

Obliga digitalización a elevar seguridad (Reforma 18/05/18)

Obliga digitalización a elevar seguridad (Reforma 18/05/18) Ulises Díaz Cd. de México (18 mayo 2018).- Los protocolos de seguridad y protección para industrias y Gobiernos no han crecido a la par que la permeación de la digitalización y el Internet de las Cosas, lo cual está multiplicando el riesgo de una catástrofe si no se crean mecanismos de protección adecuados, según el Foro Económico Mundial (WEF, por sus siglas en inglés). El reporte "El Internet de las Cosas Industrial: un protocolo de seguridad" da varios ejemplos de ataques cibernéticos, como el secuestro de infraestructura digital que ocurrió en Ucrania, donde el Gobierno de ese país tuvo que pagar millones para permitir que se pudiera acceder a los sistemas de control de aeropuertos, vías férreas, estaciones energéticas y otros controles de infraestructura. En México, si bien no se menciona en este documento, casos similares han ocurrido con el sistema de pagos interbancarios del Banco de México, así como intentos por robar la base de datos del Instituto Nacional Electoral (INE) e información de la Secretaría Nacional de la Defensa (Sedena). El WEF menciona que el diseño de una estrategia tiene que hacerse a través de múltiples niveles, que van desde los fabricantes de equipos y programas, pasando por proveedores de redes y servicios de almacenamiento en la nube y hasta los operadores directos, lo cual complica el diseño de estrategias. "Es necesario crear un sistema que reduzca la posibilidad de riesgo, por lo cual es necesario que se cree un protocolo general que cubra los puntos más generales y después se refuercen los detalles a partir de necesidades específicas", dice el documento. La urgencia del WEF viene a partir de que en la economía global, para 2030, la digitalización podría hacer que la producción se incrementara en 14.2 mil millones de dólares, lo cual significaría que este factor se convertiría en el principal motor de productividad y crecimiento en la siguiente década. Sin embargo, si no se toman las precauciones adecuadas para asegurar esta infraestructura, los cada vez más crecientes riesgos asociados con el ciberespacio dejan vulnerable esta oportunidad de mejora para la producción y la generación de crecimiento y bienestar. "Un protocolo de seguridad no puede ser controlado específicamente por ningún participante, ni hay una categoría discernible de actores que deben estar encargados específicamente de la gobernanza. "Cuando la posibilidad del riesgo está tan extendida, la seguridad preventiva y operativa no puede ser confinada a un sólo factor sino que tiene que ser entendida a través de una aproximación colectiva con obligaciones mutuas", dice el reporte.