



II Estudio de Bienestar Digital

Septiembre 2026

Informe completo de resultados

Autoevaluación del Bienestar Digital

Uso consciente

Ciberseguridad

Protección de datos

Confianza online

Muestra analizada: 365 respuestas válidas

Trabajo de campo: 24 de junio – 21 de julio de 2026

Dirección: Unión Española Creadores

Estudio elaborado por

Fernando Pena Vivero

Estefanía Cárcel Esteban

Juan Vicente Oltra Gutiérrez

Dirección de proyecto

Inés Berazadi Rozpide (Dirección ING)

Cristóbal Gázquez (Dirección UEC)

Índice

1. Resumen ejecutivo	4
1.1. Los diez hallazgos principales	4
2. Ficha técnica y metodología	6
2.1. Diseño del estudio	6
2.2. Estructura del cuestionario	6
2.3. Escala de interpretación	6
2.4. Advertencia metodológica	7
3. Perfil de la muestra	8
3.1. Distribución por edad	8
3.2. Distribución por nivel de estudios	8
3.3. Tipo de usuario	8
4. El resultado global	9
4.1. Puntuación total	9
4.2. Distribución por niveles	10
4.3. El bloque que el sistema señala como prioritario	10
5. Resultados por bloque	11
5.1. Ranking completo de las 27 preguntas	12
6. Análisis pregunta a pregunta	14
6.1. Bloque 1 · Tus hábitos de uso	14
6.2. Bloque 2 · Ciberseguridad	15
6.3. Bloque 3 · Protección de datos, dispositivos y sesiones	17
6.4. Bloque 4 · Prevención de riesgos y gestión de incidencias	18
6.5. Bloque 5 · Huella digital y bienestar	19
7. Segmentaciones	20
7.1. Por tramo de edad	20
7.2. Por nivel de estudios	22
7.3. Por tipo de usuario	22
8. Correlaciones entre bloques	23
8.1. Dos ejes independientes	24
8.2. Co-ocurrencia de déficits	24
9. Cuatro perfiles de usuario	29
10. La brecha de autopercepción	31
11. Conclusiones y recomendaciones	32
11.1. Las conclusiones del estudio	32
11.2. Los titulares más destacados	32
11.3. Recomendaciones por prioridad	33

Índice

12. Análisis desde la psicología del comportamiento 36

- 12.1. Dos sistemas de procesamiento, dos tipos de conducta digital 36
- 12.2. La arquitectura del hábito: señal, rutina, recompensa 37
- 12.3. El refuerzo intermitente y por qué el desplazamiento infinito no cansa 37
- 12.4. El sesgo de optimismo y el efecto tercera persona 37
- 12.5. El sueño como variable mediadora 38
- 12.6. Comparación social y uso pasivo 39
- 12.7. Aprendizaje por observación: por qué el ejemplo pesa más que la norma 39
- 12.8. Del diagnóstico a la intervención: cuatro principios operativos 40

13. Marco de ciberseguridad: qué protege realmente cada conducta 41

- 13.1. Reconocer un fraude y estar protegido frente a él son cosas distintas 41
- 13.2. Por qué la ingeniería social funciona y por qué aquí no ha funcionado 42
- 13.3. La cadena de credenciales: el ataque que no necesita engañar 42
- 13.4. El correo electrónico como llave maestra 42
- 13.5. No todos los segundos factores protegen igual 43
- 13.6. Permisos, copias y superficie de exposición 43
- 13.7. De la estafa masiva al fraude documentado 44
- 13.8. El marco normativo que ampara al usuario 44

14. Protocolos prácticos 45

- 14.1. El plan de 30 días 45
- 14.2. Protocolo 1 · Asegurar el correo principal 46
- 14.3. Protocolo 2 · Migrar a un gestor de contraseñas 46
- 14.4. Protocolo 3 · Auditoría de la huella pública 47
- 14.5. Protocolo 4 · Dormitorio sin pantallas 48
- 14.6. Protocolo 5 · Medir antes de reducir 48
- 14.7. Protocolo 6 · Acuerdo de uso con los menores del entorno 49
- 14.8. Protocolo 7 · Copias de seguridad y prueba de restauración 50
- 14.9. Protocolo 8 · Las primeras 24 horas ante un fraude bancario 50
- 14.10. Protocolo 9 · Cuando notifican una filtración de datos 51
- 14.11. Lista de verificación por bloques 52

15. Limitaciones del estudio 53

Anexos 54

- Anexo 1. Las preguntas del cuestionario 54
- Anexo 2. Resultados de las 27 preguntas 58
- Anexo 3. Bibliografía y referencias 59



1. Resumen ejecutivo

El II Estudio de Bienestar Digital recoge 365 autoevaluaciones completas, un cuestionario de 27 preguntas con respuesta única y escala de 1 a 4 puntos distribuidas en cinco bloques temáticos. La puntuación total oscila entre 27 y 108 puntos.

Los titulares del estudio

La muestra dibuja una población digitalmente competente en lo defensivo y claramente desbordada en lo atencional. Reacciona bien ante una amenaza explícita como un SMS fraudulento, una llamada sospechosa, o una wifi pública. El 90,7 % de acierto en prevención de riesgos convive con un 64,9 % en hábitos de uso, y el 62,5 % consulta el móvil ya acostado.

1.1. Los diez hallazgos principales

- 1. La puntuación media es de 82,9 puntos sobre 108, el 76,7 % del máximo.** La mediana se sitúa en 83 puntos y la desviación típica en 9,2. Ninguna persona de la muestra cae en la zona de alerta: el mínimo observado es de 56 puntos y el máximo, de 105.
- 2. Solo el 9,3 % alcanza el nivel de bienestar sólido.** El 56,7 % se sitúa en equilibrio razonable y el 34,0 % permanece en zona en desarrollo. El grueso de la muestra está, por tanto, en una franja intermedia claramente mejorable.
- 3. Existe un desequilibrio muy marcado entre bloques.** Prevención de riesgos alcanza el 90,7 % del máximo posible y ciberseguridad el 83,9 %, mientras que hábitos de uso se queda en el 64,9 % y huella digital y bienestar en el 68,9 %. La distancia entre el bloque más fuerte y el más débil es de casi 26 puntos porcentuales.
- 4. Los dos ámbitos son estadísticamente independientes.** Las correlaciones dentro del área de seguridad son altas (hasta $r = 0,616$) y las del área de uso también ($r = 0,481$), pero entre ambas áreas caen a la franja 0,22-0,40. Estar bien protegido no predice en absoluto usar bien el móvil.
- 5. La conducta de riesgo más extendida es el móvil en la cama:** el 62,5 % lo consulta al acostarse y un 38,4 % lo hace todas las noches. Es el ítem con la puntuación media más baja de todo el cuestionario (2,18 sobre 4).
- 6. Hay una brecha clara de autopercepción.** El 84,9 % afirma llevar el control de su relación con la tecnología, pero entre esas mismas personas el 58,7 % mira el móvil en la cama y el 50,6 % reconoce no controlar su tiempo de pantalla.
- 7. La edad mejora los hábitos, no la seguridad.** La correlación de la edad con hábitos de uso y con huella y bienestar es fuerte y significativa, mientras que con ciberseguridad y con protección de datos no lo es. De los 20-29 a los 50-59 años la puntuación total sube 9,2 puntos.
- 8. El nivel de estudios no discrimina en absoluto.** Las medias de estudios medios, universitarios y postgrado son 82,7, 82,9 y 82,3 puntos respectivamente. El bienestar digital no es una cuestión de credenciales académicas.

9. Emergen cuatro perfiles de usuario claramente diferenciados, dos de ellos con puntuaciones globales parecidas pero problemas opuestos: los «blindados pero enganchados» (27,1 %) y los «prudentes analógicos» (24,4 %). Tratarlos con el mismo mensaje preventivo sería un error.

10. La propia muestra reconoce dónde está el problema. El 57,0 % tiene los hábitos de uso como bloque prioritario de mejora y un 28,8 % la huella digital y el bienestar; solo un 1,6 % la ciberseguridad y un 1,1 % la prevención de riesgos.

Conclusión fundamental

El fraude ya no se siente como la principal amenaza para el bienestar digital de esta muestra: el principal riesgo es el propio hábito, y ese hábito se concentra en la noche, en la comparación social y en el ejemplo que se da a los menores.



2. Ficha técnica y metodología

2.1. Diseño del estudio

El instrumento es la Autoevaluación del Bienestar Digital: un cuestionario autoadministrado de 27 preguntas cerradas con cuatro opciones de respuesta ordenadas de menor a mayor grado de bienestar digital. Cada opción puntúa de 1 (conducta más desfavorable) a 4 (conducta óptima), de modo que la puntuación total se mueve entre 27 y 108 puntos.

Parámetro	Detalle
Universo	Personas usuarias de servicios digitales que acceden voluntariamente al test
Muestra analizada	365 respuestas válidas y completas
Trabajo de campo	Del 24 de junio al 21 de julio de 2026
Técnica	Cuestionario autoadministrado online, respuesta única por pregunta
Extensión	27 preguntas distribuidas en 5 bloques temáticos
Escala	1 a 4 puntos por pregunta; total de 27 a 108 puntos
Muestreo	No probabilístico, por autoselección (muestra de conveniencia)

2.2. Estructura del cuestionario

Los cinco bloques se han diseñado para abordar diferentes aspectos relacionados con las tecnologías, de tal manera que no tienen el mismo número de preguntas ni preguntan por los mismos temas exactamente, por lo que sus puntuaciones no se deben comparar en términos absolutos. A lo largo del informe se utiliza sistemáticamente el porcentaje sobre el máximo posible de cada bloque.

Bloque	Contenido	Preguntas	Rango
B1 • Tus hábitos de uso	Tiempo de pantalla, notificaciones y consumo automático	P1-P7 (7)	7-28
B2 • Ciberseguridad	Contraseñas, doble factor, phishing y permisos de apps	P8-P14 (7)	7-28
B3 • Protección de datos	Bloqueo, sesiones, privacidad y copias de seguridad	P15-P19 (5)	5-20
B4 • Prevención de riesgos	Recuperación de accesos y reacción ante incidencias	P20-P23 (4)	4-16
B5 • Huella digital y bienestar	Impacto ambiental, ánimo, control y menores	P24-P27 (4)	4-16

2.3. Escala de interpretación

El sistema clasifica cada puntuación total en uno de los cuatro niveles definidos por el cuestionario. Esta terminología es la utilizada a la hora de expresar los resultados encontrados en el estudio. Los diferentes niveles muestran una graduación de menor a mayor. Obsérvese con atención la siguiente tabla:

Puntos	Nivel	Lectura
27-53	Zona de alerta	La relación con lo digital pasa factura; requiere medidas inmediatas
54-79	Zona en desarrollo	Base razonable con puntos flojos que dejan expuesto en momentos concretos
80-94	Equilibrio razonable	Relación sana y segura; el margen está en los detalles
95-108	Bienestar sólido	Uso consciente, seguro y deliberado de la tecnología

2.4. Advertencia metodológica

La muestra es de autoselección: Es decir, responde quien decide hacer un test de bienestar digital, un perfil previsiblemente más sensibilizado que la población general. Los resultados describen a esta muestra y no son extrapolables al conjunto de la población. Todas las medidas son autoinformadas, con el sesgo de deseabilidad social que ello podría implicar, especialmente en el bloque de ciberseguridad.



3. Perfil de la muestra

3.1. Distribución por edad

La muestra se concentra con claridad en las edades centrales de la vida activa: los tramos de 20 a 49 años reúnen el 87,4 % de las respuestas. Los extremos están poco representados, lo que obliga a leer con prudencia los resultados de los menores de 20 años (9 casos) y de los mayores de 59 (7 casos).

Tramo de edad	n	% de la muestra	Puntuación total media
Menos de 20	9	2,5 %	74,7
20 - 29	98	26,8 %	79,3
30 - 39	134	36,7 %	82,9
40 - 49	86	23,6 %	86,0
50 - 59	31	8,5 %	88,5
Más de 59	7	1,9 %	80,9

3.2. Distribución por nivel de estudios

El 63,3 % de la muestra tiene estudios universitarios o de postgrado, una proporción muy superior a la del conjunto de la población española. Es el rasgo más evidente del sesgo de autoselección del estudio.

Nivel de estudios	n	% de la muestra
Universitarios (licenciatura o grado)	171	46,8 %
Medios (enseñanza secundaria o similar)	128	35,1 %
Postgrado (máster o doctorado)	60	16,4 %
Básicos (primaria o similar)	5	1,4 %
Ninguno	1	0,3 %

3.3. Tipo de usuario

La pregunta admite respuesta múltiple. Contabilizando también a quienes marcan «todas las anteriores», 116 personas (31,8 %) se identifican como creadoras de contenido y 189 (51,8 %) como clientes de banca digital. Un 30,1 % se define únicamente como usuario, sin ninguna de las dos condiciones anteriores.

Perfil declarado	n	% de la muestra
Cliente de banca digital (incluye «todas las anteriores»)	189	51,8 %
Creador de contenido (incluye «todas las anteriores»)	116	31,8 %
Solo usuario	110	30,1 %
Todas las anteriores	51	14,0 %



4. El resultado global

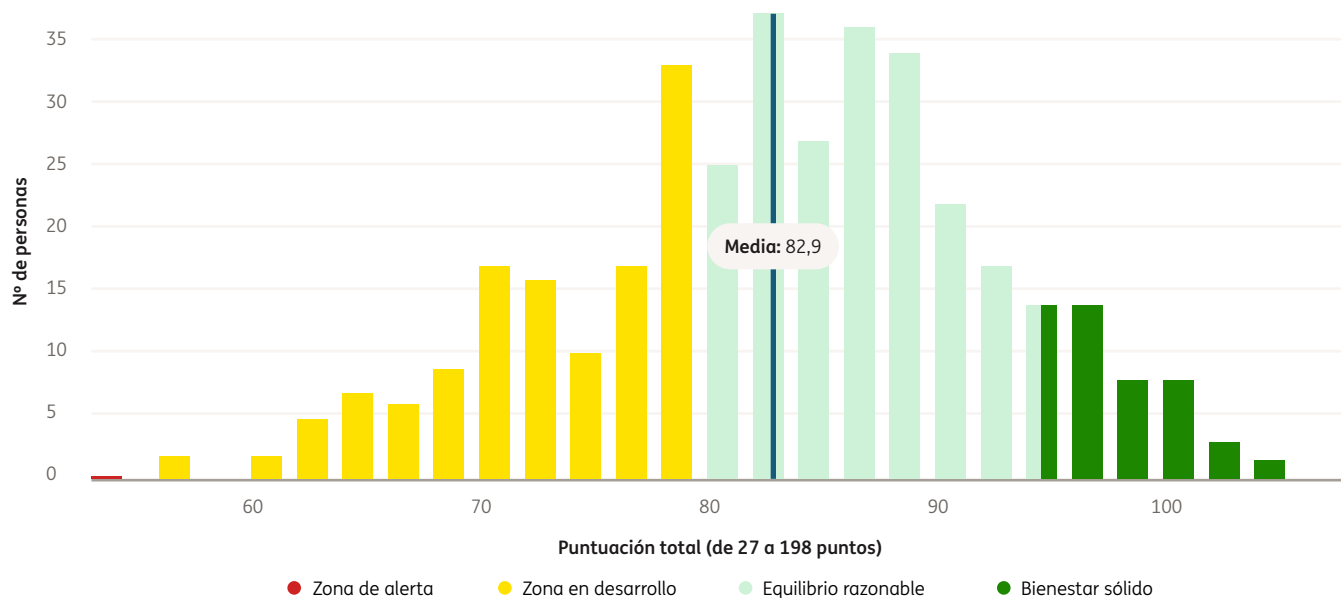
4.1. Puntuación total

La puntuación media es de 82,9 puntos sobre 108, el 76,7 % del máximo. La mediana se sitúa en 83 puntos y la desviación típica en 9,2, lo que indica una distribución bastante compacta y simétrica alrededor de la media. El recorrido observado va de 56 a 105 puntos: nadie alcanza el máximo teórico y nadie desciende a la **zona de alerta**.

La forma de la distribución es relevante por sí misma. No hay dos poblaciones separadas, sino una única masa central: la mitad de la muestra se concentra entre 78 y 89 puntos.

Distribución de la puntuación total

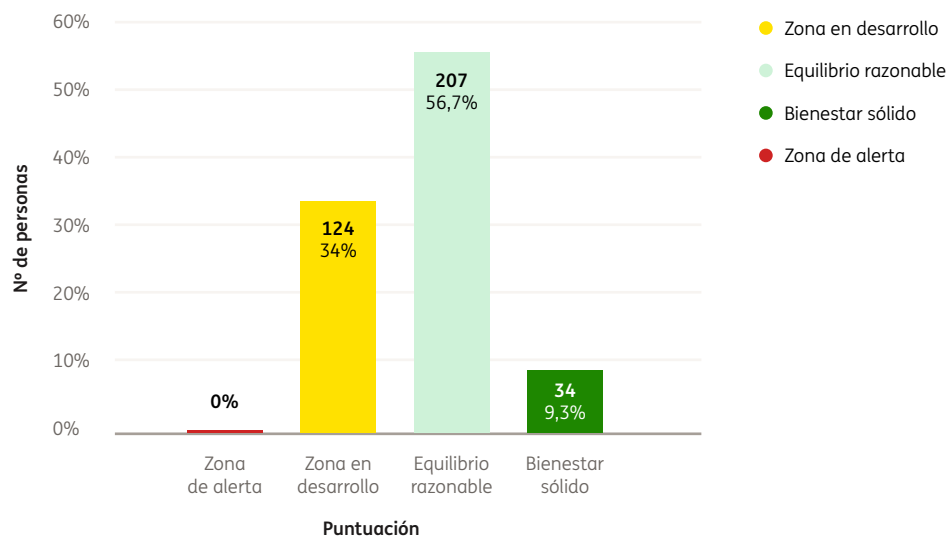
De las 365 respuestas



Datos extraídos de la muestra del II Estudio de Bienestar Digital ING/UEC

4.2. Distribución por niveles

Número de personas en cada nivel de la escala del cuestionario



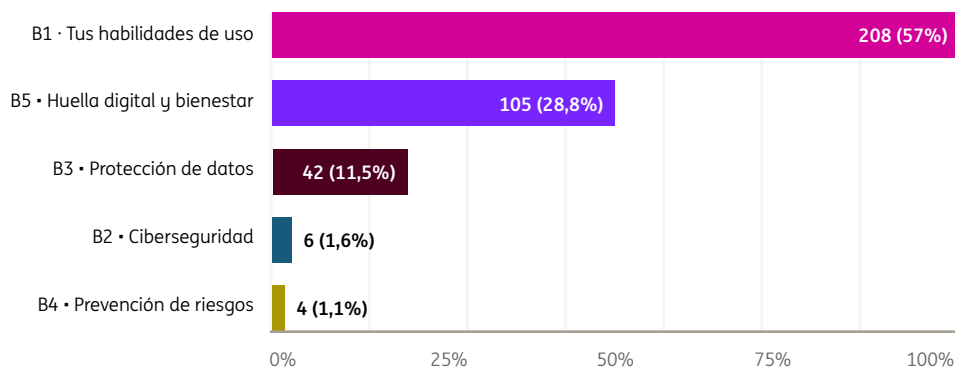
Ninguna de las 365 personas se sitúa en la zona de alerta. Este dato, que en una lectura rápida podría parecer una buena noticia exige una matización: Tenemos que tener en cuenta que quien responde voluntariamente a un test de bienestar digital difundido por canales especializados no es quien está en la peor situación.

En el otro extremo, solo 34 personas (9,3 %) alcanzan el nivel de bienestar sólido. La conclusión operativa es que el margen de mejora no está en un grupo minoritario de usuarios problemáticos, sino en la enorme franja central de personas razonablemente competentes que arrastran dos o tres hábitos claramente deficitarios.

4.3. El bloque que el sistema señala como prioritario

Bloque señalado por el sistema como prioritario

De mejora para cada persona



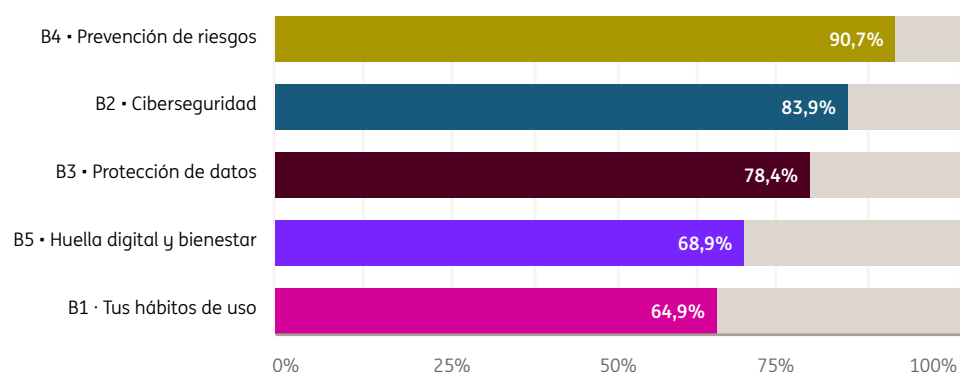
El algoritmo del cuestionario asigna a cada participante su bloque más débil. El resultado es concluyente: en 208 casos (57,0 %) el bloque más débil (que implica una mayor necesidad de mejora) son los hábitos de uso y en 105 (28,8 %) el bloque más débil la huella digital y el bienestar. Entre ambos suman el 85,8 % de la muestra. Los tres bloques defensivos se reparten el 14,2 % restante: la protección de datos, dispositivos y sesiones aparece como prioridad en 42 casos (11,5 %), la ciberseguridad en 6 (1,6 %) y la prevención de riesgos en 4 (1,1 %).

« Ocho de cada diez participantes tienen su punto más débil en cómo usan la tecnología. »



5. Resultados por bloque

Porcentaje medio alcanzado sobre el máximo posible de cada bloque



Bloque	Media	Máximo	% del máximo	Desv. típica	Mínimo
B4 • Prevenção de riesgos	14,50	16	90,7 %	1,51	5
B2 • Ciberseguridad	23,50	28	83,9 %	2,74	14
B3 • Protección de datos	15,67	20	78,4 %	2,49	8
B5 • Huella digital y bienestar	11,02	16	68,9 %	2,18	5
B1 • Tus hábitos de uso	18,17	28	64,9 %	4,09	9

El perfil es inequívocamente en forma de sierra. Los tres bloques defensivos (prevención, ciberseguridad y protección de datos) se mueven entre el 78 % y el 91 % del máximo, mientras que los dos bloques que tienen que ver con la **autorregulación del uso** y con el **bienestar personal** se quedan entre el 65 % y el 69 %.

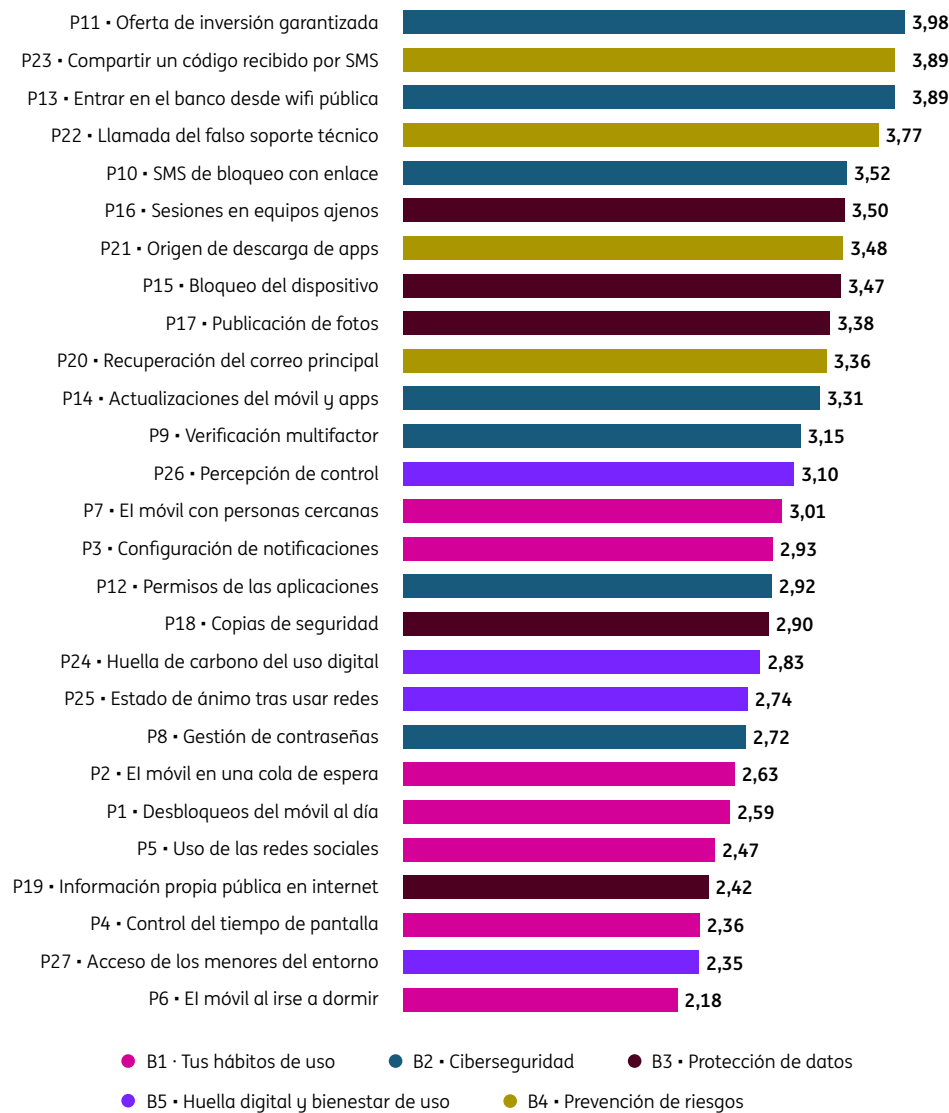
Obsérvese también la dispersión, que suele pasarse por alto y aquí resulta un dato interesante y muy informativo: el bloque de **hábitos de uso** tiene una desviación típica de 4,09 puntos, casi el triple que el de **prevención de riesgos** (1,51). Esto viene a decir que en materia de cuidado y prevención del fraude casi todo el mundo responde muy parecido; sin embargo, en materia de hábitos relacionados con el uso de la tecnología hay diferencias enormes entre unas personas y otras. El bloque 1 de “Tus hábitos de uso” es el que realmente separa a la muestra y, por tanto, el que más información aporta sobre cada persona.

Una precisión importante sobre lo que mide el cuestionario

Los 27 ítems son conductuales: preguntan qué hace la persona, no qué sabe. Por eso conviene evitar la lectura fácil de “saben mucho de seguridad pero tienen malos hábitos”. Lo que los datos muestran es una diferencia entre dos tipos de conducta: la que se activa ante una amenaza explícita y reconocible (un SMS con un enlace, una llamada urgente, una wifi abierta) y la que exige sostenerse sola, sin que nadie la interpele, día tras día. La primera funciona muy bien en esta muestra y cuando se activa una amenaza los sujetos afirman responder de forma adecuada; la segunda, mucho peor.

5.1. Ranking completo de las 27 preguntas

Puntuación media de cada pregunta
De la más deficitaria a la más sólida



El gráfico anterior condensa el diagnóstico del estudio. Las siete preguntas peor puntuadas incluyen cinco de las siete del bloque de **hábitos de uso**. Las siete mejor puntuadas incluyen las cuatro del bloque de **prevención de riesgos** y las tres preguntas de **ciberseguridad** planteadas como situaciones de fraude explícito.

Las 5 preguntas que evidencian las áreas de mejora más importantes	Media
P6 • El móvil cuando te vas a dormir	2,18
P27 • Acceso de los menores del entorno al móvil e interne	2,35
P4 • Conocimiento y control del tiempo de pantalla	2,36
P19 • Información propia pública en internet	2,42
P5 • Uso de las redes sociales	2,47

Las 5 preguntas más sólidas que evidencian los aspectos mejor trabajados	Media
P11 · Oferta de inversión con rentabilidad garantizada	3,98
P13 · Entrar en el banco desde una wifi pública	3,89
P23 · Compartir un código recibido por SMS	3,89
P22 · Llamada urgente del falso soporte técnico	3,77
P10 · SMS de bloqueo de cuenta con enlace acortado	3,52

La distancia entre los extremos es de 1,80 puntos sobre una escala de 4, casi la mitad del recorrido posible. Y el patrón es nítido y bien definido:

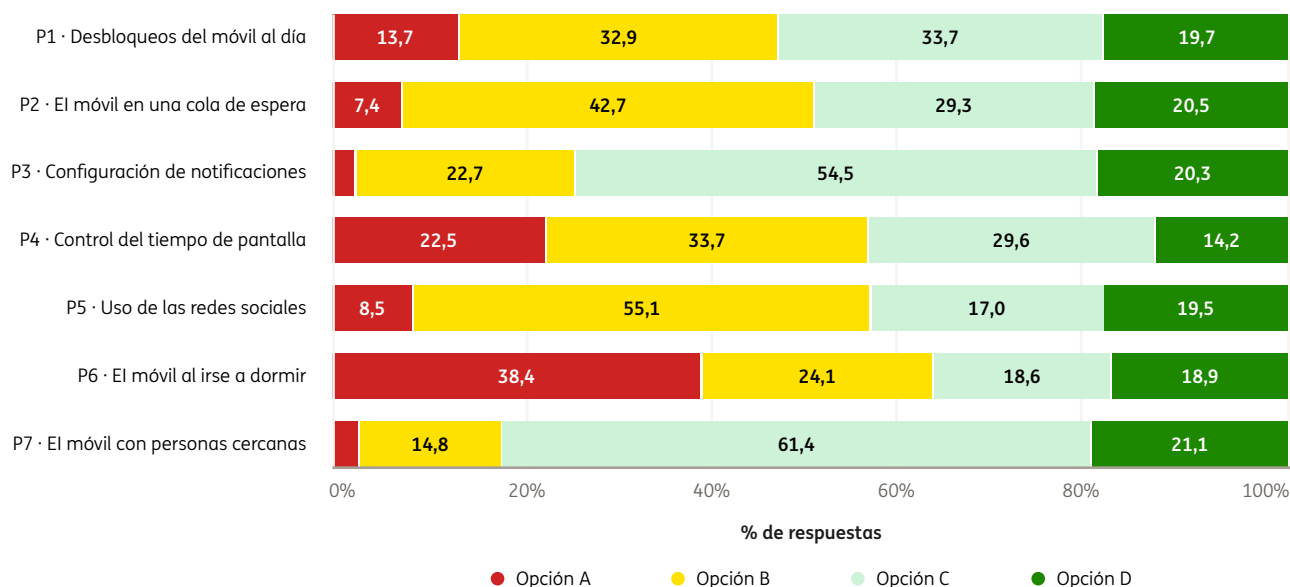
- Cuando la amenaza viene de fuera y está señalizada, la muestra responde casi perfecto”
- Cuando la conducta depende únicamente de la propia voluntad y se repite a diario, el resultado cae drásticamente”

6. Análisis pregunta a pregunta

En los gráficos de esta sección, cada barra reparte el 100 % de las respuestas de una pregunta entre las cuatro opciones, de la menos favorable (a, en rojo) a la óptima (d, en verde). Las cifras dentro de las barras son porcentajes.

6.1. Bloque 1 · Tus hábitos de uso

Distribución de respuestas Preguntas 1 a 7



El bloque 1 es el bloque más débil del estudio (64,9 % del máximo) y también el más heterogéneo. Dentro de él conviven resultados razonables y otros francamente preocupantes que implicarían acciones vinculadas con la educación de los individuos en hábitos de uso saludable.

El móvil en la cama (P6): el punto más deficitario del estudio

Con 2,18 puntos de media es el peor ítem de las 27 preguntas. El 38,4 % reconoce que todas las noches se acuesta y mira el móvil un rato, y otro 24,1 % lo hace algunas veces: en conjunto, el 62,5 % de la muestra lleva la pantalla a la cama. Solo el 18,9 % declara no consultarlo ni en la cama ni antes de dormir.

El dato merece atención especial porque es el que enlaza de forma más directa con la salud: la exposición a pantallas en el momento del sueño retrasa el inicio del descanso y degrada su calidad y profundidad del sueño. El descanso reparador es habitualmente un dato de alta relevancia muy vinculado con el bienestar psicológico y el estado de ánimo al día siguiente. No es un hábito más de la lista; es probablemente el que más consecuencias arrastra.

El tiempo de pantalla (P4): más de la mitad no lo controla

Un 22,5 % reconoce que su tiempo de pantalla es muchísimo y que no tiene control sobre ello, y un 33,7 % lo intuye por encima de lo que le gustaría. Sumados, el 56,2 % de la muestra admite un tiempo de pantalla superior al deseado. Solo el 14,2 % afirma no depender demasiado del móvil.

El consumo automático (P1, P2, P5)

Las tres preguntas que miden el automatismo dibujan el mismo cuadro. El 46,6 % desbloquea el móvil de forma refleja o sin llevar la cuenta (P1); el 50,1 % saca el móvil en una cola sin pensarlo o ya lo llevaba en la mano (P2); y el 63,6 % reconoce que se le pasan las horas en las redes o que entra «un momento» y se le va más de media hora (P5). Esta última es especialmente reveladora: la opción b —entrar un momento y perder media hora sin darse cuenta— la marca el 55,1 % de la muestra, la concentración de respuestas más alta de todo el cuestionario en una sola opción intermedia.

Lo que sí funciona: notificaciones y presencia (P3, P7)

Frente a lo anterior, el 74,8 % declara recibir solo las notificaciones importantes o aplicar sistemas de restricción por franjas, y el 82,5 % afirma guardar el móvil o atenderlo solo si es importante cuando está con personas que le importan. Son las dos preguntas mejor puntuadas del bloque (2,93 y 3,01).

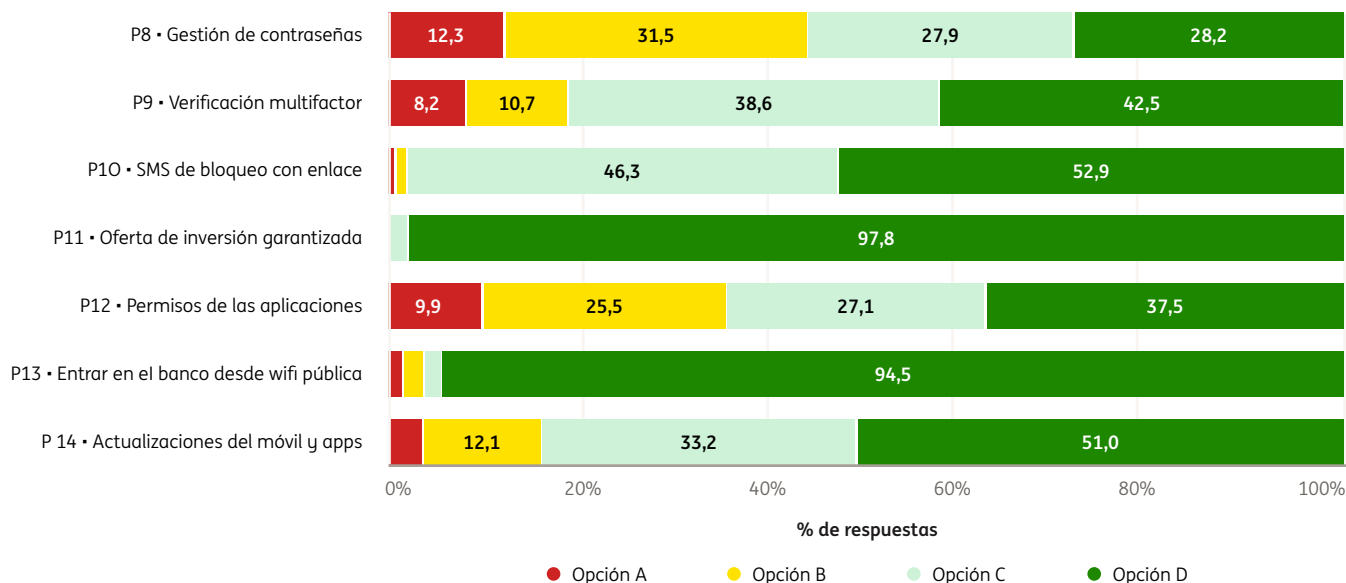
Lectura del bloque 1

La muestra ha interiorizado las medidas visibles y socialmente sancionadas (silenciar notificaciones que puedan molestar a otras personas, no mirar el móvil delante de otros) pero no las invisibles, las que solo se sostienen ante uno mismo y de las que solo uno mismo toma nota: por ejemplo, el rato con el móvil en la cama, el desbloqueo automático cuando esperamos en una cola, la media hora que se escurre en el carrusel infinito de las redes sociales. Según esto, podemos entender que **“la cortesía digital está razonablemente bien resuelta, pero la autorregulación, no.”**

6.2. Bloque 2 · Ciberseguridad

Distribución de respuestas

Preguntas 8 a 14



Es el segundo bloque más alto (83,9 %), pero la media global esconde una división muy nítida entre dos tipos de pregunta.

Ante el fraude explícito, los resultados son casi perfectos

El 97,8 % rechaza de plano la oferta de inversión con rentabilidad garantizada (P11) y acude a entidades reguladas; ningún participante marca las dos opciones peores. El 94,5 % evita entrar en el banco desde una wifi pública y usa datos móviles o una red de confianza (P13). Y el 99,2 % no pincha el enlace del SMS de bloqueo de cuenta (P10), aunque conviene matizar el dato: el 46,3 % se limita a borrar el mensaje mientras que el 52,9 % da el paso adicional de verificar por el canal oficial.

En las conductas de mantenimiento, los resultados son mediocres

La gestión de contraseñas (P8) es la pregunta más floja del bloque, con 2,72 puntos. Un 12,3 % usa la misma clave o casi la misma en todo y un 31,5 % maneja varias sin criterio: el 43,8 % de la muestra tiene, por tanto, una gestión de contraseñas insegura. Solo el 28,2 % utiliza un gestor de contraseñas, que es la única respuesta realmente robusta.

La verificación multifactor (P9) muestra un panorama mejor pero incompleto: el 42,5 % la tiene activada en todas sus cuentas importantes y un 38,6 % solo en algunas, normalmente correo y banco. Un 18,9 % no la tiene activada en casi ningún sitio o desconoce qué es.

Los permisos de las aplicaciones (P12) reparten a la muestra casi por cuartos: el 37,5 % revisa cada permiso y concede solo los estrictamente necesarios, pero un 35,3 % acepta todo o lo revisa muy por encima. Las actualizaciones (P14) están mejor resueltas, con un 84,1 % que las tiene en automático o las instala pronto.

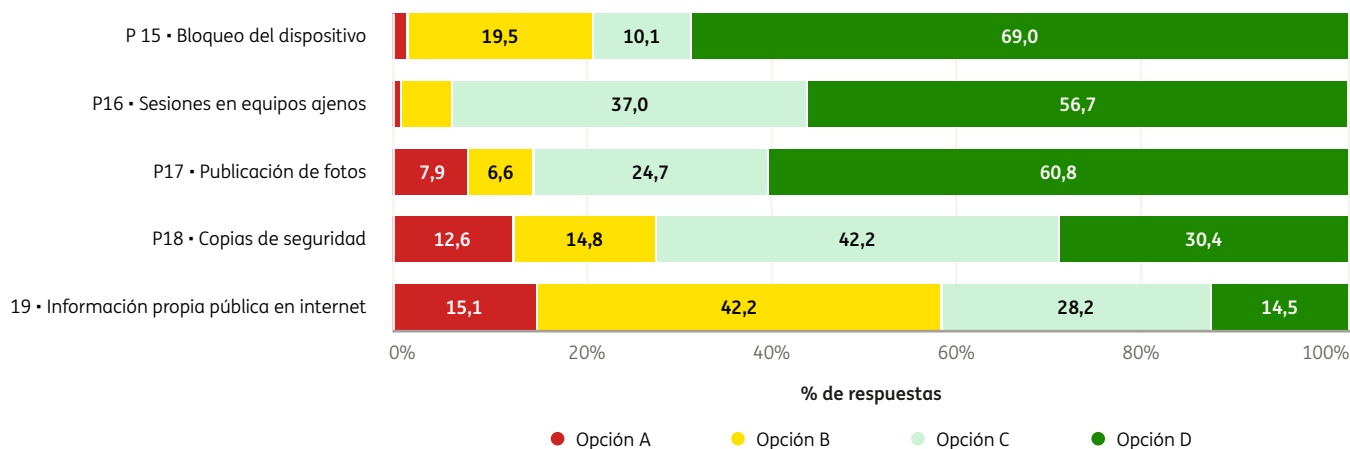
Lectura del bloque 2

La distancia entre P11 (3,98) y P8 (2,72) resume el bloque entero. Reconocer una estafa es un acto puntual que la muestra ejecuta casi sin fallo; mantener un gestor de contraseñas es una rutina sostenida que menos de un tercio ha adoptado y no la tienen por costumbre. La protección de esta muestra **depende demasiado de su capacidad de reacción** y demasiado poco de su infraestructura creada como un hábito.

6.3. Bloque 3 · Protección de datos, dispositivos y sesiones

Distribución de respuestas

Preguntas 15 a 19



Con un 78,4 % del máximo, este bloque ocupa una posición intermedia, aunque contiene una de las preguntas más deficitarias del estudio.

El bloqueo del dispositivo (P15) está bien resuelto: el 69,0 % usa biometría o PIN robusto con bloqueo automático rápido, y solo un 1,4 % no tiene ningún bloqueo. El cierre de sesiones en equipos ajenos (P16) es la segunda pregunta más alta del bloque: el 93,7 % cierra sesión al terminar y más de la mitad usa además ventana privada y comprueba después.

La publicación de fotos (P17) obtiene 3,38 puntos, con un 60,8 % que controla la audiencia, no comparte ubicación en tiempo real y revisa quién aparece en la imagen. Persiste, sin embargo, un 14,5 % que publica al momento o casi sin pensarlo.

Las copias de seguridad (P18) y la huella pública (P19)

Un 27,4 % perdería casi todos o bastantes de sus datos si mañana perdiera el móvil. Es un porcentaje alto para un riesgo que no depende de ningún atacante, sino de un simple accidente.

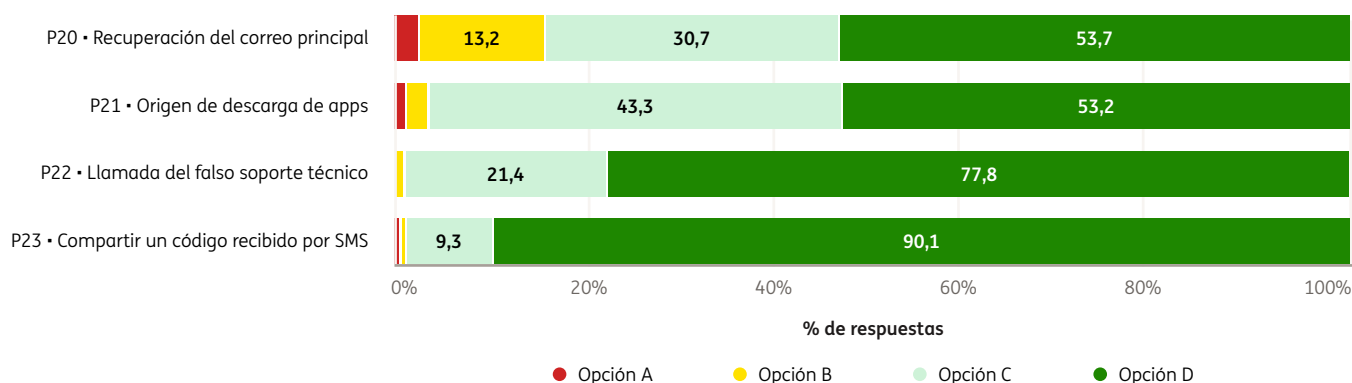
La pregunta 19 es la cuarta peor de todo el cuestionario (2,42 puntos). El 15,1 % nunca ha mirado qué información suya hay pública en internet y un 42,2 % lo miró alguna vez por curiosidad hace bastante tiempo: el 57,3 % de la muestra, por tanto, no tiene ni idea de cuál es su exposición pública actual. Solo el 14,5 % la revisa y la gestiona activamente cerrando cuentas antiguas.

« La muestra protege bien el dispositivo que tiene en la mano y muy mal el rastro que ha ido dejando durante años. »

6.4. Bloque 4 · Prevención de riesgos y gestión de incidencias

Distribución de respuestas

Preguntas 20 a 23



Es el bloque más alto del estudio (90,7 % del máximo) y también el más homogéneo: su desviación típica de 1,51 puntos es la menor de los cinco bloques, lo que significa que aquí casi todo el mundo responde igual y responde bien.

El 90,1 % nunca comparte un código de verificación recibido por SMS sin comprobación absoluta (P23) y el 77,8 % cuelga ante una llamada de falso soporte y contacta únicamente por el canal oficial (P22). La descarga de aplicaciones (P21) también está resuelta: el 96,5 % descarga casi siempre o únicamente desde tiendas oficiales.

El eslabón débil: la recuperación del correo (P20)

La pregunta 20 desentona con el resto del bloque: es la única por debajo de 3,4 puntos. Un 2,5 % no sabría por dónde empezar si perdiera el acceso a su correo principal, un 13,2 % lo intentaría sin tener nada preparado y un 30,7 % recuerda haber configurado algo en su día pero tendría que buscarlo. En total, el 46,3 % de la muestra no tiene claro cómo recuperaría su cuenta de correo.

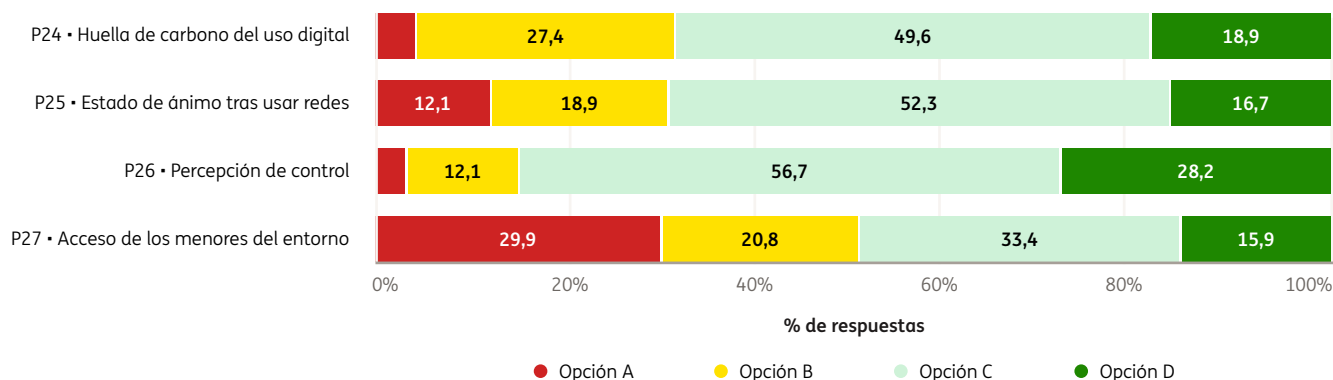
Por qué esta pregunta importa más de lo que parece

El correo principal es la llave maestra de la identidad digital: es la vía de restablecimiento de contraseñas de prácticamente todos los demás servicios, incluida la banca. Que casi la mitad de una muestra que puntúa un 90,7 % en prevención de riesgos no tenga resuelta su recuperación convierte este ítem en la vulnerabilidad más rentable de todo el estudio: es barata y fácil de corregir, y su fallo es catastrófico.

6.5. Bloque 5 · Huella digital y bienestar

Distribución de respuestas

Preguntas 24 a 27



Con un 68,9 % del máximo, es el segundo bloque más bajo y el que reúne las preguntas de naturaleza más diversa: impacto ambiental, estado de ánimo, percepción de control y educación digital de los menores.

Los menores (P27): la segunda peor pregunta del estudio

Con 2,35 puntos de media, la pregunta sobre cómo acceden los menores del entorno al móvil y a internet es la segunda más deficitaria de las 27. Un 29,9 % describe un acceso bastante libre y sin normas claras y un 20,8 % gestiona el asunto por la vía de la prohibición sin explicar motivos ni hábitos saludables. Es decir, la mitad de la muestra (50,7 %) no acompaña educativamente a los menores de su entorno: o los deja solos o les prohíbe sin más. Solo un 15,9 % describe un acompañamiento con normas pactadas, explicación de riesgos y ejemplo propio.

Este resultado es el que tiene mayor efecto multiplicador de todo el estudio, porque no afecta solo a quien responde: se transmite. Y conecta directamente con el bloque 1, ya que el ejemplo propio —el móvil en la mesa, el móvil en la cama— es la parte del acompañamiento que no se puede delegar en ninguna herramienta de control parental.

El efecto en el ánimo (P25)

Un 12,1 % se siente peor después de un buen rato en redes sociales, con comparación, ansiedad o sensación de tiempo perdido, y un 18,9 % se queda algo inquieto o disperso: el 31,0 % de la muestra reconoce un efecto negativo. Un 52,3 % dice sentirse más o menos igual y solo un 16,7 % afirma sentirse bien porque las usa de forma intencionada y limitada.

La huella ambiental (P24)

El conocimiento existe pero no se traduce en conducta: el 49,6 % sabe que el uso de internet genera huella de carbono y a veces lo tiene en cuenta, pero solo el 18,9 % aplica hábitos concretos. Un 31,5 % no lo sabía o no lo tiene en cuenta. Es la dimensión con más recorrido divulgativo del cuestionario y, a la vez, la menos urgente en términos de riesgo personal.

La percepción de control (P26)

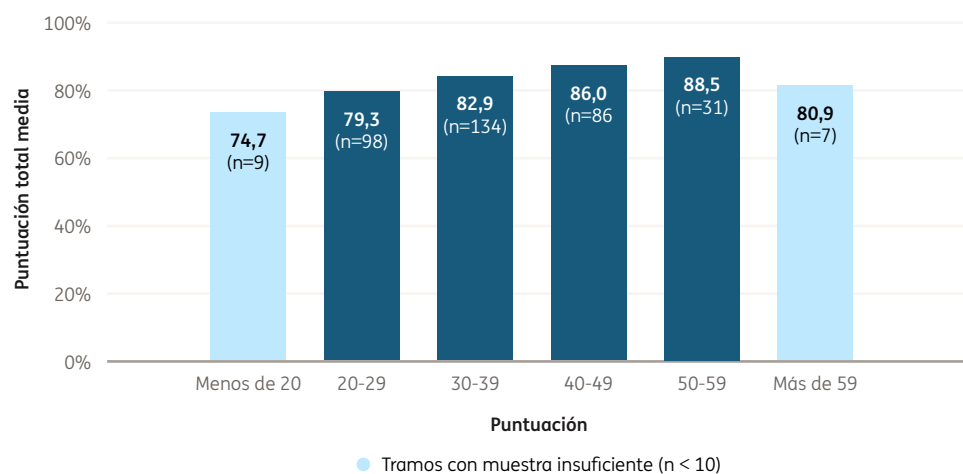
El 84,9 % de la muestra afirma tener el control de su relación con la tecnología: un 56,7 % describe un equilibrio con altibajos y un 28,2 % declara control pleno. Solo un 15,1 % reconoce ir a remolque. Este dato, contrastado con el resto del cuestionario, da lugar al hallazgo que se analiza en el capítulo 10.



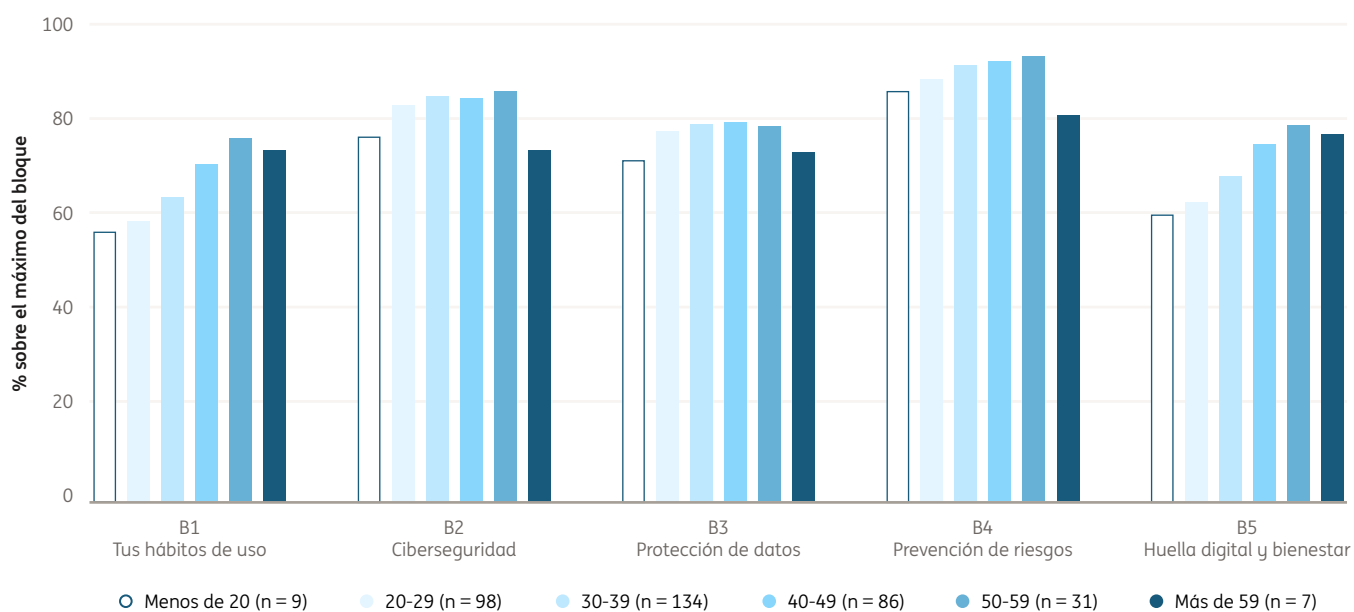
7. Segmentaciones

7.1. Por tramo de edad

Puntuación total media por tramo de edad



Resultado en cada bloque según el tramo de edad



Datos extraídos de la muestra del II Estudio de Bienestar Digital ING/UEC

La edad es la única variable sociodemográfica con capacidad explicativa en este estudio. El análisis de varianza sobre los tramos con muestra suficiente arroja una diferencia claramente significativa ($F = 13,54$; $p = 2,3 \times 10^{-8}$), y la puntuación total crece de forma monótona desde los menores de 20 años hasta los 50-59.

Tramo de edad	n	Total	B1	B2	B3	B4	B5
Menos de 20	9	74,7	56,3 %	76,2 %	71,1 %	86,1 %	59,7 %
20 – 29	98	79,3	58,5 %	83,0 %	77,5 %	88,3 %	62,6 %
30 – 39	134	82,9	63,5 %	84,9 %	79,1 %	91,5 %	67,9 %
40 – 49	86	86,0	70,6 %	84,3 %	79,3 %	92,4 %	74,6 %
50 – 59	31	88,5	76,0 %	85,8 %	78,5 %	93,1 %	78,4 %
Más de 59	7	80,9	73,5 %	73,5 %	72,9 %	80,4 %	76,8 %

Dónde mejora la edad y dónde no

El detalle por bloques es más interesante que el total. La correlación de Spearman entre el tramo de edad y cada bloque revela que la mejora no es uniforme, sino que **se concentra por completo en el eje de la autorregulación**:

Bloque	rho de Spearman	p	Interpretación
B5 · Huella digital y bienestar	0,399	< 0,001	Asociación clara y significativa
B1 · Tus hábitos de uso	0,381	< 0,001	Asociación clara y significativa
B4 · Prevención de riesgos	0,139	0,008	Asociación débil pero significativa
B2 · Ciberseguridad	0,077	0,140	Sin asociación significativa
B3 · Protección de datos	0,036	0,489	Sin asociación significativa

Del tramo de 20-29 al de 50-59 los hábitos de uso pasan del 58,5 % al 76,0 % del máximo —17,5 puntos porcentuales de mejora— y la huella y el bienestar del 62,6 % al 78,4 %. En cambio, la ciberseguridad apenas se mueve (del 83,0 % al 85,8 %) y la protección de datos permanece prácticamente idéntica (77,5 % frente a 78,5 %).

Un contraste que merece atención

Los tramos jóvenes de esta muestra no son descuidados con la seguridad: puntúan igual que sus mayores en ciberseguridad y en protección de datos. Lo que los distingue es la gestión de su tiempo, de su descanso y de su exposición emocional a las redes. El discurso público sobre «jóvenes e internet» suele centrarse en el riesgo de fraude, que aquí no aparece como diferencial, y suele desatender la autorregulación, que es donde está toda la brecha.

7.2. Por nivel de estudios

Nivel de estudios	n	Total	B1	B2	B3	B4	B5
Medios (secundaria o similar)	128	82,7	65,8 %	83,2 %	77,4 %	90,3 %	69,2 %
Universitarios (grado o licenciatura)	171	82,9	64,7 %	83,9 %	79,0 %	90,5 %	69,0 %
Postgrado (máster o doctorado)	60	82,3	62,3 %	85,1 %	78,5 %	91,4 %	67,2 %

El resultado es rotundo por su ausencia de efecto: las tres categorías con muestra suficiente arrojan medias de 82,7, 82,9 y 82,3 puntos. El análisis de varianza no detecta ninguna diferencia ($F = 0,09$; $p = 0,911$). El nivel de estudios no explica absolutamente nada del bienestar digital de esta muestra.

Es más, la única tendencia perceptible apunta en dirección contraria a la intuición: el grupo con postgrado obtiene la puntuación más baja en hábitos de uso (62,3 %) y en huella y bienestar (67,2 %), a la vez que la más alta en ciberseguridad (85,1 %). Un mayor nivel formativo se asocia aquí a algo más de solidez técnica y, si acaso, a algo más de dependencia del dispositivo, probablemente por razones profesionales.

« El bienestar digital no se estudia, se practica. Ningún título académico protege del móvil en la mesilla de noche. »

7.3. Por tipo de usuario

Los 116 participantes que se identifican como creadores de contenido obtienen una media de 83,2 puntos, frente a 82,7 de los 249 restantes. La diferencia no es estadísticamente significativa ($t = 0,50$; $p = 0,619$). Contra lo que podría esperarse, los creadores no muestran peores hábitos de uso: puntúan incluso ligeramente por encima en el bloque 1 (66,2 % frente a 64,3 %) y en huella y bienestar (70,2 % frente a 68,3 %). Su relación con las redes es profesional y, por tanto, más deliberada.

Entre los 189 clientes de banca digital se aprecia el patrón simétrico: puntúan por encima en ciberseguridad (85,1 % frente a 83,0 %) y por debajo en hábitos de uso (63,9 % frente a 65,9 %) y en huella y bienestar (67,7 % frente a 70,2 %). Son diferencias pequeñas, de dos puntos porcentuales, pero coherentes: la familiaridad con la operativa bancaria digital refuerza la seguridad, no la autorregulación.

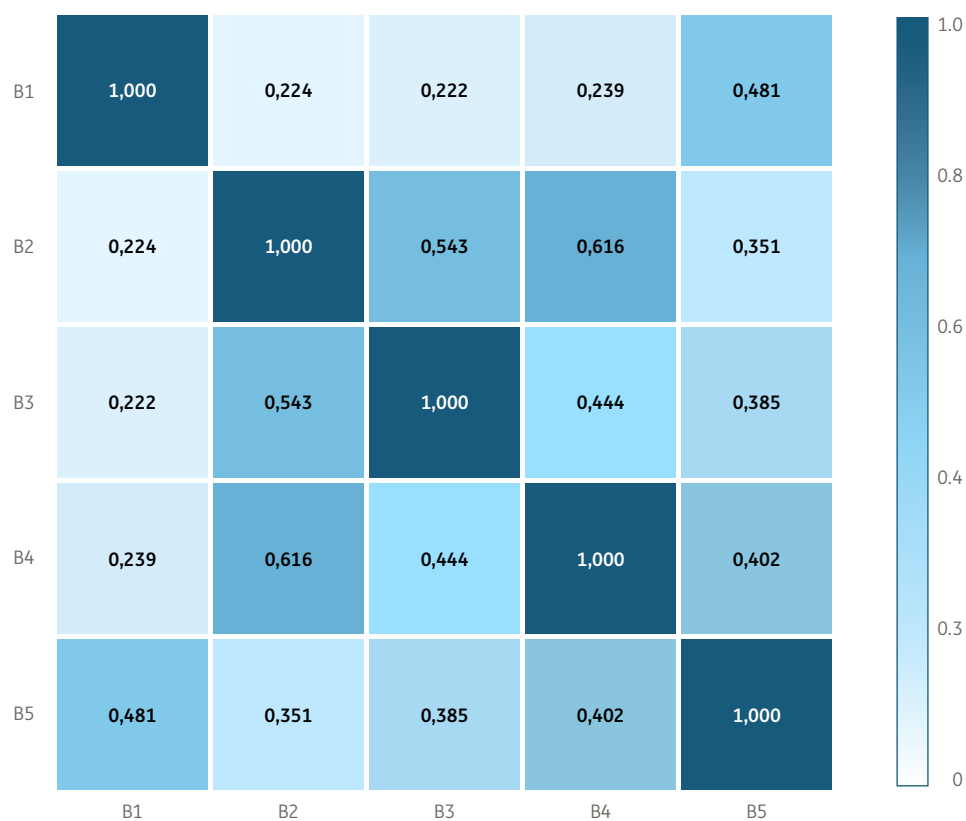
Nivel de estudios	n	Total	B1	B2	B3	B4	B5
Creadores de contenido	116	83,2	66,2 %	83,2 %	78,5 %	90,4 %	70,2 %
Resto de la muestra	249	82,7	64,3 %	84,3 %	78,3 %	90,8 %	68,3 %
Clientes de banca digital	189	82,9	63,9 %	85,1 %	78,7 %	91,0 %	67,7 %
No clientes de banca digital	176	82,9	65,9 %	83,0 %	78,0 %	90,2 %	70,2 %



8. Correlaciones entre bloques

Matriz de correlaciones de Pearson

Entre las puntuaciones de los cinco bloques



La matriz de correlaciones es un resultado interesante dentro del estudio, porque revela que el bienestar digital no es una competencia única sino dos competencias distintas que apenas se solapan.

Pareja de bloques	r de Pearson	p	Interpretación
B2 Ciberseguridad × B4 Prevención	0,616	< 0,001	Asociación fuerte
B2 Ciberseguridad × B3 Protección	0,543	< 0,001	Asociación fuerte
B1 Hábitos × B5 Huella y bienestar	0,481	< 0,001	Asociación moderada-fuerte
B3 Protección × B4 Prevención	0,444	< 0,001	Asociación moderada
B4 Prevención × B5 Huella	0,402	< 0,001	Asociación moderada
B3 Protección × B5 Huella	0,385	< 0,001	Asociación moderada
B2 Ciberseguridad × B5 Huella	0,351	< 0,001	Asociación débil-moderada
B1 Hábitos × B4 Prevención	0,239	< 0,001	Asociación débil
B1 Hábitos × B2 Ciberseguridad	0,224	< 0,001	Asociación débil

8.1. Dos ejes independientes

Las correlaciones se agrupan de forma nítida. Los bloques 2, 3 y 4 forman un racimo interno con valores de 0,44 a 0,62: quien protege bien sus contraseñas también hace copias de seguridad y también sabe reaccionar ante una llamada fraudulenta. Los bloques 1 y 5 forman un segundo racimo con $r = 0,481$: quien regula su tiempo de pantalla también se siente mejor después de usar las redes y da mejor ejemplo a los menores.

Entre ambos racimos, en cambio, las correlaciones caen a la franja 0,22-0,40. La más baja de todas es precisamente la que uniría los dos extremos del cuestionario: hábitos de uso con protección de datos ($r = 0,222$).

Qué implica esta independencia

Que el bienestar digital no puede tratarse como una única competencia que se «tiene» o «no se tiene». **Un programa formativo que refuerce la ciberseguridad no mejorará los hábitos de uso, y viceversa.** Son dos objetivos distintos, con destinatarios parcialmente distintos, que requieren dos intervenciones distintas. Es también la razón por la que la puntuación total, tomada aisladamente, es un indicador engañoso: dos personas con 83 puntos pueden tener problemas exactamente opuestos.

8.2. Co-ocurrencia de déficits

El apartado anterior trabaja con las puntuaciones agregadas de los cinco bloques. Este desciende al nivel de la conducta concreta y responde a una pregunta distinta: cuando una persona falla en un ítem, ¿falla también en los que están conceptualmente próximos? La respuesta importa para el diseño de cualquier acción, porque determina si conviene dirigirse a conductas sueltas o a paquetes de conductas que viajan juntas.

Para cada par de ítems se ha construido una tabla de contingencia de dos por dos, dicotomizando cada pregunta en la conducta deficitaria frente al resto, y se ha aplicado la prueba de ji-cuadrado con corrección de continuidad de Yates. Se acompaña de dos medidas del tamaño del efecto: el coeficiente phi, que en tablas de dos por dos equivale a la V de Cramér, y la razón de momios con su intervalo de confianza al 95 %. En todos los cruces las frecuencias esperadas superan holgadamente el mínimo exigido por la prueba.

Contraseñas y verificación multifactor

El primer cruce enfrenta el uso de gestor de contraseñas (P8, opción d) con la cobertura completa del segundo factor (P9, opción d).

Respuesta del usuario	MFA en todas las cuentas	MFA parcial o nula	Total
Usa gestor de contraseñas	69 (67,0 %)	34 (33,0 %)	103
No usa gestor de contraseñas	86 (32,8 %)	176 (67,2 %)	262
Total	155	210	365

$\chi^2 (1) = 33,94; p < 0,001; \phi = 0,311; \text{razón de momios} = 4,15 \text{ (IC 95 \% : 2,56 - 6,75)}.$

La asociación es fuerte y va en la dirección esperada, pero el dato relevante para la intervención es el otro: dos de cada tres personas que no usan gestor de contraseñas tampoco tienen el segundo factor completo. En términos absolutos, 176 participantes —el 48,2 % de la muestra— acumulan simultáneamente las dos carencias de configuración más importantes del bloque de ciberseguridad. No son dos problemas que afecten a poblaciones distintas: son el mismo problema en las mismas personas.

La lectura inversa es igual de útil. Entre quienes sí usan gestor, el 67,0 % tiene además el segundo factor en todas sus cuentas, frente al 32,8 % de quienes no lo usan: la probabilidad de tener la protección completa se multiplica por cuatro. Quien da el paso de instalar un gestor tiende a dar también el siguiente, lo que sugiere que esa primera acción funciona como puerta de entrada al resto de la configuración.

Verificación multifactor y recuperación del correo

El segundo cruce es el más intenso de todos los analizados y conecta las dos piezas que sostienen el acceso a la identidad digital: el segundo factor (P9) y la recuperación de la cuenta de correo (P20).

Respuesta del usuario	Recuperación no resuelta	Recuperación resuelta	Total
MFA en todas las cuentas	38 (24,5 %)	117 (75,5 %)	155
MFA parcial o nula	131 (62,4 %)	79 (37,6 %)	210
Total	169	196	365

$\chi^2 (1) = 49,91; p < 0,001; \phi = 0,375; \text{razón de momios} = 5,11 \text{ (IC 95 \% : 3,22 - 8,09)}.$

El 62,4 % de quienes tienen el segundo factor incompleto tampoco sabe cómo recuperaría su correo principal. Son 131 personas, el 35,9 % de la muestra, en las que coinciden las dos condiciones que convierten un incidente ordinario en una pérdida irreversible de identidad digital: una cuenta raíz sin proteger del todo y sin vía de retorno configurada. Es el subgrupo de riesgo mejor definido de todo el estudio y, a la vez, el que se corrige con menos esfuerzo, porque ambas carencias se resuelven en la misma sesión de quince minutos.

Huella pública y copias de seguridad

El tercer cruce enfrenta dos conductas que no comparten amenaza —una protege frente a terceros y la otra frente a un accidente— pero sí comparten naturaleza: ninguna produce consecuencias visibles mientras no ocurre nada.

Respuesta del usuario	Perdería datos	Tiene copia	Total
No conoce su huella pública	75 (35,9 %)	134 (64,1 %)	209
Revisa su huella pública	25 (16,0 %)	131 (84,0 %)	156
Total	100	265	365

$\chi^2 (1) = 16,73; p < 0,001; \phi = 0,220; \text{razón de momios} = 2,93 \text{ (IC 95 \% : 1,76 - 4,90)}.$

Quien no ha mirado nunca qué información suya circula tiene más del doble de probabilidades de no tener resueltas sus copias de seguridad. La asociación es moderada, pero su interés no está en la magnitud sino en lo que revela sobre el mecanismo: no se trata de dos competencias distintas que casualmente coinciden, sino de una misma disposición a no ocuparse de lo que no reclama atención. Ambas conductas comparten el rasgo de no tener quien las pida.

Percepción de control y tiempo de pantalla

El cuarto cruce traduce a tabla de contingencia la brecha que el capítulo 10 desarrolla en detalle, y permite contrastarla estadísticamente en lugar de describirla.

Respuesta del usuario	No controla su tiempo de pantalla	Lo tiene controlado	Total
Afirma tener el control (P26 c/d)	157 (50,6 %)	153 (49,4 %)	310
Reconoce ir a remolque (P26 a/b)	48 (87,3 %)	7 (12,7 %)	55
Total	205	160	365

$\chi^2(1) = 23,99$; $p < 0,001$; $\phi = 0,264$; razón de momios = 6,68 (IC 95 %: 2,93 - 15,23).

La asociación es significativa, lo que confirma que la autopercepción no es aleatoria: quien reconoce ir a remolque acierta, y lo hace de forma contundente, porque el 87,3 % de ese grupo declara efectivamente no controlar su tiempo de pantalla. El problema está en la otra fila. Entre quienes afirman tener el control, el reparto es prácticamente una moneda al aire: el 50,6 % reconoce un tiempo de pantalla superior al deseado. La autoevaluación funciona como detector cuando es negativa y no discrimina nada cuando es positiva. Dicho de otro modo, decir «voy a remolque» es información fiable; decir «lo controlo» no aporta información alguna sobre la conducta real.

Por qué esta asimetría condiciona cualquier acción divulgativa

Un mensaje que interpele a quien se reconozca con dificultades alcanzará al 15,1 % de la muestra, y a ese grupo lo alcanzará bien. Los 157 participantes que creen tener el control y no lo tienen —el 43,0 % del total— quedan fuera de cualquier convocatoria formulada en esos términos, porque no se dan por aludidos. Es el argumento cuantitativo detrás de la recomendación de sustituir la advertencia por la medición.

Un contraste entre ejes: el cruce que no aparece

Los cuatro cruces anteriores emparejan conductas del mismo eje. El siguiente cruza deliberadamente los dos ejes descritos en el apartado 8.1, enfrentando la principal carencia de seguridad con la principal carencia de hábito.

Respuesta del usuario	Mira el móvil en la cama	No lo consulta en la cama	Total
Usa gestor de contraseñas	58 (56,3 %)	45 (43,7 %)	103
No usa gestor de contraseñas	170 (64,9 %)	92 (35,1 %)	262
Total	228	137	365

$\chi^2(1) = 1,97$; $p = 0,161$; $\phi = 0,080$; razón de momios = 0,70 (IC 95 %: 0,44 - 1,11).

No hay asociación. El intervalo de confianza incluye holgadamente el valor 1 y el tamaño del efecto es prácticamente nulo. Saber si una persona usa gestor de contraseñas no permite anticipar en absoluto si se lleva el móvil a la cama. Este resultado negativo es, en realidad, uno de los más informativos del capítulo: confirma a nivel de conducta individual lo que el apartado 8.1 mostraba a nivel de bloques, y lo hace con la comparación más exigente posible, la de los dos ítems que mejor representan cada eje.

Un cruce que la intuición sitúa mal

El último cruce enfrenta el peor ítem del estudio, el móvil en la cama (P6), con el efecto anímico tras el uso de redes sociales (P25). Es una asociación que cabría esperar intensa y no lo es.

Respuesta del usuario	Malestar o dispersión	Neutro o bienestar	Total
Mira el móvil en la cama	79 (34,6 %)	149 (65,4 %)	228
No lo consulta en la cama	34 (24,8 %)	103 (75,2 %)	137
Total	113	252	365

$\chi^2 (1) = 3,42$; $p = 0,064$; $\phi = 0,103$; razón de momios = 1,61 (IC 95 %: 1,00 – 2,58).

La diferencia va en la dirección esperada —el malestar es diez puntos porcentuales más frecuente entre quienes llevan la pantalla a la cama— pero no alcanza el umbral convencional de significación. Sin la corrección de continuidad el valor quedaría justo por debajo de 0,05, lo que sitúa el resultado exactamente en la frontera y desaconseja presentarlo como hallazgo. El intervalo de confianza de la razón de momios, que toca el valor 1 por su extremo inferior, apunta en el mismo sentido.

Conviene ser explícito al respecto, porque es un dato que resultaría cómodo redondear al alza: los datos de este estudio no permiten afirmar que quien mira el móvil en la cama se sienta peor tras usar las redes sociales. Sugieren una tendencia, nada más. La explicación más plausible es que el instrumento mide ambas conductas de forma demasiado gruesa (cuatro opciones cada una) y que entre ellas media una variable, la calidad del descanso, que el cuestionario no recoge.

Cuántos déficits acumula cada persona

Los cruces por pares describen relaciones de dos en dos. La pregunta final es cuántas carencias coinciden en la misma persona. Se han seleccionado las cinco conductas de configuración que el informe identifica como críticas y se ha contado cuántas presenta cada participante.

Nº de carencias acumuladas	Personas	% de la muestra	% esperado si fueran independientes
Ninguna	40	11,0 %	2,0 %
Una	54	14,8 %	12,9 %
Dos	77	21,1 %	30,9 %
Tres	71	19,5 %	34,1 %
Cuatro	86	23,6 %	17,1 %
Las cinco	37	10,1 %	3,0 %

Carencias consideradas: no usar gestor de contraseñas (71,8 % de la muestra), segundo factor incompleto (57,5 %), recuperación del correo sin resolver (46,3 %), huella pública desconocida (57,3 %) y copias de seguridad insuficientes (27,4 %).

La comparación entre las dos últimas columnas es la conclusión del apartado. Si las cinco conductas fueran independientes entre sí, la distribución se concentraría en el centro y los extremos serían muy poco frecuentes. Lo que se observa es lo contrario: hay cinco veces más personas sin ninguna carencia de las esperables y más del triple de personas que acumulan las cinco. La correlación media entre pares de carencias es de 0,247, y la distribución resultante se aleja del centro hacia los dos extremos.

El resultado práctico es que el 53,2 % de la muestra acumula tres o más de las cinco carencias, mientras que solo el 11,0 % no presenta ninguna. La media es de 2,60 carencias por persona. Conviene recordar que se trata de una muestra autoseleccionada, con nivel formativo alto y previsiblemente sensibilizada, y que puntúa un 83,9 % en el bloque de ciberseguridad.

Qué implica la co-ocurrencia para el diseño de la intervención

Los déficits de configuración no están repartidos: se concentran. Una acción dirigida a una sola de estas conductas alcanza a un grupo que, en su mayoría, presenta otras dos o tres carencias simultáneas y que no las resolverá por su cuenta. Esto favorece las intervenciones de paquete —una sesión que resuelva gestor, segundo factor y recuperación del correo a la vez— frente a las campañas monotemáticas. Y refuerza el argumento del apartado 8.1 en el sentido contrario: dentro de cada eje conviene agrupar, pero entre ejes hay que separar, porque no se dirigen a las mismas personas.

Nota sobre las pruebas realizadas

Se han efectuado seis contrastes sobre la misma muestra, lo que eleva la probabilidad de obtener al menos un resultado significativo por azar. Aplicando la corrección secuencial de Holm-Bonferroni, los cuatro cruces presentados como significativos lo siguen siendo con holgura, ya que sus valores p se sitúan entre $4,3 \times 10^{-5}$ y $1,6 \times 10^{-12}$, muy por debajo de los umbrales corregidos. Los dos cruces no significativos siguen sin serlo. La corrección no altera, por tanto, ninguna de las conclusiones de este apartado.

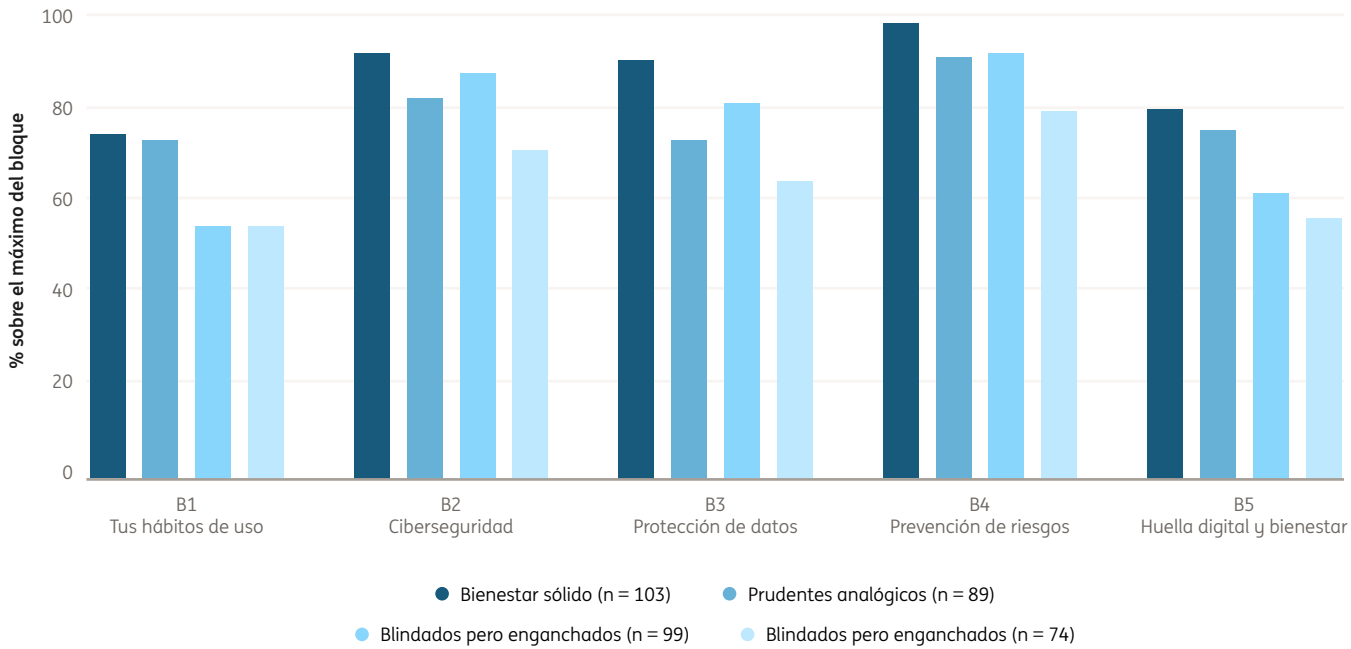
Todas las variables son dicotomizaciones de escalas ordinales de cuatro puntos, lo que supone una pérdida de información deliberada a cambio de una lectura más directa. Los puntos de corte se han fijado con criterio sustantivo y antes de calcular ningún contraste: en las preguntas donde solo la opción d describe la conducta protegida (P8, P9, P20) el corte separa esa opción del resto; en las demás se separan las dos opciones desfavorables (a y b) de las dos favorables (c y d). Y, como en el resto del informe, la asociación estadística entre dos conductas declaradas no permite establecer relación causal alguna entre ellas.



9. Cuatro perfiles de usuario

Para comprobar la advertencia anterior se ha realizado un análisis de conglomerados por k-medias sobre las cinco puntuaciones de bloque estandarizadas. La solución de cuatro grupos es la que ofrece una interpretación más clara y reparte la muestra de forma equilibrada.

Perfil de cada conglomerado en los cinco bloques



Perfil	n	% muestra	Total	B1	B2	B3	B4	B5
Bienestar sólido	103	28,2 %	93,0	74,4 %	91,6 %	90,5 %	97,9 %	79,9 %
Prudentes analógicos	89	24,4 %	84,7	73,4 %	82,1 %	73,3 %	90,9 %	75,1 %
Blindados pero enganchados	99	27,1 %	80,4	55,0 %	87,1 %	80,8 %	91,6 %	61,2 %
Vulnerables globales	74	20,3 %	69,8	54,8 %	71,2 %	64,4 %	79,1 %	56,4 %

Blindados pero enganchados (27,1 %)

Es el perfil más singular del estudio. Puntúan por encima de la media en los tres bloques defensivos —87,1 % en ciberseguridad, 91,6 % en prevención— y se desploman en los dos de autorregulación: 55,0 % en hábitos de uso y 61,2 % en huella y bienestar. Su puntuación total, 80,4 puntos, los sitúa en la zona de equilibrio razonable, lo que enmascara por completo el problema. Es también el grupo más joven de los cuatro.

Prudentes analógicos (24,4 %)

El espejo del anterior. Gestionan bien su tiempo (73,4 % en hábitos) y su bienestar (75,1 %), pero son el grupo más flojo en protección de datos (73,3 %), por debajo incluso de la media general. Usan poco y bien, pero tienen su infraestructura descuidada: copias de seguridad, revisión de la huella pública, gestión de contraseñas.

El argumento central del estudio, en una comparación

Los “blindados pero enganchados” (80,4 puntos) y los “prudentes analógicos” (84,7 puntos) están separados por apenas cuatro puntos en la escala global y tienen problemas diametralmente opuestos. Un mensaje único dirigido a ambos fallaría con los dos: al primero le sobra información sobre fraude y le falta acompañamiento en hábitos; al segundo, justo lo contrario.

Bienestar sólido (28,2 %) y vulnerables globales (20,3 %)

Los dos perfiles restantes son los esperables: un grupo que puntúa alto en todo (93,0 puntos de media, con un 97,9 % en prevención de riesgos) y un grupo que puntúa bajo en todo (69,8 puntos), que concentra la vulnerabilidad real de la muestra y que representa una de cada cinco personas. Nótese que incluso este último grupo obtiene un 79,1 % en prevención de riesgos: el reflejo defensivo ante el fraude explícito está presente en toda la muestra, sin excepción de perfil.

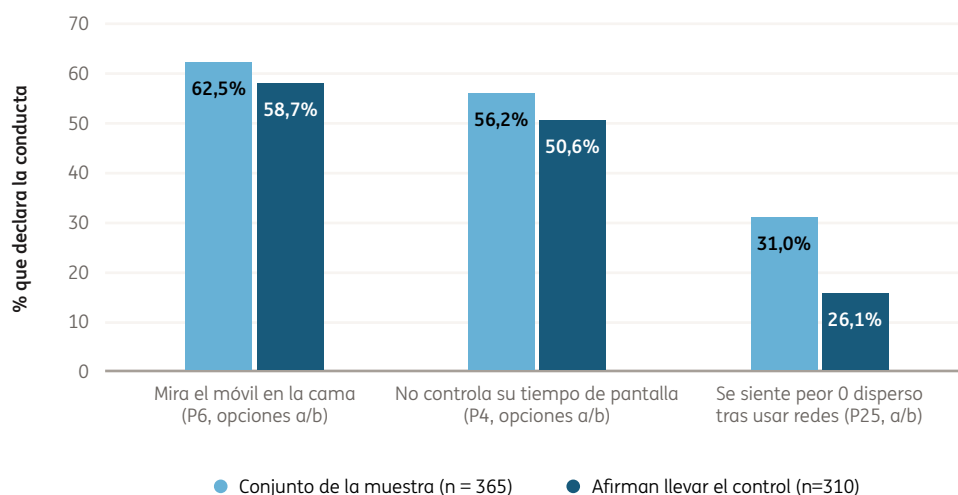


10. La brecha de autopercepción

El cuestionario incluye en la pregunta 26 una autoevaluación global: «En tu relación con la tecnología, ¿quién manda?». Cruzarla con las respuestas conductuales del bloque 1 permite medir hasta qué punto la muestra se conoce a sí misma.

Conductas declaradas por el conjunto de la muestra

Y por quienes afirman tener el control de su relación con la tecnología

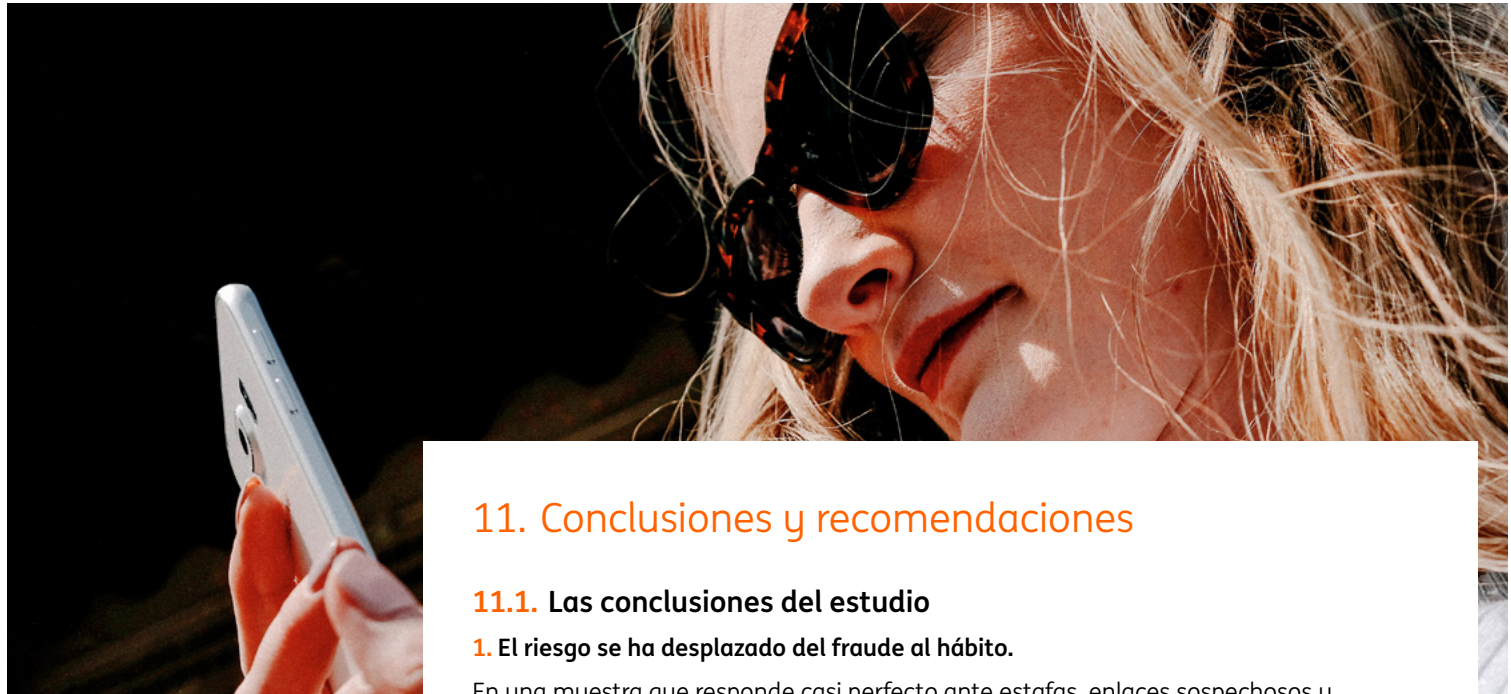


El 84,9 % de la muestra afirma llevar el control. Entre esas mismas 310 personas, el 58,7 % mira el móvil en la cama, el 50,6 % reconoce que su tiempo de pantalla es superior al que le gustaría o que no lo controla, y el 26,1 % declara sentirse peor o disperso tras un rato en redes sociales. Su puntuación media en el bloque de hábitos de uso es del 66,9 % del máximo: apenas dos puntos porcentuales por encima de la media general del bloque.

La brecha no es un fallo de sinceridad. Es un fenómeno bien documentado en psicología: la percepción de control se construye sobre los momentos en que efectivamente decidimos, como dejar el móvil en una reunión, silenciar las notificaciones, y no sobre los automatismos, que por definición no se registran del todo conscientemente. Nadie recuerda los cuarenta desbloques del día; todo el mundo recuerda la vez que decidió no mirar.

Consecuencia práctica

Cualquier intervención que dependa de que la persona reconozca previamente que tiene un problema va a alcanzar, como mucho, al 15,1 % que ya lo admite. Para el 84,9 % restante, el punto de entrada no puede ser la advertencia, sino el dato: el propio informe de tiempo de pantalla del dispositivo, el número real de desbloques, la hora exacta de la última consulta antes de dormir. La medición precede a la motivación.



11. Conclusiones y recomendaciones

11.1. Las conclusiones del estudio

1. El riesgo se ha desplazado del fraude al hábito.

En una muestra que responde casi perfecto ante estafas, enlaces sospechosos y llamadas fraudulentas, el problema real está en el uso cotidiano: la noche, el desbloqueo automático y la media hora que se escurre en las redes. La agenda de la divulgación digital debería reflejar ese desplazamiento.

Se requiere una intervención en educación para fomentar hábitos de uso saludable desde la infancia para lograr que esos adolescentes sean adultos con hábitos instaurados. Del mismo modo, se requiere divulgación centrada en la vida adulta para fomentar hábitos de uso más saludables.

2. Seguridad y autorregulación son competencias independientes.

La evidencia estadística es sólida: las correlaciones entre los dos ejes caen a la franja 0,22-0,40. Nadie debería suponer que quien está bien protegido usa bien la tecnología.

3. La reacción está resuelta; el mantenimiento, no.

Dentro incluso del bloque de seguridad, las conductas puntuales de respuesta ante una amenaza puntúan casi el máximo, mientras que las rutinas sostenidas como el gestor de contraseñas, las copias de seguridad, la recuperación del correo, la revisión de la huella pública... se quedan muy por debajo.

4. La edad mejora el uso, no la protección.

El discurso habitual sobre nativos digitales se invierte aquí: los jóvenes de la muestra se protegen igual de bien que sus mayores, pero gestionan mucho peor su tiempo, su descanso y su exposición emocional.

5. La mitad de la muestra no acompaña a los menores de su entorno.

Es el hallazgo con mayor efecto multiplicador del estudio, porque lo que se transmite a la siguiente generación no es la norma, sino el ejemplo.

11.2. Los titulares más destacados

1. Seis de cada diez participantes se llevan el móvil a la cama.

El 62,5 % lo consulta ya acostado y el 38,4 % lo hace todas las noches. Es la peor de las 27 conductas evaluadas (2,18 sobre 4).

2. Sabemos esquivar una estafa, pero no soltar el móvil.

El 97,8 % rechaza una oferta de inversión fraudulenta y el 94,5 % no entra en su banco desde una wifi pública, pero solo el 14,2 % afirma no depender demasiado del móvil. La distancia entre el bloque de prevención de riesgos (90,7 %) y el de hábitos de uso (64,9 %) es de casi 26 puntos.

3. Ocho de cada diez creen que controlan su relación con la tecnología; sus propias respuestas dicen otra cosa.

El 84,9 % declara llevar el control. Entre esas mismas personas, el 58,7 % mira el móvil en la cama y el 50,6 % reconoce no controlar su tiempo de pantalla.

4. La mitad de los adultos no acompaña a los menores de su entorno.

El 29,9 % describe un acceso libre y sin normas claras y el 20,8 % lo gestiona prohibiendo sin explicar. Solo el 15,9 % pacta normas, explica los motivos y da ejemplo.

5. El bienestar digital no se estudia: se practica.

Estudios medios, universitarios y postgrado obtienen 82,7, 82,9 y 82,3 puntos. Ninguna diferencia ($p = 0,911$). Ningún título protege del móvil en la mesilla de noche.

6. Los jóvenes no son más descuidados con la seguridad: lo son con su tiempo.

El tramo de 20-29 años puntúa prácticamente igual que el de 50-59 en ciberseguridad (83,0 % frente a 85,8 %), pero 17,5 puntos porcentuales por debajo en hábitos de uso.

7. Solo tres de cada diez usan un gestor de contraseñas.

El 28,2 %. Frente a ellos, el 43,8 % repite la misma clave o maneja varias sin criterio.

8. Casi la mitad no sabría recuperar su correo, que es la llave de toda su identidad digital.

El 46,3 % no tiene resuelto cómo recuperar el acceso a la cuenta desde la que se restablecen todas las demás.

9. Uno de cada tres se siente peor después de usar las redes.

El 31,0 % reconoce comparación, ansiedad, dispersión o sensación de tiempo perdido.

10. Nadie suspende, pero solo uno de cada diez sobresale.

Ningún participante cae en zona de alerta y apenas el 9,3 % alcanza el nivel de bienestar sólido: el 90,7 % restante tiene margen de mejora.

11.3. Recomendaciones por prioridad

Las siguientes recomendaciones se ordenan por relación entre impacto y coste, tomando como criterio los ítems más deficitarios y su capacidad de arrastre sobre el resto.

Prioridad	Actuación	Base en los datos
1	Establecer una franja sin pantalla antes de dormir y sacar el móvil del dormitorio	P6 es el peor ítem del estudio (2,18); el 62,5 % lleva la pantalla a la cama
2	Configurar y verificar los métodos de recuperación del correo principal	El 46,3 % no sabría recuperar la llave maestra de toda su identidad digital
3	Adoptar un gestor de contraseñas	Solo el 28,2 % lo usa; el 43,8 % tiene una gestión insegura
4	Pactar y explicar normas de uso con los menores del entorno, empezando por el ejemplo	El 50,7 % deja acceso libre o prohíbe sin explicar
5	Revisar y depurar la huella pública propia y cerrar cuentas antiguas	El 57,3 % no ha mirado su exposición pública o lo hizo hace años
6	Consultar el informe de tiempo de pantalla del propio dispositivo antes de fijar objetivos	El 56,2 % declara un tiempo superior al deseado; la brecha de autopercepción alcanza al 84,9 %
7	Completar el doble factor en todas las cuentas importantes, no solo en correo y banco	Solo el 42,5 % lo tiene en todas
8	Activar copias de seguridad automáticas	El 27,4 % perdería casi todos o bastantes datos ante una pérdida del dispositivo

Se sugieren las siguientes recomendaciones de una manera detallada:

1. Intervenir sobre el entorno, no sobre la fuerza de voluntad.

Los ítems más deficitarios no describen decisiones, describen automatismos: el 46,6 % desbloquea el móvil de forma refleja y el 55,1 % entra «un momento» en redes y pierde media hora. Una conducta automática no se corrige con una intención, porque no pasa por la deliberación. Se corrige cambiando la señal que la dispara. En la práctica: sacar el cargador del dormitorio, dejar el móvil en otra habitación durante la cena, retirar las aplicaciones de la pantalla de inicio. Añadir tres segundos de fricción es más eficaz que proponerse usarlo menos.

2. Medir antes de motivar.

El 84,9 % cree tener el control, de modo que cualquier intervención que exija reconocer previamente un problema alcanzará, como mucho, al 15,1 % restante. La brecha no es falta de sinceridad: la percepción de control se construye sobre los momentos en que decidimos (dejar el móvil en una reunión) y no sobre los automatismos, que no se registran conscientemente. El punto de entrada no puede ser la advertencia, sino el autorregistro: el informe de tiempo de pantalla del propio dispositivo, el número real de desbloques, la hora exacta de la última consulta. El dato propio abre la puerta que la advertencia genérica cierra.

3. Tratar el sueño como la primera palanca, no como una consecuencia más.

El móvil en la cama es el peor ítem del estudio y el que más consecuencias arrastra, porque el descanso media entre el uso del móvil y el estado de ánimo del día siguiente. Los bloques de hábitos y de bienestar correlacionan entre sí ($r = 0,481$), y esta es la conducta que más eficientemente conecta ambos. Si solo puede cambiarse un hábito, que sea este: una franja de treinta a sesenta minutos sin pantalla antes de dormir, con el dispositivo fuera del dormitorio.

4. Sustituir la prohibición por el acompañamiento, empezando por el modelado.

La mitad de la muestra deja a los menores sin normas o les prohíbe sin explicar. Ninguna de las dos vías genera autorregulación: la ausencia de norma no la enseña y la prohibición sin motivo produce obediencia mientras dura la vigilancia, no criterio propio. Lo que sí la genera es la norma pactada y explicada, sostenida por el ejemplo. Y aquí el estudio cierra el círculo: el adulto que mira el móvil en la cama y en la mesa está enseñando eso, con independencia de qué controles parentales haya instalado. El acompañamiento empieza por el bloque 1 del propio adulto.

5. Atender a qué se hace en las redes, no solo a cuánto tiempo se pasa en ellas.

El 31,0 % se siente peor o disperso tras usarlas, un malestar que la literatura asocia sobre todo a la comparación social ascendente y al consumo pasivo, no al tiempo en sí. Reducir minutos sin cambiar el uso puede dejar intacto el efecto sobre el ánimo. La intervención útil discrimina: depurar a quién se sigue, sustituir el consumo pasivo por interacción intencionada, y usar como indicador el estado de ánimo al salir de la aplicación en lugar del contador de minutos.

6. Entrevistas a expertos independientes

En el desarrollo del estudio se ha entrevistado a dos expertas en el campo que investiga este estudio. Se trata de la psicóloga, escritora e influencer Alicia González (@aliciagonzalezpsicologia) y la criminóloga, experta en ciberseguridad, escritora e influencer María Aperador (@mariaaperador)

Alicia González (@aliciagonzalezpsicologia)

Para la psicóloga Alicia González, hablar de hábitos digitales saludables no significa necesariamente demonizar las pantallas o establecer una lucha contra el teléfono móvil. La cuestión fundamental estaría en analizar qué lugar ocupa la tecnología en nuestra vida cotidiana y qué estamos dejando de hacer cuando recurrimos constantemente a ella. “El uso automático del teléfono puede aparecer en momentos de aburrimiento, incomodidad o ansiedad”, afirma la experta psicóloga. Consultar las redes sociales nada más despertarnos, mirar el móvil mientras hablamos con otra persona o sentir la necesidad de comprobar constantemente si hemos recibido alguna notificación son comportamientos que pueden terminar convirtiéndose en hábitos difíciles de modificar. “No se trata únicamente de cuánto tiempo pasamos con el móvil, sino de preguntarnos para qué lo estamos utilizando y qué necesidad estamos intentando cubrir.”, afirma.

Para la psicóloga sería especialmente importante recuperar cierta intencionalidad en el uso de la tecnología. Algunas medidas sencillas pueden marcar una diferencia: evitar comenzar y terminar el día mirando el teléfono, silenciar notificaciones que no sean importantes, crear momentos sin pantallas o aprender a tolerar pequeños espacios de aburrimiento sin buscar estímulos inmediatos.

También resulta relevante prestar atención a la comparación constante que pueden favorecer las redes sociales. El contacto continuo con versiones seleccionadas y aparentemente perfectas de la vida de otras personas puede terminar condicionando nuestra percepción sobre lo que deberíamos estar haciendo, consiguiendo o sintiendo. La clave, por tanto, no estaría en eliminar la tecnología de nuestra vida, sino en conseguir que sea una herramienta que utilizamos conscientemente y no un hábito que dirige automáticamente nuestra atención.

María Aperador (@mariaaperador)

Para la experta en ciberseguridad María Aperador, buena parte de los riesgos digitales actuales no dependen exclusivamente de grandes conocimientos informáticos. Muchos ataques se apoyan en algo mucho más cotidiano: la confianza, la urgencia, el miedo o el desconocimiento de las personas. Correos que simulan proceder de nuestro banco, mensajes de WhatsApp de supuestos familiares que necesitan dinero con urgencia, enlaces fraudulentos, perfiles falsos o contraseñas reutilizadas en distintas plataformas forman parte de amenazas cada vez más habituales.

“El ciberdelincuente muchas veces no necesita hackear un dispositivo”, afirma, “le basta con conseguir que nosotros mismos le facilitemos la información.” Por eso, uno de los pilares de la ciberseguridad sería aprender a desconfiar de determinadas situaciones antes de actuar. Si un mensaje genera urgencia, solicita datos personales, pide realizar un pago o incluye un enlace inesperado, detenerse unos segundos y verificar la información puede evitar numerosos problemas.

Entre los hábitos digitales básicos que conviene incorporar se encuentran utilizar contraseñas diferentes y robustas, activar la verificación en dos pasos, mantener dispositivos y aplicaciones actualizados y evitar compartir públicamente información que pueda utilizarse posteriormente para suplantarnos o engañarnos.

“Tenemos que empezar a pensar en nuestra información personal como algo que también necesita protección.” Para ello la experta nos mostró diferentes dispositivos “antiespía” como protectores de pantalla para móvil y para portátil que impide que lean el dispositivo personas cercanas no autorizadas.

Las perspectivas de Alicia González y María Aperador confluyen en una misma idea: usar la tecnología de manera consciente.

Desde el punto de vista psicológico, significa preguntarnos cómo afecta a nuestra atención, nuestras relaciones, nuestro descanso o nuestra autoestima. Desde la ciberseguridad, implica conocer los riesgos, proteger nuestra información y aprender a detectar posibles intentos de manipulación.



12. Análisis desde la psicología del comportamiento

Las páginas anteriores describen lo que hace la muestra. Este apartado se ocupa de por qué lo hace. La distinción importa porque el patrón que devuelve el estudio (una competencia defensiva casi impecable conviviendo con una autorregulación deficitaria) no es un accidente ni una contradicción: es exactamente lo que predice la literatura sobre formación de hábitos, toma de decisiones y percepción de riesgo. Entender el mecanismo es lo que permite pasar del diagnóstico a la intervención.

12.1. Dos sistemas de procesamiento, dos tipos de conducta digital

La psicología cognitiva contemporánea describe el funcionamiento mental a partir de dos modos de procesamiento que operan en paralelo. Un modo rápido, automático, asociativo y de bajo coste atencional, que resuelve la inmensa mayoría de las decisiones cotidianas sin llegar a la conciencia. Y un modo lento, deliberado, secuencial y costoso, que se activa cuando la situación es novedosa, cuando algo interrumpe la rutina o cuando percibimos una señal de riesgo. Esta arquitectura dual, sistematizada por Kahneman (2011) a partir del trabajo previo de Stanovich y West (2000), es probablemente el marco más útil para leer los resultados de este estudio.

Obsérvese qué preguntas resuelve bien la muestra y cuáles no. El SMS con un enlace acortado (P10), la llamada urgente del falso soporte técnico (P22), la oferta de inversión con rentabilidad garantizada (P11), la petición de un código recibido por SMS (P23): todas ellas son interrupciones. Rompen la rutina, llegan marcadas con una anomalía perceptible y activan el modo deliberado. Y en todas ellas la muestra puntúa por encima de 3,5 sobre 4.

Ahora obsérvese las preguntas peor puntuadas. Desbloquear el móvil decenas de veces al día (P1, 2,59), sacarlo en una cola (P2, 2,63), abrir una red social «un momento» (P5, 2,47), mirarlo en la cama (P6, 2,18). Ninguna de ellas es una decisión en sentido estricto. Son secuencias aprendidas que se disparan ante una señal contextual y se ejecutan sin pasar por la deliberación. No fallan porque la persona decida mal: fallan porque la persona no llega a decidir.

La consecuencia central para el diseño de cualquier intervención

Un mensaje de concienciación solo puede influir sobre conductas que pasen por el modo deliberado. Por eso las campañas contra el fraude han funcionado tan bien (actúan sobre una conducta que ya era consciente) y por eso las campañas sobre tiempo de pantalla funcionan tan mal: intentan corregir con argumentos una conducta que nunca llega a formularse como pregunta. La información es una herramienta adecuada para el sistema deliberado e ineficaz para el automático.

12.2. La arquitectura del hábito: señal, rutina, recompensa

Un hábito, en la definición operativa de Wood y Neal (2007), es una asociación aprendida entre una señal del contexto y una respuesta, que con la repetición se vuelve independiente del objetivo que originalmente la motivaba. La clave de esa definición está en la última parte: el hábito sobrevive a su propia utilidad. La persona sigue desbloqueando el móvil aunque no espere nada, porque la señal —el hueco entre dos tareas, la espera en la cola, el silencio antes de dormir— basta para disparar la secuencia.

El estudio ofrece una demostración casi de manual de este mecanismo. En P2, el 50,1 % saca el móvil en una cola sin pensarlo o ya lo llevaba en la mano: la señal es la espera. En P6, el 38,4 % lo consulta todas las noches al acostarse: la señal es la cama. En P5, el 55,1 % entra «un momento» y pierde media hora: la señal es el propio icono de la aplicación. Ninguna de las tres conductas responde a una necesidad concreta; las tres responden a un contexto.

De aquí se deriva un principio de intervención que atraviesa todo este informe: si la conducta la dispara el contexto, el punto de intervención es el contexto y no la voluntad. Retirar el cargador del dormitorio, sacar las aplicaciones de la pantalla de inicio o dejar el móvil en otra habitación durante la cena no son consejos menores de sentido común: son modificaciones de la señal, que es el único eslabón de la cadena sobre el que se puede actuar antes de que la rutina se ejecute. Duckworth y colaboradores (2016) sistematizaron esta idea al distinguir entre estrategias de autocontrol situacionales, que modifican el entorno, y estrategias cognitivas, que exigen resistencia en el momento; las primeras resultan sistemáticamente más eficaces, precisamente porque no dependen de un recurso que se agota.

12.3. El refuerzo intermitente y por qué el desplazamiento infinito no cansa

Los programas de refuerzo de razón variable (recompensas impredecibles en frecuencia y magnitud) generan las pautas de respuesta más persistentes y más resistentes a la extinción que se conocen desde los trabajos originales de Skinner (Ferster y Skinner, 1957). Es el principio de la máquina tragaperras y es, con una fidelidad notable, el principio de diseño de cualquier muro de contenido con desplazamiento continuo: la mayoría de los elementos son irrelevantes y de vez en cuando aparece uno que compensa, sin que sea posible anticipar cuándo.

Esto explica dos datos del estudio que de otro modo resultarían desconcertantes. El primero es la enorme concentración de respuestas en la opción b de P5: el 55,1 % de la muestra —la mayor acumulación en una sola opción intermedia de todo el cuestionario— describe entrar con una intención breve y salir mucho después. Esa discrepancia entre la duración prevista y la real es la firma característica del refuerzo intermitente. El segundo es el resultado de P25: solo el 16,7 % afirma sentirse bien tras usar las redes sociales. Una conducta muy repetida que produce poca satisfacción declarada no es una paradoja; es el perfil esperable de una conducta mantenida por refuerzo intermitente y no por el disfrute.

« El desplazamiento continuo no engancha porque sea placentero, sino porque es impredecible. Se sostiene por la posibilidad de la recompensa, no por la recompensa. »

12.4. El sesgo de optimismo y el efecto tercera persona

Hemos documentado previamente la brecha central del estudio: el 84,9 % afirma llevar el control de su relación con la tecnología, y dentro de ese mismo grupo el 58,7 % mira el móvil en la cama y el 50,6 % reconoce no controlar su tiempo de pantalla. Conviene subrayar que esto no es un problema de sinceridad. Es un fenómeno documentado desde hace décadas y con tres mecanismos concurrentes bien identificados.

El primero es el sesgo de optimismo descrito por Weinstein (1980): las personas tienden a estimar que su probabilidad de sufrir un resultado negativo es menor que la de los demás, y esa tendencia es más acusada cuanto más controlable se percibe el riesgo. Como el uso del móvil se percibe como plenamente controlable (“puedo dejarlo cuando quiera”), es un terreno especialmente propicio para el sesgo.

El segundo es el efecto tercera persona, formulado por Davison (1983): tendemos a considerar que los medios y sus mecanismos de persuasión influyen más sobre los demás que sobre nosotros mismos. Aplicado a este estudio, es la razón por la que una persona puede reconocer sin dificultad que las redes sociales están diseñadas para retener la atención y, simultáneamente, no aplicarse ese diagnóstico a sí misma.

El tercero es un asunto de disponibilidad en la memoria. La percepción de control se construye a partir de episodios recuperables, y los episodios recuperables son precisamente las decisiones deliberadas: la vez que se dejó el móvil en una reunión, la tarde que se silenciaron las notificaciones. Los automatismos, por definición, no dejan huella narrativa. Nadie recuerda los cuarenta desbloques del día; todo el mundo recuerda la vez que decidió no mirar. El balance mental resultante está sesgado por construcción.

El modelo transteórico de Prochaska y DiClemente (1983) añade la implicación operativa: quien no reconoce el problema se encuentra en fase de precontemplación, y en esa fase la advertencia no solo es ineficaz, sino que puede generar reactancia. Lo que mueve a una persona de la precontemplación a la contemplación no es un argumento externo, sino la constatación de una discrepancia entre la propia imagen y el propio dato.

Por qué la medición precede a la motivación

Si el 84,9 % de la muestra no percibe un problema, cualquier intervención que exija reconocerlo previamente alcanzará como mucho al 15,1 % restante. El punto de entrada para el resto no puede ser la advertencia, sino el autorregistro: el informe de tiempo de pantalla del propio dispositivo, el número real de desbloques, la hora exacta de la última consulta antes de dormir. El dato propio no discute con la autoimagen: la corrige sin confrontarla.

12.5. El sueño como variable mediadora

P6 es el peor ítem del cuestionario (2,18 sobre 4) y también, con diferencia, el que arrastra más consecuencias. La literatura sobre pantallas y descanso identifica tres vías de afectación que conviene distinguir, porque la divulgación tiende a reducirlas a la primera.

- **La vía fotobiológica.** La exposición lumínica en el tramo horario previo al sueño retrasa la secreción de melatonina y desplaza la fase circadiana. Es la vía más citada y, probablemente, la de menor magnitud en condiciones reales de uso doméstico.
- **La vía de la activación cognitiva.** El contenido consumido —conversaciones pendientes, noticias, comparación social, vídeos diseñados para sostener la atención— mantiene el nivel de alerta que el organismo necesita reducir para iniciar el sueño. Esta vía depende de qué se mira, no de cuánta luz emite la pantalla.
- **La vía del desplazamiento temporal.** El tiempo dedicado a la pantalla en la cama se resta directamente del tiempo en cama disponible para dormir. Es la vía más simple y, en términos de horas perdidas, la más determinante.

A estas tres se añade un fenómeno específico bien caracterizado: la procrastinación del sueño (Kroese y colaboradores, 2014), esto es, retrasar voluntariamente la hora de acostarse sin ninguna razón externa que lo justifique. Los autores la interpretan como un fallo de autorregulación al final del día, cuando la capacidad de control es menor y la persona reclama para sí un tiempo de ocio que la jornada no le ha dejado. Es una descripción notablemente precisa de lo que describe el 62,5 % de esta muestra. La razón por la que este ítem merece la primera prioridad del informe no es únicamente su puntuación. Es su posición en la cadena causal: el descanso media entre el uso del dispositivo y el estado de ánimo, la capacidad atencional y la propia autorregulación del día siguiente. Los bloques 1 y 5 correlacionan entre sí ($r = 0,481$) y esta es la conducta que conecta ambos de forma más directa. Intervenir sobre el sueño es intervenir aguas arriba.

12.6. Comparación social y uso pasivo

El 31,0 % de la muestra declara sentirse peor, inquieto o disperso tras un rato en redes sociales (P25). El marco explicativo de referencia sigue siendo la teoría de la comparación social de Festinger (1954), y en particular la distinción posterior entre comparación ascendente (con quien percibimos por encima) y descendente. Las plataformas sociales presentan una particularidad estructural: al mostrar contenidos seleccionados y editados, generan un flujo casi ininterrumpido de comparaciones ascendentes, en el que la vida cotidiana propia se contrasta con los mejores momentos ajenos.

La investigación posterior ha matizado el papel del tiempo de uso. Los trabajos de Verduyn y colaboradores (2017) diferencian entre uso pasivo (consumir sin interactuar) y uso activo (conversar, publicar, responder) y encuentran que el efecto negativo sobre el bienestar se asocia sobre todo al primero, con la comparación social como mecanismo mediador.

Por su parte, Orben y Przybylski (2019) demostraron, con grandes conjuntos de datos, que la asociación entre tiempo total de pantalla y bienestar adolescente es real pero de magnitud pequeña, comparable a la de otras variables cotidianas de escaso peso explicativo.

La conclusión práctica es que el indicador relevante no es el contador de minutos, sino el tipo de uso y el estado de ánimo al salir de la aplicación. Una intervención centrada exclusivamente en reducir tiempo puede dejar intacto el efecto sobre el ánimo si el uso restante sigue siendo pasivo y comparativo. Depurar a quién se sigue tiene, previsiblemente, más impacto que restar quince minutos.

12.7. Aprendizaje por observación: por qué el ejemplo pesa más que la norma

P27 es la segunda peor pregunta del estudio (2,35) y la que tiene mayor efecto multiplicador, porque su resultado no se agota en quien responde. La mitad de la muestra (50,7 %) describe un modelo sin acompañamiento: acceso libre y sin normas claras en el 29,9 % de los casos, prohibición sin explicación en el 20,8 %.

La teoría del aprendizaje social de Bandura (1977) explica por qué ninguna de las dos vías genera autorregulación. La ausencia de norma no enseña nada, y la prohibición sin motivo produce obediencia mientras dura la supervisión, no criterio propio; en cuanto la vigilancia desaparece, la conducta reaparece sin haber incorporado ningún principio. Lo que sí transmite criterio es la combinación de norma pactada, explicación del motivo y, sobre todo, modelado, es decir, la observación de la conducta del adulto de referencia.

La literatura sobre mediación parental converge en la misma dirección al distinguir entre mediación restrictiva (limitar el acceso), mediación activa o instructiva (explicar y conversar sobre lo que se ve) y co-uso (compartir la actividad). La mediación activa se asocia de forma consistente con mejores resultados en competencia digital y en uso problemático, mientras que la restrictiva pura muestra efectos limitados y a veces contraproducentes en la adolescencia.

Aquí el estudio cierra su propio círculo. El adulto que consulta el móvil en la cama y en la mesa está enseñando eso, con independencia de qué herramienta de control parental haya instalado. Y son precisamente los tramos de 20 a 39 años, los de peores hábitos propios, los que peor acompañan.

12.8. Del diagnóstico a la intervención: cuatro principios operativos

El marco anterior permite ordenar las recomendaciones del informe según el mecanismo sobre el que actúan, que es la única forma de anticipar cuáles funcionarán.

Principio	Mecanismo psicológico	Traducción operativa
Intervenir sobre la señal, no sobre la voluntad	Los hábitos se disparan por claves contextuales, no por decisiones	Cargador fuera del dormitorio; aplicaciones fuera de la pantalla de inicio; móvil en otra habitación durante las comidas
Medir antes de motivar	Sesgo de optimismo y precontemplación: no se corrige lo que no se percibe	Dos semanas de autorregistro sin objetivos antes de fijar ningún límite
Concretar la intención en plan	Las intenciones de implementación («si ocurre X, haré Y») superan a los propósitos genéricos	No «usaré menos el móvil», sino «a las 23:00 el móvil se queda en la cocina»
Sostener la conducta con el compromiso social	La norma compartida sostiene lo que la voluntad individual no sostiene	Acuerdos familiares explícitos, franjas pactadas, retos de equipo

El tercero de estos principios merece una precisión, porque es el que más se malinterpreta. Gollwitzer (1999) demostró que la eficacia de un propósito aumenta sustancialmente cuando se formula como un vínculo explícito entre una situación concreta y una acción concreta, en lugar de como un objetivo abstracto.

La razón encaja exactamente con el marco de este capítulo: una intención de implementación delega el control en la señal contextual, de modo que la conducta deseada se dispara con el mismo automatismo con el que se disparaba la indeseada. No exige más fuerza de voluntad; exige menos.

Una advertencia sobre la lectura psicológica de estos datos

Todas las medidas de este estudio son autoinformadas y transversales. El marco teórico expuesto permite interpretar los patrones observados y orientar la intervención, pero no autoriza a establecer relaciones causales entre las variables medidas. Conviene además evitar el vocabulario clínico: los datos describen conductas de uso automático en población general, no adicciones. La categoría diagnóstica de adicción a las pantallas no está reconocida como tal en las clasificaciones vigentes, salvo el trastorno por uso de videojuegos, y su empleo divulgativo tiende a estigmatizar sin aportar precisión.



13. Marco de ciberseguridad: qué protege realmente cada conducta

Las veintisiete preguntas del cuestionario describen conductas, pero cada conducta se corresponde con una amenaza concreta y con un mecanismo de defensa concreto. Este apartado hace explícita esa correspondencia, porque de ella depende que las recomendaciones del informe se ordenen por riesgo real y no por familiaridad del público con cada tema. El resultado de ese ejercicio es incómodo: la muestra está muy bien preparada frente a la amenaza que más se divulga y peor preparada frente a la que más probabilidades tiene de materializarse.

13.1. Reconocer un fraude y estar protegido frente a él son cosas distintas

Los indicadores de detección son excelentes: el 97,8 % rechaza la oferta de inversión con rentabilidad garantizada (P11), el 99,2 % no pincha el enlace del SMS de bloqueo bancario (P10), el 94,5 % evita operar con el banco desde una wifi pública (P13), el 90,1 % nunca comparte un código de verificación (P23) y el 96,5 % descarga aplicaciones solo desde tiendas oficiales (P21). Son cifras que reflejan el efecto acumulado de más de una década de campañas de entidades financieras, cuerpos policiales e INCIBE, y no deben minimizarse.

Ahora bien, todas esas preguntas miden lo mismo: la capacidad de reaccionar correctamente ante un intento de engaño dirigido a la persona. Es una defensa que requiere que el atacante intente engañar. Y hay toda una familia de ataques que no necesita engañar a nadie, porque opera sobre credenciales que ya circulan, sobre sesiones abiertas o sobre información pública. Frente a esa familia, la conducta relevante no es la detección sino la configuración, y ahí los resultados del estudio son claramente inferiores.

Conducta medida	Amenaza frente a la que protege	Requiere
P10, P11, P22, P23 · Reacción ante fraude	Ingeniería social dirigida (phishing, smishing, vishing)	Atención en el momento del intento
P8 · Gestión de contraseñas	Relleno de credenciales tras una filtración ajena	Configuración previa y sostenida
P9 · Verificación multifactor	Uso de credenciales robadas o filtradas	Configuración previa, cuenta por cuenta
P20 · Recuperación del correo	Secuestro de la cuenta raíz de la identidad digital	Configuración previa y verificación periódica
P18 · Copias de seguridad	Pérdida, avería, robo y cifrado por ransomware	Configuración automática
P19 · Huella pública	Fraude personalizado e ingeniería social documentada	Revisión periódica y gestión activa
P12 · Permisos de aplicaciones	Recolección excesiva de datos personales	Revisión en la instalación y después

La columna de la derecha contiene la clave del capítulo. Todo lo que la muestra hace bien pertenece a la categoría «atención en el momento». Todo lo que hace mal pertenece a la categoría «configuración previa». No es una diferencia de conocimiento: es una diferencia entre una conducta que alguien te pide ejecutar y una conducta que nadie te va a pedir nunca.

13.2. Por qué la ingeniería social funciona y por qué aquí no ha funcionado

El fraude por ingeniería social no ataca sistemas, ataca los atajos de decisión de las personas. Los principios descritos por Cialdini (1984): autoridad, urgencia y escasez, prueba social, reciprocidad y compromiso, son el repertorio habitual. Por ejemplo: un remitente que se presenta como el banco (autoridad), un plazo perentorio para evitar el bloqueo de la cuenta (urgencia), una oportunidad limitada de inversión (escasez), un asesor que dedica tiempo y genera confianza antes de pedir nada (reciprocidad).

El motivo por el que esta muestra resiste bien es que los escenarios planteados en el cuestionario están señalizados: contienen una anomalía perceptible (un enlace acortado, una petición de dinero, una llamada no solicitada, un código que alguien pide que interrumpa el procesamiento automático y activa la deliberación. La pregunta pertinente, que el instrumento no permite responder, es qué ocurriría ante un intento no señalizado: un mensaje sin faltas, en el canal habitual, con datos personales correctos y en un momento en que la persona efectivamente espera esa comunicación. Ahí es donde se dirige la evolución del fraude, y ahí es donde la huella pública deficiente de la muestra (P19) se convierte en el factor determinante.

13.3. La cadena de credenciales: el ataque que no necesita engañar

El 43,8 % de la muestra reutiliza la misma contraseña o maneja varias sin criterio (P8), y solo el 28,2 % utiliza un gestor con claves únicas. Esta es, técnicamente, la grieta más importante del estudio, y conviene explicar por qué con precisión.

El relleno de credenciales (credential stuffing) consiste en tomar pares de usuario y contraseña procedentes de filtraciones de terceros y probarlos de forma automatizada contra otros servicios. No requiere descifrar nada, no requiere vulnerabilidad alguna en el servicio atacado y no requiere que la víctima cometa ningún error en el momento del ataque: el error se cometió años antes, al reutilizar la clave. El único requisito es que la misma combinación funcione en dos sitios.

El contraste con los datos de detección de fraude es elocuente. La misma persona que identifica sin dudar un SMS fraudulento tiene, según los datos de este estudio, una probabilidad cercana al 44 % de estar reutilizando en su banco o en su correo una contraseña que quizá ya figura en algún volcado de credenciales. La defensa que domina no cubre el vector que más probabilidades tiene de afectarle.

El gestor de contraseñas resuelve el problema por una vía que encaja con el marco del capítulo anterior: elimina la decisión. Una vez instalado, el usuario deja de elegir contraseñas, deja de recordarlas y deja de reutilizarlas, no porque se esfuerce más, sino porque el sistema ya no se lo pide. Es una medida de configuración única con efecto permanente, exactamente el tipo de intervención que esta muestra necesita.

13.4. El correo electrónico como llave maestra

El dato más infravalorado del estudio está en P20: el 46,3 % de la muestra no tiene claro cómo recuperaría el acceso a su correo principal. Un 2,5 % no sabría por dónde empezar, un 13,2 % lo intentaría sin nada preparado y un 30,7 % recuerda haber configurado algo pero tendría que buscarlo.

La razón por la que esto importa es estructural. Prácticamente todos los servicios digitales, incluida la banca, delegan su procedimiento de restablecimiento de contraseña en la dirección de correo asociada. Eso convierte a esa cuenta en la raíz del árbol: quien la controla puede iniciar el restablecimiento de todo lo demás, y quien la pierde pierde con ella la vía de recuperación de la mayoría de sus servicios. La cuenta de correo no es un servicio más del inventario; es el punto único de fallo de la identidad digital de una persona.

El escenario de peor consecuencia combina tres elementos que el estudio muestra por separado: una contraseña reutilizada (43,8 %), una cuenta de correo sin segundo factor —el 38,6 % lo tiene solo en algunas cuentas, y la de correo queda fuera con frecuencia— y ningún método de recuperación verificado (46,3 %). Cuando coinciden los tres, un incidente que debería resolverse en diez minutos se convierte en una pérdida irreversible.

La vulnerabilidad más rentable de corregir del estudio

Que casi la mitad de una muestra que puntúa un 90,7 % en prevención de riesgos no tenga resuelta la recuperación de su correo convierte este ítem en la mejor relación entre coste y beneficio de todo el informe. Es barato de corregir (diez minutos de configuración: teléfono de recuperación, dirección alternativa, códigos de respaldo guardados fuera del dispositivo), es verificable y su fallo es catastrófico e irreversible.

13.5. No todos los segundos factores protegen igual

El 42,5 % de la muestra declara tener verificación multifactor en todas sus cuentas importantes y el 38,6 % solo en algunas. El cuestionario no distingue el tipo de segundo factor, y esa distinción es relevante desde el punto de vista técnico porque la resistencia al fraude varía sustancialmente entre unos y otros.

Tipo de segundo factor	Resistencia al phishing	Vector de ataque principal
Código por SMS	Baja	Duplicado fraudulento de la tarjeta SIM e interceptación; el código puede ser solicitado por el atacante en tiempo real
Aplicación de códigos temporales (TOTP)	Media	El código sigue siendo transferible: la víctima puede ser inducida a dictarlo
Notificación push de aprobación	Media	Fatiga de notificaciones: envío repetido hasta que la víctima acepta por agotamiento
Llave física o clave de acceso (FIDO2 / passkeys)	Alta	Vinculada al dominio legítimo: no es transferible ni utilizable en un sitio suplantado

La lectura conjunta con P23 es interesante. El 90,1 % de la muestra afirma que nunca compartiría un código recibido por SMS sin una comprobación absoluta, lo que es precisamente la defensa que necesita el factor más débil de la tabla. Es decir, la muestra compensa con atención la fragilidad técnica del método más extendido. Funciona, pero es una defensa que depende de acertar cada vez, mientras que las claves de acceso trasladan esa garantía al propio protocolo. La recomendación operativa no es sustituir todo de golpe, sino priorizar el factor más robusto disponible en las dos cuentas raíz: correo y banco.

13.6. Permisos, copias y superficie de exposición

Tres conductas del estudio comparten una característica que explica su persistencia: no producen ninguna consecuencia visible en el momento, de modo que el usuario nunca recibe la información que corregiría su comportamiento.

En permisos de aplicaciones (P12), el 35,3 % acepta sin revisar o revisa muy por encima. El modelo de consentimiento de los sistemas operativos móviles ha mejorado notablemente —permisos granulares, concesión temporal, avisos de acceso en segundo plano—, pero sigue descansando en una decisión que se toma en el peor momento posible: cuando el usuario quiere empezar a usar la aplicación. El criterio técnico es simple y conviene divulgarlo tal cual: un permiso solo se justifica si la función principal de la aplicación es imposible sin él.

En copias de seguridad (P18), el 27,4 % perdería bastantes o casi todos sus datos ante una pérdida del dispositivo. Es una cifra alta para un riesgo que no depende de ningún atacante. La referencia clásica sigue siendo válida: tres copias de los datos, en dos soportes distintos, con una de ellas fuera del domicilio o del dispositivo principal. Para el usuario doméstico esto se traduce en copia automática en la nube más una copia local periódica, y —esto es lo que casi nadie hace— una comprobación anual de que la restauración funciona realmente.

En huella pública (P19), el 57,3 % no ha comprobado nunca qué información suya es accesible o lo hizo hace mucho tiempo, y solo el 14,5 % la gestiona activamente. Es la peor pregunta de todo el ámbito de seguridad y la que conecta con la evolución previsible del fraude, según se detalla a continuación.

13.7. De la estafa masiva al fraude documentado

La información pública sobre una persona es la materia prima de la ingeniería social dirigida. Nombre, empleador, entorno familiar, rutinas, viajes recientes, aficiones y contactos permiten construir un mensaje que no presenta ninguna de las anomalías que la muestra detecta tan bien: llega en el momento verosímil, en el canal esperado y con los datos correctos.

A esto se añade la disponibilidad de herramientas de síntesis de voz e imagen, que reducen a minutos la fabricación de una prueba de identidad aparentemente sólida a partir de material publicado por la propia víctima. El resultado es que el factor de verificación tradicional —reconocer la voz de quien llama— ha dejado de ser fiable, y la contramedida ya no es técnica sino de procedimiento: verificar por un canal distinto e independiente del que originó la petición, siempre, incluso cuando todo encaja. Es exactamente lo que el 77,8 % de la muestra dice hacer en P22; el reto es sostener ese criterio cuando la petición procede de alguien conocido.

« La muestra está preparada para el fraude genérico y masivo. Su punto débil es el fraude construido a medida a partir de lo que ella misma ha publicado y ya no recuerda. »

13.8. De la estafa masiva al fraude documentado

Buena parte de las conductas evaluadas tiene un respaldo jurídico que conviene conocer, porque convierte una recomendación de higiene digital en un derecho ejercitable.

- **Derecho de supresión.** El artículo 17 del Reglamento General de Protección de Datos reconoce el derecho a obtener la supresión de los datos personales, y la doctrina del Tribunal de Justicia de la Unión Europea en el asunto Google Spain (2014) extendió su aplicación a los resultados de los motores de búsqueda. Es la herramienta que da soporte a la recomendación de depurar la huella pública: no depende de la buena voluntad del prestador.
- **Derechos digitales en el ordenamiento español.** El título X de la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales recoge, entre otros, el derecho a la desconexión digital en el ámbito laboral y disposiciones específicas sobre la protección de los menores en internet, lo que dota de base normativa a la conversación sobre límites de uso y sobre acompañamiento.
- **Marco europeo de identidad digital.** El Reglamento (UE) 2024/1183, conocido como eIDAS 2, en vigor desde mayo de 2024, crea la Cartera Europea de Identidad Digital, que los Estados miembros deben poner a disposición de la ciudadanía a finales de 2026. Su despliegue modificará de raíz el escenario descrito en este capítulo, al desplazar el peso de la autenticación desde la contraseña hacia credenciales verificables con divulgación selectiva de atributos.
- **Marco de seguridad de las entidades.** La Directiva (UE) 2022/2555 (NIS2) y, en el ámbito financiero, el Reglamento (UE) 2022/2554 sobre resiliencia operativa digital (DORA) elevan las exigencias de gestión de riesgos y notificación de incidentes de los operadores. Para el usuario, la consecuencia relevante es que el eslabón institucional de la cadena está cada vez más regulado, lo que desplaza el punto débil relativo hacia el extremo doméstico: la contraseña reutilizada y la cuenta de correo sin recuperación configurada.

La conclusión técnica del estudio en una frase

La protección de esta muestra depende demasiado de su capacidad de reacción y demasiado poco de su configuración. Reaccionar bien exige acertar todas las veces; configurar bien exige acertar una sola. Cualquier acción divulgativa que aspire a mejorar el resultado debería trasladar esfuerzo desde la primera categoría, ya saturada, hacia la segunda.



14. Protocolos prácticos

Los temas anteriores explican qué ocurre y por qué. Este contiene lo que hay que hacer. Cada uno de los nueve protocolos que siguen responde a un ítem deficitario concreto del estudio, indica los pasos en el orden en que deben ejecutarse, señala cómo comprobar que la medida ha quedado bien aplicada y estima el tiempo necesario. Están redactados para poder entregarse sueltos, de modo que puedan reutilizarse como fichas divulgativas, material de taller o contenido para clientes sin necesidad de acompañarlos del informe completo.

El criterio de ordenación es el mismo que rige el capítulo de recomendaciones: relación entre el impacto esperado y el esfuerzo exigido. Y el criterio de redacción procede del capítulo 12: siempre que ha sido posible, la acción propuesta modifica el entorno o la configuración en lugar de apelar a la fuerza de voluntad, porque las conductas que el estudio identifica como deficitarias son en su mayoría automatismos y no decisiones.

Cómo usar estos protocolos

Ninguna persona necesita necesariamente los nueve. El capítulo 9 del informe describe cuatro perfiles con problemas distintos. Como regla general: quien puntúa alto en seguridad y bajo en hábitos debe empezar por los protocolos 4, 5 y 6; quien presenta el patrón inverso, por los protocolos 1, 2 y 3. Aplicar más de dos protocolos a la vez reduce la probabilidad de completar cualquiera de ellos.

14.1. El plan de 30 días

Para quien prefiera una secuencia cerrada en lugar de elegir protocolos sueltos, el siguiente calendario distribuye las acciones de mayor impacto en cuatro semanas, alternando medidas de configuración —que se hacen una vez— con medidas de hábito, que necesitan repetición. El orden no es arbitrario: la primera semana no exige cambiar ninguna conducta, precisamente para no encontrar resistencia en el arranque.

Semana	Acción	Tipo	Tiempo
1	Activar el informe de tiempo de pantalla del dispositivo y no hacer nada más que mirarlo (protocolo 5)	Medición	5 min + observación
1	Asegurar la recuperación del correo principal (protocolo 1)	Configuración	15 min
2	Sacar el cargador y el móvil del dormitorio durante catorce noches (protocolo 4)	Hábito	10 min de preparación
2	Instalar un gestor de contraseñas y migrar las cinco cuentas críticas (protocolo 2)	Configuración	40 min
3	Completar el segundo factor en todas las cuentas importantes (protocolo 2, fase 3)	Configuración	30 min
3	Activar la copia de seguridad automática y probar una restauración (protocolo 7)	Configuración	20 min
4	Auditar la huella pública propia y cerrar cuentas antiguas (protocolo 3)	Revisión	60-90 min
4	Acordar y escribir las normas de uso con los menores del entorno (protocolo 6)	Acuerdo	45 min

Al cabo de los treinta días quedan resueltas de forma permanente las cinco vulnerabilidades de configuración que el estudio identifica (recuperación del correo, contraseñas, segundo factor, copias y huella pública) y quedan iniciadas las dos que dependen de repetición: el dormitorio sin pantallas y la medición del tiempo de uso.

14.2. Protocolo 1 · Asegurar el correo principal

Responde a: P20. El 46,3 % de la muestra no tiene claro cómo recuperaría el acceso a su cuenta de correo principal. Tiempo estimado: 15 minutos. Frecuencia: una vez, con revisión anual.

El correo principal es la vía de restablecimiento de contraseña de prácticamente todos los demás servicios, incluida la banca. Perder el acceso a esa cuenta no equivale a perder un servicio: equivale a perder la llave de todos.

Pasos

- **Identificar la cuenta raíz.** Comprobar cuál es la dirección de correo asociada a las cuentas bancarias, a la tienda de aplicaciones y a las redes sociales. Si son varias, este protocolo se aplica a todas ellas.
- **Registrar un teléfono de recuperación** en los ajustes de seguridad del proveedor de correo, y verificar que el número es el actual y no uno de una línea dada de baja.
- **Registrar una dirección de correo alternativa** distinta de la principal, preferiblemente en otro proveedor, para que un problema con uno no bloquee el acceso al otro.
- **Descargar los códigos de respaldo de un solo uso** que ofrece el proveedor y guardarlos fuera del dispositivo: impresos en casa o en el gestor de contraseñas. No en el propio correo, que es precisamente la cuenta a la que no se podrá acceder.
- **Activar el segundo factor** en esa cuenta, empleando el método más robusto que ofrezca el proveedor, según la tabla del apartado 13.5.
- **Revisar las sesiones y los dispositivos con acceso** y cerrar los que ya no se usen. Es habitual encontrar equipos antiguos con sesión abierta.
- **Revisar las reglas de reenvío automático.** Una regla de reenvío desconocida es uno de los signos más frecuentes de que una cuenta está comprometida.

Verificación

El protocolo no está completo hasta que se comprueba. Cerrar la sesión en el navegador e intentar entrar de nuevo utilizando únicamente uno de los métodos de recuperación configurados. Si el proceso funciona sin recurrir a la contraseña memorizada, la cuenta está asegurada. Repetir esta comprobación una vez al año.

14.3. Protocolo 2 · Migrar a un gestor de contraseñas

Responde a: P8 y P9. El 43,8 % reutiliza contraseñas o las maneja sin criterio y solo el 28,2 % usa un gestor; el 38,6 % tiene el segundo factor solo en algunas cuentas. Tiempo estimado: 40 minutos iniciales y unos minutos por sesión durante las semanas siguientes. Frecuencia: una vez.

El error más común al abordar esta migración es intentar cambiar todas las contraseñas de golpe. Es la vía más rápida al abandono. El procedimiento siguiente reparte el esfuerzo en tres fases y aprovecha el uso cotidiano para completar el trabajo sin sesiones dedicadas.

Fase 1 Instalación y cuentas críticas (40 minutos)

Elegir un gestor —vale el integrado en el sistema operativo o en el navegador si eso reduce la fricción; un gestor imperfecto en uso es mejor que uno excelente sin instalar—, crear una contraseña maestra larga que no se haya usado nunca en ningún otro sitio y memorizarla. Después, cambiar únicamente las contraseñas de cinco cuentas: correo principal, banco, tienda de aplicaciones, red social principal y cualquier servicio donde haya datos de pago guardados. Cada nueva contraseña la genera el gestor y no se memoriza.

Fase 2 Migración por uso (semanas siguientes)

No abrir ninguna sesión dedicada. Cada vez que un servicio pida la contraseña en el uso normal, cambiarla en ese momento y guardarla en el gestor. En cuatro o cinco semanas la mayoría del inventario está migrado, y lo que no se ha usado en cinco semanas probablemente sea una cuenta que conviene cerrar, lo que enlaza con el protocolo 3.

Fase 3 Segundo factor (30 minutos)

Activar la verificación en dos pasos en todas las cuentas de la fase 1, empezando por el correo. Donde el servicio ofrezca clave de acceso o llave física, elegir esa opción; donde solo ofrezca aplicación de códigos o SMS, activar lo disponible, que siempre es mejor que nada. Guardar los códigos de respaldo en el gestor.

Un apunte sobre la resistencia más frecuente

La objeción habitual (“no me fío de dejar todas mis contraseñas en un mismo sitio”) tiene una respuesta corta: ya están todas en un mismo sitio, que es la memoria de la persona, y por eso se repiten. El riesgo real medido en este estudio no es que un gestor sea comprometido, sino que la misma clave que protege el banco haya aparecido ya en la filtración de un foro cualquiera.

14.4. Protocolo 3 · Auditoría de la huella pública

Responde a: P19. El 57,3 % no ha comprobado nunca qué información suya es pública o lo hizo hace años; solo el 14,5 % la gestiona. Tiempo estimado: entre 60 y 90 minutos. Frecuencia: anual.

Pasos

- **Buscar el propio nombre** entre comillas en dos motores de búsqueda distintos y revisar las tres primeras páginas de resultados, en la pestaña general y en la de imágenes. Anotar lo que aparezca y no debería.
- **Buscar también la dirección de correo y el número de teléfono**, que suelen devolver resultados distintos a los del nombre: perfiles antiguos, foros, listas de contacto publicadas por terceros.
- **Comprobar si el correo figura en filtraciones conocidas** mediante un servicio de consulta de brechas. Toda cuenta que aparezca implica cambiar su contraseña y, sobre todo, cambiar esa misma contraseña en cualquier otro sitio donde se hubiera reutilizado.
- **Inventariar y cerrar cuentas antiguas**. Revisar el correo buscando mensajes de bienvenida o de recuperación para localizar servicios olvidados. Cerrar formalmente en lugar de dejar de usar: una cuenta abandonada sigue almacenando datos y sigue expuesta a las filtraciones del proveedor.
- **Revisar la audiencia de lo publicado** en las redes que se mantengan activas, con atención especial al contenido antiguo, que suele conservar la configuración de privacidad que tenía cuando se publicó.
- **Ejercer el derecho de supresión** cuando exista contenido que no se puede retirar directamente, según el modelo que figura a continuación.

Modelo breve de solicitud de supresión

Dirigido al responsable del tratamiento o, en el caso de resultados de búsqueda, al formulario habilitado por el buscador. Conviene conservar copia y acuse de recibo.

Solicito, al amparo del artículo 17 del Reglamento (UE) 2016/679, la supresión de los datos personales que se indican a continuación, así como su retirada de los resultados de búsqueda asociados a mi nombre. Adjunto copia de documento identificativo. Se indica la dirección exacta del contenido y el motivo de la solicitud. Ruego confirmación de la actuación realizada en el plazo previsto en el artículo 12 del citado Reglamento.

Si la solicitud no se atiende, cabe reclamación ante la Agencia Española de Protección de Datos. Este modelo es orientativo y no sustituye al asesoramiento jurídico en casos complejos, especialmente cuando el contenido afecta a terceros o procede de fuentes periodísticas.

14.5. Protocolo 4 · Dormitorio sin pantallas

Responde a: P6, el peor ítem del estudio (2,18 sobre 4). El 62,5 % consulta el móvil ya acostado y el 38,4 % lo hace todas las noches. Tiempo estimado: 10 minutos de preparación. Frecuencia: catorce noches seguidas para instaurar el hábito.

Este es el protocolo con mejor relación entre esfuerzo y beneficio de todo el informe, porque el descanso media entre el uso del dispositivo y el estado de ánimo, la atención y la capacidad de autorregulación del día siguiente. La preparación es más importante que la fuerza de voluntad: si el móvil está en la mesilla, la decisión hay que tomarla cada noche; si está en la cocina, no hay decisión que tomar.

Preparación, una sola vez

- Trasladar el cargador a otra habitación, preferiblemente lejos del dormitorio.
- Conseguir un despertador independiente. Es el obstáculo práctico que hace fracasar la mayoría de los intentos.
- Programar el modo de concentración o no molestar en una franja fija, por ejemplo de 23:00 a 7:00, con una lista breve de contactos exceptuados para urgencias familiares.
- Elegir de antemano con qué se sustituye el rato de pantalla: lectura en papel, música, cualquier cosa que ocupe ese hueco. Retirar un hábito sin sustituirlo deja un vacío que el hábito anterior tiende a rellenar.

Las dos primeras semanas

Conviene anticipar que las tres o cuatro primeras noches resultarán incómodas y que esa incomodidad no es señal de que el método no funcione, sino de que la señal contextual sigue activa y no encuentra su respuesta habitual. Marcar en un calendario visible las noches cumplidas ayuda más de lo que parece, porque convierte una conducta invisible en un registro.

Para quien no pueda o no quiera sacar el dispositivo de la habitación, la versión mínima del protocolo consiste en dejarlo fuera del alcance del brazo desde la cama. Es notablemente menos eficaz, pero mantiene el principio: introducir fricción física entre la señal y la conducta.

14.6. Protocolo 5 · Medir antes de reducir

Responde a: P4 y P26. El 56,2 % declara un tiempo de pantalla superior al deseado y el 84,9 % afirma llevar el control, una combinación que el capítulo 10 identifica como la brecha central del estudio. Tiempo estimado: 5 minutos de configuración y dos semanas de observación.

El orden de este protocolo es su única particularidad, y es innegociable: primero se mide sin cambiar nada y solo después se fija un objetivo. La razón está en el capítulo 12: quien no percibe un problema no responde a las advertencias, pero sí responde a la discrepancia entre lo que creía y lo que ve. Fijar un límite antes de medir convierte el ejercicio en una imposición externa; medir primero lo convierte en una conclusión propia.

Semanas 1 y 2 Solo observar

Activar el informe de uso que incorpora el propio sistema operativo y consultarlo una vez a la semana, sin fijar ningún límite ni proponerse nada. Anotar tres cifras: el tiempo total diario medio, el número de desbloques y las dos aplicaciones que encabezan la lista. Antes de mirar el informe por primera vez conviene escribir la propia estimación, porque la diferencia entre lo estimado y lo real es el dato que produce el efecto.

Semana 3 Un solo objetivo

Elegir únicamente la aplicación que encabece la lista y fijarle un límite diario un 20 % inferior al uso medido, no una cifra ideal. Los objetivos ambiciosos fracasan y el fracaso desacredita el método entero. Si el límite se cumple con holgura durante una semana, se baja otro escalón.

Semana 4 Cambiar el uso, no solo el tiempo

Según se expone en el apartado 12.6, el malestar asociado a las redes sociales se vincula sobre todo al consumo pasivo y a la comparación social, no al tiempo en sí. Por eso el indicador que conviene adoptar a partir de aquí no es el contador de minutos, sino una pregunta al salir de la aplicación: cómo se siente uno ahora comparado con

hace veinte minutos. Depurar a quién se sigue, silenciando las cuentas cuya lectura empeora sistemáticamente el ánimo, suele tener más efecto que restar quince minutos al contador.

14.7. Protocolo 6 · Acuerdo de uso con los menores del entorno

Responde a: P27, la segunda peor pregunta del estudio (2,35). El 50,7 % deja acceso libre sin normas claras o prohíbe sin explicar; solo el 15,9 % pacta, explica y da ejemplo. Tiempo estimado: 45 minutos de conversación. Frecuencia: revisión cada seis meses o en cada cambio de etapa escolar.

El apartado 12.7 explica por qué ni la ausencia de norma ni la prohibición sin motivo generan autorregulación. Lo que sí la genera es la norma pactada, explicada y sostenida por el ejemplo del adulto. Escribirla importa: un acuerdo verbal se reinterpreta cada noche, uno escrito y visible no.

Contenido mínimo del acuerdo

Apartado	Qué debe concretar
Dónde	Espacios sin dispositivo para todos, empezando por los dormitorios y la mesa durante las comidas
Cuándo	Franjas horarias concretas, con hora de entrega del dispositivo por la noche
Qué	Plataformas permitidas y edad mínima declarada por cada una; quién aprueba las instalaciones nuevas
Con quién	Con quién se puede hablar y qué hacer ante un contacto desconocido o un contenido incómodo
Qué no se comparte	Ubicación en tiempo real, imágenes de otras personas sin permiso, datos del centro escolar, contraseñas
Qué pasa si algo sale mal	Compromiso explícito de que contarle no acarrea castigo; esta cláusula es la más importante de todas
Qué se compromete el adulto	Las mismas reglas de espacio y horario, y la revisión periódica del acuerdo

La última fila no es un gesto simbólico. Es la parte del acuerdo que determina si funciona, porque el aprendizaje por observación no distingue entre la norma enunciada y la conducta observada, y en caso de contradicción prevalece la segunda. El adulto que consulta el móvil en la cama está enseñando eso con independencia de qué controles parentales haya instalado.

Sobre las herramientas de control parental

Son útiles como apoyo y como red de seguridad en las edades más tempranas, pero no sustituyen al acuerdo. Un control técnico se elude, se desactiva o deja de aplicarse cuando el menor usa otro dispositivo, y no enseña criterio: produce obediencia mientras dura la supervisión. La herramienta acompaña a la norma, no la reemplaza.

14.8. Protocolo 7 · Copias de seguridad y prueba de restauración

Responde a: P18. El 27,4 % perdería bastantes o casi todos sus datos si mañana perdiera el móvil. Tiempo estimado: 20 minutos. Frecuencia: configuración única y comprobación anual.

Es el único riesgo del estudio que no necesita atacante: basta una caída, un robo o una avería. La referencia habitual sigue siendo la regla de las tres copias: tres ejemplares de los datos, en dos soportes distintos, con uno de ellos fuera del dispositivo principal.

- **Activar la copia automática** en la nube del propio sistema operativo, comprobando que incluye fotografías, contactos, mensajes y documentos, y no solo la configuración del dispositivo.
- **Añadir una copia local periódica** en un disco externo o en el ordenador, con una frecuencia realista: trimestral es mejor que semanal si semanal no se va a cumplir.

- **Comprobar el espacio disponible.** La causa más frecuente de copia interrumpida es una cuenta de almacenamiento llena que dejó de avisar hace meses.
- **Probar la restauración.** Recuperar un archivo concreto desde la copia y verificar que se abre. Una copia que nunca se ha restaurado es una hipótesis, no una copia.

Conviene añadir un matiz técnico: la sincronización no es una copia de seguridad. Un archivo borrado o cifrado por un programa malicioso se propaga a todos los dispositivos sincronizados en cuestión de segundos. La protección real la aporta el historial de versiones, que la mayoría de los servicios ofrece durante un periodo limitado y que conviene conocer antes de necesitarlo.

14.9. Protocolo 8 · Las primeras 24 horas ante un fraude bancario

Este apartado tiene carácter divulgativo y describe el procedimiento general; no constituye asesoramiento jurídico ni sustituye la consulta profesional en casos concretos.

Responde a: el bloque 4 y, en particular, a la necesidad de que la reacción esté decidida antes de que ocurra. Tiempo estimado: la secuencia completa se ejecuta el mismo día.

La rapidez determina el resultado, y la rapidez depende de no tener que averiguar nada en el momento. Este es el orden de actuación.

Momento	Actuación
Minuto 0	Bloquear la tarjeta o la operativa desde la aplicación del banco, sin esperar a hablar con nadie. Es la acción más rápida disponible y es reversible.
Minutos 1-15	Llamar al teléfono oficial de la entidad, el que figura en el reverso de la tarjeta o en la aplicación, nunca el que aparezca en un mensaje recibido. Notificar la operación no autorizada y pedir el número de incidencia.
Primera hora	Cambiar las credenciales de banca electrónica y, si se han introducido datos en algún sitio, las de la cuenta de correo asociada. Revisar las sesiones abiertas y las reglas de reenvío del correo.
Primeras horas	Reunir las pruebas antes de que desaparezcan: capturas del mensaje o de la web, número del remitente, hora exacta, importe y referencia de la operación.
Mismo día	Presentar reclamación escrita a la entidad, con acuse de recibo, solicitando expresamente la devolución del importe de la operación no autorizada.
Mismo día o siguiente	Denunciar ante la Policía Nacional o la Guardia Civil y conservar copia con número de referencia; es documentación necesaria para el resto del proceso.
En paralelo	Consultar con el servicio gratuito y confidencial de ayuda en ciberseguridad de INCIBE, en el teléfono 017 o por sus canales de mensajería, que orienta sobre los pasos y sobre la recopilación de pruebas.

Los plazos que conviene conocer

El Real Decreto-ley 19/2018, de servicios de pago, establece que ante una operación de pago no autorizada el proveedor debe devolver el importe de inmediato y, a más tardar, al final del día hábil siguiente a aquel en que la operación se le notificó, salvo que tenga motivos razonables para sospechar fraude y los comunique por escrito al Banco de España. La misma norma limita con carácter general a 50 euros la cantidad que el titular puede verse obligado a soportar por operaciones no autorizadas derivadas de un instrumento de pago extraviado o sustraído, con las excepciones que la propia norma detalla, entre ellas la actuación fraudulenta o el incumplimiento gravemente negligente de las obligaciones de custodia.

Si la entidad no responde o la respuesta no es satisfactoria, el siguiente paso es el servicio de atención al cliente de la propia entidad, que dispone de quince días hábiles para responder cuando la reclamación se refiere a servicios de pago. Agotado ese trámite, cabe acudir al Departamento de Conducta de Entidades del Banco de España, cuya reclamación es gratuita y se presenta por vía electrónica.

Qué no hacer

No responder al mensaje ni volver a llamar al número desde el que llegó la comunicación. No instalar ninguna aplicación de asistencia remota que se solicite por teléfono, porque es el vector habitual de la segunda fase del fraude. No borrar los mensajes recibidos: son la prueba. Y no dar por perdido el importe sin reclamar formalmente por escrito, porque la reclamación verbal no activa los plazos legales.

14.10. Protocolo 9 · Cuando notifican una filtración de datos

Responde a: la grieta descrita en el apartado 13.3, donde el 43,8 % de la muestra reutiliza contraseñas. Tiempo estimado: 20 minutos por aviso.

El aviso de que un servicio ha sufrido una brecha suele generar una reacción insuficiente: cambiar la contraseña de ese servicio y dar el asunto por cerrado. El problema es que el valor de una credencial filtrada no está en el servicio de origen, sino en todos los demás sitios donde esa misma combinación funcione.

- Cambiar la contraseña del servicio afectado.
- Cambiar esa misma contraseña en cualquier otro sitio donde se hubiera reutilizado, aunque no guarde ninguna relación con el servicio filtrado. Este es el paso que casi nadie completa y el único que cierra realmente el riesgo.
- Activar el segundo factor en el servicio afectado si no lo tenía.
- Revisar los movimientos y las sesiones abiertas de las cuentas asociadas al correo que figuraba en la filtración.
- Extremar la desconfianza durante las semanas siguientes: los datos filtrados alimentan campañas de fraude personalizado que citan información real para resultar creíbles.

Si la contraseña estaba en un gestor y era única, este protocolo se reduce al primer punto. Esa diferencia (veinte minutos de trabajo frente a treinta segundos) es el argumento más concreto a favor del protocolo 2.

14.11. Lista de verificación por bloques

Resumen operativo de los nueve protocolos, organizado según los cinco bloques del cuestionario, para poder utilizarse como hoja de control independiente.

Bloque	Comprobación	Protocolo
B1 · Hábitos de uso	El móvil se carga fuera del dormitorio y hay despertador independiente	4
B1 · Hábitos de uso	El informe de tiempo de pantalla está activo y se ha consultado este mes	5
B1 · Hábitos de uso	Solo llegan notificaciones de personas, no de aplicaciones	5
B2 · Ciberseguridad	Todas las contraseñas de las cuentas críticas son únicas y están en un gestor	2
B2 · Ciberseguridad	El segundo factor está activo en correo, banco y tienda de aplicaciones	2
B2 · Ciberseguridad	Los permisos de las aplicaciones se han revisado en los últimos doce meses	3
B3 · Protección de datos	La copia de seguridad automática está activa y se ha probado una restauración	7
B3 · Protección de datos	Se ha buscado el propio nombre y se han cerrado las cuentas antiguas este año	3
B4 · Prevención de riesgos	La recuperación del correo principal está configurada y verificada	1
B4 · Prevención de riesgos	Los códigos de respaldo están guardados fuera del dispositivo	1
B4 · Prevención de riesgos	El teléfono oficial del banco está guardado en la agenda antes de necesitarlo	8
B5 · Huella y bienestar	Existe un acuerdo de uso escrito con los menores del entorno	6
B5 · Huella y bienestar	Se han silenciado las cuentas cuya lectura empeora el ánimo	5

El criterio que ordena los nueve protocolos

Siete de los nueve son medidas de configuración: se ejecutan una vez y siguen protegiendo sin que la persona vuelva a intervenir. Solo dos (el dormitorio sin pantallas y la medición del uso) exigen repetición, y son precisamente los dos que responden a los ítems peor puntuados del estudio. Esa proporción no es casual: es la traducción operativa del hallazgo central del informe, que la protección de esta muestra depende demasiado de su capacidad de reacción y demasiado poco de su configuración.



15. Limitaciones del estudio

- **Muestra de autoselección.** Los participantes deciden voluntariamente hacer un test de bienestar digital, lo que sesga la muestra hacia personas ya sensibilizadas. La ausencia total de casos en zona de alerta es, con toda probabilidad, un artefacto de este sesgo y no un dato poblacional.
- **Medidas autoinformadas.** Todas las respuestas son declaraciones del propio participante, sin verificación objetiva. El sesgo de deseabilidad social es previsiblemente mayor en el bloque de ciberseguridad, donde la respuesta correcta es más evidente, lo que podría estar inflando su resultado.
- **Sobrerrepresentación de estudios superiores.** El 63,3 % de la muestra tiene formación universitaria o de postgrado, muy por encima de la población general. Este sesgo resulta, no obstante, menos problemático de lo habitual, dado que el nivel de estudios no muestra ningún efecto sobre los resultados.
- **Tramos extremos de edad con muestra insuficiente.** Los grupos de menos de 20 años ($n = 9$) y de más de 59 ($n = 7$) no permiten conclusiones fiables y se han excluido de los contrastes estadísticos.
- **Diseño transversal.** Los datos describen un momento único y no permiten establecer relaciones causales ni medir evolución.



Anexos

Anexo 1. Los diez hallazgos principales

Bloque 1. Tus hábitos de uso

Tiempo de pantalla, notificaciones y consumo automático

1 ¿Cuántas veces calculas que desbloqueas el móvil a lo largo de un día normal?

- a Constantemente, decenas de veces. Es casi como un acto reflejo, desbloqueo sin ni siquiera pensar en ello.
- b Con mucha frecuencia, pierdo la cuenta. A menudo lo desbloqueo por el hábito de mirar la pantalla.
- c Bastantes veces al día, casi en todas por necesidad de hacer algo con él
- d Solo cuando necesito hacer algo específico (revisar mensajes o apps concretas). Es siempre un uso intencionado.

2 Estás esperando en una cola. Lo primero que hace tu mano es...

- a Seguramente ya tenía el móvil en la mano antes de llegar a la cola.
- b Sacar el móvil casi sin pensarlo.
- c Mirar el móvil solo si estoy esperando algo concreto en él.
- d Quedarme tranquilo/a sin necesidad de mirar el móvil.

3 ¿Cómo tienes configuradas las notificaciones de tus aplicaciones?

- a Casi todo activado; el móvil me suena o se ilumina con frecuencia la pantalla.
- b Tengo bastantes notificaciones activadas, aunque muchas de ellas no son urgentes.
- c Solo recibo las importantes (mensajes, llamadas).
- d Solo las importantes y uso un sistema que restringe todas las notificaciones: modos de concentración, silencio por franjas horarias, etc.

4 Si tuvieras que decir ahora mismo tu tiempo medio de pantalla diario...

- a Reconozco que es muchísimo y no tengo mucho control sobre ello.
- b Lo intuyo, es más de lo que me gustaría, pero lo voy controlando más o menos
- c En general lo tengo controlado, aunque algunos días se me vaya el tiempo usándolo
- d No me he preocupado porque no dependo demasiado del móvil.

5 ¿Cuál de estas frases se parece más a ti con las redes sociales?

- a Se me pasan horas enteras en los carruseles de las redes sociales, es algo habitual.
- b Algunas veces entro “un momento” y se me va más de media hora sin darme cuenta
- c Entro con un objetivo y suelo salir al cumplirlo
- d Las reviso de forma muy puntual y el resto del día no las toco

6 ¿Qué papel tiene el móvil cuando te vas a dormir?

- a Todas las noches me acuesto y lo miro un rato.
- b Algunas veces lo miro antes de dormirme.
- c Lo uso un poco, pero intento dejarlo un rato antes de ir a dormir
- d Habitualmente no lo consulto en cama ni antes de irme a dormir

7 Cuando estás con personas que te importan, ¿cuánto aparece el móvil?

- a** Lo consulto con frecuencia, aunque esté en compañía de otra persona
- b** Lo miro cada poco “por si acaso”
- c** Si estoy con otra persona, solo atiendo al móvil si es algo importante
- d** Lo guardo y estoy presente con esa persona

Bloque 2. Tu ciberseguridad

Contraseñas, doble factor, phishing y permisos de apps

8 ¿Cómo gestionas tus contraseñas?

- a** Uso la misma o casi la misma en todo
- b** Tengo varias, que voy combinando sin un criterio concreto
- c** Son distintas, pero las recuerdo de memoria y para los sitios importantes uso contraseñas únicas
- d** Uso un gestor de contraseñas con claves únicas y robustas

9 ¿Tienes activada la verificación multifactor o MFA (dos o más factores para acceder) en tus cuentas importantes?

- a** No sé muy bien qué es eso
- b** Sé lo que es, pero no la tengo activada en casi ningún sitio o en ninguno.
- c** La tengo en algunas cuentas (correo o banco)
- d** La tengo en todas mis cuentas importantes

10 Recibes un SMS o mensaje de mensajería instantánea (WhatsApp, Telegram...): “Su cuenta del banco ha sido bloqueada. Verifique aquí: bit.ly/xxxx”. ¿Qué haces?

- a** Pincho el enlace para arreglarlo cuanto antes
- b** Pincho para ver qué es, pero solo miro sin poner datos
- c** No pincho; lo borro sin más
- d** No pincho; entro yo a la app oficial del banco o llamo al teléfono que ya conozco del banco para comprobarlo

11 Recibes un mensaje (por redes sociales, WhatsApp o email) con una oportunidad de inversión: “Invierte hoy con nosotros y consigues alta rentabilidad garantizada en poco tiempo. Empieza con solo X€”. Incluso te llaman para asesorarte y generarte confianza. ¿Qué haces?

- a** Invierto cuanto antes para no perder la oportunidad
- b** Busco algo de información y, si parece fiable, hago una pequeña inversión de prueba
- c** Desconfío, investigo la empresa y solo invertiría si veo que está regulada y es legítima
- d** No invierto; ignoro el ofrecimiento y, si me interesa invertir, acudo a entidades reguladas que ya conozco o verifico en fuentes oficiales antes de tomar cualquier decisión

12 Cuando instalas una app y te pide permisos (cámara, micrófono, contactos, ubicación)...

- a** Acepto todo para que funcione rápido, sin revisar nada de las condiciones
- b** Acepto revisando algo de las condiciones, muy por encima.
- c** Acepto revisando bien las condiciones (y si algo no me genera confianza no lo acepto)
- d** Reviso cada apartado bien y cada permiso que doy. Solo concedo los permisos en los que confío y que vea que son estrictamente necesarios

13 Estás en una wifi pública (cafetería, aeropuerto) y vas a entrar en tu banco. Lo más prudente es...

- a** Entrar con normalidad, no pasa nada
- b** Entrar con normalidad, pero vigilando que no se abran ventanas extrañas
- c** Entrar rápido para hacer el trámite y salir lo antes posible.
- d** Conectarme con mis datos móviles o solo desde una red de confianza

14 ¿Qué haces con las actualizaciones de tu móvil y tus apps?

- a** Las ignoro; llevo meses sin actualizar
- b** Las hago cuando el móvil ya casi no me deja seguir usándolas
- c** Las hago de vez en cuando
- d** Las tengo en automático o las instalo enseguida

Bloque 3. Cómo proteges tus datos, dispositivos y sesiones

Bloqueo, sesiones abiertas, privacidad y copias de seguridad

15 ¿Cómo se desbloquea tu móvil?

- a** No tiene ningún bloqueo
- b** Con un patrón o PIN sencillo (1234, una fecha...)
- c** Con PIN no muy sencillo
- d** Con biometría o un PIN robusto, cuidando mucho que nadie mire mi pantalla mientras lo introduzco y teniendo un bloqueo automático rápido

16 Cuando usas un ordenador que no es tuyo (trabajo, biblioteca, de un familiar)...

- a** Inicio sesión y no me preocupo de cerrarla
- b** Algunas veces se me olvida cerrar sesión
- c** Cierro sesión al terminar
- d** Uso ventana privada (navegador de incógnito), cierro todo al terminar y reviso después que la sesión se haya cerrado.

17 Vas a publicar una foto de tus vacaciones. ¿Qué tienes en cuenta?

- a** La publico al momento, sin pensarlo
- b** La publico, aunque a veces pienso en algunas medidas de seguridad
- c** Evito mostrar datos sensibles (ubicación en directo, billetes, matrículas)
- d** Controlo la audiencia, no comparto ubicación en tiempo real y reviso qué y quién sale en la imagen

18 Si mañana pierdes el móvil o se rompe, ¿qué pasa con tus fotos y datos?

- a** Los perdería casi todos
- b** Perdería bastantes
- c** Quizá perdería algo, pero tengo copia de lo más importante
- d** Tengo copias automáticas y podría restaurarlo prácticamente todo

19 ¿Sabes qué información tuya hay pública en internet (al buscar tu nombre, cuentas antiguas...)?

- a** Nunca lo he mirado
- b** Lo he mirado alguna vez por curiosidad, hace bastante tiempo
- c** Lo reviso de vez en cuando
- d** Lo reviso y lo gestiono: cierro cuentas viejas y cuido mi privacidad

Bloque 4. Prevención de riesgos y gestión de incidencias

Tu capacidad para anticiparte y reaccionar ante un problema

- 20 Si perdieras el acceso a tu correo principal, ¿podrías recuperarlo?**
- a** No sabría por dónde empezar
 - b** Lo intentaría, pero no tengo nada preparado
 - c** Sí, hice algo hace tiempo que tenía que ver con la recuperación, podría buscarlo para ver cómo era.
 - d** Tengo clara la forma de recuperación y no sería problema
- 21 Cuando descargas una app, ¿desde dónde lo haces normalmente?**
- a** Desde cualquier sitio que encuentre o que me compartan, no me fijo mucho
 - b** Desde buscadores o webs
 - c** Casi siempre desde tiendas oficiales
 - d** Únicamente desde tiendas oficiales, leyendo la información del desarrollador, las valoraciones y los permisos que me pide
- 22 Recibes una llamada de alguien que dice ser tu banco o de soporte técnico que dice que hay una incidencia y te pide actuar con urgencia para impedir bloqueos de tu cuenta, ¿qué haces?**
- a** Sigo las instrucciones para resolverlo rápido
 - b** Escucho y accedo, aunque me genera ciertas sospechas
 - c** Cuelgo, lo ignoro y me despreocupo
 - d** Cuelgo y accedo o me comunico únicamente por un canal oficial a mi banco
- 23 Si alguien inesperado te llama o te escribe y en la conversación te pide un código que te ha llegado por SMS, ¿qué haces?**
- a** Se lo doy para seguir con el trámite que me está indicando
 - b** Se lo doy si quien llama me ha dicho que llama de una empresa que conozco
 - c** No le doy el código, pero me quedaría con dudas.
 - d** Nunca comparto claves o códigos de verificación que me llegan al móvil sin una comprobación y una seguridad absoluta de que no es un fraude.

Bloque 5. Huella digital y bienestar

Impacto ambiental, efecto en tu ánimo y uso intencionado

- 24 ¿Sabías que el uso de internet (herramientas de IA, correos, streaming, nube) también genera huella de carbono?**
- a** No tenía ni idea
 - b** Algo había oído, pero no lo tengo muy en cuenta
 - c** Lo sé y a veces lo tengo en cuenta
 - d** Lo sé y aplico hábitos del cuidado del medio ambiente vinculados con mi utilización de redes e internet.
- 25 Después de un buen rato en redes sociales, lo más habitual es que te sientas...**
- a** Peor: comparación, ansiedad o sensación de tiempo perdido
 - b** Algo inquieto/a o disperso/a
 - c** Más o menos igual
 - d** Bien, porque las uso con control, de forma intencionada y limitada
- 26 En tu relación con la tecnología, ¿quién manda?**
- a** La tecnología me maneja a mí; voy a remolque de notificaciones, apps y deslizamientos en redes sociales durante demasiado tiempo
 - b** Más bien ella que yo, la mayor parte del tiempo.
 - c** Hay equilibrio, con altibajos. Controló la mayor parte del tiempo, pero a veces se me va.
 - d** Tengo control. Yo decido cuándo, cómo y para qué las uso.

27 ¿Cómo los menores de edad de tu entorno más cercano tienen acceso habitualmente a la telefonía móvil e internet?

- a Tienen generalmente acceso bastante libre y sin normas claras.
- b Se gestiona todo por la vía de la prohibición cuando no se quiere que el menor lo use, pero no se explica mucho el motivo ni los hábitos de uso saludable
- c Existen con los menores algunos hábitos y límites explicados y acordados.
- d Se observa un claro enfoque en la educación digital de los menores y el acompañamiento pactando normas y explicando los motivos concretos de esas normas, explicando los riesgos del mal uso y dando ejemplo frente a ellos.

Anexo 2. Resultados de las 27 preguntas

Porcentaje de respuestas en cada opción y puntuación media. Las opciones están ordenadas de menor (a) a mayor (d) grado de bienestar digital.

P	Bl.	Pregunta	% a	% b	% c	% d	$\bar{x}$
P1	B1	¿Cuántas veces calculas que desbloqueas el móvil a lo largo de un día normal?	13,7	32,9	33,7	19,7	2,59
P2	B1	Estás esperando en una cola. Lo primero que hace tu mano es...	7,4	42,7	29,3	20,5	2,63
P3	B1	¿Cómo tienes configuradas las notificaciones de tus aplicaciones?	2,5	22,7	54,5	20,3	2,93
P4	B1	Si tuvieras que decir ahora mismo tu tiempo medio de pantalla diario...	22,5	33,7	29,6	14,2	2,36
P5	B1	¿Cuál de estas frases se parece más a ti con las redes sociales?	8,5	55,1	17,0	19,5	2,47
P6	B1	¿Qué papel tiene el móvil cuando te vas a dormir?	38,4	24,1	18,6	18,9	2,18
P7	B1	Cuando estás con personas que te importan, ¿cuánto aparece el móvil?	2,7	14,8	61,4	21,1	3,01
P8	B2	¿Cómo gestionas tus contraseñas?	12,3	31,5	27,9	28,2	2,72
P9	B2	¿Tienes activada la verificación multifactor o MFA (dos o más factores para...	8,2	10,7	38,6	42,5	3,15
P10	B2	Recibes un SMS o mensaje de mensajería instantánea (WhatsApp, Telegram...)...	0,3	0,5	46,3	52,9	3,52
P11	B2	Recibes un mensaje (por redes sociales, WhatsApp o email) con una oportuni...	0,0	0,0	2,2	97,8	3,98
P12	B2	Cuando instalas una app y te pide permisos (cámara, micrófono, contactos, ub...	9,9	25,5	27,1	37,5	2,92
P13	B2	Estás en una wifi pública (cafetería, aeropuerto) y vas a entrar en tu banco...	1,6	1,9	1,9	94,5	3,89
P14	B2	¿Qué haces con las actualizaciones de tu móvil y tus apps?	3,8	12,1	33,2	51,0	3,31
P15	B3	¿Cómo se desbloquea tu móvil?	1,4	19,5	10,1	69,0	3,47
P16	B3	Cuando usas un ordenador que no es tuyo (trabajo, biblioteca, de un familiar...	0,8	5,5	37,0	56,7	3,50
P17	B3	Vas a publicar una foto de tus vacaciones. ¿Qué tienes en cuenta?	7,9	6,6	24,7	60,8	3,38
P18	B3	Si mañana pierdes el móvil o se rompe, ¿qué pasa con tus fotos y datos?	12,6	14,8	42,2	30,4	2,90
P19	B3	¿Sabes qué información tuya hay pública en internet (al buscar tu nombre, cu...	15,1	42,2	28,2	14,5	2,42
P20	B4	Si perdieras el acceso a tu correo principal, ¿podrías recuperarlo?	2,5	13,2	30,7	53,7	3,36
P21	B4	Cuando descargas una app, ¿desde dónde lo haces normalmente?	1,1	2,5	43,3	53,2	3,48
P22	B4	Recibes una llamada de alguien que dice ser tu banco o de soporte técnico qu...	0,0	0,8	21,4	77,8	3,77
P23	B4	Si alguien inesperado te llama o te escribe y en la conversación te pide un...	0,3	0,3	9,3	90,1	3,89
P24	B5	¿Sabías que el uso de internet (herramientas de IA, correos, streaming, nube...	4,1	27,4	49,6	18,9	2,83
P25	B5	Después de un buen rato en redes sociales, lo más habitual es que te sientas...	12,1	18,9	52,3	16,7	2,74
P26	B5	En tu relación con la tecnología, ¿quién manda?	3,0	12,1	56,7	28,2	3,10
P27	B5	¿Cómo los menores de edad de tu entorno más cercano tienen acceso habituale...	29,9	20,8	33,4	15,9	2,35

Elaboración propia a partir de las 365 respuestas del II Estudio de Bienestar Digital. Autoevaluación del Bienestar Digital. Cuestionario elaborado por Fernando Pena Vivero, Estefanía Cárcel Esteban y Juan Vicente Oltra Gutiérrez.

Anexo 3. Bibliografía y referencias

- Bandura, A. (1977). Social learning theory. Prentice-Hall.
- Cialdini, R. B. (1984). Influence: The psychology of persuasion. William Morrow. [Ed. cast.: Influencia. La psicología de la persuasión.]
- Davison, W. P. (1983). The third-person effect in communication. *Public Opinion Quarterly*, 47(1), 1–15.
- Duckworth, A. L., Gendler, T. S. y Gross, J. J. (2016). Situational strategies for self-control. *Perspectives on Psychological Science*, 11(1), 35–55. <https://doi.org/10.1177/1745691615623247>
- Ferster, C. B. y Skinner, B. F. (1957). Schedules of reinforcement. Appleton-Century-Crofts.
- Festinger, L. (1954). A theory of social comparison processes. *Human Relations*, 7(2), 117–140.
- Gollwitzer, P. M. (1999). Implementation intentions: Strong effects of simple plans. *American Psychologist*, 54(7), 493–503.
- Kahneman, D. (2011). Thinking, fast and slow. Farrar, Straus and Giroux. [Ed. cast.: Pensar rápido, pensar despacio. Debate, 2012.]
- Kroese, F. M., De Ridder, D. T. D., Evers, C. y Adriaanse, M. A. (2014). Bedtime procrastination: Introducing a new area of procrastination. *Frontiers in Psychology*, 5, 611. <https://doi.org/10.3389/fpsyg.2014.00611>
- Orben, A. y Przybylski, A. K. (2019). The association between adolescent well-being and digital technology use. *Nature Human Behaviour*, 3(2), 173–182.
- Prochaska, J. O. y DiClemente, C. C. (1983). Stages and processes of self-change of smoking: Toward an integrative model of change. *Journal of Consulting and Clinical Psychology*, 51(3), 390–395.
- Stanovich, K. E. y West, R. F. (2000). Individual differences in reasoning: Implications for the rationality debate? *Behavioral and Brain Sciences*, 23(5), 645–665.
- Verduyn, P., Ybarra, O., Résibois, M., Jonides, J. y Kross, E. (2017). Do social network sites enhance or undermine subjective well-being? A critical review. *Social Issues and Policy Review*, 11(1), 274–302. <https://doi.org/10.1111/sipr.12033>
- Weinstein, N. D. (1980). Unrealistic optimism about future life events. *Journal of Personality and Social Psychology*, 39(5), 806–820.
- Wood, W. y Neal, D. T. (2007). A new look at habits and the habit-goal interface. *Psychological Review*, 114(4), 843–863. <https://doi.org/10.1037/0033-295X.114.4.843>

Normativa y jurisprudencia

- 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 (NIS2). DOUE L 333, de 27 de diciembre de 2022.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. BOE núm. 294, de 6 de diciembre de 2018.
- Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera. BOE núm. 284, de 24 de noviembre de 2018.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD). DOUE L 119, de 4 de mayo de 2016.
- Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero (DORA). DOUE L 333, de 27 de diciembre de 2022.
- Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento del Marco Europeo de Identidad Digital (eIDAS 2). DOUE L, de 30 de abril de 2024.

Tribunal de Justicia de la Unión Europea. Sentencia de 13 de mayo de 2014, Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos y Mario Costeja González, asunto C-131/12.

Recursos institucionales

Agencia Española de Protección de Datos. Canal prioritario y ejercicio de derechos.

<https://www.aepd.es>

Banco de España. Portal del Cliente Bancario. Departamento de Conducta de Entidades.

<https://cliente bancario.bde.es>

Instituto Nacional de Ciberseguridad (INCIBE). Línea de Ayuda en Ciberseguridad, 017.

<https://www.incibe.es>

Instituto Nacional de Ciberseguridad (INCIBE). Oficina de Seguridad del Internauta (OSI).

<https://www.osi.es>