LITORALPRESS

Fecha: 08-07-2024
Medio: Revista Logistec
Supl. : Revista Logistec
Tipo: Noticia general
Título: NUEVA LEY DE CIBERSEGURIDAD: UN AVANCE EN UN CAMINO DE DESAFÍOS.

Pág. : 56
Cm2: 434,1

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

SLEMAN ALCANTAR JADUE
HELPING COMPANIES TO BECOME DIGITAL AND SECURE.

NUEVA LEY DE CIBERSEGURIDAD: UN AVANCE EN UN CAMINO DE DESAFÍOS.

LA PROMULGACIÓN DE LA NUEVA LEY MARCO DE CIBERSEGURIDAD EN CHILE ES UN SALTO SIGNIFICATIVO CUANDO HABLAMOS DE PROTEGER LOS ACTIVOS DIGITALES, LOS CUALES NOS PERMITEN ADEMÁS RESGUARDAR DE MEJOR FORMA LOS OTROS ACTIVOS NO SIEMPRE CONSIDERADOS, TALES COMO LA REPUTACIÓN DE LA EMPRESA O, EN EL CASO DE LAS PERSONAS, SUS DATOS PERSONALES.

Para poder cumplir con la nueva reglamentación debemos conocer sus puntos más importantes. A modo de resumen, destacamos algunos de sus aspectos centrales:

1. La ley crea una institucionalidad ANCI, Agencia Nacional de Ciberseguridad, que estará encargada de los principios y la normativa que regirán las acciones de ciberseguridad de los órganos de la Administración del Estado y la relación entre éstos y los particulares.

2. La ley entrega a la ANCI la capacidad de gestionar las incidencias, establecer los requisitos mínimos para la prevención, contención, resolución y respuesta frente a los incidentes de ciberseguridad que se generen.

3. La ley entrega a la ANCI, la facultad de establecer DEBERES y SANCIONES. Establecer las atribuciones y obligaciones tanto de los órganos del Estado como de las instituciones privadas que posean infraestructura crítica de la información, estableciendo mecanismos de control y un sistema de infracciones y sanciones.

4. La Ley establece quienes estarán sujetos a la misma, se organizan en 2 grupos: los Sujetos Obligados y los Operadores de importancia vital. Es muy largo de explicar en detalle cada definición, lo cual espero poder ahondar en otra columna.

5. La ley establece multas que van desde las 5.000 UTM hasta las 40.000 UTM dependiendo de la gravedad y otros factores, entre los cuales destaca una de los mas importantes, la obligación de informar cualquier ataque o incidente de ciberseguridad, en un plazo máximo de 3 horas de ocurrido el incidente (o al menos de la toma de conocimiento del mismo), el no informar algún evento, desencadenará las multas. Lo utilidad de informar es generar una alerta al resto de los involucrados, de manera que en tiempo y forma tomen precauciones de los que está sucediendo y trabajando unidos nos defendemos de mejor forma.

Para comprender la necesidad de una ley como esta, es primordial entender el escenario que hemos vivido en Chile cuando hablamos de ataques de ciberseguridad y el impacto en el último tiempo. Primero, se debe considerar el impacto que ha tenido la creciente digitalización de los distintos servicios, la rapidez con que ha ocurrido y la extensión de su implementación en los negocios de todas las industrias. Esto ha ampliado la superficie expuesta en forma exponencial, lo cual le entrega mayor campo de acción a los Ciber-delincuentes.

Chile se encuentra en el 4° lugar de países en Latinoamérica más afectados por ciberataques durante el 2023 con 21 incidencias de Ransomware, superado sólo por Brasil, México y Argentina. (fuente Entel Digital). Los ataques más representativos incluyen ingeniería Social, Phishing, Malware y Ramsomware. El año 2023 Chile sufrió más de 700 mil Ciberataques, según un estudio de Cyber Threat Activity, Trellix; otros análisis hablan de más 2 millones de ataques, dependiendo de cómo se analicen y cuáles son las fuentes. Sin embargo, concentrándonos en lo importante, el sector Financiero/Bancario representa casi el 50% de dichos ataques, el 20% ocurre en el sector público y los 30% restantes ocurren en el resto de las industrias.

Es necesario precisar que un ataque NO SIEMPRE ni necesariamente tiene como finalidad obtener recompensas monetarias, aun siendo los más frecuentes, hay que tener claro que los ataques también tienen intencionalidad de distinta naturaleza, como puede ser afectar reputación de una empresa, detener un servicio, provocar una caída de sistemas o simplemente vanagloriarse de tener la capacidad de ejecutar un ataque más simbólico que dañino. Otro punto importante de tener en cuenta, que no siempre se visibiliza, es considerar que las "ganancias" se estiman en varias decenas de trillones de dólares anuales, tranquilamente podríamos pensar que estamos frente a toda una industria del Ciber-crimen.