



INVESTIGACIÓN PÚBLICA · MODELO CUANTITATIVO · AGOSTO 2026

Contenido filtrado: consecuencias económicas y de seguridad

Informe orientativo para creadores que monetizan contenido por suscripción o venta

Resultado principal

No existe una tasa pública y universal que permita afirmar cuánto dinero pierde un creador por cada filtración. Este informe explica los posibles efectos económicos y de seguridad mediante evidencia agregada y ejemplos ficticios, sin calcular daños individuales ni utilizar información confidencial de personas reales.

ECONOMÍA

Impacto

Escenarios ilustrativos

SEGURIDAD

Riesgo

Suplantación y fraude

PRIVACIDAD

Mínimo

Datos agregados y ficticios

Preparado por Creator Privacy Check

Investigación y responsabilidad humana: Ricardo Narváez · Apoyo documental y metodológico: Ayerí Solari

Moers, Alemania · 27 de agosto de 2026

Qué puede explicar este informe de forma responsable

La filtración de contenido monetizado puede producir tres clases de daño: sustitución de ventas o suscripciones, costes de respuesta y pérdida derivada de suplantación o fraude. Esos efectos no ocurren siempre ni con la misma intensidad. La accesibilidad, la exclusividad, la repetición, la dependencia económica y la capacidad del contenido filtrado para sustituir una compra son determinantes.

Conclusiones

- No hay evidencia pública suficiente para fijar un porcentaje universal de pérdida específico para creadores por suscripción o venta directa.
- La literatura sobre música y cine confirma que existe desplazamiento, pero sus coeficientes varían ampliamente; trasladarlos sin ajustes a creadores sería metodológicamente incorrecto.
- Las cifras de fraude e impostores demuestran un riesgo económico real a escala agregada, pero no permiten atribuir automáticamente una pérdida a un creador concreto.
- El enfoque defendible es explicar dimensiones de riesgo y mostrar escenarios ficticios —prudente, central y severo— sin convertirlos en una valoración individual.
- La suplantación debe evaluarse como dimensión de seguridad separada, salvo que existan pérdidas observadas y documentadas.

Finalidad del informe

Esta es una pieza informativa y preventiva para comprender posibles consecuencias. No anuncia ni incorpora un servicio CPC de cálculo de pérdidas, peritación económica o valoración contable.

Alcance y límites

Este informe utiliza fuentes públicas, datos agregados y ejemplos ficticios. No analiza identidades, perfiles ni contenido de personas reales. Su marco orientativo ayuda a comprender factores de riesgo, pero no sustituye una valoración contable, jurídica o pericial ni se aplica para estimar el daño económico de un cliente.

Qué sabemos y qué no sabemos

Evidencia pública	Qué demuestra	Qué no permite afirmar
FTC · fraudes 2024	Las estafas de impostores generaron pérdidas declaradas por 2.950 millones USD; el fraude total declarado alcanzó 12.500 millones USD.	No mide pérdidas específicas de creadores ni atribuye el daño al contenido filtrado.
FTC · fraude iniciado en redes sociales	Desde 2021, una de cada cuatro personas que declaró perder dinero señaló que el fraude comenzó en redes sociales.	No convierte cada perfil expuesto en una víctima ni estima probabilidad individual.
FBI/IC3 · suplantación y toma de cuentas	La información pública y el material audiovisual pueden apoyar phishing, ingeniería social, clonación de voz y acceso a cuentas.	No ofrece un coeficiente monetario específico por creador.
EUIPO · infracción digital	La infracción persiste en múltiples categorías de contenido y los sitios infractores pueden monetizar tráfico y publicidad fraudulenta.	No incluye una muestra específica y representativa de creadores de suscripción.
Estudios económicos sobre música y cine	La copia no autorizada puede desplazar consumo pagado, pero el efecto cambia según contexto, producto, calidad, momento y consumidor.	No justifica usar una única tasa de sustitución en el sector creador.

Principio metodológico

El número de enlaces, copias o visualizaciones no equivale directamente a ventas perdidas. Una misma copia puede no desplazar ninguna compra, desplazar una parte de una compra o afectar a varias renovaciones. Por ello el modelo separa exposición, capacidad de sustitución y pérdida monetaria.

Regla de prudencia

Una métrica debe poder ser explicada, repetida y revisada. Si faltan datos, el resultado se declara «no estimado» en vez de rellenarlo con una cifra aparente.

Seis dimensiones que pueden agravar las consecuencias

Las siguientes dimensiones permiten entender por qué dos filtraciones pueden tener consecuencias muy diferentes. La escala de 0 a 5 se incluye únicamente para ilustrar intensidad relativa; no constituye una puntuación comercial, una probabilidad ni un porcentaje de ingresos perdidos.

Factor	Peso	Pregunta de control	0 → 5
E · Exposición	25 %	¿Cuánto contenido aparece y con qué recurrencia?	Ninguno → masivo/recurrente
A · Accesibilidad	20 %	¿Qué tan fácil es encontrar, abrir o redistribuir las copias?	Residual → inmediato/público
S · Sustituibilidad	20 %	¿La copia puede reemplazar razonablemente una compra o renovación?	Complementaria → sustituto cercano
D · Dependencia	15 %	¿Qué proporción de ingresos depende de ese contenido o canal?	Marginal → dominante
P · Persistencia	10 %	¿Hay réplicas, reaparición o múltiples dominios/canales?	Aislada → persistente
I · Suplantación	10 %	¿Facilita falsos perfiles, fraude, phishing o daño reputacional?	Sin señales → explotación activa

Lectura correcta

Una exposición extensa, fácil de encontrar, persistente y capaz de sustituir una compra merece mayor atención. Si además existen perfiles falsos o intentos de fraude, la seguridad debe tratarse de forma prioritaria y separada del posible impacto económico.

Intensidad orientativa	Lectura informativa	Posible prioridad
0–1	Señales inexistentes o muy limitadas	Documentar y mantener vigilancia básica.
2–3	Señales parciales o exposición moderada	Revisar canales, accesos y posibles vías de actuación.
4–5	Exposición extensa, persistente o explotación activa	Preservar evidencias y acudir a plataformas, organismos o especialistas adecuados.

Por qué una filtración puede afectar a los ingresos

Los siguientes elementos explican cómo podría construirse un escenario económico en términos generales. Se presentan con fines educativos, utilizando únicamente cifras ficticias. CPC no solicita ingresos, credenciales ni información bancaria para prestar sus servicios y no calcula pérdidas individuales.

Variable	Definición	Fuente
R30	Ingresos brutos hipotéticos del producto/canal en 30 días.	Dato ficticio usado para explicar el modelo.
B	Proporción hipotética vinculada al contenido expuesto.	Supuesto ilustrativo.
A	Accesibilidad: 0,25 residual; 0,50 media; 1,00 alta.	Hallazgos públicos documentados.
s	Sustitución de escenario: 5 %, 15 % o 30 %.	Hipótesis de estrés, no coeficiente sectorial.
C	Coste de respuesta: horas × valor/hora + gastos externos.	Tiempo y facturas observadas.
Ch	Pérdida por cancelación o caída de ventas medida antes/después.	Solo con serie real comparable.

Ejemplo conceptual

Exposición económica ilustrativa = $R30 \times B \times A \times s$

No representa una pérdida real ni un cálculo que CPC ofrezca a clientes.

Tres ejemplos ficticios

Caso	Supuestos	Prudente 5 %	Central 15 %	Severo 30 %
Bajo	$R30 \ 2.000 \text{ €} \cdot B \ 25 \% \cdot A \ 0,25$	6 €	19 €	38 €
Medio	$R30 \ 5.000 \text{ €} \cdot B \ 50 \% \cdot A \ 0,50$	63 €	188 €	375 €
Alto	$R30 \ 10.000 \text{ €} \cdot B \ 80 \% \cdot A \ 1,00$	400 €	1.200 €	2.400 €

Estos importes solo muestran cómo cambian los resultados al variar los supuestos. No representan expectativas para una persona real. La reputación y la suplantación no se convierten automáticamente en dinero; hacerlo sin datos observados duplicaría riesgos y generaría falsa precisión.

El daño no termina en la venta perdida

Una filtración puede aportar material para crear perfiles falsos, responder preguntas de verificación, ejecutar phishing, desviar seguidores, extorsionar o atacar cuentas. La fotografía, la voz, los alias y los patrones públicos pueden combinarse con datos obtenidos en otras fuentes.

Señal observable	Riesgo	Respuesta prioritaria
Perfiles duplicados o cuentas con nombres similares	Desvío de pagos, reputación y fraude a seguidores	Verificar identidad pública; reportar; conservar evidencias.
Mensajes que imitan tono, voz o imagen	Ingeniería social y estafa dirigida	Aviso público; palabra de seguridad; no confirmar datos por DM.
Intentos de recuperación de cuenta o SIM	Toma de cuenta	2FA con aplicación o llave; códigos de recuperación fuera de línea.
Enlaces falsos de pago o suscripción	Robo de dinero y credenciales	Publicar dominios/canales oficiales; monitorizar imitaciones.
Reaparición en múltiples sitios	Persistencia y amplificación	Registro por fecha/dominio; retirada priorizada; seguimiento.

Lectura separada de los riesgos

El posible impacto económico, la exposición de información y la suplantación deben explicarse por separado. Esta distinción evita presentar como dinero perdido un daño que todavía es una posibilidad y permite que el creador busque la ayuda adecuada según el problema observado.

Alerta ética

No publicar URL, alias sensibles, capturas explícitas ni detalles que faciliten nuevas búsquedas. El informe entregado al cliente debe usar acceso temporal y código único, conforme al proceso CPC.

Qué hace —y qué no hace— Creator Privacy Check

CPC sí realiza	Resultado para el cliente	CPC no realiza
Investiga exposición en fuentes digitales públicas y dentro del alcance autorizado.	Identificación de información posiblemente expuesta.	No accede a cuentas privadas ni solicita contraseñas.
Clasifica qué tipo de información aparece y dónde se encuentra.	Hallazgos organizados, comprensibles y documentados.	No redistribuye ni conserva el contenido investigado.
Explica posibles medidas que el cliente puede adoptar.	Recomendaciones prácticas vinculadas a los hallazgos.	No garantiza la retirada ni representa legalmente al cliente.
Señala plataformas, organismos o profesionales pertinentes.	Orientación sobre la vía adecuada para continuar.	No presta asesoramiento jurídico, contable ni pericial.
Entrega un informe privado mediante acceso temporal protegido.	Documento trazable con enlace y código único.	No calcula pérdidas económicas individuales.

Texto breve para Facebook

¿Qué consecuencias puede tener una filtración?

No existe una cifra universal: una copia no equivale automáticamente a una venta perdida. La accesibilidad, la persistencia, la capacidad de sustituir una compra, la dependencia económica y el posible uso para perfiles falsos influyen en las consecuencias. Creator Privacy Check investiga si existe información digital expuesta, qué tipo de información es y dónde aparece. Documentamos los hallazgos y explicamos posibles medidas o vías de ayuda, sin calcular pérdidas individuales ni convertir una posibilidad en una cifra aparente. La investigación se limita a fuentes públicas autorizadas; no solicitamos contraseñas ni almacenamos el contenido investigado en la web.

Llamada sugerida: «Conoce tu exposición antes de que se convierta en un problema económico o de identidad».

Del conocimiento general al caso concreto

Las medidas generales pueden reducir determinados riesgos, pero no permiten saber por sí solas si existe información expuesta, qué alcance tiene, dónde aparece ni si se está replicando. Esa respuesta requiere una investigación delimitada, verificación de coincidencias y documentación de los hallazgos.

Si necesitas conocer tu exposición digital real, Creator Privacy Check (CPC) puede investigar fuentes públicas autorizadas, identificar y clasificar los hallazgos y preparar un informe privado adaptado a tu caso.

Bibliografía principal

Federal Trade Commission (2025). *New FTC Data Show a Big Jump in Reported Losses to Fraud to \$12.5 Billion in 2024.* <https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024>

Federal Trade Commission (2024). *Consumer Sentinel Network Data Book 2024.* https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf

Federal Trade Commission (2023). *Social media: a golden goose for scammers.* <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers>

FBI Internet Crime Complaint Center (2024). *The Use of Social Engineering and Phishing to Circumvent Multi-Factor Authentication.* <https://www.ic3.gov/PSA/2024/PSA240411>

FBI Internet Crime Complaint Center (2024). *Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud.* <https://www.ic3.gov/PSA/2024/PSA241203>

EUIPO (2024). *Online Copyright Infringement in the European Union.* https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2024_online_copyright_infringement/2024_online_copyright_infringement_in_the_EU_FullR_en.pdf

EUIPO (2024). *Online advertising on IPR-infringing websites and apps.* <https://www.euipo.europa.eu/en/publications/online-advertising-on-ipr-infringing-websites-and-apps-2024>

Aguiar & Waldfogel, NBER (2015). *Streaming Reaches Flood Stage: Does Spotify Stimulate or Depress Music Sales?* <https://www.nber.org/papers/w21653>

Danaher, Smith & Telang, NBER (2013). *Piracy and Copyright Enforcement Mechanisms.* <https://www.nber.org/papers/w19150>

Poort et al. (2018). *Global Online Piracy Study / displacement estimates for films (SSRN record).* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2844167

UK National Cyber Security Centre. *Social media: how to use it safely.* <https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely>

Nota metodológica final

Consultas realizadas con fuentes públicas disponibles al 27 de agosto de 2026. Las cifras agregadas se conservan en su unidad y contexto originales. Los escenarios del 5 %, 15 % y 30 % son supuestos de estrés deliberadamente transparentes; no representan tasas observadas del sector de creadores. El modelo debe recalibrarse cuando CPC disponga de series anónimas suficientes y consentimiento válido para su uso estadístico.