TODO TIPO DE INFORMACIÓN EN LA WEB NECESITA DE CIBERSEGURIDAD

Dr. Roberto Morales Estrella
Profesor Investigador de la UAEH

17 Julio de 2023

La ciberseguridad cada vez tiene más relevancia en la nueva economía científico-tecnológica. De todos es sabido que vivimos una sociedad en acelerada transformación, los procesos históricos anteriores, se registraban con mayor lentitud, pero hoy los escalamientos son a mayor velocidad y profundidad, por la intensidad del desarrollo tecnológico, los comportamientos de la sociedad en general, han pasado de ser procesos evolutivos a mutaciones aceleradas.

La ciberseguridad nace con el internet y con las plataformas tecnológico-virtuales, teniendo como antecedente la red ARPANET, construida por la Agencia de Proyectos Avanzados del Pentágono de los EEUU; en la medida que éstas plataformas y la multiplicidad de sus aplicaciones, escalan su transformación, también los ciber-delincuentes perfeccionan sus tecnologías, siendo las más frecuentes el ramsomware y el malware, como el llamado phising; a través de las cuales secuestran o sustraen información, la cual venden en el mercado negro, y/o piden rescate.

Los ciberataques a las actividades industriales se multiplicaron, sobre todo después de la pandemia, por lo que la ciberseguridad, es ya una prioridad en todo tipo de organización, sin que sea la excepción el nivel individual; la sociedad actual está estructurada, en torno a una oposición bipolar, entre la red del internet y el yo, como lo precisó Manuel Castells, en su Prologo de la Red y el Yo (Manuel, 2023), por ello la ciberseguridad es fundamental en nuestra vida.

Según el INEGI (, INEGI, 2023, págs. 1-2), por acoso cibernético o ciberacoso se entiende “como un acto intencionado, ya sea por parte de un individuo o un grupo, teniendo como fin el dañar o molestar a una persona mediante el uso de tecnologías de información y comunicación, en especifico, el internet”

Las cifras de INEGI identifican a 105 millones de personas de 12 años y más como usuarios de internet en 2022, el 79% de esa población utilizó internet en cualquier tipo de dispositivo móvil o fijo, correspondiendo el 44% de mujeres; el 20.8% de esa población de 12 años y más a nivel nacional, fueron víctimas de ciberacoso en 2022, por entidad federativa correspondió al Estado de Hidalgo el 23.5% superior a la media nac
ional.

Las medidas de seguridad que se aplicaron por parte de los usuarios, son las contraseñas como las claves, huellas digitales y patrones de desbloqueo, pero no han sido suficientes.

Para Yuval Noah Harari (Harari, 2017, págs. 400-431) "el Dataísmo sostiene que el universo consiste en flujos de datos, y que el valor de cualquier fenómeno o entidad, está determinado por su contribución al procesamiento de datos". El riesgo de la información como paradigma, también lo plantea Noah Harari, cuando describe que la humanidad, en el siglo XVIII, pasó de una visión teocéntrica, basada en los algoritmos bioquímicos (imaginación), a una visión homocéntrica, al considerar que el único conocimiento verdadero es el científico, pero en el siglo XXI el Dataísmo podría dejar de lado a los humanos, al pasar de una visión homocéntrica a una visión datacéntrica.

Por la acelerada digitalización, todo individuo, familia, organización pública y privada, y sectores productivos, como comerciales, que digitalizan sus procesos y actividades, participan interactivamente en la dimensión virtual del ciberespacio, que se intensificará cada vez más con otros espacios como el metaverso, dando lugar al surgimiento de tres tipos de mercado: el de bienes y servicios; el de la información, incrementándose a ritmo de cada click, y trasmitiéndose a la velocidad de la imaginación; finalmente está el mercado negro de los datos, cuyos actores son los ciber-delincuentes o hackers, el Dark web (Steve, 2022) mueve recursos por 8 billones dd.

El Foro Económico de Davos planteó en su informe Global Cybersecurity Outlook 2022 (, World Economic Forum, 2022) pasar de la ciberseguridad a la ciber-resiliencia, que contempla la formación de capital humano especializado, desarrollar y aplicar nuevas tecnologías, asegurando la protección de la información.

La ciberseguridad no solo son metodologías y herramientas tecnológicas, que eviten y/o mitiguen el riesgo de ciberataques, constituye un factor fundamental para la estrategia operativa, tanto de empresas, como de gobiernos, en tal dimensión la ciberseguridad requiere de tres componentes estratégicos: el legal, el tecnológico, pero sobre todo el éti
co.