ANDERSEN

Tips

Ley Orgánica para el Fortalecimiento de la Ciberseguridad

Mediante la publicación de la Ley Orgánica para el Fortalecimiento de la Ciberseguridad, se estableció un marco normativo orientado al fortalecimiento de la ciberseguridad nacional, la protección de los servicios esenciales y de la infraestructura crítica digital, así como a la prevención, gestión y respuesta frente a incidentes de seguridad informática.

Para la aplicación de esta normativa, sus disposiciones serán exigibles a i) las entidades del sector público relacionadas con la gestión de servicios esenciales o infraestructura crítica digital, ii) prestadores de servicios digitales respecto de los elementos bajo su esfera de control y a las iii) personas jurídicas privadas responsables de infraestructura crítica digital o vinculadas a la continuidad de servicios esenciales.

En este contexto, los prestadores de servicios digitales deberán implementar medidas técnicas y organizativas para garantizar la confidencialidad, integridad y disponibilidad de la infraestructura y los servicios provistos; realizar la evaluación y gestión de riesgos respecto de los componentes bajo su control; informar oportunamente sobre vulnerabilidades o incidentes que afecten los recursos contratados; cooperar en la gestión de incidentes; y establecer un punto de contacto técnico permanente con las entidades contratantes.

Adicionalmente, la ley dispone que la recepción, coordinación y seguimiento de los reportes de incidentes se realizará a través del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional), organismo que contará con autonomía técnica y operativa para ejecutar acciones de prevención, detección y respuesta. Los incidentes que afecten la confidencialidad, integridad o disponibilidad de activos digitales deberán notificarse dentro de las setenta y dos (72) horas siguientes a su detección.

Asimismo, se reconoce expresamente que las actividades de evaluación de vulnerabilidades, pruebas de penetración o hacking ético no constituirán infracción administrativa siempre que cuenten con autorización previa y escrita del titular, se ejecuten con fines de seguridad y sean realizadas por profesionales habilitados.

Por otro lado, la normativa incorpora un régimen administrativo sancionador para el incumplimiento de las obligaciones de ciberseguridad y clasifica las infracciones en leves, graves y muy graves. Las multas para servidores públicos oscilan entre uno (1) y cuarenta (40) salarios básicos unificados, mientras que para entidades privadas y empresas públicas podrán alcanzar entre el 0,1% y el 1,5% del volumen de negocio del ejercicio económico anterior, según la gravedad de la infracción.

La determinación de las sanciones deberá considerar criterios como la gravedad del daño o riesgo ocasionado, la reincidencia, la cooperación con la autoridad, la capacidad económica del infractor y la criticidad del servicio afectado. Cabe señalar que la Disposición Transitoria Segunda establece un régimen diferenciado para la aplicación de las sanciones, señalando que únicamente para sectores con órganos de control especializados y normativa previa en materia de riesgos y seguridad digital (por ejemplo, sector financiero y de telecomunicaciones) serán aplicables a partir de la vigencia de la ley.

Los procedimientos sancionadores se sustanciarán conforme al Código Orgánico Administrativo (COA). Adicionalmente, la ley establece un período de adecuación de veinticuatro (24) meses para los sectores que no cuenten con regulación previa en materia de ciberseguridad, durante el cual la fiscalización tendrá carácter preventivo y de acompañamiento técnico. El ente rector contará con doce (12) meses para expedir la normativa técnica necesaria para su implementación.

La ley entró en vigor a partir de su publicación en el Registro Oficial.