La alfabetización digital y ciberseguridad ante la vulnerabilidad empresarial

"Cada modelo de negocios y cada industria será transformada"

− Klaus Schwab en el Foro Económico Mundial
Davos-discurso

Nadie pudo haber previsto la magnitud de las circunstancias que nos dejó el pasado año con la crisis sanitaria ocasionada por el SARVS-COV 2 que lamentablemente ha ido evolucionando, pero ¿Será el único que deba evolucionar? Dentro del efecto domino que contrajo y afectó tanto a las piezas globales de economía, sociedad, salud, derechos humanos y claro seguridad internacional.

Se ha aprendido ya sea por vía voluntaria o forzada el significado de resiliencia de cada actor y sujeto dentro del escenario internacional entonces como objetivo se visualiza: Potenciar los pilares tanto de alfabetización digital como ciberseguridad a fin de apostar por una estrategia de pivotaje ante los retos que conlleva la transición a la era digital de manera que seamos conscientes y hábiles como ciudadanos y corporativo para manejar las virtudes digitales a nuestro favor.

Esta transición abrupta al mundo digital trajo consigo a relucir las deficiencias que se venían arrastrando, así como los nuevos retos que deben enfrentarse –se explicará a detalle en los párrafos siguientes-. Por lo que me remite abordar dentro del campo de las habilidades directivas que, cuando se establece un objetivo de desarrollo debe fomentar el desenvolvimiento de la inteligencia. Me refiero a inteligencia como la manera de comportarse del ejecutivo y/o equipo empresarial en diversas situaciones, cómo hacer versátil el manejo de su *status quo.*

De acuerdo al profesor José Arrioja de la Facultad de Contaduría y Administración- UNAM, expositor de una *masterclass* afirma que "El verdadero examen de inteligencia no es qué tanto sabemos sino, ¿Cómo nos comportamos cuando no sabemos qué hacer y cómo hacemos y respondemos ante determinadas situaciones? Ese, es el verdadero reto y objetivo" de manera que

la cuestión aquí es que, de los tiempos de necesidad, de los tiempos de crisis surge la oportunidad para aquellos quienes está dispuestos a romper con el paradigma y ser creativos para implementar estrategias de pivotaje a pesar de los retos.

Con esta base se abordará bajo las líneas de la alfabetización digital y ciberseguridad ante la vulnerabilidad empresarial actual a través del método de un estudio de caso bajo las directrices de exponer hechos, problemas y abordar soluciones.

Hechos:

- Globalmente nos encontramos bajo la transición de la Tercera Revolución Industrial hacia la Cuarta Revolución Industrial –incluso en algunos países se puede hablar ya de una Quinta Revolución Industrial- y reafirmando lo dicho por Klaus Schwab la reconfiguración de modelos de negocios es una verdad inherente y cada vez más tangible.
- La crisis sanitaria condujo a un estado de incertidumbre donde en el sector económico comenzó a manifestar los efectos implícitos, tales como los niveles de producción bajaron y el aislamiento perjudicó la oferta bajo el método tradicional de compra.
- Mientras que se multiplicó el comercio electrónico. Vamos desde lo simple, durante la pandemia varios negocios incidentalmente empezaron a digitalizarse al ofrecer sus productos a través de mensajería instantánea y redes online.
- Incrementó el ocio digital: Las plataformas de *video-streaming* por ejemplo, de acuerdo a los datos del *Statista en* una estimación de datos generados en un minuto: *Netflix* hay 28, 000 suscriptores viendo contenido, en *Instagram* 695, 000 *stories* compartidas, *WhatsApp/Messenger* 69,000 mensajes enviados, en *Tik tok 5, 000* descargas hechas y por último *YouTube* 500 horas de videos subidos.
- Así como la dinámica de la teleducación y el teletrabajo también llamado *home office.*

Problemas:

- El dilema de la accesibilidad es el clímax de esta historia si bien está al uso de gobiernos, empresas o cualquier buen ciudadano también se encuentra a merced del crimen organizado, *hackers*, pedófilos o terroristas.

- Que va desde colocar un hardware encima de los cajeros automáticos, vulnerabilización de cuentas, manipulación de masas a través de las *fakes news*, drogas virtuales-auditivas, cuentas *bitcoin* usadas por criminales, delincuencia informática organizada o incluso ciberterrorismo.
- Ahora desde la óptica empresarial, ¿El cibercrimen sólo afecta a las grandes corporaciones o también a las PyMES? La respuesta es que cualquier organización puede ser un blanco de un ciberataque. 4/10 empresas fueron víctimas de un ciberataque. De acuerdo a las afirmaciones tanto por Cesar González experto en financiación y sostenibilidad del BBVA como por Roberto Martínez analista senior de seguridad del equipo global de investigación y análisis, *Kaspersky.*
- ¿Cuáles son las principales fuentes de ataques? De acuerdo a la Encuesta Global de Seguridad de la Información 2020, existen cinco categorías:

    a) Agentes externos: Grupos del crimen organizado de tinte político
    b) Agentes externos: Organizaciones hacktivistas de tinte económico
    c) *Insiders* (debilidades de factor humano) sin motivación maliciosa
    d) Lobos solitarios
    e) *Insiders* con dolo malicioso

- Ahora hablando sobre la categoría del teletrabajo dentro de éste se propiciaron nuevos riesgos: La transición que se hizo de trabajar en una oficina a un trabajar en casa afirma Felix Barrios director del HUB de ciberseguridad del TEC de Monterrey “tres de cuatro empleados de la organización no recibieron ningún tipo de información de cómo proteger la información”. Al llevarse a sus equipos domésticos la información de las organizaciones y no contar con la protección para *malwares* -por mencionar un ejemplo- y en consecuencia infectar las redes corporativas. Relevante por qué, ¿Qué implica una fuga de datos? 1. Acceder a las bases de clientes y 2. Exponer y comprometer a terceros.
- ¿Qué tipos de ataques son los más conocidos? El que debe destacarse es vía la extracción de datos, el denominado *ransomware.* Este es, un *software* que encripta los datos de los

servidores y a cambio pide dinero -normalmente *bitcoins*-. Por infortunio ha evolucionado y hay diferentes formas de ataque e inclusive dentro del *ransomware,* hay diferentes variantes. De hecho, te das cuenta que la empresa ya fue comprometida, meses antes y el *ransomware* fue la etapa final.

- Entra en escena el doble factor de presión porque uno se deja encriptado los datos de la empresa (dado que, a pesar de pagar el rescate, no garantiza que se te desncripte además propicia que se aliente este tipo de actos) y dos publicar o subastar por internet al mejor postor la base de dato de la empresa.

Soluciones:

A causa de este escenario tanto de hechos como de retos, la razón de ser es apostar por estrategias de pivotaje. Es el motivo del cambio de modelos de negocios a fin de potenciar las virtudes digitales a nuestro favor, del mismo modo conocer que existen riesgos y vulnerabilidades por hacer frente y la ciberseguridad comienza a cobrar relevancia.

Tanto por la especialista en Derecho informático, Alejandra Morán como por Félix Barrios, director del *hub* de ciberseguridad del TEC de Monterrey: la ciberseguridad será determinada en función de qué y de a quién se quiera proteger. Así que son dos pilares que deben potenciarse: la alfabetización y la ciberseguridad dado que se complementan mutuamente.

Como paso inicial sería un error suponer que para proteger mi empresa lo primero y absoluto es comprar el plan de ciberdefensa más costoso. A veces se puede invertir en tecnología de alta gama pero al final significa un gasto y no una inversión por no saber utilizarla. El analista *senior* de seguridad del equipo global de inversiones, Roberto Martínez afirma que la mejor forma de atacar un cibercrimen antes de acudir a servicios profesionales y creer que la seguridad se logra instalando programas, lo más importante es hacer un análisis de riesgos y una autoevaluación. Por lo que como primeros pasos se sugiere:

- Contar y proveer de un nivel de conocimiento suficiente y de capacitación a todos.

- Elevar la ciberseguridad como un tema de negocio y no exclusivo de auditoría o del departamento del control interno.
- Hemos dicho en función a lo que se quiere proteger, los factores clave son: Tamaño de la organización, los tipos de activos que maneja. Para ir más allá de la continuidad del negocio, lograr identificar el punto comprometido dado no hay una certeza si sólo se deja pasar.
- Dentro del ABC de la ciberseguridad son imprescindibles la gestión de contraseñas de accesos, política de capacitación, sistemas de anti-virus y por supuesto respaldos en infraestructura diferente, debe ser más de uno.
- Evaluar qué tipo de ciberataques hay alrededor de la categoría de mi negocio.
- Entonces ahora sí podemos hablar sobre tecnología de alta gama que puede funcionar como herramienta potencial a nuestro favor. Así es invertir en inteligencia artificial, específicamente inteligencia de amenazas. En plataformas de analítica avanzada centrada en ciberseguridad a fin de detectar, prevenir y mejorar procesos operativos. Tal es el caso de la innovadora *Google-cloud* por ejemplo, las empresas y bancas financieras están apostando por esta alianza a fin de mejorar su posicionamiento y por supuesto su estrategia de ciberseguridad con el uso de la inteligencia artificial a su disposición.
- Invertir en el llamado *blockchain* que si es bien dirigido tiene muchas virtudes. Interesante porque es una tecnología financiera basado en la encriptación de información codificada sobre una transacción en la red. Puede ser usada para crear una identidad universal que permita el acceso de servicios básicos, hacer las transferencias de dinero más rápidas, directas y a un costo menor.

El punto crucial no es volverte un experto sino un usuario consciente y corresponsable además de fomentarlo en tu equipo de trabajo. Haciendo honor a las palabras de la especialista Morán que fueron, son y serán un aguijón para mí: “Se exhorta a seguir aprendiendo, porque siempre hay que aprender y beneficiarse porque es una herramienta y del mismo modo crear una conciencia porque es una responsabilidad social, legal y profesional”.

Fuentes de consulta:

- Arriojo, J (2020, 12 noviembre) *masterclass Método de estudio de caso*- FCA/FES Aragón
- Blanco, J *Google cloud incorpora la inteligencia artificial a la estrategia de ciberseguridad de BBVA-podcast (2021, 10 de septiembre) BBVA [video].YouTube.* (3) Google Cloud incorpora la inteligencia artificial a la estrategia de ciberseguridad de BBVA -Podcast - YouTube
- Flores, J (2021, 18 septiembre) *Red 5G y cómo nos cambiará la vida, 14 mayo*, https://www.nationalgeographic.com.es/ciencia/que-es-5g-y-como-nos-cambiara-vida_14449
- González, F. (2021, 14 septiembre) *Blockchain, [*ponencia] Diplomado de Tecnopolítica [en línea]
- Lewis M, Statista. Facebook. Consultado 15 de septiembre 2021. (1) Facebook
- Martínez R, Barrio F (2020, 4 noviembre) *Ciberseguridad: ¿Cómo defenderse? (aunque seas una PyME)* AMEX Business Class [en línea] Webinar American Express
- Morán, A. (2020, 29 de agosto) *Ciberseguridad*, [ponencia] Diplomado de Tecnopolítica, México, FES Acatlán, UNAM [modalidad en línea]
- Orlowski J –Lanier, J (2020), The social dilema- Netflix.
- Schwab*, K (2020, 16 de septiembre) La Cuarta Revolución Industrial,* World Economic Forum-Debat., Pp 4-16http://40.70.207.114/documentosV2/La%20cuarta%20revolucion%20industrial-Klaus%20Schwab%20(1).pdf