Spread the love

A medida que se multiplican los ciberataques a empresas, y que los efectos de tales incidentes son más graves, la reflexión relativa a los ciber-incidentes es más intensa. Van surgiendo sugerencias y recomendaciones expertas relativas prácticas corporativas internas y externas (respecto de proveedores, clientes, y otros con quienes interrelacionan en el curso de su actividad)

NYC_by Jara IPM

- **Desde el punto de vista de las relaciones de las empresas con terceros,** se han sugerido ya algunas orientaciones tendentes a minimizar los riesgos derivados del entorno digital. Entre ellas, la **revisión de sus prácticas contractuales para adaptar las definiciones y alcance de las exclusiones de responsabilidad pactadas**. Estas prácticas son especialmente relevantes en sectores como el del transporte de viajeros. ; o en las empresas de transporte y distribución energética, por mencionar algunos de los que recientemente han sufrido grandes pérdidas, o han visto su actividad totalmente paralizada como consecuencia de ciberataques (sirva de ejemplo el ataque a *Colonial Pipeline,* y los eventos de 6 de mayo de 2021). También son importantes para la gestión pública de infraestructuras y servicios que, al igual que el sector privado, han sufrido importantes ataques cibernéticos (véase los que afectaron a varias ciudades de Texas en 2019).

- Otro conjunto de prácticas recomendadas para la prevención de riesgos cibernéticos consiste en la **contratación, mantenimiento y actualización de seguros contra ciberriesgos** cuyo alcance y coberturas pueden variar sustancialmente. Pueden cubrir gran variedad de riesgos como la seguridad de elementos físicos susceptibles de recibir daños materiales fruto de una intervención ilícita en los sistemas digitales de la empresa; daños derivados de pérdidas de datos (y los relativos a los gastos necesarios para recuperarlos), pasando por la contratación de expertos que van desde la recuperación de datos electrónicos hasta el análisis experto del ataque, y la defensa en el caso (probable) de que se interpongan litigios contra el asegurado después de un ciberataque, o que éste decida interponerlos. Hoy, las prácticas comerciales prudentes hacen que la contratación de seguros contra ciber-riesgos sea fundamental, hasta el punto de que la ausencia de esta cobertura puede, en si misma dar lugar a acusaciones de falta de diligencia por parte de los administradores.

NYC_by Jara IPM. One Trade Center Tower

- Continuando en esta enumeración, la **contratación de expertos externos especializados en la prevención y control de los ciberataques se considera una buena práctica.** Los especialistas en ciberseguridad desempeñan un papel importante para minimizar la exposición, para detectar y supervisar los riesgos así como para establecer protocolos de seguridad de la infraestructura de información de una empresa. Como buena práctica, la contratación de estos expertos es también interesante como defensa en caso de litigio derivado de un ciberataque, en el sentido de que la empresa afectada puede aportar, a su favor, que sus protocolos estaban supervisados por expertos.

- No es menos relevante, que la entidad cuente con **profesionales cualificados en su seno** como el CISO –*Chief Information Security Officer*- o el CSO, *Chief Security Officer* , o el CIO *Chief information Officer*, figuras que se van introduciendo en la práctica, en los estándares de seguridad como NIST o ISO, y van penetrando el ámbito normativo positivo. En este sentido, recordamos algunas entradas anteriores en este blog, como la relativa al Responsable de Información (exigido a las administraciones conforme al Esquema Nacional de Seguridad y también a ciertas empresas que contratan con la administración), que debe ser una figura distinta del Responsable de Seguridad y también del Responsable del Servicio en los términos del Real Decreto 3/2010. O el Responsable de Seguridad de la Información en los Operadores de Servicios esenciales, conforme al Real Decreto 41/2021) Como ya anunciábamos, estas figuras de altos ejecutivos se van haciendo habituales en la práctica y han sido reforzadas mediante su inclusión en estándares de ciberseguridad como los NIST e ISO (familia 2700), y en recomendaciones de los CERN nacionales.