HOJA INFORMATIVA

PROYECTO DE REGLAMENTO DE AUDITORÍA DE SEGURIDAD CIBERNÉTICA

CYBER

La Ley de Privacidad del Consumidor de California (CCPA por sus siglas en inglés) ordena a la Agencia establecer reglas que requieran que ciertas empresas completen auditorías anuales de ciberseguridad. La Agencia ha elaborado una auditoría de ciberseguridad, pero aún 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. Este proyecto de reglas *no* está vigente y está sujetos a cambios.

¿QUIÉN necesitaría completar una auditoría de ciberseguridad?

Cualquier "empresa" que deba cumplir con la CCPA[1] y cumpla cualquiera de los siguientes criterios:

1 La empresa obtuvo el 50% o más de sus ingresos anuales el año anterior a partir de la venta o distribución de la información personal de sus consumidores.

O

2 La empresa obtuvo más de $28 millones[2] en ingresos brutos anuales el año pasado **Y**

- Recopila, utiliza, divulga, retiene o procesa la información personal de 250.000 o más consumidores, **O**
- Recopila, utiliza, divulga, retiene o procesa la "información personal sensible" de 50.000 o más consumidores.

¿CÓMO completaría una empresa una auditoría de ciberseguridad?

1 Seleccione un auditor.

2 Proporcione toda la información que el auditor solicita y no oculte hechos importantes.

3 Presente los resultados de la auditoría a las personas de mayor rango en el negocio responsables de su programa de ciberseguridad.

4 Presente una certificación de finalización a la Agencia.

CYBER

¿QUIÉN podría ser el auditor y QUÉ tendría que hacer?

- El auditor deberá estar calificado, ser imparcial e independiente, y utilizar herramientas profesionales, procedimientos y normas de auditoría.
- El auditor podría ser alguien que trabaje en la empresa o fuera de ella. Si un auditor fuera interno, tendría que informar a la junta directiva, al órgano rector o al órgano rector de la empresa o ejecutivo de más alto cargo que no tiene responsabilidad directa sobre el programa de ciberseguridad.
- Ya sea que trabaje en el negocio o no, el auditor tendría que:
  - Determinar qué sistemas necesitarían ser auditados y cómo serían evaluados;
  - Revisar documentos, realizar pruebas y entrevistar a personas de manera independiente para respaldar los hallazgos de la auditoría; y
  - Certificar que completaron una auditoría independiente e imparcial.

¿QUÉ incluiría una auditoría de ciberseguridad?

- Una descripción de los sistemas que están siendo auditados.
- La información que el auditor utilizó para realizar decisiones y por qué apoyó sus hallazgos.
- Una evaluación de cómo la empresa protegió información personal a través de su programa de ciberseguridad.
- Una descripción de cómo la empresa siguió su propias políticas y procedimientos de ciberseguridad.
- Una descripción de las brechas y debilidades del programa de ciberseguridad y cómo el negocio planea abordarlos.
- Una descripción o ejemplo de las notificaciones de violación de datos que fueron enviadas a los consumidores o agencias, la información relacionada y las correcciones.
- Las fechas en que se revisó y presentó el programa de ciberseguridad al personal de mayor rango de la empresa responsables del programa de ciberseguridad.
- Una certificación de que la empresa no influyó en las decisiones o evaluaciones del auditor, y que la empresa revisó y comprendió los hallazgos de la auditoría.

Las formas comunes en que una empresa protege la información personal incluyen:

- Autenticación multifactorial
- Encriptación
- Gestión de cuentas y controles de acceso
- Inventario y gestión de la información personal y del sistema de información de la empresa
- Entrenamiento en ciberseguridad
- Respuesta a incidentes

CYBER

¿Cómo completaría un negocio una auditoría de ciberseguridad si utiliza proveedores de servicios o contratistas para proporcionar los servicios de ciberseguridad del negocio?

El proveedor de servicios o contratista del negocio estaría obligado a proporcionar al negocio la información necesaria para llevar a cabo la auditoría de ciberseguridad del negocio. El auditor del negocio podría obtener información de ellos como parte del proceso de auditoría de ciberseguridad del negocio.

¿CUÁNDO tendría que completar una empresa su auditoría de ciberseguridad?

Una empresa tendría 24 meses para completar su primera auditoría de ciberseguridad y presentar su certificación de finalización a la Agencia. Luego completaría una auditoría de ciberseguridad y presentaría una certificación anualmente.

¿Qué pasaría si una empresa completara una auditoría o evaluación de ciberseguridad para otro propósito, o tuviera una certificación de ciberseguridad? ¿Eso contaría para su auditoría anual de ciberseguridad de CCPA?

Una empresa no tendría que rehacer la misma auditoría de ciberseguridad. Sin embargo, si la auditoría, evaluación o certificación no cumple con todos los requisitos del proyecto de reglamento, las empresas tendrían que agregar necesario.

[1] 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.

[2] Incluye el incremento legalmente requerido para dar cuenta del incremento del Índice de Precios al Consumo. Ver borrador de actualización a las Regulaciones Existentes, marzo de 2023, en § 7005(b)(1), disponible en https://cppa.ca.gov/meetings/materials/20240308_item4_draft_update.pdf.

[3] 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 Actualizado de las regulaciones existentes, marzo de 2023, en § 7001(ii) (incluida la adición de “[p]or información personal de los consumidores que la empresa tiene conocimiento real tienen menos de 16 años de edad” según la definición), disponible en https://cppa.ca.gov/meetings/materials/20240308_item4_draft_update.pdf; y "¿Qué es la información personal?" hecho hoja, disponible en https://cppa.ca.gov/resources.html.

Recursos: Código Civil § 1798.185(a)(15)(A); Anteproyecto de Normatividad: Reglamento de Auditoría de Ciberseguridad, Diciembre de 2023, disponible en https://cppa.ca.gov/meetings/materials/20231208_agenda_item2a_cybersecurity_audit_regulations_clean.pdf.