La Ciberseguridad y la Industria 4.0

Johnny E. Urdin González,
Instituto Tecnológico Metropolitano, Medellin Colombia, Maestría en seguridad Informática
urdin-23@live.com

Resumen.- ***La industria 4.0 un modelo que pretende establecer mecanismos que apoyen a los procesos productivos, con interacción directa máquina - sistemas computacionales - humanos, claramente se sabe que detrás de todo este complejo desarrollo se debe implementar mecanismos de seguridad de igual manera complejos para evitar perdidas de información y más aún la perdida del sistema completo, la Ciberseguridad será quien provea formas de mitigar riesgos que comprometan en pequeña y en gran medida la vida del sistema a implementar, el reto de la industria empresarial sera adaptarse a la bien llamada Cuarta revolución industrial (era de la digitalización) en la que todo interactúa para lograr un fin especifico "dar continuidad al negocio, usando tecnología en todos los procesos productivos".***

Palabras claves.- ***industria, organizaciones, producción, seguridad, desarrollo sustentable, innovación tecnológica***

I. INTRODUCCIÓN.

Las ciencias computacionales se han convertido en parte sustancial en las organizaciones, ya sean estas públicas o privadas, tanto en ámbito comercial, administrativo y productivo, la industria 4.0 proporciona una serie de elementos tecnológicos que sin duda ayudarán a las organizaciones de nivel general a la consecución de los objetivos, no obstante hay que tener en cuenta que para la implementación de esta, es importante establecer mecanicismos de seguridad que contribuyan y den soporte a las diferentes implementaciones tecnológicas y así lograr permanentemente la continuidad del negocio. El presente trabajo de investigación pretende mostrar de manera general, a cerca del desafío que deberán asumir las empresas especialmente las de producción para lograr soluciones optimas y sustentables a través de inversión tecnológica, misma que dará un cambio significativo en todos los niveles empresariales.

II. LA INDUSTRIA 4.0

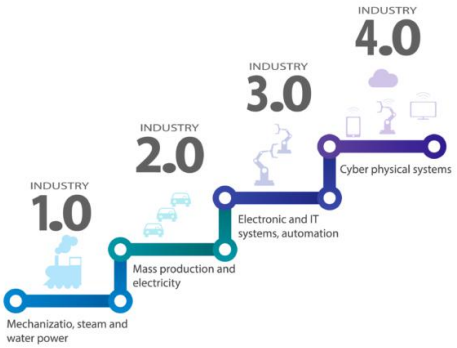

Fig. 1 Desarrollo Industrial

Haciendo un poco de historia de aspectos relacionados con la industrialización, pues notamos que para cada etapa del escalafón que se muestra en la fig. 1, las industrias han tenido que atravesar por una serie de cambios para asegurar su continuidad, esto es, estar a la vanguardia no solo en tecnologías sino también a la par con los profesionales que proporcionen métodos para crear funcionalidades experimentales en todo ámbito y así poder inyectar a sus procesos, mecanismos que proporcionen nuevas fuentes de conocimiento y ademas de la tendencia al desarrollo del comercio como tal.

Al hablar de la industria 4.0, estamos haciendo referencia a que modelos conceptuales de la nueva industria se atribuyen a la anterior con el fin de mejorar los procesos productivos, en este caso la incorporación del Internet de las cosas, la robótica, sistemas basados en inteligencia artificial, ademas de la computación en la nube, electrónica de procesos, realidad aumentada, entre otros, todos estos manejados en tiempo real, para lograr un único objetivo; dar continuidad a la industria, y ademas al desarrollo de esta misma, ya que proporcionará nuevas tendencias que nos dispararán aún mucho más lejos.

Cambio o no ya al solo pensarlo se vuelve algo muy interesante, generalmente al iniciar el proceso de transición existirán un millón de interrogantes, de como?, cuando hacerlo? Estamos preparados para afrontar este reto?, lo ideal es pensar en que este cambio nos generará muchos beneficios y ademas proporcionará una entrada a la conciencia de la inversión tecnológica para el desarrollo de procesos mucho mas rápidos y con tendencias vanguardistas.

En términos generales la Industria 4.0 se atribuye al termino "Fabrica Inteligente" o "Internet aplicado a la Industria", es decir mecanismos informáticos avanzados (Internet de las cosas) se adaptan a la formulación de nuevas estrategias de creación de productos.

Una primera etapa de este tipo de tecnología se contrajo con la nueva forma de venta, a través de canales electrónicos, claro que no esta ligado a la forma de producir, pero si a la manera de agilizar el proceso, una manera segura y eficiente (Distribución electrónica por internet).- este enfoque de distribución logro alcanzar escaños bastante significativos, pues ahora los comercios se manejan electrónicamente hasta el punto de crear también productos no tangibles que inmediatamente llegan al demandante después de realizar la transacción.

Ahora pues bien, la computación en la nube provee una manera rápida y fiable de registrar datos e información útil, la cual estará disponible todo el tiempo; a través de internet, la robótica es otro de los elementos tecnológicos que han marcado significativamente el progreso industrial, pues el uso de robots es muy común, la tecnología inalámbrica y el uso de redes de datos alámbricas proponen interconexión entre los

sistemas computacionales y las grandes maquinas de fabricación, la industria 4.0 intenta reunir todo este conglomerado de tecnología y aplicarlo a los procesos productivos, todo en tiempo real.

Este modelo sin duda obligará a las empresas a invertir mucho mas en tecnología y a disponer de procesos llevados a cabo por profesionales altamente capacitados que manejaran la complejidad del asunto y ademas darán soporte para que el sistema en general no decaiga. Con este razonamiento se pretende interaccionar a todo el sistema de fabricación, y llevarlo a un entorno digital, en la que participen personas y maquinas, dándose soporte unas con otras.

Veamos ahora un Modelo de fabricación Europeo basada en el comportamiento del ecosistema digital, no es difícil darnos cuenta que todo esta interactuado, no sin dejar de lado la tendencia sustentable y de innovación que se pretende alcanzar.

Fig. 2 Modelo Europeo, Informe CODDI - Industria 4.0

III. LA CIBERSEGURIDAD

Ciberseguridad en términos generales se puede definir como la protección de los activos de información a través del tratamiento de las diversas amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran ***interconectados***[1].

Es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Las propiedades de seguridad incluyen uno o más de las siguientes: disponibilidad, integridad (que puede incluir autenticidad y el no repudio) y confidencialidad(ITU, 2008, p.3)[2]

Es la Preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio, definiendo a su vez ciberespacio como el entorno complejo resultante de la interacción de personas, software y servicios en Internet, a través de dispositivos tecnológicos y redes conectadas a él, que no existen en ninguna forma física[3].

La Ciberseguridad es una disciplina relativamente nueva. Los estándares ISO, IEC e ISO / IEC desarrollados en los últimos 25 se pueden aplicar años para ayudar a resolver los desafíos de la Ciberseguridad. Ciberseguridad existente y emergente marcos en todo el mundo hacen referencia a las normas ISO, IEC e ISO / IEC como fuentes útiles de información. Implementar el marco de seguridad cibernética, o un programa de seguridad cibernética, requiere un enfoque iterativo para identificar, evaluar y gestionar el riesgo y evaluar la implementación de marco de referencia. ISO / IEC 27001 ya proporciona un marco de gestión de riesgos que se puede aplicar a priorizar e implementar actividades de Ciberseguridad dentro de una organización[4].

Desde el punto de vista de las organizaciones toda empresa que desee acuñar los modelos de la nueva industria, deberían establecer paramétricas de seguridad que se enmarcan en los artículos citados, las buenas practicas de seguridad proporcionaran una manera bastante eficiente de continuar con la cadena de producción. Otra situación importante que se debe tener en cuenta es la de que hacer cuando los riesgos que se mantienen controlados, de alguna manera exploten. Este último sin duda es un tema que siempre nos ha preocupado y que jamás hay que dejarlo de lado, pues las amenazas vienen de donde uno menos se lo espera, y sin medidas que nos ayuden a controlar pues el sistema en general fracasará.

Los robos más importantes de información pueden afectar a tres tipos de aspectos: Económico.- si te roban las contraseñas o tienen acceso a sistemas online como bancos, Paypal, bitcoins; Lúdico.- se refiere a la pérdida de fotografías, acceso a información sensible como repositorios en la nube; De imagen.- si roban cuentas de las redes sociales, pueden llegar a suplantar la identidad y diñarla. Es necesario que los usuarios sean conscientes de las nuevas normas de juego que imponen Internet y las nuevas tecnologías y conozcan tanto los mecanismos más importantes que utilizan los atacantes como cuáles de nuestras identidades pueden ser interesantes para ellos.

En una encuesta realizada por Telefónica fundación:

Fig. 3 Datos de Telefónica 2015

Como vemos una cifra relativamente alta de usuarios no tienen controles de ningún tipo, podría deberse al desconocimiento o a la no conciencia de los peligros que actualmente existen en internet, dicho de otra manera somos vulnerables todo el tiempo a cualquier tipo de amenazas, y obviamente las organizaciones aún más, pues los ciberladrones

[1] ISACA -2016
[2] ITU-T X.1205:2008
[3] ISO/IEC 27032:2012
[4] ISO/IEC 27032:2012

extraen cosas mucho mas valiosas que una simple contraseña, y atacan al lado mas débil, los usuarios que operan los equipos de computo.

Hay que tener en cuenta también que los términos de Ciberseguridad no solo son para robo de información sino también que un ataque podría dañar todo un sistema computacional interaccionado, y mas aun si nos adentramos en este nuevo campo de la industria 4.0.

Fig. 4 Tomado de le-vpn - PAOLA RINALDI

Para garantizar la Ciberseguridad, hay que delegar un poco de tiempo para investigar e instalar todo el software necesario, y en ocasiones hardware, solo se requerirá la intervención humana para cuando haya que mantener y actualizar todos los sistemas, en la Fig. 4 se muestra solo algunos de los problemas que se tendrían si no se consensúa e invierte en Ciberseguridad.

IV. IMPACTO DE LA CIBERSEGURIDAD EN LAS ORGANIZACIONES

"Ref. [8]. Ciberataque, se puede definir como cualquier ataque a la seguridad de la información a través de una red de comunicaciones pública o privada (Internet o redes corporativas) y es considerado actualmente como un riesgo global que afecta personas, organizaciones y estados, afectando plataformas tecnológicas de cualquier tipo y tamaño al aprovechar las vulnerabilidades de las personas, de las tecnologías y de los procesos".

"Ref. [8]. El origen de la Ciberseguridad se remonta a mediados de los años 80´s con la aparición de los primeros virus y gusanos que infectaban los sistemas de cómputo personal a través de redes de comunicaciones. La aparición y difusión del uso de Internet fue abonando también a la propagación de distintos tipos de "malware" que infectaban a los sistemas de cómputo personal y a las primeras redes de área local (LAN). Con la aparición de las primeras redes de computadoras los ataques se fueron proliferando y de igual modo se hacían cada vez más especializados y enfocados a vulnerar sistemas específicos con objetivos previamente definidos, estudiados y seleccionados por los atacantes".[5]

V. CONCLUSIONES.

Optar por modelos industriales que permitan mejorar los procesos es algo que todas las empresas de producción deberían desarrollar, no solo por el bienestar propiamente dicho de la organización sino para satisfacer de mejor manera la demanda (publico en general).

La conciencia informática y la aplicación de nuevas tecnologías darán un plus a las organizaciones, pero así mismo mientras más avanza, nos vemos cada vez más vulnerables a ataques externos, por esta razón el personal debe ser calificado y capacitado en gran medida para abarcar este complejo ecosistema.

Generar una conciencia de seguridad aplicando políticas, y dando seguimiento al mismo, estableciendo controles avanzados a nivel de usuario y promoviendo el cambio les dará a las organizaciones la tan anhelada estabilidad productiva, siendo capaces de satisfacer aquellos espacios que muchas veces quedan como brechas, finalmente, jefes, operarios, y público en general estarán desarrollándose juntos y obteniendo el provecho de lo que crearon.

VI. REFERENCIAS.

- ✓ [1] Fundación Telefónica, *Ciberseguridad, La protección de la información en un mundo digital,* Primera edición, 28013 Madrid (España): © Editorial Ariel S.A., 2016.
- ✓ [2] Teknisk rapport, *SIS-ISO/IEC TR 27103:2018,* Edition 1, 2018-03-15, 2018
- ✓ [3] F. J.Valencia Duque, *Ciberseguridad,* Colombia
- ✓ [4] C. C. Sánchez, *Trabajo de Fin de Grado Industria 4.0,* Universidad de La Rioja, España: 2016.
- ✓ [5] Y. Cortés, C. Berenice, I.Landeta, J. B. Chacón, J. Aguilar Pereyra, F. Larios Osorio, *El Entorno de la Industria 4.0: Implicaciones y Perspectivas FuturasConciencia Tecnológica*, núm. 54, 2017.
- ✓ [6] A. I. Basco, G. Beliz, D, Coatz, P Garnero, *La industria 4.0, Fabricando el Futuro,* Ciudad de Buenos Aires, Julio de 2018.
- ✓ [7] J. L. del Val Román, *Industria 4.0: la transformación digital de la industria,* Deusto, coddiinforme, 2018
- ✓ [8] J. Garibay, *Web Seminar: El impacto de la ciberseguridad en las organizaciones*, 12 septiembre, 2018

[5] Web Seminar: El impacto de la ciberseguridad en las organizaciones