HORIZONTE DE LA SEGURIDAD INFORMÁTICA EN LA ERA DE LA INDUSTRIA 4.0

Information security horizon in the age of industry 4.0

JOHN ALEXANDER RICO FRANCO[1]

Recibido:12 de abril de 2020. Aceptado:02 de mayo de 2020

DOI: http://dx.doi.org/10.21017/rimci.2020.v7.n14.a84

Resumen

La sociedad actual, gracias a la tercera revolución industrial, se ha apoyado en la tecnología como mecanismo de evolución hacia una forma de vida digital, en donde actualmente los dispositivos computacionales inteligentes cada vez son más comunes y por ende permean con mayor facilidad a todos los ámbitos, y junto con un medio de telecomunicaciones tan masivo y dinámico como lo es la Internet contemporánea, ha permitido visionar un nuevo modelo industrializado para la fabricación de productos y/o servicios de manera automática y autónoma; este concepto es el denominado la cuarta revolución industrial o industria 4.0, en donde la interconectividad basada en la Internet de las cosas y los elementos tecnológicos inteligentes y robotizados, despliegan de manera conjunta y armoniosa un nuevo modelo productivo, basado en una sociedad amante de la tecnología, que asume a esta, como parte integral de las actividades propias de la vida cotidiana y que su uso más que una necesidad se ha vuelto una actividad natural del ser humano[2].

Esta nueva revolución industrial, al igual que toda tendencia tecnológica de alto impacto, viene acompañada de una necesidad imperiosa de ser evaluada y resguardada desde los parámetros propios de la seguridad informática actual, la cual para la ideologia propia de la industria 4.0 puede ser algo limitada o insuficiente, ya que las actividades de seguridad informática existentes no contemplan un entorno tan masivo, distribuido, inseguro y critico como el que propone las plantas de producción de nueva generación, y por ende a la par de cómo las empresas deben evolucionar para poder adoptar los procesos de producción nativos de la cuarta revolución industrial, los especialistas en seguridad informática también deben evolucionar sus conceptos, tecnologías y actividades, para diseñar y gestionar ambientes de producción altamente seguros y alineados con los requerimientos y vulnerabilidades de la nueva generación industrial.

El presente documento tiene como finalidad el presentar como la seguridad informática actual debe empezar a ver a la industria 4.0 como su no muy lejano campo de acción, ya que sin un robusto modelo de protección a nivel tecnológico, cualquier despliegue de funciones industriales de nueva generación sería completamente catastrófico para la empresa que desee evolucionar gracias a la adopción de este nuevo arquetipo empresarial, y sin contar todos los daños colaterales que se puedan presentar de un incidente de tal magnitud. Por ende este articulo se estructura por la presentación de un contexto de que es la cuarta revolución industrial, donde se exhiben algunos fundamentos claves de esta tendencia tecnológica, para luego pasar a exhibir un análisis de seguridad sobre los diferentes segmentos que componen a una fábrica de nueva generación, para así luego identificar algunas de las tendencias más interesantes de ataque que los ciberdelincuentes modernos están empezando a desplegar para vulnerar sistemas industriales complejos, y para por ultimo presentar algunas recomendaciones finales de seguridad basadas en el estudio de las vulnerabilidades nativas de un esquema genérico de manufactura 4.0 junto con los nacientes estilos de agresiones digitales enfocados a esta novedosa pero indefensa directriz industrial de nueva generación.

Palabras clave. Industria 4.0; Internet de las Cosas; Internet de las Cosas Industrial; Malware Industrial; Computación Cognitiva; Seguridad Informática.

Abstract

Today's humanity thanks to the third industrial revolution, has relied on technology as a mechanism of evolution towards a new digital way of life, where today smart computing devices are becoming more common and therefore it started to permeate more easily on different areas of our society, and together with the help of an amazing telecommunications

1 Ingeniero de Sistemas - Especialista en Seguridad de Redes de la Universidad Católica de Colombia, con más de 10 años de experiencia como consultor independiente en proyectos referentes a temas de seguridad informática, criptografía y realización de pruebas de calidad de software. Catedrático Universitario y Docente Investigador del Grupo de Investigación, Desarrollo e Innovación Sostenible (GIDIS) de la Corporación Universitaria Republicana. Correo electrónico: johnricof@gmail.com

medium as massive and dynamic just as the contemporary Internet, has allowed to view a new industrialized model for the manufacture of industrialized products in an automatic and autonomous way; this concept is called the fourth industrial revolution or industry 4.0, where the interconnectivity based on the Internet of things and the intelligent and robotic technological elements, deploy a new and refreshing industrial model.

This new industrial revolution as well as any technological revolutionary trend with high impact for humanity, always are accompanied by an urgent need to be evaluated and safeguarded with the parameters of today's computer security, which may be limited or insufficient for the ideology of the industry 4.0, this is because the existing IT security activities are insufficient for such massive, distributed, insecure and critical environment as the proposed by the next generation production plants and therefore at the same time the companies must evolve to adopt the native production processes of the fourth industrial revolution, the computer security specialists must also develop their concepts, technologies and activities, to design and manage highly secure production environments aligned with the requirements and vulnerabilities of this new industrial generation.

The ultimate purpose of this document is to present how current IT security should begin to see the industry 4.0 as its new field of action, because without a robust technological protection model any deployment of new generation industrial functions it would be completely catastrophic for the company that wishes to evolve thanks to the adoption of this new business archetype. This article is segmented by the presentation of a context by the principles of the fourth industrial revolution, where some key foundations of this technological trend are exhibited, and then go on to exhibit a safety analysis on the different segments that make up a factory of new generation, to then identify some of the most interesting trends of attack that modern cybercriminals are beginning to deploy to violate complex industrial systems, and finally present some safety recommendations based on the study of the native vulnerabilities of a generic factory 4.0 along with the newest styles of digital aggression focused on this amazing but defenseless new generation industrial guideline.

Keywords. Industry 4.0; Internet of Things; Industrial Internet of Things; Industrial Malware; Cognitive Computing and Computer Security.

I. Introducción

La industria se encuentra en la actualidad en un momento de grandes cambios, los cuales son el resultado de una revolución en la manera de cómo las empresas han adoptado a la internet de las cosas (IoT)[2] para la creación de redes de telecomunicaciones inteligentes entre los distintos dispositivos tecnológicos propios de un modelo industrializado moderno; logrando así desplegar ambientes autónomos de intercambio de información entre diferentes actores que participan a través de una cadena de producción moderna, también permite la ejecución de acciones de manera automática por medio de dispositivos robotizados, el controlar todo el proceso productivo de manera emancipada, entre otras actividades que aporten un nivel de independencia a cualquier fabrica que desee evolucionar de manera apropiada hacia la cuarta revolución industrial.

Esta industria 4.0 plantea todo un cambio de paradigma en la producción de bienes, en el cual los productos finales son desarrollados de manera automática y autónoma, donde los sistemas de manufactura son potenciados al ser interrelacionados con múltiples procesos de negocio, tanto internos como externos a través de toda la cadena de producción, gestionando así un ambiente interconectado e inteligente de fabricación ejecutado por máquinas robotizadas, desplegado de tal manera para responder casi en tiempo real a cualquier incidente o modificación que se presente de manera espontánea o planificada.

Pero al igual que en toda tendencia revolucionaria de los últimos años, sea esta tecnológica o industrial, se han visto empañadas por las amenazas y vulnerabilidades propias de cualquier proceso de evolución radical fundamentado en la computación actual, y la cuarta revolución industrial no ha sido la excepción; ya que por ejemplo desde que se han visto los primeros avances de transformación hacia la industria 4.0, se empiezan a vislumbrar tendencias de ataques informáticos enfocados en el aprovechamiento de esta innovación industrializada, que hasta ahora se basan a groso modo en la troyanización de algunos dispositivos de hardware estratégicos para la implementación de una fabrica completamente autónoma o en el despliegue por parte de los atacantes de oleadas de múltiples variantes de malware diseñados para afectar directamente a una naciente línea de producción autónoma, ya sea a sus ele-

2 Red de comunicación que permite conectar dispositivos o "cosas" que tienen capacidad de identificación y procesado computacional, con identidad virtual propia y capacidad potencial para integrarse e interactuar de manera independiente en la red con cualquier otro elemento, ya sea este otro elemento tecnológico o un ser humano [1].

mentos tecnológicos inteligentes pero aún algo inocentes o a sus operarios humanos que en muchas ocasiones son el eslabón más débil de un sistema empresarial; todo esto en búsqueda desplegar procesos criminales de espionaje industrial o hasta llegar a sabotear las fabricas 4.0 y hacerlas inservibles al truncar a toda la línea de producción automatizada por un tiempo indefinido hasta que los dueños de la planta paguen un millonario rescate y en el mejor de los casos logren recuperar la factoría secuestrada.

Y es por este entorno industrial tan interesante que las nuevas estrategias de seguridad informática enfocadas para el aseguramiento de fábricas de nueva generación deben como primer objetivo el priorizar los riesgos autóctonos de estos modelos autónomos industriales, donde se deben especificar políticas de protección robustas y altamente infundidas en toda la empresa, para así poder fundamentar e impulsar la automatización de los procesos básicos de aseguramiento a través de toda la línea de producción del taller de cuarta generación resguardado; entonces para lograr esta meta se deben endurecer y mecanizar las medidas de seguridad informática y en general de TI de toda la organización y que estas se encuentren alineadas con las de sus asociados, en búsqueda de no solo identificar amenazas y ataques una vez estas se estén materializando, sino que se puedan anticipar y solucionar antes de que sean aprovechadas por un conglomerado de ciberdelincuentes; además se deben mejorar los mecanismos de comunicación con cada nivel de la fábrica, los cuales deberán ser utilizados para anunciar masivamente cualquier cambio interno o externo referente a actividades de seguridad computacional, lo cual abrirá canales bilaterales de identificación de puntos y dispositivos críticos y/o vulnerables dentro de la planta autónoma o de parte de alguna otra empresa coparticipe, en búsqueda de reconocer los eslabones débiles dentro de la cadena de producción distribuida multiempresarial al desplegar una alta visibilidad a través de todas la operaciones desarrolladas, así que con la fusión de estas dos macro actividades básicas pero esenciales se puede diseñar y desplegar una estrategia primitiva y nutriente de seguridad, apropiada y ceñida a las necesidades de las nuevas organizaciones refundadas bajo los principios de la cuarta revolución industrial, de la cual se puede empezar a construir un modelo más avanzado y especializado para dicho fin.

II. ¿Qué es la cuarta revolución industrial?

Cronológicamente cuando se habla de las eras de la industria, se puede segmentar en cuatro hitos que se basan en el aprovechamiento de ciertos avances específicos, donde la primera revolución industrial o industria 1.0 se basó en la explotación del agua y del poder del vapor para mecanizar ciertos procesos de producción, la industria 2.0 fue impulsada por la adopción de la electricidad para masificar y potenciar los procesos internos de las fabricas y la tercera revolución industrial se fundamento en el uso de la computación y sus derivados para automatizar manufactura de productos industrializados. El concepto de la industria 4.0 nace en Alemania, pero era previamente vislumbrado a nivel mundial bajo los conceptos del internet industrial o fabrica inteligente o producción autónoma, entre otros sinónimos[2].

Técnicamente hablando, la cuarta revolución industrial se basa en la sistematización de la fabricación y en la evolución digital de los procesos propios de una fabrica eficiente, en donde a nivel de la línea de producción, la propuesta de las fábricas 4.0 se fundamenta en sistemas inteligentes interconectados que abarcan a la mayoría o a todos los dispositivos tecnológicos estratégicos de la planta de producción.

De manera más detallada, el concepto de la cuarta revolución industrial se fundamenta totalmente en la convergencia de tecnologías digitales, físicas y biológicas, como una única metodología que cambiará el mundo industrial tal como se conoce actualmente. Esta cuarta revolución industrial o industria 4.0, no se define solo por un conjunto de tecnologías emergentes en sí mismas, sino por la transformación hacia nuevos sistemas que están construidos sobre la infraestructura de la transición digital previa, que fue la tercera revolución industrial, la cual se estipulo desde mediados del siglo XX, con la llegada de la electrónica, el impulso de la tecnología de la información y de las telecomunicaciones, junto con su masificación de implementación en distintas áreas del desempeño humano, desde simples tareas diarias hasta complejas operaciones científicas, empresariales, financieras, militares, etc.[2] [3].

Este nuevo modelo de producción masificado se fundamenta de varias tendencias tecnológicas modernas, por lo que no se podría concebir la idea de una fabrica completamente automatizada y autónoma sin el incremento evolutivo de la capacidad de procesamiento y la reducción del tamaño de los dispositivos tecnológicos aplicables a ambientes industrializados, que habilitan no sólo interconectar dispositivos industriales que habitualmente se encuentran aislados sino que además dispongan de cierta inteligencia para actuar en función de los datos que generan o reciben, gracias a su fundamentación en la computación en la nube[3] y de la internet de las cosas.

Y es por este caldo de cultivo y las condiciones dadas tanto tecnológicas, industriales y humanas, que esta industria 4.0 propone la automatización total de la manufactura, gestionada y ejecutada por sistemas ciber-físicos[4], concebidos y desarrollados bajo la simbiosis del internet de la cosas (IoT) y la computación en la nube; estos sistemas ciber-físicos están diseñados para combinar la maquinaria de producción física con tecnologías digitales, para así desplegar una línea de producción autónoma capaz de tomar decisiones descentralizadas y de cooperar a través de la Internet con otros sistemas computacionales similares y/o con expertos humanos, para así desarrollar plantas de producción emancipadas que desarrollen redes inteligentes de trabajo, con el fin de que en un futuro no muy distante se puedan controlar por sí mismas a lo largo de toda la cadena de producción; para así liberar a los seres humanos de estas actividades un poco rudimentarias y repetitivas, y avanzar hacia nuevas tendencias de mercado, potenciar productos y/o servicios nuevos e ir innovando la investigación industrial.

Uno de los grandes impulsores de esta naciente revolución industrial es la evolución de la internet de las cosas (IoT) hacia una internet de las cosas industrial (IIoT)[5], concepto mucho más complicado de evaluar debido a que este se refiere a sistemas de mayor complejidad compuestos a partir de otros sistemas y que son capaces de aprender las interacciones que tienen con el mundo físico propio de una planta de producción, de forma que convierten los entornos de fabricación industrial en inteligentes, pero que facilitan la interconexión de diferentes dispositivos inteligentes y maquinaria robotizada en una red única y altamente condensada; tendencia que genera la aparición de nuevos elementos nativos de las plantas industriales modernas, como lo son máquinas inteligentes de ensamblaje de alta precisión totalmente robotizadas y los sistemas de control industrial (ICS), donde este último dispositivo se está divisando como uno de los posibles puntos de interés para los ciberdelincuentes al momento de querer comprometer a una entidad industrializada de nueva generación, debido a que estos son los responsables de monitorear y controlar a los distintos elementos tecnológicos estratégicos de una fabrica 4.0, hecho que los convierte en un punto de cosecha de información sensible industrial bastante aprovechable y en un aliado estratégico al momento de desplegar alguna actividad criminal sobre la cadena de producción propia de la cuarta generación industrial [7].

A futuro, se contempla que serán los países más avanzados los que adoptaran con mayor facilidad y rapidez, los cambios provenientes de esta nueva revolución industrial, pero serán las economías emergentes y países en estado de evolución los que podrán sacarle mayor beneficio en el largo plazo, ya que se estipula que la industria 4.0 tiene el potencial de elevar los niveles de ingreso globales y mejorar la calidad de vida de poblaciones enteras. Sin embargo, el proceso de transformación sólo beneficiará directamente a las economías y países que sean capaces de innovar y ajustarse a esta inevitable tendencia industrial, por eso desde ya se

3 Cuando se refiere al concepto de computación en la nube (Cloud Computing) se habla sobre la tendencia tecnológica que permite ofrecer servicios de computación sin necesidad de realizar instalaciones de software o cambios de configuración o mantenimiento en los equipos de computo en los cuales se ejecutan dichos servicios, buscando así implementar una prestación de servicios computacionales a través de una red de datos; siendo la Internet su mayor canal de comunicación, debido a su alto impacto global [4].

4 Concepto de dotar a los componentes u objetos físicos típicos de cualquier entorno industrializado de trabajo, de capacidades de computación y de comunicación para convertirlos en objetos inteligentes, los cuales permiten así superar a los simples sistemas empotrados actuales en cuanto a capacidad, seguridad, escalabilidad, adaptabilidad y usabilidad, pudiendo trabajar en conjunto formando ecosistemas distribuidos y totalmente autónomos [5].

5 Es una tipología de IoT donde las "cosas" a interconectar son las máquinas, personas y objetos dentro de en un ambiente industrializado [6].

evalúa que aquellas empresas que no se adapten a la industria 4.0, colapsarán al ser superadas inclementemente por la competencia que si logre superar el umbral de adopción de esta nueva revolución empresarial [8].

Ya en lo referente a las actividades laborales realizadas por los seres humanos en plantas de producción de nueva generación, se vislumbra que estas labores también sufrirán un cambio radical al momento de implementarse en fabricas totalmente autónomas, el paradigma de acción de las personas evolucionará hacia actividades que en la actualidad no existen, en empresas que usan tecnologías nuevas y posiblemente desconocidas, basadas en los modelos productivos 4.0, y probablemente bajo condiciones de interacción industrial que ningún ser humano previamente haya experimentado [9].

III. Evaluacion de seguridad informática referente a la industria 4.0

Para poder analizar cómo se debe enfocar la concepción de la seguridad computacional sobre modelos productivos de nueva generación, se van a realizar dos actividades primordiales; la primera es la evaluación de riesgos y vulnerabilidades de los diferentes componentes de una planta genérica propia de la visión de la cuarta revolución industrial y la segunda un repaso de los más llamativos hitos referentes a ataques específicos a ambientes de producción que se han presentado en los últimos años, para así poder identificar cuáles son las posibles necesidades y requerimientos para el aseguramiento y fortalecimiento de fábricas automáticas y autónomas, y la tendencia de actuación que están tomando los ciberdelincuentes para el aprovechamiento de una tendencia tan interesante, riesgosa y vulnerable como lo es la industria 4.0.

3.1. Análisis de los componentes y de sus vulnerabilidades de una planta de nueva generación

Las plantas de fabricación inteligentes serán el núcleo de la cuarta revolución industrial, concepto que abarca desde grillas computacionales autónomas, pasando por procesos de logística digital, hasta llegar al uso de sistemas de control altamente sensibles, entre otros dispositivos y metodologías tecnológicas y de manufactura modernos, los cuales se interconectarán entre sí a través de la Internet de las cosas industrial, generando un ambiente de trabajo totalmente integrado donde se logrará que en dichas plantas de producción de cuarta generación las máquinas robotizadas y los demás elementos tecnológicos propios de una fábrica de esta índole se comuniquen bajo un modelo de enjambre apoyado en la computación en la nube, el cual posibilitará el tomar decisiones de manera independiente, sagaz, rápida y oportuna, mientras que se implementarán procesos de inteligencia artificial apoyadas en robots e impresoras 3D para transformar la manera en el cómo se desarrollan los productos y servicios industrializados de manera automática y autogestionada, actividades revolucionarias que por lógica cambian radicalmente la forma en cómo los seres humanos interactúan en dichas fabricas de nueva generación [10].

Y gracias a la revolucionaria conceptualización de la industria 4.0, también se debe cambiar el paradigma de cómo las empresas reaccionan al momento de verse amenazadas digitalmente, ya que frente a la posibilidad de tener un ecosistema de producción totalmente interconectado y autónomo, se requiere implementar modelos de seguridad informática que sean totalmente transversales a la cadena de producción inteligente, abarcando desde el proceso de diseño hasta el momento de la entrega del producto al cliente, por ende es crítico razonar sobre como son los diferentes componentes o secciones conceptuales de una planta de producción de cuarta generación paso a paso y desde allí vislumbrar cuales podrían ser las vulnerabilidades nativas de cada una de esas instancias de producción autogestionadas:

3.1.1. Radiografía de seguridad informática de un modelo industrial 4.0

3.1.1.1. Segmento # 1 – Realización de actividades fundamentadas en la computación en la nube

El procesamiento computacional posicionado en la nube, habilitará el uso de algoritmos avanzados para la toma de decisiones y algoritmos de análisis en tiempo real, entre otros métodos basados

en la computación cognitiva[6], que permitirán alimentar los distintos procesos industriales 4.0 desplegados por la cadena de producción de nueva generación.

Esta es una fase crítica del funcionamiento de una planta de nueva generación, ya que para nadie es un misterio que la Internet actual es bastante insegura y muchas veces utilizada de manera desprolija por parte de los responsables de las telecomunicaciones digitales a nivel empresarial, ya que usualmente estos procesos se descuidan en búsqueda de reducciones económicas y/o de flexibilidad para la implementación de nuevos servicios basados en el protocolo IP; pero con la llegada de la transición de múltiples procesos computacionales empresariales hacia la nube, que anteriormente se hacían internamente y por ende resguardados en las organizaciones, ha impuesto una nueva mentalidad sobre la importancia de la Internet en modelos industrializados actuales y aun mas con la inminente llegada de las fábricas 4.0 fundamentadas en la Internet de las cosas industrial, donde un "simple" hurto de datos digitales críticos puede llegar a comprometer salvajemente a toda una línea de producción multiempresarial autónoma a niveles catastróficos [10].

3.1.1.2. Segmento # 2 – Cadena de producción inteligente y autónoma:

Genéricamente hablando, una línea de producción de cuarta generación se conceptualiza a través de dispositivos autómatas de ensamble, sistemas de cómputo y control que se interrelacionaran a través de una red de componentes industriales interconectados por medio del protocolo IP, ya que con la fusión de estos elementos se gestionará un ambiente de trabajo completamente integral donde todos estos módulos se comunicaran digitalmente para desarrollar reportes automáticos de desempeño y para la realización de tareas de operación y mantenimiento remotas o locales, o completamente independientes, según sea al grado de avance en inteligencia artificial adoptado por la empresa dueña de dicha cadena de producción 4.0 [12].

De manera específica en referencia a la línea de fabricación 4.0, esta se fundamentará en dos elementos de producción, los primeros serian los robots de ensamblado industrial, cuya actividad sería la de desplegar todas las actividades de producción automatizadas y los segundos serian las impresoras 3D, con las cuales se agilizarían los procesos de desarrollo de prototipos y de impresión de elementos detallados de los productos a desarrollar.

Desde el punto de vista de la seguridad informática, se debe resaltar que el canal de comunicación entre los procesos inteligentes fundamentados en la computación en la nube y el taller inteligente que los aprovechará, será diseñado y gestionado para que los distintos dispositivos autómatas de producción y los sistemas de computo y de telecomunicaciones de la planta inteligente se entrelacen de manera transparente y nativa para trabajar autónomamente, generando una única red de manufactura industrial, distribuida, autogestionada y masiva, hecho el cual presenta un gran riesgo desde el punto de vista de la seguridad computacional, ya que como es lógicamente previsible, las comunicaciones basadas en el protocolo IP contemporáneas no son lo suficientemente robustas y seguras para poder desplegar estos procesos tan delicados y críticos para el funcionamiento protegido de una fábrica de nueva generación; ya que en varias ocasiones los responsables de la seguridad informática a nivel empresarial en búsqueda de una reducción de costos, garantizar agilidad de procesos o por simple pereza, pueden llegar a dejar bastas zonas de red débilmente resguardadas o simplemente sin supervisión, creando un escenario ideal para un atacante que desee robar información sensible de la empresa y/o bajo la ideología de la industria 4.0 llegar al punto de secuestrar a la línea de producción al realizar modificaciones tóxicas en los protocolos de mantenimiento y/o de operación remota.

6 La computación cognitiva es un modelo de simulación de procesos propios del pensamiento del ser humano bajo una estructura tecnológica inteligente donde se implementan algoritmos de aprendizaje mecanizado e independiente; estos sistemas obtienen conocimientos provenientes de minas de datos especializadas de donde se gestionan sus conclusiones a partir de los distintos datos provenientes de estos repositorios expertos al refinar sus deducciones por medio de reconocimiento de patrones, pudiendo así anticipar nuevas inquietudes y estructurar soluciones tanto para problemas conocidos como para potenciales [11].

Ya sobre los dispositivos nativos de una cadena de producción de nueva generación se puede inferir que:

- Las impresoras 3D siempre tendrán un halo riesgo latente, el cual radica en el hecho de que estas van a manejar los planos de modelado de piezas clave de la línea de producción y/o de los productos finales, por lo cual el robo dicha información sensible que estas van a contener, puede convertirse en una actividad muy apetecida por parte de los cibercriminales, ya que estos planos pueden ser vendidos a la competencia de la empresa vulnerada bajo el marco del espionaje industrial.

- En lo referente a los dispositivos robóticos, siempre los atacantes pueden infectarlos a través de malware a la medida para afectar su correcto funcionamiento, hasta el punto de frenar a la línea de producción al secuestrar remotamente a elementos de ensamble estratégicos, para así posteriormente pedir un rescate de estos si se desea recuperar la fábrica autónoma confiscada criminalmente.

3.1.1.3. Segmento # 3 – Modelos de suministro y almacenaje de cuarta generación

Bajo la premisa de la industria 4.0, los procesos de aprovisionamiento y de almacenamiento de insumos requeridos por la fábrica inteligente para su operación, se estipulan que serán realizados de manera automática por medio de vehículos autónomos que interactúan directamente con los robots de la línea de ensamblado, tanto para el aprovisionamiento de los insumos básicos para la banda de producción como para cuando el producto ya se encuentre finalizado y se requiera su almacenamiento en bodega para después ser despachado a los distribuidores encargados de su entrega a los clientes finales [10] [12].

En el momento de gestionar procedimientos de abastecimiento y de bodegaje completamente automatizados, estos pueden verse vulnerados bajo el aprovechamiento de riesgos de seguridad informática provenientes de los dispositivos robotizados para este fin, los cuales pueden verse fuertemente afectados en el momento que se desplieguen ataques de denegación de servicio por parte de ciberdelincuentes que bloqueen el correcto funcionamiento de los vehículos autónomos, esto en búsqueda de obstruir a la cadena de aprovisionamiento y/o de almacenaje de la planta de producción de nueva generación y por ende obstaculizar su correcto funcionamiento hasta llegar a un punto quiebre y hacerla suspender labores debido a improductividad por escases de materia prima o ahogarse por sobreproducción represada debido a fallas en el almacenamiento de los productos previamente finalizados.

3.1.1.4. Segmento # 4 – Sistemas de control

En una cadena de producción inteligente y completamente autónoma, se desplegarían variados tipos de sensores de vigilancia incrustados en las diferentes máquinas que compondrían el proceso de producción, estos sensores alimentarían directamente a un software de control basado en la inteligencia artificial que sería el directo responsable de administrar y vigilar a todos los procesos desarrollados por la factoría 4.0, acciones que irían desde la detección de sectores de la línea de producción que empiezan a volverse obsoletos y la solicitud automática de su actualización hasta la toma de decisiones menos trascendentes como lo es la automatización de las tareas de recarga de los insumos de las impresoras 3D [12].

Desde la visión de la seguridad informática es crítico evaluar la importancia que tendrían los sistemas de control industriales (ICS) desplegados a través de toda una planta de producción 4.0, ya que estos dispositivos cuando no se encuentren completamente resguardados, pueden llegar ser una verdadera pesadilla para la implementación de las metodologías de trabajo presentadas por la cuarta revolución industrial, puesto que por labor estratégica que estos desempeñarían en el proceso de automatización de una cadena de producción inteligente pueden llegar a convertirse en un vector de ataque ideal y por ende contundente para cualquier criminal que desee vulnerar a una fábrica de nueva generación [7].

Los sistemas de control industrial (ICS) actuales, es un concepto general que engloba a diferentes tipos de sistemas de control computarizados que son aplicados en un modelo industrial formalizado, los ICS congregan a controles sistematizados como los sistemas de control distribuidos

(DCS)[7], los sistemas de supervisión, control y adquisición de datos (SCADA)[8] y controladores lógicos programables (PLC)[9]; hecho que hace que los ICS sean sistemas de control híbridos altamente simbióticos, donde los sistemas de evaluación que agrupa son contemplados como un único modelo, robusto y completamente aglomerado; por ende al momento de evaluar una arquitectura de control ICS en un entorno de producción propio de la cuarta generación industrial, no se deben estudiar independientemente a los sistemas SCADA, DCS y PLC de manera individualizada sino como un único sistema de control industrial.

Entonces bajo la ideología de la industria 4.0, formalmente se estipula que un sistema ICS acopiará un grupo de elementos de control que interactuaran entre sí para la correcta vigilancia de un proceso industrial completamente automatizado, sin importar cuales estos sean, siempre y cuando estos sean los apropiados para la vigilancia de la línea de producción inteligente a resguardar; estos sistemas de control unificados trabajaran con el uso de sensores que alertaran sobre cualquier incidente o actividad inusual sobre el proceso controlado bajo los parámetros suministrados por algunas variables de evaluación previamente indicadas por los especialistas humanos, estos sensores alimentaran a herramientas especializadas en diagnostico y mantenimiento remoto, las cuales serán utilizadas de manera distante por especialistas humanos para prevenir, identificar y/o recuperarse de fallos en la cadena de producción o para suspender operaciones anormales sobre el proceso controlado, pero estos sensores también podrán enviar información directamente a un controlador ubicado físicamente en la planta, el cual realizará las mismas tareas pero de manera local; estos escenarios de despliegue de sistemas de control industrial dependerán del nivel de autonomía de la fabrica y de su grado de integración con los principios de la cuarta revolución industrial.

Estas actividades remotas o locales de control serán acompañadas de elementos actuadores los cuales serán utilizados para corregir directamente sobre la línea de producción los incidentes detectados previamente por los sensores; todo este ciclo de detección, diagnostico y corrección se realizará de manera autónoma en forma de circuitos repetitivos, que bajo la metodología de los ICS contemporáneos se llama bucles de control y estos circuitos son programados, ejecutados e inspeccionados a través de una interface humano – máquina (HMI), por la cual el experto humano puede gestionar todas las actividades del sistema de control industrial desde la configuración de los actuadores y de los sensores, pasando por el control de los algoritmos de vigilancia, hasta observar el estado del proceso controlado acompañado de información histórica de consulta sobre toda la cadena de producción evaluada.

Ya desde la dogmatica de la seguridad computacional, como primera instancia se debe referir que inicialmente los sistemas ICS actuales fueron concebidos para ser desplegados en ambientes industriales aislados desde todo punto de vista, hecho el cual los hace completamente seguros frente a ataques remotos de ciberdelincuentes, ya que la única manera de acceder a estos es físicamente en

7 Son sistemas de control industrial modernos compuestos por múltiples procesadores independientes que son asignados a distintos puntos de control dentro de una planta industrial automatizada, pero que se encuentran interconectados entre sí a través de una red de comunicación para el despliegue de un sistema enjambre de control central, pero sin perder su esencia de trabajo individual, ya que su gran característica es el poder aislar y sectorizar los procesos de vigilancia, logrando así que frente a un fallo, este se encapsule exclusivamente al procesador afectado y no se llegue a afectar a toda la línea de producción [13].

8 Los sistemas de supervisión, control y adquisición de datos (SCADA) son sistemas computarizados especializados en la recopilación y análisis de datos en tiempo real, ideales para la monitorización y control de procesos industrializados modernos; grosso modo se puede inferir que estos se componen de distintos elementos de software y de hardware, donde los dispositivos físicos son los responsables de compilar y distribuir datos provenientes de la línea de producción al sistema de software, el cual almacena y procesa dicha información, y la utiliza para gestionar informes de supervisión y control, los cuales serán presentados a los expertos humanos de manera oportuna y bajo formatos normalizados para dicha actividad, gestionando así alertas cuando las condiciones de trabajo se vuelven inestables y por ende potencialmente peligrosas [14].

9 Los controladores lógicos programables o autómatas programables son dispositivos computacionales modulares programados para la ejecución de una actividad en particular dentro de un proceso de producción automatizado, los cuales han llegado a reemplazar a los modelos de control clásicos basados en secuenciadores de tambor, relés mecánicos, interruptores, entre otros dispositivos maquinales tradicionales, los cuales ya son obsoletos frente a los requerimientos propios de la filosofía de la industria 4.0; ya que los PLC si generan información digital de su operación, la cual es utilizada para su retroalimentación a través de los ICS para orientar las acciones de mejora requeridas para potenciar o recomponer, de manera local o remota a una cadena de producción industrial autónoma [15].

zonas resguardadas en las instalaciones de la planta industrial, pero con la apertura proveniente de la Internet de las cosas industrializada propia de la de las fabricas 4.0, los sistemas de control estratégicos van a perder su capa de protección implícita e inexpugnable, haciéndolos completamente vulnerables frente a los riesgos y amenazas de un ambiente tan peligroso como lo es la Internet, hecho que es un riesgo altamente sensible para cualquier empresa que desee convertir a su línea de ensamblado tradicional en una de nueva generación, debido a la delicada labor que los ICS desarrollan dentro de un proceso de producción completamente automatizado.

Y de igual manera que cualquier dispositivo tecnológico, la protección los ICS se basa en los tres pilares icónicos de la seguridad informática, que son la disponibilidad, integridad y confidencialidad de estos y de los datos sensibles que contienen y manipulan [16]:

- Disponibilidad: Garantizar que la información defendida siempre se encuentre disponible para los actores que tienen la aprobación para acceder a ella por parte de sus legítimos dueños.

- Integridad: Se debe certificar que la totalidad de la información resguardada se encuentre completamente protegida y manteniéndola exactamente como fue generada originalmente, para garantizar que no se puedan realizar modificaciones parciales o alteraciones totales a dichos datos por parte de terceros no autorizados para dicha actividad.

- Confidencialidad: Impedir la divulgación de los datos sensibles a entes externos no avalados, en donde la información solamente será consultable con el debido y acreditado permiso.

Y teniendo en cuenta a estos fundamentos básicos de seguridad informática y el funcionamiento y la importancia de los sistemas de control industriales, algunos de los riesgos propios de estos pueden ser:

- Los sistemas de control industrial actuales al ser mecanismos bastante robustos y aparentemente seguros al estar implementados en ambientes de trabajo resguardados, hacen que los distribuidores de estos se confíen y descuiden los procesos de actualización y parcheo sobre las vulnerabilidades detectadas en sus productos, haciendo que estas actividades de reajuste o corrección sean habilitadas semanas o meses después de que es identificada una amenaza, generando brechas de seguridad en la ventana de tiempo entre la detección del problema y de su solución.

- Los ICS al ser desplegados sobre toda la línea de fabricación, pueden llegar a generar caídas intencionales de producción bajo efecto dómino, las cuales se podrían accionar en el momento de interferir con el correcto funcionamiento de dispositivos estratégicos de una fábrica de cuarta generación; ya que al generar modificaciones insospechadas o adversas desde sistemas de control industriales vulnerados por infección de malware a mecanismos tecnológicos clave, se pueden afectar colateralmente a otros elementos de la línea de producción inteligente y así sucesivamente hasta hacerla colapsar.

- En cuanto a la conectividad de los ICS con redes de datos basadas en el protocolo IP, estos dispositivos modernos vienen actualmente preconfigurados de fabrica con especificaciones de acceso a la herramienta, de encriptado y de seguridad general estandarizados, por ende altamente conocidos tanto por los especialistas industriales como por los delincuentes informáticos que desean aprovecharse de estos, al conocer de antemano sus credenciales de acceso por defecto, la manera en cómo estos cifran los datos que generan y manipulan, entre otros conceptos de funcionamiento que puedan ser aprovechados de manera delincuencial.

- Al ser algo susceptibles a modificaciones externas una vez estos han sido vulnerados, pueden ser utilizados para engañar a los operarios humanos al presentar informes catastróficos de operación previamente manipulados por el atacante, en búsqueda de generar pánico en los opera-

rios y sugestionarlos para que estos realicen actividades de contingencia sobre la cadena de producción, las cuales usualmente son muy drásticas y que afectarían de mala manera a un proceso de fabricación totalmente automatizado.

- Debido a que la actividad propia de los ICS requieren que estos elementos se encuentren trabajando casi en tiempo real y con bajos tiempos de latencia, hace que se conviertan en flemáticos e ineficaces sistemas al momento de ser resguardados por herramientas de antivirus y/o antimalware; ya que estos al estar en constante monitoreo y evaluación de las tareas ejecutadas por su anfitrión, hacen que este se desempeñe ligeramente más lento de lo usual, hecho que es casi imperceptible para la mayoría de las actividades industriales actuales, pero totalmente inaceptable para los requerimientos de las fabricas 4.0.

3.1.1.5. Segmento # 5 – Distribución de los productos finales:

Un proceso industrial 4.0, va a finalizar en el momento en que se haga la entrega automática desde la bodega del producto final a los distribuidores humanos o autómatas para su entrega al comprador, si es a un distribuidor humano allí culminará el proceso autónomo, pero si es por medio de un autómata se finalizará hasta la entrega al cliente [17].

Al igual que en el análisis de la seguridad en los modelos de suministro y almacenaje de cuarta generación, el proceso de distribución de los productos de manera autónoma se verá fuertemente afectado en el momento en que se ataquen los dispositivos autómatas de entrega, puesto que estos al no estar disponibles para realizar su labor, generaran cuellos de botella o directamente una suspensión fulminante del proceso de comercialización de los productos finalizados; eventos desafortunados que introducirán demoras en este proceso final de la cadena de producción 4.0, las cuales posiblemente serán asociadas a incapacidad de cumplimiento por parte de la empresa afectada, o al desconocimiento en el uso apropiado de los recursos tecnológicos aplicados bajo las premisas de la cuarta revolución industrial, entre otras posibles concepciones adversas, que se convertirán en indicadores negativos de productividad, los cuales frente a un mercado industrial tan competitivo como es el proyectado a un futuro no muy lejano, serán fulminantes al momento de querer surgir y diferenciarse gracias a la adopción de nuevas metodologías tecnológicas de última generación.

IV. Tendencias delictivas sobre modelos industrializados modernos

Día tras día, la tecnología se está permeando con fuerza y a profundidad en distintas actividades de la humanidad, desde labores rutinarias hasta complejas funciones militares e industriales; pero a futuro estas acciones computacionales ya no serán meros mecanismos de soporte para el potenciamiento de la productividad de los profesionales humanos, sino que serán un reemplazo total en las actividades cíclicas y por ende predecibles que estos desempeñan en la actualidad, para poder deslindarlos de estas labores redundantes y proyectar a las personas a nuevas áreas de conocimiento originadas y nutridas por la industria 4.0, así como lo hicieron los antiguos hitos transformistas industriales.

Al hacer esta masiva evolución industrial de lo análogo a lo digital, se van a presentar diferentes falencias propias en la adopción de tendencias tecnológicas modernas por parte de modelos de producción clásicos, para el caso de los arquetipos industriales la llegada de la cuarta revolución industrial va a venir de la mano con la Internet de las cosas y la autonomía de fabricación, lo cual va a traer consigo la apertura de las plantas industriales a redes de datos conglomeradas y altamente distribuidas, hecho que va abrir a un modelo de producción bastante hermético hacia sistemas de fabricación basados en la computación en la nube, lo cual por supuesto va a exponer a dichas empresas a los riesgos y ataques propios de un ambiente tan mutable e inseguro como lo es la Internet.

Otro aspecto a tener en cuenta sobre la seguridad informática en ambientes de producción de cuarta generación, es el hecho que por mas futurista que se perciba este nuevo modelo industrial, los ciberdelincuentes contemporáneos ya han

empezado a vislumbrar cual será su papel en este nuevo, interesante e inocente modelo industrial y económico, puesto que ya se han desplegado en la actualidad algunas estrategias criminales que apuntan a afectar determinados elementos clave a ser implementados en plantas de producción 4.0.

4.1. A nivel de software

En los últimos años, se ha visto una marcada insurrección de malware exclusivamente diseñado para atacar a infraestructuras organizacionales industrializadas, este tipo de software dañino se fundamenta en dos mecánicas de operación; la primera se enfoca en vulnerar a empresas especificas en donde se identifica previamente las vulnerabilidades nativas de la víctima con el fin de facilitarle al intruso el acceder a información confidencial de dicha clase especifica de empresa o a infringir su perímetro de seguridad especifico; y la segunda es donde se apunta a cualquier esquema de infraestructura tecnológica asociada al proceso productivo automatizado propio de cualquier fabrica, por ejemplo hay diferentes cepas de malware especializados en vulnerar sistemas SCADA, ya que estos al ser usualmente implementados de manera algo desatendida para garantizar su flexibilidad de acción dentro de una cadena de producción automatizada, se han convertido en uno de los vectores de ataque predilectos de los ciberdelincuentes.

La forma de dispersión y de infección de este tipo de malware especializado en atacar ambientes industrializados innovadores, usualmente inicia desde los dispositivos tecnológicos con acceso a Internet que se encuentran en la periferia de la red de datos de la compañía, en donde el atacante se aprovecha de las vulnerabilidades propias de las aplicaciones de tipo cliente con conexión abierta a una red IP, para así generar el punto de acceso del virus a través de un foco de contaminación inicial y desde allí infectar a los demás dispositivos interconectados al elemento contagiado de nivel cero y así sucesivamente se sigue replicando hasta la instalación del malware a través de toda la cadena de producción contaminada.

Este tipo de malware tan particular tiene como su gran representante y pionero a Stuxnet, el cual fue por primera vez identificado como software nocivo en junio de 2010.

4.1.1. Stuxnet

Se estipula que la meta general de Stuxnet era la de afectar directamente al plan nuclear de países señalados por la comunidad internacional como peligrosos como lo son Irán e Israel, ya que este malware de manera muy prolija afectaba directamente a dispositivos de centrifugado nucleares, al hacerlos trabajar de manera descontrolada hasta llegar a su falla física, imposibilitando así la fabricación de armas nucleares por parte de naciones en guerra o con fines desconocidos, al sabotear el proceso de enriquecimiento de uranio, hecho el cual si no se realiza con la debida precaución y control puede llegar a efectuar una fusión nuclear devastadora [18].

En si Stuxnet atacaba quirúrgicamente a dispositivos de control de procesos industriales de Siemens, que usualmente son asociados a plantas nucleares iranís e israelitas en tareas de centrifugado nuclear.

Este malware fue tan elaborado y peligroso en su momento, que fue concebido para utilizar firmas digitales[10] legales generadas por empresas especializadas y de amplio uso en conexiones seguras entre actores empresariales de alta reputación, hecho que lograba engañar a mecanismos de seguridad profesionales al corroborar que las firmas digitales presentadas por el ejecutable del malware eran de confianza y por ende no se desconfiaba de su instalación y ejecución en un dispositivo industrial resguardado. Hecho que hace pensar que Stuxnet y otras clases de malware industriales de alto impacto, puede que lleven meses o hasta años dispersándose y ejecutándose de manera invisible y afectando silenciosamente a distintos tipos de sistemas computacionales empresariales sin importar su finalidad, desde modelos simples de empresas de pequeña o mediana trascendencia,

10 El concepto de firma digital al igual que la firma manuscrita, es utilizada para confirmarle al receptor de un documento la procedencia de este, logrando así confirmar quien es la entidad autora del mensaje digital y también permite confirmar que el documento no ha sido alterado en el transcurso de emisión a recepción del mensaje, puesto que se puede corroborar si este ha sido modificado desde que este fue firmado por el ente autor [19].

hasta sofisticadas arquitecturas militares, gubernamentales, multinacionales, etc… [18] [20]

Pero Stuxnet aparte de que era completamente furtivo a herramientas profesionales de seguridad informática, se caracterizaba por apuntar directamente a sistemas SCADA aplicables en plantas nucleares, los cuales pueden ser semejantes a los requeridos en una fábrica basada en la cuarta revolución industrial, y que también este se podía actualizar remotamente por parte de sus desarrolladores ciberdelincuentes por medio de descargas que se ejecutaban directamente en la memoria del dispositivo corrompido para así no dejar ningún archivo residual de dichas modificaciones, características que hacen a este virus atómico una verdadera amenaza imperceptible y bastante nociva si se modifica para afectar a una planta de producción 4.0.

De manera técnica se especifica que Stuxnet fue el primer malware completamente enfocado a afectar sistemas industriales automatizados, aunque estos fueran plantas nucleares despliegan un modelo de ejecución similar, sino más complejo que el de una fábrica de cuarta generación, y que también fue el pionero en desplegar una variante de rootkit para controladores programables lógicos (PLC), elementos fundamentales en los sistemas de control industrial (ICS) modernos, el cual hacia que el malware se escondiera directamente en el código del controlador haciéndose pasar por la verdadera función encargada de manejar la velocidad del motor de centrifugado y por ende era descartado en las tareas de análisis de software malicioso [21].

El método de contaminación de Stuxnet era algo simple, este iniciaba infectando a un punto vulnerable de la red de datos de la planta nuclear asaltada y desde ese punto de inserción empezaba a contagiar a todo sistema de control a través de la intranet de la planta, para después reprogramar dichos dispositivos especializados para que afectasen directamente a las actividades de centrifugado nuclear.

En su momento Stuxnet fue bastante eficiente y nocivo, ya que al alterar de mala manera las velocidades de los mecanismos de condensación segura de uranio, generaba distorsiones y variaciones no deseadas en estos dispositivos de alta precisión, haciendo que estos se malograran rápidamente al dañar sus rotores por aumentos desmedidos de presión, entonces se analiza que Stuxnet modificaba los valores dentro del PLC / SCADA responsable de controlar el funcionamiento de dichos motores de centrifugado nucleares, estos ICS siempre funcionaron correctamente pero eran reprogramados con una calibración desmedida por los ciberdelincuentes, haciendo que la presión dentro de las centrifugadoras fuera mucho más alta de lo recomendado por el fabricante, mientras que el rootkit PLC engañaba a los operarios humanos al presentarles valores normales de presión interna, lo cual ocultaba lo que en realidad estaba pasando dentro del procesamiento nuclear hasta que ya era demasiado tarde y saltaran las medias de seguridad propias de los ambientes de procesado atómico para evitar llegar a cualquier incidente catastrófico, pero ya con los rotores de centrifugado destruidos [20] [21].

Al analizar a Stuxnet de manera detallada, se puede apreciar desde el punto de vista estratégico y de estudio, que este malware fue bastante contundente y especifico para afectar a una estructura tecnológica tan segura como lo puede ser la de una planta nuclear, pero en lo referente a su implementación y de recursos tecnológicos aplicados para su difusión y materialización, estos eran genéricos y pueden ser fácilmente replicables para atacar a cualquier atmosfera industrial 4.0.

4.1.2. Flame

Flame fue un malware enfocado a vulnerar sistemas empresariales vástago de Stuxnet, era altamente sofisticado, tanto así que hasta la fecha varios de sus módulos son incomprensibles de analizar de manera tradicional.

Este software nocivo afectaba directamente a equipos de computo con SO Windows, el cual se distribuía a través de la redes de área local, Internet y mediante memorias USB por ejecución automática, el cual poseía módulos especializados para grabar audio, realizar capturas de pantalla, se apropiaba de texto digitado por la victima mediante sus pulsaciones de teclado, filtraba tráfico de red, graba conversaciones vía Skype e intentaba obtener información proveniente de dispositivos Bluetooth utilizados en la organización infectada; actividades delictivas bastante perjudi-

ciales para cualquier ambiente industrializado de cuarta generación. Una vez recopilada la información obtenida de los dispositivos industriales infiltrados, Flame pasaba a agrupar estos datos, junto con los documentos almacenados en el computador vulnerado, estos eran enviados a uno o varios servidores anónimos y delincuenciales dispersos alrededor del mundo; para después ser consultados por los ciberdelincuentes dueños del malware y de allí clasificar la información capturada para luego analizar cómo podían aprovecharse económica y criminalmente de esta [22].

Así como Stuxnet fue el pionero en ser el primer malware especializado para atacar modelos sistematizados industriales, Flame nos enseña lo complejo y destructivo que puede ser este tipo de software malintencionado en estructuras industriales completamente automatizadas y autónomas propias de la industria 4.0.

4.2. A nivel de hardware

A inicios de octubre de 2018, se debelo uno de los mayores incidentes de espionaje industrial y de piratería tecnológica de la actualidad con posibles repercusiones exorbitantes y a largo plazo; ya que afectaba directamente a una cadena de suministros de insumos electrónicos provenientes de China aplicados en diferentes organizaciones a nivel mundial, el cual consistía en la inserción de un ínfimo chip de vigilancia en las placas madre de múltiples servidores utilizados por multinacionales como Amazon y Apple, y en agencias militares y de inteligencia de los Estados Unidos y posiblemente de otros países. Estos chips troyanos, lógicamente nunca fueron parte del diseño original de la empresa fabricante perjudicada, la cual fue Super Micro, ya que estos estaban siendo implementados furtivamente en el proceso de manufactura subcontratada a un taller en China; hasta ahora una de las primeras hipótesis de investigación que se evalúan es que algunos grupos radicales y especialistas del gobierno chino se infiltraron en la fábrica de producción de las tarjetas madre que fueron corrompidas para facilitar el espionaje al gobierno norteamericano y algunas empresas multinacionales [23].

Desde el punto de vista técnico, estos chips troyanos al ser de un tamaño ínfimo, solamente podían guardar una limitada cantidad de instrucciones preprogramadas, por ende este código malicioso solamente podía ejecutar dos tareas, la primera era que el dispositivo corrupto se comunicara remotamente con un servidor anónimo que almacenaba mas malware, y la segunda era preparar al equipo transgredido para descargar y ejecutar automáticamente dicho programa desconocido y desde allí continuar con el proceso de espionaje.

Al momento de publicación del presente escrito, este incidente aun se encuentra en etapas recientes de indagación y corroboración de información, por ende no se cuenta con una explicación veraz y definitiva que ratifique completamente dicho ataque, y es más que entendible que al verse supuestamente vulneradas a organizaciones tan importantes como lo son las agencias militares y de inteligencia de los Estados Unidos y empresas del talente de Super Micro, Amazon y Apple, estos no han hecho ningún comentario oficial sobre esta filtración de información sensible y del uso de dispositivos adulterados que facilitaron su hurto, ni mucho menos de las implicaciones que se puedan presentar sobre la subcontratación para el desarrollo de elementos computacionales críticos en sus operaciones en países tan delicados como lo es China; y es completamente comprensible su posición, ya que es el buen nombre de dichas empresas y organizaciones es el que entra en juego bajo estas sospechas de posible negligencia operacional; pero que se referencia en el presente escrito debido a su repercusión en fabricas 4.0, al estudiar como las amenazas físicas y lógicas a la cadena de suministro de tecnología en cualquier planta de producción autónoma pueden ser tan difíciles de descubrir, comprobar y de mitigar, y como pueden llegar a gestionar de manera casi perfecta ataques de espionaje industrial en entornos empresariales modernos.

Y aunque este desafortunado incidente a nivel de hardware industrializado no pueda ser aun certificado totalmente, su simple formulación ya es un golpe sustancial para la evolución empresarial hacia modelos autónomos de desarrollo de productos bajo la concepción de la cuarta revolución industrial, porque afecta negativamente la percepción de los dispositivos físicos desplegados sobre una cadena de producción totalmente automática; hecho el cual es completamente aislado de las vulnerabilidades provenientes de las redes de datos

inseguras y abriendo así un nuevo y poco habitual vector de ataque industrial; ya que se genera un halo de desconfianza sobre uno de los grandes impulsores y promotores de los avances computacionales de los últimos años, la impresionante capacidad del pueblo chino para el desarrollo de componentes tecnológicos de calidad a bajo costo y con una portentosa tasa de productividad.

V. Sugerencias de seguridad en ambientes industriales de cuarta generación

En la actualidad las empresas de factoría industrializadas, dedican la mayoría de sus recursos y esfuerzos para asegurarse que su línea de producción se encuentra completamente funcional; pero a futuro estas prioridades deben ser radicalmente recalibradas y/o modificadas, ya que la industria de nueva generación va a desarrollar procesos industriales cada vez más perspicaces y autónomos, donde se les deben integrar medidas de seguridad informática robustas y a la medida de las necesidades de las cadenas de producción de cuarta generación, con altos niveles de detalle y consagración, y siempre anteponiendo la seguridad en sus distintos frentes, ya sea al reforzar los dispositivos tecnológicos aplicados a lo largo de toda la cadena de producción 4.0, o estratificando por niveles los permisos de acceso a la Internet, o estandarizando los métodos de autentificación y de cifrado de manera inteligente, rápida y precisa, entre otras recomendaciones practicas para el aseguramiento de una fábrica de nueva generación: [24]

5.1. Recomendaciones generales de seguridad para cadenas de producción 4.0

- Lógicamente se sugiere el uso y despliegue adecuado de distintos mecanismos tecnológicos especializados en seguridad informática en ambientes industriales, como lo son firewalls, sistemas de detección de intrusos, antivirus, tarjetas inteligentes para la identificación de personal, sistemas biométricos, aplicación de procesos criptográficos para el aseguramiento de todas las comunicaciones digitales y tareas de almacenamiento de datos, etc… en zonas estratégicas de la planta de producción 4.0.

- La topología red de datos de la organización debe ser multicapas, donde sucesivamente cada capa interna será más segura y aislada que la anterior, para que en el núcleo de la red se posicionen los dispositivos más críticos y sensibles de la empresa que por ende son los más apetecidos y codiciados por un ciberdelincuente.

- Cifrar toda la información compartida entre los distintos elementos computacionales de cualquier planta de la nueva generación, para así asegurar que, toda la información distribuida tanto internamente como externamente sea resguardada y legible únicamente a los usuarios autorizados para su visualización, garantizando así la defensa de todo dato industrial confidencial y la propiedad intelectual de los productos generados por la fabrica 4.0.

- En la medida de lo posible, se debe concebir una arquitectura de red que permita una separación lógica de la red corporativa (más cercana a la Internet, por ende, se ubica en la frontera de la red de datos empresarial) de la red de producción (en el núcleo productivo de la fabrica y su perímetro más cercano), para así encapsular a los dispositivos vitales de la planta de cualquier ataque remoto.

- Deshabilitar los puertos y servicios no utilizados o inseguros en todos los dispositivos industriales autónomos con acceso a Internet, para así evitar la materialización de brechas de seguridad no deseadas en puntos activos vulnerables de la cadena de producción.

- Implementar estrategias de degradación de los procesos internos de la cadena de producción, por si se llega a presentar algún hecho no deseado, poderlo desarticular fácilmente y por ende evitar una caída de la producción por un efecto de domino adverso.

- Asegurarse que todos los elementos de producción imprescindibles sean redundantes, para que en el momento que alguno de estos falle o se vea comprometido, sea fácilmente reemplazado y que no se afecte la productividad de la empresa.

- Limitar el acceso físico a la planta de fabricación automatizada por parte de desconocidos o de personal no certificado para interactuar con un modelo de producción tan delicado y minucioso como lo es el propuesto para las plantas 4.0.

- Cada vez que se presente algún incidente importante sobre la línea de producción autómata, y se requiera reiniciar todo el sistema, esta actividad debe desarrollarse de manera estructurada bajo un plan de contingencia y de recuperación previamente estipulado y difundido a través de toda la fábrica, el cual debe ser versátil y de rápida ejecución, ya que las demoras presentadas en el proceso de recuperación es tiempo, productividad y dinero perdidos por la empresa.

- Se debe invitar a compañías especialistas en seguridad informática para que sean asociados estratégicos directos de las industrias que deseen evolucionar sus plantas a fabricas 4.0, en búsqueda que en el momento de desarrollar el programa de aseguramiento de la línea de producción de nueva generación, este aliado colabore en todas las fases de la gestión de la estrategia de resguardo, para así aprovechar su experiencia y conocimiento en su área de experticia y que esta sea el directo responsable de identificar las amenazas y vulnerabilidades presentes entre los diferentes actores de la línea de producción autónoma y distribuida, identificar los niveles de prioridad de cada uno de estos riesgos y evaluar como serán mitigados efectivamente; para así apartar parcialmente a los demás entes asociados y a la empresa base de estas actividades especificas de seguridad informática, las cuales se pueden extrapolar de las recomendaciones dadas por los estándares ISO 27005 y NIST SP 800-30, donde su experiencia puede ser mínima o nula, y que estos se enfoquen exclusivamente en sus tareas de producción.

5.2. Recomendaciones generales de seguridad para los sistemas de control industriales (ICS):

- Se deben resguardar a los ICS de cualquier vulnerabilidad que pueda ser aprovechada por un ente criminal o que genere una brecha imprevista que genere un mal funcionamiento de la maquinaria asegurada por el ICS descuidado, esta actividad puede ser muy especifica según el tipo de sistema de control industrial a robustecer, para esto se pueden restringir puertos de comunicación que no se van a utilizar o que sean inseguros, estar en constante actualización del software del ICS, deshabilitar servicios que el dispositivo tenga pero que no serán utilizados, eliminar las credenciales de acceso que vienen por defecto de fabrica, restringir los privilegios de usuario preprogramados, etc…

- Limitar el acceso remoto y físico a los ICS, en lo referente a su resguardo local esta restricción se puede gestionar con la ubicación estratégica de dichos dispositivos en áreas seguras de la fábrica, y remotamente con el uso de firewalls que filtren el tráfico de datos provenientes de la Internet o con el uso de zonas desmilitarizadas para engañar a los delincuentes que logren acceder a las periferias de la red de datos de la fabrica.

- A todo sistema de control industrial desplegado en una planta autónoma que se desee asegurar a cabalidad se debe asegurar bajo los lineamientos de los estándares SP 800-82 del NIST y la ISA-99.

VI. Conclusiones

Que uno de los grandes beneficios que aporta la cuarta revolución industrial es el poder integrar los procesos de tecnología de la información a nivel ejecutivo con los sistemas de operación de la línea de producción, hecho que se representa en un aumento en la efectividad y una reducción considerable de costos, circunstancias que usualmente serán los desencadenantes al momento de tomar la decisión de evolucionar a una empresa hacia la industria 4.0 junto con las tendencias del mercado y de sus competidores; pero desafortunadamente en varias ocasiones estos primeros elementos son los dos únicos factores tomados en cuenta al momento de apropiar una tendencia tecnológica fértil en ambientes industrializados, pero no se evalúan los riesgos asociados a cualquier evolución computacional, ya que muchas veces se vislumbra claramente los beneficios económicos y

productivos pero no se evalúan desde la visión de la seguridad informática.

Es clave que las empresas se concienticen que las actividades propias de la seguridad computacional, no son un gasto implícito propio de la adopción de herramientas tecnológicas de productividad, sino que ya es una necesidad en un mercado cada vez más competitivo y que se está abalanzando hacia la gestión y puesta en marcha de fabricas 4.0; donde la seguridad debe ser un activo más de la empresa, que genera un valor agregado a los productos forjados por la organización, al garantizar la productividad de la cadena de fabricación autónoma bajo la premisa que estas actividades de resguardo se conviertan en un proceso de monitoreo continuo y con la menor cantidad de brechas, claro está sin llegar a afectar significativamente o colateralmente las actividades de manufactura propias de la compañía.

También se concluye que las estrategias de seguridad computacionales en plantas de producción de nueva generación deben fundamentarse en actividades dinámicas y persistentes como evaluaciones constantes de riesgos y vulnerabilidades de los dispositivos tecnológicos estratégicos de la línea de fabricación 4.0, despliegue de distintos elementos de aseguramiento digital y físico, pruebas de penetración a la red de datos de la empresa, protección bajo segmentación por capas de la intranet de la planta, uso de algoritmos criptográficos para el resguardo de la información sensible de la compañía que fluye tanto dentro de la empresa como en su salida hacia entes externos vía Internet, entre otras estrategias de aseguramiento aplicables a una fabrica propia de la cuarta revolución industrial y a su entorno operacional más cercano. Este concepto es crítico, ya que tal como se ha vislumbrado a lo largo del presente artículo, los cibercriminales modernos han empezado a perfilar sus actividades y arsenal delictivo para atacar y comprometer proto-entornos industrializados 4.0.

Que bajo el perfilamiento estricto de los elementos tecnológicos aplicados sobre una cadena de producción 4.0, los ICS son estratégicos y críticos para cualquier infraestructura industrial multiempresarial que requiera ser íntegramente interconectada y autónoma, tal como son contempladas las fábricas de cuarta generación; y que gracias a esta evolución, los sistemas de control industrial se están transformando y desvirtualizando de simples modelos mecánicos de vigilancia a plataformas digitales complejas, pero sin una estructura solida para el resguardo de datos sensibles en redes de información distribuidos y usualmente desprotegidas una vez salen de su perímetro de control, lo cual genera una amplia gama de riesgos que no se tenían planificados en la génesis de estos dispositivos de control industrial.

Y por último y por más evidente que suene o que su indicación esta de mas, se concluye que para poder generar un proceso de transformación digital industrial apropiado hacia las ideologías de la industria 4.0, se requiere de un modelo supremamente robusto de administración de riesgos y vulnerabilidades computacionales, que priorice a todos los fundamentos de la IoT, IIoT, la robótica, la computación en la nube y la informática cognitiva.

Referencias

[1] J. J Gónzales, "*IoT: Interconexión digital, un reto mayor de seguridad*"; Revista Sistemas - Publicación de la Asociación Colombiana de Ingenieros de Sistemas (ACIS); No. 143 Abril / Junio - 2017.

[2] E. Garnica, "*¡La cuarta revolución industrial! Ya está aquí. Una era de transformación digital*"; Gaceta Republicana - Publicación de la Corporación Universitaria Republicana; Año 5 No. 26 Julio / Agosto - 2018.

[3] J. J. Cano, "*Cuarta revolución industrial: Anticipo de un nuevo desarrollo de la humanidad*"; Revista Sistemas - Publicación de la Asociación Colombiana de Ingenieros de Sistemas (ACIS); No. 143 Abril / Junio - 2017.

[4] A. Huth y J. Cebula, "*The Basics of Cloud Computing*"; Documento WEB - PDF; Disponible en [https://www.us-cert.gov/sites/default/files/publications/CloudComputingHuthCebula.pdf]; 2011.

[5] K. Kim y P. R. Kumar, "*An Overview and Some Challenges in Cyber-Physical Systems*"; Documento WEB - PDF; Disponible en [http://cesg.tamu.edu/wp-content/uploads /2014/09/An-Overview-and-Some-Challenges-in-Cyber-Physical-Systems.pdf]; 2014.

[6] J. Conway, "*The Industrial Internet of Things: An Evolution to a Smart Manufacturing Enterprise*"; Documento WEB - PDF; Disponible en [http://www.mhi.org/media/members/15373/ 13111 1777451441650.pdf]; 2015.

[7] A. A. Cardenas, S. Amin y S. Sastry, "*Research Challenges for the Security of Control Systems*"; Documento WEB - PDF; Disponible en [https: // people.eecs.berkeley.edu/~sastry/pubs/Pdfs% 20of%202008/CardenasResearch2008.pdf]; 2008.

[8] P. Bedard-Maltais, "*Industry 4.0: The New Industrial revolution ¿Are Canadian manufactures ready?*"; Documento WEB - PDF; Disponible en [https:// bridgr.co/wp-content/ uploads/2017/06/bdc-etude-manufacturing-en.pdf]; 2017.

[9] M. Crnjac, I. Veza y N. Banduka, "*From Concept to the Introduction of Industry 4.0*"; Documento WEB - PDF; Disponible en [https://bib.irb.hr/datoteka/ 894382.IJIEM_ 24.pdf]; 2017.

[10] H. Heynity y M. Bremicker, "*The Factory of the Future*"; Documento WEB - PDF; Disponible en [https:// assets.kpmg.com/content/dam/kpmg/ es/pdf/2017/06/the-factory-of-the-future.pdf]; 2016.

[11] D. A. Zuluaga, "*Era Cognitiva: Una realidad tangible*"; Revista Sistemas - Publicación de la Asociación Colombiana de Ingenieros de Sistemas (ACIS); No. 142 Enero / Marzo – 2017.

[12] European Factories of the Future Research Association; "*Factories 4.0 and Beyond*"; Documento WEB - PDF; Disponible en [https://www.effra.eu/sites/ default/files/factories40_beyond_v31_public. pdf]; 2016.

[13] P. Holecko, "*Overview of Distributed Control Systems Formalisms*"; Documento WEB - PDF; Disponible en [https://core.ac.uk/download/pdf/8986878. pdf]; 2008.

[14] K. Stouffer, J. Falco y K. Kent; "*Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems*"; Documento WEB - PDF; Disponible en [https://www.dhs.gov/sites/default/ files/publications/csd-nist-guidetosupervisor yanddataccquisition-scadaandindustrialcontrol systemssecurity-2007.pdf]; 2006.

[15] A. R. Kiran, B. Venkat, Ch. Sree Vardhan y Neel Mathews, "*The Principle of Programing Logic Controller and its role in Automation*"; Documento WEB - PDF; Disponible en [http://www.ijett journal.org/volume-4/issue-3/IJETT-V4I3P250. pdf]; 2013.

[16] M. Whitman, "*Principles of Information Security*"; Editorial: Course Technology; 2011.

[17] Deloitte University Press, "*The smart factory: Responsive, adaptive, connected manufacturing*"; Documento WEB - PDF; Disponible en [https:// www2.deloitte.com/content/dam/insights/ us/ articles/4051_The-smart-factory/DUP_The-smart-factory.pdf]; 2017.

[18] J. P. Farwell y R. Rohozinski, "*Stuxnet and the Future Cyber War*"; Documento WEB - PDF; Disponible en [https://www2.cs.duke.edu/courses/common/ compsci092/papers/cyberwar/stuxnet2.pdf]; 2011.

[19] A. Maiorano, "*Criptografía: Técnicas de desarrollo para profesionales*"; Editorial: Alfaomega; 2009.

[20] A. Matrosov, E. Rodionov, D. Harley y J. Malcho, "*Stuxnet Under the Microscope*"; Documento WEB - PDF; Disponible en [https://www.esetnod32.ru/ company/ viruslab/analytics/doc/Stuxnet_ Under_the_Microscope.pdf].

[21] R. Langer, "*To Kill a Centrifuge: A techical analysis of what Stuxnet´s creators tried to archive*"; Documento WEB - PDF; Disponible en [https://www.langner. com/wp-content/uploads/ 2017/03/to-kill-a-centrifuge.pdf]; 2013.

[22] M. J. Caro, "*Flame: Una nueva amenza de ciberespionaje*"; Documento WEB - PDF; Disponible en [http://www.ieee.es/Galerias/fichero/docs_ informativos/2012/DIEEEI34-2012_Flame_ Ciberespionaje_ MJCB.pdf]; 2012.

[23] J. Robertson y M. Riley, "*The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies*"; Documento WEB - PDF; Disponible en [https:// www.bloomberg.com/news/ features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies]; 2018.

[24] M. Ciampa, "*Security+ Guide to Network Security Fundamentals*"; Editorial: Course Technology; 2011.