Reflexiones sobre la seguridad de la información

DOI: 10.29236/sistemas.n155a2

Retos y expectativas en la economía 5.0. Despliegue de los asistentes digitales (robots en software)

Resumen
La quinta revolución industrial nos vuelve a invitar a que los robots en software nos asistan y que sean ellos los que hagan las tareas repetitivas para que los seres humanos tengamos tiempo de ser innovadores, resolvamos problemas impredecibles, comprendamos las emociones de nuestra humanidad y que, mediante el pensamiento crítico podamos complementarnos con los demás.

Palabras claves
Economía Lineal, Economía Circular, Transformación Digital, Ciberseguridad.

Introducción

En algunas ocasiones, al terminar la jornada y revisar retrospectivamente lo realizado, sentimos que hacemos diariamente tareas repetitivas. Tenemos la sensación de que somos autómatas; nos sentimos como si fuéramos robots, pues todos los días reproducimos actividades como leer correos, diligenciar hojas electrónicas, volcar hojas electrónicas en los sistemas de información de la organización para la que trabajamos y un sinnúmero de reportes, entre otras.

En el caso específico del oficial de seguridad o CISO, que ejecuta actividades propias como hacer análisis de vulnerabilidades, penetrar fallas, hacer análisis de riesgos de ciberseguridad y seguridad de la información, ayudar a ejecutar controles para gestionar la seguridad de la información, se tiene la impresión de un parecido con los robots. Aún con la pasión con que las ejecutamos, nos percatamos de que estas son tareas repetitivas, especializadas, propias de un autómata.

Ahora, frente a un evento no predecible como la pandemia COVID-19, nos invade la sensación de estar encasillados, sin esperanzas y llenos de incertidumbre por el creciente número de muertos debido al virus. Afortunadamente, estamos reunidos en familia y, estando en nuestros hogares debido al aislamiento obligatorio decretado por el Gobierno Nacional, nos colman sentimientos de gratitud con Dios que antes no teníamos con tanta frecuencia. Son sentimientos fuertes que expresan agradecimiento con lo que nos rodea, con lo que nos provee la naturaleza, en especial con nuestras familias, con nuestras parejas y hasta con nuestras empresas, pues nuevamente constatamos que nada está establecido perpetuamente; que todo cambia y debemos adaptarnos al cambio.

El autor de este documento considera que el Covid-19 es un evento aleatorio de tipo catastrófico por los efectos de los impactos económicos y sociales causados, que pudo haber sido prevenido, la capacidad de enfrentar eventos aleatorios es único de los seres humanos, pero estamos sumergidos en las actividades repetitivas del quehacer diario, por lo tanto la transformación hacia una economía circular es inevitable, y la seguridad de la información y la ciberseguridad no pueden escapar a la atracción tan fuerte como la generada por la economía 5.0, esta nos brinda la capacidad de resolver problemas no predecibles mediante la creación de nuevas ideas, en cambio de continuar haciendo tareas repetitivas que no generan valor.

Economía circular

Vivimos y nos desenvolvemos en una economía lineal donde pare-

ciera que la razón de existir es la adquisición de propiedades y productos de forma repetitiva, en un ciclo de no terminar. Independiente de la clase social en la que estemos enmarcados, todos queremos obtener cada vez más productos, sin importar a dónde se dirijan los residuos del proceso desde su diseño hasta su creación, por lo tanto, no existe una conciencia colectiva del efecto a largo plazo de no reciclar. Esto se evidencia cuando desechamos artículos al haber finalizado su ciclo de vida o, peor aún, cuando queremos renovarlos porque anhelamos tener en nuestras manos la última tecnología disponible en el mercado, así objetivamente no la necesitemos.

En la economía lineal pueden observarse las siguientes fases desde la entrada de las materias primas que intervienen en el proceso, hasta la obtención del producto final: extracción, refinamiento, fabricación, ensamblaje, generación de desechos o residuos y entrega del producto final. Es muy importante anotar que las materias primas están encasilladas en una obsolescencia programada; por ejemplo, un firewall de perímetro para BD y/o aplicaciones Web, un control DLP, como algunos otros productos de ciberseguridad, después de tres o cuatro años, serán obsoletos por la obsolescencia programada y los residuos no reutilizados; en consecuencia, fue impactada negativamente la naturaleza. Por ello en la actualidad, somos el reflejo de la cuarta revoluciónn industrial; una sociedad de consumo desmedido e irresponsable con la naturaleza, y estos recursos naturales disminuidos son los que le dejaremos a las futuras generaciones, nuestros hijos.

En esta cuarta revolución industrial o Economía 4.0, el ser humano ha creado tecnologías innovadoras y disruptivas que nos han permitido iniciar la transformación digital de sociedades y gobiernos. Algunas de estas tecnologías son la computación en la nube, la analítica de grandes volúmenes de datos o Big Data, la Inteligencia Artificial, la impresión 3D, IoT y los lenguajes de programación RPA (por sus siglas en inglés, automatización de procesos mediante robots), entre otros (Deloitte, 2020).

Sin embargo, no todo es negativo en la cuarta revolución industrial; actualmente, los novedosos “trabajadores digitales” o “asistentes digitales” están siendo aprovechados por las diferentes industrias para reducir costos, disminuir la probabilidad de errores en los procesos, mejorar la actitud y aumentar la moral de los empleados humanos.

RPA + Inteligencia Artificial + Analítica de patrones, le permite hoy al ser humano enfocarse en las tareas más humanas, es un inicio incipiente de la colaboración entre humanos y robots de software. En el presente año, emergerán tecnologías robóticas con apoyo de otras

Figura 1: Tecnología disruptiva RPA (Elaboración propia)

de inteligencia artificial, que le sugerirán al humano, de forma automática, cuáles actividades repetitivas se pueden automatizar.

El punto más alto de la cuarta revolución industrial es la transformación digital de las empresas, que aún se está dando y durará unos años más, antes de que la explotemos en la incipiente quinta revolucion industrial. Por ejemplo, en Colombia la banca y las telecomunicaciones hacen uso intensivo de la robótica por software en sus operaciones y ciberseguridad, pero el sector salud, defensa y justicia, por nombrar algunos, estan distantes de iniciar la transformacion digital, la mejor evidencia es como estamos afrontando la pandemia Covid-19 a nivel judicial, segun lo informado por los medios de comunicacion locales.

En la naciente quinta revolución industrial, la base será la economía circular, cuyo objetivo no será la adquisición de productos, sino la adquisición de servicios.

Entonces veremos muchos productos de ciberseguridad y seguridad de la información en forma de servicios; por ejemplo, protección contra amenazas IoT, protección contra amenazas de la inteligencia artificial en automóviles autónomos, protección, gestión y analítica de riesgos emergentes, entre otros.

Por lo tanto, la cantidad de innovación requerida será un factor crítico para evitar la destrucción de los ecosistemas en los que vivimos a causa de la extracción desmedida de materias primas o insumos para fabricar los productos que se venderán como servicios. Esta quinta revolución industrial propone el complemento del hombre con la máquina; será común encontrarnos en nuestros trabajos con los llamados "ciberhumanos": parte humano, parte máquina. Es decir, humanos hibridos que tendran piernas y hasta brazos ciberneticos.

Hoy en la cuarta revolucion industrial encontramos en el sector financiero, en especial en las organizaciones bancarias como, por ejemplo, Bancolombia, unos 12.000 robots en software que asisten a los trabajdores bancarios (Attended Bot) y unos 3.000 robots en software que ya no requieren de intervencion humana (Unattended Bot) (Otálvaro, 2019).

La cuarta revolución industrial construyó las tecnologías disruptivas que serán utilizadas y explotadas masivamente en la naciente quinta revolución industrial; en esta, podrán observarse las siguientes fases: producción, consumo y reciclaje.

Se define la economía circular como "Repensar, Reutilizar, Reparar,

Figura 2: Trabajador o asistente digital (Elaboración propia)

Figura 3: Iniciando la Transformación Digital (Elaboración propia)

Restaurar, Re-manufacturar, Reducir, Re-proponer, Reciclar y Recuperar" (Minambiente, 2018).

Los principios de la economía circular, son: diseñar para minimizar el desperdicio, mantener productos y materiales en uso, regenerar los sistemas naturales; esto nos trae las siguientes ventajas: mejorar el capital y proteger el medio (Naturaleza), hacer mejor gestión de los ciclos técnicos y biológicos, minimizar el impacto de los residuos en la naturaleza (AMV, 2018).

El autor de este articulo considera que la transformación digital que comenzó en la cuarta revolución industrial debe iniciar como un cambio de cultura y, sobre todo, en un cambio de actitud mental. Un buen inicio es hacer una alineación de nuestra organización con la propuesta de la economía circular, para lo cual debemos crear, en nuestras organizaciones, un proceso o área, o Centro de Excelencia (CoE) donde se puedan repensar nuestros productos y servicios como servicios digitales puros. Creo que no hemos terminado la cuarta y ya estamos en la quinta revolución industrial.

Las tecnologías disruptivas son herramientas muy poderosas, pero no deben ser la piedra angular, pues el hecho de invertir en herramientas no garantiza el éxito de la transformación digital; primero deben revisarse las estrategias para alinear la

inversión. Un libro interesante de David Rogers, titulado *The Digital Transformation Playbook: Rethink Your Business for the Digital Age,* propone que debemos reevaluar nuestro actual negocio, revisando las estrategias sobre cinco aspectos importantes del negocio: "Los Clientes, La Competencia, Los Datos, La Innovación y el Valor" (Rogers, 2016).

La quinta revolución industrial nos vuelve a invitar a que los robots en software nos asistan y que sean ellos los que hagan las tareas repetitivas para que los seres humanos tengamos tiempo de ser innovadores, para que nos dediquemos a resolver problemas impredecibles, para que comprendamos las emociones de nuestra humanidad y para que, mediante el pensamiento crítico, podamos complementarnos con los demás para visualizar una sociedad más humanitaria, más incluyente, más equilibrada, más segura para con la información y la vida, y sobre todo más compasiva con los demás.

Seguridad informática hace 10 años

En los últimos 10 años hemos visto la aplicación de la economía lineal en la seguridad de la información. Como, por ejemplo, hemos visto evolucionar la seguridad informática hacia la ciberseguridad, y hoy encontramos que las organizaciones, en general, entienden que existe un concepto más alto llamado "seguridad de la información", que contiene a la ciberseguridad; es decir, contempla la seguridad informática cuando interactúa mediante Internet para intercambiar información.

Además, hemos estado monitoreando y poniendo controles sobre la información en uso, información en reposo e información en movimiento. En controles, hemos visto pasar el firewall de perímetro hacia el firewall personal, ahora moviéndose el firewall con el usuario debido a los dispositivos móviles, IoT y servicios en la nube.

El antivirus basado en firmas estáticas (hash) evolucionó hacia el antimalware basado en heurística y ahora en analítica y comportamiento anómalo de patrones. Las redes sociales ahora son canales de comunicación críticos para entender los comportamientos de consumo y las necesidades de los clientes, pero suponen riesgos de seguridad en la información.

Adicional a estos cambios, el factor humano se ha transformado en un componente de los nuevos mapas de riesgos en línea usados en ciberseguridad para determinar un estado temporal de la ciberseguridad. La protección de fuga de información o DLP (*Data Leak Prevention*) basada en el apagado y encendido de puertos evolucionó hacia el DLP basado en analítica y tendencia de patrones sobre el comportamiento del usuario. Hemos visto pasar la gestión de los

riesgos conocidos hacia los riesgos emergentes y ahora es evidente la gestión integrada de los riesgos a nivel corporativo.

En los últimos 10 años, también hemos visto que finalmente los países establecieron leyes para la protección de los datos personales por parte de las organizaciones. En Colombia, por ejemplo, existe la Ley 1581 de 2012 y para proteger los datos reservados de las organizaciones se expidieron los Decretos 1377 de 2013, Decreto 886 de 2014 y el Decreto 1759 de 2016.

El cumplimiento de normas como la ISO 27001, ISO 31000, ISO 22301 e ISO 27032, para citar algunas, se han convertido en un estándar a seguir por la mayoría de las organizaciones, por lo menos para gestionar los riesgos conocidos. La norma ISO 27001:2013 propone dos controles importantes para proteger la información: Clasificación de la información en el control A.8.2.1 y el Etiquetado de la Información en el control A.8.2.2. También propone clasificar la información en por lo menos cuatro categorías: información pública, información privada o de uso interno, información secreta" e información personal.

La medición de comportamientos observables en seguridad de la información mediante indicadores y métricas como las denominadas PKI (indicadores de riegos de rendimiento) y KRI (indicadores de riesgos de seguridad), entre otros, son el lenguaje comúnmente utilizado en los procesos de cumplimiento, riesgos, ciberseguridad y seguridad de la información.

Asistentes digitales: breve prospectiva para 2030

Veremos innovación al entrelazar diferentes áreas del conocimiento para evitar ataques dirigidos que buscan denegación de servicios críticos a la sociedad debido a la aparición de nuevas enfermedades sin vacunas que atacarán a poblaciones específicas a nivel mundial, es muy probable que aparezcan los servicios de hacking biológico, es decir hacking a nivel genético.

Ataques a tecnologías fuertemente implementadas en servicios como el RPA, la Inteligencia Artificial y el Blockchain, entre otros, debido a la naturaleza inherente de la vulnerabilidad en esos servicios, así como a la ausencia de análisis de riesgos emergentes de ciberseguridad y seguridad de la información.

Los atacantes utilizarán Robótica, Analítica e Inteligencia Artificial para predecir comportamientos y preparar los ataques e intrusiones a los servicios de la quinta revolución industrial.

Entonces, debemos estar a la vanguardia y adelantarnos al cambio, diseñando procesos altamente robotizables y resilientes; estaremos un paso adelante y preparados para asumir el reto que plantea una economía circular, de servicios co-

mo producto final, de respuesta ágil como factor común, y de escalabilidad y agilidad de los productos y procesos para atender rápidamente las nuevas y cambiantes necesidades del mercado.

Conclusiones

1. Las situaciones imprevistas como el COVID-19 nos retan y nos presionan a innovar, a experimentar cruzando elementos de diferentes áreas del conocimiento. Estos eventos inciertos nos presionan a crear en medio de la desesperanza, pues al estar en medio de las dos revoluciones industriales más notables de la historia de la humanidad, es una clara invitación a transformarnos digitalmente, siendo el momento de reinventarnos en todo nivel.

2. Debemos hacer que los robots de software nos asistan y que sean ellos los que hagan las tareas repetitivas para que nosotros seamos innovadores, para que nos dediquemos a resolver problemas impredecibles, para que comprendamos las emociones de nuestra humanidad y que, mediante el pensamiento crítico, podamos complementarnos con los otros y visualizar una sociedad más humanitaria, más incluyente, más equilibrada, más segura y, sobre todo, más compasiva con los demás.

3. Hasta la cuarta revolución industrial, la raza humana muestra señales de una enfermedad mental similar a la esquizofrenia: muestra de ello es el consumo y producción desenfrenados; queremos crecer y producir sin tener la mínima responsabilidad sobre el impacto de nuestros residuos en la naturaleza.

4. En la quinta revolución industrial, tendremos en nuestras oficinas los ciberhumanos, compañeros de trabajo humanos con partes cibernéticas

5. Las empresas multinacionales tendrán un proceso o área de economía circular para repensar los actuales productos y servicios como servicios puros que la sociedad pagará por su utilización o consumo.

6. Los productos de seguridad de la información y ciberseguridad también se venderán como servicios puros.

7. La Inteligencia Artificial se aplicará a los diferentes ámbitos de la vida real y, en particular, a la seguridad de la información, pero también será vulnerada.

Referencias

Jorge Otálvaro, VP Bancolombia. (12 de julio 2019) *Automation Anywhere*. Recuperado el 22 de mayo de 2020 https://www.youtube.com/watch?v=DI4MtfW8Z8U.

Ministerio de Ambiente y Desarrollo Sostenible - Minambiente. (2108, Noviembre) *Colombia le apuesta a las 9R en*

economía circular. Recuperado el 23 de mayo de 2020 de https://www.minambiente.gov.co/index.php/noticias/4225-colombia-le-apuesta-a-las-9r-en-economia-circular.

Ateneo Mercantil de Valencia - AMV. (18 de junio 2018) *Economía Circular - Ciclo Cuarta Revolución Industrial*. Recuperado el 24 de mayo de 2020 de https://www.youtube.com/watch?v=VxeYSUTtF6g.

Rogers, D. (2016). *The Digital Transformation PlayBook, Rethink your business for the digital age*, Columbia Business School.

Deloitte (2020). *Tendencias de tecnología 2020*. Deloitte Insights. De: https://www2.deloitte.com/content/dam/Deloitte/co/Documents/technology/(7)%20Horizonte%20siguiente.pdf

***Armando E. Carvajal R**.: Es Ingeniero de Sistemas de la Universidad INCCA de Colombia, cuenta con una especialización en "Construcción de Software para redes" de la Universidad de los Andes y una maestría en "Seguridad informática" de la Universidad Oberta de Cataluña (España). Se desempeña como Arquitecto de soluciones en la empresa Globaltek, organización especializada en Seguridad de la Información y Robótica de procesos. Ha sido conferencista en las jornadas internacionales de Seguridad Informática ACIS Colombia desde 2007; tiene experiencia dictando especializaciones en seguridad informática. Autor del libro "Fundamentos en la Inseguridad de la Información, Tomo I: Un enfoque basado en la práctica", Editorial Académica Española.*