La Gestión de la Cadena de Suministro en la Era de la

Industria 4.0

IBM

CEL Centro Español de Logística

ÍNDICE DE CONTENIDOS

Carta IBM 03

Carta CEL 04

01 | La sociedad conectada y la Industria 4.0 05

02 | De la cadena de suministro al ecosistema de suministro 10

03 | Las tecnologías y drivers de la Industria 4.0 15

04.1 | CiberSeguridad en el Sector Estratégico del Transporte 21

04.2 | CiberSeguridad en la Industria 4.0 25

04.3 | La Directiva Europea de Seguridad NIS y la Protección de Infraestructuras Críticas 30

05 | Los profesionales del Siglo XXI: Nuevas competencias y gestión del cambio 34

06 | Implicaciones legales de la Industria 4.0 40

07.1 | Caso práctico: Walmart 45

07.2 | Caso práctico: El Sector Cárnico 49

07.3 | Caso práctico: Plataforma Wonder 53

08 | La empresa como sistema complejo adaptativo 58

09 | En busca de nuevas formas de relación entre organizaciones y profesionales para mejorar la eficiencia operativa 64

Apéndice | Autores y Empresas 69

Luis Pérez Ballestero

Consumer Products Industry Lead
en IBM Global Business Services

Vicepresidente del Centro Español de Logística

En la actualidad, en muchos medios de comunicación y foros de debate se está hablando de La Cuarta Revolución Industrial. Esto indica que se está produciendo una disrupción en la sociedad y en la economía que es propiciada por una serie de nuevas tecnologías e innovaciones que están cambiando drásticamente la forma en que los consumidores, las empresas o las instituciones se desenvuelven.

Como veremos en este documento, esta cuarta revolución industrial también llamada Industria 4.0, se desencadena según los expertos, por la confluencia de una serie de tecnologías (Big Data, Internet de las cosas, Cloud Computing, Robotización, Inteligencia Artificial, Blockchain, etc.) que está posibilitando un cambio profundo en la forma de vida de las personas y en los modelos de negocio de las empresas que adoptan estas tecnologías. Pero más allá del análisis de las causas de la revolución y de las tecnologías citadas, nos interesa resaltar las distintas implicaciones en temas tales como la seguridad, los aspectos legales, el impacto en los recursos humanos, los ecosistemas empresariales y, muy en particular, en los aspectos relacionados con la Cadena de Suministro. En efecto, estamos empezando a hablar de la Logística 4.0 que en definitiva no es otra cosa que la aplicación de los conceptos y tecnologías habilitadoras de la Industria 4.0 a los procesos de la Cadena de Suministro.

Por ejemplo, en cuanto a la seguridad, es evidente que con la explosión del volumen de datos que se está produciendo en la sociedad y los miles de millones de dispositivos conectados que existen en el planeta, están apareciendo riesgos que es necesario conocer con objeto de aplicar las herramientas de ciberseguridad requeridas para el nuevo contexto.

Otro de los aspectos más complejos de los cambios que se están produciendo en esta cuarta revolución industrial es el relacionado con las implicaciones legales. Sólo por citar un ejemplo, la proliferación de datos y el almacenamiento de éstos en la nube, han sido algunas de las causas que han derivado en la creación del nuevo Reglamento de Protección de Datos a nivel europeo (GDPR) que tiene fuertes implicaciones en la protección de datos personales en la Unión Europea.

Asimismo, uno de los asuntos más críticos de la Industria Conectada y de la creciente digitalización de la sociedad, es su impacto en los recursos humanos y en las nuevas competencias que se requieren en este nuevo contexto digitalizado. Hace años que se habla de la "brecha digital" y una de las mayores amenazas de esta revolución es que incremente de forma aún más acusada la desigualdad entre ciertos colectivos de profesionales digitales y otros que no hayan adquirido esas nuevas capacidades.

De todas las tecnologías habilitadoras de la Industria 4.0, una de las que pensamos en IBM que va a tener un mayor impacto en la transformación de la cadena de suministro es la llamada Blockchain. Las cadenas de bloques son bases de datos distribuidas que permiten crear un registro compartido e invariable de cada transacción asociada a un activo. Las Blockchains son ideales para gestionar los procesos entre empresas mejorando la visibilidad, la eficiencia y la confianza entre las partes. De este modo, permiten resolver los problemas de vulnerabilidad y costes de las cadenas de suministros tradicionales. Como ejemplo ilustrativo del uso de Blockchain en la cadena de suministro, en este documento se presenta un proyecto que IBM está realizando con Wallmart para mejorar drásticamente la mejora de la trazabilidad de la cadena alimentaria.

En conclusión, tanto en IBM como en el Centro Español de Logística, creemos que estamos viviendo una época de enormes cambios producidos por todos estos factores, y pensamos que los profesionales de la cadena de suministro deben estar atentos a estos cambios para poder aplicarlos en sus empresas. Confiamos que esta guía CEL contribuya a mejorar el conocimiento sobre los retos y oportunidades que la nueva Logística 4.0 puede aportar a los profesionales, a las empresas y a la sociedad en este nuevo contexto.

José Estrada, CLTD CSCP

Director general del Centro Español de Logística

La logística es una disciplina compleja en la que es necesario coordinar recursos, infraestructuras, organización y procesos para poder llevar a cabo la elaboración y distribución de productos o el desarrollo de servicios. Los profesionales de la logística se enfrentan a un reto constante: lograr sus objetivos satisfaciendo al cliente y con la máxima eficiencia de coste y medios.

En esta dinámica, los procesos logísticos requieren de una planificación y coordinación o sincronización con otros actores de la cadena de suministro, muy intensiva en datos. Surge la enorme relevancia de las tecnologías de la información y comunicación en la gestión de la logística actual. Esto no es algo novedoso, ya que la logística ha sido una disciplina que ha evolucionado en fiabilidad y eficiencia de forma espectacular en la última década. Un logro conseguido en gran medida gracias a la fuerte tecnificación aplicada en la gestión y la operativa de los procesos.

La realidad es que nos encontramos en un entorno cada vez más complejo. Un entorno formado por redes globales de suministro en las que aspectos como la visibilidad, la flexibilidad, trazabilidad y seguridad son claves en la interacción entre sus actores. Por otra parte, la tecnificación y robotización de los procesos productivos permiten utilizar la información generada para sincronizarlos con los procesos logísticos y, de esta manera, conseguir una mayor eficiencia. En esta ecuación también se incluyen los clientes y los empleados, que también están conectados tecnológicamente proporcionando una solución end-to-end.

Estos factores configuran el nuevo paradigma que abordamos en este estudio como Industria 4.0. Un concepto acuñado en 2011 por el gobierno alemán con el objetivo de potenciar la productividad en la actividad industrial en una economía muy desarrollada y de altos salarios como la alemana. El concepto también hace referencia a la "La Cuarta Revolución Industrial", que implica la hiperconectividad de la maquinaria, procesos, trabajadores y clientes. En este nuevo contexto, todos los actores aportan y reciben información, configurando un entorno inteligente y flexible de producción, en el que también se integrarían funciones de Ingeniería, mantenimiento de Instalaciones, etc. junto con los proveedores y clientes.

Como parte fundamental de este sistema está la logística, que aplicaría todos los principios de conectividad e inteligencia descritos, denominándose por analogía "Logística 4.0".

El desarrollo de tecnologías como el internet de las cosas (IoT), Big Data o Blockchain son algunos de los catalizadores de esta nueva revolución. Recursos que permitirán crear entornos distribuidos de gestión de las cadenas de suministro, donde todos los integrantes tendrán visibilidad de los procesos para estar alineados y reaccionar ágilmente y en tiempo real.

Pero el nuevo escenario no es sólo tecnológico, hay otros factores clave que son necesarios abordar. Entre éstos, está el impacto en el factor humano. El nuevo entorno demanda nuevos perfiles profesionales, nuevos enfoques de formación y, consecuentemente, ya está teniendo un impacto en la generación de empleo.

La digitalización de la industria y de la cadena de suministro implica nuevas relaciones y compartición de datos entre los distintos actores, para lo cual es importante conocer y gestionar las implicaciones legales que esto tiene.

Por último, otro aspecto clave es el de la ciber-seguridad. La protección y seguridad de los datos es fundamental en la arquitectura del nuevo entorno y es uno de los pilares de tecnologías como el Blockchain. Dentro de este análisis de ciber-seguridad es necesario considerar la protección de las infraestructuras críticas de energía, transporte, etc. que garanticen el normal funcionamiento del sistema.

Desde el Centro Español de Logística hemos tratado de abordar todos estos aspectos proporcionando una visión amplia del estado de la situación. La guía incluye algunos casos de éxito de implantación de estos conceptos, para lo cual hemos contado con la aportación de magníficos profesionales expertos en la materia.

Espero que el estudio sea de su agrado y consiga los objetivos planteados. Desde CEL, les animamos a continuar profesionalizando la Logística 4.0 y su implantación.

01 | La sociedad conectada y la Industria 4.0

por **Marina Rodríguez Valentín-Gamazo**
Directora
Windmill Consultants

Bienvenidos a la era "smart", a la sociedad conectada y a los negocios Inteligentes.

La digitalización ha pasado en los últimos años de ser algo con un halo de novedad y que poblaba los departamentos más avanzados de innovación de las empresas, a ser el medio ambiente en el que se desenvuelven las actividades de cada vez un número más grande de organizaciones y profesionales de todos los ámbitos.

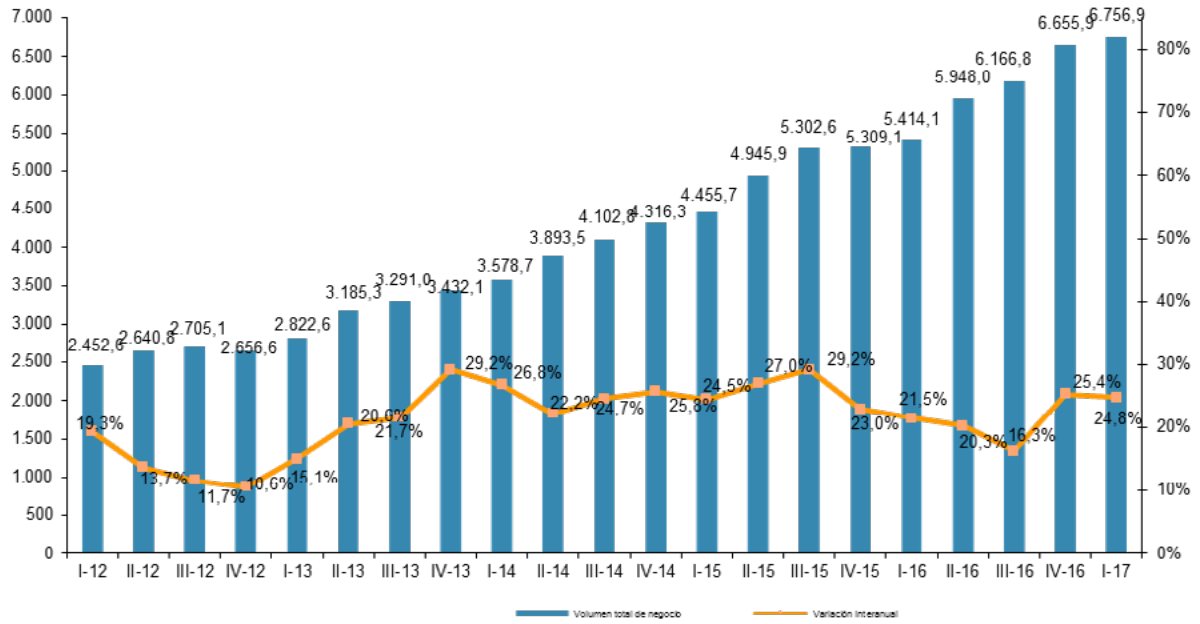
El desarrollo tecnológico exponencial en estos años ha facilitado la creación de nuevos negocios y modelos de uso "inteligentes", "smart" o "conectados" para satisfacer las necesidades de una sociedad que cada vez demanda más servicios digitales.

Si echamos la vista atrás diez años, podemos comprobar los cambios en los comportamientos de consumidores, trabajadores y en el funcionamiento de las empresas. Cambios todos habilitados por un acceso cada vez más generalizado a tecnologías digitales.

El crecimiento del comercio electrónico viene dado por la conjunción de varios fenómenos:

- Las bajas barreras de entrada:
    - La tecnología que posibilita la creación, operación y promoción de tiendas on-line es cada vez más asequible y fácil de utilizar.
    - No son necesarias grandes inversiones en tiendas y almacenes, lo que permite una oferta de productos mucho mayor.
- Multiplicación de las posibilidades de contacto con el cliente: la tecnología hace posible la llegada a clientes de todo el mundo, frente al comercio tradicional que depende de las personas que pasen frente al local comercial.
- El cliente "inteligente":
    - La compra on-line y del comercio electrónico se han normalizado.
    - Fenómeno "omnichannel" en el que el cliente se relaciona con la marca a través de varios canales: tienda, web, teléfono, redes sociales, distribuidores, plataformas.
    - Fenómeno "see now-buy now": el cliente on-line quiere recibir el pedido cuanto antes, lo cual ha desatado la competencia por "be first" y "the last mile".

EVOLUCIÓN TRIMESTRAL DEL VOLUMEN DE NEGOCIO DEL COMERCIO ELECTRÓNICO Y VARIACIÓN INTERANUAL (millones de euros y porcentaje)



Fuente: CNMC

En el estudio "Estadísticas sobre comercio electrónico en España. Primer trimestre 2017", publicado por la CNMC podemos apreciar cómo en los últimos 5 años el volumen del comercio electrónico en España se ha multiplicado por 2'75. Ha pasado de unos 2.452 millones de euros en 2012, a unos 6.756 millones de euros en 2017.

Una consecuencia esperable de este crecimiento vertiginoso es la creciente competencia y, por tanto, la necesaria innovación en los modelos de negocio, en la oferta de servicios de comercio electrónico y de entrega de productos que proponen los diferentes actores.

En relación con los modelos de negocio de venta B2C (Business to Consumer) señalamos los más relevantes:

- **Venta de productos y/o servicios y contenidos:** comercialización de stocks de producto físico o de servicios tales como viajes, o bien contenidos como películas o libros electrónicos. Estos pueden ser de una marca en concreto o de grandes plataformas de venta online que actúan como grandes almacenes y tienen una oferta variada, extensa y multimarca. En este punto merece la pena destacar el crecimiento en los últimos años de los supermercados online.

- **Ventas flash:** son campañas de duración limitada, frecuentemente unos pocos días en las que se vende un stock concreto de una gama de productos concreta. Por ejemplo, zapatillas de deporte o electrónica de consumo.

- **Portales de comparación de precios** que actúan como agregador de ofertas y que intermedian entre clientes y proveedores. Son muy famosos los comparadores de seguros+.

- **Venta por cupones o ventas grupales:** las webs logran importantes descuentos por volumen mediante la agregación de compradores de un mismo producto o servicio.

- **Las suscripciones:** el cliente se suscribe a la compra de un producto mensual en un rango de precio prefijado y recibe dicho producto todos los meses en su domicilio. Son famosos las suscripciones a productos de belleza, vino, café, libros...

- **Las plataformas de economía colaborativa** en que los particulares ofertan sus capacidades, conocimientos y recursos. Destacamos, entre otros, la oferta de servicios de transporte y entrega dentro de las ciudades, el compartir vehículos, la oferta de espacios de almacenamiento y trasteros de particulares.

Las empresas proponen una experiencia de compra cada vez más personalizada, lo que se concreta en una oferta amplia de posibilidades de entrega de los pedidos tanto en

la fecha como en el lugar. Así, encontramos rangos que van desde la entrega en un plazo de pocas horas dentro del mismo día, hasta a entregas no inmediatas con fecha y hora fijas. Igualmente, se puede dejar el paquete en el domicilio del cliente o en otros puntos de recogida acordados.

Más allá de comercio electrónico, en el momento actual estamos al borde de una nueva oleada de digitalización que está penetrando en todos los ámbitos de la sociedad. Queremos destacar en este informe varios de estos impactos:

Las ciudades y las infraestructuras inteligentes

Utilizan la conectividad, las comunicaciones y la explotación de los datos para responder mejor a las necesidades de los ciudadanos, empresas e instituciones en un amplio rango de servicios: seguridad, educación, sanidad, limpieza, medio ambiente etc.

Esto incluye la disponibilidad de datos que permiten el seguimiento y gestión del tráfico y de ello se pueden servir las empresas de logística para el seguimiento de la mercancía, optimización de rutas en función del tráfico, control de la ubicación de clientes y transportistas mediante geolocalización

El transporte inteligente

En fase de desarrollo y conocemos innumerables iniciativas de fabricantes tradicionales y start-up. Este tipo de modalidad de transporte aboga por explotar la potencialidad de la conectividad, el big data y la inteligencia artificial para solucionar los retos de la movilidad, la contaminación y la seguridad.

- Hoy ya es una realidad el vehículo conectado (coche/camión/barco/avión) que ofrece servicios de conducción inteligente gracias a la conectividad. Así puede recibir información en tiempo real sobre tráfico, climatología, precios de combustibles, estado del vehículo etc., que facilita y optimiza el transporte.

- Los drones para la entrega de mercancías también son una realidad y son viables desde el punto de vista técnico. Sin embargo, se abren muchos interrogantes respecto a la seguridad, lo que hace que su uso esté fuertemente regulado e incluso prohibido.

- Vehículos Autónomos: están en fase de estudio y pruebas y es algo que no tardará en llegar aunque hoy todavía no están resuelto los retos de la seguridad y la ciberseguridad.

Los empleados conectados (smart workers)

La tecnología se pone al servicio de los trabajadores ayudándoles a ser más productivos y a mejorar su bienestar. Hay muchos tipos de herramientas y aplicaciones que aquí agrupamos en 4 grupos:

- La movilidad en forma de teléfonos inteligentes, tablets, tecnologías de voz que facilitan el desarrollo del trabajo en lugares remotos, aprovechan tiempos muertos de transporte y espera o acortan procesos

- Los "wearables" o tecnología vestible en forma de pulseras, muñequeras o cascos inteligentes para la localización, control de constantes vitales, transmisión de órdenes de trabajo.

- Realidad virtual y realidad aumentada para la visualización de órdenes de trabajo, inventarios, simulación de procesos, manejo de maquinaria.

- Robótica colaborativa: robots que realizan trabajos rutinarios y pesados por ejemplo en carga y descarga de mercancía, preparación de pedidos, etc...

LA INDUSTRIA 4.0

Merece la pena dedicar un apartado diferenciado a la digitalización de los procesos más internos y "duros" de las empresas. Las compañías dedicadas a la fabricación, junto con todo su ecosistema van a vivir una revolución particular por la adopción de alguna o varias tecnologías digitales en lo que cristaliza bajo el nombre de Industria 4.0.

Esta revolución se está dando bajo el paraguas de la denominada Industria 4.0. Un término acuñado en Alemania en el año 2011 que nace como consecuencia de una iniciativa del gobierno alemán para revitalizar la actividad industrial en el marco de países con salarios altos y un estado del bienestar muy desarrollado, frente a nuevos entrantes en este campo tales como China, India, Corea del Sur, Rusia o Brasil.

Industria 4.0 hace referencia a la Cuarta Revolución industrial. Si en la primera revolución industrial la máquina de vapor sustituyó la fuerza humana o animal en muchos procesos, en la segunda fue la electrificación de la industria y la cadena de montaje. En la tercera fue la automatización y el control informático. En la cuarta ya estamos viendo procesos y productos inteligentes, la explosión del internet industrial y la hiperconectividad de trabajadores, máquinas, productos y clientes en sistemas ciberfísicos.

Hoy ya es un objetivo estratégico de política industrial y económica de los países más desarrollados del mundo. Las inversiones ya realizadas, los proyectos en curso y las declaraciones públicas en el mismo sentido imprimen un impulso que ya es fuerte y no tiene visos de parar.

En España nuestro modelo industrial 4.0 se lanzó en 2015. Se llama "Industria Conectada" y sigue la estela alemana pero contempla las particularidades de la economía española en cuanto a sectores industriales relevantes y en cuanto al volumen de pequeñas y medianas empresas.

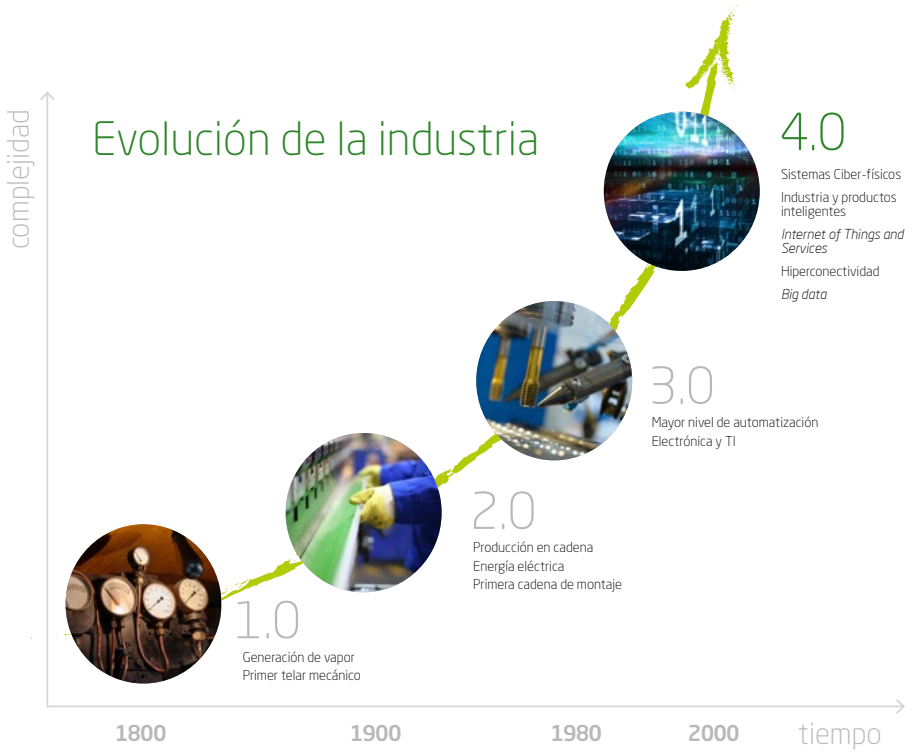
Las posibilidades que ofrece la industria 4.0 permiten una digitalización de la cadena de valor de las empresas industriales obteniendo como resultado una empresa industrial inteligente.

Esto es:

- Una organización abierta que conecta a los diferentes actores de su cadena de valor: Proveedores, clientes y empleados conectados a lo largo del ciclo de vida del producto.
- La ingeniería de producto se desarrolla en base a modelos virtuales.
- El proceso de fabricación se desarrolla en instalaciones inteligentes que permiten la gestión del mantenimiento predictivo de las infraestructuras, la inteligencia ambiental y una mejora de la eficiencia energética.
- La producción se realiza en maquinaria conectada tanto dentro como fuera de la planta de producción, que genera información para el mantenimiento predictivo.
- Por último, los empleados trabajan con herramientas digitales tales como robots colaborativos, realidad aumentada y sistemas de inteligencia artificial de apoyo a la decisión que permiten una mayor productividad y seguridad.

En definitiva, todo está conectado y generando un enorme volumen de datos. Esta información, adecuadamente gestionada ofrece innumerables oportunidades a las empresas industriales en tres ámbitos:

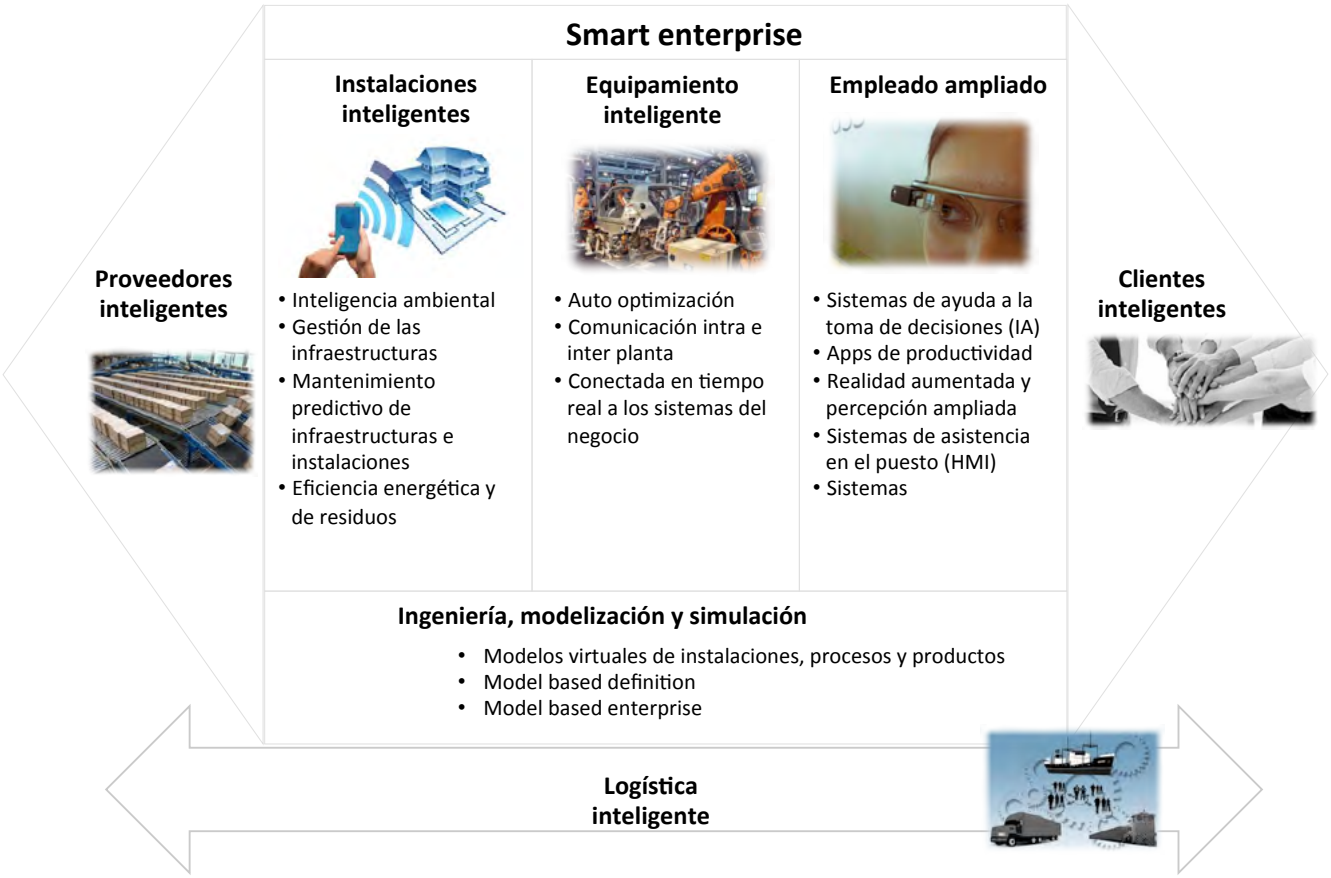
- Excelencia operativa y reducción de costes.
- Creación de nuevos productos y servicios.
- Creación de nuevos modelos de negocio.



Fuente: "Informe de Industria conectada" Ministerio de Economía, Industria y Competitividad. 2015

Desde el punto de vista de la excelencia operativa y la reducción de costes podemos obtener resultados tales como:

- Digitalización de procesos "lean" existentes y tener un cuadro de mando en tiempo real.
- En relación con el mantenimiento de maquinaria e instalaciones podemos mejorar el mantenimiento predictivo y por tanto tener mayor disponibilidad de maquinaria y reducir los costes de mantenimiento.
- Podemos mejorar sustancialmente la planificación de la demanda y como consecuencia de ello una optimización de la cadena de suministro y de los requerimientos de trabajadores y maquinaria.



Fuente: elaboración propia Willmild

- Como último ejemplo en este ámbito hablamos de la mejora de la calidad que conseguiremos mediante documentación embebida en producto, se pueden efectuar realización de controles de calidad con realidad aumentada o utilizar analítica de datos para analizar la causa raíz de forma semi-automatizada. Todo ello redundará en una reducción de costes de no calidad.

En cuanto a las posibilidades de la Industria 4.0 para la creación de nuevos negocios y desarrollo de nuevos productos o servicios, podemos decir que las oportunidades más interesantes vienen de la venta de servicios sobre productos físicos, todo ello basado en datos.

Ejemplos concretos serían:

- Servicios de pago por uso: el cliente paga el uso de maquinaria en vez de comprar la máquina.

- Venta de servicios para la obtención, análisis y toma de decisiones basados en datos.

- Oportunidades de creación de empresas de servicios tecnológicos y de negocio industriales. Por ejemplo:

  - Apps para manejo de maquinaria y líneas de producción.

  - Desarrollo e implantación de SW para la gestión de procesos de fabricación. Lo que conocemos como MES, Manufacturing Execution Systems.

  - Diseño y fabricación de robots, sensores, sistemas de realizada virtual.

02 | De la Cadena de Suministro al Ecosistema de Suministro

por **Marina Rodríguez Valentín-Gamazo**
Directora
Windmill Consultants

La actividad de la logística se encuentra viviendo en lo que podríamos llamar "La tormenta perfecta". Nada nuevo, por cierto, ya que este sector está más que acostumbrado a enfrentar retos y a sortear obstáculos. Muchos pensamos que el reto fundamental y donde se va a producir una selección de empresas vía éxito/fracaso va a residir en el ritmo en la transformación. Es decir, en cómo las empresas naveguen a través de la tormenta.

¿QUÉ ESTÁ PASANDO?

Existen una serie de fenómenos que se están dando de manera simultánea y que favorecen un cambio de condiciones, actores, procesos y tecnologías.

Como consecuencia de ello, parece acertado hablar de un profundo cambio en la definición de la logística, pasando del concepto de "Cadena de Suministro" a "Ecosistema de Suministro"

A continuación, analizamos los factores clave que propician esta transformación:

1. Nuevas formas de producción y consumo

Al hilo de lo detallado en el capítulo anterior, el sector logístico es el punto necesario de conexión entre dos realidades rápidamente cambiantes: los nuevos modelos de producción de la Industria 4.0 y los nuevos modelos sociales, de consumo y de comportamiento de las personas. Así, tanto en el mundo B2C como en el B2B las características exigidas por los que demandan servicios logísticos son:

- Más baratos.
- Más flexibles.
- Más predecibles.
- Que completen la experiencia de compra y uso y cuiden tanto al comprador como a la marca del vendedor.

¿Es posible conseguirlo?

Todos los expertos coinciden en que es posible, pero haciendo un uso intensivo de la tecnología y las alianzas. Veamos a continuación lo que esto significa:

2. El desarrollo tecnológico

Hoy, existen una serie de desarrollos tecnológicos que aportan importantes ventajas a los jugadores del campo de la logística. Muchas de estas tecnologías también son de uso intensivo en la industria 4.0.

En concreto, destacan dos ámbitos tecnológicos

- El uso masivo de los datos para tener una mejor capacidad de predicción y planificación de la demanda, de los flujos de mercancías y de los flujos de tráfico.

- La automatización de tareas repetitivas en almacén y carga.

En ambos casos, la conectividad, el famoso IoT (Internet of Things), es esencial para la generación y captura de información que posteriormente será tratada y empleada para la toma de decisiones.

En un futuro no lejano se podrá llegar una mayor automatización de la toma de decisiones mediante el uso de la Inteligencia Artificial y el Machine Learning.

Esto conlleva importantes mejoras en coste y eficiencia en tiempo. Pero no es suficiente todavía. Existen importantes retos en integración de actores, conectividad y seguridad.

3. La fragmentación de la cadena de suministro y la irrupción de nuevos actores y no tan nuevos

Nuevos entrantes:

El desarrollo tecnológico está generando un mercado de nuevas empresas de servicios logísticos, y los inversores están dedicando recursos a financiar estos desarrollos.

Podemos hablar de casos de "start-ups" centradas en el mundo del Software que carecen de activos físicos y de "legacy", de forma exitosa capturan pequeños trozos de la cadena de valor, con la consiguiente fragmentación de ésta.

También destacan ejemplos de empresas que ofrecen comparativas de precios de fletes, a otras que, siguiendo el modelo de Uber o Air BnB se dedican a ofrecer espacios libres de carga o almacenamiento.

Respecto a la cobertura del servicio de la última milla (Last Mile), aquí encontramos todo tipo de empresas que casan la demanda con la capacidad que tienen, tanto individuos como empresas no logísticas en almacenar, transportar y entregar bienes de todo tipo de forma y tamaño.

Jugadores tradicionales que se mueven a lo largo de la cadena de valor:

En la actualidad, es un hecho que mayoristas y distribuidores que tradicionalmente han confiado sus envíos a empresas especializadas en logística, están desarrollando sus propias capacidades. El ejemplo más claro es Amazon, que invierte en una flota de aviones, en el desarrollo de robots o drones. Su competencia más estrecha, Alí Baba, también está en ello.

A esto hay que añadir que los fabricantes de automoción, con los desarrollos de vehículos autónomos, quieren capturar parte de los flujos del transporte.

4. La consolidación de modelos colaborativos

Como hemos visto en el punto anterior, la concepción más tradicional de la logística cuenta con actores bien diferenciados que se encargan de ejecutar partes concretas de la cadena de suministro, estructuradas en flujos lineales.

Así, se distingue claramente al fabricante, al distribuidor mayorista, a las tiendas y al comprador. Cada uno de estos actores con un rol diferente. Y, cada uno de ellos, captura una parte concreta del valor de dicha cadena, que podemos visualizar estructurada como compartimentos estancos y en silos.

La economía colaborativa es una realidad que ha llegado para quedarse. Donde encontramos un mayor desarrollo es en la cobertura de la última milla, pero esto se está haciendo extensivo "aguas arriba".

En este contexto, para proveer de servicios de logística eficientes y flexibles, será necesario que esta colaboración madure y se desarrolle a gran escala. Algo que está suponiendo la creación de alianzas temporales y acuerdos de colaboración, Joint Ventures, así como compras y fusiones que completan capacidades, presencia en mercados o dotan de tamaño a las empresas.

LA TRANSICIÓN HACIA LA VIDA EN EL ECOSISTEMA LOGÍSTICO

Hay tres aspectos que sabemos que son esenciales:

- Afirmamos que la clave está en que las empresas del sector se adapten a la nueva realidad para no perder o para capturar el valor del ecosistema logístico.

- Nos encontramos en un momento de transición ("la tormenta perfecta") y, por tanto, tenemos pocas certezas. No existen todavía muchos casos de éxito (o de fracaso), carecemos de ejemplos maduros, de modelos fiables, de hoja de ruta.

- Sabemos que empresarios y trabajadores tendrán que elegir qué partido jugar y como todavía no están claras las reglas del juego, hay que arriesgar.

Ante este panorama, ¿cuáles son las opciones para ser competitivos en el Ecosistema?

1. Cooperación y colaboración

Dice el refrán africano "Si quieres llegar rápido camina solo, si quieres llegar lejos camina acompañado".

Sobrevivir hoy en la actividad de la logística pasa precisamente por formar parte del ecosistema y capturar trozos de la cadena de valor. Esto requiere a su vez elegir en qué nos vamos a especializar, qué papel queremos jugar y con qué socios vamos a trabajar.

También supone una oportunidad de ganar tamaño mediante compras y fusiones.

2. Innovación

Existen nuevos modelos de negocio, otras formas de operar los procesos, mercados todavía no explorados que abren un abanico de posibilidades a las empresas del sector, pero ¿cómo hacerlo?

Gracias a que vivimos en un mercado global y que la información fluye a través de las redes, es posible conocer a los actores y tendencias que ayudan en la toma de decisiones. También existen metodologías, servicios especializados y profesionales que pueden contribuir a desarrollar la innovación en la empresa.

Por último, y al hilo del apartado anterior, se puede valorar la adquisición de start-ups que complementen nuestro portfolio o que ayuden a transformar el modelo de negocio.

3. Digitalización

La logística del futuro no se entiende sin una fuerte presencia de la tecnología tanto en la concepción como en la operación del negocio. Es imperativo que empresas y profesionales dediquen recursos y tiempo a adquirir o evolucionar la infraestructura tecnológica necesaria para lograr una "logística inteligente ó 4.0". Sin ello, quedarán fuera de juego en un plazo corto.

Además, estas capacidades digitales son esenciales para abordar procesos de innovación y para integrarse en el ecosistema de suministro.

4. El Internet Físico

(el lector encontrará frecuentemente la denominación inglesa Physical Internet y representado con la letra griega π y el acrónimo PI)

Esta innovadora visión, es un caso aparte y en estos momentos se encuentra todavía en una fase temprana y académica de su desarrollo. No obstante, es importante mencionarla en esta Guía.

El Internet Físico propone un nuevo modelo de gestión de la logística, cuyo objetivo es ganar en eficiencia y permitir una interconexión de los actores del ecosistema de una manera fluida y transparente.

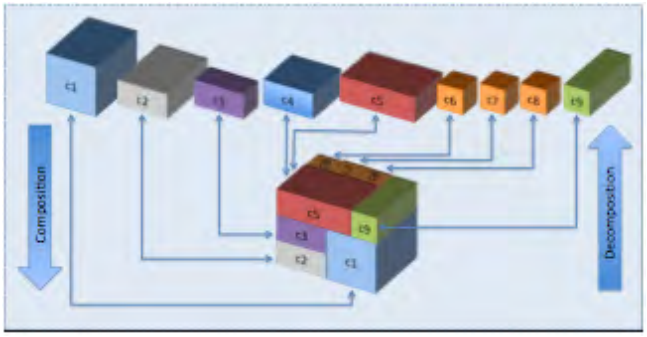
El manifiesto fundacional de este movimiento sostiene que el Internet Físico es "transformar la manera en que los objetos físicos son manejados, trasladados, almacenados, pagados y distribuidos con el objetivo de lograr una logística global eficiente y sostenible".

Tanto el nombre como la idea se inspiran en la manera en que el Internet Digital transfiere la información a escala global. Veamos a continuación cuáles son sus características:

INTERNET DIGITAL	INTERNET FÍSICO
No transmite información.	No maneja mercancías físicas.
Transmite paquetes que contienen datos.	Sólo maneja contenedores que dentro tienen las mercancías.
Los datos de cada paquete están encapsulados y no se gestionan desde internet.	Cada contenedor lleva encapsulados los bienes físicos.
Cada paquete de datos lleva un código que contiene toda la información necesaria para identificar el paquete y direccionarlo a su destino.	Los contenedores están conectados mediante un modelo de IoT (Internet de las cosas) que permite una monitorización y enrutamiento constante. Tienen un identificador único, una "etiqueta inteligente" que actúa como agente para identificar, dirigir, monitorizar y proteger a través de las redes físicas.
Cada paquete se construye exclusivamente para su transmisión y se deshace una vez entregado en destino	Los contenedores son "inteligentes", ecológicos, modulares y su tamaño es estándar a nivel mundial y varía desde el contenedor marítimo hasta una pequeña caja.
El modelo se basa en un protocolo (TCP/IP) que estructura los paquetes de datos independientemente de la infraestructura para que pueda ser procesado por diferentes sistemas y redes.	La modularidad e inteligencia de los contenedores está concebida para facilitar su movimiento, transporte, almacenamiento y consigna a través de los nodos del Internet Físico.

Hacer realidad este nuevo modelo cuenta con muchos elementos a su favor:

- La necesaria interconexión del ecosistema logístico.
- La respuesta a la demanda de los clientes: logística más rápida, más barata y más flexible.
- La buena acogida por parte de los gobiernos que quieren favorecer una mayor interoperabilidad entre países y regiones. Objetivos para los cuales existen inversiones y apoyo explícito.
- El desarrollo y abaratamiento de las tecnologías necesarias para la interconexión de los contenedores.



Una vez que hemos repasado las tendencias más actuales en la transformación de la Logística, es importante señalar que existen retos y barreras a tener en cuenta y gestionar:

- Lo primero, es que empresarios y profesionales tomen conciencia de lo que está ocurriendo y de las diferentes opciones a su disposición.
- Invertir en digitalización y en adquirir nuevas capacidades.
- Desarrollar una cultura empresarial y una manera de hacer las cosas alineada con los requerimientos de los nuevos tiempos que nos vienen.
- En la transición hacia una logística hiperconectada se encuentra el desafío más inmediato, relacionado con la seguridad/ciberseguridad. Asegurar el servicio ante amenazas aún no familiares para una buena parte del sector requerirá de un liderazgo decidido, de una formación adecuada a todos los profesionales y de las herramientas tecnológicas que aseguren la resiliencia de la actividad logística.

FUENTES

- *"Shifting patterns: The future of the logistics Industry"* PWC. 2016
- *"Physical Internet"*. Wikipedia

03 | Las Tecnologías y Drivers de la Industria 4.0

por **Carlos Junquera Uría**
Digital Operations SPGI Leader. Business Analytics & Strategy Europe
IBM Global Business Services

Hablar de Industria 4.0 aplicada a la logística y a la Cadena de Suministro es hablar de una mayor capacidad de adaptación, de flexibilidad de la producción y de la personalización de la demanda. Todo ello con una asignación más eficiente de los recursos.

Ya es conocido por todos cómo la tecnología habilita la denominada Cuarta Revolución Industrial, a través de la digitalización de los procesos, la utilización de los sistemas ciber físicos, el Internet de las Cosas, los dispositivos móviles, etc. Esta tecnología, aplicada a la cadena de suministro aproxima los mercados de oferta y demanda entre sí y con las propias plantas de producción, generando nuevos escenarios con grandes posibilidades de optimización, habilitando nuevas posibilidades de negocio, e incluyendo nuevos actores a la Cadena de Suministro, que pueden convertirse en importantes competidores.

Existen diferentes drivers tecnológicos que conducen esta revolución, entre ellos:

- Internet de las Cosas (IoT)
- Profundización en la nube
- Sistemas cognitivos
- Realidad virtual y aumentada
- Blockchain
- Robótica
- Comercio electrónico y medios de pago
- Comunicaciones y dispositivos móviles
- Impresión 3D
- Etc.

A continuación, profundizaremos en algunos de estos drivers, más relacionados con la captura de información en tiempo real, el manejo de grandes volúmenes de información y la calidad y trazabilidad de los productos.

INTERNET OF THINGS (IOT) Y LA NUBE

La posibilidad actual, física y económica, de que casi cualquier cosa pueda tener la electrónica mínima para conectarse a internet hace que el número de dispositivos conectados esté creciendo exponencialmente. Actualmente, se manejan cifras de 13.000 millones de

dispositivos conectados y una previsión de que este número se duplique en los próximos 5 años.

Este es el punto de partida básico de Internet de las Cosas. En este concepto se engloban todos los dispositivos que están conectados, enviando y recibiendo información de manera automática y relacionándose entre ellos. Ejemplo de esto sería el termómetro que activa el aire acondicionado al detectar calor.

El otro punto necesario para esta revolución es la existencia de una infraestructura necesaria para gestionar toda la información generada por esta masa de dispositivos en tiempo y forma adecuados. Afortunadamente, ya tenemos soluciones que permiten afrontar esta tarea.

La combinación de IoT más la tecnología en la nube pone a nuestro alcance una potente herramienta con infinitas posibilidades que permitirá mejorar la información sobre la cadena de suministro, optimizar los procesos asociados, disminuir riesgos y proporcionar una mejor experiencia al cliente. Algunos ejemplos de posibles aplicaciones son los siguientes:

- **Seguimiento y trazabilidad de mercancías:** Cualquier mercancía puede emitir su localización o geolocalización en tiempo real de manera continua para que sepamos en qué lugar se encuentra. Nadie tiene que incluir la información en ningún sistema, porque se realiza de manera automática con total precisión sin intervención humana.
- **Optimización de logística:** Al tener control individualizado de la situación de cada mercancía, se gana precisión en los inventarios y se puede optimizar el uso de transporte y almacenes.
- **Estado de infraestructura:** Las propias máquinas implicadas en el desarrollo de los procesos pueden alertar de fallos y anticipar periodos de mantenimiento o posibles problemas.

Para los ejecutivos relacionados con cadena de suministro, la inversión en IoT está en el tercer puesto como prioridad de inversión en transformación digital en los próximos tres años, por delante de la inversión en plataformas móviles o en automatización según el informe *"Welcome to the cognitive supply chain"* (IBM Institute for Business Value, Junio 2017) lo que nos da una idea de la importancia de este tipo de tecnología.

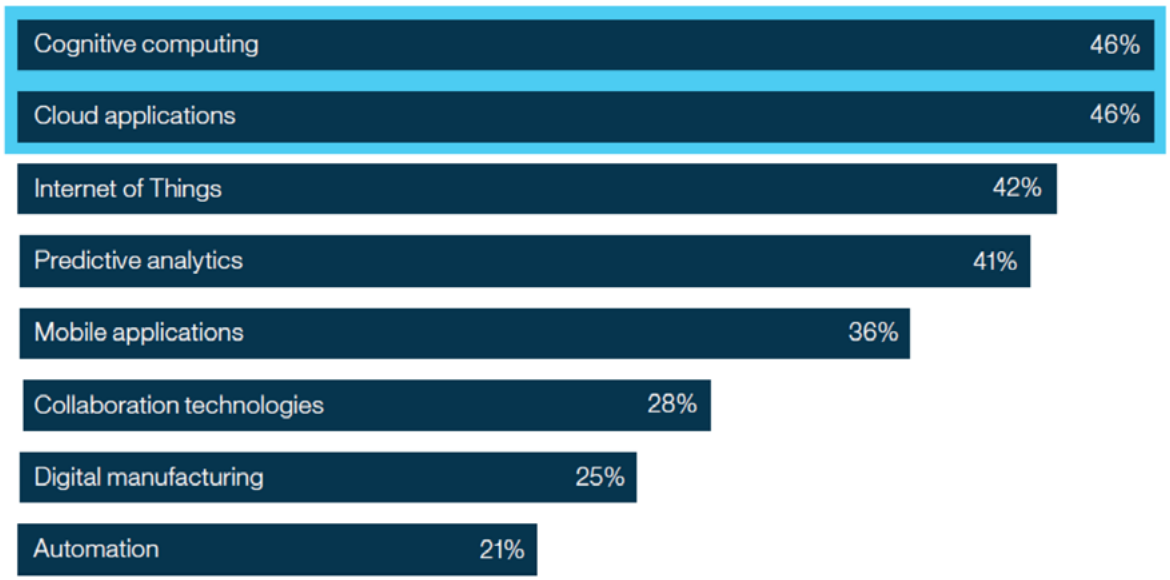
SISTEMAS COGNITIVOS

La tecnología avanza hoy más rápido que en cualquier otro momento en la historia de la humanidad. En medio del creciente mercado de nuevas tecnologías, se espera que una capacidad - Computación Cognitiva - sea revolucionaria para múltiples industrias y, de hecho, para la sociedad en general.

Se predijo que para que las cadenas de suministro se consideren "Inteligentes", han de ser:

Figure 1

Executives predict their greatest digital operations investments over the next three years



Source: IBM Institute for Business Value

- **Instrumentadas:** La información previamente creada por personas será, cada vez más, generada por máquinas con origen en sensores, GPS, medidores, etc... El inventario se contabilizará a sí mismo. Los contenedores medirán su propio contenido. Las paletas informarán si terminan en el lugar equivocado...

- **Interconectados:** Toda la cadena de suministros estará conectada, no sólo los clientes, proveedores o sistemas IT en general, sino que piezas, productos y otros objetos inteligentes usados para monitorizar la cadena de suministros.

- **Inteligentes:** La toma de decisiones en estas cadenas de suministros será mucho más inteligente. Modelos de análisis avanzados ayudarán a la hora de la toma de decisiones a evaluar las alternativas frente a un conjunto de riesgos y restricciones increíblemente complejas y dinámicas. Algunos sistemas más inteligentes incluso tomarán decisiones automáticamente - aumentando la capacidad de respuesta y limitando la necesidad de la intervención humana.

Los sistemas cognitivos:

- No se programan como los ordenadores actuales.

- Entienden el lenguaje natural de las personas.

- Son capaces de analizar imágenes.

- Son capaces de analizar la información de la Internet de las Cosas.

- Y lo más importante: son capaces de aprender de la información que van captando.

Las aplicaciones más comunes de estas tecnologías dentro de la cadena de suministro están dirigidas a la calidad del material, el mantenimiento preventivo y la gestión de riesgos desde el suministro hasta la producción y la provisión al cliente. La computación cognitiva resuelve muchos de sus desafíos en los procesos de las cadenas de suministros end-to-end.

Las empresas pueden aplicar la tecnología cognitiva a la planificación de ventas y operaciones y a otros conjuntos masivos de datos sobre la cadena de suministros para gestionar la volatilidad de la demanda, las restricciones de la oferta, la programación de la producción y la distribución dinámica, etc.

La tecnología cognitiva puede aumentar la interacción con personas a través de la asignación de recursos, la distribución de personas y los procesos de programación.

Las capacidades de aprendizaje de las máquinas aplican algoritmos a los flujos de datos operativos masivos para analizar, rastrear y predecir interrupciones en las cadenas de suministros.

Las prioridades, los planes y el propósito de emplear las capacidades cognitivas en tres áreas de la cadena de suministro distintas y complejas:

- Desarrollo de Productos

- Adquisición

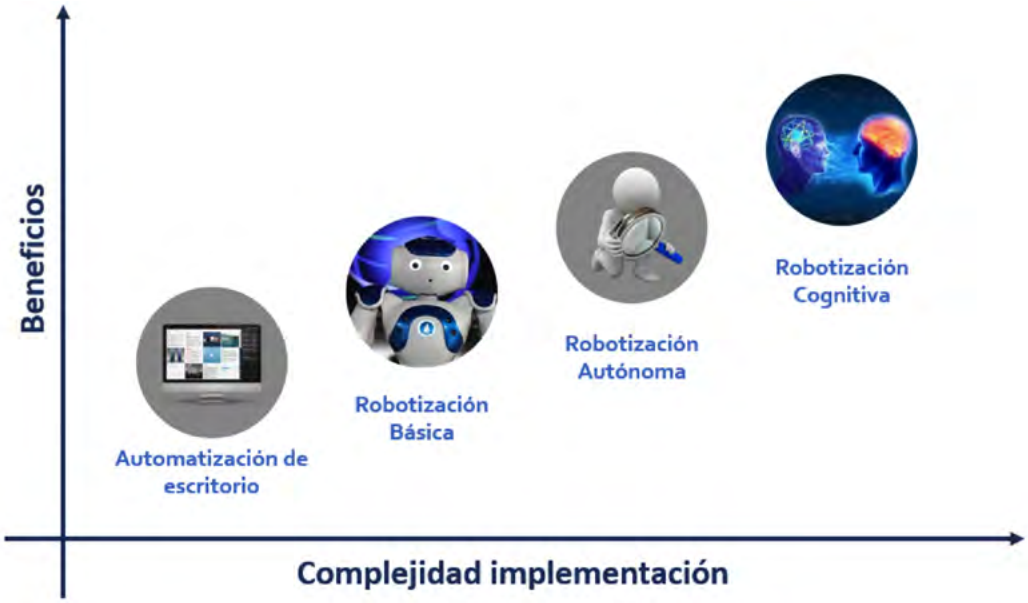
- Fabricación

En la fabricación, la colaboración con robots es posible gracias a la inteligencia artificial que habilita a dichos robots

Figure 2

Cognitive computing can derive the most value from these data sets

Source: IBM Institute for Business Value



a moverse de una manera segura alrededor de los seres humanos que trabajan junto a ellos en la producción.

Algunos ejemplos de casos de usos en la incorporación de sistemas cognitivos a la cadena de suministro pueden ser los siguientes:

- **Capacidad para "prometer":** Aprovechar el conocimiento de la demanda de clientes en tiempo real y alinear mejor la fecha comprometida con la fecha real.

- **Estrategia para el almacenamiento:** Combina datos de máquinas de manipulación de materiales conectados con datos espaciales y de ubicación, así como con datos de productos existentes para optimizar las reglas y políticas existentes para el almacenamiento de inventario.

- **Determinación de la ruta de producción:** Aumentar los controles avanzados de procesos con datos de máquina, consumo de energía, segmento de clientes, las campañas con datos de oferta y demanda para secuenciar y programar procesos y rutas de producción, así como responder rápidamente a los cambios cuando sea necesario.

- **Planificación de stock seguro:** Optimizar los niveles de stock con seguridad a un nivel más granular con el uso de información adicional del sistema dependiente tanto del proveedor como del cliente.

ROBOTIZACIÓN DE SISTEMAS

La robotización o automatización de procesos es otra de las características que marcará el desarrollo de la Industria 4.0.

En este apartado nos estamos refiriendo a la ejecución de procesos de manera automática por parte de robots. Entiéndase robot como cualquier sistema capaz de ejecutar un proceso, es decir, puede ser **un programa de ordenador que ejecuta acciones** o robots físicos que realizan tareas en el mundo real. En esta sección se pretende señalar especialmente la capacidad de automatización y robotización de los procesos repetitivos que actualmente están realizando personas en lugar de sistemas informáticos.

Según el informe *"Seizing the Robotic Process Automation Market"* (Everest Group, octubre 2015) alrededor del 25 por ciento del total del tiempo laboral se invierte en tareas repetitivas. Esto nos da una idea del enorme potencial de reducción de costes que encontramos en esta iniciativa de mejora. Esta mejora es aplicable a todos los trabajos relacionados con la cadena de suministro pero, en concreto, para los trabajos relacionados con las áreas de tecnologías de la información. La reducción de gasto en procesos de externalización que incluyan automatización podría llegar a ser de alrededor del 70 por ciento según el anterior informe.

La robotización requiere un estudio previo de la situación del área a mejorar para identificar los procesos

candidatos y reorganizar el trabajo aislando este tipo de tareas. Después, como suele ocurrir en tecnologías tan novedosas, se recomienda una aplicación gradual de las medidas de cambio. En concreto, se definen cuatro fases según la madurez de la organización afectada:

- **Automatización tradicional (o de escritorio):** El robot reproduce acciones humanas previamente "grabadas" sobre los programas tradicionales. Es decir, el robot abre programas e imita los "clicks" del ratón o el manejo del teclado.

- **Robotización de procesos básica:** Los procesos tradicionales se modifican y adaptan al nuevo entorno. Se definen **reglas simples** que actúan sobre **datos estructurados** (datos ordenados y con formato, como una hoja de cálculo). El robot sigue las reglas y ejecuta los procesos.

- **Robotización de procesos autónoma:** Se definen reglas complejas que actúan sobre **datos no estructurados** (por ejemplo, una conversación humana o una foto) y permiten automatizar procesos de mayor complejidad.

- **Robotización de procesos cognitiva:** En un entorno como el anterior, al robot se le dota de **capacidades de análisis** basadas en la experiencia (acierto en las decisiones tomadas) y se le otorga un margen de decisión libre para modificar las propias reglas en búsqueda de una mejora en la proporción de aciertos, manejando excepciones y casos nuevos no previstos de manera correcta.

Los beneficios principales de estas iniciativas, además de la reducción de costes ya mencionada, son principalmente tres:

- **Disponibilidad 24x7:** El robot trabaja ininterrumpidamente por lo que el aumento de rendimiento es sensible. Esto es especialmente útil en monitorización de procesos críticos o en tareas de gran volumen.

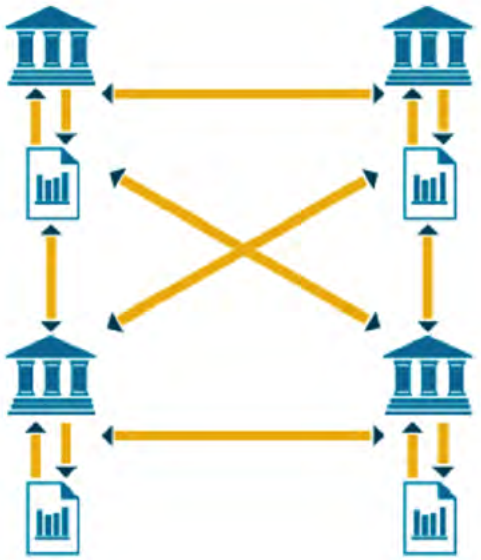
- **Escalabilidad ágil:** Aumentar el número de robots disponibles es casi instantáneo permitiendo una gestión más ágil de períodos de trabajo de mayor intensidad.

- **Ausencia de errores:** Una vez adaptados los procesos, definidas las reglas y aisladas las excepciones, la ejecución es realizada sin errores de manera continua.

El primer objetivo de la robotización son los procesos repetitivos de menor valor laboral, que pueden ser incluso causa de frustración a trabajadores humanos, es necesario acompañar ese proceso con una gestión del cambio adecuada para hacer que las personas se capaciten y habiliten para realizar tareas de mayor valor.

BLOCKCHAIN

Otra de las tecnologías disruptivas que forman parte del modelo de Industria 4.0 es Blockchain.



Cada integrante de la red Blockchain tiene acceso a la información compartida (toda o parte, según su perfil) y colabora en la verificación de la información según el mecanismo de consenso elegido para la red.

Blockchain no es otra cosa que una base dve datos compartida entre un grupo de entidades interesadas, pero con unas características especiales que la hacen revolucionaria:

- **Distribuida:** Cada entidad que necesite consultar los datos almacenados puede tener una copia propia de la base de datos, completa y actualizada en tiempo real.

- **Inmutable:** Cada registro del Blockchain está sellado en el tiempo y enlazado al registro anterior. Por diseño, la información introducida en Blockchain no es modificable. No es posible realizar modificaciones o alteraciones sin romper la lógica interna y corromper la base de datos.

- **Consensuada:** Cada registro introducido en la base de datos requiere el acuerdo de las entidades implicadas. Esto se logra por diferentes mecanismos y asegura que el dato introducido es fiable.

Un análisis rápido de las características de esta tecnología ya empieza a mostrar su potencial en los entornos adecuados. Estos entornos serán aquellos donde se requiera un seguimiento de las transacciones a modo de "libro de cuentas" o "diario de eventos" entre varias partes implicadas. En estos entornos las ventajas son evidentes:

- **Ahorro de tiempo:** El sistema de validación de cada transacción está ya implementado y mejora cualquier otra vía de consenso anterior.

- **Eliminación de intermediarios:** Se produce un ahorro en auditoría y cuadre de resultados entre partes, ya que el sistema lo implementa por diseño.

- **Reducción de riesgos:** Los datos introducidos no pueden ser modificados de manera accidental o intencionada sin una fácil detección del fraude. La base de datos se comparte entre las entidades de la red con lo cual hay copias actualizadas en varias localizaciones.

- **Incremento de la confianza:** Mejora en la relación entre partes y disminución de los costes asociados a litigios o malentendidos.

Los casos de uso son infinitos. En una primera aproximación a los relacionados con cadena de suministro, podemos identificar un par de ejemplos:

- **Seguimiento de mercancías o materias primas:** Se puede registrar el avance de cualquier mercancía paso a paso de manera rápida y segura por toda la cadena de suministro. Aquí se abren posibilidades de enriquecer esta tecnología con otras asociadas al Internet de las Cosas (IoT) como se ha visto anteriormente y formar soluciones mixtas que multipliquen los beneficios para el negocio.

- **Auditoría con reguladores:** Si se incluye al regulador en nuestra red de Blockchain y forma parte de los mecanismos de consenso, el cumplimiento de los estándares legales se consigue de manera automática sin necesidad de generar informes posteriores ni realizar informes de auditoría adicionales.

Las grandes empresas ya están invirtiendo en este tipo de iniciativas colocando a Blockchain en una de las 10 primeras prioridades de inversión en transformación digital para 2018 (Gartner).

04.1 | CiberSeguridad en el Sector Estratégico del Transporte

por **Rafael Pedrera**
Jefe de la Sección de Operaciones
Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC)

La Ley por la que se establecen medidas para la protección de las infraestructuras críticas (también conocida como Ley PIC) y su Real Decreto vieron la luz allá por abril de 2011.

Han pasado ya varios años y su implementación ha dado muchos y diversos frutos en el ámbito de la seguridad, y en concreto en el de la ciberseguridad, una disciplina que por aquel entonces era una "preocupación menor" para los profesionales de la seguridad y que hoy en día ha crecido hasta llegar a ocupar el primer lugar en sus agendas.

Nos encontramos en 2017: vamos a conocer cómo es la situación actual en materia PIC, qué nuevos organismos han surgido para fortalecer la ciberseguridad nacional de los sectores estratégicos, cómo funcionan en conjunto y cómo afecta a la cadena de suministro. Como reciente novedad y reforzando la línea iniciada hace 10 años, el CNPIC ha cambiado su denominación mediante el Real Decreto 770/2017 de 28 de julio, por el que se desarrolla la estructura básica del Ministerio del Interior. Mediante el Art.2 el CNPIC pasa a denominarse "Centro Nacional de Protección de Infraestructuras y Ciberseguridad", reconociendo el papel que la mejora de la ciberseguridad juega en la protección de nuestras infraestructuras.

CNPIC
CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD

SISTEMA PIC – ESTADO DE LA IMPLEMENTACIÓN

En la pirámide normativa que articula la implementación de la Ley PIC, nos encontramos junto a la cúspide al Plan Nacional para la Protección de las Infraestructuras Críticas (PNPIC), pieza fundamental de la que dimana el resto de normativa y cuya primera versión data de 2007, hace ya 10 años, y que fue actualizado en 2016 mediante la instrucción 1/2016 de Secretaría de Estado de Seguridad.

En esta actualización del PNPIC de 2016 se encuentran importantes añadidos respecto al primer plan. Una de las más relevantes de cara a la sociedad es la inclusión de los operadores críticos dentro de los órganos participantes en la implantación del PNPIC, junto con Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO), las

Pirámide normativa PIC

Fuerzas y Cuerpos de Seguridad del Estado (FFCCSE), los Cuerpos de Policía de las Comunidades Autónomas con competencias en seguridad pública y, por supuesto, el CNPIC. En el ámbito de la ciberseguridad y dentro de esta participación de los operadores críticos en el PNPIC, se vienen a destacar expresamente las figuras del Jefe de Seguridad de la Información o CISO (Chief Information Security Officer) y/o los Equipos de Seguridad de las Tecnologías o SOC (Security Operation Center) de las respectivas organizaciones como interlocutores naturales con los CERTs (Computer Emergency Response Team) nacionales, siempre a través de la Oficina de Coordinación Cibernética (OCC) del CNPIC (de la que hablaremos más adelante) y con conocimiento del Responsable de Seguridad y Enlace (RSE) de la organización, figura definida en la Ley PIC.

Debajo del PNPIC nos encontramos con la Ley PIC y su Real Decreto correspondiente, donde se establecen los distintos Planes que conformarán el resto de la pirámide normativa. El primero de ellos es el Plan Estratégico Sectorial (PES) de cada uno de los sectores estratégicos definidos en el Anexo de la Ley PIC, elemento fundamental y base de los siguientes planes. Cada PES tiene como alcance en todo el territorio nacional y viene a definir, en cada uno de los sectores contemplados en el anexo de la Ley PIC, cuáles son los servicios esenciales proporcionados a la sociedad, el funcionamiento general de éstos, las vulnerabilidades del sistema, las consecuencias potenciales de su inactividad y las medidas estratégicas necesarias para su mantenimiento; es como una "foto panorámica" de cada sector. En concreto, y en el ámbito que nos interesa, el Sector Transporte se divide en una serie de subsectores, cada uno con su correspondiente PES: Transporte Aéreo, Transporte Ferroviario, Transporte Marítimo y Transporte por Carretera. La Comisión PIC aprobó en 2015 el PES de cada uno de estos subsectores por lo que las infraestructuras críticas que incluyen están identificadas, lo cual nos lleva al siguiente paso: El Plan de Seguridad del Operador (PSO) y el PPE (Plan de Protección Específico).

El PSO se describe como los documentos estratégicos definidores de las políticas generales de los operadores críticos para garantizar la seguridad del conjunto de instalaciones o sistemas de su propiedad o gestión. Estos deberán establecer una metodología de análisis de riesgos que garantice la continuidad de los servicios proporcionados por dicho operador y en la que se recojan los criterios de aplicación de las diferentes medidas de seguridad que se implanten para hacer frente a las amenazas identificadas, tanto las físicas como lógicas. Los PPE son los documentos operativos donde se deben definir las medidas concretas ya adoptadas y las que se vayan a adoptar por los operadores críticos para garantizar la seguridad integral (física y lógica) de sus infraestructuras críticas.

La consideración en los PSO y PPE de la existencia de posibles amenazas de tipo lógico o cibernético fue una gran novedad en el momento de la promulgación de la Ley PIC, y era considerado entonces como algo casi anecdótico. No hace falta decir que en pocos años la realidad de las amenazas provenientes del ciberespacio se ha impuesto y la sociedad es consciente de su existencia, aunque todavía, para el ciudadano, usuario final de los servicios esenciales (agua, energía, transporte, telecomunicaciones, etc.), quizás le parezca una vicisitud lejana y que no afecta

a su quehacer diario. Esto también está cambiando, y no faltan ejemplos recientes de ciberataques que afectan a la cadena de transporte.

Uno de ellos es el ciberataque WannaCry de mediados de mayo de este año, una infección masiva a escala mundial mediante un malware que aprovechaba vulnerabilidades en sistemas Windows que fueron filtradas apenas dos meses antes del incidente, vulnerabilidades presuntamente robadas a la NSA (National Security Agency) de los EE.UU., que las estaba utilizando para realizar sus propias operaciones. Este ataque, aunque no estaba diseñado para agradir a la cadena de transporte, afectó a empresas de dicho sector dado su carácter masivo. El ataque volvía a repetirse un mes después, de forma más sofisticada y virulenta, esta vez con el nombre de Petya.

Pronto las noticias de que había puertos afectados saltaron a la red, y los problemas con los que se enfrentaron no se pudieron ocultar: el 90 por ciento de los bienes de consumo nos llegan por vía marítima, la mayoría de ellos en contenedores y las empresas encargadas de gestionar su transporte (evidentemente mediante medios informáticos) habían visto afectados dichos sistemas por WannaCry y Petya. El gigante del transporte marítimo A.P. Moller-Maersk llegó a reconocer que el malware se había extendido afectando a la operativa global de la compañía, aunque sin llegar a cuantificar el grado de impacto.

WannaCry y Petya cifran los sistemas de información inutilizándolos, y la clave para su descifrado es suministrada por los autores del ataque a cambio del pago de un rescate... y muchas veces ni habiendo pagado el rescate se podía acceder a su descifrado. El daño estaba hecho, y el resultado en los puertos el previsible: contenedores perdidos, contenedores sin carga identificada, contenedores identificados pero sin destino, retrasos en las operaciones de remolque de botes y de carga de combustible... En un plano más cotidiano, aquellos que compramos vía internet productos a China para recibirlos por paquetería pudimos comprobar el retraso con el que los productos llegaban a su destino final.

¿CÓMO NOS PROTEGEMOS DE UN CIBERATAQUE A LA CADENA DE SUMINISTRO?

Hoy en día los ciberataques han crecido en complejidad, al haber crecido a su vez en sofisticación y medios defensivos los sistemas. Es una "escalada armamentística" de armas y medios defensivos que han ido dejando atrás la figura del hacker solitario que se infiltraba en los sistemas más por afán de superación y de enfrentarse a retos tecnológicos. El panorama ha cambiado completamente y mafias, agencias de inteligencia e intereses de estado se encuentran tras los ciberataques en su mayor parte, creándose un mercado oculto de tráfico de datos y servicios de hacking que mueve más dinero que el tráfico de drogas a nivel mundial.

Dado este panorama, es fundamental contar con medios de protección a la altura, y como no, esto no pueden ser sólo tecnológicos ni basarse sólo en el conocimiento de un reducido grupo de personas. Para ello se promulgó en 2013 la Estrategia Nacional de Ciber Seguridad (ENCS) que nos proporciona una serie de líneas de acción y actores responsables de llevarlas a cabo con el fin de crear un "ecosistema de la ciberseguridad" en la que los responsables de los activos tecnológicos nacionales y, cómo no, los responsables de la ciberseguridad de las infraestructuras críticas nacionales, puedan sentirse arropados en su batalla diaria.

En el plano de la respuesta ante un ciberincidente que afectase a una infraestructura crítica, en España contamos con el CNPIC como "órgano ministerial encargado del impulso, la coordinación y supervisión de todas las actividades que tiene encomendadas la Secretaría de Estado de Seguridad en relación con la protección de las Infraestructuras Críticas en el territorio nacional" (Ley PIC). En esta línea, el CNPIC apostó desde sus inicios por la ciberseguridad, creando la Oficina de Coordinación Cibernética (OCC) en su seno, y que se según el reciente RD 770/2017 tiene como funciones "ejercer como canal específico de comunicación entre los Centros de Respuesta a Incidentes Cibernéticos (CSIRT) nacionales de referencia y la Secretaría de Estado de Seguridad, desempeñando la coordinación técnica en materia de ciberseguridad entre dicha Secretaría de Estado y sus organismos dependientes".

Estos CSIRT a los que se refiere el RD son conocidos también como CERTs (anteriormente referidos) son equipos con altas capacidades técnicas y de respuesta ante un ciberincidente, coordinados entre sí a nivel nacional

y con otros CERTs a nivel internacional. En España los CERTs de referencia son dos: el CCN-CERT, dependiente del Centro Nacional de Inteligencia (CNI) y focalizado en dar servicio a entidades y operadores del ámbito público; y el CERTSI (CERT de Seguridad e Industria), que da servicio a ciudadanos, empresas y operadores críticos del ámbito privado. Este CERTSI está además operado conjuntamente tanto por personal del Ministerio de Energía, Turismo y Agenda Digital como por personal de la propia OCC perteneciente a Fuerzas y Cuerpos de Seguridad del Estado.

¿Cómo se ejerce esta coordinación ante un ciberataque que afectase a un operador del sector transporte? En primer lugar, el operador debe contar con su propio Departamento de Ciberseguridad, encargado de la primera respuesta. El responsable o CISO sabe que cuenta además con las capacidades del CERTSI o del CCN-CERT (según su ámbito sea público o privado). Ambos operativos 24x7, para en caso de que así lo necesite o requiera asistirle en las labores de contención del ciberataque, mitigación de sus efectos y recuperación de sus sistemas, labores propias de la gestión de un ciberincidente. Esta asistencia se canaliza a través de la OCC, la cual realiza un seguimiento desde el minuto cero de la evolución del ciberincidente. En paralelo, esta OCC puede activar, a requerimiento del operador crítico, la intervención de las Unidades Tecnológicas de la Policía Nacional o de la Guardia Civil, para iniciar la fase de investigación y persecución del delito cometido, el cual puede ser un acto de ciberdelincuencia o de ciberterrorismo.

En definitiva, la cadena de suministro que se asienta en la actividad de los operadores críticos y estratégicos del sector estratégico del transporte tiene una indudable dimensión cibernética imprescindible para llevar a cabo su función de una forma económica y eficiente. A fin de asegurar que los activos tecnológicos que sustentan está operativa sean seguros y resilientes ante un ciberataque, el CNPIC propone la realización de una serie de planes en los que la ciberseguridad es un elemento esencial. Esta implementación de la ciberseguridad no sólo recae en el operador crítico o estratégico, el Estado pone a su disposición diversos organismos y departamentos que lo asisten tanto en el plano técnico como en el de la lucha contra la ciberdelincuencia y el ciberterrorismo, todo ello de forma coordinada mediante la OCC.

04.2 | CiberSeguridad en la Industria 4.0

por **Rafael Rodríguez de Cora**
Director general
Computer Aided Logistics (CALS)

Estamos en el segundo decenio del Siglo XXI, en la llamada Sociedad de la Información, que marca la transición del siglo XX al siglo XXI, también identificado como el paso de la Sociedad Industrial a la Posindustrial.

Aunque el término "Sociedad de la Información" se acuñó en los años 80 del siglo pasado, es al comienzo del presente milenio cuando se considera agotado este concepto y se incorporan otros términos al lenguaje común. Aparecen: la Sociedad del Conocimiento o la Sociedad de la Inteligencia, al considerar la Información como parte de nuestro ecosistema industrial, social y de los negocios.

Desde que Sir Tim Berners-Lee a principio de los años 90 del pasado siglo creara la *world wide web*, el acceso a la información de todo tipo ha ido creciendo y, en paralelo, la información en sí misma también ha aumentado de manera exponencial en volumen y valor.

Las comunicaciones ofrecen mayor ancho de banda a menor precio y la generalización de la conectividad ha hecho posible que no sólo las personas se conecten entre sí o accedan a sistemas remotos sin importar dónde se ubiquen físicamente, de igual manera las máquinas y los dispositivos se han incorporado a la también llamada Sociedad Conectada.

Es la "invasión" conocida como el Internet de las Cosas (IoT), que ya algún autor la define como "Las redes sociales de las máquinas" o "La incorporación de las máquinas a las Redes Sociales".

Está cambiando la manera de hacer negocios, los procesos industriales se controlan a distancia, los clientes y proveedores necesitan estar interconectados y no se puede formar parte de la sociedad sin estar conectado.

Los Negocios 4.0 se multiplican y diversifican, nuevas oportunidades surgen continuamente y entre estos negocios hay uno que está al máximo nivel, aumentando año tras año y sin que se aprecie en el horizonte que vaya a desaparecer o al menos disminuir: Se trata de la llamada **"Ciber-Delincuencia"**.

Hemos conseguido "amontonar" tanta cantidad de Información almacenada en lugares físicos remotos y desconocidos, que se habla de la ubicuidad de la información y como consecuencia las Ciudades Inteligentes (Smart Cities), también empiezan a ser consideradas como Ciudades Ubicuas (Ubiquitous Cities).

Para completar un resumen del panorama actual debemos empezar a considerar otra característica que identifica a esta sociedad que es la abundancia de medios y como

consecuencia el derroche, así se empieza a denominar a la generación Y o de los "post millenials". Disponemos de potencia de cálculo, de almacenamiento y de ancho de banda casi ilimitados y con un precio a veces insignificante.

El llamado *"abandomware"* está empezando a constituir un problema por la cantidad importante de programas, rutinas, e incluso sistemas, que el autor decide olvidarlos incompletos en algún lugar de fácil acceso y que pueden contener información útil para fines espurios.

Los conocimientos tecnológicos son cada vez más profundos y más estrechos, aumentando la especialización y como consecuencia reduciendo la visión conceptual y formal de la empresa, la industria, el mercado y la Sociedad.

LA SEGURIDAD

Si empezamos hablando de Seguridad para particularizar los conceptos en la llamada ciber-seguridad, primero debemos definir el término que según el diccionario de la RAE es:

> **Seguridad.** - *Cualidad de seguro.*
> **Seguro.** - *Libre y exento de riesgo.*
> **Riesgo.** - *Contingencia o proximidad de un daño.*

No sería descabellado construir la siguiente definición:

"Seguridad es la cualidad de estar libre y exento de la contingencia o proximidad de un daño".

En la vida real y más allá del rigor académico, el término se modifica para cada contexto y cuando se intenta conciliar el idioma español con el inglés, es fácil que se complique. Como ejemplo, citemos la aplicación de Seguridad a las voces inglesas "Safety" y "Security" en los entornos industriales.

Para alinearnos con el espíritu de la presente Guía CEL, nos centramos en la **Ciber-Seguridad.**

El primer problema es que no existe en el diccionario de la RAE, por ello tenemos acudir a las definiciones en inglés. Si consultamos en Google el término *"cybersecurity definition"*, encontramos 540.000 resultados que pueden dar luz para encontrar una definición que nos satisfaga.

No hemos revisado todas las definiciones, pero de la lectura de varias comprobamos que es común el término "proteger" redes, ordenadores, programas y datos de daño o acceso no autorizado.

También nos parece interesante la definición de ISACA que hemos traducido como: "La suma de esfuerzos invertidos en abordar los ciber-riesgos, muchos de los cuales han sido considerados **improbables**".

Ciber-riesgo para ISACA es un grupo de riesgos (no uno específico), que se diferencian por la tecnología, vector de ataque, características, etc. pero que tienen en común el potencial de provocar un gran impacto y que alguna vez al menos se les ha considerado improbables.

Nos parece importante la referencia que hace ISACA a que en algún momento se hayan considerado improbables los ciber-riesgos porque este es el origen de muchas brechas de seguridad.

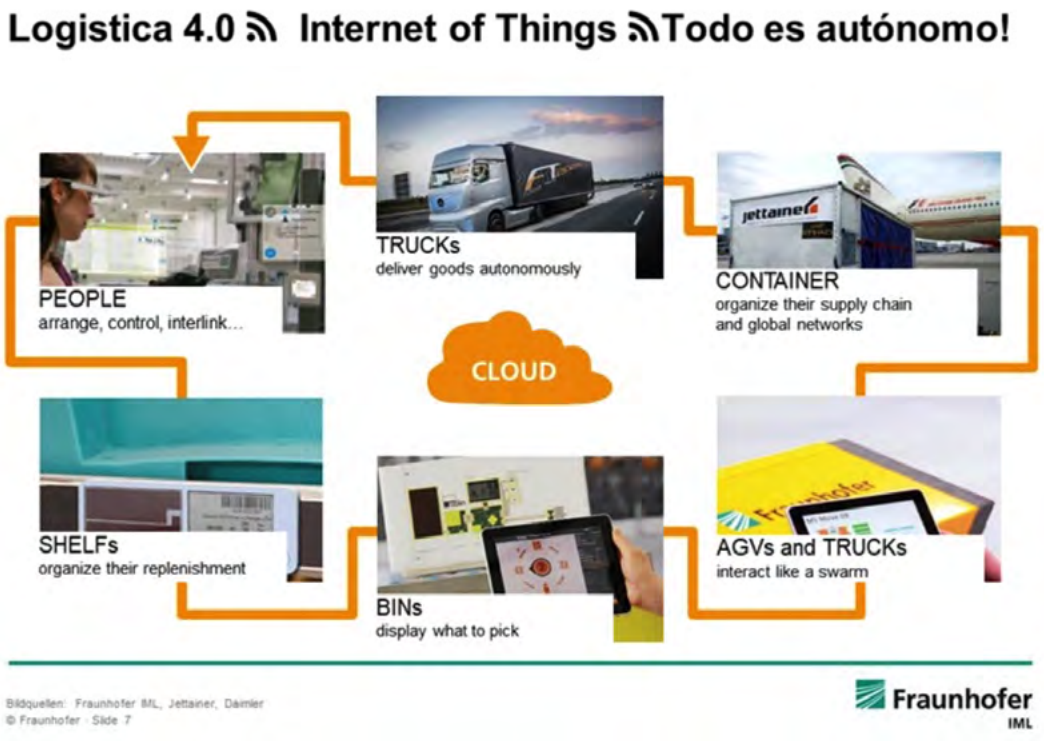
Más allá de esta digresión semántica, queremos establecer unos conceptos básicos que desarrollaremos a lo largo del capítulo.

Esta sociedad está construida sobre una tecnología inherentemente insegura como es el protocolo TCP/IP. Cuando fue diseñado en los años 70 basándose en el concepto de conmutación de paquetes que introdujo Leonard Klienrock a principios de los años 60, no se consideró la vulnerabilidad de los elementos conectados (equipos individuales o PC, equipos de proceso masivo, redes, procesos industriales, etc., etc.).

Cuando se lanzan al mercado productos, equipos o servicios, el proveedor no considera la Seguridad como una característica tan importante como el alcance funcional o el precio, pero el cliente tampoco.

Tenemos ejemplos en todas partes sin excepción:

- El vehículo autónomo (AGV), como los robots, son dispositivos conectados.
- Los sistemas de control de rutas e identificación de vehículos.
- EL SCM (Gestión de la Cadena de Suministro).
- Dispositivos IoT.
- El llamado e-commerce y su repercusión en la logística.



Podríamos continuar con ejemplos, pero baste con pensar en los nuevos desafíos de la Industria 4.0 que ya ha obligado a dar una respuesta con la llamada Logística 4.0.

Los continuos avances tecnológicos aumentan la vulnerabilidad y como consecuencia la Inseguridad.

No se trata de frenar el grado de avance tecnológico, pero sí considerar la seguridad, la protección o la defensa como una característica necesaria de cualquier producto/servicio. La instalación más avanzada puede quedar bloqueada por un ataque de denegación de servicio o sus procesos pueden ser inutilizados o, lo que es peor, pervertidos por la inserción de un malware.

Un empleado puede abrir un email y descargar un fichero aparentemente inofensivo, activando un ataque de consecuencias dramáticas.

Sólo pretendemos alertar tanto a los responsables de la adquisición de productos y servicios como a los usuarios de los sistemas que las medidas de protección y prevención, aunque se basan en tecnología, no son únicamente tecnológicas con un responsable concreto e identificado.

Es altamente ineficaz la política de llamar al responsable de las tecnologías de seguridad para que aplique medidas y así proteger un producto o servicio que la empresa acaba de adquirir o lanzar al mercado, porque será tarde.

De igual manera, las organizaciones deben incorporar la seguridad a su modelo de negocio y evaluar el nivel de riesgo que quieren y pueden asumir porque podemos hablar de graves daños reputacionales, multas por incumplimientos normativos que afecten gravemente la cuenta de resultados y también la imposibilidad de proveer productos/servicios al no cumplir los códigos de seguridad que se incorporan a los contratos de suministro.

Se repite que la seguridad debe abordarse de manera holística, pero en la realidad las empresas mantienen sus estructuras jerárquicas piramidales y cada departamento vertical entiende de "su seguridad" encargando a IT la responsabilidad tecnológica.

Es tiempo de abordar la seguridad con un "enfoque sistémico". Es decir, considerar la empresa y su seguridad como un sistema en su totalidad, complejidad y dinámica. En resumen: la organización en su totalidad es mucho más que la suma de las partes.

Hay diferentes metodologías, pero hemos elegido la propuesta por Sogeti.

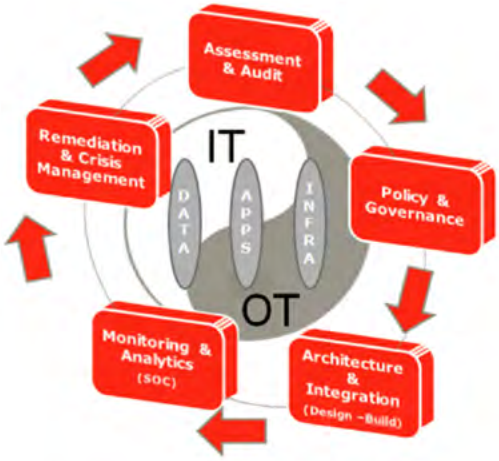
Evaluación y Auditoría: Identificación de riesgos y vulnerabilidades, así como del nivel actual de madurez en seguridad.

Políticas y Gobernanza: Servicios de consultoría orientados al análisis de riesgos, desarrollo de políticas de seguridad, concienciación, formación y organización.

Arquitectura e Integración: Definición de la arquitectura de seguridad elegida y la implantación de los componentes de seguridad.

Seguimiento y Analítica: Visibilidad de todos los incidentes de seguridad en sistemas de información que requieren acciones correctivas y mantenimiento. Detección de eventos que supongan comportamientos hostiles.

Remediación y Gestión de crisis: Gestión de crisis extremo a extremo (típicamente después de un ataque o infección masivos).



Fuente: SOGETI

Nos parece completa sencilla y que contempla tanto el ambiente IT como el OT que deben convivir en la Industria 4.0

Otro aspecto importante es la implantación de un **sistema de gestión de la seguridad integrada** y en tiempo real que nos permita hacer un seguimiento pormenorizado con proyección sobre el negocio, solo así los máximos responsables podrán conocer el impacto de sus decisiones y aproximarse a un modelo de Inversión en Seguridad como contrapunto a la situación actual donde únicamente se controla el Gasto en Seguridad.

HERRAMIENTAS / TECNOLOGÍA DE SEGURIDAD / PROTECCIÓN / DEFENSA

Para poder implantar medidas de Defensa en una Organización primero habrá que conocer las vulnerabilidades y los vectores de ataque que podemos recibir. Instalar "lo último en ciberseguridad" o lo que se considere la solución más avanzada puesta en el mercado por la empresa más potente, solo sirve para que el que tome la decisión se sienta más protegido, pero la organización no lo estará necesariamente en la misma proporción.

Los planes de seguridad tendrán como primer objetivo informar de manera clara a la Dirección las repercusiones en el negocio de los ataques más frecuentes que puedan recibirse. Así como las medidas de prevención, remediación y recuperación de desastres. De esta forma, se conocerá el coste de estas medidas en comparación con el valor de los daños y así tomar la decisión que sólo corresponde a los máximos responsables y el nivel de convivencia con el riesgo que la organización decide asumir. Esto es el llamado *Risk Appetite*, una mala traducción literal del inglés llamamos Apetito de Riesgo.

Los ataques pueden ser dirigidos en los cuales los delincuentes estudian una organización para identificar sus brechas y vulnerabilidades, preparando de esta manera el ataque. También pueden ser masivos donde se utilizan herramientas de carácter general y cuando el código maligno alcanza un objetivo y se infiltra en un sistema, comunica el éxito al origen y se identifica la víctima para completar la "acción".

Estos ataques suelen utilizar medios baratos que reportan el mayor beneficio al atacante. Según la publicación *Information Age*, la media de permanencia de un ataque en un sistema antes de ser descubierto es de 200 días, tiempo suficiente para lograr sus objetivos.

Los principales vectores de ataque en 2016 fueron:

- Ataques de denegación de servicio.
- Malware y Ransomware.
- Ataques a Aplicaciones específicas.
- Ataques a Aplicaciones web.

Las Herramientas más comunes a tener en cuenta bajo un enfoque sistémico de la ciberseguridad es que, al considerarlas individualmente ofrecen un nivel de protección inferior al que se puede obtener aplicando un Plan Global para la Organización.

- Protección contra código malicioso malware. (Antivirus).
- Protección contra ingeniería social y fraude.
- Contingencia y continuidad.
- Protección de las comunicaciones.
- Protección de los datos (copias de seguridad).

- Hábitos de conductas seguras.
- Herramientas para situar a las personas en el centro de la seguridad.

La principal característica de la Sociedad 4.0 es la interconexión. En el área que nos ocupa, la producción, suministros, pedidos de clientes y distribución estarán interconectados y en todos estos procesos los dispositivos conectados tendrán mayor protagonismo. La ciberinseguridad crecerá con la ubicuidad de los procesos, los controles, los automatismos y los sistemas. Recientemente, ya hemos asistido a ataques de denegación de servicio a través de una red de *"zombies"* (botnet) creada con dispositivos conectados, cámaras de video-vigilancia y Smart TV que en la actualidad no son muy numerosos en comparación con las previsiones de crecimiento.

Debe diferenciarse entre la solución a los ataques y la gestión de los riesgos, que debe ser integrada y en tiempo real. La costumbre de asociar los ataques y sus medidas de protección y prevención a los informáticos, es poco eficaz. Las medidas deben aplicarlas especialistas y la gestión debe llevarla a cabo generalistas y ambos colectivos suelen hablar "diferentes idiomas".

"La Herramienta Universal" no existe. Sólo la cooperación entre diversas herramientas y medidas de seguridad, podrá acercarse al nivel de convivencia con el riesgo que se esté dispuesto a asumir.

El porcentaje del presupuesto en seguridad que se dedique a programas anuales de concienciación para los usuarios (empezando por la Alta Dirección), debe estar en consonancia con el riesgo de ataques cuya brecha de seguridad proviene frecuentemente de las malas prácticas de las personas.

Como ejemplo, un ataque de ransomware (cifrado de ficheros), comienza con la apertura de un fichero por parte de un usuario. Son las conocidas campañas de phising o usurpación de personalidad y es recomendable que cada empresa medite sobre este riesgo y el coste de crear hábitos seguros en los empleados.

Se pueden instalar las herramientas más caras y sofisticadas del mercado, pero solo alcanzarán el máximo grado de efectividad si forman parte de propio Plan de Seguridad. Éste debe permitir convivir en el Universo conectado con un nuevo orden superpuesto al geoestratégico, geopolítico o geoeconómico, donde las fronteras convivirán con los dominios genéricos de Internet (COM, NET, ORG, EDU, GOB y MIL).

Podemos concluir que las Organizaciones (empresas, negocios), experimentarán en paralelo un mayor grado de desarrollo y un mayor nivel de inseguridad ("ciber –inseguridad") que vendrán dados por la necesidad constante de incrementar la conectividad, la ubicuidad y el uso intensivo de información.

Los planes de protección y las medidas de seguridad serán más exhaustivas y costosas, cambiaremos los presupuestos de gasto en seguridad, por planes de inversión y al igual que nuestros clientes incluirán en los contratos de suministro medidas mínimas de seguridad verificables, nosotros haremos lo mismo con nuestros proveedores.

04.3 | La Directiva Europea de Seguridad NIS y la Protección de Infraestructuras Críticas

por **José Valiente**
Director
CCI, Industrial Cybersecurity Center

El transporte (aéreo, marítimo, fluvial, por ferrocarril y por carretera) es un servicio esencial con infraestructuras críticas, y sus operadores estarán obligados por la transposición de la Directiva de Seguridad de las Redes y de la Información (NIS, por sus siglas en inglés) a notificar los ciberincidentes de cierto impacto a partir de mayo de 2018.

La NIS aprobada por el parlamento europeo el 6 de julio de 2016, tiene su origen, como idea, en 2001 en la convención de Budapest, único cibertratado con el objetivo de la armonización universal de la normativa del derecho penal nacional y la persecución penal de los delitos relacionados con Internet. Ratificado por España en 2010.

Son múltiples los esfuerzos de la Unión Europea por impulsar la protección contra los ciberataques, para lo cual se han llevado acabo diversas iniciativa y publicación de documentos entre los que cabe destacar;

- En 2001, COM (2001)209 "Seguridad de las redes y de la información. Propuesta para una política europea".
- En 2004, la Comisión Europea estableció ENISA con el objetivo de desarrollar la cultura NIS.
- En 2006, se publica COM (2006) 251"Estrategia para una sociedad de información segura".
- En 2009, una Decisión del Consejo 2009/C 321.01 "De un enfoque europeo común sobre la seguridad de la información y de las redes".
- De 2010, COM (2010) 245 "Una agenda digital para Europa".

Los esfuerzos en la última década de la Unión Europea se han centrado en la protección de infraestructuras críticas, desarrollando el "Programa Europeo de protección de infraestructuras críticas (EPCIP)", COM (2006) 786, la Directiva (2008) 114/UE y la Comunicación y el Plan de Acción COM(2009) 149, y de 2011 la Comunicación "Resultados y siguientes pasos. El camino para la seguridad global de la red" COM (2011).

La Directiva que se transpone pretende implantar una cultura de ciberseguridad en las empresas y entidades que gestionan servicios esenciales para la sociedad y la economía de los distintos países que son estados miembro y, por ende, para el buen funcionamiento del mercado interior.

La prestación de esos servicios está cada vez más ligada a las redes y sistemas de información por el tratamiento tan intenso de los datos (personales o no) mediante técnicas de "Big Data" y por la creciente automatización de los procesos internos de producción y gestión económica. Ello implica, a su vez, una mayor exposición a los riesgos que existen en el empleo de una red abierta y global. En este caso, Internet es un canal por el cual también se difunden infecciones de virus y programas maliciosos que pueden llegar a interferir en la prestación de servicios esenciales, provocar fugas de datos personales, comprometer información confidencial de valor comercial y afectar, en fin, al funcionamiento de dicho mercado interior. Como demuestran las estadísticas de los CERTs españoles, el número de incidentes gestionados ha ido en aumento en los últimos años.

Por ello, la Directiva impone a las entidades gestoras de servicios esenciales, así como a los prestadores de ciertos servicios digitales considerados clave en el funcionamiento de Internet. La obligación de establecer sistemas de gestión de la seguridad de la información en sus organizaciones y de notificar a las autoridades los incidentes que tengan especial gravedad. Así mismo, obliga a los Estados miembros a dotarse de los medios para supervisar el cumplimiento de estas obligaciones y a velar porque existan equipos de respuesta a incidentes de seguridad con capacidad para proteger a las empresas de la propagación de estos incidentes. Así mismo, impulsa la cooperación entre autoridades nacionales y el intercambio de información como medio para elevar el nivel de seguridad en la Unión Europea frente a amenazas de carácter transfronterizo.

La directiva exigirá la aplicación a partir del 10 de mayo de 2018 de las disposiciones de transposición de la Directiva en cada Estado; la adaptación de las Estrategias nacionales de seguridad de las redes y sistemas de información a los contenidos mínimos establecidos en su artículo 7, y la determinación de las entidades obligadas a cumplir la Directiva, por prestar servicios esenciales, antes del 9 de noviembre de 2018.

En España, los operadores de infraestructuras críticas se verán mínimamente afectados por la nueva Ley que transpone la directiva. Esto es debido a que la ley 8/2011 para la protección de infraestructuras críticas y su reglamento contemplan la mayoría de las directrices de la directiva NIS, y por lo tanto de la nueva ley que se publique.

Es importante aclarar que el término Infraestructura Crítica se emplea por los Estados para definir instalaciones y sistemas sobre los que recaen servicios esenciales cuyo funcionamiento no permite soluciones alternativas. Las infraestructuras críticas existentes en un estado, se agrupan dentro de sectores estratégicos: aquellos que son esenciales para la seguridad nacional o para el conjunto de la economía de un país (defensa, energía, aeroespacial, nuclear, administración, financiero, etc.).

La Protección de las Infraestructuras Críticas surge como respuesta de los gobiernos a los riesgos y a la necesidad de proteger el complejo sistema de infraestructuras que dan soporte y posibilitan el normal desenvolvimiento de los sectores productivos, de gestión y de la vida ciudadana en general. Para ello, los distintos países han abordado dicha problemática bajo distintas perspectivas, que se pueden resumir en: establecimiento de un marco normativo estricto; fomento de las relaciones público-privadas; establecimiento de un marco normativo básico acompañado de una serie de medidas para fomentar las relaciones público- privadas. En cualquier caso, el objetivo fundamental de la Protección de las Infraestructuras Críticas es el desarrollo, implantación o mejora de las medidas de seguridad oportunas, tanto en su vertiente física como lógica/cibernética, que deben acometer los operadores propietarios o responsables de su gestión, de cara a garantizar un nivel de protección adecuado.

Si bien las actividades derivadas de la Protección de las Infraestructuras Críticas presentan un criterio común, salvo ligeras variaciones en función del país del que se trate, el concepto de Ciberseguridad Industrial que tan solo hace unos pocos años no estaba tan extendido, empieza a cobrar un relevante importancia.

La Ciberseguridad Industrial trata de mejorar la resistencia de los sistemas industriales y su recuperación, ante acciones hostiles o inesperadas que puedan afectar al correcto funcionamiento de los procesos industriales.

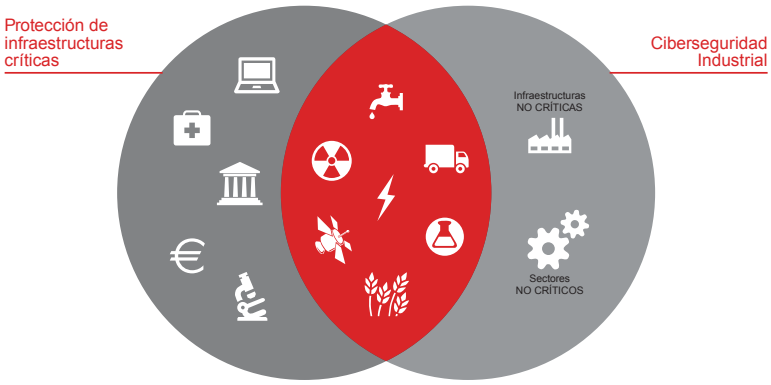
Definimos la Ciberseguridad Industrial como el conjunto de prácticas, procesos y tecnologías, diseñadas para gestionar el riesgo del ciberespacio derivado del uso, procesamiento, almacenamiento y transmisión de información utilizada en las organizaciones e infraestructuras industriales, utilizando las perspectivas de personas, procesos y tecnologías. Esto incluye el patrimonio tecnológico de las industrias, entendiendo como tal aquellos activos intangibles que se derivan del trabajo intelectual, específicamente una idea, invención, secreto industrial, proceso, programa, dato, fórmula, patente, copyright, marca, aplicación, derecho o registro. Este patrimonio, puede ser o no catalogado como una infraestructura crítica (dependiendo del sector en el que se enmarque) pero siempre será el principal activo a proteger por las industrias.

Desde un punto de vista operativo, la Ciberseguridad Industrial sería de aplicación en todos los entornos que

contengan sistemas de control industrial. Estos sistemas controlan procesos físicos que van desde la producción y distribución de energía, a la manufactura automatizada, pasando por la logística, las industrias alimentaria, aeronáutica, aeroespacial, farmacéutica, de telecomunicaciones o de automoción y, en definitiva, cualquier proceso que requiera algún tipo de automatización mecanizada.

La Protección de Infraestructuras Críticas requerirá en ocasiones el uso de métodos y tecnologías propias de la Ciberseguridad Industrial, pero no todas las acciones de la Ciberseguridad Industrial estarán asociadas a una Infraestructura Crítica, aunque dentro de su ámbito de actuación puedan ser igualmente importantes.

Por lo tanto, atendiendo al número de instalaciones que abarca la Ciberseguridad Industrial, ésta es un concepto más amplio que la Protección de Infraestructuras Críticas, ya que la mayoría de las instalaciones industriales existentes no estarán catalogadas como críticas. Sin embargo, la Protección de Infraestructuras Críticas, abarca sectores que no están incluidos dentro del ámbito de la Ciberseguridad Industrial, ya que algunos de estos sectores como la Administración Pública, o el sector financiero no tienen el componente industrial requerido para estar dentro del ámbito de la Ciberseguridad Industrial.



Fuente: "La Protección de Infraestructuras Críticas y la Ciberseguridad Industrial", CCI, octubre de 2013

Por lo tanto, es evidente que existen importantes sinergias entre los dos conceptos, PIC y CI, que lejos de suponer una duplicación de esfuerzos, si éstos están bien orientados, son complementarios y pueden apoyarse mutuamente.

En el caso de la Protección de Infraestructuras Críticas, es habitual que la aproximación nazca en los niveles superiores, debido a las exigencias de cumplimiento legislativo y desde ahí se extienda hacia los inferiores. Este camino, como todos los que tienen su origen en la alta dirección, es rápido, pero tiene como punto de partida unos requisitos más o menos abstractos que pueden diluirse al llegar a niveles inferiores, haciendo que las medidas implantadas no aporten el valor real planeado, sino que se queden en acciones para la galería únicamente destinadas a lograr el cumplimiento legislativo exigido, según se indica en el documento publicado por CCI "La Protección de Infraestructuras Críticas y la Ciberseguridad Industrial" [Ref. 001].

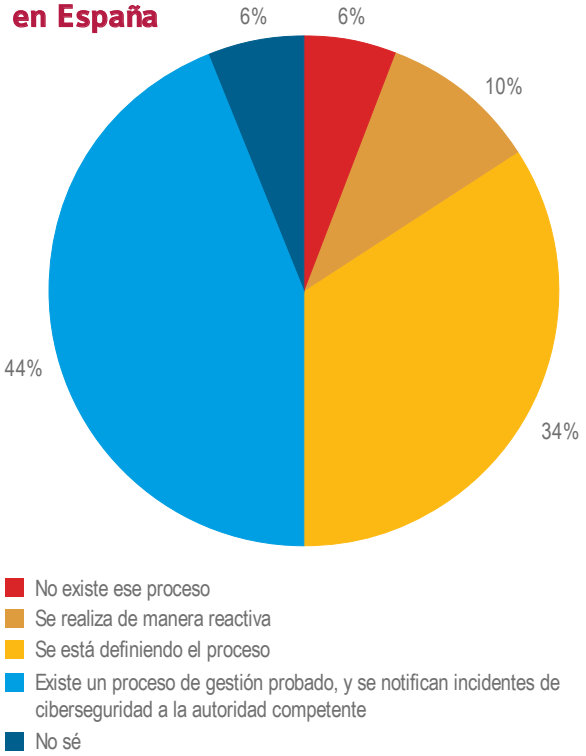
Cada vez es mayor el número de organizaciones industriales que han empezado a dar pasos firmes para afrontar los desafíos que supone la Ciberseguridad Industrial. La existencia de organismos públicos como el CNPIC y la Oficina de Coordinación Cibernética (OCC) del Ministerio del Interior, e INCIBE, del Ministerio de Industria, Energía y Turismo, encargados de coordinar e impulsar la protección de infraestructuras críticas, así como la reciente actualización del Plan Nacional de Protección de las Infraestructuras Críticas (PNPIC) que pone especial acento en la protección ante ciberataques son una clara apuesta del Estado en este sentido. Por otra parte, la mayor adopción de estándares reconocidos internacionalmente como IEC 62443, o de guías como la publicada por CCI recientemente, "Guía para la Construcción de un SGCI: Sistema de Gestión de la Ciberseguridad Industrial" [Ref. 002] lo están facilitando. Una prueba de los avances que se están produciendo es la existencia de un conjunto consolidado de proveedores de servicios y profesionales de la ciberseguridad en la automatización de procesos industriales que se encuentran recogidos, en su gran mayoría, en el "Catálogo de Proveedores de Servicios y Soluciones de Ciberseguridad Industrial" [Ref. 003], publicado en 2015 por el CCI, y que ha sido renovado en 2017, el cual se ha convertido en una herramienta fundamental para ayudar a las organizaciones industriales a cubrir sus necesidades en este campo.

Es cierto, que todavía debería avanzarse en metodologías que permitan el desarrollo de productos seguros desde el diseño y en la capacidad por parte de los clientes de verificar la seguridad de los componentes utilizados en sus redes y sistemas, especialmente ahora, que se están definiendo nuevos modelos como Industria 4.0 o Internet Industrial de las Cosas. Esta nueva era de la digitalización industrial es una oportunidad única para empezar a contemplar la ciberseguridad en las etapas más tempranas, como así se recoge en el documento "Ciberseguridad en el Ciclo de Vida de un Proyecto de Automatización Industrial" [Ref. 004] también publicado en 2016 por el CCI.

Por lo general, es habitual asumir que las acciones emprendidas para mejorar la Ciberseguridad Industrial en una organización estarán enfocadas en la continuidad de sus procesos de negocio. Sin embargo, hoy en día, gran

parte de los incidentes de ciberseguridad tienen como objetivo obtener acceso a la propiedad industrial de las organizaciones, las cuales deben establecer las salvaguardas necesarias para proteger su conocimiento especializado, que supone uno de sus activos más valiosos. Aunque como podemos apreciar en la siguiente gráfica, en el 56% de los operadores de infraestructuras críticas en España, todavía no existe un proceso de gestión de incidentes probado. Algo imprescindible para cumplir con la directiva NIS.

Proceso de gestión de incidentes en Operadores de Infraestructuras críticas en España



Cualquier organización en el ámbito de la logística cuenta hoy en día con importantes procesos que sustentan su negocio. Buena parte estos procesos basados sobre sistemas de control industrial, al igual que su información y sistemas corporativos, deben ser protegidos, puesto que cualquier incidente en su entorno puede suponer importantes pérdidas económicas y en muchos casos hasta personales.

La Ciberseguridad Industrial es la disciplina que aborda esa protección y por tanto es indispensable para estas organizaciones estar en este ecosistema, de forma que permanezcan actualizadas en los últimos avances, puedan intercambiar experiencias con organizaciones similares y tengan acceso a información de primera mano. La única vía de éxito en este ámbito es la colaboración que puede conseguirse asegurando la existencia de actores independientes cuya finalidad sea impulsar la Ciberseguridad Industrial y ejercer de catalizador dentro del ecosistema, como es el caso internacional del Centro de Ciberseguridad Industrial.

CONCLUSIONES

La normativa inminente, como es la directiva NIS, y el riesgo constatado por los incidentes cibernéticos constantes, es un aviso que puede convertirse en importantes pérdidas económicas y en muchos casos hasta personales.

Las organizaciones de transporte, y las que forman parte de la cadena de suministro, ya no pueden permitirse en un escenario global, como el nuestro, no gestionar todavía los riesgos tecnológicos derivados de la automatización cada vez mayor de su operación.

REFERENCIAS

[Ref. 001]
CCI. "Mapa de Ruta de la Ciberseguridad Industrial en España".
1 de julio de 2013.
URL: https://www.cci-es.org/mapa

[Ref. 002]
CCI. "Guía para la Construcción de un SGCI: Sistema de Gestión de la Ciberseguridad Industrial".
30 de marzo de 2016.
URL: https://www.cci-es.or g/SGCI

[Ref. 003]
CCI. "Catálogo de Proveedores de Servicios y Soluciones de Ciberseguridad Industrial".
31 de marzo de 2015 (Primera edición). Edición actual 7 de abril de 2016.
URL: https://www.cci-es.org/catalogo

[Ref. 004]
CCI. "Ciberseguridad en el Ciclo de Vida de un Proyecto de Automatización Industrial".
5 de mayo de 2016.
URL: https://www.cci-es.org/ciclo

05 | Los profesionales del Siglo XXI: Nuevas competencias y gestión del cambio

por **Marina Rodríguez Valentín-Gamazo**
Directora
Windmill Consultants

Al hilo de todos los cambios y disrupciones que están transformando la Cadena de Suministro y que están contemplados en esta guía, es imperativo hacer referencia a los profesionales que trabajan en este campo. Como veremos a lo largo de este capítulo, tanto puestos de trabajo como trabajadores, se ven impactados de lleno por los hábitos de consumo, la tecnología y la Industria 4.0.

De forma resumida, la Logística del presente y del futuro cercano es más rápida, más segura, más barata y personalizada.

Para llegar a esto, los trabajadores no podrían haberlo hecho, sin contar con el gran aliado que es la tecnología que está implantándose a todos los niveles y que a su vez abre nuevos interrogantes y retos en su gestión.

Las palancas tecnológicas más destacables son las siguientes:

- La automatización progresiva mediante la hiperconectividad, la movilidad, el IoT, el desarrollo de la robótica colaborativa y la utilización de los "wearables".
- El uso masivo de los datos cristaliza en sistemas de Inteligencia Artificial que planifican trabajos y toman decisiones de forma autónoma.
- Las plataformas tecnológicas colaborativas que permiten conectar de manera directa oferta y demanda (P2P) de servicios logísticos a todos los niveles: almacenamiento, transporte y reparto.

A continuación, veamos con más detalle estas tecnologías y su impacto.

LOS WEARABLES

Los "wearables" o su definición española, "tecnología vestible" o "tecnología corporal" se refiere a dispositivos electrónicos que llevamos encima para realizar una función concreta y con el que interactuamos.

El desarrollo de estos dispositivos en su diseño HW, en capacidad de proceso, experiencia de usuario y precios asequibles está favoreciendo una importante adopción de estas tecnologías tanto en el ámbito de uso personal como empresarial.

Se trata de aliados muy importantes para los trabajadores que realizan tareas manuales en campo (fábrica, almacén...) y que no tienen un puesto de trabajo fijo.

Unos ejemplos de los dispositivos wearables que se están empleando en el ámbito de la Industria 4.0 y de la Cadena de suministro inteligente son:

- Gafas de realidad aumentada para realizar picking mediante visión, guiando al personal a través del almacén.
- Casco inteligente que monitoriza constantes vitales y que transmite ordenes de trabajo.
- Escáner en forma de anillo.
- Tablets y pequeños ordenadores montados sobre una muñequera que se pueden manejar por voz.
- Auriculares inalámbricos para trabajar con aplicaciones gestionadas por voz.

Los wearables introducen una nueva forma de trabajar y aumenta la satisfacción laboral ya que son dispositivos intuitivos, fácil de aprender, con instrucciones claras y precisas. También permite tener mayor visibilidad y control de la fuerza laboral e incluso mejora la formación con manuales cargados en el dispositivo.

Para las empresas y el cliente final:

- Reduce los paseos, el tiempo necesario para la selección de ítems y los errores.
- Reduce tiempos y costes mediante la mejora del flujo de información.
- Mejora la flexibilidad en el servicio, trazabilidad de los envíos, multicanalidad y disminución de tiempo.
- Facilita el seguimiento de activos y supervisión de inventarios.

ROBÓTICA COLABORATIVA O SENSITIVA

Hasta ahora, los robots en plantas estaban encerrados en celdas de fabricación sin contacto con humanos. Hoy la robótica permite que los robots interactúen con los humanos en lo denominado Robótica Colaborativa/ Sensitiva. Esto es:

Los robots o cobots (del inglés "collaborative robots"): no utilizan vallado de seguridad, son fácilmente programables, por personal no cualificado y sin conocimientos de programación.

Los robots colaborativos son una solución interesante para las pymes ya que realizan trabajos repetitivos y pueden ser programados por personal no cualificado sin conocimientos de programación.

Los robots sensitivos: van más allá de los colaborativos porque tienen sensores que les permite trabajar con los humanos. Están diseñados con formas redondeadas y tienen control de fuerza en los ejes para que se paren ante un obstáculo y pueden desconectarse para no dañar a operarios.

El grado de penetración de los robots en almacenes y transporte todavía no es muy alto. Según el informe de DHL "La robótica en la logística" de 2016, el 80% de las tareas de la logística todavía son manuales debido "a la complejidad del trabajo y al manejo de una amplia gama de cosas diferentes en un número infinito de combinaciones de forma conjunta con humanos y en espacios confinados".

No obstante, la tecnología está desarrollando a gran velocidad una nueva generación de robots de alta sensibilidad y bajo coste que puedan ver, moverse y reaccionar frente al entorno, así como trabajar en tareas de precisión junto con humanos. Según este estudio de DHL, las tareas que podrían realizar son:

- **Pick & Place:** Reduce la duración de los ciclos de paletización y despaletización.

- **Paletizado y empaquetado:** El cobot se encarga de estas tareas según los niveles de calidad y exigencia más elevados.

INTELIGENCIA ARTIFICIAL

Esta tecnología impulsa el desarrollo de cadenas de suministro inteligentes que utilizan sistemas de aprendizaje automático. Esta logística autónoma y basada en datos, permitirá grandes niveles de optimización en la fabricación, logística, almacenamiento y entrega. A su vez, tiene un impacto muy significativo en las personas en varios frentes:

a. Optimización

La asignación y optimización de recursos es una palanca clave de la logística y la IA sirve para la predicción de la demanda->la gestión de stocks->asignación automática de equipos de trabajo en almacén.

Otro de los usos de la IA es la predicción de rutas de transporte y entrega mediante el estudio y análisis de datos obtenidos del seguimiento del transporte a través de satélite haciendo que la ruta de entrega sea lo más eficaz posible.

b. Tratamiento de problemas complejos

El nivel de incertidumbre, volatilidad y personalización de la logística del presente plantea una enorme variabilidad de situaciones y problemas. Asignar personas a resolverlo, resulta bastante costoso, además de proclive al error.

En cambio el uso de algoritmos permite solucionar estos problemas de manera fiable y barata. Por ejemplo sirve para tratar situaciones inesperadas de tráfico, atascos y colapso de vías de comunicación, y seleccionar mejores rutas y modalidades de transporte para la realización de entregas

c. Latencia cero

Significa tener un tiempo de reacción inmediato. Uno de los mayores obstáculos es la complejidad organizativa, la dispersión de la información en varios departamentos, así como el flujo de aprobaciones. Esto supone que las personas dediquen mucho tiempo y esfuerzo a la recopilación de información y a pasar por diferentes "puertas" de la organización.

Gracias a la Inteligencia Artificial se puede conseguir que la información fluya a través de las redes corporativas y se pueda operar con ella de manera ágil y precisa.

d. El transporte autónomo

Aunque ya es un hecho en su fase de I+D y laboratorio, la implantación masiva de la conducción autónoma todavía está por llegar ya que tiene serios impactos a todos los niveles.

Desde le punto de vista del trabajo y la seguridad, se abren interrogantes tales como la potencial desaparición de los conductores y las profesiones relacionadas con el transporte. También el potencial daño que los vehículos puedan hacer a los peatones, a otros vehículos, a las mercancías, etc… y por último las atribuciones de responsabilidad en caso de accidente.

Dentro del transporte autónomo merece la pena señalar el caso especial de los Drones y el alto potencial que tienen para el campo de la logística, porque realmente serían la solución a muchos problemas.

Las profesiones relacionadas con la operación (pilotos) y mantenimiento de drones han despertado grandes expectativas. Sin embargo, esto es cuestionable en este momento por las mismas razones de vacío legal y restricciones regulatorias que hemos mencionado anteriormente.

LAS PLATAFORMAS COLABORATIVAS

Son "Marketplaces" que conectan a usuarios con ofertantes de todo tipo de servicios relacionados con la cadena de suministro. Ya existen las que promocionan y alquilan por un periodo determinado espacios libres en almacenes y en camiones, pero estas no tienen un impacto directo en el empleo. Sin embargo, queremos destacar aquí aquellas que están teniendo una adopción y crecimiento más rápido. Se trata de aquellas plataformas que ofrecen transporte de mercancías dentro de las ciudades para cubrir la última milla hasta el punto de entrega al usuario.

Estas empresas propician el crecimiento del número de transportistas individuales que trabajan por horas bajo el régimen de autónomos. En España, estamos viendo en las grandes ciudades la presencia de ciclistas repartiendo paquetes y comida bajo la marca de alguna de estas plataformas colaborativas.

¿Cuáles son las oportunidades y los retos para el empleo en la Cadena de Suministro del siglo XXI?

Tras analizar lo expuesto en este capítulo, vemos cómo la implantación de la cadena de suministro del siglo XXI trae consigo numerosas ventajas para los trabajadores y empresarios. No obstante, como en todo cambio disruptivo se dejan atrás tecnologías, formas de trabajar, conocimientos, profesiones, etc.

Nos encontramos en plena transformación, la Industria 4.0 y la Logística Inteligente todavía no están maduras y por ello se abren muchos interrogantes en relación con las personas y el empleo.

A continuación, se realiza un análisis de las ventajas y oportunidades y de los retos que tenemos que enfrentar para hacer realidad esa cadena de suministro inteligente:

	OPORTUNIDADES	RETOS
SEGURIDAD Y SALUD	El internet de las cosas y los empleados conectados facilitan que se pueda localizar a los trabajadores en áreas de trabajo extensas y/o peligrosas, y se puedan monitorizar sus constantes vitales para prevenir ciertos riesgos en la salud.	Existen muchas preguntas y dudas acerca de cómo tratar los datos que genera el empleado en su actividad y cómo proteger su privacidad. Mientras esto no se solucione, no se desarrollará la logística inteligente a gran escala.
	La ergonomía en la realización del trabajo manual se ve beneficiada por la asistencia de robots, "wearables" o exoesqueletos. Con ellos se pueden reducir patologías, accidentes y bajas laborales.	Los robots, "wearables" y exoesqueletos son nuevos elementos que a su vez conllevan nuevos riesgos que hay que gestionar y que habrá que aprender a trabajar con ellos.
	Una planificación más precisa y certera gracias a algoritmos de inteligencia artificial favorece la reducción del estrés y ansiedad derivada de la imprevisibilidad y variabilidad de la carga de trabajo.	Una carga de trabajo optimizada y precisa, probablemente requerirá menos trabajadores, lo cual puede generar desmotivación y riesgos psicosociales.

	OPORTUNIDADES	RETOS
NUEVAS PROFESIONES	**La automatización de tareas y actividades.** Por ejemplo: • Tareas manuales rutinarias como el paletizado. • Tareas intelectuales no rutinarias: planificación y optimización de rutas de transporte. Implica que aparecen nuevas tareas y actividades a realizar. Esto supone nuevas oportunidades profesionales y nuevos nichos de empleo. Motivación e ilusión por el desarrollo profesional y la empleabilidad.	¿Cómo realizar una transición suave entre el mundo analógico y digital? Identificación temprana de actividades y tareas en extinción: • Gestionar las potenciales pérdidas del puesto de trabajo. • Redefinición de roles y funciones. • Determinar qué nuevas capacidades y conocimientos son necesarias. • Poner en marcha un plan de capacitación y soporte al cambio.
	Un mercado laboral activo y dinámico con puestos de trabajo de mayor cualificación: conocimientos y competencias para trabajar en entornos digitales.	¿Cómo gestionar la "brecha digital"? Con el objetivo de preparar y capacitar a los trabajadores para incorporarse o adaptarse a las nuevas reglas del juego. De lo contrario habrá bolsas de desempleo de larga duración y con bajas posibilidades de reincorporarse a la actividad.
	Nuevos nichos de empleo en la economía colaborativa: Ventajas para el cliente: Se puede lograr una gran flexibilidad y personalización en la entrega de mercancías, así como precios muy bajos por el servicio. Ventajas para el trabajador: Gracias a esto se genera actividad laboral e ingresos para los trabajadores. En definitiva, se genera empleo.	Retos de seguridad en la cadena de Suministro: existen vacíos legales en cuanto a la asignación de responsabilidades en caso de accidente, pérdida, robo... ya que son trabajadores autónomos sin vinculación laboral con las plataformas y con salarios muy bajos que muchas veces no permiten tener seguros de responsabilidad civil, etc. En cuanto a los retos para los trabajadores, podemos afirmar que existen dudas acerca de la calidad del empleo ya que en muchos casos hay vacíos legales que pueden llevar a la desprotección de los trabajadores o a la creación de "falsos autónomos" cuando en realidad existe una dependencia laboral. Estas situaciones hacen que los trabajadores no tengan vinculación y pertenencia, ni planes de formación, de prevención de riesgos laborales, etc.

No queremos cerrar este capítulo sin hacer una serie de consideraciones que es bueno tener en cuenta a la hora de pensar en el futuro del trabajo en la Logística del siglo XXI.

- España es un país de PYME. La digitalización puede ser un impulsor para la competitividad y sostenibilidad de muchas y un factor de motivación y empleabilidad para sus trabajadores.

- La mayoría de las PYME se enfrentan a 4 obstáculos para lograrlo:

1. Falta de fondos o desconocimiento de las fuentes de financiación.

2. Desconocimiento de la tecnología y sus posibilidades.

3. No tienen personas preparadas para llevar a cabo este tipo de proyectos.

4. No tienen líderes preparados para el cambio.

- Es importante el soporte y la guía para las pequeñas y medianas empresas desde instituciones, centros de formación, patronales...

- Es necesario un relevo generacional y el desarrollo de una cultura de trabajo digital a todos los niveles de la empresa.

- Por último, destacamos que tanto sindicatos como patronal coinciden en la urgencia de iniciar el diálogo social para facilitar la implantación de la tecnología de forma ordenada y que los Agentes Sociales se involucren en ordenar este cambio.

06 | Implicaciones legales de la Industria 4.0

por **Ramón Mesonero-Romanos**
Socio CECA MAGAN Abogados y responsable de Área de Estrategia, Negocio y Transformación Digital
Comtrust

y **Noemi Brito**
Socia de Legistel y responsable del Área de IT Governance, Risk and Compliance (IT GRC)
Comtrust

*La **Industria 4.0**[1] también denominada la **Cuarta Revolución Industrial**[2], implica una nueva era marcada por la interrelación de tecnologías digitales, físicas y biológicas, que da lugar a un mundo lleno de oportunidades. Este escenario se erige sobre la infraestructura de la anterior revolución digital, al tratarse de un proceso ascendente donde las empresas y fábricas están abocadas a una necesaria adaptación a través de la implementación de estas tecnologías. Esto ocurre no solo para soportar y contrarrestar la competencia, sino también para buscar la eficiencia y rentabilidad e, incluso, su propia supervivencia, a través de ineludibles procesos de conversión digital.*

Según estimaciones de estudios recientes, la digitalización de productos y servicios aportará a los ingresos de la industria más de 110.000 millones euros/año en Europa durante los próximos cinco años. También dará lugar a un aumento del empleo de un 6 por ciento. Cerca de un tercio del crecimiento de la producción industrial general en Europa se debe ya a la absorción de las tecnologías digitales[3].

Como ha manifestado el Comité Económico y Social europeo (CESE), la digitalización de la industria es un aspecto fundamental de una transformación más amplia de la economía europea que incluye la robotización, las ciencias de los materiales y los nuevos procesos de producción[4]. Y esta transformación pone a las empresas y a las organizaciones ante el reto de no perder el tren de la nueva revolución digital y frente a la encrucijada de adaptarse de forma rápida a todos los cambios que se están produciendo a nivel global. En otras palabras, la

1 Es importante consultar documentos sobre la estrategia europea Industria 4.0 como, por ejemplo, el Dictamen del Comité Económico y Social Europeo sobre el tema «Industria 4.0 y transformación digital: camino a seguir»: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52016AE1017&from=ES, o el informe de la Eurocámara al respecto: http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/568337/EPRS_BRI(2015)568337_EN.pdf, o las recientes comunicaciones de la Comisión Europea sobre la digitalización de la industria: https://ec.europa.eu/digital-single-market/en/news/communication-digitising-european-industry-reaping-full-benefits-digital-single-market y http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52016DC0180&from=EN

2 Interesante consultar publicaciones del WEF a este respecto: https://www.weforum.org/es/agenda/2017/02/magnitud-e-implicaciones-de-la-cuarta-revolucion-industrial y https://www.weforum.org/es/agenda/archive/fourth-industrial-revolution/. También son importantes las políticas europeas relacionadas con este tema: https://ec.europa.eu/digital-single-market/en/fourth-industrial-revolution y http://europa.eu/rapid/press-release_IP-16-1407_es.htm y http://europa.eu/rapid/press-release_MEMO-16-1409_en.htm

3 Remítase a la pág.4 de la COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES "Digitalización de la industria europea. Aprovechar todas las ventajas de un mercado único digital". COM (2016) 180 final: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52016DC0180&from=EN

4 Ver pág.3 del siguiente Dictamen del CESE: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52016AE1017&from=ES

fábrica inteligente y conectada ha llegado para quedarse, todo ello, en desarrollo de las políticas europeas a favor de la digitalización del sector industrial[5].

Este constante proceso de reinvención para mejorar lo presente y adaptarse a las demandas crecientes del mercado y de los consumidores obliga al legislador a estar en un constante proceso de adaptación y regulación normativa, pues como ya se ha mencionado en este estudio, hablar de Industria 4.0, implica necesariamente hablar del mercado de los macrodatos, de Big Data, de Internet de las Cosas, de Robótica e Inteligencia Artificial, de Cloud Computing, de Blockchain, o de Impresión 3D, y un sinfín de cuestiones que no hacen sino incrementar la velocidad del cambio. Tal es la velocidad que estamos adquiriendo gracias a estas herramientas, que las mejoras y los nuevos procesos producen efectos multiplicadores en términos de evolución e innovación, sin perjuicio de otros tantos efectos como los relacionados con el mercado laboral[6].

No cabe duda de que aprovechar las ventajas que nos proporcionan las TICS asociadas a la Industria 4.0 es una palanca de mejora de las empresas cada vez más globales, permitiendo modificar los productos, los procesos y los modelos de negocio casi en tiempo real. Todo ello, en base a la información de valor obtenida mediante mecanismos *"data driven"*[7] y algoritmos específicos que hayan sido generados a tal efecto, provocando también la digitalización de toda la cadena de valor, lo que optimizará sin duda la competitividad y productividad a través de la utilización más eficiente e intensiva de las tecnologías digitales aplicadas a dichos procesos. En definitiva, consistirá en una automatización intensiva de la manufactura valiéndose de la combinación de maquinaria física y tangible con procesos digitales capaces de tomar decisiones descentralizadas y cooperar entre ellos y con humanos mediante el internet de las cosas y la inteligencia artificial, entre otras tecnologías emergentes.

Por consiguiente, al calor de las nuevas políticas, la utilización y el aprovechamiento de las mencionadas ventajas digitales supone una gran oportunidad para ampliar y expandir el mercado. Si bien entran en juego otros factores determinantes en el nuevo ecosistema 4.0, como es su **regulación normativa**. Todo ello, en orden a aportar la necesaria seguridad jurídica tanto a las personas, cuanto a las empresas, sistemas y procesos, tan relevantes en la sociedad actual.

ARMONIZACIÓN DEL MERCADO ÚNICO DIGITAL E INDUSTRIA CONECTADA

En palabras de Günther H. Oettinger, Comisario de Economía y Sociedad Digitales: «*Europa no puede situarse a la vanguardia de la revolución digital con 28 normativas diferentes para los servicios de telecomunicaciones, derechos de autor, seguridad informática y protección de datos. Necesitamos un mercado europeo que permita la aparición de nuevos modelos de negocio y el crecimiento de las empresas emergentes y que ofrezca a la industria la posibilidad de aprovechar la Internet de las cosas. También las personas tienen que invertir, mejorando sus competencias informáticas, tanto en su trabajo como en su tiempo de ocio*»[8].

La **estrategia del mercado único digital** tiene como objetivo abrir las oportunidades digitales para las personas y las empresas, propiciando el principio de la libre circulación de la información. Así como una sólida economía europea de los datos, capaz mejorar la posición de Europa como líder mundial en la economía digital. Por otro lado, evita la fragmentación normativa para permitir economías de escala y un aumento significativo de las transacciones, dentro y fuera de la Unión, entre los operadores de redes y proveedores de servicios eficientes. Al mismo tiempo, garantiza una protección eficaz de los consumidores y usuarios, como fin último para la estimulación del crecimiento y la eliminación de las barreras y obstáculos existentes con vistas a un verdadero Mercado Único Digital con un **marco regulatorio realmente homogéneo.**

Este marco regulatorio único es indispensable para la evolución e innovación constante del sector de las TICS, con independencia del sector de actividad al que este adscrito, en aras a la seguridad jurídica de los servicios digitales y la confianza en los mismos, pudiéndose generar reticencia y desconfianza en caso contrario.

Se prioriza, por tanto, la armonización de las distintas legislaciones nacionales de los Estados miembros de la UE en lo referente a los elementos clave para el pleno avance, desarrollo y uso de las tecnologías de esta revolución industrial. De esta forma, se articula el Mercado Único Digital como un espacio donde acoger todas aquellas instrucciones, independientemente de su forma (directivas, reglamentos, propuestas, etc.) basando sus objetivos sobre

5 Puede conocer más acerca de las iniciativas europeas relativas a la digitalización de la industria a través de este enlace: https://ec.europa.eu/digital-single-market/en/policies/digitising-european-industry

6 Véase, por ejemplo, el Dictamen del Comité Económico y Social Europeo sobre «Los efectos de la digitalización sobre el sector de los servicios y el empleo en el marco de las transformaciones industriales»: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52015AE0765&from=ES

7 Al respecto, puede remitirse a una reciente publicación de la Comisión Europea sobre los elementos que soportan la economía europea de los datos: https://ec.europa.eu/digital-single-market/en/towards-thriving-data-driven-economy

8 Puede consultarse esta intervención a través del comunicado de prensa de la Comisión Europea titulada "Estrategia para el Mercado Único Digital: la Comisión Europea acuerda ámbitos de actuación": http://europa.eu/rapid/press-release_IP-15-4653_es.htm

tres pilares fundamentales. A saber:

1. **Mejorar el acceso de los consumidores y empresas a los bienes y servicios digitales en toda Europa.**

2. **Creación de las condiciones equitativas para que florezcan las redes digitales y los servicios innovadores.**

3. **Maximizar el potencial de crecimiento de la economía digital.**

En consonancia con lo anterior, y partiendo del enfoque global adoptado por la UE en torno al impulso de la digitalización de la industria, destacan asimismo los siguientes pasos relacionados:

- Coordinación de las iniciativas nacionales y regionales sobre la digitalización de la industria manteniendo un diálogo permanente con todos los agentes participantes a escala de la UE.

- Creación de un marco de gobernanza con los Estados miembros y la industria.

- Centralización de la inversión en las asociaciones público-privadas de la UE.

- Inversión de 500 millones de euros en una red paneuropea de «centros de innovación digital» (centros de excelencia en tecnología) donde las empresas podrán obtener asesoramiento y poner a prueba las innovaciones digitales.

- Establecimiento de proyectos piloto a gran escala para reforzar la Internet de las Cosas, la fabricación avanzada y las tecnologías en las ciudades y los hogares inteligentes, los coches conectados o los servicios sanitarios móviles;

- Adopción de una legislación, resistente al paso del tiempo, que respalde la libre circulación de datos y aclare la propiedad de los datos generados por los sensores y los dispositivos inteligentes, así como la revisión de las normas sobre seguridad y responsabilidad de los sistemas autónomos;

- Presentación de una agenda sobre las cualificaciones de la UE que contribuya a dotar a las personas de las competencias necesarias para encontrar empleo en la Era Digital.

Sin perjuicio de lo anterior, y en lo que se refiere a las normas prioritarias para impulsar la innovación digital, la Comisión Europea propone medidas normativas concretas respecto a cinco ámbitos prioritarios: **5G, computación en la nube, Internet de las Cosas, tecnologías de datos y ciberseguridad.** También es necesario acelerar el desarrollo de normas comunes y soluciones y estándares interoperables[9].

Asimismo, tal y como pone de manifiesto la UE, la digitalización del tejido industrial trae consigo nuevos desafíos reglamentarios. Por ejemplo, en lo que concierne a los datos que generan la gran cantidad de nuevos productos inteligentes, a la responsabilidad de los sistemas más autónomos y a la seguridad, con una creciente necesidad de interacción entre las personas y los dispositivos inteligentes.

La digitalización de la industria: Aproximación a la perspectiva regulatoria.

Si atendemos a los trabajos desarrollados por la UE, varias son las disyuntivas normativas que deben atenderse, a saber:

- **Big Data y Analytics[10]:** sin duda la recopilación y evaluación exhaustiva de los macrodatos y, en general, de los datos procedentes de muchas fuentes diferentes, como equipos y sistemas de producción, así como sistemas de gestión empresarial y de clientes, se convertirán en elementos esenciales para apoyar la adecuada toma de decisiones en tiempo real. Este elemento, junto al Internet de las Cosas (IoT) y el Cloud Computing conforman un grupo que, por sí solo, necesita de una serie de medidas para su correcta aplicación en la industria 4.0:

    - Mejorar el acceso de los consumidores y las empresas a los bienes y servicios digitales (comercio electrónico, contenidos digitales, suprimir bloqueos geográficos, derechos de autor, IVA).

    - Crear el entorno en el que puedan prosperar las redes y servicios digitales. (Inversión infraestructuras, normativa en materia de telecomunicaciones y medios, espectro y 5G, plataformas en línea y contenidos ilegales, datos personales).

9 Interesante consultar esta Comunicación acerca de las prioridades de estandarización en el seno del mercado único digital: https://ec.europa.eu/digital-single-market/en/news/communication-ict-standardisation-priorities-digital-single-market

10 Puede acceder a las políticas europeas en relación a la estrategia de impulso del "Big Data" a través del siguiente enlace informativo: https://ec.europa.eu/digital-single-market/en/policies/big-data

- Crear una economía y sociedad digitales en Europa con potencial de crecimiento a largo plazo.

- Desarrollar de forma plena el principio de la libre circulación de los datos, de forma que no se frustren los objetivos de crecimiento económico dispuestos por la UE, si bien aplicando aquellos criterios de "anonimización" y demás garantías asociadas en caso de tratarse de información y datos de carácter personal.

Sin lugar a duda, la explotación inteligente, pormenorizada y segmentada de la información permitirá establecer renovadas estrategias empresariales, comerciales y de negocios dirigidos y personalizados a los fines pretendidos, posibilitando al mismo tiempo un mayor control del usuario sobre su información personal. La cuestión estriba en diferenciar y separar de todo el flujo de información que a través de estos procesos se pueda generar, qué información está considerada como dato de carácter personal y cual no, e integrarlo en un marco normativo consensuado y homogéneo. Principalmente, y desde la perspectiva legal en el denominado "business inteligence", dotar de protección al ámbito de los datos personales es quizás el elemento primordial en la utilización de esta tecnología que tantas ventajas competitivas genera.

En este sentido, la reforma reciente del marco europeo de protección de datos, con el Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en lo sucesivo, «RGPD»), da un primer paso para la armonización, tratamiento y protección uniforme de la información de datos de carácter personal en territorio de la UE. Ahora bien, tal y como se esboza de forma clara en el Considerando 13 del RGPD, *"(...)el buen funcionamiento del mercado interior exige que la libre circulación de los datos personales en la Unión no sea restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales. (...)"*.

Por lo tanto, con este Reglamento, se pretende establecer un marco amplio y uniforme de protección en torno a este derecho fundamental, lo que, como en éste mismo se apunta, no debería suponer un bloqueo de la economía europea. Es fundamental, por tanto, encontrar el equilibrio adecuado entre los intereses comerciales legítimos y los derechos fundamentales que garantizan la protección de los datos personales y la intimidad tal y como, por otra parte, señala de forma específica la Comisión Europea en su Comunicación sobre Digitalización de la Industria Europea[11].

- **IoT (Internet of Things):** el internet de las cosas está permitiendo que los dispositivos de campo interactúen entre sí, permitiendo controladores más centralizados, según sea necesario, o también descentralizar el análisis o la toma de decisiones permitiendo las respuestas en tiempo real automatizadas y eficaces. De esta forma, las estaciones de trabajo saben qué pasos de fabricación deben realizar para qué producto y cómo adaptarse a ello. Pero todos estos nuevos desafíos y oportunidades llevan parejos cautelas y protecciones desde la perspectiva legal que han de ser objeto de regulación. Entre ellos, además de los

11 Resulta accesible desde el siguiente enlace web: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52016DC0180&from=EN

aspectos propios en materia de protección de datos (normativa que pivota muy directamente sobre todas las TICS), mencionar la Directiva sobre armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos radioeléctricos es fundamental para el desarrollo conjunto y armonizado de la tecnología, ciberseguridad por las eventuales responsabilidades que se pudieran generan por el acceso indebido a dichos productos y el control de los mismos, entre otras cuestiones.

- **Cloud Computing:** la nube cada vez alberga más servicios y aplicaciones en los que se apoya la industria. Al mismo tiempo, este sistema o plataforma aumenta su capacidad de respuesta haciendo posible su uso en un mayor número de actividades, incluso aquellas que supervisan y controlan los procesos y recursos. Por este motivo, la iniciativa de digitalización de la industria europea se encuentra íntimamente ligada con la Iniciativa europea de Cloud Computing[12].

- **Robotización:** el modelo actual de la industria no desconoce su uso, pero su automatización va en aumento de manera exponencial a la par que lo hace su capacidad para conectarse a los distintos elementos que conforman la cadena de valor industrial. El regulador deberá atender en este sentido al régimen de responsabilidad civil que se aplique en caso de accidente, ya sea desde el punto de vista de la responsabilidad objetiva o de la gestión de riesgos, tal y como se apunta en la Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre esta cuestión y otras en relación con las normas de Derecho civil y robótica[13].

- **Ciberseguridad:** como resultado de las características del modelo industrial 4.0 es esencial contar con comunicaciones seguras y fiables, así como una sofisticada gestión de identidad y acceso a máquinas y usuarios. Ante la evidente importancia que la ciberseguridad[14] tiene para la protección y mantenimiento de una industria plenamente conectada y dependiente de estos sistemas comunicados, la Comisión trabaja en poder llevar a cabo las medidas oportunas para ligar el concepto de la industria 4.0 con el de seguridad[15]. Para ello, pretende establecer un marco comunitario de certificación de la ciberseguridad para los productos y servicios de las TIC; así como reforzar las capacidades de seguridad cibernética de la UE creando un régimen de responsabilidad asociado a posibles quiebras o violaciones de la seguridad de establecimientos, contenidos o datos detentados por las empresas y organizaciones en ejercicio de sus actividades.

De esta forma, tanto las iniciativas europeas tendentes a la consecución del Mercado Único Digital, como las específicamente dirigidas a la digitalización de la industria, se han de elaborar atendiendo al impacto disruptivo de los anteriores aspectos en el plano normativo.

DIGITALIZACIÓN DE LA CADENA DE VALOR

No podemos finalizar una reseña relacionada con la Industria 4.0, sin mencionar la digitalización de la cadena de valor. Si hay un punto en común a nivel internacional entre todas las predicciones realizadas en torno al futuro de la industria, sin duda, lo encontramos en la necesaria digitalización de la cadena de valor. Ésta supondrá un incremento exponencial del valor añadido respecto del actual modelo industrial, aumentando su potencial de crecimiento y aportando una herramienta decisiva en clave de competitividad. Las principales compañías del sector ya se encuentran inmersas en procesos de este tipo. De la misma manera, los distintos Estados Miembros de la UE han elaborado una serie de programas destinados a fomentar la digitalización de sus tejidos industriales y, así,, regular todos los aspectos que la hacen posible.

La digitalización se impone como un instrumento de cambio necesario que, en el caso de las fábricas inteligentes, se caracteriza por la interconexión de máquinas y de sistemas en el propio emplazamiento de producción (control de producción, gestión de stock, gestión logística, etc.) y también por un flujo de intercambio de información en tiempo real con el exterior. Es decir, con el nivel de oferta y demanda; y/o con los clientes; y/o con los competidores; y/o con otras fábricas inteligentes; donde la intervención de diferentes agentes es obvia, cada uno con su propia tecnología, derechos e intereses comerciales. Sin duda, todo esto, debe coordinarse a nivel normativo a fin de no obstaculizar el pleno despliegue del potencial económico inherente a la Industria 4.0.

12 Puede consultar la misma a través del siguiente enlace: https://ec.europa.eu/digital-single-market/en/news/communication-european-cloud-initiative-building-competitive-data-and-knowledge-economy-europe

13 Se recomienda ampliar la información sobre esta temática a través de los siguientes enlaces informativo: http://www.europarl.europa.eu/RegData/etudes/ATAG/2017/599250/EPRS_ATA(2017)599250_ES.pdf; http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//ES y http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-582.443+01+DOC+PDF+V0//ES

14 Para mayor información puede accederse al siguiente contenido de interés: https://www.certsi.es/blog/ciberseguridad-industria-4-0

15 Puede consultar el siguiente enlace de interés: https://ec.europa.eu/digital-single-market/en/cybersecurity-industry

07.1 | Caso Práctico: Walmart

por **Germán Andrés Sánchez Couso**
Blockchain & Business Transformation Consultant
IBM

La comida es necesaria para la vida. Sin embargo, con bastante frecuencia las personas no tienen presente que el alimento que van a consumir puede ser perjudicial para ellas y el medio ambiente según las condiciones del producto.

Según la OMS los costos asociados a las enfermedades transmitidas por los alimentos varían de 55 a 93 mil millones de dólares americanos sólo en los Estados Unidos. Y una tercera parte de los productos para el consumo humano en el mundo se pierde por razones de seguridad o logística, de un total de 1.300 millones de toneladas al año de alimentos perdidos según la FAO.

En base a lo anterior, la industria alimentaria se enfrenta a grandes desafíos actualmente:

- El sistema actual de alimentos se está agotando porque:
    - En la cadena de valor de los alimentos hay una gran cantidad de procesos manuales basados en papel físico, tareas administrativas onerosas, requisitos regulatorios crecientes y multas cada vez mayores por fraude en los productos.
    - Hay una falta de visibilidad en los certificados de inocuidad de los alimentos y en los informes de auditoría
- Existen múltiples intermediarios para obtener los productos de la granja de un agricultor a la mesa de un consumidor: proveedores, procesadores, empresas de logística, reguladores, etc....
- El intercambio de datos en este ecosistema generalmente se limita a los participantes de la cadena de valor, quienes tienen contacto directo entre ellos y ninguno tiene una visión completa y actualizada de la cadena de suministro.

Por ejemplo, cuando una manzana llega finalmente a la mesa de un comensal, éste no tiene forma alguna de verificar su origen o las afirmaciones de embalaje como "orgánico". Otro caso consiste en que el comprador del producto espera que la comida esté apta para su consumo, porque si deben retirarse los alimentos contaminados de la venta al público, esta orden no se emite en el momento oportuno por el retraso de tiempo que causa detectar el origen del problema en el alimento.

Los problemas anteriores hacen que los consumidores clamen por una mayor transparencia a la industria alimentaria, quieren saber de dónde proviene su comida, cómo se cultiva, cosecha y transporta. Lo anterior es un reto y una tarea difícil de realizar, pero la tecnología Blockchain puede ayudar considerablemente a conseguirla.

QUÉ ES BLOCKCHAIN Y POR QUÉ USARLO EN LA CADENA DE VALOR DE LA ALIMENTACIÓN: CASO WALMART

Varias compañías y organizaciones están explorando cómo usar la tecnología de registro compartido e inmutable conocida como Blockchain para optimizar sus procesos y aprovechar las principales características que provee la tecnología a las cadenas de valor como son la procedencia, el consenso, la inmutabilidad y finalidad.

La cadena de distribución de alimentos funciona actualmente, pero es normal que la información esté incompleta al proceder de distintas fuentes y formatos totalmente independientes y, en este punto es dónde Blockchain puede aportar valor.

Qué es Blockchain

Blockchain es una tecnología que permite proporcionar la trazabilidad de extremo a extremo en una cadena de valor de negocio.

La razón de esta traza completa es que todos los participantes del ecosistema comparten o disponen de una copia de un único libro mayor de registro de información inmodificable por un tercero no autorizado. En este se incluyen todos los cambios de propiedad y estado de cualquier activo, ya sea un alimento o un coche.

Todas las actuaciones autorizadas a los participantes en la cadena de valor están incluidas en un Smart Contract, que es la parte de Blockchain que alberga la lógica de negocio. Para el caso de la cadena de suministro alimentaria, es la parte del sistema que permite que un agricultor solo introduzca la información relevante a su parte de la cadena de proceso como la fecha de recogida del producto en su cultivo.

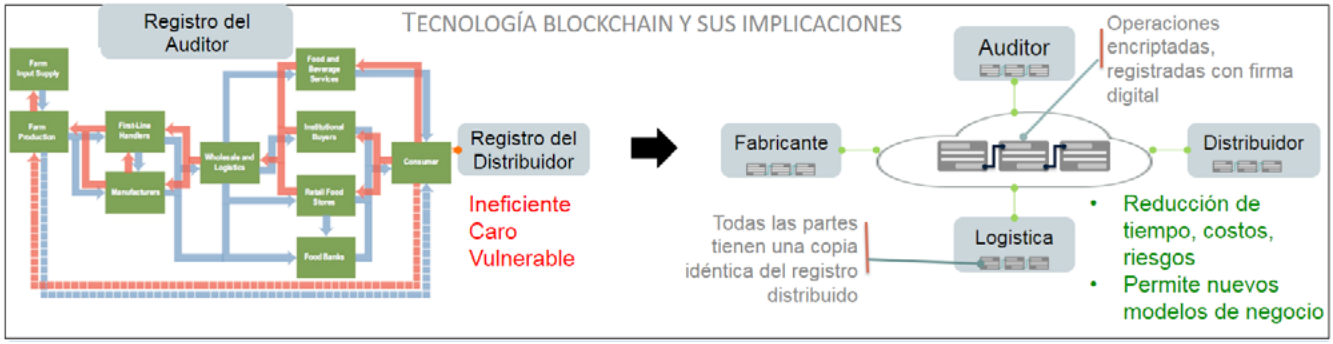
Además, sólo puede actualizarse por consenso entre los participantes de la cadena de valor, es decir, para el caso de la alimentación solo pueden modificar información el agricultor, distribuidor, regulador sanitario y demás participantes autorizados que intervengan. Para certificar lo anterior todas las transacciones que se registran en el libro mayor compartido son encriptadas y gozan de firma digital para dar la mayor seguridad posible.

La información que consultan y modifican los participantes es la misma para todos, porque todos están consultando los mismos datos al usar una copia fidedigna o el mismo libro mayor compartido, formando una red autorizada, confiable y fácilmente escalable. Esto permite a los participantes del ecosistema intercambiar datos y realizar transacciones con confianza, mejorando la transparencia y la eficiencia dentro de la cadena de suministro.

Por qué usarlo en la cadena de valor de la alimentación: Caso Walmart

Las tecnologías existentes no pueden escalar en la medida que crecen tanto la red de alimentos como las disposiciones gubernamentales. Esto implica que la cadena de suministro de alimentos involucra a muchas personas, organizaciones y reguladores que realizan distintas tareas o entran a formar parte de la cadena de valor de los alimentos en distintos momentos.

IBM se asoció con Walmart, el minorista más grande del mundo para hacer que la cadena de suministro de alimentos global sea más transparente y confiable gracias a Blockchain. Para conseguir este objetivo acordaron empezar en octubre de 2016 el desarrollo de un piloto de una nueva solución disruptiva para obtener una trazabilidad de alimentos más transparente, fiable y eficiente.



Fuente: IBM Blockchain

Dentro de esta iniciativa escogieron aplicar la nueva tecnología a la cadena de valor de la carne cerdo que se vende en China, porque este país es el mayor consumidor del mundo, donde a la mitad de la población (Encuesta realizada a +130.000 personas) le preocupa la sanidad alimentaria y el 68% de los incidentes en alimentación son causados por fraudes en la comida.

En una reunión anual de inversionistas de esta compañía, se reveló que el ensayo inicial había producido resultados muy alentadores. Frank Yiannas (Vicepresidente de Seguridad Alimentaria de Walmart) demostró cómo pudo averiguar la información de seguimiento de un producto gracias a Blockchain en solamente 2,2 segundos mientras que usando las tecnologías vigentes esta tarea tarda hasta 7 días.

Esto ayudará a reducir el tiempo de respuesta cuando se descubren los alimentos contaminados, así como permitir realizar recogidas selectivas de alimentos en un tiempo mucho menor al actual

No sólo la trazabilidad facilitada a través de Blockchain puede mejorar la seguridad de los alimentos. También puede ayudar a reducir el fraude en la industria porque permite registrar fehacientemente la procedencia de cada fase de la cadena de valor, es decir, incluir a su responsable y las tareas ejecutadas.

DETALLE DEL CASO DE USO

El objetivo principal de este caso de uso es proveer al cliente de Walmart una transparencia total sobre los productos que está consumiendo.

Esto se conseguiría gracias a que Blockchain permitirá a los clientes y participantes autorizados consultar rápidamente todas las fases de la cadena de valor. Para conseguir el objetivo anterior, la tecnología debería:

- Dar permisos de visibilidad en tiempo real para los distintos participantes en la cadena de valor como distribuidores, auditores, consumidores, reguladores, etc.
- Proveer trasparencia de extremo a extremo de cada fase de la cadena de suministro.
- Permitir la ejecución de transacciones seguras para todas las partes
- Identificar y determinar la procedencia y trazabilidad de la cadena de valor para los distribuidores, auditores, consumidores y demás intervinientes
- Proveer inmutabilidad e inviolabilidad de la información imputada y de las transacciones ejecutadas, gracias a la lógica incluida en el Smart-Contract
- Permitir una ejecución más fácil de las tareas de auditoría y cumplimiento para los auditores, distribuidores, proveedores y reguladores
- Mantener una documentación segura de información clave sobre materias primas (Por ejemplo: Certificados de Origen), maquinaria, procesamiento y logística
- Crear paquetes de productos con etiquetas que lleven un código QR para identificarlos fácilmente
- Facilitar la recuperación de la información de trazabilidad. Por ejemplo, la aplicación debe ser fácil de usar con aplicaciones móviles para algunos usuarios.
- Comprobar el cumplimiento respecto a varios puntos predeterminados como la maquinaria usada, fechas de caducidad o cantidades de productos

REPRESENTACIÓN GRÁFICA DE LA SOLUCIÓN

Fuente: IBM Blockchain

Con la solución planteada por IBM, hecha en la tecnología Blockchain, todos los participantes tendrían acceso a una red privada de negocios y contarían con las siguientes funcionalidades a su disposición:

- Capacidad de procedencia, es decir, identificar qué hace cada persona en cada fase de la cadena de valor

- Asociación del etiquetado del producto (Código QR de cada alimento) con los datos almacenados en el libro mayor compartido

- Agregación y desagregación de los datos de producto

- Visibilidad de extremo a extremo de la cadena de valor, para la consulta de información.

- Analítica básica

Para ello los participantes debían registrar sus tareas dentro del sistema Blockchain por el medio predeterminado para ellos, así el agricultor lo registraba desde su smartphone por medio de una aplicación móvil y el personal de Walmart por medio de sus sistemas adaptados para ello.

Todos estos pasos quedarían registrados en el sistema Blockchain y serían consultables de manera inmediata gracias al código QR de cada producto.

Por otra parte, terceros interesados autorizados como un auditor también pueden utilizar la aplicación para almacenar sus informes de inspección en el libro mayor de registro. Este reporte asociado al producto puede ser recuperado y verificados para dar constancia de su validez.

Los resultados del prototipo para la compañía, como se ha mencionado antes en este mismo artículo han sido muy positivos. Gracias a ellos, han desarrollado un plan estratégico para extender el uso de la tecnología Blockchain a otros productos de su extensa oferta, involucrando a más proveedores y participantes de su ecosistema de negocio.

El objetivo final de este plan es el mismo que el conseguido con el piloto desarrollado: Aumentar la transparencia con el cliente, tener una visibilidad completa de la cadena de valor y reducir los tiempos para solventar posibles situaciones críticas en la sociedad por falta de transparencia y fraude en los productos que distribuye Walmart.

07.2 | Caso Práctico: El Sector Cárnico

por **María Orive Palacín**
Responsable de Comunicación
ASTI

ASTI Mobile Robotics ha desarrollado un AGV (Automatic Guided Vehicle) para la industria cárnica que controla la trazabilidad y el rendimiento de los productos de embuchado, bajo la supervisión del peso, que permite determinar mediante el cálculo de mermas, el momento en el proceso de secado y curado. Gracias a este sistema, se crea una imagen en tiempo real del estado de la producción y del almacén, conociendo los movimientos del producto y la gestión automática entre secaderos hasta determinar el momento preciso en el que está preparado para su consumo.

La evolución y el cambio marcan el día a día en cualquier área del sector industrial. Hoy el reto es el desarrollo de las smart factories que protagonizan herramientas como big data, machine learning, virtualización, robotización colaborativa o digitalización de procesos. Factores comunes en las llamadas 'fábricas inteligentes' que exploran sistemas perspicaces de autocontrol y capacidad de recuperación para gestionar el mayor número posible de dispositivos conectados. La automatización de procesos y el intercambio de información con el exterior son las metas que se buscan alcanzar ahora. Esto es especialmente importante en la industria alimentaria, donde se notan los avances y desarrollos en la materia de forma relevante, dejando a un lado cada vez más trabajos manuales. Además, permiten mayor flexibilidad, eficiencia, repetición precisa del tratamiento, mayor higiene y protección de los productos y de los empleados. Entre esos progresos, destaca desde hace años la automatización de tareas.

Muchas de las operaciones que no aportan valor al producto final y que hace unos años eran realizadas por seres humanos, hoy las ejecutan vehículos de forma autónoma. Y si, además, al mismo tiempo, permiten aportar inteligencia a sus recorridos, la ventaja es óptima. Ese era el reto para ASTI Mobile Robotics.

Desde sus inicios, una de las características que definen a ASTI, ingeniería burgalesa que se dedica a la robótica móvil, es la búsqueda de soluciones a medida para las necesidades de sus clientes. ASTI no es sólo un habilitador de la Industria 4.0, automatizando plantas en 4 continentes de sectores industriales como automóvil, alimentación, cosmética, farma o aeronáutica, sino que es un fabricante de productos conectados que trabaja con una estrategia clara por ofrecer más y mejores servicios de conectividad e integración con sus clientes, mantenimiento predictivo, análisis de performance, entre otros.

En la actualidad, aun teniendo la gama más extensa del mercado de AGVs (Automatic Guided Vehicles), líder en la fabricación en Europa de los Vehículos de Guiado Automático según el estudio de la Universidad de Hannover, como expertos en procesos y conectividad industrial, la ingeniería burgalesa sigue adaptando cada vehículo autónomo a las demandas que se van generando en el mercado, lo que permite incrementar la competitividad, la flexibilidad y el time to market de sus clientes. Y en esa constante evolución, la industria cárnica requería un sistema para controlar la producción de embuchados dentro de la propia automatización, ya existente en el sector para evitar el registro manual todavía hoy palpable en muchas fábricas.

ASTI Mobile Robotics se puso a trabajar sobre ese reto marcado por el mercado hasta la creación de un sistema de automatización del control de la producción de embuchados bajo la supervisión del peso del producto, que permitiese determinar mediante el cálculo de mermas, cuál es el proceso de secado y curado. Esto implica conocer si el producto se encuentra en su punto óptimo para el consumo y así darlo por terminado y listo para la venta o si, por el contrario, necesita mayor tiempo de maduración. En conjunto, gracias a este sistema, se crea una imagen en tiempo real del estado de la producción y del almacén, trazabilidad de los movimientos de producto y gestión automática de los traslados del mismo entre secaderos hasta determinar el momento preciso en el que está preparado para su consumo. En definitiva, machine learning que permite pasar de ser reactivos a proactivos. Es un proceso innovador, ya que este procedimiento se realizaba de forma artesanal y manual hasta la llegada de este vehículo autónomo que permite al mismo tiempo el control sobre la producción.

AGVS INTELIGENTES

Estos AGVs han sido diseñados para introducirse por debajo del rack donde se cuelgan en "perchas" los productos en los que permanecen ahí desde su salida del área de embuchado hasta su empaquetado en la zona de preparaciones de pedidos. Al encajar el rack, el vehículo calcula el peso y con la diferencia, se consigue el control de la producción.

Los racks se mueven de forma autónoma con los vehículos de guiado automático diseñados por ASTI, a través de un sistema integrado de elevación. Los AGVs cuentan con un sistema de pesado a bordo, conociendo en todo momento el peso de cada uno y, por ende, la merma para calcular el estadio preciso en el proceso de curado, mediante un sistema de identificación informático detrás de esos vehículos que permite la supervisión del funcionamiento de la planta de manera remota, con una simple conexión a Internet.

Estos vehículos autónomos cuentan con una carga máxima de 1.500 kilos y de pesado equivalente. La velocidad que pueden desarrollar, garantizando la fiabilidad de los sistemas de seguridad, es de 1,5 m/s. Su sistema de doble motorización le confiere máxima maniobrabilidad incluso sin estar equipado, de momento, con un sistema omnidireccional. Adicionalmente, el sistema proporciona trazabilidad total del producto por medio de tecnología RFiD. Cada rack está equipado con un tag RFiD que le sirve de matrícula identificativa, con referencias, subfamilia, peso a la entrada, peso a la salida, tiempos de estancia en secaderos, centros de curado, estado y fecha de alta. Con toda esa información, se da seguimiento a todo el proceso productivo de cada producto acabado.

Normalmente, este sistema de AGVs está formado por varios vehículos que se encargan de realizar tanto los movimientos entre el área de embuchado y de curado, como los que conectan los centros de curado con los secaderos, y los que se llevan a cabo entre los distintos secaderos. También se encargan de transportar los racks con producto terminado a la zona de preparación de pedidos. A lo largo del tiempo de maduración, el producto desprende líquidos y otras sustancias que ensucian los racks. Por eso, después de finalizar el proceso de producción y tras la retirada de producto final, es necesario que los racks pasen por un proceso de limpieza para dejarlos preparados para ser nuevamente cargados con el siguiente lote de producto. Todos esos movimientos hasta el área de lavado y suministro de racks vacíos al área de embuchado se realizan igualmente por medio de los AGVs de forma automática.

TRAZABILIDAD Y CONTROL DE RENDIMIENTOS

En resumen, este sistema permite generar procesos óptimos y robustos adecuados a la demanda de producción que cada orden de fabricación genera. Existe una trazabilidad total del producto en calidad y cantidad, que permite un control exhaustivo de rendimientos en la fabricación, así como de desperdicios. Por lo tanto, se consigue mayor eficiencia y competitividad. Esto supone la generación de métodos óptimos y robustos adecuados a la demanda de producción que cada orden de fabricación genera.

En cuanto a la tecnología de este sistema, hay una parte hardware, que está compuesta por los vehículos de guiado automático, diseñados a la medida de este proceso y con un sistema de tracción 'quad' que permite moverse de forma precisa en un entorno altamente resbaladizo, como suele ser el de la industria cárnica; y una parte software, en tres capas diferenciadas: la primera es para el control de la trazabilidad y la producción; la segunda es para la optimización del tráfico de la flota de vehículos y la tercera es para la gestión de las comunicaciones con todo el sistema de climatización, puertas automáticas, sistemas informáticos de control, entre otras. Por tanto, el sistema es capaz de comunicar con el resto de máquinas en planta, de gestionar la producción en remoto y de dar trazabilidad del producto a lo largo de todo el proceso de curado.

OTROS AGVS EN LA INDUSTRIA CÁRNICA

Este 'quad' es solo uno de los vehículos de guiado automático de ASTI que, en la actualidad, se utilizan en la industria cárnica. Otros que también se emplean en el sector en estos momentos son los apiladores, tanto SPE 160 (1.600 kg) como SPE 200 (2.000 kg). Estos vehículos autónomos se usan, sobre todo, para el transporte de contenedores tanto llenos de producto como vacíos en los distintos puntos del flujo productivo y, los de mayor capacidad, transportan racks metálicos con producto procedente de las zonas de cocido y curados con destino a un almacén automático donde mantenerlos.

También se emplean en el sector las conocidas retráctiles que se encargan de posicionar los palés en el interior de las cámaras de expediciones. Asimismo, las transpaletas de acero inoxidable transportan tinas también de acero de hasta 2.500 kg de peso entre las estaciones de amasado de producto destinado a cámaras, y de éstas a las posiciones donde se inicia el proceso de embutición de las masas de cocidos. Además, disponen de báscula incorporada para comunicar el peso de producto recogido en las estaciones de amasado.

CONCLUSIONES

En definitiva, evolución visible dentro de las fábricas que las acercan a las smart factories de la Cuarta Revolución Industrial o Industria 4.0. La automatización es fundamental en esta nueva era y, cada vez más, una automatización inteligente que aporte información en todo ese proceso productivo, que permita optimizar los recursos dejando a un lado todo lo que no aporta valor. No es un tema de futuro. Las técnicas de machine learning de inteligencia artificial aplicadas a la automatización en la toma de decisiones estratégicas son demandadas en la actualidad por el mercado con el objetivo de incrementar la competitividad de las empresas. Las soluciones de inteligencia artificial permiten seguir las tendencias, comprender modificaciones y monitorizar cambios. Imprescindibles en las industrias del mañana. Y cada vez más necesarias en las fábricas de hoy.

07.3 | Caso Práctico: Plataforma Wonder

por **Jesús Poveda**
Responsable de Iniciativas Innovadoras
Centro de Innovación para la Logística y Transporte de Mercancías (CITET)

La complejidad del sector logístico global se caracteriza en sus operaciones por diversos aspectos. Estos son: la alta fragmentación de operadores, su capilaridad y la subcontratación de servicios; la intermodalidad, la no exclusividad general en la estructura de la cadena de valor que supone que un transportista u operador recoja, transporte o entregue mercancías de otros cargadores; la diversidad de operadores, en especialización, tamaño y despliegue; y la heterogeneidad de los sistemas de información y de gestión de los operadores.

En consecuencia, se ven afectados los costes de gestión a lo largo de la cadena de valor de un envío, se requieren sucesivas introducciones de datos y se generan incidencias y pérdidas con el impacto que ello supone en los recursos empleados, en la fiabilidad de las entregas, en la reputación comercial de los operadores y, en definitiva, en sus respectivas cuentas de resultados.

Junto a ello, en el sector existe un enfoque generalizado a considerar el envío o expedición como la base de identificación, frente al bulto que es el objeto real de transporte.

QUÉ ES LA PLATAFORMA WONDER Y PARA QUÉ SIRVE

A la vista de esta situación y ante la diversidad y concurrencia de operadores y cargadores en la cadena de valor del transporte y de la logística, surge una mejora de alto interés para el sector, la **Plataforma WONDER.**

WONDER es una solución estandarizada que permite tener la trazabilidad integral en tiempo real de cualquier tipo de envío a nivel bulto, y la comunicación entre todos los eslabones de la cadena de transporte, independientemente de que el envío se esté realizando en redes abiertas o redes cerradas. Esto se consigue gracias a la lectura de un código IUB (identificador único de bulto estándar y normalizado). El IUB permite la utilización concurrente de tecnologías automáticas de identificación y captura de datos y además es legible por el ser humano.

La gestión de la Plataforma WONDER corresponde a **CITET,** el **Centro de Innovación en Logística y Transporte de Mercancías,** que como agencia emisora, es la única entidad que de manera centralizada genera los códigos IUB según las reglas contenidas en la especificación

de AENOR EA_0056, y es el único organismo autorizado para generar los códigos y para grabar los datos electrónicos en el soporte RFID haciendo posible:

- La asignación de un elemento de identificación único e indubitado del bulto desde el momento de la recogida de modo que pueda utilizarse de manera normalizada por todos los agentes involucrados.

- La utilización de medios automáticos de identificación y de captura de datos (AIDC en sus siglas inglesas) que incluyen tanto códigos de barras como códigos en soporte RFID, de modo que:

    - El código pueda ser leído electrónicamente, reduciendo o eliminando errores.

    - Mediante dispositivos RFID puedan realizarse múltiples lecturas concurrentes y en un sólo acto.

    - El código de identificación puede leerse de manera mecánica y complementaria tanto por medio de lectores RFID como de códigos de barras lineales y bidimensionales, además de la propia identificación alfanumérica que incorpora.

    - Permite conocer con una simple lectura la identidad del cargador de origen, garantizando así la confidencialidad de los tráficos entre operadores.

- Que los medios automáticos de identificación y de captura de datos utilizados, así como las reglas que regulan la estructura codificada de los identificadores de objetos, de compactación o de formateado estén regulados por normas internacionales aplicables a esta especificación. En concreto, los siguientes:

    - Las normas ISO/IEC 15417:2007 e ISO/IEC 18004:2015.

    - Las normas aplicables a los sistemas de Identificación por Radio Frecuencia (RFID) tanto en sus protocolos de codificación de datos y de las funciones de su memoria lógica (ISO/IEC 15962:2013), como de las comunicaciones por radio frecuencia UHF en las bandas entre 860 MHz y 960 MHz (ISO/IEC 18000-63:2013).

- Que la identificación del bulto sea la base para dotar de estructura de identificación normalizada para una transmisión electrónica de datos (EDI) que:

    - Permita a cada parte acceder a la identificación sustantiva del bulto.

    - Permita generar ficheros normalizados de identificación de bultos y de trazabilidad de los procesos entre operadores y generadores de carga desde la recogida hasta la entrega.

    - Facilite la gestión de incidencias y la reasignación de envíos a cualquiera de los operadores y generadores de carga.

El esquema de funcionamiento en la utilización del IUB entre los distintos operadores del sistema se recoge en la figura que sigue a continuación:

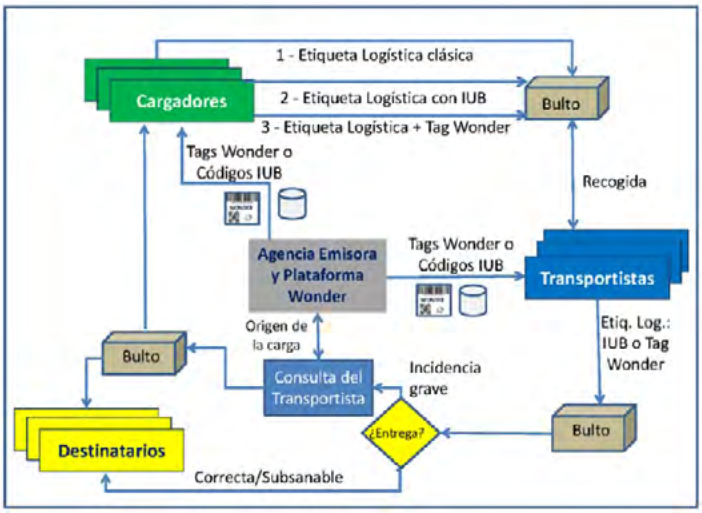


Figura 1 – Esquema de funcionamiento de la utilización del IUB (Elaboración propia CITET)

El intercambio electrónico de datos entre los agentes, incluido el código IUB de cada bulto se organiza a partir de los tres documentos siguientes:

1. Número Global de Localización (GLN)

Es un documento previo, estructural, de declaración de un punto operacional. Es también un código que facilita la identificación única de las entidades que van a intervenir en los mensajes transaccionales. Así, por un lado, reemplaza la necesidad de incluir cada vez la información relevante sobre la entidad y su localización y, por otro, permite que el sistema de información lleve a cabo el enrutamiento de los datos a su destino correcto sin intervención manual alguna.

Un código GLN se refiere a un código único e indubitado de identificación de una entidad legal, de un establecimiento

físico, de una función o de una dirección digital en cualquier parte del mundo.

Cualquier información relevante de una cadena de suministro o de transporte tiene la posibilidad de ser codificada mediante un GLN para su identificación en los mensajes electrónicos de identificación de las partes concurrentes con el fin de facilitar un procesado fiable y automático y de simplificar el procesado de datos.

Figura 2 – Esquema de funcionamiento de la utilización del IUB (Elaboración propia CITET)

El GLN puede representarse mediante códigos de barras que sean susceptibles de incorporarse a los estándares de etiqueta utilizados de manera generalizada, además, puede utilizarse dentro de los mensajes electrónicos en la identificación de las partes concurrentes, de modo que a partir de un código de identificación puede obtenerse el conjunto de elementos que lo caracterizan y que se han de utilizar en el resto de mensajes EDI.

Los GLN se pueden estructurar en al menos cuatro usos principales que no son excluyentes entre sí, sin perjuicio de que se debe disponer de un GLN separado cuando una organización necesite distinguir entre varias localizaciones diferenciadas. Tales usos son los siguientes:

- Entidad legal (EL).
- Localización física (LF).
- Función organizativa (F).
- Localización digital (LD).

La información asociada a cada GLN se mantiene de forma segura por **CITET** en la base de datos centrales de la Plataforma. Así, en el caso de que se produzca cualquier cambio dentro de la organización correspondiente, se actualiza rápidamente su representación en el GLM y se aseguran las comunicaciones o los datos asociados a los envíos.

Un mismo GLN puede utilizarse para identificar varias localizaciones de tipos diferentes en cuanto no se genere un conflicto de identificación: un caso común es el de que una compañía utilice un mismo GLN para su entidad legal y para una localización física, que podría ser la única o principal.

De este modo, el GLN:

- Es una herramienta fundamental previa para el envío de mensajes transaccionales en el Intercambio Electrónico de Datos (EDI) y para la gestión masiva de datos.
- Se puede representar mediante un código de barras para identificar localizaciones físicas o para facilitar información relevante en la cadena de suministro o la facturación.

El código GLN tiene una estructura de caracteres alfanuméricos que incluye los elementos siguientes:

- Un prefijo inicial de carácter alfabético que corresponde a CITET.
- Un conjunto de caracteres numéricos que identifican de manera conjunta y no significativa a la empresa u organización asociada y a la correspondiente entidad, función o localización física, en un código que es asignado por CITET.
- Un dígito numérico de control generado con un algoritmo a partir de los caracteres anteriores.

2. Informe de Transporte

El Informe de Transporte tiene como objetivo identificar un Transporte entre las partes con inclusión de los elementos necesarios y suficientes para que pueda ser llevado a cabo de manera satisfactoria a lo largo de los tramos o fases en que se desarrolle. Esto es, con independencia de que puedan participar diferentes agentes en el mismo hasta la entrega final del envío o destinatario.

Referido a la dinámica de las operaciones, es un primer mensaje transaccional y con objeto de identificar un transporte o envío entre las partes con la inclusión de los elementos que de manera necesaria o contingente puedan aparecer en el mismo:

- Su cabecera con los datos generales del envío, de su emisor y de su receptor.

- Los datos del punto de recogida del envío.
- Los datos del punto intermedio de entrega.
- Los datos del destinatario.
- Los datos del pagador del servicio, en el caso de que pague el destinatario final.
- Los datos de cada uno de los bultos incluidos en el envío, con su código IUB correspondiente.

En caso de que en un envío existan distintos eslabones en la cadena de transporte, los datos de cada emisor del mensaje no tienen por qué coincidir necesariamente con los del cargador o del agente que realiza la primera recogida. Del mismo modo, los datos del punto de entrega intermedio no tienen por qué coincidir con los del destinatario final. Ningún agente que participe en la cadena puede tener acceso a los datos de los demás agentes con los que no tenga relación directa en su fase correspondiente del envío. Sólo pueden tener acceso a los datos del destinatario.

Un Informe de Transporte se envía como resultado de una petición de transporte referida a un envío con un mismo destino final.

3. Informe de Evento

El Informe de Evento tiene como objeto un mensaje en el que cada una de las partes de una determinada fase del transporte pueda transmitir a través de la Plataforma WONDER a su contraparte y al sistema un mensaje con los datos del último estado de su envío, incluyendo el referido a la entrega o la recogida. Así como dar noticia de las posibles incidencias generadas que puedan ser transmitidas a continuación a las partes interesadas (cargador, transportista, operador o destinatario).

Esto es referido a la dinámica de operaciones y con el objeto de que las partes transmitan de manera electrónica la entrega o la recogida de un determinado envío, su estado, valoración general de recepción y posibles incidencias generadas. Puede contar con los elementos siguientes:

- Datos de cabecera, con el tipo de evento generado, los datos de emisor y del receptor del mensaje, la fecha y hora y, en su caso, la identificación referida al envío que se haya podido generar;
- Datos de cada uno de los bultos del envío, que incluyan:

1. Su código IUB.
2. La valoración de la recepción de cada bulto.
3. En su caso, la incidencia generada en el bulto, la imputación inicial de la misma y su fecha, hora y minuto.
4. La información correspondiente al estado y a las incidencias producidas. Una vez que se haya transmitido al sistema se puede comunicar por la Plataforma WONDER a las partes interesadas (cargador, transportista, operador o destinatario) para que éstas puedan adoptar las acciones pertinentes a su resolución.
5. Como una expedición o envío puede contener varios bultos, cada uno de ellos debe ser identificado de manera individual mediante su correspondiente IUB.

Ejemplo de etiqueta en formato pequeño:

Figura 3 – Ejemplo de etiqueta sin RFID (Elaboración propia)

Ejemplo de etiqueta con RFID:

Figura 4 – Ejemplo de etiqueta con RFID (Elaboración propia)

PROCEDIMIENTOS Y USO

La identificación de un bulto integrado en el sistema se realiza de la siguiente manera:

1. CITET, agencia emisora, es la única entidad que de manera centralizada genera los códigos IUB según las reglas contenidas en la especificación de AENOR EA_0056 y en una serie única de numeración para todo el conjunto.

    - CITET es el único organismo autorizado para generar los códigos y para grabar los datos electrónicos en el soporte RFID.

    - Ningún organismo distinto a CITET puede disponer de opciones de generación de nuevos códigos ni tampoco de la modificación de los existentes.

2. CITET registra de manera centralizada todos los códigos de identificador único de bulto (IUB) generados, almacenados, asignados y entregados a los operadores o cargadores adheridos al sistema, con el fin de asegurar:

    - Su trazabilidad.

    - Su estatus.

    - La eliminación de los riesgos de cualquier generación de códigos duplicados.

Para ello, agrupa los códigos en lotes, de modo que quedan definidos y registrados en cuanto a su contenido, el número de elementos y el cargador u operador, junto al destinatario.

En el caso de utilizar como soporte para el IUB un tag o etiqueta RFID se registra asimismo su TID.

3. Para facilitar la lectura por los usuarios del sistema, el código IUB se representa utilizando los medios o soportes complementarios siguientes:

    - En todos los casos mediante un código alfanumérico, apto para la lectura humana.

    - En el caso de uso de etiquetas RFID, mediante el código electrónico de producto (CEP): ISO/IEC 18000-63:2013 (RFID) e ISO 15962:2013

08 | La empresa como Sistema Complejo Adaptativo

por **Rafael Rodríguez de Cora**
Director general
Computer Aided Logistics (CALS)

En el Capítulo de Conclusiones de la Guía anterior publicada por el CEL "Seguridad de la Información en la Cadena de Suministro y las Infraestructuras Críticas" (CEL, 2013) ya apuntábamos a que la seguridad debía plantearse como un ***Ecosistema Integrado*** *y que las organizaciones se deberían analizar y desarrollar como* ***entes vivos****, con distintos tipos de componentes y con características distintas pero manejadas de una manera sistémica (Wikipedia-Living Systems).*

Por lo tanto, se intenta en este capítulo ampliar estos conceptos y poner más foco en una perspectiva global y holística para que las empresas puedan (y deban) gestionarse como un sistema vivo. De cara a los retos planteados en el mundo actual, las empresas, las organizaciones y los individuos deben plantearse este tipo de nuevos enfoques ante la complejidad, si quieren sobrevivir.

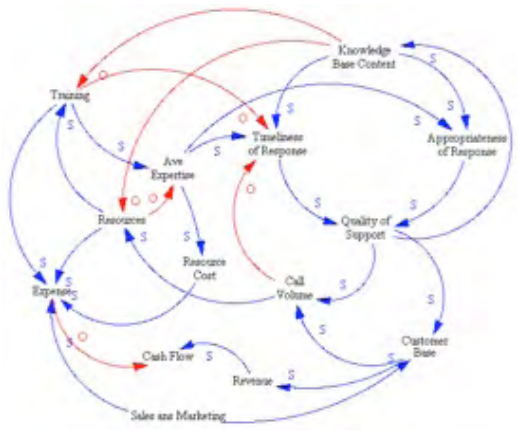
Los **sistemas vivos** incluyen plantas, animales, personas, etc., y también algunos creados por el hombre, tales como comunidades, organizaciones, sociedades, naciones y la aldea global. También se agrupan entre ellos, con una cierta interdependencia formando **Ecosistemas**, que deberían estar en equilibrio.

No vamos a entrar en las definiciones detalladas de los

Sistemas ni de la Teoría General de Sistemas (Bertalanffy 1950, 1968) puesto que estos conceptos se tratan en otras publicaciones anteriores del autor, pero nos sirven ahora para definir el contexto.

Lo que sí queremos destacar, es que esta Teoría sirve para llevar a cabo la importantísima transformación desde el Pensamiento Lineal al **Pensamiento Sistémico.**

Esto se pone de manifiesto en el ya conocido ejercicio del gobierno norteamericano sobre qué pasaría si se materializa un ciberataque a las infraestructuras críticas de



Ecosistemas, Sistemas y Modelos

las energías y un país se queda sin energía eléctrica (caso que dio lugar en su día a una película: **American Blackout**).

Ciberataque. 10 días sin energía eléctrica. Impactos progresivos:

- Cae el suministro eléctrico.
- Cae la telefonía.
- Cae el transporte.
- Faltan suministros básicos.
- Por encima del 6º piso no puede llegar el agua.
- Sobrecarga de los servicios de emergencia.
- Salud pública decae.
- Contaminación por residuos sin recoger.
- Desconfianza y miedo de la población (disturbios, supervivencia, etc.).
- Tiempos peligrosos y difíciles. Contravención de las leyes.
- Preparación para lo peor. Sube el número de víctimas.
- Defensa de la Nación. El ejército tiene que tomar el control.
- Vuelve la energía. Se tarda mucho tiempo en recoger los pedazos y volver a la situación anterior.

El **Pensamiento Sistémico** vuelve a surgir actualmente con fuerza por el impacto de los Ciberataques y el concepto de Seguridad Integral en las Organizaciones. Ya no valen las soluciones simplistas para los problemas complejos. Si no se tiene una concepción holística de los problemas, no se pueden implantar soluciones adecuadas.

"Nos encontramos con Sistemas Complejos todos los días (...)." (Sánchez Sánchez, 2004). Los Sistemas Complejos se encuentran en cualquier ámbito y campo, tales como en la Economía, la Educación, la Física, la Sociología, la Biología, la Política, la Psicología, y otras disciplinas. El sector de la Logística y el Transporte, con sus distintas modalidades es un ejemplo claro de Sistema Complejo. Para la explicación de Sistemas Complejos y de la realidad, siempre tenemos que apoyarnos en modelos.

De hecho, estos sectores van a sufrir y están sufriendo ya grandes cambios para transformarse en un ecosistema logístico integrado y cuyos motores de cambio ya se han comentado en capítulos anteriores, con relación a la sociedad interconectada y a la Industria 4.0.

Cuando se tratan de abordar y solucionar conflictos en los Ecosistemas, se debe contar siempre con un enfoque sistémico. Algunos modelos que se proponen a continuación pueden servir para la transformación de los Sistemas, incluyendo Sistemas Complejos Adaptativos y Organizaciones. Entendemos que con esta perspectiva se debería hablar de Red de Suministro o de Ecosistema Logístico, más que de Cadena de Suministro, como se ha comentado también anteriormente.

Sistemas Complejos e Interconectados

SISTEMAS COMPLEJOS ADAPTATIVOS

Partimos de la definición del libro "The Quark and The Jaguar" de Murray Gell-Mann sobre **Sistemas Complejos Adaptativos:** (Gell-Mann, 1995) *"Un Sistema Complejo Adaptativo es un Sistema que **adquiere información** (del entorno y del propio Sistema), **identifica regularidades** y las **condensa** en un **"esquema" o "modelo"**, y que actúa luego sobre el entorno de acuerdo con dicho modelo".*

Los sistemas complejos adaptativos tienen algún tipo de meta, objetivo o propósito **(Finalidad)**. Normalmente, definido con anterioridad por algún otro proceso del Entorno, de nivel superior. Para sobrevivir, los Sistemas Complejos Adaptativos están en conflicto permanente entre fuerzas internas y externas que ayudan o frenan su desarrollo, sostenibilidad y cumplimiento de objetivos. Este conflicto permanente ha creado sistemas específicos para la supervivencia en organismos vivos, como por ejemplo el sistema inmune. (Rodríguez de Cora, 2014).

El Entorno de un Sistema consiste en todos los objetos y fuerzas internas o externas al Sistema, de manera que un cambio en los atributos o acciones del entorno afectan al sistema y viceversa.

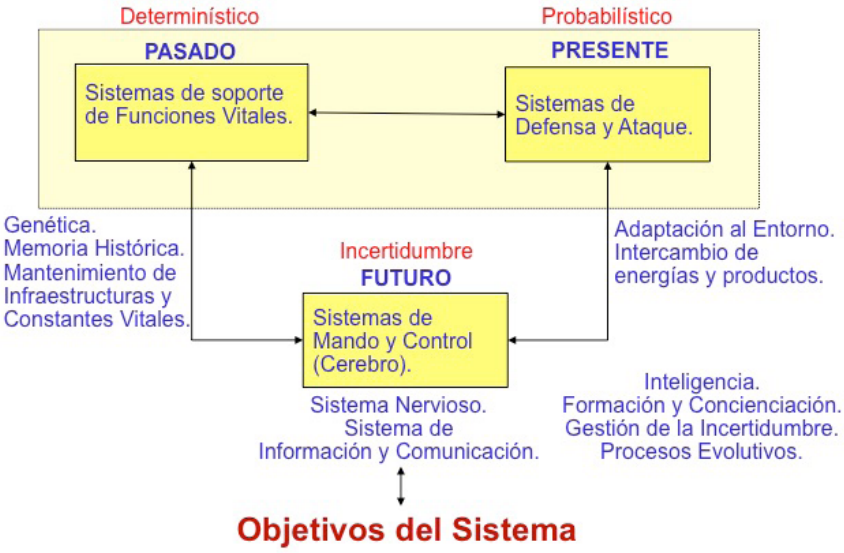
Las organizaciones y corporaciones diseñados por humanos son sistemas vivos con **objetivos y ciclos de vida.** Deben gestionarse y controlarse con estos conceptos en mente. Los diferentes subsistemas y objetivos deben estar bien identificados. Los sistemas vivos no solamente son sólo **Biología** sino también **Cultura**. Esto es, dependen de sí mismos y del entorno para su supervivencia y para la consecución de sus objetivos. La vida es una gestión de riesgos continua.

Esto es, todos los sistemas vivos comienzan por una **genética o genoma**, que proviene del pasado (evolución) y que es de carácter **V** (cómo se han diseñado o creado – normalmente por otros sistemas externos). Los sistemas logísticos y de transporte se han diseñado y concebido quizá para otros objetivos y entorno de los actuales. ¿Convendría una "adaptación genética de los mismos?

Esta "genética" o genoma tiene que **interactuar y desarrollarse en su entorno natural o artificial,** que es de naturaleza **probabilística,** para mantener sus estructuras, para gestionar los recursos para distribuir productos y servicios, etc. Normalmente, se debe contar para ello con interrelación con otros sistemas de nivel superior de apoyo.

Por último, los sistemas deben **manejar el futuro incierto** mediante mecanismos de toma de decisiones frecuentemente sin toda la información pertinente, para llevar a cabo sus objetivos. Para ello, normalmente las organizaciones modernas están sustentadas fundamentalmente por Sistemas de Información y Comunicación y, de hecho, son más unas gestoras de informacion, que de generación de productos o servicios específicos.

Un Modelo Triangular correspondiente a un Sistema Complejo Adaptativo, sería el siguiente:



Modelo Triangular para Sistemas Complejos Adaptativos
(Elaboración propia CALS)

Las organizaciones, como sistemas vivos, son "Sistemas abiertos". Los sistemas abiertos mantienen un intercambio continuo con sus entornos, importando y exportando materia y energía. Esto lo llevan a cabo con múltiples funciones, incluyendo la **membrana** que separa el Sistema del entorno y preserva su identidad. La membrana al ser un subsistema orgánico también está expuesta a riesgos y a controles.

Desde el punto de vista sistémico, las funciones más elementales son las siguientes:

Soporte y Funciones Vitales para la supervivencia. Esto implica el mantenimiento de infraestructuras y de las constantes vitales. Cada organismo vivo depende del intercambio de material y energía con el entorno, para sobrevivir. En una organización esto puede ser recursos

financieros, información y/o personas. El entorno no sólo ofrece recursos y energías sino también peligros; puede tener un impacto negativo en el Sistema mediante agentes nocivos o tóxicos y otras acciones que pueden destruir los atributos de alguno de sus componentes o del Sistema completo.

Sistemas de Defensa y Ataque. En la interacción con el entorno y adaptación a mismo, los mecanismos de defensa y ataque se deben contemplar desde el punto de vista militar, o desde el punto de vista de un organismo vivo que ya ha "inventado" a través de los años, sistemas eficaces de defensa y ataque.

Sistemas de Mando y Control. En esta función se contempla básicamente el sistema de Información y Comunicación para la toma de decisiones.

La Información es transversal. Sin embargo, la información es un término muy elusivo. En términos militares las distintas funciones requieren **distintos niveles de Información:**

- Estratégica.
- Táctica.
- Operativa.

Y a distintos niveles de disponibilidad y velocidades de respuesta:

- Estática / Infraestructuras. Sleep (t0) **Mantenimiento de estructuras.**
- Dinámica / Metabolismo. Normal (t1) **Mantenimiento de equilibrio metabólico.**
- Dialéctica / Combate. War (t2) **Operaciones. Gestión de Crisis, Emergencias.**

En definitiva, esta función debe coordinar el resto de las funciones del sistema para mantener el equilibrio interno, el equilibrio externo y el cumplimiento de los objetivos del sistema.

GESTIÓN DEL CAMBIO

Durante todo su ciclo de vida, las organizaciones también deben gestionar los cambios para sobrevivir. En las organizaciones, la Dirección debe provocar el cambio para adaptarse al entorno cambiante y en cierta medida para superar sus limitaciones genéticas. En casi todos los sistemas naturales (biológicos, sociales, etc.) se tiene el concepto de ciclo, por lo que el cambio debe ser distinto en cada etapa del ciclo. El cambio afecta a la **genética**, a la **interacción con el entorno** y a la **toma de decisiones.**

El Cambio debe planificarse también con metodologías apropiadas que tengan en cuenta **procesos sistémicos de transformación.**

Los cambios están ocurriendo actualmente en las siguientes áreas:

A. Cambios Políticos y Sociales

B. Cambios Económicos

C. Cambios Organizativos

D. Cambios Tecnológicos

E. Cambios en las Actitudes de las personas

Normalmente, los planes empresariales suelen tener metodologías y planes para seguir haciendo lo mismo que antes, pero sin tener en cuenta o adaptarse al cambio o incluso casi siempre con unos objetivos de crecimiento que pueden no ser realistas y que son anti- sistémicos.

Si el Cambio no está gestionado adecuadamente y no tiene en cuenta los otros cambios del Entorno, los factores internos y externos pueden acabar destruyendo al Sistema.

En las organizaciones humanas todo esto está muy vinculado al concepto importantísimo de **"valores"**. El sistema de valores de un individuo, de una organización específica, de un grupo o de una sociedad es determinante cuando:

- Se fijan y definen los Objetivos
- Se definen los Planes y Estrategias
- Se gestionan los Cambios
- Se evalúan e implementan los Riesgos y los Controles

La Sociedad de la Información trae consigo una nueva ética para las organizaciones y un cambio de valores (Parra Luna, 2001). Esto no sólo implica una nueva mentalidad para el servicio a los clientes, sino que también genera una nueva relación con los empleados e incluso con la competencia. Los nuevos valores implican que las organizaciones no pueden estructurarse ni gestionarse aisladamente, sino que deben tener en cuenta al entorno y a los *"stakeholders"*.

Últimamente, se está trabajando en las universidades en proyectos y herramientas para simular comportamientos empresariales desde un punto de vista sistémico que desarrollen las habilidades y conocimientos integrales y sistémicos que los profesionales necesitan. Esto es, conocimiento práctico, global e integrador de la gestión de las distintas funciones empresariales; desarrollo de habilidades y competencias; desarrollo de la capacidad de trabajo en equipo y visión holística, entre otras. (Puebla, 2017). El intercambio de experiencias e información entre Universidad-Empresa es fundamental para el manejo de la Complejidad.

CONCLUSIONES

Los **nuevos paradigmas** y la complejidad existente no pueden gestionarse ni solucionarse con conceptos y metodologías antiguos ni obsoletos. Se puede obtener una gran ayuda de la Teoría General de Sistemas y de otras fuentes para la resolución de problemas complejos.

Se debe establecer una **Política Integral de Seguridad e incorporación de esta función como subsistema**, también basada en conceptos sistémicos, que tenga en cuenta aspectos físicos, lógicos y otros aspectos en relación con amenazas internas y externas, a distintos niveles y grados.

Desarrollo de estos nuevos conceptos y modelos prácticos en base a funciones orgánicas de un sistema vivo, a tener en cuenta, tales como las siguientes:

- Definición de los subsistemas orgánicos vivos de la Organización de acuerdo a las funciones vitales de un Sistema Complejo Adaptativo. Por un lado, las Condiciones Internas y Gestión de Riesgos para la supervivencia, desde el punto de vista de un sistema aislado. Por otro lado, se debe plantear el punto de vista del Sistema, dentro de un Ecosistema en el que habrá que analizar las relaciones entre los distintos sistemas que lo componen. El sistema deberá ser suficientemente flexible para cambiar de objetivos si las circunstancias cambian.

- Definición de los límites superiores e inferiores de cada función o subsistema, para determinar las métricas e indicadores clave y su resiliencia. La Resiliencia es la capacidad del sistema o subsistema para recuperarse de un impacto o de un estrés o daño y ser capaz de volver al estado inicial de funcionamiento normal en el menor tiempo posible. Este tipo de métricas ayudarán también a determinar si el subsistema afectado o el Sistema en sí mismo necesitan Soporte externo de otros sistemas en el entorno. Esto se lleva a cabo a través de la medida y monitorización de los indicadores clave que puedan estar fuera de rangos. Por ejemplo, en el caso de servicios de seguridad y emergencias, tales como el Sistema nacional de salud, cuerpos y fuerzas de seguridad del estado, bomberos, etc. Esto es, preparación y respuestas ante emergencias.

- Definición de la flexibilidad, condiciones y grados de apertura-cierre de la membrana de la organización. Evaluación de Amenazas, Riesgos y Controles en las interfaces. Vínculos y procedimientos de intercambio con sistemas de menor nivel (subsistemas internos) y mayor nivel (supra-sistemas en el entorno o ecosistema).

- Definición y delimitación de los distintos Teatros de Operaciones. Condiciones Externas y Gestión del Entorno (Ecosistema) para cumplir con Objetivos, en los cinco espacios actuales donde se desenvuelven las organizaciones (Tierra, Mar, Aire, Espacio y Ciberespacio). Evaluaciones de Amenazas, Riesgos y Controles Internos y Externos en cada uno de los teatros de operaciones. También podríamos añadir otro espacio de operaciones donde se libran batallas, tal como el Espacio Mental (comportamientos personales y culturales) que, pese a no ser material, es quizá uno de los más importantes al estar ligado a las emociones.

- Definición de los mecanismos de toma de decisiones respecto a las Condiciones Internas y Externas para el Cumplimiento de Objetivos. Planes de Acción, Gestión de la incertidumbre y desconocimiento del entorno. Evaluaciones de Amenazas, Riesgos y Controles Internos y Externos en el futuro. Funciones de prevención (Sensores en el ecosistema, Inteligencia, Medida de variables), Detecciones, Inspecciones y Respuestas.

- Asociaciones e interacciones con otros organismos. Vínculos externos con el Ecosistema. Dependencias de otras organizaciones o de infraestructuras externas, cuando se rompe la resiliencia de la organización aislada. Compartimiento de recursos con competidores. Entornos colaborativos.

- Entender que estamos en un Ecosistema global y con las nuevas tecnologías se puede tener (o sufrir) un impacto en cualquier sitio y momento. Las organizaciones deben pensar ahora globalmente y actuar local y globalmente también. En este sentido, el World Economic Forum (WEF 2016), define periódicamente los riesgos globales para el mundo, lo que puede servir como base para analizar los impactos a nuestras propias organizaciones.

REFERENCIAS

- CEL 2013, Guía de Seguridad de la Información en la Cadena de Suministro y en las Infraestructuras Críticas. *Centro Español de Logística*

- BERTALANFFY, L. V., 1950. An Outline of General System Theory. *British Journal for the Philosophy of Science* 1, p. 114-129.

- BERTALANFFY, L. V., 1968. General System Theory. *New York: George Braziller.*

- GELL-MANN, M., 1995. The Quark and the Jaguar. *London: Abacus.*

- PARRA LUNA, F., 2001. An Axiological Systems Theory: Some Basic Hypotheses. *Madrid: John Wiley & Sons.*

- PUEBLA, I., 2017. Gamification as a Systemic Tool. II Congreso América-Europa, Europa-América, Los Valores del Quijote. *Villanueva de los Infantes, España, 28 de Junio – 2 de Julio 2017.*

- RODRIGUEZ DE CORA, R., 2014. Integral Security of Organisations as Living Systems: A Systemic Approach to GRC. *Reg. General de la Propiedad Intelectual 15 de noviembre de 2016. Nº de Asiento Registral 16/2017/2675.* Registrado Madrid 2016.

- SANCHEZ SANCHEZ, A., 2004. Complex Systems: The science of the XXI Century. *Madrid: IMDEA Matemáticas, Universidad Carlos III.*

- WEF-(WORLD ECONOMIC FORUM), 2016. Global Risks 2016. 11th Edition. *Davos, Switzerland.* Disponible en: https://www.weforum.org/

- WIKIPEDIA - LIVING SYSTEMS: https://en.wikipedia.org/wiki/List_of_systems_of_the_human_body

09 | En busca de nuevas formas de relación entre organizaciones y profesionales para mejorar la eficiencia operativa

por **Ramón García García, CFPIM CLTD CSCP ESLog**
Director de Innovación y Proyectos
Centro Español del Logística

La industria y logística 4.0 operando de manera conjunta dentro de las cadenas de suministro globalizadas, facilitan la conexión entre los mercados de oferta y demanda (entre sí) y con las propias plantas de producción. Generan nuevos escenarios con grandes posibilidades de optimización, habilitan nuevas oportunidades de negocio, e incluyen nuevos actores a la Cadena de Suministro, que pueden convertirse en importantes competidores.

La llegada de esta Nueva Era en la Gestión Empresarial, nos abre la posibilidad de trabajar en un entorno de negocio conectado, basado en el uso intensivo de tecnologías de la información y comunicación. Plantea un nuevo reto a las organizaciones que necesitan adaptarse y, en muchos casos, encontrar la forma de continuar aportando valor en un contexto con un alto grado de transformación digital, respecto a la forma tradicional de hacer negocios. Si este reto no se aborda de la manera adecuada, es fácil quedarse fuera del mercado, como se demuestra en revoluciones tecnológicas anteriores.

Las organizaciones que quieran llevar a cabo esta adaptación, tienen que considerar que en esta Nueva Era Tecnológica se suman nuevos parámetros muy relevantes a los ejes del cambio organizativo tradicionales (personas, procesos y tecnologías). Y aparecen dos nuevos: Seguridad de la Información e Implicaciones Legales respecto a esta nueva manera de enfocar procesos y nuevos negocios.

En torno a los nuevos parámetros que surgen en torno a los ejes tradicionales, cabe destacar: En torno a las Personas, las nuevas profesiones y necesidades de cualificación que surgen y surgirán en este contexto altamente tecnificado. En cuanto a los Procesos, debemos ser muy conscientes del aumento de la exigencia en su propia definición. Es clave la generación de valor e implementación que exige el hecho de que van a estar conectados en tiempo real. Por último, respecto a las Tecnologías, han de permitir la conexión de los procesos dentro de las empresas, con sus proveedores y clientes de una manera eficiente y económica basada en un entorno de máxima fiabilidad, conectividad, visibilidad y rapidez. Todo esto en un contexto

de hiperconectividad entre actores: maquinaria, procesos, trabajadores, proveedores y clientes; integrándose con funciones de Ingeniería o mantenimiento de Instalaciones en un contexto inteligente y flexible. En esta dinámica, los procesos logísticos requieren de una planificación, coordinación y sincronización con todos los actores de la cadena de suministro. En este sentido, el acceso rápido y el tratamiento fiable de los datos, son parte fundamental del éxito de estos procesos.

Con el objetivo de ayudar a las organizaciones en cómo abordar este nuevo reto que plantea la participación en las cadenas de suministro conectadas, la presente Guía CEL realiza un análisis detallado, de la mano de diferentes expertos, y del resultado de varios casos de éxito, que abarcan las principales consideraciones al respecto de los cinco ejes del cambio organizativo en la Era 4.0 anteriormente enunciados: personas, procesos, tecnologías, seguridad de la información e implicaciones legales, de los que a continuación se enuncian las principales conclusiones de sus aportaciones.

La sociedad conectada y la Industria 4.0

Es un hecho que la intersección entre el desarrollo y abaratamiento de la tecnología, y un cambio en el comportamiento de los consumidores (que ahora tienen mayor poder de selección, decisión y prescripción), da como resultado nuevas formas de comprar y consumir.

Los datos son clarificadores a la hora de reflejar el crecimiento sostenido del comercio electrónico y de la existencia de una oferta de consumo digital cada vez más variada e innovadora.

Para dar respuesta a esta demanda emergente surge a su vez un modelo industrial denominado Industria 4.0. Este marco de referencia nace en Alemania como resultado de su política industrial que persigue poner en valor el potencial de las comunicaciones, la tecnología y los datos al servicio de una industria líder y competitiva.

La industria 4.0 posibilita entre otras cosas:

- La creación de ecosistemas industriales que conectan a todos los actores de una actividad concreta y que trabajan de manera transparente y orquestada.
- Surgen modelos de negocio disruptivos basados en la explotación de los datos generados por personas, máquinas y productos.
- Mejora sustancialmente la eficiencia y la calidad de las operaciones industriales.

De la cadena de suministro al ecosistema de suministro

La cadena de suministro no es ajena a la disrupción tecnológica y a los cambios en los modelos de producción, compra y consumo. Podemos afirmar que se encuentra en plena transformación y las empresas del sector tendrán que adaptarse a las nuevas reglas de juego. Esto requiere:

- Proporcionar a los clientes una logística personalizada, flexible y barata.
- Incorporarse al mundo 4.0 y digitalizarse.
- Innovar en el modelo de negocio, en operaciones o en productos, y así definir su propósito y nicho de mercado ante una cadena de suministro cada vez más fragmentada.
- Aprovechar el potencial de los modelos colaborativos para crecer.

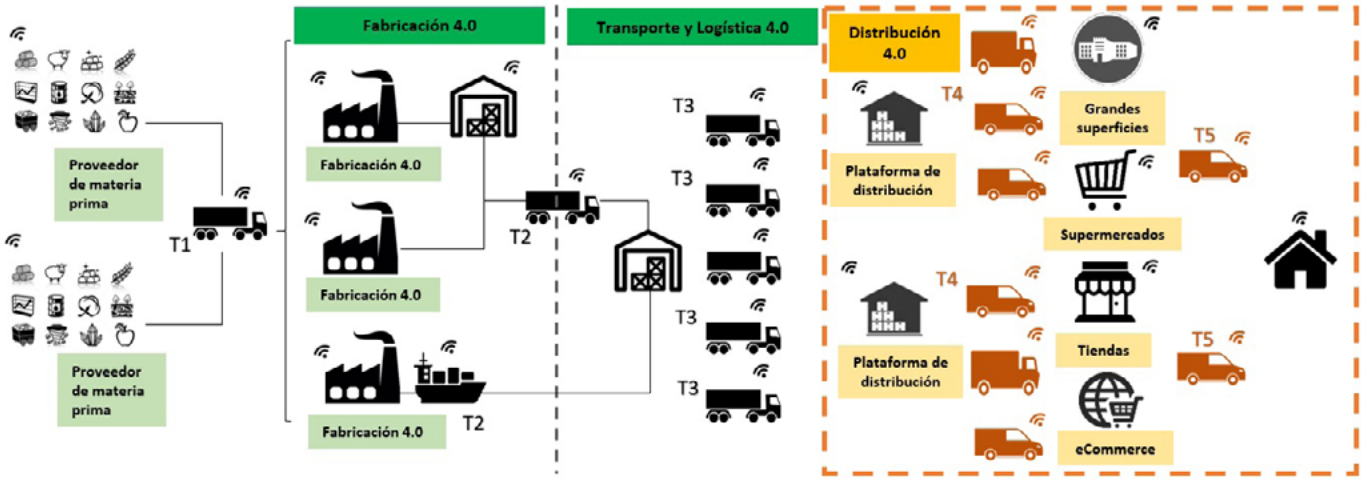
Este panorama no está exento de retos:

- Comprender lo que está pasando, las oportunidades y amenazas.
- Tener un compromiso firme con la innovación y el desarrollo tecnológico.
- Tomar decisiones en cuanto al posicionamiento y modelo de negocio.
- Contratar los profesionales y desarrollar la cultura empresarial adecuada.
- Generar una fuerte sensibilidad hacia la ciberseguridad
- Liderar el cambio.

Las tecnologías y Drivers de la Industria 4.0

Al igual que en otras áreas de los procesos productivos, las mejoras tecnológicas están facilitando nuevas posibilidades en la cadena de suministro, en concreto, las nuevas capacidades de las tecnologías de la información, alimentadas por el aumento masivo de datos provenientes de sistemas ciberfísicos y sensores dentro de la propia cadena de suministro habilitan posibilidades que hasta ahora sólo se podían imaginar en el mejor de los casos.

Esta situación representa un reto que exige a las empresas sumergirse en la transformación digital. Aquellas que adquieran mayores capacidades digitales, no sólo



Fuente: elaboración propia CITET

incrementarán su capacidad productiva y mejorarán su calidad y relación con el cliente. También serán pioneras en nuevos espacios que les permitirán explorar otras posibilidades de negocio, asegurando los actuales, defendiéndose ante posibles intrusiones de empresas, incluso ajenas al negocio, pero con altas capacidades tecnológicas.

Si consideramos el dato como una "nueva materia prima", los procesos de la cadena de suministro son una inmensa fuente de materia prima. Visto de ese modo, la tecnología orientada a la captura, automatización, trazabilidad, gestión y análisis de la información, así como la facilitación de la toma de decisiones de forma rápida y distribuida a lo largo de toda la cadena, apoyada por la inteligencia artificial, se convierte en un "nuevo activo productivo" que diferenciará de forma drástica a los competidores en el mercado.

CiberSeguridad en la Industria 4.0 y en el Sector Estratégico del Transporte

La llamada Sociedad 4.0, donde está incluida la Industria 4.0, ha incorporado nuevos modelos de negocio que sólo podrían llevarse a cabo en la Sociedad Conectada. También ha permitido el nacimiento de nuevos tipos de delincuencia llamada "ciber-delincuencia".

Las organizaciones tienen que adaptar sus procesos y modelo de negocio para que, incorporando todas las medidas de seguridad a su alcance, alcancen un nivel de protección acorde con el apetito de riesgo que establezcan y los niveles de cumplimiento normativo y ético que deseen alcanzar.

La Directiva Europea de Seguridad NIS y la Protección de Infraestructuras Críticas

La normativa inminente, como es la directiva NIS, y el riesgo constatado por los incidentes cibernéticos constantes, es un aviso que puede convertirse en importantes pérdidas económicas y en muchos casos hasta personales.

Las organizaciones de transporte, y las que forman parte de la cadena de suministro, ya no pueden permitirse en un escenario global -como el actual- no gestionar los riesgos tecnológicos derivados de la automatización (cada vez mayor) de su operación.

Las profesiones de la logística del siglo XXI: oportunidades y retos

La aplicación práctica de los desarrollos tecnológicos que sustentan una logística 4.0 tiene un reflejo inmediato en sus trabajadores y las profesiones que desempeñan.

- La automatización progresiva de las tareas logísticas mediante el IoT, la movilidad, el desarrollo de la robótica colaborativa y la utilización de los "wearables".

- Gracias a la conectividad se podrán obtener grandes cantidades de datos que alimenten sistemas de Inteligencia Artificial. Estos se encargan de realizar la planificación de la demanda, el reparto de cargas de trabajo, la asignación de tareas y son capaces de tomar decisiones de forma autónoma.

- Las plataformas tecnológicas colaborativas que permiten conectar de manera directa oferta y demanda (P2P) de servicios logísticos a todos los niveles: almacenamiento, transporte y reparto. Con ello, surgen nuevos profesionales autónomos que pueden prestar dichos servicios directamente si necesidad de ser contratado por empresas especialistas en logística.

Esto conlleva oportunidades para los trabajadores desde el punto de vista de una reducción de los riesgos laborales, abre nuevas oportunidades de desarrollo profesional hacia puestos de mayor valor y complejidad para gestionar toda esa tecnología logística y se crean nuevos nichos de empleo en la economía colaborativa.

Al mismo tiempo, surgen interrogantes acerca de cuántos y qué puestos de trabajo pueden desaparecer a causa de la automatización; qué riesgos existen por trabajar junto a robots; cómo cerrar la brecha digital y preparar a los trabajadores para la Logística 4.0 y qué calidad de empleo pueden tener los trabajadores autónomos de las plataformas.

Implicaciones legales de la Industria 4.0

Hablar de Industria 4.0, supone necesariamente hablar del mercado de los macrodatos, de Big Data, de Internet de las Cosas, de Robótica e Inteligencia Artificial, Computación en la nube, de Blockchain, o de Impresión 3D, 5G y un sinfín de cuestiones que tienen incidencia directa en la evolución, desarrollo y expansión de la sociedad actual y que se encuentran a la orden del día.

No obstante, en este nuevo ecosistema 4.0, entran en juego otros factores determinantes como es la regulación normativa. Todo esto, en orden a aportar la necesaria seguridad jurídica tanto de las personas como de las empresas. Es necesario analizar y dotar de medios para poner en marcha la estrategia del mercado único digital. Esta aspiración tiene el objetivo de abrir las oportunidades digitales al mercado, fomentar el principio de la libre circulación de la información, y una sólida economía europea de los datos, eliminando las barreras y obstáculos existentes con vistas a propiciar un marco normativo consensuado y homogéneo para todos.

Caso de Éxito Walmart

La introducción de la tecnología Blockchain ha demostrado resultados muy valiosos para la compañía, gracias a sus características de inmutabilidad, finalidad y trazabilidad. Como consecuencia, se ejecutó un plan estratégico para extender el uso de la tecnología Blockchain, involucrando a más proveedores y participantes de su ecosistema de negocio.

Estos objetivos alcanzados permitirán a Walmart que mejore la relación con sus clientes, dándoles mayor visibilidad y transparencia y solventar posibles situaciones críticas a la sociedad por falta de transparencia y fraude en sus productos.

Caso de Éxito Industrias Cárnicas

En definitiva, observamos una evolución visible dentro de las fábricas, cada vez más cerca del concepto *smart factories* de la Cuarta Revolución Industrial o Industria 4.0. La automatización es fundamental en esta Nueva Era y, cada vez más, una automatización inteligente que aporte información en todo ese proceso productivo, que permita optimizar los recursos dejando a un lado todo lo que no aporta valor. No es un tema de futuro. En la actualidad, las técnicas de *machine learning* de inteligencia artificial aplicadas a la automatización en la toma de decisiones estratégicas son demandadas por el mercado, con el objetivo de incrementar la competitividad de las empresas. Las soluciones de inteligencia artificial permiten seguir las tendencias, comprender modificaciones y monitorizar cambios. Imprescindibles en las industrias del mañana. Y cada vez más necesarias en las fábricas de hoy.

Plataforma WONDER

Desde el punto de vista del sector logístico, la interconectividad y el flujo de información debe ser bidireccional en toda la cadena de valor. Desde el origen de esta cadena, que es el sector de la producción, hasta el final, con la entrega del producto al cliente.

Una industria conectada 4.0 debe tener información 100 % fiable de todos los eslabones de la cadena de suministro, y lo más cercana a tiempo real posible. Por ello, la distribución es una fuente de información básica y de alto valor para el sector productivo.

La Plataforma WONDER propone implantar un estándar en la codificación y la comunicación en el sector logístico que redunde en una mejora en la interconectividad y la planificación de la distribución. Por ejemplo, reduciendo el número de incidencias que afectan a los envíos o la llamada "logística inversa" (devolución de envíos por errores en el proceso de entrega), gracias a la comunicación entre los agentes de la cadena y la posibilidad de tener información en tiempo real sobre la trazabilidad de los mismos.

La Empresa como Sistema Complejo Adaptativo

Los nuevos paradigmas y la complejidad existente no se pueden gestionar ni solucionarse con conceptos y metodologías antiguos ni obsoletos. El Enfoque Sistémico

para la resolución de problemas complejos sería de gran ayuda para abordar esta nueva realidad.

Se debe establecer una Política Integral de Seguridad e incorporación de esta función como subsistema, también basada en conceptos sistémicos, que tenga en cuenta aspectos físicos, lógicos y otros aspectos en relación con amenazas internas y externas, a distintos niveles y grados.

Se sugiere enfocar la organización como un Sistema Complejo Adaptativo, que es un Sistema que adquiere información del entorno y del propio Sistema, identifica irregularidades y las condensa en un "esquema" o "modelo", que actúa luego sobre el entorno de acuerdo con dicho modelo".

El desarrollo de estos nuevos conceptos y modelos prácticos debe hacerse en base a funciones orgánicas de un "Sistema vivo". De igual modo, la definición de los subsistemas orgánicos vivos de la organización debe hacerse de acuerdo con las funciones vitales de un Sistema Complejo Adaptativo.

Deben establecerse los límites superiores e inferiores de cada función o subsistema, para determinar las métricas e indicadores clave y su resiliencia. Son necesarios mecanismos de toma de decisiones respecto a las Condiciones Internas y Externas para el Cumplimiento de Objetivos. Planes de Acción, Gestión de la incertidumbre y desconocimiento del entorno.

La Sociedad Conectada obliga a establecer asociaciones e interacciones con otros organismos del Ecosistema.

Consideraciones finales

En la Cuarta Revolución Industrial como elemento disruptor en la sociedad y la economía, destaca las distintas implicaciones en temas tales como la seguridad, los aspectos legales, el impacto en los recursos humanos, los ecosistemas empresariales y, muy en particular, en los aspectos relacionados con la Cadena de Suministro.

Por lo tanto, para esta Nueva Era, es necesario que las organizaciones adopten un nuevo marco tecnológico, de seguridad de la información, profesional y legal ante la complejidad del entorno.

Esta realidad, se encuentra dentro del nuevo paradigma de la Industria 4.0 que requiere de una alta interdependencia de la denominada Logística 4.0 para lograr sus objetivos de conectividad y eficiencia operativa. Por todo ello, empezamos a hablar de la Logística 4.0 como la aplicación necesaria de los conceptos y tecnologías habilitadoras de la Industria 4.0 a los procesos de la Cadena de Suministro.

La presente Guía planteada por CEL e IBM, expone la tesis de que esta nueva realidad debería denominarse "Cadena de Suministro 4.0" y no de forma separada. En concreto, el estudio considera cada uno de los dos factores (Industria y Logística) claves para este nuevo escenario que debe ser observado en todo su conjunto.

Apéndice | Autores

José Estrada, CLTD CSCP, es director general del Centro Español de Logística desde 2007, además de vicepresidente de CITET, el Centro de Innovación para la Logística y el Transporte por Carretera, y Presidente de la alianza logística del Arco Mediterráneo ELMED (European Logistics Mediterranean). De 2009 a 2015, ocupó el cargo de secretario general de la European Logistics Association.

Estrada cuenta con una experiencia de 30 años, desarrollados en torno a la Logística y las Operaciones para distintos entornos. Ha trabajado para empresas consultoras como Indra y PricewaterhouseCoopers, donde realizó numerosos proyectos en estas áreas para empresas industriales y de servicios. Así como en Lucent Technologies, donde fue responsable de diversas áreas de Planificación y Gestión de Materiales para varias de sus fábricas.

José Estrada es Ingeniero Industrial y está certificado en APICS CPIM, CSCP y CLTD. Ha sido profesor asociado de la Universidad Carlos III, y profesor colaborador en diversos programas en Escuelas de Negocio como EOI, ESIC, Universidad Europea o GBS entre otras.

www.linkedin.com/in/jose-estrada-344525b/

Luis Pérez Ballestero, ha trabajado durante más de 30 años en numerosos proyectos de Rediseño de Procesos, Estrategia, e Implantación de Sistemas en distintas industrias tales como Consumer Products, Retail, Travel & Transport, etc. Sus principales áreas de experiencia son Procesos de Operaciones y Logística, Implantación de sistemas ERP (principalmente SAP), CRM y BI y Program & Project Management.

Pérez Ballestero tiene dilatada experiencia (>20 años) en la industria de Productos de Consumo y ha trabajado como Consultor, Team Leader, SME, Project Manager y Project Partner en diferentes proyectos en segmentos como Personal Care, Bebidas (Cerveceras, Refrescos, Vinos), Home Care, Tabaco, Food, etc. Dentro de IBM, y durante más de 7 años Luis ha sido lider de la industria de Consumer Products en IBM GBS en la Region South-West de Europa. Actualmente, es responsable de la industria de Consumer Products en España, Portugal, Grecia e Israel trabajando como Account Partner para diferentes clientes.

Antes de IBM, trabajó para PriceWaterhouseCoopers y Control Data Corporation. En la actualidad, es vicepresidente del Centro Español de Logistica (CEL).

www.linkedin.com/in/luis-perez-ballestero-3389a53/

Ramón García, CFPIM CSCP CLTD ESLog, es director de Innovación y Proyectos en el Centro Español de Logística y Director General de CITET (Centro de Innovación para la Logística y el Transporte por Carretera). Cuenta con más de 20 años de experiencia en el área de la Gestión de la Cadena de Suministro desarrollados en empresas de ámbito multinacional (BASF, GlaxoSmithKline y Grupo El Corte Inglés) desempeñando roles técnicos, de gestión de proyectos y consultoría.

Desde 2001, colabora como profesor Asociado en la Universidad Carlos III, la Universidad Camilo José Cela y diversas escuelas de negocio impartiendo materias relacionadas con la Dirección de Operaciones, Logística, Calidad y TIC´s aplicadas al sector Logístico y Transporte.

Es Licenciado en Administración y Dirección de Empresas y Licenciado en Economía por la Universidad Carlos III de Madrid, Master en Gestión de la Calidad por Centro de Estudios Universitarios Ramón Areces (CEURA) y Master Universitario en Logística para los Sistemas de Seguridad y Defensa por la Universidad Rey Juan Carlos. Ha obtenido la Certificación Europea en Logística (ESLog) que otorga ELA (European Logistics Association), es "Certified Supply Chain Professional (CSCP)" y "Certified in Logistics, Transportation and Distribution (CLTD)" por APICS y gracias a su contribución a la profesión logística es "Certified Fellow in Production and Inventory Management (CFPIM)" por APICS.

https://www.linkedin.com/in/ramon-garcia-garcia-cfpim-cscp-cltd-eslog-1781909/

Marina Rodríguez Valentín-Gamazo es Licenciada en Humanidades; máster en Digital Business por el ISDI; en Dirección de Empresas por el Instituto de Empresa y en Dirección de RRHH por la Escuela de Organización Industrial. Cuenta con más de 15 años de experiencia como Consultor de Estrategia especializada en el diagnóstico, diseño y transformación de modelos organizativos, capacidades y cultura empresarial en industrias complejas como la Aeronáutica, las telecomunicaciones, manufacturing y energía.

En la actualidad, su actividad se centra en proyectos de cambio y gestión del Talento en la era de la Industria 4.0

https://www.linkedin.com/in/marina-rodriguez-b952931/

Carlos Junquera Uría, es el responsable del área de Operaciones Digitales en España, Portugal, Grecia e Israel dentro de IBM Global Business Services.

En los últimos 20 años, ha participado y liderado proyectos de digitalización dentro de la cadena de suministro en industrias de los sectores más diversos, desde el petrolífero al farmacéutico, pasando por la industria de alimentación, metalurgia, papelera, transporte ferroviario y por carretera, fabricantes de bienes de equipo, constructores, etc. En los últimos cinco años, se ha especializado en proyectos en las áreas de Internet de las Cosas, Analítica Predictiva y Soluciones Cognitivas.

https://www.linkedin.com/in/carlosjunquerauria/

Rafael Rodríguez de Cora es licenciado en Informática por la Universidad de Chile, título que le fue convalidado posteriormente en España. Ha sido Consultor Independiente llevando a cabo tareas de Consultoría, Auditoría Informática y Formación para diversas empresas y organismos y ha trabajado como consultor en diversas empresas internacionales entre las cuales cabe destacar: Arthur Andersen & Co. y Price Waterhouse & Co. Ha sido socio y promotor de diversas empresas nacionales de Informática entre las cuales cabe destacar: Penta Consultores, S.A., Aroc Consultores, S.A.

Tiene una extensa experiencia en formación, siendo participante como asesor técnico de la OEI, en la III Conferencia Iberoamericana de Ministros de Educación.

En la actualidad, es socio fundador y presidente de las empresas Computer Aided Logistics, S.L. (CALS) y de Computer Aided GRC, S.L. (CAGRC), donde lleva a cabo entre otras, funciones como la definición de políticas generales y técnicas de las empresas, Consultoría y Formación y Soluciones Integrales para los Sistemas de Información.

Es secretario general de la Sociedad Española de Sistemas Generales (SESGE)

https://www.linkedin.com/in/rafael-rodr%C3%ADguez-de-cora-0286293/

Rafael Pedrera es el jefe de la Sección de Operaciones del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), donde desarrolla sus funciones coordinando la respuesta proporcionada por las unidades tecnológicas de las Fuerzas y Cuerpos de Seguridad del Estado y por los CERTs ante un ciberincidente que afectase a las infraestructuras críticas nacionales.

Pedrera combina esta actividad con la participación como profesor en el curso de experto universitario "Ciberseguridad en sistemas de control industrial / SCADA" de la UNED. Adicionalmente, trabaja como experto independiente de la Comisión Europea en la evaluación de proyectos relacionados con la ciberseguridad industrial.

Es ingeniero técnico en informática de sistemas y máster universitario especializado en ciberseguridad. Ha realizado gran cantidad de cursos relacionados con esta temática, destacando el curso "Industrial Control Systems Cybersecurity" del Departamento de Seguridad (DHS) de los Estados Unidos.

https://www.linkedin.com/in/rafael-pedrera-mac%C3%ADas-55024420/

María Orive Palacín, es licenciada en Periodismo por la Universidad Pontificia de Salamanca y en Administración y Dirección de Empresas por la Universidad de Burgos. Orive cuenta con una amplia experiencia en medios de comunicación. Después de dos años en el departamento de Comunicación e Imagen de Cajaviva, además de colaboraciones con otros gabinetes de prensa y medios, se incorpora al departamento de Comunicación y Marketing de ASTI Technologies Group, líder europeo en robótica móvil.

https://www.linkedin.com/in/mariaorivepalacin/

Noemí Brito Izquierdo y **Ramón Mesonero-Romanos**, abogados y responsables del Área de IT Governance, Risk and Compliance y Estrategia, Negocio y Transformación Digital de Comtrust, respectivamente.

Brito, es socia de Legistel. Además, es máster en Derecho de Telecomunicaciones y Sociedad de la Información por la Universidad Carlos III de Madrid. Es vocal de la Junta Directiva de ENATIC (Asociación Nacional de Expertos de la Abogacía Digital): www.enatic.org, donde además es la actual coordinadora de su Comisión de Empresa. Igualmente, es miembro del Comité de Dirección del "Data Privacy Institute" (Asociación Nacional de Fomento de la Seguridad de la Información, ISMS Forum Spain), Miembro del Comité Técnico Operativo del Capítulo español del CSA (Cloud Security Alliance) y CDPP (Certified Data Privacy Professional) por ISMS Forum Spain, miembro del Comité de Dirección de la Sección TIC de AEADE (Asociación Europea de Arbitraje) y árbitro TIC nacional.

Por su parte Mesonero-Romanos, es un abogado especialista en derecho digital. Socio de CECA MAGAN ABOGADOS. Máster en Asesoría Jurídica de Empresas del IE, Master en Derecho de Nuevas Tecnologías de ICADE y MBA Executive en la Escuela Europea de Negocio. Cuenta con una larga trayectoria y expertis en la materia de más de 20 años. Responsable y director legal de los proyectos de transformación digital, desde las diferentes perspectivas (transaccional/ecommerce- activos intangibles y privacidad).

Para más información www.comtrust.es

Noemí Brito Izquierdo:
https://www.linkedin.com/mynetwork/invite-sent/noemibrito/?isSendInvite=true

Ramón Mesonero Romanos:
https://www.linkedin.com/in/ramonmesoneroromanos/

Germán Sánchez es licenciado en Economía por la Universidad de Salamanca, dispone de un máster de Consultoría y Gestión de Empresas de la Universidad Politécnica de Madrid y actualmente realiza sus estudios de máster in Business Administration (MBA) en el Instituto de Empresa.

Es consultor de Negocio especializado en Blockchain (todas las industrias) y Banca (específicamente en Riesgo Crediticio para Banca Comercial y Mayoristas). En lo referente a su experiencia de Blockchain ha formado parte del equipo que desarrolló el primer proyecto de Prueba de Concepto para banca a nivel mundial en Singapur. Actualmente, se dedica al desarrollo y análisis del negocio de esta tecnología y a prestar servicios de consultoría en la región.

Durante los últimos diez años, ha completado y liderado todas las tareas funcionales y de gestión en todo el proyecto de ciclo de vida en los principales clientes y diferentes tipos de proyectos (estrategia, definición de procesos de negocio, despliegues e implantación de tecnologías de la información, etc. ...).

https://www.linkedin.com/in/german-andres-sanchez-couso-68b91b25/

Jesús Poveda Gutiérrez, Ingeniero Industrial y máster en Supply Chain Management, Logística Integral y Operaciones, actual responsable de innovación en el Centro de Innovación para la Logística y el Transporte por Carretera y con una dilatada experiencia como gestor de proyectos de I+D+i tanto nacionales como europeos en sectores como el Transporte, la Energía y el Aeroespacial.

Ha trabajado en departamentos de apoyo logístico en el sector Defensa en multinacionales como General Dynamics y ha sido responsable de la Plataforma Tecnológica Nacional en Logística Integral, Intermodalidad y Movilidad, Logistop.

Destaca también su actividad como responsable de proyectos europeos en el Instituto Nacional de Técnica Aeroespacial dependiente del Ministerio de Defensa.

https://www.linkedin.com/in/jesús-poveda-gutiérrez-0a91a625

José Valiente, es director y responsable de Coordinación y Comunicación del Centro de Ciberseguridad Industrial. Especialista en consultoría Tecnológica y de Seguridad. Cuenta con más de 20 años de experiencia trabajando en grandes consultoras, en las que ha desarrollado su carrera profesional tanto en el ámbito de tecnologías de la información, como en el sector de la automatización industrial.

Ha participado en más de una docena de publicaciones sobre ciberseguridad industrial, así como en múltiples congresos, eventos y cursos especializados en ciberseguridad.

Actualmente dispone de múltiples certificaciones en soluciones de fabricantes de seguridad y TI, así como las certificaciones profesionales CISM de ISACA y Global Industrial Cyber Security Professional (GICSP) de GIAC.

https://www.linkedin.com/in/jvaliente/

Apéndice | Empresas

CEL

Desde 1978, el Centro Español de Logística (CEL) es la asociación de referencia nacional e internacional para la gestión de la cadena de suministro en España. Está centrada en aportar valor a sus socios a través del conocimiento y la innovación en la gestión logística. Para ello, actúa como referente del sector gracias a la investigación, compilación, selección y actualización de las más innovadoras técnicas de gestión logística y de las tendencias de negocio emergentes en la economía global. Participa en la divulgación y difusión constante del know how, innovación y buenas prácticas. Aúna a las organizaciones y profesionales de la logística en foros de análisis para intercambiar y detectar las mejores prácticas y técnicas gestoras relacionadas con la cadena de suministro.

En 2018, el Centro Español de Logística cumplirá 40 años trabajando por y para la profesión logística.

www.cel-logistica.org

IBM

Empresa de tecnología, fundada en 1924, que fabrica y comercializa hardware y software para computadoras, ofrece servicios de infraestructura, alojamiento en la nube y consultoría en una amplia gama de áreas relacionadas con la tecnología de la información, desde supercomputación hasta nanotecnología.

Con vocación de investigación, IBM lidera año tras año el ranking de empresas con mayor número de patentes en EEUU, y a lo largo de su historia, empleados suyos han recibido cinco premios Nobel, cuatro Premios Turing, nueve National Medals of Technology y cinco National Medals of Science.

En el ámbito de Internet de las Cosas y tecnología cognitiva lidera los cuadrantes de las principales empresas analistas gracias a sus soluciones con Watson.

www.ibm.com/es

Computer Aided Logistics (CALS)

Empresa creada en 1997 para ofrecer soluciones tecnológicas en el entorno de la logística y el transporte, con la idea básica de presentar al mercado una alternativa claramente diferenciada en aquellos servicios y productos que puedan considerarse estratégicos para las empresas, con un alto nivel de Retorno de la Inversión (ROI).

En CALS estamos comprometidos con la Evolución de la Tecnología, la Seguridad de los Sistemas y el futuro de nuestros Clientes, para que éstos puedan contemplar las Nuevas Tecnologías como el factor estratégico para el desarrollo de su negocio.

CALS también es una compañía especializada en proporcionar herramientas para implantaciones GRC (Governance, Risk & Compliance) y Seguridad de las TIC, siendo Distribuidor, entre otras, de Ideagen, Boldon James, Acuity, ABATIS y BeOne, empresas líderes en soluciones de gestión de riesgos, de seguridad y de protección de datos.

Esta estrategia nos permite el intercambio de tecnologías, formación y oportunidades de negocios entre Asia, América Latina y Europa, que ponemos también a disposición de nuestros clientes.

www.calogistics.com

Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC)

Órgano responsable del impulso, coordinación y supervisión de todas las políticas y actividades relacionadas con la protección de las infraestructuras críticas españolas y con la ciberseguridad en el seno del Ministerio del Interior. El CNPIC depende del Secretario de Estado de Seguridad, máximo responsable del Sistema Nacional de Protección de las Infraestructuras Críticas y de las políticas de ciberseguridad del Ministerio.

La Oficina de Coordinación Cibernética (OCC) es el órgano técnico de coordinación del Ministerio del Interior en materia de ciberseguridad, creado mediante Instrucción del Secretario de Estado de Seguridad 15/2014, de 19 de noviembre, estando sus funciones reguladas por el Real Decreto 770/2017, de 28 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior. Depende funcionalmente de la Secretaría de Estado de Seguridad y orgánicamente del CNPIC.

La OCC ejerce como canal específico de comunicación entre los Centros de Respuesta a Incidentes Cibernéticos (CSIRT) nacionales de referencia y la Secretaría de Estado de Seguridad, desempeñando la coordinación técnica en materia de ciberseguridad entre dicha Secretaría de Estado y sus organismos dependientes. Además, es el punto de contacto nacional de coordinación operativa para el intercambio de información con la Comisión Europea y los Estados miembros, en el marco de lo establecido por la Directiva 2013/40/UE, de 12 de agosto, relativa a los ataques contra los sistemas de información.

www.cnpic.es

ASTI Mobile Robotics, transforming the future together

Ingeniería de robótica móvil, dedicada al estudio, diseño, fabricación, puesta en marcha y mantenimiento de soluciones de intralogística automatizada. ASTI Mobile Robotics está especializada en soluciones de transporte interno, es decir, del movimiento de materiales y productos dentro de las empresas, mediante vehículos de guiado automatizado, llamados AGVs (Automated Guided Vehicles). La ingeniería cuenta con la gama más extensa del mercado y es experta en procesos y conectividad industrial. ASTI Mobile Robotics forma parte del holding ASTI Technologies Group, leading forward, un conjunto de empresas formado por la ingeniería de robótica móvil, por ASTI Technologies Distribution, por ASTI Consulting Services y la Fundación ASTI, además de participaciones en otras compañías tecnológicas.

El talento internacional de ASTI Technologies Group, mayoritariamente perfiles técnicos, está formado por cerca de 180 personas provenientes de 8 nacionalidades y culturas distintas con un factor común: la motivación para desarrollar con energía y servicio al cliente un gran trabajo en equipo, dentro de un ambiente de respeto y humildad que permita cumplir la misión de incrementar la competitividad de sus clientes.

www.asti.es

CCI

El Centro de Ciberseguridad Industrial (CCI) es una organización independiente, internacional, sin ánimo de lucro, cuya misión es impulsar y contribuir a la mejora de la Ciberseguridad Industrial, en un contexto en el que las organizaciones de sectores como el de fabricación o el energético juegan un papel crítico en la construcción de la Sociedad actual, como puntales del estado del bienestar.CCI afronta ese reto mediante el desarrollo de actividades de investigación y análisis, generación de opinión, elaboración y publicación de estudios y herramientas, e intercambio de información y conocimiento, sobre la influencia, tanto de las tecnologías, incluidos sus procesos y prácticas, como de los individuos, en lo relativo a los riesgos -y su tratamiento- derivados de la integración de los procesos e infraestructuras industriales en el Ciberespacio.

CCI es, hoy, el ecosistema y el punto de encuentro de las entidades -privadas y públicas- y de los profesionales afectados, preocupados u ocupados de la Ciberseguridad Industrial; y es, asimismo, la referencia hispanohablante para el intercambio de experiencias y la dinamización de los sectores involucrados en este ámbito.

www.cci-es.org

CITET

Centro de Innovacion para la Logistica y Transporte de Mercancia por Carretera (CITET).

Asociación Empresarial sin ánimo de lucro fundada en 2007, que se ocupa de organizar actividades de difusión tecnológica y proyectos de innovación para la mejora competitiva y sostenbilidad del sector de la logística y el transporte. Intenta poner en contacto la oferta y la demanda tecnológica para el sector de la logística y el transporte, así como introducir tecnologías de otros sectores a éste. Para ello, organiza talleres, conferencias, jornadas, seminarios y congresos y dinamiza proyectos de I+D+i y busca con sus socios financiación pública o privada a los mismos. Desde 2016, está registrada como Agrupación Empresarial Innovadora (Clúster de Innovación para la Distribución de Mercancías Sostenible) en el Ministerio de Economía, Industria y Competitividad.

La actividad de CITET se enmarca en torno a cuatro grandes bloques:

1. Dinamizacion y gestion de proyectos de I+D+i (nacionales y europeos)

2. Consultoria TIC y Sectorial.

3. Organizacion de jornadas técnicas y de difusion tecnologica en torno a la innovación y sostenibilidad en logística.

4. Gestión de iniciativas sectoriales innovadoras.

www.citet.es

Windmill Consultants

En Windmill Consultants ayudamos a organizaciones, equipos y profesionales a adquirir y desarrollar las capacidades, la cultura y el talento para navegar con éxito en una economía y sociedad global y digital.

www.windmillconsultants.com

Comtrust

COMTRUST es un proyecto legal innovador y disruptivo dirigido a aportar soluciones de alto valor añadido a las empresas que utilicen la tecnología como aliada estratégica en su proceso de consolidación, expansión y crecimiento. Con una visión 360, queremos ofrecer al mercado una batería de soluciones y alternativas que permita al cliente centrarse en su negocio siendo la parte de innovación legal un aliado estratégico en el proceso de estrategia global de la compañía. En definitiva nuestra misión es detectar, entender y comprender las necesidades de nuestros clientes, aprovechando las ventajas competitivas de la ley y ponerlas a su beneficio siempre desde una perspectiva preventiva.

www.comtrust.es

IBM

www.ibm.com/es

CEL Centro Español de Logística

www.cel-logistica.org