Actualización Legislativa
Proyecto de Ley Marco sobre Ciberseguridad e Infraestructura Crítica

Boletín Nº: 14847-06
Fecha sesión: 08 de noviembre de 2023

Comisión: Seguridad Ciudadana de la Cámara de Diputados
Etapa: Segundo trámite constitucional

Principales puntos de la discusión:

a. Se establecen los siguientes principios:
    1. Principio de control de daños.
    2. Principio de cooperación con la autoridad.
    3. Principio de coordinación según principios que rigen a la administración pública.
    4. Principio de seguridad en el ciberespacio.
    5. Principio de respuesta responsable.
    6. Principio de seguridad informática.
    7. Principio de racionalidad.
    8. Principio de seguridad y privacidad por defecto y desde el diseño.

b. La Agencia Nacional de Ciberseguridad tendrá la facultad de requerir a los organismos de la Administración del Estado y a las instituciones privadas calificadas como operadores de servicios esenciales, acceso a la información necesaria para prevenir la ocurrencia de incidentes de ciberseguridad o para gestionar uno que ya hubiera ocurrido.

c. Los operadores de servicios esenciales deberán contar con certificaciones de ciberseguridad que determine la Agencia mediante reglamento. En esta materia, la Agencia tendrá la facultad de homologar certificaciones técnicas internacionales o extranjeras en materia de ciberseguridad mediante resolución fundada de su director.

d. Se establece un plazo especial de 15 días para el ejercicio de los recursos aplicables de la Ley Nº 19.880.

e. Se establecen los requisitos para la realización de hacking ético. Estos son:
    1. Encontrarse inscrito en el registro que, al efecto, lleve la Agencia.
    2. Que el acceso se haya realizado habiendo informado previamente a la Agencia.
    3. Que el acceso y las vulnerabilidades detectadas hayan sido reportadas al responsable del sistema informático y a la Agencia tan pronto se hubiere realizado.
    4. Que el acceso no haya sido realizado con el ánimo de apoderarse o de usar la información contenida en el sistema informático, ni con intención fraudulenta. Tampoco se podrá haber actuado más allá de lo que era necesario para comprobar la existencia de una vulnerabilidad, ni utilizando métodos que pudieran conducir a denegación de servicios, a pruebas físicas, utilización de código malicioso, ingeniería social, y alteración, eliminación, exfiltración o destrucción de datos.
    5. No haber divulgado públicamente la información relativa a la potencial vulnerabilidad.
    6. Que se trate de un acceso a un sistema informático de los organismos de la Administración del Estado. En el resto de los casos, requerirá el consentimiento del responsable del sistema informático.
    7. Haber dado cumplimiento a las demás condiciones sobre comunicación responsable de vulnerabilidad que, al efecto, hubiere dictado la Agencia.

Próximamente: Se citará a una nueva sesión de la Comisión para votar las indicaciones faltantes. Una vez concluida la discusión en particular por parte de la Comisión, pasará a votarse el articulado en general en la Cámara de Diputados.

Documento elaborado por Christian Yepsen (cryepsen@uc.cl) y Sebastián Dueñas (sfduenas@uc.cl)
Programa de Derecho, Ciencia y Tecnología UC