



Delitos informáticos y compliance corporativo

La creación o la tipificación de nuevos delitos informáticos que se está concretando en Chile implica, en esencia, que determinadas conductas contra la data de sistemas, servidores y redes, siempre dolosas e intencionales, serán sancionadas penalmente o con penas privativas de libertad. Si, además, se establece en la ley sobre responsabilidad penal de las empresas la necesidad de ser ellas diligentes, en la prevención corporativa de su comisión y para evitarse riesgos legales y reputacionales, el aporte será doble.

Dejando de lado la amenaza de sanciones o reproche jurídico al delincuente que los cometa —sea un empleado o un funcionario interno, sea un agente externo que accesa los sistemas—, la consecuencia importante para los sistemas de gestión de la información (SGSI), de empresas y servicios públicos es la necesidad de ser diligentes en su prevención. Esa diligencia a una empresa se la exigirán sus accionistas, y a un servicio público los ciudadanos, pero fundados en normas y responsabilidades diversas, con lo cual, la base jurídica para prevenir o precaver formalmente en los ámbitos del cumplimiento normativo no es la misma.

El objetivo esencial es exigir pre-constituir diligencia, prevenir de la mejor manera posible e invirtiendo los recursos necesarios en proporción a la envergadura de los sistemas, donde implementar monitoreos externos ante la radical conectividad vía redes de la gestión moderna será tan esencial como mantener corriendo programas antivirus. No es simple “customizar” estándares de gestión segura como las ISO 27001 -controles incluídos si la realidad de la criminalidad informática es desconocida o mal ponderada. Así, por ejemplo, seguir responsabilizando a los bancos por la suplantación en el uso de los sistemas de autenticación mediando fraude a los clientes del banco —eso es el phishing- cuestiona dominios de seguridad que nunca podrán ser controlados, al ser externos a la entidad, también engañada y víctima del delito. No es simple tampoco preparar planes de cumplimiento normativo si primero no se conoce cuál es la real contingencia que se generará ante un delito informático, sus perjuicios probables o esperables y que además puede cometerse en forma sostenida en el tiempo. En ambos ámbitos, de SGSI y de compliance, nada puede hacerse si la empresa o el servicio público no han determinado cuál es su información crítica.

Además, puestos en el terreno de establecer modelos y programas de cumplimiento normativo y preventivo, analizándose los riesgos inherentes al procesamiento “de empresas” que tratan la información con fines de lucro, las acciones idóneas para prevenir riesgos y evitar los daños reputacionales, y los derivados del incumplimiento de normas legales y directrices internas, no obedecen a la misma lógica de lo que debe hacer un servicio público, siempre con menos recursos y presupuestos.

La interrogante correcta será entonces preguntarse si hubo o no prevención, conforme a la normativa vigente. Con estos parámetros, técnicos y jurídicos, puede abordarse con objetividad y sin demagogia el análisis de casos como el hackeo o acceso indebido al Banco de Chile, el ransomware que afectó al Banco del Estado o el hackeo de que fue víctima la base de datos de claves únicas gestionada por el Estado, y existen las normas legales vigentes para ello.

