Newsletter
Centro de Investigaciones y Estudios Estratégicos
ANEPE

Editorial

Tecnología, sociedad y "nueva normalidad"

Fuente: Electrolopolis. Disponible en: https://www.electropolis.es/blog/desarrollo-las-nuevas-tecnologias/

La pandemia del Coronavirus nos sigue presentando un sinnúmero de nuevos desafíos, los que debemos enfrentar de manera urgente. Estos no solo se relacionan con el desarrollo de una vacuna o antídoto, sino que nos han impulsado a replantearnos la manera en que se han desenvuelto las relaciones sociales y, en particular, el ámbito laboral.

Hasta hace unos meses, el "teletrabajo" o trabajo a través de plataformas digitales era una actividad ejercida por pocos, y con el tiempo se ha transformado en la solución a las restricciones sanitarias, alentando a gran parte de la fuerza laboral a adaptarse a este modelo. Por otra parte, este nuevo trato tecnológico aún continúa generando trastornos, principalmente, en aquellos que no estaban preparados o bien no contaban con el adecuado acceso, motivando la aceleración de procesos gubernamentales globales para que el conjunto de la sociedad pueda gozar de los beneficios tecnológicos. Entre ellos se encuentran: el Internet de las Cosas (IoT), 5G, inteligencia artificial (IA), *Big Data* y Ciberseguridad, por nombrar los predominantes.

En el entorno global, y en Chile particularmente, se avanza en la discusión sobre el 5G, una tecnología que podría ofrecer mayores y mejores prestaciones laborales, pudiendo extenderse a otros ámbitos como el hogar. El cuestionamiento instalado en la discusión es hasta dónde se extendería la penetración, puesto que podría implicar un cambio de equipos, aumento de costos, o bien quedar fuera de coberturas, entre otras preocupaciones, como el tema de la protección de los datos personales.

Por otro lado, la IA ha alcanzado una preponderancia en este nuevo trato, puesto que el contar con este tipo de habilidades tecnológicas, permite mejorar sustancialmente los procesos productivos. Si a lo anterior se adiciona una gestión empresarial desde "la nube", sin duda que transforma la relación empresa-trabajador-cliente.

Este particular escenario digital se encuentra condicionado al desarrollo de la dimensión de ciberseguridad. En efecto, cuestiones como la *Deep Web; Malware; Cyber-attack; Hackers*, son variables que imponen desafíos sobre la manera de asegurar y proteger las funciones anteriormente mencionadas.

Considerando lo relevante del debate en torno a estas temáticas, y en especial la penetración del 5G en el país y los efectos de la Ciberseguridad, el CIEE pone a disposición una serie de artículos publicados en diferentes plataformas, los que invitan a la reflexión sobre la necesidad de contar con políticas públicas que puedan proporcionar la debida protección y seguridad.

CIEE-ANEPE

5G, la nueva revolución tecnológica

Elsa Uriburu

El Tribuno, 5 de septiembre 2020

Las redes móviles están en evolución continua desde que se crearon, pero ninguna provoca tantos debates como la 5G. Se trata de una tecnología global, que hace posibles nuevas aplicaciones de mayor velocidad y menor latencia (tiempo de respuesta) para usos personales y como así también en nuevas aplicaciones destinadas a la industria, con objetos y equipos conectados a internet que podrán dialogar entre ellos sin la intervención humana.

Ofrece condiciones para responder con mayor capacidad a la variedad de necesidades y exigencias tecnológicas, el despliegue de las infraestructuras de comunicación de esta nueva generación deberá mejorar los nuevos usos tales como el desarrollo de la realidad virtual, ciudades y transportes inteligentes, el manejo de máquinas a distancia, equipos interconectados entre sí, telemedicina, en la educación a distancia, entretenimientos...

La gran diferencia es la mayor calidad y la cantidad de datos que podrán intercambiar sin saturar las redes; además, permitirá la cohabitación de aplicaciones y usos diversos unidos en la misma tecnología. Se estima que ofrecerá una capacidad 10 veces superior a la de la 4G. […]

En Europa, La 5G-PPP (Public Private Parterner-ship) reúne a los sectores privado y público para la investigación. Cuenta con un presupuesto de 700 millones de euros dispuestos por la Unión Europea con el propósito de disminuir la dependencia tecnológica de los EE.UU. y Asia, y mantener gran parte del mercado mundial.

La sombra de China

Esta tecnología es el objeto de tensiones internacionales entre China y EEUU, fundamentalmente por dos razones la soberanía nacional y la guerra comercial declarada entre ambos. En este contexto los americanos presionan a otros países para limitar la utilización de los equipos chinos Huawei.

La Asociación Mundial GSMA, que reagrupa las principales empresas de la industria de telecomunicaciones, estima que "si los operadores del sector no pueden recurrir a los equipos ofrecidos por Huawei habrá un retraso considerable para desarrollar la red de acuerdo a los plazos estimados y el costo será mayor a nivel europeo" (55 mil millones de euros), ya que Huawei tiene mejores precios y el tiempo de entrega de los equipos en principio es más rápido. Además, la GSMA considera que tener solo dos proveedores reduce la competencia.

Las tecnologías en el campo de las telecomunicaciones que se desarrollaron desde hace décadas constituyen la principal fuente de exposición a las radiofrecuencias en la población en general y en el ámbito laboral, asociadas al aumento de la utilización, tanto aquella que proviene de los equipos transmisores y de emisoras fijas (antenas de radio, tele, estaciones de radio base para telefonía móvil, Wi-Fi) o las procedentes de los equipos móviles (teléfonos fijos, móviles, tabletas)

Una atmósfera de emisiones

Para poder identificar y evaluar científicamente los riesgos sanitarios potenciales de la 5G es necesario distinguir las bandas de frecuencias identificadas en la que se apoyara la nueva generación. En una primera etapa son las mismas bandas utilizadas para las redes actuales 2G, 3G, 4G, posteriormente nuevas bandas específicas para la 5G serán asignadas: 3,5GHz y aquellas situadas alrededor de 26 GHz, (actualmente ya existen plataformas de experimentación abiertas a otros actores que los tradicionales de telecomunicaciones permitiendo identificar nuevos usos y posibilidades de la 5G, en la banda de 26GHz, tales como los vinculados a la logística y seguimiento de los transportes en puertos, estaciones de trenes, eventos deportivos u otros tipos de servicios vinculados con empresas innovadoras usando cobertura interconectadas)

[…] Los estudios indican que los efectos en la banda de 3,5GHz serían similares a la exposición que tenemos entre los campos electromagnéticos

y el cuerpo humano con el uso de la TV, radio, telecomunicaciones móviles, WI-FI. No se verifican efectos para la salud a corto plazo.[…]

La 5G utilizará antenas "inteligentes", pequeños dispositivos que permiten focalizar las emisiones en una zona específica. La fuerza de las emisiones será mucho mayor, pero limitada en tiempo y en espacio (en teoría). Los métodos de mediciones deberán adaptarse a esta nueva modalidad tecnológica específica de la 5G a fin de precisar sus efectos colaterales. […]

Mito y realidad

Aquellos que se oponen a la nueva tecnología temen a los efectos en la salud y organizan manifestaciones y foros de discusión solicitando que se detengan los despliegues de las instalaciones de antenas en nombre del principio de precaución hasta tanto no se pruebe científicamente que no existe perjuicio para la salud pública y que no se superaran los límites tolerados en las emisiones actuales.

En el marco del debate "en tonos de color verde" lo paradójico es que los que se oponen a la 5G hoy probablemente serán los mismos que mañana acusarán a los operadores de telecomunicaciones y a los gobiernos de no haber hecho todo lo posible para evolucionar hacia esa tecnología.

Si se demoran o postergan las inversiones se pone en riesgo a los sectores industriales como el automotriz, la medicina, el sector hospitalario, educación; ellos serán las víctimas del retraso, necesitan de la 5G para ser competitivos en servicios y productos y para innovar en la batalla mundial y no solamente europea.

Si bien las redes actuales ya permiten avances en diversas industrias, la nueva tecnología permitirá mejorar aún más la capacidad y la velocidad; además facilitará muchas otras aplicaciones por ejemplo para la telemedicina o educación a distancia.

La COVID 19 demostró la importancia estratégica de las redes de telecomunicaciones, ya que fueron las únicas que ayudaron a continuar y hacer frente al funcionamiento de la economía cuando otras actividades y servicios estaban paralizados, vías férreas, líneas aéreas, puertos, transporte terrestre. No hay que subestimar las nuevas tecnologías, dejemos trabajar a los científicos al sector privado y público sobre un tema tan complejo. Las inquietudes son legítimas la solución es dialogar, explicar, informar, llevar acabo los estudios y pruebas necesarias y fijar el cuadro de las normas técnicas pertinentes.

URIBURU, Elsa. 5G, la nueva revolución tecnológica. El Tribuno, 5 de septiembre 2020. [en línea] [fecha de consulta 15 de septiembre 2020] Disponible en: https://www.eltribuno.com/salta/nota/2020-9-5-0-0-0-5g-la-nueva-revolucion-tecnologica

Opinión: ¿cuál es la demanda de la sociedad en materia de Seguridad y Defensa?

Claudio Ernesto Pasqualini
Infobae, 12 de Septiembre de 2020

La supervivencia ha sido, desde los orígenes de la humanidad, la principal preocupación de las personas. Esta supervivencia incluye el plano individual, de su grupo familiar y, luego, de su tribu o pueblo. Así también, hoy en día, la principal preocupación de cualquier persona siempre será velar por la seguridad propia, de sus afectos y, de acuerdo con una deseable conciencia nacional, de su patria. Todo esto, tomado en su concepción más amplia.

La sociedad no percibe la Defensa como una necesidad hasta que no se materializa alguna amenaza concreta, porque cuando esto ocurre, ya es tarde para empezar a prepararse. No podemos dejarnos llevar por la falsa ilusión de que vivimos en una "zona de paz" y de que no existen actores externos que afectan a nuestro país de distintas formas y según sus propios intereses. La coexistencia pacífica no se logra debilitándose unilateralmente, sino a partir de la fortaleza propia y manteniendo un proporcional equilibrio militar. Solo así una Nación puede tomar decisiones autónomas.

Podemos entender que una buena parte de la sociedad se focalice en reclamar por la inseguridad vigente y no por pedir mejores Fuerzas Armadas. Sin embargo, los que tienen la obligación de prestar especial atención a estas últimas, debido a su conocimiento en materia de

relaciones internacionales y por el deber de aplicar un pensamiento estratégico, son los responsables de conducir un país.

Disponer del sistema de defensa que la Nación necesita requiere de un largo proceso de planeamiento estratégico y de preparación. Aplicar una mirada cortoplacista puede tener consecuencias catastróficas; por eso, la conformación de Fuerzas Armadas eficientes y operativas no se puede improvisar, sino que requiere de muchos años de equipamiento, capacitación y adiestramiento.

En la actualidad, el mundo se encuentra inmerso en un continuo proceso de transformación, cada vez más vertiginoso e impredecible, donde los más fuertes y preparados son quienes lo conducirán, aprovechando las oportunidades que se vayan presentando o que ellos mismos generarán.

[…] Por todo lo expresado anteriormente, una de las principales preocupaciones debería ser el análisis de la situación en la que nos encontramos y la planificación de hacia dónde se deberían encaminar las políticas de Seguridad y Defensa, como políticas de estado. Se necesita una clara mirada hacia el futuro, consensuada con todas las fuerzas políticas del país, de modo de garantizar su continuidad, más allá del gobierno de turno. Es tiempo de pensar en algo nuevo en materia de seguridad y defensa.

Desde una prestigiosa universidad, se está trabajando en la creación de un espacio que centre su atención en el monitoreo, análisis y evaluación de los temas de Seguridad y Defensa, dentro de los ámbitos nacional e internacional, de modo de enriquecer las distintas visiones y posturas que predominan actualmente para que se pueda profundizar el conocimiento sobre dichos temas, junto con otros espacios similares ya existentes, respetando la libertad de pensamiento y propiciando una mirada amplia, plural y desideologizada.

Las preguntas e inquietudes son muchas, y van desde el análisis de una legislación acorde a los tiempos en los que vivimos, hasta la reestructuración y organización de las fuerzas de seguridad y las fuerzas policiales. A nivel mundial y regional, ¿qué mirada hay sobre el tema, qué labor han desarrollado los países vecinos?

Estos últimos son tan solo algunos de los interrogantes que pueden plantearse, que anhelamos que especialistas y académicos de todos los ámbitos nos ayuden a responder. Creemos que eso contribuirá a encontrar soluciones a las amenazas, los riesgos y los desafíos que nos presenta el mundo actual, tanto dentro como fuera de nuestro territorio, para hacer un uso más eficiente de los recursos con los que cuenta el Estado, con el objetivo de asegurar sus intereses vitales y, fundamentalmente, la vida, la libertad, el bienestar y los bienes de todos los argentinos.

PASQUIALINI, Claudio. Opinión: ¿cuál es la demanda de la sociedad en materia de Seguridad y Defensa? Infobae, Opinión, 12 de septiembre 2020. [en línea] [fecha de consulta 15 de septiembre 2020] Disponible en: https://www.infobae.com/def/defensa-y-seguridad/2020/09/12/opinion-cual-es-la-demanda-de-la-sociedad-en-materia-de-seguridad-y-defensa/

Ciberseguridad: claves para entender su vigencia, dinámica y heterogeneidad en el mundo

Mariano Bartolomé

Infobae, 26 de Septiembre de 2020

Desde mediados de la década de los 80, la informática ha abandonado el ámbito estrictamente científico para ocupar un lugar cada vez más importante en nuestra vida cotidiana. En particular, de la mano de los dispositivos móviles, su presencia llegó a volverse omnipresente. El desarrollo de la llamada “internet de las cosas” (IoT) indica que esta situación se acentuará aún más en el corto y mediano plazo. El sociólogo Manuel Castells ha ayudado a dimensionar cuantitativamente la cuestión, al indicar que, a fines del año pasado, los usuarios de internet rondaban los 4200 millones, contra apenas 40 millones en 1996; mientras que los aparatos de telefonía celular, que en 1991 eran unos 16 millones, en la actualidad estarían superando los 7000 millones.

Como es sabido, este fenómeno presenta un nítido correlato en el campo de la seguridad, donde ocupa un lugar central el acceso a los llamados “comunes globales”, dominios que no están bajo el control ni bajo la jurisdicción de ningún Estado,

pero cuyo uso es objeto de competencia por parte de actores estatales y no estatales de todo el planeta. Así las cosas, a los cuatro dominios o ámbitos tradicionales de la Defensa –terrestre, marítimo, aéreo y aeroespacial– se sumó el cibernético, que los atraviesa.

La ciberseguridad atiende a las amenazas que se desarrollan en este quinto dominio, el ciberespacio, y alcanza todos los niveles de la interacción social, desde las relaciones interpersonales hasta las dinámicas del tablero global. En este último plano, en forma recurrente, se ejecutan ciberataques de diferente tipo, en función de variados objetivos estratégicos. Como bien señala un especialista español, hoy estos ataques responden a estrategias de poder, coacción e influencia deliberadas.

Ciberterrorismo: acción y reacción

Las cuestiones de ciberseguridad no han disminuido en intensidad durante el presente año. De hecho, en la reunión del Foro de Davos celebrada en el mes de enero, el secretario general de la ONU, António Guterres, incluyó las amenazas tecnológicas entre los cuatro "jinetes del Apocalipsis" que provocan incertidumbre e inestabilidad globales. Completaron la lista el cambio climático, la desconfianza de los ciudadanos en sus instituciones y las tensiones geopolíticas. Esta pesimista lectura no se vio modificada a partir de la aparición del COVID-19 y la pandemia que se propagó a lo largo de grandes regiones, y frente a la cual la población aún no tiene inmunidad. Por el contrario, desde la eclosión de esta difícil situación sanitaria que alcanzó a cada rincón del planeta, el ciberespacio ha sido escenario de numerosos acontecimientos, protagonizados por actores estatales y no estatales.

Las organizaciones terroristas se incluyen entre los actores no estatales que se valen del ciberespacio para alcanzar sus metas. El grupo salafista-yihadista "Estado Islámico" es un buen ejemplo de ello. Hace unos meses, se descubrió en España un conjunto de redes virtuales empleadas por ese grupo terrorista para llevar a cabo procesos de adoctrinamiento y difusión masiva de sus postulados, abogando por la no integración de sus seguidores en la sociedad occidental, cuyos valores rechazan.

Aun más importante, los operadores de esas redes tenían instrucciones de localizar a blancos potenciales de sus acciones terroristas en diferentes países. Pero en este campo también se registran iniciativas en sentido inverso, como fue el caso de la operación coordinada por Europol en noviembre del año pasado, que contó con la participación de una docena de Estados miembros y varios proveedores de internet. Con esa ofensiva digital, se neutralizaron más de 25.000 cuentas asociadas a esa organización islamista, material de difusión y canales de comunicación asociados a al-Amaq, su agencia de prensa.

A pesar de esos denodados esfuerzos, no ha cesado el uso del ciberespacio por parte de esas organizaciones. Tanto el Estado Islámico como Al Qaeda intentaron capitalizar en su beneficio la situación generada por el COVID-19, sosteniendo a través de sus redes que la epidemia consistía en un castigo divino contra China –por su maltrato a la minoría musulmana de Xinjiang– y contra las sociedades apóstatas de Occidente. […]

Cibercrimen, deep web y ataques maliciosos

Los criminales no les fueron en zaga a los terroristas. La actual pandemia fomentó, en términos cuantitativos, una expansión de la cibercriminalidad. La comercialización de supuestas vacunas contra el virus a través de circuitos alternativos, como la deep web ("internet profunda"), fue una de sus manifestaciones más nítidas. Diversas redes ilegales, algunas de dimensiones internacionales, dominaron miles de dominios relativos al coronavirus para, con esta herramienta, intentar obtener beneficios millonarios.

El llamado phishing fue uno de los formatos empleados con mayor recurrencia: se enviaban correos electrónicos fraudulentos, aparentemente de las autoridades sanitarias locales e incluso de la mencionada OMS, que invitaban al receptor a visitar páginas web apócrifas, desde las que se solicitaba información personal, incluso nombres de usuario o contraseñas. De hecho, en Argentina se registraron casos de este tipo,

consistentes en falsos formularios en línea del programa gubernamental Alimentar. Así, se instaba a la víctima a hacer clic en enlaces que descargaban en su computadora malwares o ransomwares, es decir, programas que extraen datos sin consentimiento del usuario, o que vedan su acceso a la información almacenada, y luego su ejecutor solicita una suerte de rescate.

[…]Otro grave episodio, ocurrido seis meses más tarde, tuvo como blanco al hospital catalán "Moisès Broggi", varios de cuyos sistemas operativos quedaron bajo el control de criminales que exigieron un rescate para su normalización.

Infraestructuras críticas, un blanco vulnerable

El empleo del ciberespacio en términos de seguridad es igualmente intenso en las dialécticas interestatales. Y abarca un enorme espectro de manifestaciones que, al menos en el campo de la teoría, incluyen el enfrentamiento directo entre las partes en el ciberespacio; o, dicho de otro modo, la ciberguerra. Abonando esta perspectiva, autores de diferente formación aventuran, incluso desde la ficción, futuros conflictos bélicos librados enteramente en ese dominio.

Por ahora, este escenario tendría una escasa probabilidad de ocurrencia, pues, como señaló Heli Tiirmaa-Klaar, lo que en todo caso podrá haber son conflictos armados en el mundo físico con una faceta "ciber". Esta especialista estonia, que coordinó la política del ciberespacio en la Unión Europea, considera que sería más plausible la situación inversa: una operación de agresión en el ciberespacio, que falle y escale al uso de la fuerza cinética.

La situación parece no haber llegado a ese punto límite y sigue desarrollándose en niveles inferiores a ese "umbral", niveles que incluyen las operaciones orientadas a afectar las llamadas "infraestructuras críticas". Nos referimos aquí a activos de vital importancia para la seguridad, el gobierno y la economía nacionales, y para la confianza ciudadana, que incluyen, como un elemento central, la prestación de servicios esenciales a la población.

Determinar el "quién"

La cuestión de la "atribución" continúa siendo un elemento clave en las crisis desatadas por ciberataques de un Estado contra las infraestructuras críticas de actores homólogos. En general, como se constató en los mencionados casos de Estonia y Ucrania, resulta prácticamente imposible reunir evidencia contundente sobre los autores intelectuales –que pueden haber delegado la ejecución en proxies o actores por encargo, que no son estatales–, lo que hace difícil sustentar una "legítima defensa" en los términos del marco normativo de Naciones Unidas.

Esto no quita que, con intenciones disuasivas sobre eventuales acciones de la contraparte, un Estado haga conocer sus capacidades para generar daño a través del ciberespacio. En este sentido, a mediados del año pasado desde el US Cyber Command, se hizo saber que se habían ejecutado múltiples y profundas incursiones en la red eléctrica rusa, insertando códigos informáticos propios, como respuesta a medidas similares instrumentadas por Putin, además de su injerencia en cuestiones políticas domésticas estadounidenses. […]

Además de EE.UU., también Alemania ha acusado a Rusia en los últimos tiempos, en relación con el desvío de sus conductas en el ciberespacio. En concreto, responsabilizó a Putin por el ciberataque perpetrado contra el Bundestag (Parlamento alemán) hace un lustro, cuando varios legisladores recibieron un falso correo electrónico procedente de Naciones Unidas con información sobre Ucrania, lo que hacía que descargaran involuntariamente un malware que terminó paralizando el sistema informático y posibilitó el robo de aproximadamente 16 gigas de información. Las pesquisas de los servicios de seguridad germanos concluyeron que el responsable de la agresión era Dimitri Badin, un cuadro del servicio de inteligencia militar ruso también involucrado por el FBI en el hackeo a las elecciones estadounidenses de 2016.

Espionaje, robo de datos y 5G

El caso del Bundestag nos recuerda que el espionaje no está excluido de las acciones que desarrollan los Estados entre sí en el quinto

dominio. En este sentido, hoy el centro de la escena está ocupado por el nítido deterioro de los vínculos entre EE. UU. y China a lo largo de los últimos años. Dentro de este conflictivo panorama donde interactúan factores múltiples y heterogéneos, se incluyen los contrapuntos en torno al origen de la actual pandemia, una de cuyas teorías apunta a un centro de guerra biológica en la ciudad de Wuhan. […]

En torno al eje del espionaje, también se enmarcan las posturas de Washington respecto a la tecnología 5G y las compañías chinas Huawei y ZTE, que han sido catalogadas como verdaderas "amenazas a la seguridad nacional" desde el momento en que sus redes pueden ser veladamente empleadas para la recolección de información por cuenta y obra del Partido Comunista Chino.

¿Serían igualmente críticas las posiciones oficiales de Estados Unidos, el Reino Unido y otras potencias occidentales respecto al peligro que supone Huawei sobre las garantías y los derechos de los ciudadanos si el régimen político chino se asemejara a una democracia en el sentido occidental del término? Es imposible saberlo a ciencia cierta, pues toda respuesta a este interrogante es especulativa. Lo que no puede descartarse es que la naturaleza autoritaria de ese régimen exacerbe los temores en otras partes del mundo, como lo sugieren las declaraciones que formuló la presidenta de la Cámara de Representantes de EE.UU. en la última edición de la Conferencia de Múnich. En ese cónclave, pese a sus diferencias ideológicas, Nancy Pelosi hizo causa común con la Casa Blanca, al considerar que "tener un 5G dominado por una autocracia es la forma más insidiosa de agresión".[…]

Big Data, vigilancia digital y aparatos represivos

Hoy en día, los debates sobre la interacción entre tecnologías digitales empleadas por los aparatos estatales, por un lado, y los derechos de la población, por otro, exhiben aristas que van mucho más allá del caso de Huawei. En China y otras naciones del Extremo Oriente, incluso democracias consolidadas como Japón y Corea del Sur, los gobiernos han echado mano a sistemas de vigilancia digital, basados en el manejo de Big Data, para enfrentar a la pandemia. Estos mecanismos registran y supervisan cada movimiento de los ciudadanos, evaluando su impacto en la crisis sanitaria y facilitando, en consecuencia, el proceso de toma de decisiones. […] Ahora bien, medidas de ese tenor podrían ser consideradas en Occidente como amenazas a la privacidad y a las libertades de expresión y asociación.

En suma, el puñado de hechos relativamente recientes apenas descrito permite ratificar la enorme vigencia de las cuestiones asociadas al ciberespacio en materia de seguridad, así como los diferentes formatos que ellas pueden adoptar. Lejos de disminuir la vulnerabilidad de los Estados, las sociedades que los conforman y los ciudadanos que las integran, los daños que pueden sufrir en el dominio cibernético tenderán a aumentar, según lo aseguran todos los reportes sobre este tópico, independientemente de su procedencia o de su carácter público o privado. La interacción del dominio cibernético con el espectro electromagnético y con la Inteligencia Artificial (IA) influirá en la fisonomía de tales vulnerabilidades.

La comunidad internacional en su conjunto, desde una escala global hasta niveles regionales, debe elaborar respuestas acordes a estos desafíos, generando e implementando decisiones que permitan lidiar de manera efectiva con este escenario. En nuestro hemisferio en particular, la Organización de Estados Americanos (OEA) ha llevado adelante importantes iniciativas en este campo, en algunos casos en conjunto con el sector empresario, siempre promoviendo la participación de los gobiernos nacionales. Sin embargo, frente a este tipo de amenazas y riesgos, ningún esfuerzo será excesivo.

BARTOLOMÉ, Mariano. Ciberseguridad: claves para entender su vigencia, dinámica y heterogeneidad en el mundo. Infobae, Opinión, 26 de septiembre 2020. [en línea] [fecha de consulta 30 de septiembre 2020] Disponible en: https://www.infobae.com/def/defensa-y-seguridad/2020/09/26/ciberseguridad-claves-para-entender-su-vigencia-dinamica-y-heterogeneidad-en-el-mundo/?fbclid=IwAR3CVCyiqkIeKfprZkN8Bk1IlDcPCQLjwxHto-L_N9WumSZ5O8S7S55HhQI

Las habilidades que vas a necesitar en la nueva normalidad digital

Àngela Zorrilla

La Vanguardia, 30 de septiembre 2020

Llevamos meses reafirmando que la crisis sanitaria de la COVID-19 ha supuesto un revulsivo en el mercado laboral. Sin olvidarnos de que ha sido una crisis con consecuencias en el ámbito de la salud, social y económico, también debemos reconocer que ha ayudado a revolucionar el trabajo y sus metodologías en muchas empresas, acelerando su digitalización. Antes del coronavirus, casi un 69% de empleados españoles quería teletrabajar, pero su empresa no se lo permitía. […]

El coronavirus ha dado voz, entre otros, al teletrabajo y ha abierto las puertas a una visión más digital y transformadora en todas las compañías. 6 de cada 10 empresas confiesan que han tenido que modificar la estrategia digital debido a la crisis del coronavirus. Y es que a nadie le sorprende ya tener que asistir a una reunión virtual o verse trabajando cómodamente desde su casa.

[…] La revolución ha llegado para quedarse y lo hará de la mano de empleos hasta ahora inexistentes y de trabajadores formados como nunca hasta ahora. ISDI (Instituto Superior para el Desarrollo de Internet), la primera escuela de negocios nativa digital, lo tiene claro: la clave para destacar en este escenario es la "cualificación de las personas"; es decir, empoderar y capacitar a todo este talento. Pero ¿cómo deben ser estos nuevos trabajadores?

Para sobrevivir en esta economía digital y destacar entre la creciente competencia, los profesionales deben desarrollar nuevas aptitudes y fomentar una visión no solo de presente, sino de futuro. Como definen desde ISDI, es necesaria una educación basada en el concepto de lifelong learning. Es decir, en esta era de cambios abrumadores todos vamos a necesitar realimentar constantemente nuestros conocimientos y adquirir nuevas habilidades que nos permitan mantenernos actualizados. En resumen: con metodologías "de ayer" sólo se podrán gestionar los negocios "de ayer".

Los empleos del futuro (que ya están aquí)

La propia escuela, en su mapa de profesiones digitales del año pasado, ya destacaba el papel crucial de perfiles como los traductores digitales –capaces de reinterpretar la visión estratégica de las empresas– o perfiles como los Business intelligence analysts, UX designers o Trade marketing digital managers… […] En realidad el 90% de los puestos de trabajo actuales (y futuros) exigirá competencias digitales cuando en España el 32% de la población tiene muy poco nivel en estas habilidades.

El futuro va de tendencias globales y de estas nuevas skills. De intentar adelantarse al frenético ritmo (y sobre todo cambiante) del mercado laboral y de la realidad en la que vivimos. ISDI, líder en educación digital, identifica tres grandes tendencias que van a condicionar la contratación de talento en los próximos meses: aparecerán nuevos perfiles estratégicos, más híbridos y con enfoques más complejos y completos; se acelerará la contratación de empleados para áreas con un claro futuro como Marketing, Data o Seguridad; y se llevará a cabo una revisión de las habilidades y capacidades que se demandaban en un candidato hasta la fecha, valorando cada vez más las soft skills como la resiliencia o la flexibilidad.

[…] Hoy además es clave aportar habilidades tecnológicas y una nueva percepción del entorno laboral. Cada vez más, las empresas buscan perfiles que sepan trabajar por objetivos y tengan una clara orientación a resultados. Y es que el cambio cultural donde el presentismo ha dejado paso a la consecución de las metas ya se ha producido. Y más, teniendo en cuenta el escenario actual dibujado tras el paso del estado de alarma en el país.

La tecnología, al final, debe verse por las compañías como un facilitador para lograr sus objetivos clave. […]

Ayudar a las empresas a transformarse digitalmente

Para ser protagonistas de este nuevo marco, las empresas (y sus empleados) deben adaptarse y dirigir su propia revolución digital. […]

[…] Como explica Dionís Guzmán, director de ISDI en Barcelona, la capital es “la ciudad con mayor porcentaje de startups, que equivale prácticamente al 35% del total de startups del estado y es la tercera ciudad europea preferida por los founders europeos para instalar sus proyectos”. Del mismo modo, Guzmán asegura que “Barcelona se ha convertido en el destino favorito de muchas corporaciones de la economía tradicional” que escogen la ciudad “para establecer sus hubs digitales encargados de la transformación de multinacionales como Nestlé, Purina o LIDL que, desde aquí, definen las líneas maestras de sus estrategias digitales a nivel mundial”.

[…] Al final, empresas, líderes y trabajadores deben prepararse –y sobre todo formarse- para el mundo cambiante y volátil en el que vivimos. Y nativos digitales como ISDI aseguran que el fenómeno de la digitalización “no solo es inevitable” sino que, además, es “positivo, divertido y apasionante”.

ZORRILLA, Ángela. Las habilidades que vas a necesitar en la nueva normalidad digital. La Vanguardia, 30 de septiembre 2020. [En línea] [fecha de consulta 30 de septiembre 2020] Disponible en: https://www.lavanguardia.com/economia/20200903/483229896038/nueva-normalidad-digital-estas-habilidades-necesitas-brl.html