La industria 4.0, tecnología de la información y ciberseguridad

Lo que nos interesa a los ingenieros.

Eduardo Carozo Blumsztein

Introducción

El presente artículo intenta enfocar los principales beneficios, impactos y desafíos tecnológicos del desarrollo de la Industria 4.0, en una visión holística evitando proponer soluciones puntuales.

Industria 4.0, un cambio real

La nueva transformación tecnológica, cambia los modelos de negocios, los liderazgos en múltiples sectores de la economía, los mercados de trabajo y los comportamientos de consumo de la sociedad moderna.

Se espera que su fuerza disruptiva sea la mayor que ha existido y los primeros vientos ya estén revolucionando los sectores financieros, logísticos y comerciales. Existen varios ejemplos ya operativos donde los ahorros generados por la optimización de los procesos o la eliminación de intermediarios superan ratios del 50% en industrias como la aviación, el transporte o la hotelería.

Como se puede visualizar en el gráfico 1, el ingreso de 50 millones de usuarios a *pokemon-go*, sólo tardó 19 días, frente a los exitosos cuatro años de la *world wide web*. Además, debe notarse que esa aplicación fue la primera que pudo implicar seriamente a muchos millones de usuarios en el manejo y gestión de una aplicación de realidad aumentada, logrando una clara interacción entre el mundo físico y el mundo digital.

Por otra parte, cada vez más estamos vinculando los aspectos de control de corte biológico en las nuevas aplicaciones y dispositivos, tanto en animales como en la interacción de lo electrónico, con las funciones biológicas del cuerpo humano. La profusión de dispositivos *wearables* e implantes para resolver problemas cerebrales, cardíacos o nerviosos es cuantiosa y todos ellos tienen su momento de conectividad e intercambio de información con diferentes sistemas y redes.

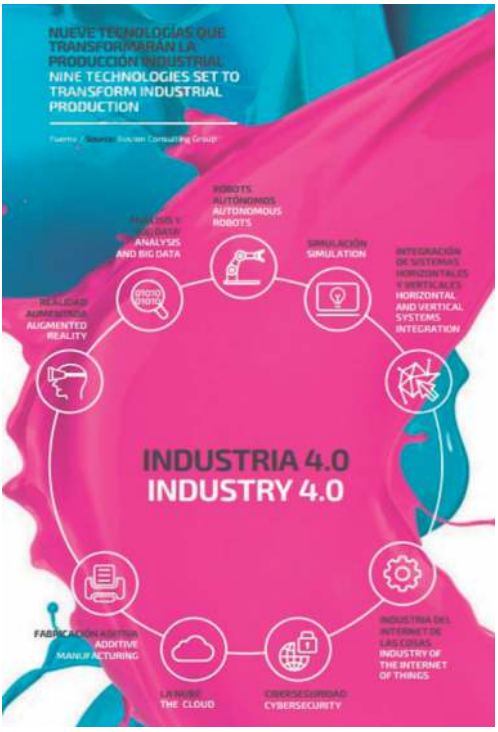
Imaginemos que necesitemos comprar una chaqueta. En no más de cinco años, podremos ordenar en forma verbal a algo que luce como un espejo (con realidad virtual sobrepuesta), en un probador de una tienda, qué estilo, tipo de paño y color, forma de cuello y bolsillos, tamaño y forma de botones, qué interiores y exteriores, etc., y luego superponer la prenda a mi cuerpo

Gráfico 1

con mi ropa actual, verlo en realidad virtual en tres dimensiones y en caso de que sea de mi agrado, darle aceptar al pseudo-espejo para que lo construya.

Al salir del probador las impresoras 3D y los robots de costura, estarán realizando esa prenda exclusiva y en los cinco minutos siguientes nos será entregada. Al salir de la tienda el sistema de reconocimiento facial nos identificará, y asociando el producto que he adquirido, realizará el cobro en forma directa a nuestra cuenta bancaria.

Esta es una escena que hace unos cinco años se consideraba futurista, pero ya es completamente posible y es parte de la nueva revolución industrial, llamada la cuarta revolución industrial.



Esta revolución no cambiará sólo lo que hacemos, sino en buena parte lo que somos. Como mostramos en los ejemplos anteriores, la misma se vivirá en tres espacios esenciales para la humanidad: la física, la digital y la biológica. Durante esta revolución, las industrias elevarán a un nuevo nivel el grado de digitalización de sus procesos y maquinarias.

Algunos países (como Uruguay) consideran estos cambios como una nueva oportunidad de re-industrialización, en la cual se pueda sostener el actual ritmo de crecimiento económico, a pesar del envejecimiento progresivo de su población. En los análisis prospectivos más relevantes se pronostica que se producirán en los próximos 20 años más bienes y servicios que en los últimos 50 años (Siemmens).

En el modelo propuesto por el BCG (*Global Management Consulting*), se observa que la ciberseguridad se considera con el mismo grado de importancia que otras dimensiones más conocidas en el mundo tecnológico como *IoT*, *Big Data Analysis*, Robótica, la nube, etc.

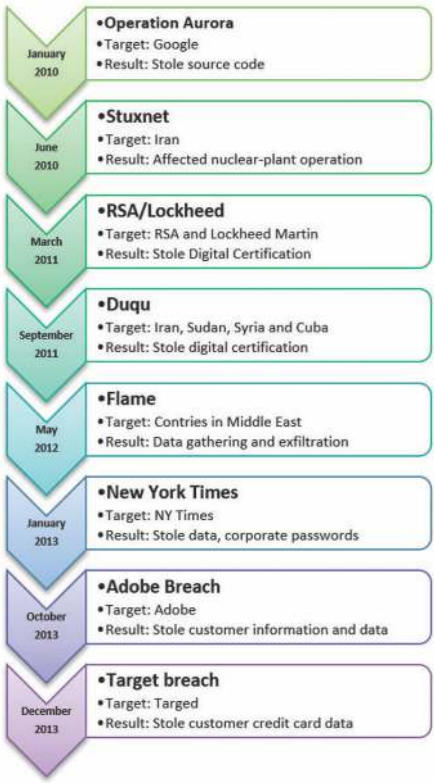
Ciberseguridad y la industria 4.0

¿Qué papel le toca en este escenario futuro a la seguridad de la información, seguridad informática, ciberseguridad y demás definiciones existentes?

En el momento de escribir estas líneas, hemos sufrido el ataque de WannaCry, han sido afectados en pocas

horas más de 300.000 equipos alrededor del mundo. Fue el ataque más visible a nivel global del que hay registro.

La prensa ha escrito ríos de tinta sobre dicho *malware* y la mayoría de las personas no conoce cómo se propaga, pero lo que todos entienden es que su información queda encriptada y que le aparece un aviso que le pide dinero para devolver su información, o la pierden… ¿Qué pasaría si en lugar de robar fotos familiares en PC's particulares, se pudiera robar información asociada a las configuraciones de los sistemas de control automático de las ciudades inteligentes? o ¿se ingresara al servidor de historias clínicas de una entidad médica y se capturara la información de sus pacientes?, ¿cuánto dinero se podría cobrar por esa información? o ¿se tomará el control sobre la nube transaccional financiera de un servicio de *home-banking* de un banco internacional? Estos ataques descritos o ya se dieron o están actualmente ocurriendo y son parte de la historia reciente.



Desde hace un tiempo equipos de investigadores de entidades con alto grado de capacidad financiera están desarrollando e instalando *malware* específico en los sistemas de información críticos alrededor del mundo, con la intención de efectuar ataques selectivos en el momento más adecuado, (o dicho de otra manera: cuando brinde máxima rentabilidad en términos de impacto). Dichas herramientas denominadas APT (*Advanced Persistent Treath*), en general, son utilizadas por agencias de seguridad de las diferentes potencias mundiales y otras entidades no gubernamentales, con finalidades no explícitas. Uno de los ejemplos que tomó notoriedad últimamente es la herramienta *eternalblue*, supuestamente desarrollada por la NSA (*National Security Agency*). La misma fue publicada por el grupo de *hackers* "Shadow Brokers" y en unas semanas la misma fue masivamente explotada para distribuir a nivel global el *ransomware WannaCry*, con el que comenzamos esta sección.

Estas herramientas se desarrollan con el objetivo de pasar inadvertidas y quedar instaladas ocasionalmente por años sin activarse en los diferentes sistemas objetivos. Dado que no se conoce su funcionamiento previo (por ser *zero day exploit*) se vuelve vital tener implementado en toda red que gestione sistemas de información críticos, seguridad en profundidad, gestionando los paquetes en diferentes segmentos de red e instalando inspección de paquetes en cada segmento especializado, no permitiendo la salida de paquetes de datos diferentes a lo esperado por diseño en la red. La implementación en algunos de estos segmentos de soluciones IPS (*Intrusion Prevention Systems*) es también una buena práctica requerida. Para aquellas soluciones basadas en comunicaciones *web* (la mayoría de las actuales), debería ser de uso obligatorio la implementación de un *Web Application Firewall* (WAF).

Las aplicaciones y anexos a los sistemas de información críticos deben ser tratados con el mismo nivel de exigencia que la implementación original, teniendo en cuenta aspectos de seguridad lógica, física y ambiental, debiendo ser testeados en forma detallada y explícita contra fraude, cumplimiento de *performance* y usabilidad, gestionando su ciclo de desarrollo, *testing*, producción y resguardo, en ambientes separados.

Por otra parte, resulta esencial la concientización permanente de las amenazas existentes en los usuarios de los mismos. Es definitivamente el punto más débil de la cadena y los usuarios son víctimas fáciles de múltiples engaños, tanto en la instalación de aplicaciones y utilización de código, (básicamente intentando ahorrar costos con código pirata, o creyendo que todo lo gratis se puede instalar sin validación, etc.), como también en la pérdida de sus credenciales de acceso. Para el acceso a información más sensible debería implementarse a los procesos de autenticación clásicos, algún componente de análisis biométrico adicional,

como reconocimiento facial, de huella digital o similares.

El proceso de migración a la nube, conlleva algunos cuidados extraordinarios en los procesos de control de acceso y gestión de interconexiones y es necesario incorporar además algunas barreras de criptografía avanzada, y en lo posible *firewall* de acceso a bases de datos.

Integridad y transparencia de los contratos en la Revolución 4.0

En el año 2016 nace *Ethereum*, basada en tecnología *Blockchain* que permite elaborar contratos inteligentes en forma autónoma y certificada ya sea persona-persona, persona-máquina, máquina-máquina. Estos contratos pueden ser predefinidos, pero se pueden firmar automáticamente y la figura del notario la realiza la *blockchain* en forma inmediata, con los requerimientos de integridad, disponibilidad y confidencialidad que se requieran en cada caso.

Este cambio, provocará un aumento sustantivo de la velocidad de desarrollo de las diferentes redes, porque será posible establecer *Smart-contracts* en tiempo real entre los diferentes dispositivos sin intervención humana. De esa manera, un dron podrá entregar paquetes a terminales de expendios de alimentos robóticas y autónomas, para alimento de humanos y definir en tiempo real las transacciones comerciales necesarias, sin peligro de robos, pérdidas de dinero o de información.

La gestión de los contratos por la *blockchain*, posibilita dos aspectos fundamentales desde la visión de ciberseguridad, además de la validación automática: la Integridad y Disponibilidad, de información clave. Una red basada en la tecnología *blockchain* en

la medida que va evolucionando ciclo a ciclo, permite que la información contenida en los contratos se vaya haciendo más estable e inmutable, convirtiéndose en un grupo de transacciones aseguradas y verificables por los distintos involucrados en tiempo real.

Esto permite integridad, transparencia y sobre todo la interactividad en tiempo real con dispositivos y personas para mejorar las redes comerciales en forma sustantiva. Esta tecnología está llamada a ser el futuro elemento que gestione la transaccionalidad y la vincule con la gestión comercial en forma definitiva.

Adicionalmente, resulta muy fácil generar sistemas de control de trazabilidad de procesos industriales de manera de poder asegurar la calidad de todos los proveedores de una cadena de valor compleja.

Debe considerarse muy seriamente este tipo de soluciones, tanto públicas como privadas, para la nueva Industria.

Conclusiones

Está todo listo para que las cadenas productivas mundiales migren a la Industria 4.0, solo deberán ajustarse las conductas asociadas a aseguramiento de la información (hacerlas más robustas) en todas las fases de desarrollo, producción, telecomunicaciones y desarrollar planes de contingencia y centros de respuesta, porque los problemas asociados a incidentes de seguridad del futuro tendrán un impacto mucho mayor si ocurren.

Es un mundo apasionante donde nuestros técnicos tienen un rol fundamental. Tendremos posibilidades casi infinitas, pero casi todas las nuevas implementaciones dependen tener un robusto sistema de seguridad de la información, nunca deberíamos olvidarlo.

Eduardo Carozo Blumsztein. *Ingeniero con Maestría en Telecomunicaciones. Es gerente de Comercialización de ITC SA. Ha dirigido proyectos en el área de ciberseguridad desde hace más de 12 años, en organizaciones como Antel, Agesic, OSE, en Uruguay, Carboclor, BA-Csirt en Argentina, Senatics y COPACO en Paraguay, EcuCERT en Ecuador, Cicte de OEA, Inteco de España, Proyecto AMPARO de Lacnic entre otros. Ha sido orador en varias universidades tales como UNAM y Politécnico Nacional de México, UPM de España, Universidad de Chile, Universidad de Buenos Aires. Es docente de posgrado del Instituto de Computación de la Facultad de Ingeniería de la Universidad de la República (Udelar) y de grado en Seguridad Informática de la Universidad de Montevideo, integra el equipo de representantes académicos de Criptored de la Universidad Politécnica de Madrid.*