



# HOJA INFORMATIVA

## PROYECTO DE REGLAMENTO SOBRE EVALUACIÓN DE RIESGOS



La Ley de Privacidad del Consumidor de California (CCPA por sus siglas en inglés) ordena a la Agencia establecer regulaciones que exijan que ciertas empresas realicen evaluaciones de riesgos. La Agencia ha redactado reglamentos de evaluación de riesgos, pero no ha iniciado el proceso formal de elaboración de normas. Esta hoja informativa explica las regulaciones provisionales para ayudar a las personas a comprender y participar en el proceso de elaboración de reglas. Estos proyectos de reglas *no* están vigentes y están sujetos a cambios.

### ¿QUIÉN necesitaría realizar una Evaluación de Riesgos?

Una “empresa” que deba cumplir con la CCPA<sup>1</sup> tendría que realizar una evaluación de riesgos antes de llevar a cabo cualquiera de las siguientes acciones:

- 1 Vender o compartir información personal de los consumidores.**
- 2 Recopilar, utilizar, divulgar, retener o procesar de otro modo los datos "sensibles" de los consumidores.<sup>2</sup>**
- 3 Utilizar tecnología de toma de decisiones automatizada (ADMT por sus siglas en inglés) para una “decisión importante” o para una “elaboración de perfiles exhaustiva”.**
  - “ADMT” es tecnología que toma decisiones, o en la que una persona confía para tomar una decisión (por ejemplo, una herramienta de selección de currículums que una empresa utiliza para determinar qué solicitantes contratará).
  - Decisiones significativas” son decisiones que tienen consecuencias importantes para los consumidores (por ejemplo, decisiones de proporcionar o negar servicios financieros, vivienda, seguros, oportunidades educativas o laborales, servicios de atención médica o bienes o servicios esenciales como comestibles, medicamentos o combustible).
  - La “elaboración de perfiles extensiva” incluye analizar la personalidad, los intereses, el comportamiento o la ubicación de los consumidores en su lugar de trabajo, en la escuela o en lugares públicos (por ejemplo, usar tecnología de reconocimiento facial en una tienda para identificar posibles ladrones) o para dirigirles anuncios.



RIESGO

4

#### Utilizar información personal para entrenar ADMT o inteligencia artificial (IA) que podría usarse:

- Para identificar personas (por ejemplo, tecnología de reconocimiento facial);
- Para identificación o elaboración de perfiles físicos o biológicos (por ejemplo, analizar las expresiones faciales o los gestos de las personas para inferir su estado emocional);
- Para tomar decisiones importantes;
- Generar deepfakes (por ejemplo, imágenes falsas de personas reales que se presentan como veraces o auténticas); o
- Operar modelos generativos.

## ¿QUÉ incluiría una evaluación de riesgos?

- La razón por lo que la empresa necesita realizar cualquiera de las actividades enumeradas anteriormente.
- Los tipos de información personal que la empresa recopilaría, usaría, divulgaría y conservaría para realizar la actividad.
- Cómo es que la empresa realizaría la actividad (por ejemplo, cuántos consumidores se verían afectados, qué les diría la empresa sobre el uso de su información personal, quién más podría estar involucrado, qué tecnología planea usar; y para ciertos usos de ADMT, cómo la empresa utilizaría el ADMT para tomar decisiones).
- Los beneficios y consecuencias para los consumidores asociados con dicha actividad y las protecciones que los planes comerciales implementarán.

- Los beneficios incluyen beneficios para la empresa, los consumidores, otras partes interesadas y el público.
- Las consecuencias para los consumidores podrían incluir, por ejemplo, el acceso no autorizado a su información personal, discriminación basada en características protegidas (por ejemplo, raza o género), no proporcionar suficiente información a los consumidores para que puedan comprender cómo se utilizaría su información personal o generar costos adicionales para consumidores.
- Ejemplos de protecciones incluyen cifrado y tecnologías que mejoran la privacidad. Las empresas que utilicen ADMT para tomar una decisión importante o elaborar un perfil extenso también tendrían que identificar si evaluó el ADMT para garantizar que funcionó según lo previsto, además de las garantías de precisión y no discriminación que planeaba poner en su lugar.





- Las personas de la empresa que contribuyeron, revisaron y aprobaron la evaluación de riesgos.
- Si la empresa iniciará la actividad.



**Nota: A una empresa no se le permitiría iniciar una actividad si los riesgos para la privacidad de los consumidores superaran los beneficios de la actividad.**

## ¿CUÁNDO tendría que realizar o actualizar una empresa una evaluación de riesgos?

Una empresa tendría que realizar una evaluación de riesgos antes de iniciar cualquiera de las actividades enumeradas anteriormente. También tendría que revisar (y actualizar si es necesario) sus evaluaciones de riesgos, al menos una vez cada tres años, para asegurarse de que sigan siendo correctas.

Si algo importante cambiara en cómo la empresa lleva a cabo dicha actividad (por ejemplo, si necesitaba recopilar información personal más confidencial), la empresa tendría que actualizar inmediatamente su evaluación de riesgos.



### ¿Cómo completaría una empresa su evaluación de riesgos si utilizara proveedores de servicio o contratistas para realizar la actividad?

El proveedor de servicios o el contratista de la empresa estaría obligado a proporcionar a la empresa la información necesaria para realizar la evaluación de riesgos. Una empresa podría obtener información de ellos como parte de su proceso de evaluación de riesgos.

## ¿QUÉ tendría que presentar un negocio a la Agencia, y CUÁNDO?

Una empresa tendría 24 meses para presentar a la Agencia: (1) una certificación de que realizó sus evaluaciones de riesgos según lo establecido en el proyecto de reglamento; y (2) evaluaciones de riesgos abreviadas.



### ¿Qué es una “evaluación de riesgos abreviada”?

Una evaluación de riesgos abreviada es una versión reducida de la evaluación de riesgos completa. Incluiría qué actividad desencadenó la evaluación de riesgos; por qué el negocio necesitaba hacer esa actividad; los tipos de información personal necesaria para la actividad y si incluyen información personal sensible; y las protecciones implementadas.



Después de su primera presentación, la empresa presentaría su certificación y cualquier evaluación de riesgos abreviada nueva o actualizada anualmente.

Si la Agencia o el Procurador General solicitaran una evaluación de riesgos íntegra de una empresa, la empresa tendría 10 días hábiles para proporcionarla.

### **¿Qué pasaría si una empresa realiza una evaluación de riesgos para que la misma actividad cumpliera con otras leyes? ¿Eso contaría para su evaluación de riesgos CCPA?**

Una empresa no tendría que rehacer la misma evaluación de riesgos. Sin embargo, si la evaluación de riesgos no cumpliera con todos los requisitos en las regulaciones provisionales, el negocio tendría que agregar lo necesario.

---

<sup>1</sup> La CCPA generalmente no se aplica a organizaciones sin fines de lucro o agencias gubernamentales. Para más información, ver "¿Mi empresa debe cumplir con la CCPA?" hoja informativa en <https://cppa.ca.gov/resources.html>.

<sup>2</sup> La información personal confidencial incluye cosas como números de Seguro Social, información financiera, geolocalización precisa, información de salud e información personal de los niños. Para obtener más información, consulte el Código Civil § 1798.140(ae); Borrador de actualización de las regulaciones existentes, marzo de 2023, en § 7001(ii), disponible en [https://cppa.ca.gov/meetings/materials/20240308\\_item4\\_draft\\_update.pdf](https://cppa.ca.gov/meetings/materials/20240308_item4_draft_update.pdf), (incluida la adición de "[p]or información personal de los consumidores que la empresa tiene conocimiento real es menor de 16 años" a la definición); y "¿Qué es la información personal?" hoja informativa, disponible en: <https://cppa.ca.gov/resources.html>.

Recursos de apoyo: Código Civil § 1798.185(a)(15)(B); Borrador del Reglamento sobre evaluación de riesgos y tecnología de toma de decisiones automatizada, marzo de 2024, disponible en [https://cppa.ca.gov/meetings/materials/20240308\\_item4\\_draft\\_risk.pdf](https://cppa.ca.gov/meetings/materials/20240308_item4_draft_risk.pdf).