




# LA IMPORTANCIA ESTRATÉGICA DE LA CIBERSEGURIDAD

Dr. Roberto Morales Estrella  
Profesor Investigador de la  
UAeh

05 Junio de 2023



El presente texto es un adelanto, de un trabajo más profundo, sobre un tema que 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.

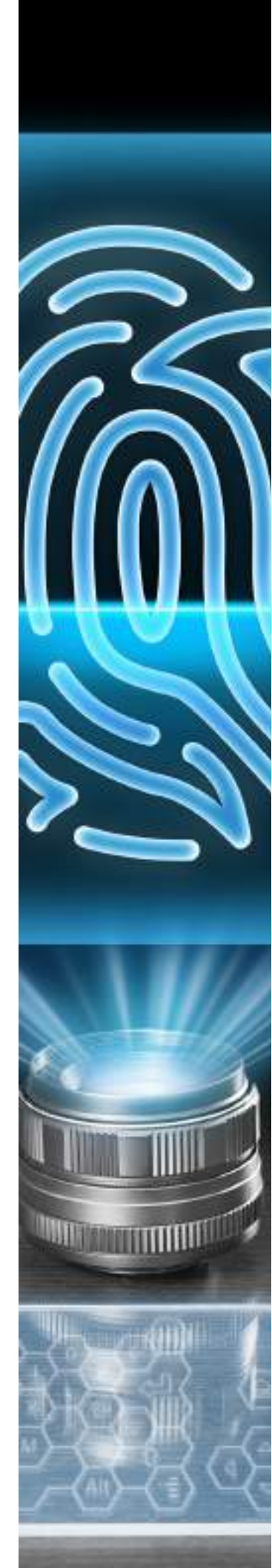
La ciberseguridad nace con el internet y con las plataformas tecnológico-virtuales, teniendo como antecedente la red ARPANET, construida por la Agencia de Proyectos Avanzados del Pentágono de los EEUU; en la medida que éstas plataformas y la multiplicidad de sus aplicaciones, escalan su transformación,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

De los 156 mil millones de ciberataques registrados en Latinoamérica, en el primer semestre del 2022, el 51% corresponden a México, 5 mil 862, son ataques a pequeñas y medianas empresas, ubicándonos en el 2º lugar.

El impacto en 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, incluyendo el nivel individual, dada su transversalidad; en sociedades como la nuestra que están estructuradas, en torno a una oposición bipolar entre la red del internet y el yo, como lo precisó Manuel Castells (2000, citado en su prólogo); por ello la ciberseguridad es fundamental en nuestra vida.

El acelerado proceso de digitalización tecnológica, ha venido abarcando cada vez más actividades empresariales, gubernamentales y de la sociedad, dando lugar al surgimiento de tres tipos de mercado: uno centrado en el intercambio de productos y servicios, que incluyen la educación y la necesaria formación de una masa crítica de expertos en el manejo, comprensión y creación de nuevas herramientas tecnológicas, como extensión de los resultados logrados, en los procesos de I+D+i; el otro mercado es el de la información, cuya generación es a ritmo de cada click, como su trasmisión a la velocidad de la imaginación, entorno a este mercado de información, está el mercado negro de los datos, cuyos actores son los ciberdelincuentes o hackers.





El cibercrimen crece al ritmo de los clicks, que hacen posible las interacciones y el flujo constante de grandes volúmenes de información de manera ilegal. Los ataques cibernéticos, representarán un valor de mercado (Mckinsey 2023) de más de 10 billones de dólares para el 2025.

Para contrarrestar los ciberataques, se estima que las empresas, han erogado 150 mil millones de dólares, sin embargo los ciberdelincuentes surgen como hongos, en esta era hiperconectada del 5G y del 6G; los ciberdelincuentes son tan numerosos como ocultos para la mayoría, los más peligrosos nunca son atrapados, o sea que la impunidad es un factor que prevalece, dada su creciente destreza biotecnológica.

Trascendió en una publicación de AVG.com ( J. Regan, e I. Belcic 2022) que entre los hackers mas famosos estan: Ellion Guton, quien a los 16 años se le sorprendió hackeando a la empresa TalkTalk; otro detectado es Evgeni Milkhailovich Bogachev, quien generó una red de bots (GameOver Zeus) infectando con ransomware, a millones de ordenadores en todo el mundo, las autoridades de los EEUU y de otras naciones, están ofreciendo 3 mdd como recompensa para localizarlo.

Existen otros miles más, que buscan la forma de realizar ciberataques depredando empresas y organizaciones públicas, México no ha sido la excepción.

También hay empresas especializadas en ciberseguridad, existen más de 200 en nuestro país (R. Contreras 2023), su función principal es dar soluciones de ciberseguridad, garantizando la integridad de los sistemas de información y la confidencialidad de los datos. Los más conocidos son: hola. Innovación; ESET; Akamai; OneseQ; GMV; Hornet Security y Kaspersky entre otros tantos.

La ciberseguridad no solo son metodologías y herramientas tecnológicas, que eviten y/o mitiguen el riesgo de ciberataques, es un factor fundamental para la estrategia operativa, tanto de empresas como de gobiernos, en tal dimensión requiere un componente ético y legal.