE
MEDIADORES FINANCIEROS TITULADOS DE ESPAÑA



MEDFIN
MEDIADORES FINANCIEROS
- Mediación en Finanzas, Préstamos, Valores.- EAFI -



SUMARIO

Actualidad Corporativa págs. 3-6

Deducción en el IRPF por cancelación de hipoteca tras venta de vivienda habitual. pag.3

El índice de referencia del INE para la actualización del alquiler sube en agosto al 2,19% pag.4

La inversión inmobiliaria en España crece un 42% interanual pag.5

La contratación de oficinas en Europa crece un 8% en el primer semestre de 2025... pag.6

Información de Actualidad págs. 7-12

La rentabilidad del alquiler en España pags.7-8

La inflación altera la percepción del valor y del dinero en hogares e inversiones pags.9-11

Previsión de incremento en las transacciones inmobiliarias pags.12-13

Formación Continuada págs. 14-23

Ciberriesgos pags.14-22

Cuestionario Formativo.- Formulación de preguntas referentes al Área de Formación Continuada..... pag.23

Respuestas correctoras correspondientes al Área de Formación Continuada. pág.13

La Agrupación Técnica Profesional de Mediadores Financieros Titulados de España ha adoptado las medidas y niveles de seguridad de protección del REGLAMENTO EUROPEO (UE) 2016/679. Los datos personales proporcionados por usted son objeto de tratamiento automatizado y se incorporan a un fichero titularidad de la Agrupación Técnica Profesional de Mediadores Financieros Titulados de España, que es asimismo la entidad responsable del mismo, inscrito en el Registro General de la Agencia Española de Protección de Datos. Usted podrá ejercitar los derechos de acceso, rectificación, cancelación y en su caso, oposición, enviando una solicitud por escrito, acompañada de la fotocopia de su D.N.I., dirigida a C. Gascó Oliag, nº10-1º-1ª, C.P. 46520 de Valencia. Para el caso de que quiera realizarnos alguna consulta o sugerencia lo puede realizar en la siguiente dirección de correo electrónico: medfin@atp-guiainmobiliaria.com

Ejemplar: Gratuito

Recepción: Periódica

Edición: MEDFIN

Imprime: Gráficas Alhorí

Pablo Vallecillos Carrillo

D.L.: V-3256-2011

E-mail: medfin@atp-guiainmobiliaria.com



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

Web: www.atp-medfin.com



ACTUALIDAD Corporativa

DEDUCCIÓN EN EL IRPF POR CANCELACIÓN DE HIPOTECA TRAS VENTA DE VIVIENDA HABITUAL

El Tribunal Económico-Administrativo Central (TEAC) ha establecido que los contribuyentes que vendan su vivienda habitual y utilicen el importe obtenido para cancelar la hipoteca podrán aplicar la deducción por inversión en vivienda habitual en el Impuesto sobre la Renta de las Personas Físicas (IRPF), siempre que la vivienda se haya adquirido antes del 31 de diciembre de 2012.



Hasta ahora, la Agencia Tributaria rechazaba esta posibilidad al considerar que, tras la venta, la vivienda dejaba de tener la condición de habitual. El TEAC corrige este criterio y aclara que lo relevante no es el origen del dinero utilizado, sino el destino del pago, es decir, la cancelación del préstamo vinculado a la vivienda habitual.

De este modo, los contribuyentes que cumplan los requisitos legales podrán incluir en la deducción las cantidades destinadas a cancelar el préstamo, con el límite anual de 9.040 euros establecido por la normativa.

CAMBIO 2025

Cómo reclamar la deducción por vivienda habitual tras vender tu casa



deducción IRPF al cancelar hipoteca tras vender vivienda

La resolución se basa en el caso de un contribuyente que vendió su vivienda en el año 2018 y canceló el préstamo el mismo día, aplicando la deducción en su declaración.

La Agencia Tributaria regularizó su situación e impuso una sanción, ahora anulada por el TEAC, que ordena la devolución de lo ingresado indebidamente y unifica el criterio para futuras actuaciones.

EL ÍNDICE DE REFERENCIA DEL INE PARA LA ACTUALIZACIÓN DEL ALQUILER SUBE EN AGOSTO AL 2,19%

Índice de referencia del alquiler

Tasas con las que se calcula

Tasa de variación anual del IPC
Tasa de variación anual de IPC subyacente
Tasa de variación anual media ajustada

Periodicidad y dónde se publica

Mensualmente en la web del INE

Contratos a los que aplica

Todos los contratos de arrendamiento de vivienda firmados tras la entrada en vigor de la Ley de Vivienda, en mayo de 2023

Quien y cómo se puede actualizar la renta

Si está indicado en el contrato
El propietario puede actualizar la renta una vez al año
Hay que avisar al inquilino con 30 días

El Instituto Nacional de Estadística (INE) ha publicado el índice de referencia para la actualización anual de los contratos de alquiler, que se situó en el 2,19% interanual en agosto de este año, frente al 2,15% del mes anterior, es el más alto desde enero de 2025 y representa además la tercera subida mensual consecutiva.

Eso significa que las rentas de alquiler que se revisen ahora podrán subir hasta un 2,19%, según establece dicho índice, que se aplica a los contratos firmados tras la entrada en vigor de la ley de vivienda, el 25 de mayo de 2023.

Desde que entró en vigor este índice de referencia de arrendamiento, las subidas han sido del 2,2 % para el mes de noviembre; del 2,28% en diciembre; del 2,19 % en enero; del 2,08% en febrero; del 1,98 % en marzo; del 2,09 % en abril; del 1,% en mayo; del 2,1 % en abril; del 2,15% en julio y del 2,19 % en agosto.



Índice de Referencia del Alquiler

Rango de valores de precio de alquiler

ORIENTATIVO

Todos los nuevos contratos

OBLIGATORIO

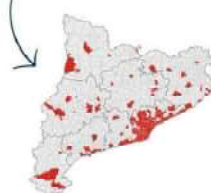
Todos los nuevos contratos en zonas de mercado residencial tensionado

- ¿Quiénes?
- Grandes tenedores
 - Grandes tenedores y pequeños propietarios de viviendas que no hayan estado arrendadas en los últimos 5 años

¿Dónde se aplica?

Zonas de mercado residencial tensionado actualmente en España

140 municipios de Cataluña



¿Dónde lo puedo consultar?

Web del Ministerio de Vivienda

<https://serpavi.mivau.gob.es>



VT L

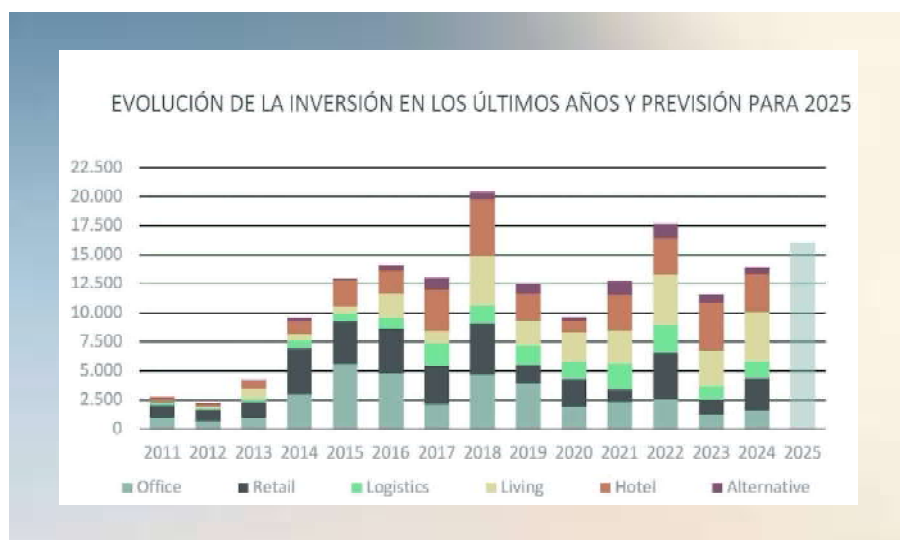
El mercado de inversión inmobiliaria mantiene su fortaleza en Europa, aunque con ritmos desiguales. Según un informe reciente, el volumen total de operaciones en el continente alcanzó unos 130.000 millones de euros en los tres primeros trimestres de 2025, lo que supone un aumento del 1,5 %. En España, sin embargo, la cifra se disparó hasta los 11.800 millones, un 42 % más interanual, mostrando la capacidad de atracción del país frente a la moderación europea.

El estudio sitúa a España entre los destinos más activos junto a los países nórdicos y del sur de Europa. Este impulso se concentra en segmentos como residencias de estudiantes y senior living, con operaciones relevantes, además de la reactivación del mercado de oficinas y el dinamismo de sectores hotelero, retail e industrial-logístico. Los datos cifran en 8.263 millones la inversión acumulada en el primer semestre de 2025, un 44 % más que el año anterior.

Los profesionales consultados prevén que el ejercicio cierre con un volumen cercano a 17.000 millones € en España, una de las mejores cifras de la última década. En el conjunto europeo, se anticipa un crecimiento del 7 % al cierre de 2025, impulsado por mercados resilientes y operaciones corporativas de gran tamaño. La inversión inmobiliaria sigue siendo un termómetro directo de la confianza empresarial y del atractivo de los activos físicos frente a la volatilidad financiera.

¿Por qué España mantiene un ritmo inversor superior a la media europea?

Los segmentos de residencial alternativo, especialmente estudiantes y senior living, concentran el mayor número de operaciones por rentabilidades y estabilidad de flujos. A ellos se suman la logística, que sigue en expansión, y el turístico, impulsado por la recuperación del consumo. Esta diversificación está sosteniendo la evolución del mercado y compensando la moderación en otros países europeos.



La contratación de oficinas en Europa crece un 8% en el primer semestre de 2025

La contratación de oficinas en Europa ha aumentado un 8% interanual durante el primer semestre de 2025. Este crecimiento ha estado liderado por el sector de servicios profesionales y empresariales, que ha representado el 26% del total, frente al 24% registrado en el mismo periodo de 2024.

Los profesionales inmobiliarios internacionales destaca que, este comportamiento refleja la resiliencia del sector, especialmente entre empresas usuarias dedicadas a actividades contra cíclicas en expansión, como despachos de abogados y firmas de auditoría.

Varios mercados europeos han registrado un crecimiento destacado de la contratación de oficinas por parte de empresas de servicios profesionales y B2B. Fráncfort es el que ha experimentado un mayor repunte, pasando del 21% al 32% de cuota por parte de este segmento de actividad, impulsado por el alquiler de 37.760 m² por parte de KPMG, mientras Ámsterdam lidera en términos proporcionales, con un 47% del total de contratación en su mercado gracias a la contratación de 44.000 m² por parte de UWV. En el CBD de París, los servicios profesionales también han superado los niveles históricos, alcanzando el 25% de la actividad, más del doble de su media de cinco años (12%). En Madrid, la actividad de este sector ha estado en línea con el periodo anterior, mientras en la Ciudad Condal destacan los más de 14.000 m² contratados por Deloitte.



El segundo sector más activo ha sido el de banca, seguros y finanzas, con un 20% del total de contratación de oficinas en Europa. Aunque supone un ligero descenso respecto al 22% de H1 2024, se mantiene muy por encima del 16% registrado en 2020, lo que indica una dinámica sostenida, respaldada por las políticas corporativas de asistencia a la oficina.

La tasa de disponibilidad en oficinas prime en los principales mercados europeos ronda el 3%. Las rentas prime han subido un 6,1% interanual en el segundo trimestre de 2025, mientras que los proyectos de nueva promoción siguen siendo limitados, acercándose a mínimos de la última década. Además, en activos no prime de menor tamaño, los propietarios están optando por la renovación para mejorar su comercialización.

La ubicación de las oficinas se ha vuelto cada vez más relevante para las compañías. Los usuarios priorizan zonas céntricas y bien conectadas y además buscan edificios de mayor calidad para reducir emisiones y atraer talento. Según el informe, las empresas están menos dispuestas a renunciar a estos factores, lo que ha intensificado la competencia por el espacio prime disponible en las ciudades europeas.



INFORMACIÓN *de Actualidad*



La rentabilidad del alquiler en España

El mercado del alquiler residencial en España sigue mostrando una clara tendencia al alza. Según un informe reciente, la rentabilidad bruta se situó en el 6,74 % en julio de 2025, lo que supone un incremento de setenta centésimas frente al mismo periodo del año anterior. Esta evolución refleja un escenario en el que los propietarios encuentran en el arrendamiento un refugio cada vez más atractivo, mientras los inquilinos se enfrentan a una oferta limitada y precios en ascenso.



**Rentabilidad
de alquiler**

El análisis revela que un propietario que adquirió una vivienda tipo de 90 m² por 216.810 euros, con una renta mensual media de 1.218 euros, obtuvo 14.623 euros brutos anuales. Estas cifras coinciden con las conclusiones del Banco de España sobre el mercado del alquiler residencial, donde se analizan los principales determinantes de la evolución del sector y los indicadores de esfuerzo para los hogares. La convergencia entre estadísticas privadas y fuentes oficiales refuerza la visión de un mercado tensionado en el que la rentabilidad supera ya el 7 % en varias capitales de provincia.

El ranking elaborado por profesionales del sector, muestra que Tarragona lidera con una rentabilidad del 8,07 %, seguida de Jaén (7,35 %), Ávila (7,10 %), Castellón de la Plana (7,05 %) y Córdoba (7,05 %). En el extremo opuesto, Donostia - San Sebastián presenta la rentabilidad más baja (3,67 %), seguida de Palma (4,35 %), Pamplona (4,59 %), Cádiz (4,60 %) y Málaga (4,63 %). Incluso grandes capitales como Madrid (5,03 %) y Barcelona (6,88 %) muestran rendimientos moderados, lo que confirma que la rentabilidad más elevada se concentra en ciudades medias y con precios de acceso más competitivos.

- Rentabilidad bruta del alquiler en España en julio de 2025: 6,74 %.
- Aumento de 70 centésimas respecto a julio de 2024 (6,04 %).
- Vivienda tipo: 90 m², precio medio 216.810 euros, renta mensual media 1.218 euros.
- Ingreso anual bruto medio: 14.623 euros.
- Rentabilidad más alta: Tarragona (8,07 %).
- Rentabilidad más baja: Donostia - San Sebastián (3,67 %).

¿Qué factores impulsan la rentabilidad del alquiler?

La escasez de oferta, la presión de la demanda y el aumento sostenido de los precios de compra y arrendamiento.

¿Dónde se localizan las mayores oportunidades de inversión?

En capitales medias con precios más competitivos, como Tarragona, Jaén o Ávila, donde la rentabilidad supera el 7 %.

La rentabilidad del alquiler se consolida como uno de los indicadores clave para entender el futuro del mercado inmobiliario.

La inflación altera la percepción del valor y del dinero en hogares e inversiones

El escenario económico actual, marcado por una inflación persistente y tensiones geopolíticas, está modificando la manera en que consumidores e inversores toman decisiones. En los hogares, el miedo a nuevas subidas de precios impulsa conductas como el consumo anticipado, la compra impulsiva o el ahorro mal orientado.



En los mercados financieros, el vértigo se impone sobre la lógica, dando paso a una “parálisis por análisis” que puede hacer perder oportunidades reales.

Según algunos profesionales en la materia, las emociones están condicionando cada vez más las decisiones económicas. La inflación no solo erosiona el poder adquisitivo, también distorsiona nuestra percepción del valor y del dinero, transformando la forma de comprar, invertir y priorizar. Una situación que coincide con las advertencias del Banco de España sobre la inflación, donde se subraya la necesidad de educación económica para interpretar correctamente estos fenómenos.

Conceptos como la “anestesia inflacionaria”, la “ilusión monetaria” o el “sesgo de urgencia” explican por qué muchos ciudadanos adoptan decisiones precipitadas, desde compras compulsivas hasta inversiones conservadoras sin base racional. En este contexto de sobreinformación, los titulares pesan más que los análisis, la intuición sustituye al razonamiento y el miedo se convierte en un motor de decisiones costosas.

Datos relevantes

- La inflación erosiona el poder adquisitivo y distorsiona la percepción del dinero.
- En los hogares provoca consumo anticipado, ahorro mal orientado y compras impulsivas.
- En los mercados financieros se impone la intuición frente al análisis profundo.
- Conceptos como la ilusión monetaria y el sesgo de urgencia explican decisiones erráticas.

Los activos conservadores se convierten en refugio, aunque no siempre sean la mejor opción.

¿Qué es la anestesia inflacionaria?

Es el fenómeno por el cual los consumidores se acostumbran a la subida de precios y acaban normalizándola en sus decisiones diarias.

¿Cómo afecta la inflación a los inversores?

Condiciona sus decisiones desde el miedo, priorizando la intuición frente al análisis racional y reforzando la preferencia por activos conservadores.

El miedo puede ser legítimo, pero cuando gobierna nuestras decisiones nos aleja de la racionalidad.

¿Cómo ha cambiado la percepción del valor y el dinero en tiempos de inflación?

En el actual escenario económico marcado por una inflación persistente, tensión geopolítica e incertidumbre financiera, comprender el comportamiento del inversor y del consumidor final se ha convertido en una herramienta esencial para la toma de decisiones. La psicología económica del comprador en tiempos de inflación ha cambiado de la mano de una modificación de la percepción del valor y del dinero. Así lo advierte una de las principales compañías de España y Portugal en gestión de soluciones y servicios para entidades financieras y compañías inmobiliarias.

En este sentido, algunos expertos subrayan que, tanto los consumidores como los inversores, se enfrentan hoy a un entorno emocionalmente más complejo que racional. “La inflación no solo erosiona el poder adquisitivo, también distorsiona nuestra percepción del valor y del dinero. Cambia la forma en que compramos, invertimos y priorizamos”, afirman los expertos.

La llamada ‘anestesia inflacionaria’, por la cual los consumidores se acostumbran progresivamente al alza de precios, convive con fenómenos como la ilusión monetaria, en el que el consumidor puede sentirse más rico porque ha



recibido un aumento salarial, aunque ese incremento no supere el alza de los precios; o el sesgo de urgencia, una distorsión cognitiva que lleva a las personas a priorizar tareas o decisiones que parecen urgentes, aunque no sean importantes. Estos fenómenos empujan a decisiones de consumo impulsivas o conservadoras sin base racional.

Desde el lado inversor, el miedo ha ganado un protagonismo desmedido. Se destaca cómo las emociones están condicionando más las inversiones que los datos reales. “Hoy se reacciona más a un titular que a un análisis profundo. Vivimos en un contexto de sobreinformación donde la intuición sustituye al razonamiento, y eso genera decisiones erráticas que pueden ser muy costosas”. Esta situación ha reforzado la tendencia a buscar refugio en activos conservadores, aunque no siempre sean la mejor opción objetiva.

El impacto psicológico de la inflación genera una sensación de pérdida de control que se traduce en decisiones reactivas y, muchas veces, erróneas. En los hogares, el miedo a que los precios sigan subiendo desencadena conductas como el consumo anticipado, la compra impulsiva o el ahorro mal orientado. En los mercados financieros, el vértigo se impone sobre la lógica, dando paso a una “parálisis por análisis” que puede llevar a perder oportunidades reales. “El miedo es una emoción legítima, pero cuando gobierna nuestras decisiones, nos aleja de la racionalidad”.

Ante este panorama, se reivindica el papel fundamental de la Psicología Económica como disciplina para ayudar a interpretar y modular nuestras reacciones. “No podemos controlar el mercado ni anticipar todos los escenarios, pero sí podemos entrenar nuestra forma de responder. Invertir en autocontrol, en educación financiera y en una estrategia flexible puede ser más rentable a largo plazo que cualquier oportunidad especulativa”.

Factores que Afectan el Valor del Dinero



PREVISIÓN DE INCREMENTO EN LAS TRANSACCIONES INMOBILIARIAS

El 73% de los inversores institucionales prevé un aumento en las transacciones inmobiliarias en los próximos dos años, frente al 64% registrado en 2024.



Los análisis realizados destacan que, vuelve la confianza en el sector inmobiliario gracias al repunte de las valoraciones y la confianza de los inversores. En este sentido, los inversores institucionales elevan al 39% sus previsiones de alzas en las valoraciones en los próximos dos años, frente al 2% y 27% registrados en 2023 y 2024 respectivamente. El optimismo también crece en torno a la rentabilidad, con el 80% de los encuestados que espera que la rentabilidad total aumente o se mantenga estable, manteniendo la tendencia al alza desde el 64% del año pasado y el 45% del año anterior.

«El repunte de la confianza marca un verdadero punto de inflexión. Tras más de dos años de cautela, la confianza está volviendo a medida que las valoraciones se estabilizan e incluso comienzan a aumentar, y crece el interés en determinadas estrategias inmobiliarias. En este nuevo ciclo, se recomienda a los inversores que aprovechen las oportunidades de crecimiento estructural impulsadas por tendencias como la digitalización, la urbanización, la energía y la vivienda».

A medida que las condiciones del mercado se estabilizan, las estrategias de menor riesgo recuperan su atractivo, con el 61% de los inversores que prevé aumentar sus asignaciones a estrategias core o core+, frente al 40% del año pasado. Este cambio señala un interés creciente por activos seguros con generación de ingresos, así como un retorno más amplio al mercado.

El segmento residencial se alza como el activo más valorado, con un 47% de los inversores que lo sitúan en primer lugar, seguido de las estrategias de 'modern living', como las residencias de estudiantes, residencias para personas mayores y coliving, con un 21%. El segmento logístico continúa despertando interés (16%), por delante de oficinas (9%), hostelería (5) y retail (3%).

Las mejoras operativas también ganan atractivo. Tres de cada cuatro inversores dan prioridad a las transiciones de 'brown-to-green' y a las remodelaciones, lo que pone de relieve el interés estratégico por la sostenibilidad y la mejora de los activos como palancas clave para la creación de valor a largo plazo.

Continúa la década de las infraestructuras

Los inversores siguen aumentando las asignaciones de capital a infraestructuras, lo que confirma una tendencia sostenida desde hace varios años que refleja la creciente importancia estratégica de esta clase de activos. El 35% de los inversores institucionales tiene previsto aumentar su participación en infraestructura, mientras que el 57% espera mantener sus asignaciones actuales.

Este crecimiento se ve respaldado por la mejora de las oportunidades de inversión: el 80% de los inversores afirma que hoy en día hay mejores oportunidades de inversión en infraestructuras que en años anteriores, lo que supone un aumento con respecto al 48% de 2023 y un nuevo incremento con respecto al 73% de 2024.

Este optimismo, además, se ve reforzado por las expectativas de rendimiento: el 44% de los encuestados prevé un aumento de las valoraciones de las infraestructuras en los próximos dos años, mientras que solo el 10% espera que disminuyan.

El aumento de las asignaciones a infraestructuras se ve respaldado por tendencias a largo plazo que influyen cada vez más en las decisiones de inversión. Casi el 40% de los encuestados se centra en activos relacionados con la transición energética, mientras que el 37% se centra en infraestructuras digitales, como redes de fibra óptica o centros de datos, superando a sectores tradicionales como los servicios públicos (10%) y el transporte (10%).

Una tendencia que está cobrando importancia es la convergencia entre el sector inmobiliario y el de infraestructuras, ya que más del 86% de los inversores consideran ahora que las estrategias combinadas de estos dos sectores son atractivas o están dispuestos a explorarlas, lo que pone de relieve el creciente interés por enfoques de inversión integrados, sostenibles e inteligentes. Este cambio refleja una visión más amplia de que las fronteras entre el sector inmobiliario y de infraestructuras se están difuminando, a medida que los inversores buscan soluciones holísticas alineadas con las tendencias estructurales a largo plazo.

Por su parte, algunos expertos en la materia, añaden: «La década de las infraestructuras continúa, impulsada por el fuerte interés de los inversores por modernizar los activos inmobiliarios inteligentes en línea con tendencias como la digitalización, la urbanización, la energía y la vivienda».

Las coinversiones y las colaboraciones público-privadas permiten opciones de inversión más amplias en todos los perfiles de riesgo y tamaños de operaciones. La convergencia entre el sector inmobiliario y el de las infraestructuras ya no es solo una visión, sino que está cobrando fuerza”.

Los inversores continúan apostando por los criterios ESG a pesar de las dificultades

A pesar de los retos actuales, el 69% de los inversores institucionales prevé integrar más criterios ESG en sus procesos de inversión. Las barreras más mencionadas siguen siendo la complejidad normativa y la falta de datos estandarizados de alta calidad, señaladas por el 64% de los encuestados como obstáculos importantes a la hora de ampliar las estrategias de inversión sostenible.

De cara al futuro, la opinión de los inversores está dividida: el 45% cree que los criterios ESG cobrarán aún más importancia en los próximos años, mientras el 37% espera que su influencia disminuya. Solo el 13% cree que la evolución política mundial no tendrá ningún impacto en los criterios ESG, lo que pone de relieve la creciente complejidad de la relación entre la sostenibilidad y la geopolítica.

En palabras de algunos profesionales: “Incluso en medio de esta incertidumbre, hay un mensaje claro: los criterios ESG ya no son una preocupación secundaria, sino una cuestión fundamental a través de la cual se reevalúan el riesgo, el valor y el rendimiento a largo plazo, y los inversores que se adapten más rápidamente estarán en mejor posición para liderar el próximo ciclo de inversión en activos reales”.

Respuestas correctas al cuestionario del Área de Formación Continuada

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

FORMACIÓN CONTINUADA DEL

= MEDFIN =

= MEDIADOR FINANCIERO =

Viene de la edición anterior ...//...

Nivel sistémico

La interacción entre el ciberriesgo y otros riesgos como el financiero, no hace sino incrementarse a nivel sistémico. A las implicaciones del ciberriesgo a nivel individual se le añaden, a nivel sistémico, las derivadas del elevado nivel de interconexión e interdependencia entre las entidades financieras. Esto hace que el impacto de un ciberincidente en una entidad pueda extenderse a más entidades, agregándose el impacto operacional, financiero y reputacional y erosionando potencialmente la confianza en el sector, elemento crucial que podría incrementar exponencialmente el impacto a nivel sistémico. Otros escenarios con un potencial efecto sistémico serían, por ejemplo, un ataque masivo contra un número elevado de entidades o contra un proveedor crítico o fallos en un software de uso común en el sector.



Las implicaciones sistémicas para la estabilidad financiera del ciberriesgo están siendo estudiadas por las autoridades macroprudenciales. En este sentido, la JERS ha trabajado los últimos años en estudiar el impacto en la estabilidad financiera del ciberriesgo²⁰, los posibles canales de contagio a través de los que el impacto de un ciberincidente puede llegar a poner en riesgo la estabilidad financiera²¹ y potenciales medidas para mitigarlo²².

La materialización de riesgos vinculados al ciclo de crédito o al de negocio no reduciría necesariamente la probabilidad de ciberincidentes. Al contrario, un entorno recesivo podría incrementar los incentivos para realizar ataques maliciosos con motivación económica, ante la menor capacidad de generación de rentas legales de agentes tecnológicos o ante la reducción de la capacidad de las entidades de invertir en ciberresiliencia. Si bien es necesaria más investigación sobre esta cuestión, una relación neutra o de refuerzo de los ciberriesgos con respecto a los ciclos económico-financieros señala la necesidad de contar con recursos específicos de absorción de riesgos frente a estos. Estos recursos necesitarían su propia categoría y estarían adaptados a la naturaleza tecnológica de estos riesgos.

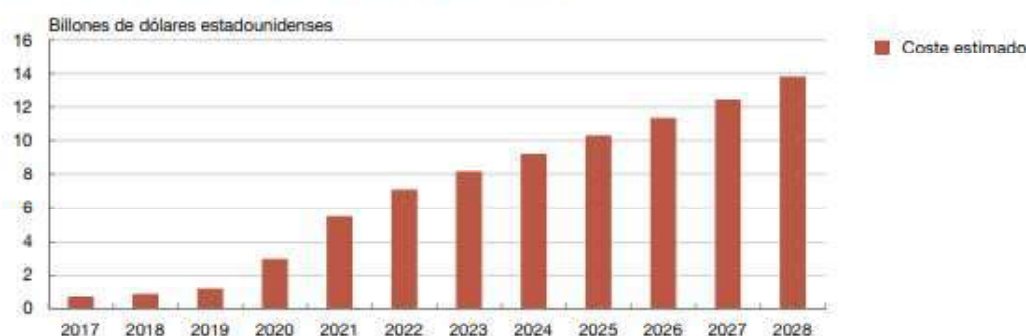
20 Véase el informe de la JERS Systemic cyber risk del 19 de febrero de 2020.

21 JERS. (2020). "The making of a cyber crash". ESRB Occasional Paper Series, 16.

22 Véase el informe de la JERS Mitigating systemic cyber risk, del 27 de enero de 2022.

Gráfico T.2
El coste estimado del cibercrimen a nivel mundial se ha incrementado cerca de un orden de magnitud en los últimos cinco años y se espera que esta tendencia creciente se mantenga

T.2.a Estimación del coste del cibercrimen a escala mundial



El impacto del ciberriesgo

Principales ciberamenazas

Existen diferentes tipos de actores de ciberamenazas, que varían en sus motivaciones, la sofisticación de los ataques y el impacto que generan. Los atacantes aficionados²³ y los activistas²⁴ normalmente buscan notoriedad y suelen realizar ataques menos sofisticados y de impacto bajo o moderado. En cuanto a los denominados insiders²⁵, suelen tener como motivación la venganza o el espionaje por cuenta de otros; su conocimiento de la compañía y su facilidad de acceso los hace potencialmente peligrosos, aunque no siempre cuentan con capacidades técnicas elevadas. Sin embargo, existen otros tipos de atacantes con capacidades técnicas muy sofisticadas y capaces de producir impactos muy importantes, con motivaciones estrictamente económicas o geopolíticas.

Los ciberataques atribuidos al crimen organizado, que persiguen un beneficio económico, no cesan de incrementarse en todo el mundo. Esto está suponiendo un coste creciente (véase gráfico T.2). La legislación existente está mayormente confinada a un entorno físico y con soberanías territoriales bien definidas, lo que la hace de difícil aplicación al mundo digital.

Existen, además, enormes diferencias entre jurisdicciones y los acuerdos globales para perseguir este tipo de crimen son prácticamente inexistentes. Esta situación, unida a la dificultad de la atribución de los delitos a sus responsables, convierten los ciberataques en un delito con escaso riesgo para el criminal y que supone un elevado coste para las entidades y los individuos afectados.

Se ha observado también un incremento de los ciberataques con motivaciones geopolíticas. Los objetivos y las técnicas utilizadas varían de unos a otros. Así, por ejemplo, como consecuencia del conflicto entre Rusia y Ucrania, partidarios de ambos bandos han lanzado numerosos ataques de denegación de servicio²⁶ contra administraciones públicas y compañías de los países que apoyaban al bando contrario, para generar inestabilidad y dificultar todo tipo de actividad en ellos, incluida la financiera. Otras veces se trata de grupos respaldados por Estados que buscan monetizar sus ataques²⁷ mediante la realización de transferencias fraudulentas²⁸, el robo de criptodivisas²⁹ o la obtención de un rescate a cambio de devolver a sus víctimas la información cifrada por los atacantes y no divulgarla (ransomware)³⁰. Otra vía utilizada por los atacantes para conseguir financiación es el robo de datos, y cada vez son más frecuentes los ciberataques financiados por Estados dirigidos a la obtención de información sensible que pueda ser de utilidad económica o política.

Han crecido el número y la sofisticación de los ciberataques contra proveedores del sistema financiero, realizados por los atacantes con mayores capacidades técnicas.

Algunos ataques se limitan a explotar vulnerabilidades existentes en los productos de hardware o software de estos proveedores³¹. Otros, más sofisticados, alteran dichos productos para introducirles debilidades que luego puedan ser explotadas³². A pesar del tiempo y de los recursos necesarios para preparar y ejecutar una operación de estas características, los atacantes pueden conseguir llegar a miles de organizaciones y empresas a través de un único punto de entrada, multiplicando extraordinariamente la eficacia y eficiencia de su ataque.

23 También llamados script kiddies.

24 Se suelen denominar hacktivistas.

25 En este contexto, un insider es un empleado que actúa con fines maliciosos contra su compañía.

26 Un ataque de denegación de servicio consiste en inundar de peticiones un sitio web hasta dejarlo inoperativo.

27 Informe del Consejo de Seguridad de las Naciones Unidas (2019).

28 Por ejemplo, el ataque al Bangladesh Bank (banco central de Bangladés) en 2016, en el que se realizaron transferencias fraudulentas a través de SWIFT por valor de más de 80 millones de dólares.

29 Por ejemplo, se estima que el grupo Lazarus, asociado al Gobierno de Corea del Norte, fue responsable del 20% de los robos de criptoactivos durante 2023, más de 300 millones de dólares.

30 Un ransomware es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción. En numerosas ocasiones dicho rescate consiste en una cantidad de criptomonedas.

31 Hay numerosos ejemplos, se puede citar la explotación de una vulnerabilidad en el software comercial de transferencia de ficheros MOVEit por parte del grupo de ransomware CLOp, que afectó a miles de organizaciones en todo el mundo en 2023.

32 El caso paradigmático es el de SolarWinds. En diciembre de 2020 se descubrió que un software distribuido por la compañía había sido alterado por un grupo de ciberatacantes para que les permitiera acceso a todos los clientes que usaban este producto. Entre los miles de afectados se encontraban numerosas agencias federales estadounidenses, así como la OTAN, el Parlamento Europeo, compañías como Microsoft, y otras.

Ciberincidentes y pérdidas

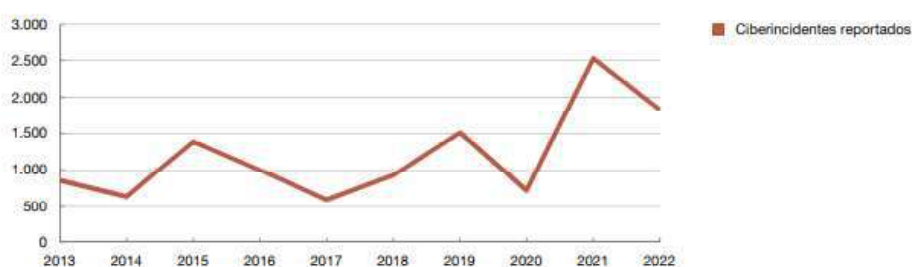
Volúmenes de ciberincidentes

En términos globales, el número de ciberincidentes no ha parado de crecer en los últimos años, con un repunte especialmente relevante de los de naturaleza maliciosa tras la pandemia de COVID-19. Como cabría esperar, el incremento de la digitalización tanto en empresas como en particulares y organismos públicos ha supuesto un aumento continuado de los ciberincidentes. Por ejemplo, se puede observar que el abrupto incremento del uso de la tecnología en el contexto de la irrupción de la pandemia de COVID-19 generó un significativo aumento global en el número de ciberincidentes reportados en el sistema financiero (véase gráfico T.3.a). Si bien tras el pico de la pandemia el aumento se ha moderado, cabe esperar que la tendencia siga siendo ascendente en el futuro.

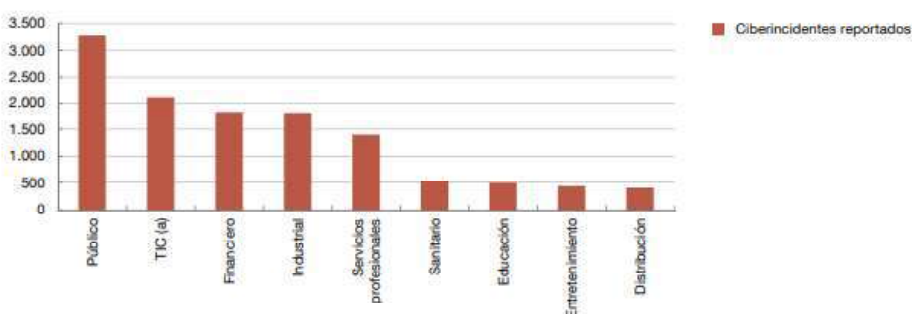
Gráfico T.3

El sector financiero continúa siendo, a escala global, uno de los que más ciberincidentes tiene. El número anual de ciberincidentes reportado en el sector financiero sigue una tendencia creciente, habiendo visto duplicado su número entre 2018 y 2022

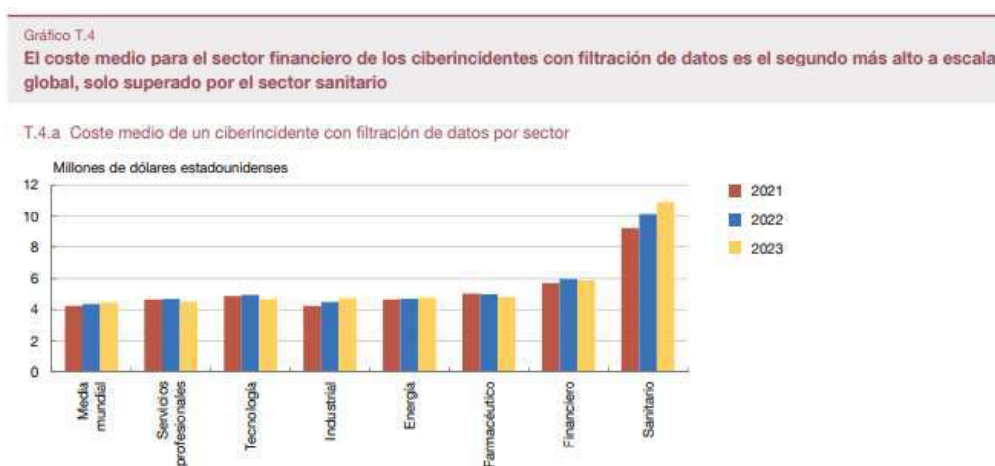
T.3.a Número global de ciberincidentes en el sector financiero



T.3.b Número global de ciberincidentes en 2022 por sector



El sistema financiero se sitúa entre los más atacados. Esta elevada prevalencia relativa de ciberincidentes en el sistema financiero (véase gráfico T.3.b) se mantiene a pesar de que, puntualmente, otros sectores puedan acaparar los ataques. Por ejemplo, el sector sanitario se situó entre los más atacados durante la pandemia de COVID-19 y en 2022 las administraciones públicas fueron el principal objetivo, en un contexto de tensiones geopolíticas (véase gráfico T.3.b).



Pérdidas

Las pérdidas asociadas a un ciberincidente pueden variar considerablemente en función de distintos factores. Como se ha visto anteriormente, por su potencial para generar un mayor impacto, los ciberincidentes maliciosos normalmente llevan asociado un mayor volumen de pérdidas para la entidad. Las filtraciones de información son uno de los ciberataques más frecuentes y con más pérdidas asociadas para una entidad. El coste medio de este tipo de incidentes para las entidades aumenta cada año, situándose en 4,45 millones de dólares en 2023 a escala global³³. El sistema financiero, además de ser de los más atacados, se encuentra entre los que mayor coste medio soporta para los ciberincidentes de filtración de datos, 5,9 millones de dólares en 2023 (véase gráfico T.4).

Los ciberseguros como mitigante parcial

La transferencia del riesgo es una estrategia con alcance limitado en el caso del ciberriesgo. Las pólizas para cubrir el ciberriesgo, también conocidas como «ciberseguros», tienen un efecto limitado, ya que las coberturas financieras que ofrecen pueden no ser suficientes para mitigar el impacto de un ciberincidente. Por ejemplo, el cobro de una indemnización no puede cubrir algunos de los impactos más importantes de un ransomware, como es la parada de los sistemas infectados de una entidad, que debe ser resuelta con la mayor rapidez posible.

Adicionalmente, se han endurecido las condiciones para los ciberseguros a escala global. El sector asegurador comenzó a cubrir el ciberriesgo sin información histórica ni conocimiento suficiente para estimar correctamente las primas. A esto se le sumó el gran incremento de la frecuencia e impacto de los ciberincidentes, lo que trajo consigo un aumento de los siniestros de ciberseguros comunicados; por ejemplo, cuadruplicándose en España entre 2017 y 2020³⁴. Este incremento, sumado a unas primas bajas, tuvo un impacto negativo en la rentabilidad de este tipo de seguros. Las compañías aseguradoras han reaccionado en los últimos años endureciendo las condiciones de renovación, incrementando las primas o añadiendo clausulado especial para excepcionar de las coberturas circunstancias como ransomware o guerras.

Gestionar el ciberriesgo para alcanzar la resiliencia individual y sistémica

Buenas prácticas, regulación y supervisión

La discusión sobre el ciberriesgo en el sistema financiero ocupa un lugar relevante en la agenda de numerosos organismos internacionales.

En paralelo al incremento de la digitalización de toda la actividad económica y del consecuente aumento de la exposición al ciberriesgo, estos organismos internacionales han emitido buenas prácticas, informes y herramientas. Entre los trabajos más relevantes de los últimos años para el sistema financiero, el FSB publicó la mencionada taxonomía Cyber Lexicon, así como unas prácticas efectivas para la respuesta y recuperación ante ciberincidentes³⁵, y está actualmente trabajando en un formato común para su notificación³⁶.

En este ámbito destaca la emisión por parte del Comité de Supervisión Bancaria de Basilea de los Principios de Resiliencia Operacional³⁷. Estos tienen el propósito de reforzar la capacidad de los bancos de resistir el impacto de eventos operacionales que pueden causar interrupciones de sus servicios críticos. El Comité señala que los bancos deben asumir como hipótesis de trabajo que este tipo de eventos ocurrirán y definir su nivel de tolerancia a la interrupción. Los principios abarcan tanto medidas preventivas y de anticipación como otras encaminadas a la respuesta y recuperación cuando se produce la interrupción en servicios críticos. Estos principios cubren aspectos de gobernanza, gestión de riesgos operacionales e identificación continua de amenazas, identificación de interconexiones e interdependencias, gestión de terceras partes, continuidad de negocio, gestión de incidentes y gestión de la tecnología, incluida la ciberseguridad. Desde su publicación, las jurisdicciones han trabajado para incorporar estos principios a su marco regulatorio y su práctica supervisora, y los bancos avanzan en adaptar a los mismos sus políticas, estrategias y marcos de gestión³⁸.

En el panorama regulatorio internacional se ha iniciado también una discusión sobre si el capital financiero es una medida adecuada para mitigar los ciberriesgos³⁹. Por ejemplo, en el escenario de una entidad afectada por un ataque de ransomware que cifrara todos sus sistemas críticos, la supervivencia de la entidad dependería de tener o no medidas técnicas que le permitieran recuperarse. El capital financiero no sería el principal elemento de resiliencia en este caso, aunque podría afectar a la capacidad de financiar el despliegue de estas medidas técnicas. En eventos menos extremos, con una pérdida parcial de los sistemas, el beneficio relativo de una mayor solvencia puede ser mayor, al disponer las entidades de más opciones de acción, que requieren de su correspondiente financiación. En cualquier caso, es necesario valorar si la resiliencia adicional frente a ciberriesgos que puede aportar una cierta cantidad de capital financiero puede alcanzarse de forma más eficiente mediante la acumulación de más recursos tecnológicos. Más aún, algunos expertos dudan sobre si los riesgos asociados a la tecnología deberían ser o no una subcategoría del riesgo operacional, dado su carácter transversal a todas las actividades, hecho que se ha exacerbado en paralelo al avance del proceso de transformación digital.

La regulación y la supervisión actúan como catalizadores para que las entidades financieras gestionen adecuadamente el ciberriesgo. Por ello, numerosas jurisdicciones, como la UE, el Reino Unido⁴⁰, Estados Unidos⁴¹ o Australia⁴² han desarrollado marcos regulatorios y supervisores, así como herramientas en este ámbito.

En la UE, hemos asistido a una intensa actividad regulatoria en materia de ciberriesgos.

La publicación en 2016 de la directiva NISD, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información, fue una clara apuesta de la UE para mejorar la ciberseguridad en todos los sectores críticos de un país, incluyendo las entidades de crédito y las infraestructuras de mercado. Esta directiva ha sido revisada y sustituida por la NIS2, que extiende aún más su ámbito de aplicación y que deberá estar transpuesta por los Estados miembros no más tarde de octubre de 2024. Podemos citar otras normas recientes como la Directiva sobre la resiliencia de las entidades críticas⁴³, el Reglamento de ciberseguridad⁴⁴ o el futuro Reglamento de ciberresiliencia⁴⁵.

33 Véase el informe de IBM Cost of a Data Breach Report 2023.

34 Según el IV Estudio Anual de Aon sobre Ciberseguridad y Gestión del Riesgo Ciber en España 2023, entre 2017 y 2020 el número de siniestros de ciberseguros comunicados en España se cuadruplicó.

35 Véase el informe del FSB Effective Practices for Cyber Incident Response and Recovery, de octubre de 2020.

36 Véase el informe del FSB Format for Incident Reporting Exchange (FIRE), de abril de 2023.

37 Véase Principles for Operational Resilience, de marzo de 2021

38 Véase BCBS Supervisory newsletter on the adoption of POR and PSMOR, de noviembre de 2023.

39 L. F. Signorini. (2021). "Implementing Basel III in the EU: remaining challenges and timing". Eurofi Magazine.

40 Véase Operational Resilience of the financial sector del Banco de Inglaterra.

41 Véase Cybersecurity and Financial System Resilience Report, CISA Cyber Resilience Review, NIST Cybersecurity Framework.

42 Véase Council of Financial Regulators. Cybersecurity.

43 Directiva UE 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo.

44 Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) nº 526/2013 («Reglamento sobre la Ciberseguridad»).

45 Propuesta de Reglamento de ciberresiliencia

Esquema T.1

Principales elementos del Reglamento DORA



FUENTE: Banco de España

El sistema financiero de la UE es el que dispone de mayor cantidad de regulación específica de los ciberriesgos. Entre otras normas sectoriales podemos citar las Directrices sobre la evaluación del riesgo de TIC [tecnologías de información y comunicación] en el marco del PRES [Proceso de Revisión y Evaluación Supervisora]⁴⁶, de 2017, y las Directrices sobre gestión de riesgos de TIC y de seguridad⁴⁷ de la EBA, que se constituyeron en un referente desde su publicación. Las relaciones con terceras partes también han sido foco de atención de la EBA, que publicó en 2019 sus Directrices sobre externalización⁴⁸. En el ámbito de las infraestructuras de mercado, el Banco Central Europeo (BCE) publicó en 2018 sus expectativas de ciberresiliencia⁴⁹, sobre la base de las directrices publicadas en 2016 por CPMI-IOSCO.

El Reglamento DORA supondrá un punto de inflexión para la ciberresiliencia del sistema financiero en la UE a partir de su aplicación en enero de 2025. DORA forma parte de la estrategia de finanzas digitales de la Comisión Europea, y su objetivo es mitigar los riesgos asociados a la

digitalización y mejorar la resiliencia del sistema financiero europeo. Contiene requerimientos para todas las entidades financieras sobre la gestión de los riesgos asociados a la tecnología, la gestión y la notificación a los supervisores de incidentes tecnológicos, la realización de pruebas sobre la resiliencia de los sistemas, y la gestión de sus relaciones con terceras partes (véase el esquema T.1).

DORA, además de su alcance microprudencial, también trata algunos aspectos de la dimensión sistémica de los ciberriesgos. Así, fomenta el intercambio de información entre instituciones y establece mecanismos de cooperación entre autoridades dentro y fuera del sistema financiero (tanto supervisoras como de otro tipo, tales como agencias de seguridad); ordena un estudio de la viabilidad de un punto único de notificación de incidentes para todas las entidades financieras europeas, y establece un marco de vigilancia sobre aquellos proveedores tecnológicos que sean críticos para el sistema financiero europeo.

En el ámbito de la supervisión microprudencial, las autoridades financieras del sector bancario europeo han incorporado el ciberriesgo tanto al seguimiento continuo y las inspecciones in situ de las entidades como a las actividades horizontales. Para ello, se han dotado de recursos especializados y han establecido metodologías y procedimientos de trabajo adaptados a las particularidades de este riesgo. Adicionalmente, la mayor parte de ellas han establecido requerimientos de notificación de ciberincidentes relevantes con el fin de detectar lo antes posible eventos adversos que pudieran requerir algún tipo de intervención por parte de las autoridades.

Además del enfoque estrictamente supervisor, muchas autoridades han establecido marcos de pruebas de ciberresiliencia basadas en inteligencia de amenazas. Estas pruebas tratan de simular un ciberataque sofisticado, y lo más realista posible, sobre los sistemas en producción de una entidad, apoyándose en información de inteligencia sobre los atacantes más probables y sus técnicas y procedimientos. Se trata de valorar las capacidades técnicas, humanas y organizativas de las instituciones para detectar el ataque y reaccionar ante él, sin que los equipos de defensa sean informados previamente de que hay una prueba en curso. La autoridad realiza en todo momento el seguimiento de la prueba para verificar que se cumplen los requisitos del marco. En el caso de la UE, 16 jurisdicciones, entre las que se incluye España, han adoptado ya el marco de pruebas del BCE, TIBER-EU50.

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 Septiembre/Octubre de 2025, continuamos con el desarrollo del tema «**Ciberriesgos**». Seguiremos con el desarrollo de este nuevo tema en la próxima edición de nuestro Boletín correspondiente a los meses de Noviembre/Diciembre 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 13 de nuestro Boletín Oficial.

1.- El impacto de un ciberincidente en una entidad puede extenderse a más entidades, agregándose:

- a) el impacto operacional, financiero y reputacional, erosionando potencialmente la confianza en el sector.
- b) las implicaciones sistemáticas para la estabilidad financiera del ciberriesgo.
- c) la materialización de riesgos vinculados al ciclo de crédito o al de negocio.

2.- El ciberriesgo en el sistema financiero de los organismos internacionales tiene gran relevancia. Por ello, a nivel internacional se ha iniciado:

- a) un sistema de normas sectoriales para la evaluación de los ciberriesgos.
- b) la confección de un reglamento para lograr la ciberresiliencia.
- c) una discusión sobre si el capital financiero es una medida adecuada para mitigar los ciberriesgos.

3.- Los principios de resiliencia operacional del Comité de Supervisión Bancaria de Basilea, tienen como principal propósito:

- a) la gestión de riesgos operacionales e identificación continua de amenazas, interconexiones o interdependencias.
- b) reforzar la capacidad de los bancos de resistir el impacto de eventos operacionales que pueden causar interrupciones de sus servicios críticos.
- c) actuar como catalizadores para que las entidades financieras gestionen adecuadamente el ciberriesgo.



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

