El BCE exige un plan. ¿Puede usted cumplirlo?

La preparación cibernética frente a la IA debe garantizarse y demostrarse. Un panorama de los hechos, las exigencias y las soluciones.

Plazo: 31 de octubre de 2026 — Plan de acción remitido al Joint Supervisory Team, con responsable designado, presupuesto y calendario.

Lo esencial en pocas palabras

El BCE exige a 109 entidades importantes un plan de acción de ciberseguridad frente a la IA, que deberá presentarse antes del 31 de octubre de 2026, dirigido personalmente al presidente del consejo de administración. No se trata de un nuevo marco normativo, sino de DORA aplicado con mayor rigor: el plan debe ser demostrable, no solo plausible. La IA reduce la ventana entre el descubrimiento de una vulnerabilidad y el ataque, de varias semanas a unos minutos, lo que hace insuficientes los ciclos de parcheo reactivos. La pregunta central: ¿sabe usted en tiempo real qué terminales opera, cuán expuestos están, y con qué rapidez puede actuar?

01

Los hechos

El 7 de julio de 2026, la supervisión bancaria del BCE envió una carta a los responsables de todas las entidades importantes (ref. SSM-2026-0301, firmada por la presidenta del consejo de supervisión, Claudia Buch). Están afectados 109 bancos bajo supervisión directa. Antes del 31 de octubre de 2026, deben presentar a su Joint Supervisory Team (JST) un plan de acción con medidas concretas, responsables designados nominalmente, presupuesto y personal asignados, así como plazos vinculantes.

El fundamento jurídico es DORA, el Reglamento (UE) 2022/2554. No se trata, por tanto, de un nuevo marco normativo; las obligaciones existentes simplemente se concretan. La carta viene acompañada de la advertencia de la JERS (Junta Europea de Riesgo Sistémico) del 25 de junio de 2026, la primera advertencia cibernética en la historia de este organismo. Al mismo tiempo, se ha aplazado el cuestionario anual sobre riesgo tecnológico, de septiembre de 2026 a febrero de 2027.

Lo que exige el BCE, de un vistazo (carta del 7 de julio de 2026) — esto es lo que exige la supervisión antes del 31 de octubre de 2026:

1. Presentación de un plan de acción de ciberseguridad frente a la IA al Joint Supervisory Team (JST) competente
2. Medidas concretas en lugar de declaraciones de intenciones, con plazos vinculantes
3. Responsables designados nominalmente para cada medida
4. Presupuesto asignado y personal designado
5. Avance demostrable en todo momento ante el JST

02

Por qué el reloj corre ahora

La presión no proviene del regulador, sino del bando contrario: los atacantes han dado un salto de capacidad. El cambio decisivo puede resumirse en una sola cifra. Construir un exploit operativo solía llevar días o semanas; con los modelos de IA de frontera, hoy bastan minutos u horas.

La JERS habla de un «colapso de los márgenes defensivos». El estándar histórico de 90 días hasta la divulgación pierde así su efecto protector.

Los datos respaldan esta valoración. En su advertencia JERS/2026/3 del 25 de junio de 2026, el organismo señala esta caída del tiempo de construcción de un exploit, de varios días o semanas a minutos u horas. En el primer semestre de 2026 se registraron 35.364 nuevas vulnerabilidades, frente a 23.656 en el primer semestre de 2025, un aumento del 49,5 %. Y el CERT-UE contabiliza, en su informe Threat Landscape 2025, nueve incidentes de seguridad en instituciones de la UE, dos de ellos con vulnerabilidades de día cero.

La advertencia de la JERS de un vistazo (advertencia JERS/2026/3 del 25 de junio de 2026):

Los modelos de IA de frontera reducen el tiempo de construcción de un exploit de varios días o semanas a minutos u horas

Clasificación como riesgo cibernético sistémico para el sector financiero europeo (elevado en junio de 2026 de «alto» a «grave»)

Importante: cuando la ventana se reduce de varias semanas a unas horas, lo que cuenta ya no es tanto la calidad de cada control por separado, sino la velocidad con la que usted puede ver su situación, priorizarla y demostrarla.

03

Asunto de la alta dirección: por qué corresponde al consejo

Que la resiliencia cibernética deba estar en la agenda del consejo de administración no es una interpretación de Tanium: es la posición explícita de las propias autoridades de supervisión y seguridad.

La carta se dirigió al CEO, no al CISO. La carta del BCE (SSM-2026-0301) se dirige directamente a los presidentes de los consejos de administración y exige una estructura de gobernanza: responsables designados, recursos asignados, plazos vinculantes.

La supervisión habla de «riesgo sistémico». La JERS utiliza el registro que normalmente se reserva a los riesgos de estabilidad financiera, como los riesgos de concentración o liquidez: el vocabulario de la responsabilidad del consejo, no el del departamento de TI.

Los Five Eyes lo formulan explícitamente: el riesgo cibernético es «un riesgo empresarial central y una responsabilidad de la alta dirección»; los consejos deben verificar que la resiliencia resiste una carga real y no existe solo sobre el papel.

El propio BCE elige un lenguaje de gobernanza y de mercado: en su carta del 7 de julio de 2026, Claudia Buch, presidenta del consejo de supervisión, menciona «posibles repercusiones profundas en la confidencialidad, la integridad y la resiliencia de sus sistemas tecnológicos». Una comunicación de mercado y de dirección, no una nota técnica interna.

La propia gestión de riesgos lo confirma: en el Allianz Risk Barometer 2026, el riesgo cibernético (1.º puesto, 42 %) y la IA (2.º puesto, 32 %) encabezan los riesgos empresariales globales, según una encuesta a 3.338 expertos en gestión de riesgos.

04

Lo que las autoridades exigen de forma coincidente

El BCE, la JERS, los Five Eyes, ENISA y el CERT-UE formulan, de forma independiente entre sí, recomendaciones ampliamente coincidentes. Las tres más citadas, ordenadas por peso en las fuentes:

1. **Visibilidad en tiempo real de todo el inventario de activos.** Una visión completa de la red y de los sistemas de información se presenta como la base de la priorización de parches basada en el riesgo; el BCE («identificar y proteger los activos expuestos a internet») y los Five Eyes también la dan por supuesta. Sin esta base, los dos puntos siguientes no son viables.

2. **Acelerar la gestión de parches y vulnerabilidades.** La exigencia más repetida en todas las fuentes: el BCE señala una gestión más rápida de vulnerabilidades como máxima prioridad a corto plazo; la JERS mide ahora el tiempo entre descubrimiento y explotación en «claramente menos de un día». Advertencia importante de la propia JERS: parchear más rápido sin criterio aumenta el riesgo de fallos operativos; el incidente de CrowdStrike de 2024 (más de 5.000 millones de dólares en daños solo entre las empresas Fortune 500) se cita como ejemplo de advertencia. El mensaje es, por tanto: parchear más rápido, pero con transparencia y control.

3. **Reducir la superficie de ataque.** Para los Five Eyes, la medida práctica número uno: limitar los accesos innecesarios y la accesibilidad externa, y cuestionar si ciertos sistemas realmente necesitan estar expuestos. El BCE y ENISA priorizan los sistemas expuestos a internet, el software de terceros y los componentes de código abierto: solo se puede reducir lo que es visible.

A continuación, con un fuerte consenso: la gestión de sistemas heredados y en fin de vida (Five Eyes: «compromisos estratégicos»), la monitorización y detección asistidas por IA bajo supervisión humana, la gestión de identidades y accesos, incluidas las identidades no humanas, los riesgos de terceros y de proveedores de IA, incluida la planificación de salida (exigida por DORA), planes probados de respuesta a incidentes y gestión de crisis, y, como marco de todo ello, la gobernanza y la responsabilidad a nivel del consejo de administración.

También aquí: todas estas recomendaciones proceden de las autoridades e instituciones citadas, no de Tanium.

05

Cinco preguntas que el CEO debe formular

El consejo de administración responde personalmente del plan de acción. Las cinco preguntas siguientes se derivan directamente de las expectativas formuladas por el BCE y la JERS en sus comunicaciones; deberían poder responderse en todo momento.

Primera — Cobertura y actualidad de los datos: ¿podemos identificar en todo momento, sin lagunas, qué terminales, servidores y cargas de trabajo en la nube operamos, incluidos los sistemas no gestionados y obsoletos? Una respuesta sólida solo es posible con un inventario en vivo que también haga visibles los sistemas desconocidos y obsoletos, no con una CMDB del mes pasado.

Segunda — Velocidad de reacción: ¿en cuánto tiempo corregimos una vulnerabilidad crítica, y esa cifra resiste una verificación? Se necesita un tiempo medio de corrección medido y con marca temporal, no una estimación aproximada.

Tercera — Capacidad de demostración: ¿podríamos presentar al JST, en poco tiempo, el avance documentado de nuestro plan? Solo si los informes pueden generarse con un clic a partir de una única fuente de datos, sin tener que recopilarse manualmente durante la noche.

Cuarta — Terceros y dependencias: ¿qué proveedores tienen acceso a nuestros sistemas, y en qué medida dependemos de ellos? Se exige una visión documentada de los accesos y las dependencias, tal como exige DORA.

Quinta — Responsabilidad y gobernanza: ¿quién asume nominalmente el plan de acción, con mandato y presupuesto? Se necesita una persona designada y localizable, no un comité ni una declaración de intenciones.

De la exigencia de la supervisión a la respuesta operativa: el BCE, la JERS y los Five Eyes indican qué hacer, visibilidad en tiempo real sin lagunas sobre todos los activos, tiempos de reacción demostrablemente cortos y avances documentados, bajo la responsabilidad del consejo. Cómo lograrlo operativamente queda abierto. Precisamente ahí radica el obstáculo real para la mayoría de las entidades: decenas de soluciones aisladas, una CMDB que va por detrás del inventario real, y pruebas que deben recopilarse manualmente. La siguiente perspectiva de solución muestra cómo cerrar esta brecha de implementación.

06

Perspectiva de solución · Tanium

La base de un plan de acción sólido: en lugar de decenas de soluciones aisladas y una CMDB que va por detrás del inventario real, Tanium apuesta por una plataforma única. Un agente ligero en cada dispositivo y una arquitectura de cadena lineal (peer-to-peer) consultan directamente todo el inventario y ofrecen respuestas sobre más de 100.000 terminales en menos de 15 segundos, escalable hasta millones de dispositivos, sin servidores de retransmisión. Así se obtiene una base de datos común y siempre actualizada, en la que convergen visibilidad, parcheo y prueba. Tanium detecta activamente los dispositivos no gestionados (Forrester: más del 98 % de cobertura), precisamente los sistemas que, de otro modo, socavan el plan de acción.

Exposure Management evalúa las vulnerabilidades y la superficie de ataque según el riesgo real y hace visibles las dependencias de terceros, de modo que el esfuerzo se dirige allí donde realmente reduce el riesgo. Y la prueba desde una única fuente genera informes listos para la supervisión con un clic, a partir de una única base de datos; el avance puede demostrarse al Joint Supervisory Team en minutos, en lugar de recopilarse durante noches enteras.

En concreto, esto se traduce en cuatro aspectos. Asset Visibility & Discover encuentra e inventaría todos los terminales, servidores y cargas de trabajo en la nube, incluidos los no gestionados y obsoletos; esto elimina los puntos ciegos y ofrece datos de inventario que resisten una inspección de supervisión. Autonomous Patch Management prioriza las vulnerabilidades críticas y despliega los parches en todo el parque sin esperar a una ventana de mantenimiento, de modo que el tiempo de corrección se acorta y se vuelve demostrable, un indicador en lugar de una estimación.

En cifras:

<15 seg	**98 %+**	**300.000**
para una respuesta sobre más de 100.000 terminales	de los terminales detectados (Forrester)	terminales en más de 40 países

Fuentes

Supervisión bancaria del BCE, carta a los responsables de las entidades importantes (ref. SSM-2026-0301), 7 de julio de 2026. bankingsupervision.europa.eu

JERS, advertencia JERS/2026/3 «sobre los riesgos cibernéticos sistémicos derivados de los modelos de inteligencia artificial de frontera», 25 de junio de 2026. esrb.europa.eu

ENISA, Threat Landscape 2025, publicado en octubre de 2025 (periodo julio de 2024 - junio de 2025). enisa.europa.eu

FIRST, 2026 Mid-Year Vulnerability Forecast, 15 de junio de 2026. first.org

CERT-UE, Threat Landscape Report 2025 — A Year in Review, publicado en abril de 2026. cert.europa.eu

DORA — Reglamento (UE) 2022/2554 sobre la resiliencia operativa digital del sector financiero, 14 de diciembre de 2022.

BCE, Supervisory Banking Statistics T1 2026 (número de entidades importantes), 19 de junio de 2026. bankingsupervision.europa.eu

Five Eyes, directrices conjuntas sobre ciberamenazas aceleradas por IA, 2026.

Allianz, Risk Barometer 2026 (encuesta a 3.338 expertos en gestión de riesgos). allianz.com

Tanium, Platform Architecture y Tanium Discover; estudio Forrester Consulting 2021 (> 98 % de detección de terminales). tanium.com

Tanium, Forrester Wave: Endpoint Management Platforms T2 2026 (Leader); casos de cliente JLL y Barclays. tanium.com

Tanium no está afiliado al BCE, a la JERS ni a ninguna otra autoridad de supervisión mencionada, y no reivindica el respaldo de ninguna de ellas. Todas las afirmaciones de carácter regulatorio se citan indicando su fuente original.

TANIUM

Autonomous IT. Unstoppable Business.