

Bienestar digital:

hacia un uso consciente de la tecnología

para luchar contra el fraude

y preservar nuestra seguridad

ing.com



1. ¿Cuál es el estado del bienestar digital en España?

1.1 Un nuevo paradigma para el bienestar (digital)

- Vivimos en un mundo cada vez más conectado gracias a las **grandes oportunidades que ofrece la digitalización**. No obstante, el modelo de uso actual (a menudo intensivo e inconsciente) está **generando también externalidades negativas que se retroalimentan**: en ocasiones se traduce en una vida digital estresante, pudiendo llegar a ser contaminante y producir además situaciones de inseguridad por los riesgos.
- Por ello, **desde ING, impulsamos un modelo de conexión consciente basado en la responsabilidad compartida** que busca proteger la integridad física y mental del usuario en red, integrando la seguridad financiera con **hábitos digitales más saludables y sostenibles** a nivel individual y colectivo. Con este objetivo, creemos que es esencial impulsar **iniciativas con las que afianzar una cultura de responsabilidad compartida** en el uso tecnológico y generar relaciones equilibradas con la tecnología.

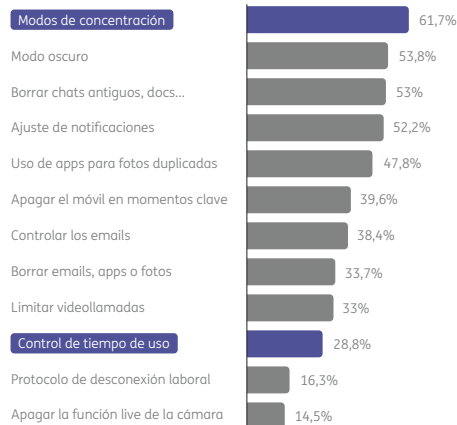
Existe una brecha crítica entre lo que sabemos y lo que hacemos

Campaña ING: yo tampoco lo sabía

- En este contexto, **el bienestar digital no puede desligarse de la protección frente al fraude**. Las entidades financieras están desplegando herramientas avanzadas de prevención, alertas inteligentes y sistemas de verificación, **pero el uso consciente por parte del ciudadano sigue siendo un factor determinante**. La responsabilidad compartida es, por tanto, un elemento estructural del nuevo paradigma digital.

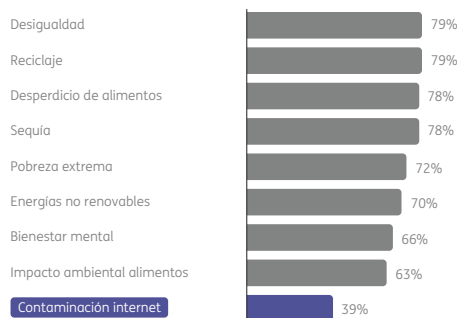
Hábitos de desconexión digital realizados habitualmente

Fuente: Estudio de Bienestar Digital de ING



Porcentaje de conocimiento en cada problemática

Fuente: Estudio de Bienestar Digital de ING



1.2 Un diagnóstico en tres factores con un mismo origen digital

El uso de la tecnología no es neutro. La ausencia de hábitos conscientes a nivel individual y estructural provoca un **impacto en cadena sobre tres áreas críticas** que tradicionalmente se han tratado por separado, pero que comparten un mismo origen: el comportamiento del usuario en la red.

- **IMPACTO EN CIBERSEGURIDAD:** la exposición constante multiplica el riesgo. Datos como que el 95% de las incidencias de ciberseguridad nacen de un error humano o que la ansiedad ante un ciberataque afecta ya al 37% de los profesionales son relevantes. A ello se suma el aumento de fraudes sofisticados, como los *deepfakes* o las campañas masivas de suplantación mediante SMS o llamadas telefónicas, que evidencian la interdependencia entre banca, telecomunicaciones y plataformas tecnológicas.
- **IMPACTO EN LA SALUD (FÍSICA, MENTAL Y PSICOSOCIAL):** la hiperconectividad y el consumo pasivo de contenidos afectan directamente al bienestar. En España, el uso diario promedio del teléfono supera las 4 horas, lo que se traduce en un aumento de estrés y ansiedad, por ejemplo, el 55% de los síntomas se asocian a las redes sociales, y problemas físicos como la fatiga visual o el sedentarismo.
- **IMPACTO EN SOSTENIBILIDAD TECNOLÓGICA:** El uso ilimitado de datos genera una huella física invisible donde acciones cotidianas, como el almacenamiento de correos obsoletos (*dark data*) o las fotos duplicadas, **consumen ingentes recursos hídricos y energéticos**. El procesamiento de IA generativa agrava este impacto al requerir hasta 10 veces más energía que una búsqueda tradicional, mientras que la descarga de un solo GB de datos llega a emitir 7 kg de CO₂.

La digitalización trae grandes oportunidades en la era digital. Fomentar un uso consciente requiere de una estrategia integral que revierte en beneficios en 3 sentidos: al cuidar nuestro cuerpo (menos estrés), cuidamos también el planeta (menos contaminación) y genera toma de conciencia en cuanto a la seguridad y la lucha contra el fraude (mayor protección en red).

2. Otros modelos en países de nuestro entorno

España es pionera en iniciativas regulatorias de salud digital y se encuentra en un momento clave de convergencia normativa en materia de ciberseguridad, protección del usuario y lucha contra el fraude. Este proceso se desarrolla en paralelo a la evolución del marco europeo, que avanza hacia mayores exigencias de protección y responsabilidad.



UNIÓN EUROPEA: ha establecido una **Declaración de Derechos y Principios Digitales**¹ y un **itinerario hacia la Década Digital 2030**², además de leyes como la **DSA (Ley de Servicios Digitales)**³. Esta normativa obliga a las grandes plataformas a auditar sus algoritmos y eliminar contenidos ilícitos.

En materia de ciberseguridad, la **Comisión Europea** ha presentado una **propuesta de nuevo reglamento para una nueva Ley de Ciberseguridad de la UE** y también la **futura PSD3** introduce nuevas obligaciones para las entidades financieras en materia de prevención del fraude. Asimismo, el **Reglamento sobre resiliencia operativa digital (DORA)** establece la obligación de intercambio de información sobre amenazas entre entidades financieras.



FRANCIA: pionera con la **Ley “El Khomri”**⁴ (Loi n° 2016-1088, 2016, Título III, Cap. II) (derecho a la desconexión) y obligaciones sobre marcadores de edad.



FINLANDIA: legislación para **prohibir el uso de teléfonos móviles en las aulas**⁵. Busca reducir las distracciones constantes y mejorar los índices de concentración y aprendizaje.



DINAMARCA: implementación de **“Estrategias Digitales hasta 2027”**⁶ enfocadas en la digitalización responsable, promoviendo ciertos criterios éticos en el uso de las nuevas tecnologías.



REINO UNIDO: **Online Safety Act (Ley de Seguridad en Línea)**⁷ para proteger a los usuarios de daños online. Impone un deber de cuidado legal y cierta responsabilidad a las empresas tecnológicas.



PAÍSES BAJOS: pionera en implementar un **modelo de responsabilidad compartida pública para combatir el fraude financiero y las estafas digitales**⁸. Basada en detectar patrones de fraude y repartir de forma equitativa la mitigación del riesgo financiero.



AUSTRALIA: implementación **del Scams Code Framework**⁹, que impone obligaciones legales y estándares de cumplimiento de ciberseguridad a bancos y empresas tecnológicas para prevenir estafas, bajo penalizaciones financieras.



ITALIA: desarrollo de un **Sandbox de Ciberseguridad**¹⁰ para el sector financiero. Se trata de un entorno de experimentación controlado que permite a las entidades financieras testar soluciones tecnológicas.



ESPAÑA: se encuentra en un **momento crítico de transposición normativa sobre seguridad en red**, donde la ciberseguridad y el bienestar digital convergen bajo nuevas exigencias:

- **Ley de Ciberseguridad**¹¹ (transposición de la **directiva NIS2** bajo el **Anteproyecto de Ley de Coordinación y Gobernanza en la Ciberseguridad**¹²): se avanza hacia un marco de responsabilidad solidaria, introduciendo la responsabilidad directa de los directivos ante brechas de seguridad. No obstante, de momento la transposición se mantiene en suspenso mientras Bruselas prepara cambios en el nuevo paquete de Ciberseguridad y el Ómnibus Digital sobre Inteligencia Artificial (IA)¹³.
- **Protección de Menores en Entornos Digitales**¹⁴: el Gobierno ha anunciado un endurecimiento regulatorio para limitar el acceso de menores de 16 años a plataformas digitales.
- **Orden Ministerial TDF/149/2025 de lucha contra estafas telefónicas**¹⁵, que obliga a las operadoras a bloquear SMS maliciosos y llamadas fraudulentas a partir de mayo de 2026.

España lidera la creación de leyes que unen bienestar y ciberseguridad bajo el modelo europeo. Este marco no solo protege a las personas vulnerables y el derecho a desconectar, sino que impone estándares de seguridad para combatir el fraude, convirtiendo la responsabilidad compartida en el motor de la confianza digital.

¹ Comisión Europea. (2022). Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital. Oficina de Publicaciones de la Unión Europea.

² Parlamento Europeo. (2022). Derechos y principios digitales: Una declaración para la transformación digital de la UE. Servicio de Investigación del Parlamento Europeo.

³ Comisión Europea. (s. f.). Ley de Servicios Digitales: Garantizar un entorno en línea seguro y responsable. Estrategia Digital de la UE.

⁴ Loi n° 2016-1088 du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels [relativa al trabajo, a la modernización del diálogo social y a la seguridad de las trayectorias profesionales] (Francia).

⁵ Ministry of Education and Culture (Finlandia). (2024). Restrictions to be placed on the use of phones and mobile devices in schools [Restricciones sobre el uso de teléfonos móviles en las aulas].

⁶ Comisión Europea. (s. f.). [Conectividad digital en Dinamarca].

⁷ Online Safety Act 2023, c. 50 (Reino Unido).

⁸ Betaalvereniging Nederland. (s. f.). Safety [Seguridad].

⁹ The Treasury (Australia). (2023). Regulating digital platform service providers [Regulación de los proveedores de servicios de plataformas digitales].

¹⁰ Banca d'Italia (s. f.). Il sandbox regolamentare [El sandbox regulatorio].

¹¹ Ministerio del Interior (España). (2025). Anteproyecto de Ley de coordinación y gobernanza de la ciberseguridad. Secretaría General Técnica.

¹² La Moncloa (2025). Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad, a efectos previstos en el artículo 26.4 de la Ley 50/1997, de 27 de noviembre, del Gobierno.

¹³ Lordiez, A. (2026). El laberinto de la Ley de Ciberseguridad en España: retrasos, presión de Europa y nuevas exigencias en camino. Demócrata.

¹⁴ La Moncloa (2026). Sánchez interviene en la sesión plenaria de la Cumbre Mundial de Gobiernos en Dubái. Presidencia del Gobierno.

¹⁵ Ministerio de Asuntos Económicos y Transformación Digital (2025). Orden TDF/149/2025, de 2025, de lucha contra estafas telefónicas. Boletín Oficial del Estado, BOE-A-2025-2870.

3. Iniciativas pioneras en el mercado para luchar contra el fraude y fomentar la ciberseguridad

En la app de ING, evitar el fraude en segundos ya es posible.



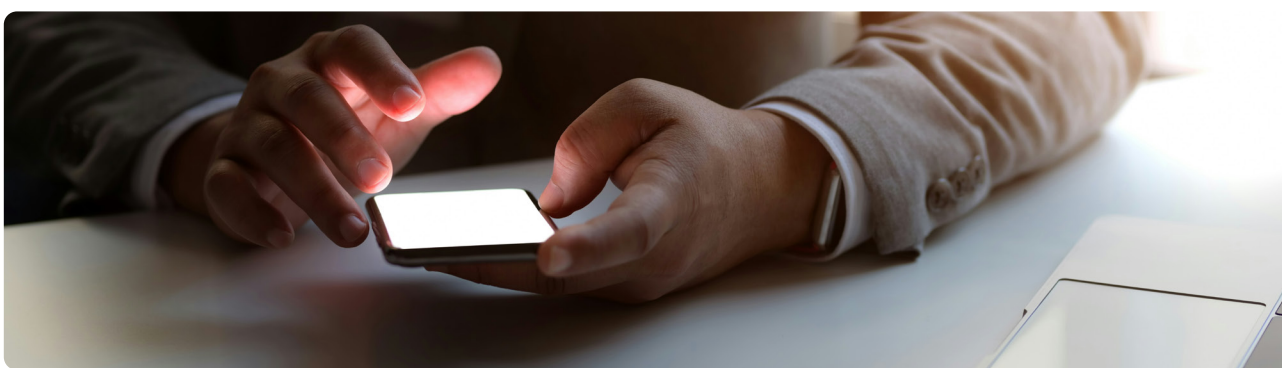
SOS Fraude¹⁶, una funcionalidad disponible en la app de ING que permite bloquear claves, tarjetas y accesos en segundos ante cualquier sospecha, eliminando la vulnerabilidad del cliente.



“¿Quién me llama?”¹⁷, un servicio que permite comprobar en tiempo real desde la aplicación si una llamada es legítima de ING, neutralizando así la suplantación telefónica.



Sistema RCS (Rich Communication Services)¹⁸, sustitución del SMS tradicional por el sistema *Rich Communication Services*, que asocia los mensajes a un perfil corporativo verificado con logotipo y marca. La adopción de este estándar garantiza la trazabilidad y autenticidad de los mensajes, reduciendo drásticamente la suplantación.



Recientemente, ING ha ampliado su ecosistema antifraude con una **nueva capa de protección en transferencias**¹⁹ que permite alertar al cliente en tiempo real cuando el sistema detecta indicios de una posible estafa. A través de la alerta, el cliente podrá decidir si continuar con la operación o si opta por detenerla con un botón específico habilitado para bloquear la acción. El sistema incorpora asimismo varios avisos consecutivos para asegurar que la decisión se toma de forma consciente e informada.



Tarjetas con CVV Dinámico²¹, tecnología que sustituye el CVV estático por un código temporal y dinámico generado en la app. Al caducar en pocos minutos, invalida los datos físicos de la tarjeta ante robos o clonaciones, eliminando la vulnerabilidad del plástico y blindando la seguridad en las compras online.



IA de Grafos (Inteligencia Artificial Semántica)²²: frente a la IA generativa convencional, esta tecnología utiliza estructuras semánticas que consultan solo fuentes expertas y hechos contrastados. Su uso en finanzas garantiza información veraz y asegura una toma de decisiones basada en datos reales.

Estas iniciativas se complementan con los **esfuerzos sectoriales como la lista blanca de SMS legítimos impulsada por la Comisión Nacional del Mercado de Valores (CNMV)**²⁰, que permite bloquear de forma más eficaz los mensajes fraudulentos. Asimismo, existen otras buenas prácticas en el mercado y a nivel regulatorio que suman en la lucha contra el fraude en línea:



Sistema IberPay Payguard, un ejemplo de colaboración en el sector financiero que permite compartir información en tiempo real entre bancos sobre cuentas utilizadas para canalizar fondos ilícitos.

En paralelo, en el **ámbito crediticio, bancos y financieras ya están compartiendo bases de datos para prevenir fraude y conocer riesgos**, evidenciando que la cooperación sectorial ya es una realidad en determinados ámbitos y puede ampliarse a otros.

¹⁶ Cybersecurity News. (2024, 25 de septiembre). ING presenta SOS Fraude, una nueva herramienta que ayuda a sus clientes a protegerse frente al fraude

¹⁷ ING. (s. f.). ¿Quién me llama? Te saca de dudas.

¹⁸ Europa Press. (2026, 20 de enero). ING también incorpora la tecnología RCS para atajar los fraudes en mensajes a móviles a sus clientes.

¹⁹ 20minutos / Servimedia. (2026, 26 de febrero). ING incorpora una nueva capa de protección antifraude en las transferencias para evitar estafas.

²⁰ Banco de España. (2025). Compendio de criterios de buenas prácticas bancarias.

²¹ BBVA (s.f.) ¿Qué es el CVV dinámico y cuál es su función?

²² CaixaBank Tech (s.f.). Grafos y Redes Neuronales: Cómo la IA Transforma las Conexiones en Valor.

4. ¿Cuáles son los retos y oportunidades para mejorar el bienestar digital a nivel individual y colectivo?

Retos	Oportunidades
Salud física, mental y psicosocial: el uso prolongado de pantallas y redes sociales causa fatiga visual (70% de los afectados), “text neck” y propicia sedentarismo. El uso antes de dormir retrasa el sueño hasta 3 horas.	Hábitos saludables: fomentar la “dieta digital” y la higiene del sueño (apagar pantallas antes de dormir) mejora el descanso y reduce el estrés.
Seguridad: el 47,4% ha sido víctima de estafas digitales y el 37% sufre ansiedad ante ciberataques. El fraude mediante <i>deepfakes</i> ha crecido un 3.000%.	Cultura de ciberseguridad: la capacitación ciudadana es la mejor defensa. Un usuario formado protege su identidad y sabe distinguir noticias falsas.
Sostenibilidad: descargar 1GB emite 7 kg de CO ₂ . Una consulta a IA consume 10 veces más energía que una búsqueda en Google.	Sobriedad digital: reducir el envío de archivos pesados, limpiar el “dark data” y alargar la vida útil de dispositivos reduce la huella de carbono.

El desafío no es el acceso a las tecnologías, sino el uso consciente. La ciberseguridad garantiza este bienestar mediante la responsabilidad compartida entre instituciones y ciudadanos, convirtiendo los retos tecnológicos en oportunidades reales de progreso.



5. Hoja de ruta para un (mayor) Bienestar Digital ante las estafas

En definitiva, es necesario avanzar hacia una **cultura de responsabilidad compartida de protección frente al fraude**, con un enfoque en el bienestar mental y protección de las personas. Para ello, es clave:



Avanzar hacia un marco europeo y nacional que consolide el paradigma de responsabilidad compartida en la lucha contra el fraude.



Involucrar a los operadores de telefonía, para luchar contra la suplantación de identidad que sufrimos las entidades financieras, consolidando la aplicación efectiva de la Orden Ministerial contra estafas telefónicas. En el proceso, **impulsar mecanismos operativos de intercambio de indicadores de amenazas entre entidades financieras y entre sectores**, para anticipar patrones de fraude en tiempo real.



Impulsar la educación y concienciación individual, de modo que **el ciudadano también conozca su papel a la hora de enfrentarse a posibles fraudes**, que no actúe con negligencia.



Concienciar a los ciudadanos a través de una educación financiera de calidad para que actúen de manera responsable y cautelosa en su actividad en red, siguiendo ciertos criterios básicos:

- **Seguir las recomendaciones de prevención del fraude** y no ignorar las advertencias explícitas sobre posible fraude en procesos de pago.
- **Proporcionar evidencias** en los casos de suplantación de identidad.
- **Cooperar adecuadamente** en los procesos de investigación del fraude.
- **Denunciar a la policía.**



En definitiva, avanzar hacia **paradigmas de responsabilidad compartida** utilizando como vector de transformación las normativas en curso y relativas a la lucha contra el fraude a nivel nacional y europeo.

El bienestar digital requiere un compromiso conjunto: los ciudadanos deben adoptar hábitos seguros y las instituciones garantizar infraestructuras resilientes.

6. Otras opiniones



Ministerio de Interior

“Durante el tercer trimestre de 2025, la **cibercriminalidad representa ya casi el 20% de la criminalidad total** en España.” (Balance Trimestral de Criminalidad)²³



Banco de España

“El **18,20% de los ciberataques** tienen lugar en el sector financiero.”²⁴



Comisión Europea

“El **acceso equitativo a la tecnología debe ir acompañado de una protección proactiva**; identificar la mejora de las capacidades digitales y la seguridad como los factores más cruciales para facilitar la transformación digital de aquí a 2030.” (Eurobarómetro Especial 2025)²⁵



OMS

“La estrategia incide en la necesidad de **contar con un sólido marco jurídico y reglamentario para proteger la privacidad, la confidencialidad y el tratamiento de los datos** sanitarios personales, y para abordar cuestiones como la ciberseguridad.”²⁶ (Proyecto de estrategia mundial sobre salud digital)



CIS

“Sobre los peligros que pueden llegar a acarrear los avances tecnológicos, **un 50,3% cree que la inteligencia artificial podría ser un problema.**”²⁷

²³ Ministerio del Interior (España). (2025). Balance de Criminalidad: Tercer Trimestre 2025. Secretaría de Estado de Seguridad.

²⁴ Escrivá, J. L. (2024, 17 de diciembre). Intervención del Gobernador del Banco de España en la inauguración de la Jornada de Ciberseguridad [Discurso]. Banco de España.

²⁵ Comisión Europea. (2025). Special Eurobarometer 2025: Report on the state of the Digital Decade [Eurobarómetro especial 2025: Informe sobre el estado de la Década Digital]. Dirección General de Redes de Comunicación, Contenido y Tecnologías.

²⁶ Organización Mundial de la Salud. (2020). Estrategia mundial sobre salud digital 2020-2025.

²⁷ Centro de Investigaciones Sociológicas. (s. f.). Nota informativa sobre la encuesta: Percepción de la ciencia y la tecnología.

Contribuimos activamente a reforzar la lucha contra el fraude digital y a avanzar hacia un mayor bienestar digital, asumiendo nuestro papel como parte de una **cadena de responsabilidades compartidas**. La seguridad financiera no depende de un único actor: requiere la acción coordinada de entidades financieras, administraciones públicas, operadores tecnológicos y ciudadanía. Desde ING trabajamos en prevención, educación financiera y uso responsable de la tecnología, convencidos de que solo desde la colaboración del conjunto del ecosistema es posible proteger de forma efectiva a las personas y fortalecer la confianza en el entorno digital.

¿Quieres profundizar?

Si necesitas ampliar información, estamos encantados de contarte más:

Nacho Rodríguez

Director de Comunicación, Relaciones Institucionales y Sostenibilidad

Tel 606 62 50 76

nacho.rodriguez.velasco@ing.com



do your thing

