UNIVERSIDAD DE LA REPUBLICA
URUGUAY

Una propuesta de adopción de la Industria 4.0

Con énfasis en la confiabilidad

Leonardo Vidal Martínez

Programa de Posgrado en Ingeniería Informática
Facultad de Ingeniería
Universidad de la República

Montevideo – Uruguay
Marzo de 2021

UNIVERSIDAD DE LA REPUBLICA
URUGUAY

Una propuesta de adopción de la Industria 4.0

Con énfasis en la confiabilidad

Leonardo Vidal Martínez

Tesis de Maestría presentada al Programa de Posgrado en Ingeniería Informática, Facultad de Ingeniería de la Universidad de la República, como parte de los requisitos necesarios para la obtención del título de Magíster en Ingeniería Informática.

Director:
Dr. Ing. Eduardo Grampín

Director académico:
Dr. Ing. Gustavo Betarte

Montevideo – Uruguay
Marzo de 2021

Vidal Martínez, Leonardo

Una propuesta de adopción de la Industria 4.0 / Leonardo Vidal Martínez. - Montevideo: Universidad de la República, Facultad de Ingeniería, 2021.

xvi, 355 p.: il.; 29, 7cm.

Director:

Eduardo Grampín

Director académico:

Gustavo Betarte

Tesis de Maestría – Universidad de la República, Programa en Ingeniería Informática, 2021.

Referencias bibliográficas: p. 176 – 355.

1. Industria 4.0, 2. Confiabilidad, 3. Transformación Digital, 4. Internet de las Cosas en la Industria. I. Grampín, Eduardo, . II. Universidad de la República, Programa de Posgrado en Ingeniería Informática. III. Título.

INTEGRANTES DEL TRIBUNAL DE DEFENSA DE TESIS

_____

D.Sc. Prof. Nombre del 1er Examinador Apellido

_____

Ph.D. Prof. Nombre del 2do Examinador Apellido

_____

D.Sc. Prof. Nombre del 3er Examinador Apellido

Montevideo – Uruguay
Marzo de 2021

Dedico esta tesis a mi querida
Agus, fuente continua de orgullo,
inspiración y motivación.

Agradecimientos

Quisiera agradecer a todas las personas que confiaron en mí, que me motivaron y apoyaron en todo momento para lograr el objetivo.

A mis colegas, por brindarme el tiempo para avanzar, alentándome para buscar el objetivo.

A mis amigos, por siempre incentivarme a continuar con este desafío y llegar a la meta.

A mi familia, por permitirme y animarme a "robarles" muchas de nuestras horas para así progresar y culminar este gran esfuerzo.

A Eduardo Grampín, por su aliento, apoyo y paciencia, por permitirme disfrutar y aprender siempre de su liderazgo positivo y por posibilitarme contar con su invaluable orientación académica.

"We must develop a comprehensive and globally shared view of how technology is affecting our lives and reshaping our economic, social, cultural and human environments. There has never been a time of greater promise, or greater peril".

Klaus Schwab

RESUMEN

La Transformación Digital es uno de los grandes impulsores de la Cuarta Revolución Industrial que ya estamos viviendo. Su aplicación a la industria, lo que en general se asocia con los conceptos Industria 4.0 e Internet Industrial, además del impacto en todos los ámbitos del diario vivir, implica enormes oportunidades y desafíos, entre ellos los vinculados a la seguridad, muchas veces motivados porque de la mano del despliegue de la Industria 4.0 viene la incorporación de dispositivos IoT, identificado frecuentemente como Internet de las Cosas en la Industria.

En esta tesis se presenta una propuesta de adopción de la Industria 4.0, con énfasis en la confiabilidad, para un sistema, una organización o un grupo de organizaciones. Para ello se propone como parte de la propuesta un Modelo de Madurez en Confiabilidad que colabora al momento de trazar una hoja de ruta a seguir para que dicha adopción sea exitosa. Dicho Modelo fue elaborado a partir de conocer cómo diferentes organizaciones a lo largo del mundo están desarrollando conocimiento, modelos de referencia y estrategias de adopción de la Industria 4.0.

Palabras claves:
Industria 4.0, Confiabilidad, Transformación Digital, Internet de las Cosas en la Industria.

ABSTRACT

Digital Transformation is one of the great drivers of the Fourth Industrial Revolution that we are already experiencing. Its application to the industry, which is generally associated with the concepts Industry 4.0 and Industrial Internet, in addition to the impact in all areas of the daily life, implies enormous opportunities and challenges, among them those linked to security, often motivated because hand in hand with the deployment of Industry 4.0 comes the incorporation of IoT devices, often identified as the Internet of Things in the Industry.

In this work, we present a proposal for the adoption of Industry 4.0, with an emphasis on trustworthiness, for a system, organization or group of organizations. To this end, a Trustworthiness Maturity Model is proposed as part of the proposal that collaborates when drawing up a roadmap to be followed for such adoption to be successful. This Model was developed from knowing how different organizations around the world are developing Industry 4.0 knowledge, reference models and adoption strategies.

Keywords:
Industry 4.0, Trustworthiness, Digital Transformation, Industrial Internet of Things.

Tabla de contenidos

Capítulo 1

Introducción

Desde hace casi una década la Transformación Digital (frecuentemente identificada como DX), una de las grandes motivadoras de la ya en curso 4ta. Revolución Industrial (4IR, por su sigla en inglés), viene impulsando cambios que impactan e impactarán en los procesos de negocio y servicios tal como los conocemos actualmente, y hasta en la forma de vivir. Ello está ocurriendo a través de las diferentes verticales, imponiendo a nivel global una Economía Digital que requiere una adecuación tanto de las partes interesadas (*stakeholders*) como también del conjuntos de procesos de negocio, tecnológicos y operativos que sustentan la Industria 4.0, para lograr así que dicho modelo económico resulte beneficioso para todos.

Las tecnologías asociadas a la 4IR están redefiniendo las economías y las sociedades; estas tecnologías *smart* poseen un potencial enorme para mejorar la calidad de vida y la salud del planeta.

La Transformación Digital se sustenta en diversos paradigmas tecnológicos que vienen siendo objetivo de estudio e investigación debido al potencial que en ellos se identifica para desarrollar e implementar servicios sustentables, eficientes, adaptables a los clientes y que terminen significando el bienestar de los ciudadanos [48]; este nivel de satisfacción en los ciudadanos es lo que algunos autores ya identifican con una nueva era industrial conocida como Sociedad 5.0.

De acuerdo a último Reporte Global de Riesgos del Foro Económico Mundial (WEF, por su sigla en inglés) [289], los ciberataques se ubican en el séptimo lugar en cuanto a la probabilidad de ocurrencia y en el octavo lugar respecto al impacto en caso de concretarse, considerándose el segundo riesgo más

preocupante para hacer negocios a nivel mundial en los próximos 10 años.

La naturaleza digital de las tecnologías 4IR (donde las personas, las máquinas y los productos estén directamente "conectados" entre sí) las hace intrínsecamente vulnerables a los ciberataques; sin embargo, la consideración de principios tales como *security-by-design* o *privacy-by-design* con el objetivo de integrar la seguridad en un sentido amplio a los nuevos productos y servicios son relegados, salvo excepciones, para intentar llegar antes al mercado.

La adopción del Internet de las Cosas (IoT por su sigla en inglés) por parte de la comunidad supone que en cuestión de muy pocos años, miles de millones de dispositivos se habrán incorporado a la red Internet y a las redes en general, y lo continuarán haciendo, incluso a tasas de crecimiento no vistas anteriormente y ni imaginadas al día de hoy, de manera que a través de sus funcionalidades, propias y combinadas, se brinden los productos y servicios que demandan los usuarios.

Los dispositivos IoT ya se están desarrollando e incorporando a Internet (y a otras redes) bajo algunas premisas fundamentales: muy bajo costo, bajo *Time-To-Market* (TTM), despliegue masivo y criterios de diseño fuertemente enfocados en obtener la funcionalidad deseada en el contexto de aplicación previsto. Lo anterior explica que, salvo en muy pocas excepciones, las posibles consecuencias de dicha adopción masiva en lo que refiere a la seguridad en la consideración más amplia del concepto, no están siendo tenidas en cuenta en tiempo y forma, lo que puede terminar siendo una barrera para la adopción de las tecnologías y servicios involucrados por parte de los ciudadanos. Por lo tanto, sin ánimo de fomentar una visión pesimista pero sí de la necesidad de un análisis crítico, deberíamos considerar a los dispositivos IoT como un potencial factor de amplificación para los cibertataques e incidentes de seguridad en general, con potenciales nunca antes imaginados, debido que significan un aumento notorio de la superficie de ataque disponible.

La incorporación del IoT a la Industria (IIoT, por su sigla en inglés), en cualquiera de sus verticales, como ser Energía, Salud, Fábrica Inteligente, Ciudades Inteligentes, Transporte, Tiendas, extrapola y extiende a dichos ámbitos los riesgos en cuanto a la seguridad asociados a IoT. En este caso también los diseños, desarrollos y despliegues actuales, en general están sustentados en soluciones propietarias que no siempre toman en cuenta estándares y mejores prácticas de seguridad, ni arquitecturas y *frameworks* que brinden una visión completa y consistente sobre cómo adoptar las tecnologías y las soluciones con

un enfoque holístico y adaptable en cuanto a la seguridad, considerando desde los procesos de negocio, el diseño, los proveedores, los contratistas, el desarrollo, la producción y la logística, hasta los productos finales en todo su ciclo de vida, pasando por las diferentes partes involucradas, incluyendo a los clientes y usuarios en general.

En lo que refiere a estándares de seguridad, recomendaciones, mejores prácticas, *frameworks* y arquitecturas de referencia a ser aplicables en este ámbito, diversos esfuerzos se están realizando para el desarrollo y la adopción de los mismos, aunque por el momento sin una visión más amplia, completa y consensuada, lo que sería deseable y hasta necesario.

1.1. Motivación y problema

La 4IR implicará un cambio muy profundo en la sociedad en general y en la industria en particular, con la incorporación masiva de tecnologías y dispositivos, a una escala nunca antes vista. Ello determinará que la cantidad de dispositivos conectados principalmente a la red Internet crezca en poco tiempo de una manera nunca experimentada, lo que puede impactar negativamente en las propiedades básicas que se deben preservar en la "red de redes": abierta, conectada, segura y confiable [150]. Hasta ahora, y salvo en contadas y particulares excepciones, la seguridad no ha sido ni es un tema de preocupación y ocupación primaria por parte de quienes proveen equipos, dispositivos y servicios en Internet. La incorporación de millones de dispositivos IoT a las redes en muy poco tiempo, más el arribo de las tecnologías de IT a los procesos de producción de la industria, generará un ambiente casi ideal para que los incidentes de seguridad proliferen en cantidad, sean cada vez más sofisticados, de mayor impacto y lleguen a sectores y servicios hasta ahora casi inmunes a ellos.

El alto riesgo que significa la incertidumbre que rodea al cambio radical mencionado en el párrafo anterior, con situaciones nunca antes experimentadas y algunas desconocidas, exige cuestionarse si los aspectos vinculados a la seguridad se deberían tratar como hasta ahora. Todo hace indicar que la respuesta es no, pero eso no significa que se haya identificado de manera clara cómo hacerlo.

Este trabajo pretende realizar un abordaje inicial a los aspectos que aparecen como más significativos a la hora de considerar la seguridad en el contexto

de IIoT y en un sentido más amplio de la palabra “seguridad”, considerando además que la proximidad de la 4IR es tal que en ciertos ámbitos el primer párrafo de esta sección habría que redactarlo en tiempo presente.

1.2. Objetivo

1.2.1. Objetivo General

Este trabajo tiene como objetivo general elaborar una propuesta de adopción de la Industria 4.0, con énfasis en la confiabilidad, que contemple las diferentes Partes Interesadas y los distintos niveles de avance en la adopción por parte de las organizaciones, mediante un Modelo de Madurez en Confiabilidad que ayude a construir una Hoja de Ruta a seguir, que sea amplia, flexible y realista.

1.2.2. Objetivos Específicos

Para la consecución del objetivo general, se identificaron los siguientes objetivos específicos:

- Conocer el Estado del Arte de la Industria 4.0, tanto en lo que refiere a conceptos vinculados, modelos de referencia, estrategias de abordaje y lecciones aprendidas.
- Asimilar el impacto de la confiabilidad en el éxito de la adopción de la Industria 4.0.
- Comprender el rol de las Partes Interesadas, su importancia para la necesaria adopción de la Industria 4.0, y sus necesidades al respecto.
- Intentar congeniar lo “mejor de los diferentes mundos explorados” durante el estudio del Estado del Arte respecto a la temática.
- Elaborar una propuesta de adopción de la Industria 4.0 lo suficientemente flexible, con enfoque horizontal y realista, para que su aplicación no sea un obstáculo en sí mismo, considerando además que las diferentes organizaciones pueden encontrarse en distintas fases respecto a la incorporación de la misma.
- Dotar a la propuesta de las características necesarias que habiliten a que sea parte de un proceso de mejora continua.

1.3. Resultados esperados

El trabajo debería proporcionar los siguientes resultados:

- Documentar el Estado del Arte respecto a la Industria 4.0.
- Generar una propuesta de adopción de la Industria 4.0 con énfasis en la confiabilidad.
- Aplicar la propuesta a un caso teórico, y obtener conclusiones.

1.4. Estructura del Documento

En esta sección se explica la estructura del resto del documento. En los próximos capítulos se presentan el Estado del Arte respecto a la Industria 4.0 o IIoT, considerando diferentes organizaciones y programas referentes en la temática. En ese sentido, se detalla a continuación y de manera concisa la organización o programa documentado en cada uno de los capítulos. El Capítulo 2 se centra en la iniciativa alemana denominada *Plattform Industrie 4.0*; el Capítulo 3 aborda el trabajo al respecto a cargo del *Industrial Internet Consortium*, que si bien actualmente es un consorcio internacional, tiene su origen en Estados Unidos; el Capítulo 4 completa el estudio del Estado del Arte haciendo foco en primer lugar, en el trabajo en la temática que se viene llevando adelante en diversas organizaciones muy relevantes para la comunidad, a saber: la agencia europea ENISA, el instituto estadounidense NIST, el IETF, la *Internet Society* y la *IoT Security Foundation*; posteriormente incursiona con las iniciativas al respecto en Singapur, Japón y China, para culminar con la referencia a otras iniciativas para impulsar la Industria 4.0, tanto específicas de algunos países como otras colaborativas entre ellos y con diferentes organizaciones. En el Capítulo 5 se presenta la Propuesta de Adopción de la Industria 4.0 con énfasis en la confiabilidad. Finalmente, el Capítulo 6 presenta las consideraciones finales, las conclusiones y algunas posibles líneas de trabajo futuro. Los Anexos permiten complementar y ahondar en diversos conceptos que son abordados en los distintos capítulos.

Capítulo 2

Plattform Industrie 4.0

En este capítulo en primer lugar se incursiona en el concepto *Industrie 4.0* (I4.0) para luego continuar con las consideraciones más relevantes de la iniciativa alemana denominada *Plattform Industrie* 4.0. Posteriormente se describe el modelo de referencia RAMI 4.0 y se culmina abordando los conceptos de activos y componentes en el contexto de la I4.0.

2.1. *Industrie 4.0*

I4.0 es uno de los proyectos adoptados en el *Action Plan* de la *High-Tech Strategy 2020* (HTS-2020). El Gobierno Alemán acordó el rápido desarrollo social y tecnológico en este ámbito y puso estructuras de cooperación entre todos los actores de la innovación en el país. El grupo de trabajo I4.0 creado por la *Research Union Economy - Science* del Ministerio Federal de Educación e Investigación [22] identificó los requisitos para un comienzo exitoso en la Cuarta Era Industrial. En octubre de 2012, el grupo de trabajo entregó su informe titulado *Implementation of recommendations for the future project Industrie 4.0*.

Las asociaciones BITKOM [21], VDMA [282] y ZVEI [294], que actualmente representan más de 6.000 empresas miembros, actuaron para la continuación y el desarrollo posterior del proyecto I4.0; así, en el año 2013 nacía la *Plattform Industrie 4.0*. En el año 2015, se amplió la Plattform Industrie 4.0, añadiéndose más actores de empresas, asociaciones, sindicatos, ciencia y política.

I4.0 [237] se refiere a la conexión de red inteligente de máquinas y procesos aplicada a la industria con la ayuda de las Tecnologías de la Información y la

Comunicación (TIC). Describe un proceso de innovación y transformación en la producción industrial donde dicha transformación es impulsada por nuevas formas de actividad económica y laboral, en un ecosistema digital y global. Se ha comenzado así el tránsito de un modelo rígido y estricto de cadenas de valor a uno flexible, dinámico, de redes de valor globales, con ambientes de cooperación no existentes hasta el momento.

El propósito fundamental de la I4.0 es facilitar la cooperación y colaboración entre diferentes objetos técnicos, lo que significa que ellos deben poder ser representados virtualmente y conectados. Un objeto técnico es un objeto que tiene valor para la organización, no quedando limitado únicamente a objetos físicos, por lo que también son objetos por ejemplo, las ideas, los archivos y el software.

Esta red inteligente es un habilitador para, entre otras cosas,

- disponer de una producción flexible: contar con una fábrica convertible que permita pensar en productos "customizados" a precios tentadores mediante una producción orientada al consumidor, donde tanto el fabricante como el cliente fortalecen su vínculo y se benefician mutuamente.
- tener una logística que se pueda optimizar, con un impacto directo en costos y eficiencia.
- potenciar el usos de la información y de los datos, tanto del proceso de producción así como también de las condiciones del producto como potenciador de la eficiencia antes mencionada.
- implantar una economía circular eficiente en la gestión de los recursos.

2.2. *Plattform Industrie 4.0*

Los impulsores de la I4.0 han identificado que su implementación implica desafíos en numerosas áreas, como ser las vinculadas a:

- la digitalización e interconexión de red en los procesos de producción
- la elaboración y adaptación de normas y estándares para los diferentes sectores industriales
- la protección de los datos
- el marco legal
- los nuevos desafíos y cambios tanto en la educación como en el trabajo

- la aparición de nuevos modelos de negocio
- la necesaria investigación y el desarrollo asociado a todo lo antes mencionado

Para ello disponen de seis grupos de trabajo [236], a saber:

- Arquitectura de Referencia, normas y estándares
- Tecnología y escenarios de aplicación
- Seguridad en sistemas interconectados
- Marco legal
- Trabajo, educación y entrenamiento
- Modelos de negocio digital para la I4.0

En la Figura 2.1 se puede apreciar la Estructura y Organización de la *Plattform Industrie 4.0*.

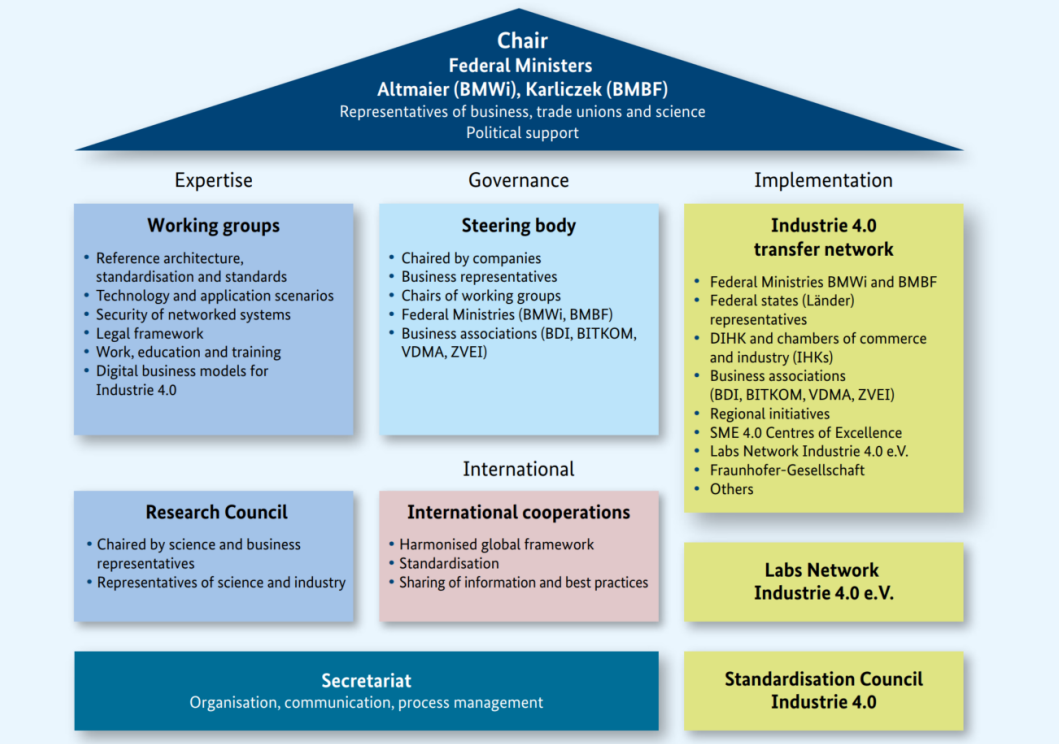


Figura 2.1: Estructura y Organización de la *Plattform Industrie 4.0*. Fuente: [232]

La *Plattform Industrie 4.0* es una red de partes interesadas (gobierno, empresas, asociaciones y comunidad académica), que coordina y promueve en Alemania, la transformación digital de la industria o dicho en otras palabras,

el desarrollo de la I4.0. Mediante acuerdos de cooperación tanto a nivel nacional como internacional busca promover, enriquecer y fortalecer los pilares de Autonomía, Interoperabilidad y Sostenibilidad, con foco en las necesidades de las Pequeñas y Medianas Empresas (SME, por su sigla en inglés) del país.
Actualmente Alemania impulsa la estrategia denominada *The High-Tech Strategy 2025* (HTS-2025) [77], a través de la cual están creando las condiciones para que la investigación y la innovación se desarrollen en un entorno caracterizado por la creatividad, la agilidad y la apertura. La estrategia se enfoca en tres grandes campos de acción: abordar los grandes desafíos, fortalecer las competencias futuras de Alemania y el establecimiento de una innovación abierta y una cultura de "atreverse". La Figura 2.2 refleja, para cada una de las áreas, los asuntos de especial interés definidos por el gobierno alemán.

Figura 2.2: *The High-Tech Strategy 2025*. Fuente: [77]

Las partes interesadas en *Plattform Industrie 4.0*, a través de su *Vision 2030* [226], formulan un enfoque holístico para el diseño de ecosistemas digitales, vitales para el éxito de la I4.0, centrándose en los siguientes campos estratégicos de acción: Autonomía, Interoperabilidad y Sostenibilidad [227], las que se reflejan en la Figura 2.3.

En un ecosistema I4.0 global, la Autonomía requiere de una Infraestructu-

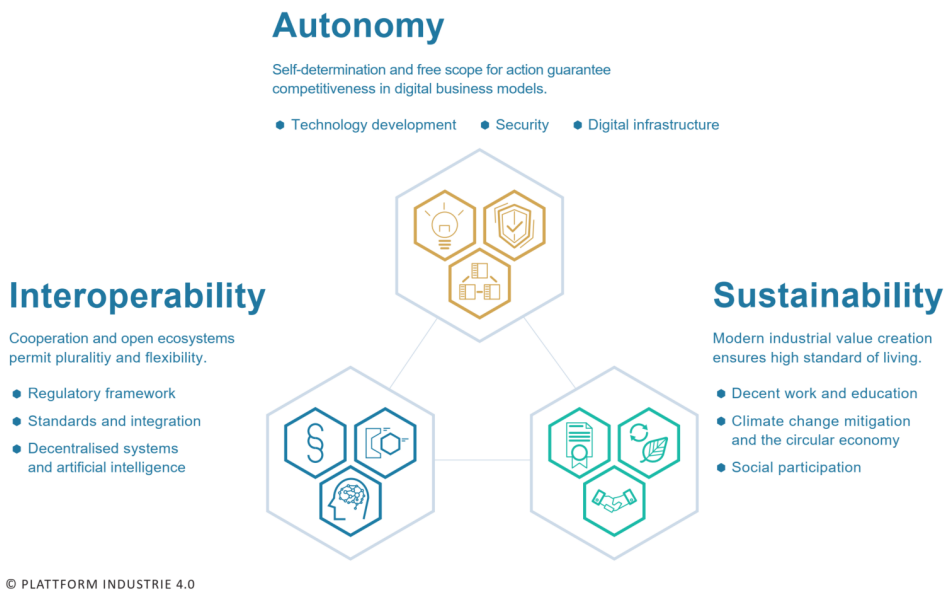


Figura 2.3: Autonomía, Interoperabilidad y Sustentabilidad. Fuente: [226]

ra Digital resiliente, igualmente accesible para todas las partes interesadas y sin restricciones, donde de manera dinámica se configuren las diferentes redes de valor que permitan el intercambio, el uso y el análisis de los datos. Para ello, tanto a nivel industrial como social, se deben establecer acciones tendientes a ofrecer en todo momento y en todo lugar condiciones de seguridad y *safety*. La Autonomía requiere también del sustento mediante actividades de investigación, desarrollo e innovación, neutrales tecnológicamente.

En lo que refiere a la Interoperabilidad, en I4.0 los tres factores claves que la sustentan son: los Estándares, el Marco Regulatorio y, la Descentralización. El primero de ellos resulta indispensable para la interoperabilidad sea posible. El segundo, permite disponer del ambiente donde, de manera acordada, la interoperabilidad ocurra en un contexto de igualdad y sin restricciones. El último factor mencionado es el impulso para la creación de valor tanto en B2B (*Business to Business*) como en B2C (*Business to Customer*).

Finalmente, la Sostenibidad tiene su apoyatura en disponer de Trabajos y Educación decentes, en la Participación Social y, en Mitigar los Cambios Climáticos y en fomentar una Economía Circular. El primero de los aspectos mencionados, no hace más que poner de manifiesto la relevancia de las personas y que ellas deben ser el motivo verdadero y final de toda esta transformación. Ello requiere que de manera proactiva o reactiva temprana se identifiquen los perfiles de formación necesarios, y que las personas accedan a la posibilidad de

formarse en ellos, en el contexto de un nuevo paradigma de aprendizaje permanente. La Participación Social representa la necesidad de que se involucren de manera activa todas las partes interesadas pues la transformación digital impactará en nuestras vidas, día tras día. Por último, la transformación digital implica, entre otras cosas, el involucrarse con los productos durante todo su ciclo de vida, potenciando la economía circular, la eficiencia, y brindando la oportunidad de proteger el medioambiente y mitigar los cambios climáticos.

La sostenibilidad implica poder cumplir con las necesidades del presente sin comprometer la posibilidad que las futuras generaciones puedan también cumplir con las suyas. Como se indica por ejemplo en [19], se identifican tres pilares los que adecuadamente articulados sustentan la sostenibilidad, a saber: el desarrollo económico (informalmente, "beneficios"), la protección al medioambiente (informalmente, "planeta") y el progreso social (informalmente, "personas").

En los últimos años se ha expandido notoriamente el uso del índice *Down Jones Sustainability Index* (DJSI) elaborado hace ya 20 años por *Standards & Poors* en colaboración con RebecoSAM, a la que año tras año se someten empresas de diferentes países y regiones como forman de evaluar su situación respecto a la sostenibilidad, a través del denominado *Corporate Sustainability Assessment* (CSA) [42] que le permite a una organización ser evaluada respecto a la sostenibilidad y disponer de una hoja de ruta para mejorar.

En resumen, y volviendo a los campos estratégicos de acción identificados, la Autonomía implica la libertad de todas las partes interesadas para la toma de decisiones de manera independiente e interactuando en un régimen de competencia justa; la Interoperabilidad entre todas las partes interesadas es necesaria para formar ese complejo ecosistema digital descentralizado y, finalmente, la Sostenibilidad permite apuntalar los valores sociales que son el sustento para el crecimiento de la economía, la preservación del medioambiente y la mejora en la calidad de vida.

2.2.1. Proyecto GAIA-X

A los efectos de potenciar la interoperabilidad, la *Plattform Industrie 4.0* se encuentra trabajando desde el año 2019 en impulsar en Europa una nueva infraestructura de datos federada: el Proyecto GAIA-X [73]. El objetivo del proyecto es interconectar infraestructuras centralizadas y descentralizadas y

que sea visualicen de manera homogénea y de forma amigable para los usuarios, sirviendo así para impulsar los procesos de innovación europeos y así, las economías de los diferentes países. GAIA-X busca así ser un ecosistema digital y abierto donde se acceda a los datos de manera segura y que brinde confianza a sus usuarios.

2.3. El modelo RAMI 4.0

En la siguiente sección se menciona qué motivó el nacimiento del modelo RAMI 4.0, se brinda una breve descripción del mismo así como también cómo se incorpora el concepto de activos y componentes en la I4.0.

2.3.1. Introducción

El Grupo de Trabajo 1 de la *Plattform Industrie 4.0*, denominado *References Architectures, Standards and Norms*, elaboró el Modelo de Referencia de la Arquitectura para Industrie 4.0 (*RAMI 4.0 - Reference Architecture Model Industrie 4.0*) el cual es reconocido tanto como un estándar DIN [49] (DIN SPEC 91345:2016-04, *Reference Architecture Model Industrie 4.0* (RAMI4.0)) así como también como un estándar IEC [7] (IEC PAS 63088:2017, *Smart manufacturing - Reference architecture model industry 4.0* (RAMI 4.0)).

La I4.0 buscó crear descripciones digitales para cada objeto durante toda su vida y considerando también sus cambios; para ello fue diseñado el modelo de referencia RAMI 4.0. El propósito de este modelo es representar los objetos o activos técnicos, y todos sus aspectos relevantes, desde su desarrollo, su producción, pasando por su uso y hasta su disposición final. Los componentes de la I4.0 proveen una descripción digital de los objetos, permitiendo así disponer de su representación virtual.

RAMI 4.0 brinda una descripción estructurada de los elementos principales de un activo utilizando para ello un modelo de tres ejes o dimensiones. La premisa que se siguió para su creación fue dividir un problema grande, con interrelaciones complejas, en varios problemas más pequeños y con mejor probabilidad de abordarlos adecuadamente, combinando los tres ejes en cada punto de la vida del activo, para representar cada aspecto relevante.

El modelo está inspirado en el *Smart Grid Architecture Model* (SGAM) definido por la *European Smart Grid Coordination Group* (SG-CG) [30].

Para representar virtualmente las configuraciones de los activos y las conexiones entre ellos, los activos son caracterizados siguiendo el *principio de descripción recursiva de los activos*, de acuerdo a las siguientes premisas:

- La descripción estructural cumple con RAMI 4.0
- La configuración colectiva de dos o más activos forma un nuevo activo, que se describe con RAMI 4.0
- Los componentes de un activo pueden representar también activos, que se describen con RAMI 4.0
- La descripción de los activos es presentada como información estructurada disponible en la denominada *Administration Shell* [221] del componente I4.0, lo que actúa como representación virtual del activo

Por lo tanto, esto significa que cualquier configuración puede ser representada digitalmente, a cualquier nivel de granularidad, describiendo activos estructurados, y combinaciones de ellos, utilizando el modelo RAMI 4.0.

2.3.2. El Modelo

Como se observa en la Figura 2.4, los tres ejes de la arquitectura de referencia del modelo RAMI 4.0 son:

- El eje de la Arquitectura ("Capas"), con seis capas que representan la información que es relevante para el rol de activo.
- El eje de "Ciclo de vida y flujo de valor", que representa la vida del activo y el proceso de valor agregado. Su desarrollo está basado en el estándar IEC 62890 [82].
- El eje de los "Niveles jerárquicos", que permite asignar modelos funcionales a las diferentes capas. Su desarrollo está basado en los estándares DIN EN 62264-1 [238] y DIN EN 61512-1 [239].

A continuación se describirá cada uno de los ejes referidos. En [229] se puede acceder a una referencia al respecto.

Eje de la Arquitectura ("Capas") - Eje vertical
Mediante este eje se describe la arquitectura en términos de propiedades y estructuras del sistema (de los activos o de la combinación de ellos) con sus funciones y datos específicos de estas, en forma de capas.

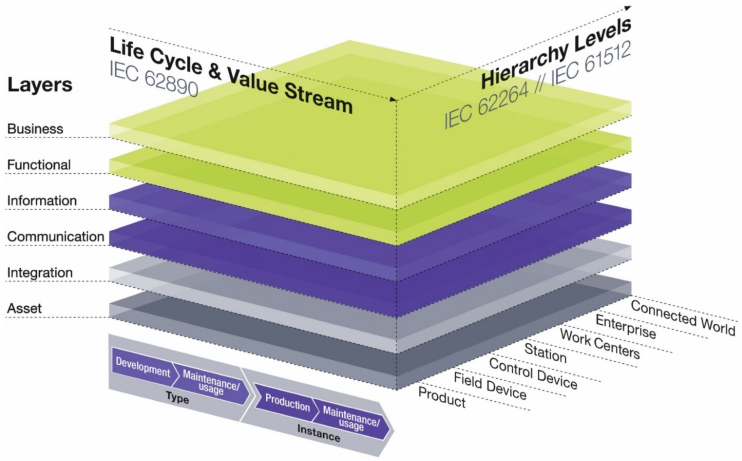


Figura 2.4: *Reference Architecture Model Industrie 4.0 (RAMI 4.0).* Fuente: [49]

Las 6 capas, en sentido descendente, son:

- Negocio
- Funcional
- Información
- Comunicación
- Integración
- Activo

Las capas no siempre deben tener contenido, nunca pueden ser salteadas y la interacción siempre debe ser entre capas adyacentes o incluso en la misma capa.

A continuación se brindará una breve descripción de los aspectos fundamentales de cada capa.

Capa del Negocio

La Capa del Negocio describe el punto de vista comercial, a saber:

- Condiciones generales organizacionales, como ser puesta en marcha de pedidos, condiciones generales de pedido o disposiciones reglamentarias
- Condiciones monetarias, como ser precio, disponibilidad de recursos, descuentos
- Aseguramiento de la integridad de las funciones en la cadena de valor agregado
- Reglas de modelado a seguir por el sistema I4.0

- Mapeo de modelos de negocio y los procesos de negocio resultantes
- Condiciones regulatorias y legales generales
- Orquestado de servicios de la capa Funcional
- Enlace entre los diferentes procesos de negocio
- Recepción en orden de los eventos de un proceso de negocio para avanzar al siguiente estado

Esta capa no involucra directamente a sistemas concretos.

Capa Funcional

Esta capa describe las funciones lógicas del activo en relación a su rol en el sistema I4.0.

Ello incluye:

- Descripción formal y digital de sus funciones
- Plataforma para la integración horizontal de diferentes funciones
- Ambiente de modelado y ejecución para procesos de negocio y servicios
- Ambiente de ejecución para funcionalidades técnicas y aplicaciones

Capa de Información

En esta capa describen los datos que son usados, generados o modificados por la funcionalidad técnica del activo.

Ello contempla:

- Ambiente de ejecución para (pre-)procesamiento de eventos
- Ejecución de reglas
- Descripción formal de modelos y reglas
- Persistencia de los datos representados por los modelos
- Aseguramiento de la integridad de los datos
- Integración consistente de diferentes datos
- Adquisición de datos nuevos
- Proporcionar datos estructurados a través de interfaces de servicio
- Recepción de eventos y su transformación en datos disponibles para la capa Funcional

Capa de Comunicación

Esta capa se encarga de describir los accesos a la información y a las funciones de los activos, por parte de sus pares.

Capa de Integración

Representa la transición del mundo físico al mundo de la información (o digital). Es la capa donde se encuentran las funciones mediante las cuales los activos son utilizados con el propósito para el cual existen.

Esta capa facilita la digitalización del activo para su representación virtual. Cada evento importante en el mundo real genera un evento en el mundo virtual, es decir, en la capa de Integración y posiblemente también en capas superiores.

Su contenido incluye:

- Proveer la representación del activo a partir de información del mismo, hardware, documentos, software, firmware
- Descripción de elementos técnicos
- Control de procesos técnicos
- Generación de eventos en el mundo virtual a partir de eventos en el mundo real
- la *Human-Machine Interface* (HMI)

Capa Activo

Esta capa representa la realidad: el activo que existe en el mundo real. Para cada ítem relevante en el mundo físico, debe existir un ítem relevante en el mundo digital. En el otro sentido -del mundo digital al mundo físico- no siempre es así.

Eje del "Ciclo de Vida y Flujo de Valor" - Eje horizontal izquierdo

Este eje es utilizado para describir el activo en un determinado momento de su vida y en una determinada ubicación, desde su producción y valor agregado asociado al uso, hasta su disposición final. A lo largo de su vida útil, cada activo tiene un estado particular, en un momento particular y en una ubicación específica. La observación de un activo se hace partiendo de la distinción, aplicable a todos, entre Tipo e Instancia; en ambos casos está presente el Uso y el Mantenimiento.

Este eje aplica tanto para las instalaciones, para las maquinarias así como también para los productos. El modelo realiza una distinción entre Tipos e Instancias. Un Tipo nace de una idea. Un Tipo se transforma en una Instancia cuando se ha completado el diseño, las pruebas, las validaciones, y el prototipado es realizado y validado; luego de ello el producto se comienza a fabricar.

A partir de ese momento, cada Instancia se fabrica a partir de las bases que fija el Tipo que lo define. Por lo tanto, cada producto fabricado es una Instancia de un Tipo y esas instancias son las que llegan a los consumidores. Para éstos, cada producto es un Tipo y, pasa a ser una Instancia cuando se lo incorpora a algún sistema. Este cambio de Tipo a Instancia puede ocurrir en varias ocasiones.

Las mejoras reportadas al fabricante respecto a un producto pueden significar un ajuste a documentos asociados a un Tipo. Este nuevo Tipo creado puede ser utilizado para crear nuevas Instancias.

Las actualizaciones en los Tipos pueden ser llevadas a las Instancias, tanto de manera automática como a demanda. Por otro lado, pueden existir *loops* de realimentación, donde la fase de Uso y Mantenimiento de una Instancia puede realimentar al Tipo, incluso en la fase de desarrollo del Tipo del producto.

La digitalización y la vinculación con los Flujos de Valor contemplada en RAMI4.0 proporcionan un enorme potencial de mejora. El poder vincular adecuadamente la información de todas las partes interesadas, desde los proveedores hasta los consumidores, pasando por los procesos internos de la fabricación, y que cada una disponga en tiempo y forma de la información relevante, potencia globalmente la eficiencia del proceso.

Tipo

El Tipo define el conjunto de propiedades que son características para todas las Instancias de un activo en particular. El Tipo de un activo es inequívocamente identificable y surge de la idea inicial, en la fase de desarrollo. Una vez que todos los *tests* necesarios para su validación han sido exitosamente completados, el Tipo es liberado para la producción de las Instancias correspondientes.

Tipo - Desarrollo

Corresponde al proceso que va desde la idea, desde el concepto asociado, hasta el primer prototipo y las pruebas asociadas. Se define el Tipo de activo y las propiedades y funcionalidades características son definidas e implementadas. Aquí encontramos las actividades que tienen que ver con el Plan de Construcción, o sea: desarrollo, construcción, simulación y prototipado.

Tipo - Mantenimiento/Uso

Se crea la información "externa" asociada al activo (hoja de datos técnica,

manuales, información de marketing) y se comienza el proceso de venta. Las actividades presentes aquí son aquellas vinculadas al mantenimiento y uso del producto, o sea: actualizaciones de software, elaboración de manual de instrucción, cambio del producto.

Instancia

La Instancia es un activo inequívocamente identificable que está caracterizada por las propiedades de un Tipo, y que tiene una vinculación inequívoca con éste.

Instancia - Producción

Las Instancias de activos se producen en función de la información de Tipo del activo. Información, por ejemplo, específica sobre la producción en la que participa, logística, datos, número de serie, entorno de operación y rendimiento operacional se asocian con las Instancias de activos.

Instancia - Mantenimiento/Uso

Es la fase de uso de la Instancia del activo por parte del comprador. Los datos de uso del producto son asociados con la Instancia y pueden ser compartidos con otros actores involucrados en la cadena de valor, como por ejemplo, el fabricante. Puede incluir mantenimiento, resolución de problemas, rediseño, actualización, optimización y, fin de uso, con reciclado o desguace.

Eje "Niveles jerárquicos" - Eje horizontal derecho

El eje "Niveles Jerárquicos"se basa en el modelo de arquitectura de referencia para una fábrica documentado en los estándares para la integración de los sistemas de control y TI empresariales, DIN EN 62264-1 (IEC 62264-1) y DIN EN 61512-1 (IEC 61512-1). Para garantizar una consideración coherente en tantos sectores como sea posible, desde la automatización de fábrica hasta la industria de procesos, los términos *Enterprise*, *Work Centers*, *Station* y *Control Device* se han tomado de las normas antes mencionadas. Los siguientes niveles jerárquicos se han considerado para reflejar las necesidades de la I4.0:

- *Connected World*, que describe la relación entre un activo o combinación de activos (como una instalación o empresa) y otro activo o combinación de activos (otra instalación o empresa), es decir, por ejemplo, una red de fábricas

- *Field Device*, que representa el nivel funcional de un dispositivo de campo inteligente, como por ejemplo, un sensor inteligente
- *Product* denota que el producto cooperativo o colaborador se fabrique como parte integral de un proceso de valor añadido de la I4.0. No sólo la planta y la maquinaria para la fabricación de productos es importante en I4.0, sino que también lo es el producto a fabricar. Por lo tanto, se ha añadido "Producto" como el nivel inferior en este eje del modelo de referencia RAMI 4.0

2.3.3. Activos en la *Industrie 4.0*

La I4.0 utiliza una extensión del concepto de activos, comprendiendo elementos como fábricas, sistemas de producción, equipos, máquinas, componentes, productos, materiales, procesos de negocio, software, documentos, planes, estándares, servicios, personas, entre otros.

En el contexto de I4.0, dentro del mundo de los objetos, podemos distinguir tres grandes grupos: el mundo humano, el mundo de la información y el mundo físico.

El primero de los grupos mencionados, el mundo humano, representa a las personas.

El mundo de la información se divide en el mundo del modelo, el mundo del estado y el mundo del archivo. El primero de ello, el mundo del modelo, contiene por ejemplo, los siguientes objetos: meta-documentos (estándares, directivas) y documentos técnicos (diagramas funcionales, diagramas de planta, descripciones de productos, procedimientos). El segundo, el mundo del estado, describe el estado actual de la información mediante, por ejemplo, medidas actuales, valores objetivo, parámetros actuales de configuración. El tercer mundo, el mundo del archivo, contiene el estado registrado y la información asociada al ciclo de vida relativa a los procesos que están teniendo lugar; dichos procesos pueden ser procesos de producción, de desarrollo, de mantenimiento, entre otros.

Finalmente, el tercer grupo, el mundo físico, incluye por ejemplo a todos los productos físicos, instalaciones, recursos, sistemas TI y programas cargados en algún sistema.

A los efectos de fijar los conceptos, un programa por sí solo es parte del mundo de la información, mientras que el mismo programa cargado en un

sistema es parte del mundo físico.

Las personas son parte del mundo físico y participan del mundo de la información. Por sus propias capacidades, tienen un estatus especial.

Portadoras de información

La misma información puede estar disponible en diferentes portadoras. Por ejemplo, y utilizando como referencia la Figura 2.5, un procedimiento (mundo de la información) puede ser un archivo *pdf* almacenado en una computadora (portadora), o estar "en la cabeza de una persona" (portadora), o impreso en un conjunto de papeles (portadora); en los tres casos, nos referimos a componentes del mundo físico. El activo de información es el mismo; lo que cambia en cada caso es la portadora del activo y en cada caso, los mecanismos de protección del activo serán diferentes, pero siempre estaremos refiriéndonos al mismo activo.

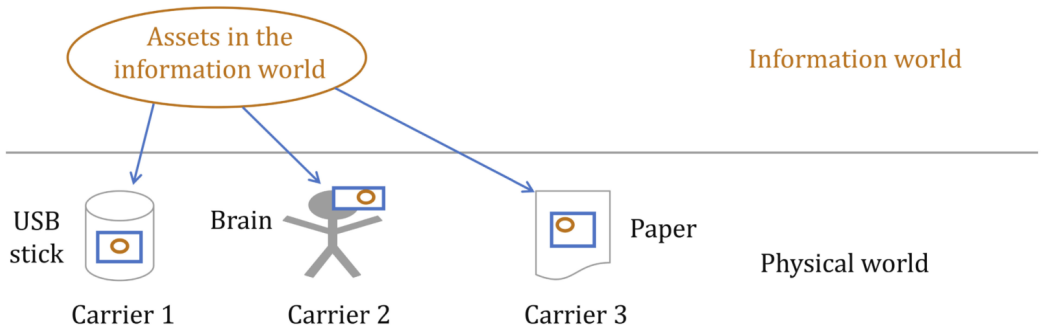


Figura 2.5: Activos y Portadoras. Fuente: [49]

Activos y el mundo de la información

Todo activo de una organización tiene valor para ella. Los activos son fabricados con un propósito específico, para cumplir un rol particular en un sistema. Ellos poseen una vida útil ("vita") y un cambio de valor asociado. El cambio de valor y de dueño son aspectos relevantes que refieren a los activos técnicos.

Algunas características de los activos

- Son diseñados, creados, usados y descartados
- Pueden ser una idea, un programa de software, un archivo, un servicio o cualquier cosa física

- Tienen una vida útil
- Son claramente identificables
- Son representados en el mundo virtual mediante su *Administration Shell* (AS)
- Pueden tener diferentes representaciones virtuales asociadas a sus diferentes propósitos
- Pueden ser combinados para crear nuevos activos con diferentes propósitos
- Son caracterizados en un proceso por medio del tiempo, su ubicación y su estado

Vida y caracterización de un activo

Como se refleja en la Figura 2.6 cada activo tiene un tiempo de vida específico durante el cual sirve el propósito para el que fue creado. Una vez que el activo es creado, este ya existe pero aun no está listo para ser utilizado. Todos los procesos que se deben recorrer desde que el activo ya está creado hasta que esté pronto para comenzar a trabajar en el lugar donde será utilizado se asocian a la fase de Provisión. Luego, comienzan dos fases: Uso y Mantenimiento. En la primera, el activo es parte de un sistema y está cumpliendo el rol para el que fue diseñado. La segunda fase, puede implicar al usuario del activo, a un servicio interno o externo o al fabricante, tanto local como remoto y con sus posibles combinaciones. El mantenimiento puede significar un rediseño (y posterior producción) o un ajuste al diseño actual.

Desde la óptica del mundo de la información, el activo es algo que existe, está en algún momento de su vida, posee capacidades de comunicación, es representado por información o datos y tiene una funcionalidad técnica.

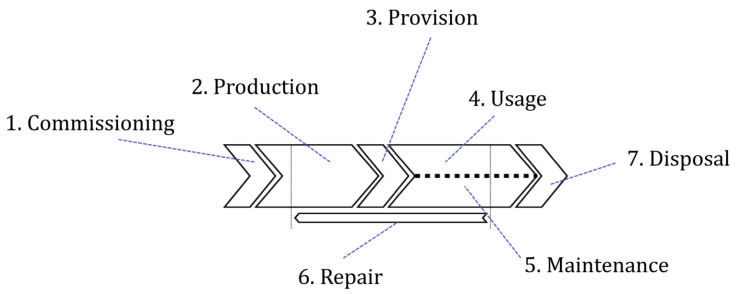


Figura 2.6: La vida de un activo. Fuente: [49]

En cuanto al mundo de la información, un activo puede caracterizarse como

se muestra en la Figura 2.7:

- Se presenta, o se da a conocer, de cierta manera (es decir, se conoce o no se conoce hasta cierto punto)
- Tiene un estado específico dentro de su vida (al menos un tipo o una instancia)
- Tiene capacidad de comunicación
- Se representa mediante información (datos)
- Tiene alguna funcionalidad técnica

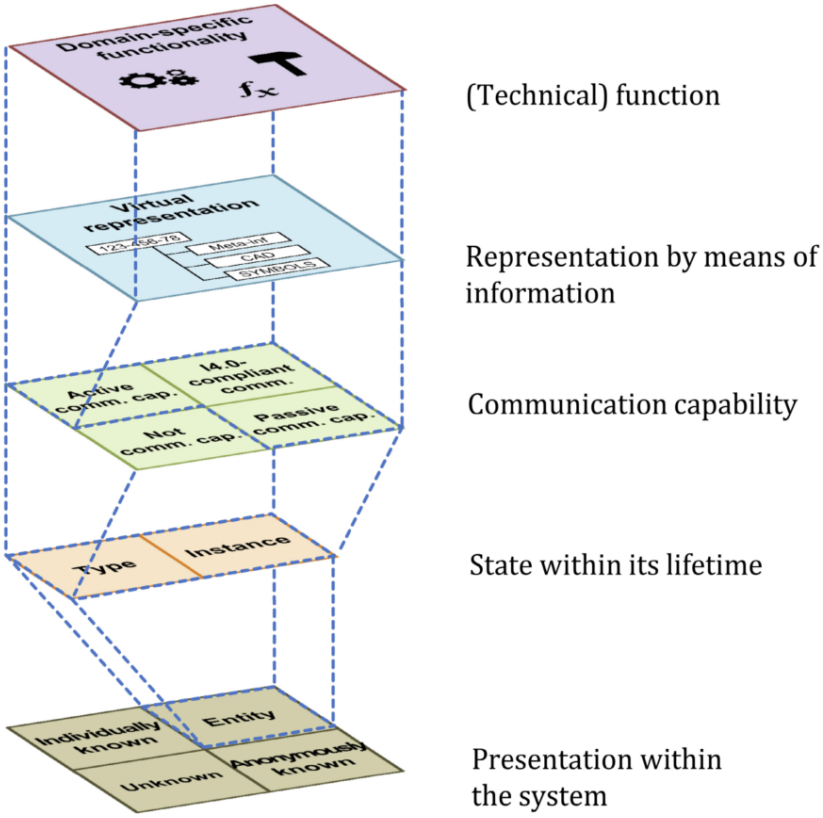


Figura 2.7: Conceptos asociados a un activo. Fuente: [49]

Los activos desde los sistemas de información

Según la cantidad de información disponible en un sistema de información respecto a un activo, se puede clasificar según las siguientes categorías:

- Desconocido
- Conocido anónimamente

- Conocido individualmente
- Administrado como una entidad

Desconocido

Se trata de un activo que no es conocido en el mundo de la información.

Conocido anónimamente

Activo que sólo es reconocido en el mundo de la información como un activo de un determinado tipo en determinado lugar.

Conocido individualmente

Se trata de los activos identificados sin ambigüedades. Un activo conocido individualmente tiene un nombre único que es conocido en el mundo de la información. El sistema tiene un método de identificación para el mundo físico y que puede asignar al nombre del objeto en el mundo de la información.

Administrado como una entidad

Se trata de aquellos activos que, dada su importancia, son administrados en el mundo de la información, pudiendo ser activos tanto del mundo físico como también del mundo de la información.

Las entidades son activos que están representados por información la que puede ser mantenida en el propio activo, en su representación o en sistemas TI, y comunicada mediante mecanismos compatibles con la I4.0. En este caso, la información involucrada supera a la mera identificación del activo, incluyendo además, por ejemplo, funciones para seguimiento del activo, para el registro de datos vinculados a su vida útil o para el monitorizado de su actividad operativa en el proceso del cual participa, como se representa en la Figura 2.8. Esta unidad funcional se conoce como *Component Manager*.

2.3.4. Componentes de la *Industrie 4.0*

Los componentes de la I4.0 son participantes global y únicamente identificables con capacidades de comunicación, que consisten de una AS y del activo como se puede observar en la Figura 2.9, con conexión digital a sistemas I4.0 y ofreciendo servicios.

En la sección 1.1 del Apéndice 1 amplia la información respecto a la *Administration Shell*.

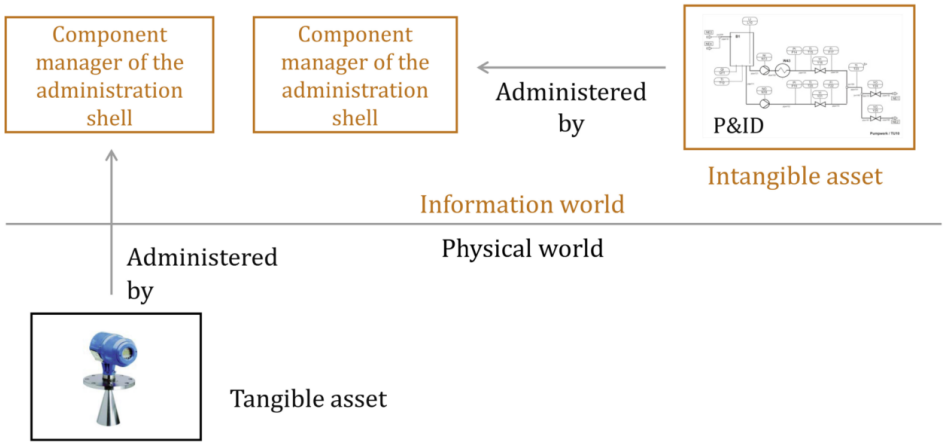


Figura 2.8: Entidades administradas por *Components Managers*. Fuente: [49]

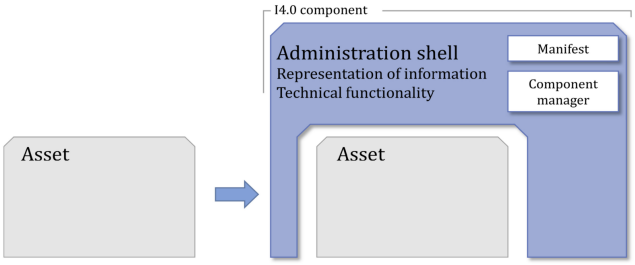


Figura 2.9: Un componente es la conexión necesaria entre un activo y el AS. Fuente: [49]

Capítulo 3

Industrial Internet Consortium

3.1. Introducción

El *Industrial Internet Consortium* (IIC) fue fundado en marzo de 2014 para reunir a las organizaciones y tecnologías necesarias para acelerar el crecimiento de la Internet Industrial, identificando, ensamblando, probando y promoviendo las mejores prácticas en la materia. Son miembros de IIC innovadores tecnológicos, líderes verticales del mercado, investigadores, universidades y organizaciones gubernamentales. Los recursos del IIC proporcionan a las organizaciones la orientación necesaria para aplicar estratégicamente las tecnologías digitales y lograr la Transformación Digital [108].

Actualmente el IIC está compuesto de 19 Grupos y Equipos de Trabajo distribuidos en 6 áreas [127]:

- Transformación Digital
- *Liaison*
- Marketing
- Seguridad
- Tecnología
- *Testbeds*

Por otro lado existe un *Steering Committee* [123] y un *Industry Leadership Council* [112] de reciente creación. Los recursos del IIC se pueden consolidar en 4 grupos [114], siendo el siguiente el contenido de cada uno de ellos:

Accelerator Program

- *IoT Challenges*
- *Test Drives*
- *Testbeds*

Toolbox

- *Project Explorer*
- *IoT Maturity Assessment*
- *Security Maturity Model*

Foundation

- *Frameworks*
- *Architecture*
- *Best Practices*

Community

- *Industry Leadership Councils*
- *Ecosystem*
- *Special Interest Groups*

3.2. Transformación Digital

Como se manifiesta en el artículo *The Road to Digital Transformation* [114], el IIC, desde su creación hace ya más de 5 años, ha elaborado varios documentos referenciales para comprender el concepto Internet Industrial, la mayoría de los cuales se abordarán en este capítulo. Algunos casos de aplicación del conocimiento generado también están plasmados en ciertos documentos que también se describirán aquí; en este caso se trata de trabajos impulsados por la tecnología más que por las necesidades concretas de los negocios. En *The Road to Digital Transformation* se manifiesta que para lograr el éxito es necesario ver la tecnología de la Internet Industrial en fábricas, en empresas energéticas, en el transporte, etc. Para lograrlo, se debe ayudar a los usuarios de tecnología de todas las industrias a hacerse cargo de su adopción, a demostrar el valor empresarial y ganar el apoyo de los líderes de las organizaciones de

esas industrias verticales. Identifican que muchas organizaciones tienen dificultades para entender cómo comenzar con un plan de proyecto y cómo la nueva tecnología de IIoT reducirá los costos y mejorará la seguridad, la eficiencia y la productividad de las operaciones. Para colaborar con las organizaciones y que alcancen la Transformación Digital [102], el IIC focaliza el esfuerzo en los 4 grupos mencionados antes: *Accelerator Program*, *Toolbox*, *Foundations* y *Community*.

3.3. *Digital Twin*

IIC define *Digital Twin* (DT) como una representación digital de una entidad (activo, proceso o sistema), incluyendo atributos y comportamientos, suficientes para cubrir los requerimientos de un conjunto de casos de uso. Se trata entonces de una réplica digital, dinámica y completa del objeto físico o lógico del mundo real, y que tiene validez durante toda la vida útil del mismo.

Los DTs son un excelente ejemplo de cómo la I4.0 impulsa una transformación profunda en la industria y en la fabricación [47, 1], ofreciendo oportunidades nunca antes disponibles, e incluso, ni imaginadas. Ello ha hecho que la tecnología DT actualmente sea considerada por la comunidad como una de las más estratégicas por su gran potencial, y que por lo tanto requiere especial atención [74, 161, 158].

Si bien los DTs se han comenzado a emplear para seguridad de dispositivos IoT (e IIoT), es necesario pensar y trabajar en la seguridad de los propios DTs. Es necesario tener presente que las amenazas en cuanto a la seguridad a las que está expuesto el DT pueden significar riesgos para su contraparte real. Las distancias entre la implementación del DT y la entidad que representa, qué tan bien representa la realidad, y qué tanto se sabe de dichas distancias, puede significar un problema de seguridad para ambos [100]. Si un atacante logra acceder a un DT podrá llegar a disponer de una visión muy cercana a la realidad de la entidad del mundo físico, lo que será un insumo valioso para un potencial ataque futuro.

En la sección 2.1 del Apéndice 2 se puede encontrar más información vinculada con el concepto *Digital Twin*.

3.4. *Industrial Internet Reference Architecture*

El *Industrial Internet Reference Architecture* (IIRA) [110] se trata de un reporte técnico elaborado por el IIC que especifica un *Industrial Internet Architecture Framework* (IIAF), que comprende puntos de vista y temas de interés para ayudar en el desarrollo, la documentación y la comunicación del IIRA.

Se trata del *framework* fundacional de la IIC para el resto de sus trabajos técnicos y sirve como guía para el desarrollo, la documentación, la comunicación y el despliegue de sistemas IIoT. Conceptualmente, el IIAF se encuentra inspirado en los conceptos del estándar ISO/IEC/IEEE 42010:2011, *Systems and software engineering — Architecture description* [160].

El objetivo del IIRA es que sea utilizado como *template* por los arquitectos de sistemas IIoT, destacándose un objetivo primordial: entender la convergencia de la *Operational Technology* (OT) y la *Information Technology* (IT) y la importancia de ello para alcanzar los beneficios de la IIoT.

Diversas partes interesadas participan al considerar sistemas complejos como los sistemas IIoT. Las partes interesadas tienen intereses entrelazados pertinentes al sistema y que pueden alcanzar todo el ciclo de vida del sistema. La complejidad del sistema requiere un marco para identificar y clasificar los intereses de las partes interesadas en categorías apropiadas. Este *framework* permite una evaluación sistemática de dichos sistemas, así como la resolución necesaria para diseñar y construir dichos sistemas.

3.4.1. *Framework* de la Arquitectura

Existe un concepto central en la arquitectura y es el denominado *viewpoint* (punto de vista). Se lo define como el conjunto de convenciones que enmarcan la descripción y el análisis de los aspectos (*concerns*) que resultan de interés en un sistema específico.

Una parte interesada es alguien o algo que tiene interés en algún aspecto del sistema y por extensión, tiene interés en algún *viewpoint* del sistema. Un *stakeholder* puede ser por ejemplo, una persona, un conjunto de personas, una organización, un sistema IIoT, o un conjunto de los anteriores.

El IIRA es el resultado de aplicar el IIAF a la clase de sistemas de interés, en este caso, los sistemas IIoT (ver Figura 3.1).

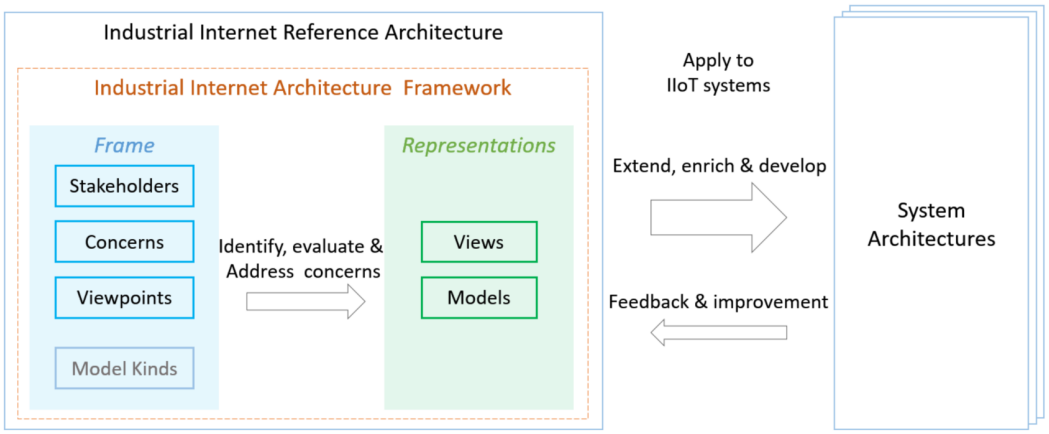


Figura 3.1: IIRA. Fuente: [110]

Viewpoints

Los *viewpoints* del IIRA son definidos analizando la variedad de casos de uso de IIoT desarrollados por el IIC, identificando las partes interesadas en los sistemas IIoT y enmarcando los aspectos de interés más adecuados. A partir de ello se identificaron cuatro *viewpoints*, organizados según muestra la Figura 3.2:

- Negocio
- Uso
- Funcional
- Implementación

Estos 4 *viewpoints* son la base para el análisis detallado de los aspectos de interés del sistema IIoT en cuestión. Es posible definir *viewpoints* adicionales para contemplar algunas situaciones particulares que así lo requieran. A continuación se brinda una primera aproximación a los Puntos de Vista definidos en el IIRA. En la Sección 2.2 del Apéndice 2 se puede encontrar una descripción más exhaustiva de los mismos.

Punto de Vista del Negocio

El punto de vista del Negocio pone foco en los temas que atañen a la identificación de las partes interesadas, su visión del negocio y los objetivos en el establecimiento de un sistema IIoT en su contexto empresarial y regulatorio.

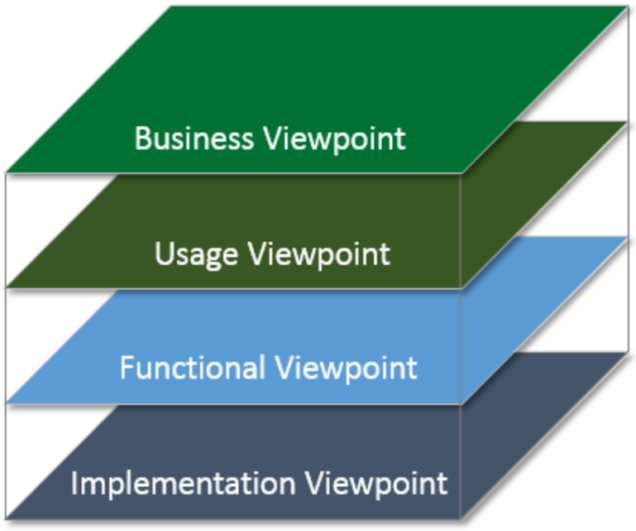


Figura 3.2: IIRA Viewpoints. Fuente: [110]

Además, identifica cómo el sistema IIoT logra los objetivos declarados a través de su mapeo a las capacidades fundamentales del sistema.

Punto de Vista del Uso

El punto de vista de Uso aborda los temas que involucran al uso esperado del sistema. Por lo general, se representa como secuencias de actividades que involucran a usuarios humanos o usuarios lógicos (por ejemplo, un sistema o componentes del sistema), que ofrecen la funcionalidad prevista para disponer de las capacidades fundamentales del sistema.

Punto de Vista Funcional

El punto de vista Funcional se centra en los componentes funcionales del sistema IIoT, su estructura e interrelación, las interfaces e interacciones entre ellas, y la relación e interacciones del sistema con elementos externos en el entorno, para apoyar los usos y actividades del sistema general.

Con el objetivo de analizar adecuadamente el punto de vista Funcional, se introduce el concepto de Dominio Funcional. Esta descomposición, a los efectos del análisis, del punto de vista Funcional en 5 dominios funcionales reafirma la relevancia de cada uno de ellos y las diferentes prioridades según la vertical industrial que se esté considerando.

Dominios Funcionales

Los 5 Dominios Funcionales definidos, como se pueden apreciar en la Figura 3.3, son:

- Control
- Operaciones
- Información
- Aplicación
- Negocio

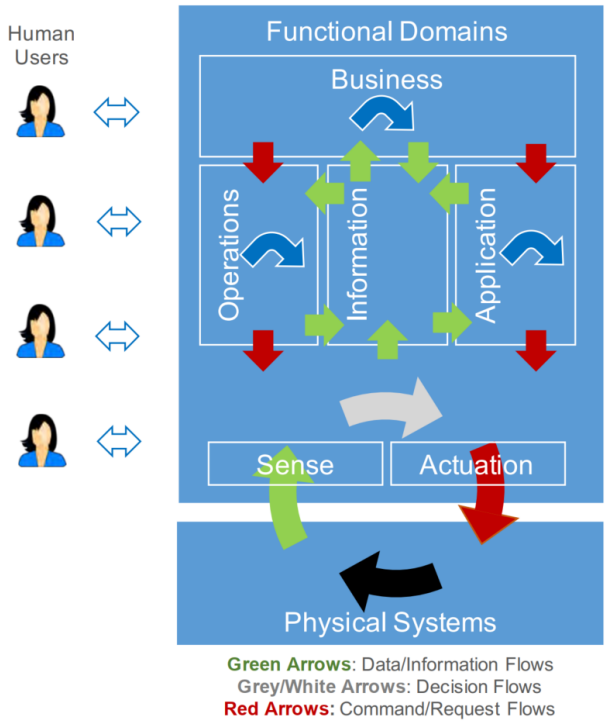


Figura 3.3: Dominios Funcionales. Fuente: [110]

Los Dominios Funcionales se describen en detalle en la sección 2.2.3 del Apéndice 2.

Punto de Vista de la Implementación

El punto de vista de la Implementación se ocupa de las tecnologías necesarias para implementar los componentes (punto de vista Funcional), sus

esquemas de comunicación y sus procedimientos durante el ciclo de vida. Estos elementos están coordinados por actividades (punto de vista de Uso) y sirven de apoyo para las capacidades del sistema (punto de vista del Negocio).

Aspectos de interés transversales

El orden en que han sido presentados los *viewpoints* (estrategia *top-down*) refleja cómo en general se da la interacción entre los mismos. El punto de vista de arriba, guía e impone requerimientos al punto de vista que está debajo suyo. Por lo otro lado, los análisis que se realizan en un punto de vista, sirven como insumo para que en el punto de vista que se encuentra encima de él, se puedan validar las decisiones tomadas, o identificar los cambios necesarios (estrategia *botton-up*), tal como se refleja en la Figura 3.4.

Los puntos de vista mencionados, Negocio, Uso, Funcional e Implementación, aportan una forma sistemática para identificar asuntos de interés en los sistemas IIoT y de las partes interesadas, pero ello no implica que el abordaje deba ser siempre de manera aislada en cada *viewpoint*, sin considerar los restantes. Estos aspectos de interés son los denominados transversales (*Cross-cutting Concerns*), siendo posibles ejemplos de ellos la seguridad o el *safety*. En general se las relaciona con propiedades de los sistemas, y más formalmente, se las denomina *Características del Sistema*, reflejando propiedades y comportamientos de los sistemas IIoT que son el resultado de los subsistemas que componen e interactúan en el sistema en cuestión, en el contexto y con el entorno donde se encuentra.

Frecuentemente las Características de los Sistemas están sujetas a regulaciones, requerimientos de cumplimientos y acuerdos contractuales, por lo que debe ser posible medirlas y evaluarlas. En este contexto, se debe tener presente que los sistemas pueden contar con componentes y soluciones de varios fabricantes, eventualmente combinados dinámicamente e incluso luego del despliegue, lo que agrega complejidad a la hora de poder evaluar los cumplimientos exigidos y/o acordados.

Es necesario entonces considerar y abordar los asuntos de interés más allá de la fase de diseño del sistema: se deberían contemplar en todo el ciclo de vida. Esta arquitectura de referencia, a través de sus puntos de vista, brinda una orientación a los procesos del ciclo de vida del sistema en cuestión, desde la concepción del sistema IIoT hasta el último día de uso, considerando su

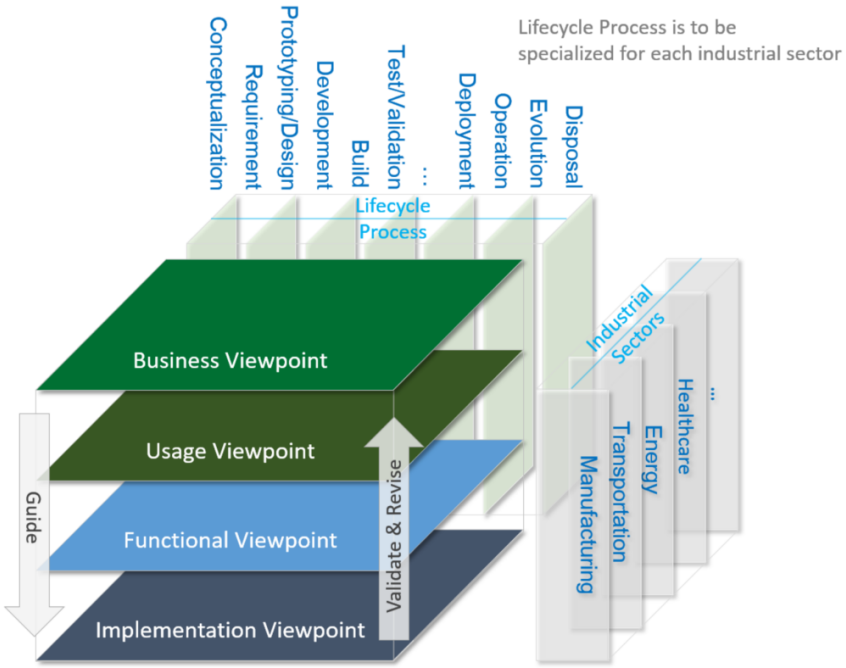


Figura 3.4: *Viewpoints*, Alcance y Ciclo de Vida. Fuente: [110]

disposición final, pasando obviamente por las etapas intermedias, como por ejemplo el diseño y la implementación.

Funciones Transversales y Características del Sistema

Los componentes funcionales mencionados y descritos en los Dominios Funcionales hacen a las funciones que generalmente son requeridas para que los sistemas IIoT operen y cumplan con los cometido básicos que impone el negocio. Además se requieren funciones adicionales que aplican a todos los dominios funcionales y que hacen posible que efectivamente las funciones inicialmente mencionadas se puedan ejecutar. Esas funciones son las que se conocen como *Funciones Transversales* (por ser transversales a los Dominios Funcionales).

Por otro lado, el comportamiento de un sistema IIoT no es la simple suma de los comportamientos de cada uno de los componentes que hacen al mismo, pues la complejidad del sistema hace que no se pueda obviar las interacciones entre sus componentes y los impactos, positivos o negativos, que eso tenga. Esas propiedades o comportamientos que emergen de la interacción entre los componentes es lo que se conoce como Características del Sistema.

El sistema y el análisis funcional Transversal se refiere en gran medida a

cómo trabaja el sistema, mientras que el análisis de las Características del Sistema hace hincapié en qué tan bien trabaja el sistema.

La realización de una Característica del Sistema en determinado nivel deseado puede depender de restricciones impuestas por otras Características del Sistema e incluso, pueden llegar a ser totalmente contrapuestas.

Por lo tanto, la IIRA elaborada por el IIC y reflejada en la Figura 3.5, pone un fuerte énfasis en las funciones necesarias para apoyar el propósito empresarial del sistema y garantizar las características adecuadas del sistema, para que las funciones se realicen correctamente y el propósito del negocio no se vea comprometido.

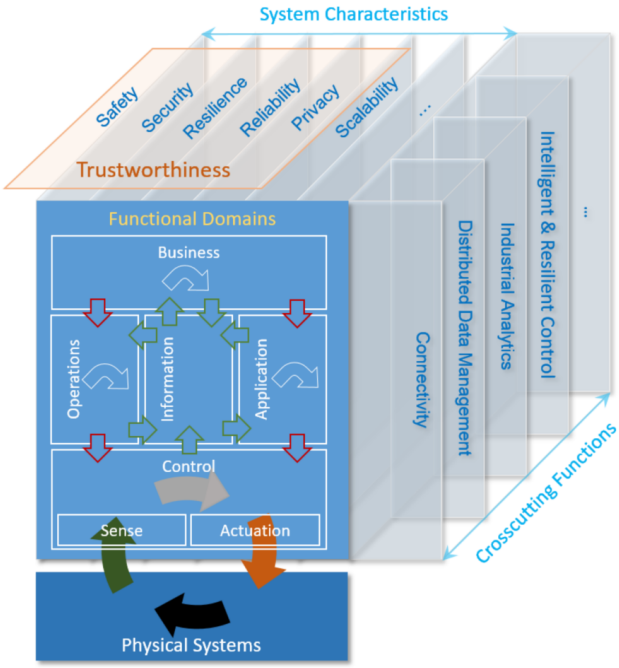


Figura 3.5: Dominios Funcionales, Funciones Transversales y Características del Sistema. Fuente: [110]

Las 6 Características del Sistema que se explicitan en la arquitectura de referencia del IIC son:

- *Safety*
- Seguridad
- Resiliencia
- Fiabilidad
- Privacidad
- Escalabilidad

Las 5 primeras conforman el concepto de Confiabilidad (*Trustworthiness*).
Las Funciones Transversales que se explicitan en la IIRA son:

- Conectividad
- Gestión de Datos Distribuidos
- Analítica Industrial
- Control Resiliente e Inteligente

Tanto para el caso de las Características del Sistema como para las Funciones Transversales, la IIRA habilita la definición de otras que enriquezcan el trabajo asociado.

En el documento *The Industrial Internet of Things Volume G2: Key System Concerns* [125] se provee un análisis adicional y más profundo de los Intereses Clave del Sistema, de manera que se disponga de una estrategia más amplia y profunda para abordar esos intereses claves que no pueden ser asignados ni a los Dominios Funcionales ni a los Puntos de Vista de la IIRA. Adicionalmente, en el documento se analiza la interacción de los intereses entre sí.

Patrones de Arquitectura

La IIRA presenta tres patrones referenciales que pueden utilizarse como punto de partida para elaborar la arquitectura del sistema en cuestión.

Los Patrones de Arquitectura identificados son:

- Tres Niveles (*Three-Tier*)
- Gestión y Conectividad en el Borde mediante *Gateway*
- Bus de Datos en Capas

En la sección 2.3 del Apéndice 2 se puede encontrar una descripción detallada de los mismos.

3.5. *Industrial Internet of Things Security Framework*

.

El objetivo inicial del *Industrial Internet of Things Security Framework* (IISF) [75] elaborado por el IIC, es viajar hacia un consenso industrial respecto a la seguridad de los sistemas IIoT, en la concepción más amplia del término.

3.5.1. Introducción

Un sistema de Internet de las Cosas Industrial (IIoT, por su sigla en inglés) conecta e integra sistemas de control industrial con sistemas empresariales, procesos de negocio, analítica y personas. Un sistema IIoT permite avances significativos en la optimización de la toma de decisiones, las operaciones y la colaboración entre un gran número de sistemas de control cada vez más autónomos.

Estos sistemas difieren de los sistemas de control industrial tradicionales al estar ampliamente conectados a otros sistemas y personas, aumentando su diversidad y escala. También difieren de los sistemas de Tecnología de la Información (TI) en que utilizan sensores y actuadores en un entorno industrial. Por lo general, se trata de sistemas que interactúan con el mundo físico, donde un cambio no controlado puede conducir a condiciones peligrosas. Este riesgo potencial aumenta la importancia de la seguridad (y del *safety*), la fiabilidad, la privacidad y la resiliencia, más allá de los niveles esperados en muchos entornos de TI tradicionales. Estos sistemas IIoT también pueden tener flujos de datos que involucran a organizaciones intermediarias, que requieren enfoques de seguridad más allá de los enfoques simples y tradicionales. Al tener una larga vida útil, los sistemas IIoT incluyen instalaciones heredadas y están regulados porque la salud humana puede estar en riesgo. Las culturas de los mundos tecnológicos operativos y de la información difieren, lo que lleva a la necesidad de integrarlas para los sistemas IIoT. Todas estas diferencias tienen implicancias en la forma en que estos sistemas deben ser asegurados.

3.5.2. Motivación

Históricamente, la seguridad en sistemas industriales confiables se basaba en la separación física y en el aislamiento de la red de los componentes vulnerables, y en la oscuridad de las reglas de diseño y de acceso a los sistemas de control críticos. La seguridad se aplicaba, y se sigue haciendo, a través de cerraduras físicas, sistemas de alarma y, en algunos casos, guardias armados. El potencial de error humano o mal uso era plasmado principalmente a través del acceso directo y las preocupaciones se centraban en interrumpir la seguridad y fiabilidad del sistema, siendo mitigados esos riesgos mediante un buen diseño, actividades de análisis y revisiones, pruebas exhaustivas y actividades de capacitación.

Los diseñadores y operadores de los sistemas industriales rara vez consideraron que estos podrían estar algún día expuestos a una red global, remotamente accesible por muchos, desde usuarios legítimos hasta gobiernos corruptos.

En las últimas décadas, el aumento del poder de cómputo cada vez más asequible, la ubicuidad de la conectividad y las técnicas de análisis de datos en evolución, han abierto la puerta a la convergencia de los sistemas de control, los sistemas empresariales e Internet. Esta convergencia está aumentando la productividad, la eficiencia y el rendimiento de los procesos operativos existentes y permite la creación de nuevas formas de aprovechar los datos de las operaciones, ofreciendo así valor empresarial creciente.

Pero con estas ventajas vienen los riesgos. Los sistemas que fueron diseñados originalmente para estar aislados ahora están expuestos a ataques cada vez más sofisticados, y los supuestos de diseño de los sistemas de OT existentes ya no se deberían aplicar por si solos. Un ataque exitoso a un sistema IIoT tiene el potencial de ser tan grave como los peores accidentes industriales hasta la fecha (por ejemplo, el desastre de Chernobyl [31], Ucrania, en 1986, o el de Bhopal [263], India, de 1984), lo que resulta en daños al medioambiente, lesiones o pérdida de vidas humanas, incluso afectando a generaciones futuras. También existe riesgo de daños secundarios, como la divulgación de datos confidenciales, la interrupción de las operaciones y la destrucción de los sistemas. Los resultados de los ataques a los sistemas IIoT pueden ser generalizados y comparables a grandes desastres naturales, incluso en el caso de errores y fallas, eventualmente combinadas con ataques.

Las organizaciones deben utilizar su experiencia para que sus sistemas IIoT

sean confiables. El uso de sensores y actuadores en un entorno industrial no es la experiencia típica de IT. OT e IT priorizan las características del sistema de manera diferente. Por ejemplo, en general, la resiliencia en IT es menos importante que en OT, y la seguridad es menos importante en OT que en IT. Estas características interactúan entre sí y pueden llegar a entrar en conflicto. En los sistemas IIoT, estas características del sistema deben converger y conciliarse entre sí en la confiabilidad (*trustworthiness*) general del sistema, tal como se ilustra en la Figura 3.6.

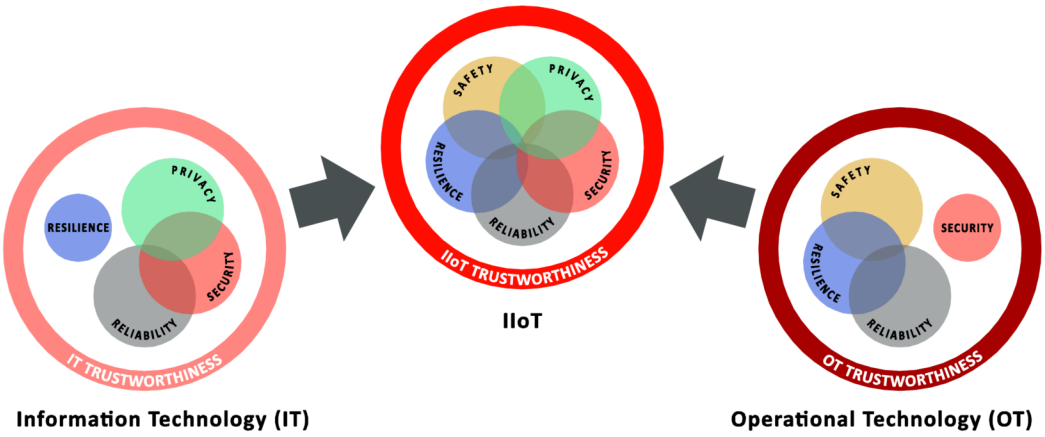


Figura 3.6: Convergencia de OT e IT - Confiabilidad. Fuente: [111]

Las organizaciones IIoT deben dar importancia al *safety* y la resiliencia más allá de los niveles esperados en muchos entornos de IT tradicionales. Desafortunadamente, hasta ahora los integrantes de los departamentos de IT rara vez "hablan el mismo idioma" que quienes se ocupan de los sistemas de OT. Los dos, IT y OT, perciben el riesgo de manera diferente, y no se pueden combinar para obtener una ganancia positiva sin una consideración equilibrada de motivaciones diferentes.

La prioridad más alta de muchos sistemas OT es la propiedad de *safety* o sea, que no sucedan lesiones o la propia muerte, que no se ponga en riesgo al público y que se proteja de daños al medioambiente. Las siguientes prioridades en el mundo OT son a menudo la calidad de la producción y el cumplimiento de los objetivos de producción, que dependen de la fiabilidad y de la resiliencia del sistema. La fiabilidad y la resiliencia son necesarias para evitar la interrupción de los procesos críticos de la sociedad, como por ejemplo la red eléctrica. Los aspectos de seguridad se consideran en OT, pero dado que la mayoría de los sistemas no están (estaban) conectados a la red, en su mayoría se enfoca en la

seguridad física.

Por otro lado, la seguridad y la privacidad son características importantes para la mayoría de los sistemas de IT, junto con la fiabilidad. La propiedad de *safety* rara vez es (era) un problema, y la resiliencia se reserva a sistemas especializados donde la continuidad del negocio es un factor motivador, por ejemplo para el caso de las transacciones financieras.

Este *framework*, el IISF, ofrece un contexto para equilibrar las consideraciones relevantes para la seguridad, en su enfoque más amplio, de las dos culturas diferentes de los mundos OT e IT.

3.5.3. Características Clave del Sistema que permiten la Confiabilidad

Las cinco características que más afectan las decisiones de confianza en el despliegue de un sistema IIoT son:

- *Safety*
- Seguridad
- Fiabilidad
- Resiliencia
- Privacidad

Ellas se identifican como las Características Clave del Sistema. Cada una de ellas debe ser asegurada adecuadamente, pudiendo existir técnicas de abordaje comunes a todas. Existen otras características del sistema como ser la escalabilidad, la usabilidad o la portabilidad que no se consideran claves, lo cual no implica que deban ser ignoradas.

Garantía de la Características Clave del Sistema

La Garantía requiere de la obtención y el análisis de evidencia que apoye el diseño, la construcción, el despliegue y las pruebas del sistema, y las actividades de operación. La garantía incluye un análisis de riesgos. Los riesgos (el efecto de la incertidumbre en los objetivos) tienen en cuenta la probabilidad de la ocurrencia de un evento y el impacto en caso de ocurrir. El diseño riguroso de un producto o sistema incluye revisiones de diseño y *testing* con el objetivo de prevenir faltas operativas y para disponer de un sistema más resiliente a potenciales eventos identificados durante el análisis de riesgos.

Los Casos de Garantía demuestran a las partes interesadas mediante evidencias de mecanismos de protección y prestaciones de seguridad, que sus expectativas para cada una de las Características Claves del Sistema se cumplen.

Safety

Safety es la condición de un sistema para operar sin riesgos inaceptables de causar lesiones físicas o afectar la salud de las personas, tanto directamente como indirectamente a través de daños a la propiedad o al medioambiente.

La garantía del *safety* radica en los esfuerzos para eliminar fallas sistemáticas y probabilísticas. Las técnicas tradicionales de evaluación de la seguridad de OT se centran en los elementos físicos y en los procesos, y en la probabilidad de una combinación de fallas que pongan en riesgo un sistema. El concepto de adversario en este contexto no estaba considerado, salvo en el caso de algún tipo de atentado. En el caso de sistemas críticos, las pruebas de aceptación de los mismos, y de sus componentes, cobran un rol fundamental a la hora de considerar el *safety*, lo que en ciertos contextos requiere del uso de simuladores.

Seguridad

Es la condición de que el sistema está protegido frente a accesos involuntarios o no autorizados, cambios o destrucción a equipos, sistemas o información, asegurando la disponibilidad, la integridad y la confidencialidad de la información. La seguridad de un sistema (IIoT) debe ser analizada en el contexto de su aplicación.

La Garantía de la seguridad en general es evaluada en términos de riesgos, considerando las amenazas, los activos, las vulnerabilidades y, las contramedidas y controles asociados.

Cuando se habla de seguridad de la información o de la seguridad de un sistema en general, se hace referencia al acrónimo de propiedades CIA: *Confidentiality*, *Integrity* y *Availability* o Disponibilidad, intentando reflejar un orden de prioridad, con todas las excepciones que se puedan identificar en diferentes sistemas y/o contextos.

En los sistemas de OT tradicionales, en general, la disponibilidad se ha considerado primordial, seguida de la integridad, siendo la confidencialidad generalmente la última en consideración, lo que lleva a considerar en dichos sistemas el acrónimo AIC.

Fiabilidad

La Fiabilidad es la habilidad de un sistema o componente para realizar las funciones requeridas en las condiciones establecidas, por un período de tiempo especificado. Ello incluye además los niveles esperados de *performance*, calidad de servicio, disponibilidad funcional y precisión. La fiabilidad está vinculada con la disponibilidad, siendo la relación entre la disponibilidad real sobre la disponibilidad programada.

El aseguramiento de la fiabilidad requiere un conocimiento detallado del ambiente operacional, de la composición del sistema, de cómo fue diseñado y fabricado, para poder llegar determinar la probabilidad de falla. También se deben considerar otros parámetros como ser configuraciones, atributos físicos, requerimientos de *uptime* y conectividad con otros sistemas y con Internet.

Resiliencia

La Resiliencia es la capacidad de un sistema o componente de mantener un nivel aceptable de servicio en presencia de una interrupción. Esto incluye la capacidad de recuperar de manera oportuna funciones perdidas, o de reasignar tareas. Frecuentemente la resiliencia es lograda diseñando el sistema de tal forma que las fallas son compartimentadas o sea, que una falla no desencadene otra.

La garantía de la resiliencia implica incorporar redundancia física y/o lógica para los elementos y las interconexiones entre ellos, los cuales deben ser adecuadamente probados para validar el correcto funcionamiento en caso de requerirse.

Privacidad

La Privacidad es el derecho de un individuo o grupo de individuos de controlar o influenciar qué información relacionada a ellos puede ser recogida y almacenada, por quién y a quién se le puede divulgar.

La garantía de la privacidad depende de si las partes interesadas esperan, o están legalmente requeridas, a tener información protegida o controlada para ciertos usos. Para ello es importante mantenerse al día con las regulaciones y estándares al respecto.

Es necesario tener especial cuidado con el objetivo de buscar minimizar el uso de los datos y abordar los riesgos asociados con el establecimiento de la identidad de las partes cuando esas identidades no deben ser reveladas.

La identidad puede revelarse mediante el examen de metadatos asociados con la parte o a través de la correlación de datos sobre la parte. La integración de los sistemas IIoT podría aumentar este riesgo. Los propios mecanismos de seguridad pueden aumentar los riesgos de privacidad al crecer la cantidad de datos recopilados y asociados con una parte.

Los riesgos vinculados a la privacidad pueden aumentar a medida que los sistemas industriales están interconectados con otros sistemas que contienen datos confidenciales, como por ejemplo un *Customer Relatioship Management* (CRM); por ejemplo, la información sobre los artículos producidos para determinados clientes podría revelarse a través de una brecha de seguridad de cualquiera de los sistemas. Riesgos adicionales pueden implicar el intercambio y la distribución inapropiada de información con terceras partes.

3.5.4. Sistemas Confiables

Un objetivo fundamental para una parte interesada en lo que refiere a un sistema es que sea confiable respecto a sus Características Claves, sus interacciones y sus dependencias.

Como pretende mostrar la Figura 3.7, la Confiabilidad es el grado de confianza que se tiene respecto a que un sistema se comporta de acuerdo con lo esperado en presencia de, fallas de los sistemas, perturbaciones ambientales, ataques y/o errores humanos, lo que constituyen las amenazas.

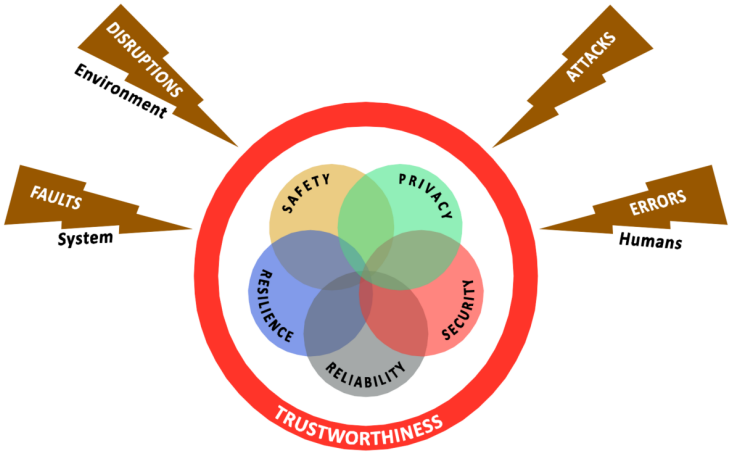


Figura 3.7: Confiabilidad de un Sistema IIoT. Fuente: [111]

Las perturbaciones ambientales, los errores humanos, las fallas de los sistemas y los ataques son las fuentes de incertidumbre que influyen en la proba-

bilidad de que un riesgo se materialice.

La confianza en el sistema proviene de poder garantizar las expectativas o sea, que diversos aspectos del sistema están bajo control, como ser la seguridad de sus datos y de su equipamiento, el *safety* de las personas y la comunidad, la protección de los activos, la protección de la privacidad de los datos, la fiabilidad de las operaciones y subsistemas, y la resiliencia del sistema. La confianza resulta esencial para el negocio, incluyendo la confianza en que las consecuencias de las decisiones y de los procesos son aceptables, y que la información del negocio es manejada adecuadamente.

Diferenciando aspectos para el aseguramiento de los sistemas IIoT

Tradicionalmente, y de acuerdo a lo expresado antes, la seguridad de los sistemas de IT y OT se ha evaluado de forma independiente, pero un sistema IIoT es más que una simple fusión de ambos. Los sistemas IIoT confiables requieren que sus funciones de seguridad, en su concepción más amplia, sean evaluadas de extremo a extremo tanto en IT como en OT. La integración de la seguridad de IT y OT requiere comprender las diferencias entre ellos y sus enfoques para evaluar y proteger los sistemas. La seguridad, las regulaciones y las normas deben evolucionar en ambos mundos, juntas y de manera coordinada, para ser eficaces.

Convergencia de IT y OT

En el pasado ha habido una fuerte separación entre IT y OT. IT cubre los sistemas informáticos y de comunicación comunes en todas las industrias. En general las aplicaciones de software se centran en las personas y el comportamiento en tiempo real suele estar limitado por los tiempos de interacción humana.

OT, por otro lado, es una combinación de hardware (inicialmente) y software (más recientemente) que recopila información y provoca cambios en el mundo físico a través de los sistemas de control. En OT, el comportamiento en tiempo real puede ser esencial para la corrección, lo que puede afectar al tipo de controles de seguridad implementados.

Esta convergencia, que se ejemplifica en la Figura 3.8, requiere que las diversas funciones que se ejecutan en el sistema IIoT siempre se consideren juntas. Es por esta razón que en la arquitectura de referencia IIRA se fusiona-

ron las funciones de IT y OT en un conjunto de Dominios Funcionales (Control, Operación, Información, Aplicación y Negocio) que cubren lo que habría que hacer de ahora en más, en lugar de seguir con lo que se ha hecho hasta ahora.

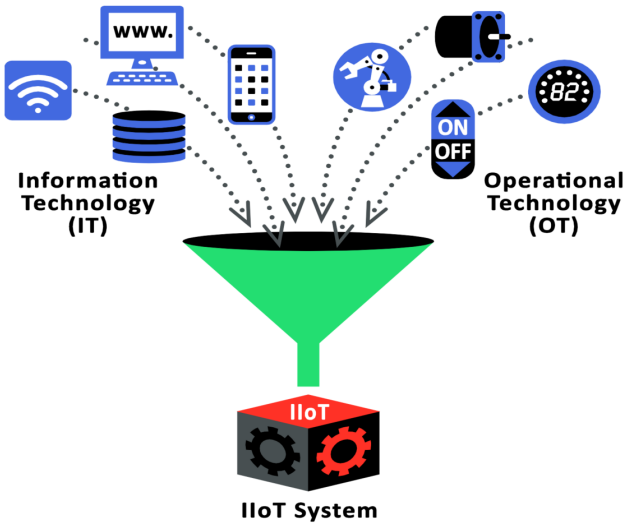


Figura 3.8: Convergencia IT/OT. Fuente: [111]

3.5.5. Puntos de Vista del Negocio

La toma de decisiones empresariales eficaces es un componente importante de los programas de seguridad industrial. Los riesgos de seguridad, así como los costos y beneficios de las diferentes posturas defensivas, deben comunicarse a los responsables de la toma de decisiones empresariales, especialmente porque a menudo no están familiarizados con los detalles de los riesgos de seguridad y las contramedidas correspondientes. Se debe establecer y mantener un programa de seguridad que proporcione gobernanza, planificación y patrocinio para las actividades de seguridad de la organización. Estas actividades deben alinearse con los objetivos generales de negocio y la estrategia de riesgo de la organización. Dicho programa de seguridad debe mantener las políticas, los mecanismos y los procesos de seguridad asociados actualizados en respuesta a los cambios en las prioridades del negocio, la disponibilidad de recursos, los riesgos que surjan y los nuevos objetivos de protección. La gestión del riesgo es un objetivo importante de un programa de seguridad (y privacidad). Esto a menudo consiste en derivar un modelo de amenaza y finalmente definir los controles de seguridad y capacidades para administrar el riesgo, teniendo en

cuenta la vida útil del sistema. En la sección 2.4 del Apéndice 2 se profundiza en los conceptos fundamentales vinculados a la gestión de riesgos.

Métricas y KPIs

Los responsables de la toma de decisiones empresariales deben supervisar los informes sobre la seguridad de sus sistemas IIoT desde el momento en que son concebidos, a través de su diseño y creación, y a lo largo de su funcionamiento. Esto se debería realizar con la misma profundidad que se supervisan otras características, como el rendimiento, el costo y la eficiencia. Las medidas y métricas correctas informan a los responsables de la toma de decisiones, a los operadores y a otras partes interesadas. Algunas de las métricas y medidas son comunes en todos los verticales; otras son únicas. Las métricas de seguridad pueden configurar un bucle continuo para identificar áreas de riesgo, aumentar la rendición de cuentas, mejorar la eficacia de la seguridad, demostrar el cumplimiento de las leyes y regulaciones y proporcionar insumos cuantificables para una toma de decisiones eficaz. Estas métricas ayudan a identificar los problemas de seguridad de forma temprana y también a una gestión y gobernanza más rápidas y eficientes. Los KPIs seleccionados para cada aplicación también mejoran la calidad del servicio, ya que permiten identificar a tiempo un problema y tomar las medidas correctivas o compensatorias adecuadas.

Consideraciones de gestión

La administración de la seguridad de IIoT implica una acción coordinada dentro de la organización y se centra en la respuesta rápida para garantizar la ejecución oportuna de las tareas de seguridad.

Hay una complejidad considerable en el orquestado de las respuestas de seguridad, y el espacio problemático se convierte rápidamente en un desafío multidimensional, tal como se refleja en la Figura 3.9. Las medidas de seguridad deben ser capaces de adaptarse a las amenazas continuamente cambiantes y a las configuraciones del sistema ("que se adapta", *Adaptability*), deben además proporcionar respuestas que minimizarán el impacto en el sistema IIoT si una amenaza de seguridad se materializa ("que responde", *Responsivity*) y además permiten que diferentes organizaciones trabajen juntas para garantizar la identificación temprana de las amenazas a la seguridad ("que cooperan", *Cooperativity*) [81].

La gestión del riesgo equilibra las amenazas contra el sistema IIoT con

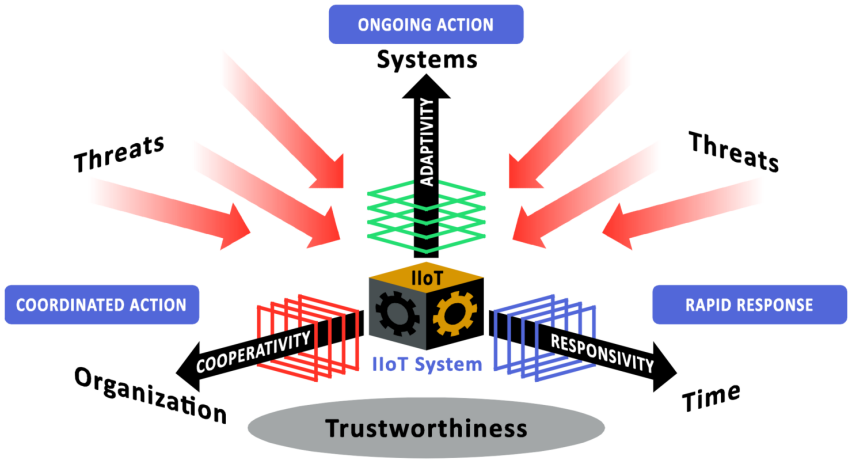


Figura 3.9: Consideraciones para la Gestión de la Confiabilidad. Fuente: [111]

las respuestas de seguridad que contrarrestan esas amenazas y el riesgo que representan. La gestión de riesgos implica acciones continuas para tomar las decisiones adecuadas basadas en la evidencia de seguridad (métricas y KPIs), así como el monitorizado de datos para priorizar las tareas de seguridad.

La seguridad debe ser adaptable para mantener la eficacia a lo largo del tiempo. El análisis de seguridad debe adaptarse a los cambios en el entorno, a las nuevas amenazas a las que está expuesto el sistema, y a las nuevas vulnerabilidades que se encuentran. Como premisa, las amenazas deben ser tratadas antes de que se materialicen.

Para lograrlo, la gestión, la ingeniería, las operaciones y los recursos humanos deben cooperar continuamente. La formulación de una respuesta rápida cuando se produce un incidente, basada en una evaluación del alcance de la amenaza de seguridad, es importante para proteger los sistemas y minimizar los daños.

Impregnación de la confianza en el ciclo de vida del sistema IIoT

Un sistema IIoT típico es un ensamblado complejo de diferentes elementos. La confiabilidad en el sistema depende de la confianza en todos los elementos que lo componen, en cómo se integran y en cómo interactúan.

La impregnación de la confianza, de acuerdo a la Figura 3.10, atraviesa todo el ciclo de vida del sistema, y no solo comprende la operación. Desde la cadena de suministro, pasando por la puesta en marcha, el aprovisionamiento, el uso regular y hasta el desmantelamiento al final de su vida útil, deben ser cuidadosamente monitorizados para garantizar que la confiabilidad se mantiene

en un nivel al menos aceptable.

El ciclo de vida de la confianza comienza con la especificación de los requerimientos del sistema por parte del usuario al proveedor de sistema, quien especifica los requerimientos de todos los componentes a los proveedores de los mismos. Cada proveedor de cada componente garantiza que las capacidades del componente cumplen con los requerimientos recibidos, lo cual es confirmado por el propio proveedor del componente, por el proveedor del sistema o por una tercera parte y lo mismo ocurrirá cuando el proveedor del sistema le entrega al usuario un sistema con las capacidades que contemplan los requerimientos que éste manifestó inicialmente.

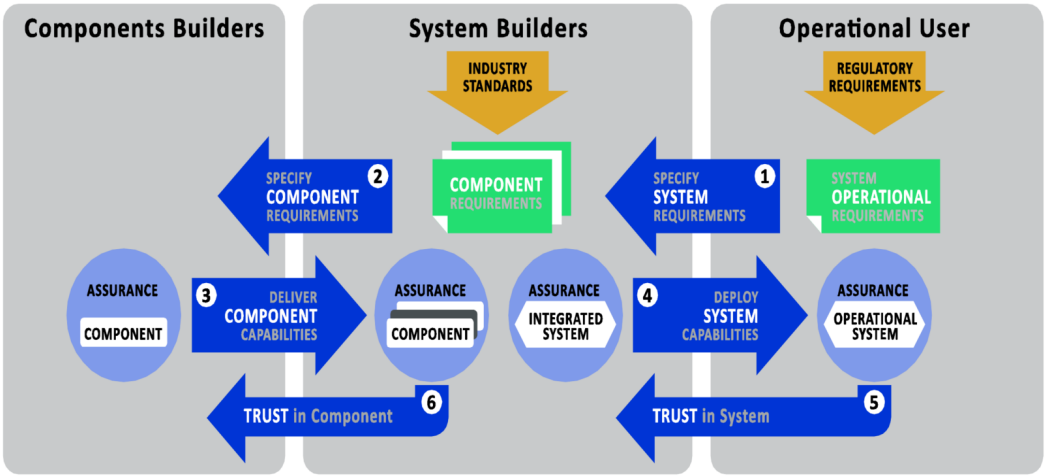


Figura 3.10: Impregnación de la Confianza. Fuente: [111]

Luego de ello, la confianza se impregna en el sistema y por lo tanto, en cada uno de sus componentes. Por lo tanto, la confianza fluye en el sentido *top-down* y la creación de la confianza fluye en el sentido *botton-up*.

En lo que refiere a los requerimientos, en general pueden existir de dos tipos: explícitos e implícitos. Los primeros son prestaciones necesarias del sistema y los segundos, características del sistema. En general existe una tendencia en hacer foco en los requerimientos explícitos, dejando (algo) abandonados los implícitos, que pueden terminar siendo los que comprometan seriamente la confianza en el sistema o en algún componente.

La fiabilidad de un componente técnico no sólo se define como la suma de la fiabilidad de sus subcomponentes. Es responsabilidad del desarrollador de componentes asegurarse que los subcomponentes funcionan correctamente junto con sus capacidades especificadas. La debilidad de un solo subcomponente

puede llevar a la pérdida de confianza en todo el sistema del cual forma parte.

En OT, la certificación en *safety* requiere el cumplimiento de las normas nacionales e internacionales así como también de la legislación nacional, que generalmente imponen pruebas rigurosas, normalmente confirmadas por laboratorios independientes y autorizados de *testing*.

En IT, es menos común implementar rigurosas pruebas de cumplimiento de *safety*. Sin embargo, cada vez es más común que los componentes diseñados para el mercado de consumo se apliquen a fines industriales, pero su resiliencia puede no estar a la altura de los estándares industriales.

Además, la vida útil de los productos para los mercados de consumo suele ser mucho más corta de lo que se requiere en el uso industrial. En cualquier caso, alguna deficiencia en la confiabilidad del elemento de IT puede tener un efecto negativo inaceptable en el proceso de OT.

Los constructores de sistemas tienen desafíos similares a los que afrontan los constructores de componentes. Tienen que asegurar que su sistema cumple con las expectativas durante toda su vida útil. Un constructor de sistemas debe ser capaz de ofrecer funcionalidad a lo largo de la vida útil esperada del sistema. Esto incluye no sólo la sustitución de componentes fallidos, sino también custodiar y mantener el conocimiento sobre el sistema construido durante toda esta vida útil.

Todas las capacidades del sistema IIoT finalmente se entregan al propietario/dueño y toda la confianza en el sistema comienza en él. El propietario/operador del sistema conlleva el riesgo del proceso operativo. Cualquier fallo en la confiabilidad del sistema, debido a la mala seguridad, *safety*, fiabilidad, resiliencia o privacidad, afectará directamente al negocio del propietario/operador.

El fracaso en estas garantías puede amenazar la existencia de un propietario/operador. La historia muestra que la mayor parte del daño, la pérdida de ingresos, los pagos por litigios y la responsabilidad por lesiones graves o muerte fueron asignados al propietario/operador porque su confianza en la entrega era demasiado alta y los requisitos no estaban suficientemente especificados para responsabilizar al proveedor.

3.5.6. Puntos de Vista Funcional y de Implementación

En la Sección 2.6 del Apéndice 2 se describen los 6 bloques funcionales que, de acuerdo al IISF, conforman el Punto de Vista Funcional desde la óptica de la seguridad; ellos son:

- Protección del *Endpoint*
- Protección de las Comunicaciones y de la Conectividad
- Monitorizado y Análisis de la Seguridad
- Gestión y Configuración de la Seguridad
- Protección de los Datos
- Modelo y Política de Seguridad

Luego, en la misma sección, se menciona cómo se vinculan los Puntos de Vista Funcional y de Implementación desde la óptica de la seguridad.

3.6. *IoT Security Maturity Model*

El IIC, ahora con la incorporación del OpenFog Consortium [**369**], elaboró y publicó el documento denominado *IoT Security Maturity Model: Practitioner´s Guide* [113], segundo documento vinculado al modelo de madurez en seguridad en el que viene trabajando el consorcio. El documento referido tiene como objetivos proveer detalles del modelo y describir cómo utilizarlo. Poco menos de un año antes, había publicado el primer documento referido a la temática, denominado *IoT Security Maturity Model: Description and Intended Use* [121], con el objetivo que las partes interesadas pudieran entender el propósito, la necesidad y la intención del modelo en cuestión.

3.6.1. *IoT Security Maturity Model: Description and Intended Use*

A continuación se mencionan los aspectos más relevantes contemplados en este documento, el último de los referidos en el párrafo anterior.

Consideraciones generales

El IIC afirma que el objetivo del Modelo de Madurez en Seguridad (SMM, por su sigla en inglés) es brindar a los proveedores de IoT la información necesaria para identificar en qué situación se encuentran en lo que refiere a la seguridad, y poder llegar a determinar cuánto deben invertir en mecanismos de seguridad, y en cuáles.

El modelo proporciona un marco de trabajo conceptual que ayuda a organizar la miríada de consideraciones disponibles respecto a los controles de seguridad que se deberían/podrían implementar para gestionar adecuadamente los riesgos y las amenazas. El marco de trabajo definido permite a la organización identificar, por un lado, el estado de seguridad actual y por otro, el estado de seguridad objetivo, lo que permite identificar el *gap* existente y comenzar a definir cómo recorrer el camino entre el estado actual y estado objetivo.

Dos conceptos fundamentales son utilizados a lo largo del documento: Madurez en Seguridad (*Security Maturity*) y Nivel de Seguridad (*Security Level*).

El primero de los conceptos, la Madurez en Seguridad, es el grado de confianza en que el estado de seguridad actual cumple con todas las necesidades organizacionales y los requerimientos relacionados con la seguridad. La ma-

durez en seguridad es una medida del entendimiento del estado de seguridad actual, su necesidad, y los costos y beneficios asociados.

El segundo de los conceptos, el Nivel de Seguridad, es una medida de la confianza en que las vulnerabilidades del sistema están siendo adecuadamente consideradas y que el sistema funciona de acuerdo a como se pretende.

Para ambos conceptos, y para una adecuada aplicación del modelo, ciertas flexibilidades son posibles, con ser aquellas que contemplan por ejemplo, la vertical de la industria en consideración, los requerimientos regulatorios implicados, los riesgos específicos en determinados ambientes, todo lo que se podría resumir en que cada organización es única (junto a su contexto) y que por lo tanto, los resultados de aplicar el modelo en dos organizaciones similares, no tienen porqué ser los mismos.

Por lo antes expresado, la adecuada utilización de este modelo debería permitir responder, al menos, tres preguntas fundamentales, considerando los requerimientos de la organización y el panorama de amenazas:

- ¿Cuál es el nivel de madurez objetivo para mi solución?
- ¿Cuál es el nivel actual de madurez?
- ¿Cuáles son los mecanismos y procesos que deben incorporar mi solución para ir del estado actual al estado objetivo?

Uso previsto del modelo

A continuación se describe el proceso que se espera que recorran la organizaciones que pretendan seguir el modelo SMM.

Se identifican dos grandes grupos de partes involucradas: las relacionadas con el área del negocio y las vinculadas con el área técnica; ambas deben trabajar de manera coordinada y colaborativa, de acuerdo al proceso reflejado en la Figura 3.11.

Las partes interesadas del área del negocio definen los objetivos en cuanto a seguridad, para la organización y para sus sistemas.

Las partes interesadas del área técnica vinculan los objetivos de seguridad definidas en el área del negocio con técnicas y capacidades tangibles, identificando el estado objetivo de madurez en seguridad, lo que facilita la generación de perfiles de seguridad. Estos perfiles de seguridad pueden ser utilizados como *templates* para evaluar la madurez en seguridad en un área de uso específica o en un sistema concreto.

Luego de tener el objetivo identificado, se debería realizar una evaluación para identificar el estado actual de madurez, reconocer el *gap* entre ellos, y poder así establecer una hoja de ruta para recorrerlo, lo que implica implementar las mejoras explicitadas en la hoja de ruta a recorrer para eliminar el *gap* identificado.

Una vez que las mejoras han sido implementadas, se debería realizar otra evaluación, con el objetivo de confirmar que el nivel alcanzado se mantiene, ante un panorama de amenazas siempre cambiante.

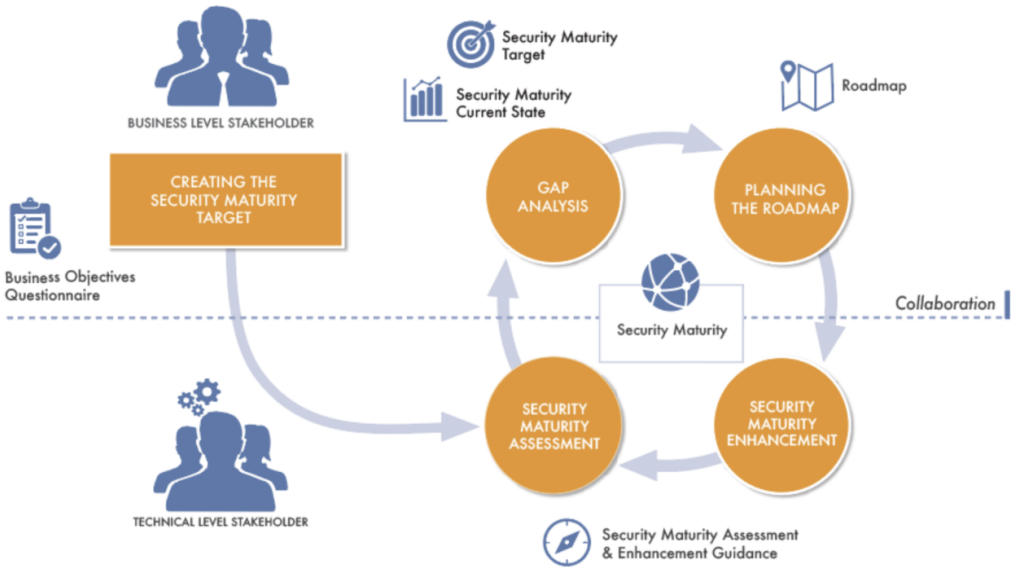


Figura 3.11: Proceso del Modelo de Madurez en Seguridad. Fuente: [121]

Un estado de seguridad persistente del sistema maduro sólo se puede lograr a través de continuas evaluaciones y mejoras de seguridad, orquestadas en el tiempo. Por lo tanto, el modelo de madurez se basa en el *Ciclo de Deming*, o ciclo *Planificar-Hacer-Verificar-Actuar* (PDCA, por su sigle en inglés), donde Actuar en este caso significa aceptar una nueva línea de base si la comprobación del resultado del paso de mejora es exitosa. Este ciclo comienza estableciendo el objetivo para la madurez en seguridad para un sistema específico. A partir de allí se inicia un proceso iterativo de alto nivel de mejora de la madurez en seguridad, como se representa en la Figura 3.12. A medida que cambian las amenazas y los enfoques de seguridad para mitigarlos, las organizaciones deben determinar con qué frecuencia se debe ejecutar el referido ciclo.

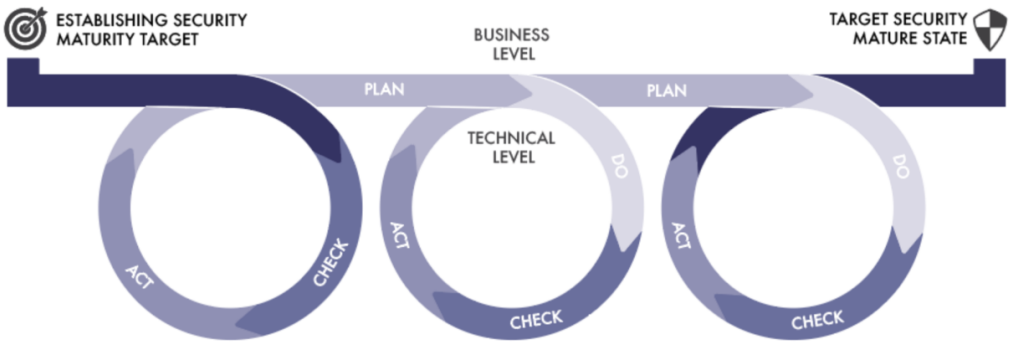


Figura 3.12: Ciclo de Mejora del Modelo de Madurez en Seguridad. Fuente: [121]

Objetivos del SMM

A continuación de enumeran los principales objetivos del SMM:

- Fomentar la colaboración eficiente y productiva entre las partes interesadas
- Identificar los indicadores de rendimiento de la seguridad
- Guiar el proceso para alcanzar el estado de madurez deseado

Requerimientos para el SMM

Los desarrolladores del SMM fueron guiados por los siguientes requerimientos:

- Aplicable en el mundo real
- Consideración de diferentes perspectivas
- Orientación de seguridad apropiada
- Adaptable a un entorno de amenazas cambiante
- Extensible y flexible

El Modelo SMM

Jerarquía de prácticas de madurez en seguridad

El SMM establece un modelo jerárquico para la Madurez en Seguridad de tres niveles: Dimensiones (nivel estratégico), Dominios (nivel de planificación) y Prácticas (nivel táctico), según se puede observar en la Figura 3.13.

Las Dimensiones buscan capturar los aspectos claves de la madurez en seguridad: Gobernanza, Establecimiento y Fortalecimiento. Cada Dimensión

contempla aspectos claves acá denominados Dominios. Finalmente, cada Dominio se compone de un conjunto de Prácticas, técnicas y organizacionales, para lograr los resultados esperados.

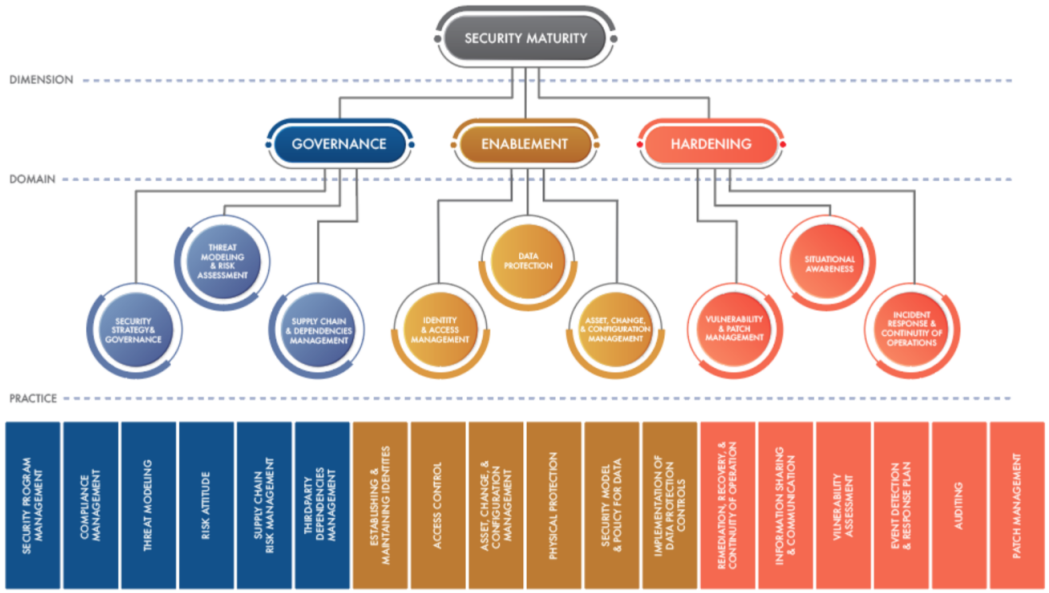


Figura 3.13: Jerarquía del Modelo de Madurez en Seguridad. Fuente: [121]

Aplicando el modelo SMM

Exhaustividad y Alcance

Dos aspectos son considerados fundamentales para por un lado determinar el progreso en la maduración de los sistemas IoT y por otro, para priorizar las prácticas de seguridad asociadas: la Exhaustividad del proceso y el Alcance de los mecanismos de seguridad utilizados.

La Exhaustividad captura el grado de profundidad, consistencia y precisión de las medidas de seguridad que sustentan las Prácticas, Dominios y Dimensiones del SMM.

El Alcance refleja el grado de ajuste a las necesidades o restricciones específicas del sistema o de la industria en cuestión. Representa el grado de "customización" de las medidas de seguridad que sustentan las Prácticas, Dominios y Dimensiones del SMM.

Puntuación y Priorización

El realizar puntuación y priorización permite evaluar el estado de madurez y establecer estrategias de seguridad basadas en métricas.

Niveles de Exhaustividad (*Comprehensiveness*)

El SMM define cinco niveles de Exhaustividad aplicables tanto a las Dimensiones, a los Dominios como a las Prácticas. Un valor más alto significa una mayor nivel de Exhaustividad en los controles de seguridad. Cada nivel incluye los requerimientos del nivel anterior. Los cinco niveles son:

- Nivel 0: Ausencia. No hay un entendimiento uniforme de cómo son aplicadas las Prácticas de seguridad y no hay requerimientos implementados. [1].
- Nivel 1: Mínimo. Están implementados los requerimientos mínimos de la Práctica de seguridad, sin actividades que permitan garantizar que se está realizando de manera adecuada
- Nivel 2: *Ad Hoc*. Los requisitos para la Práctica abarcan los principales casos de uso y los incidentes de seguridad más conocidos en entornos similares. Las medidas de garantía apoyan las revisiones *ad hoc* de la aplicación de la práctica para garantizar la mitigación de la línea de base para los riesgos conocidos
- Nivel 3: Consistente. Los requisitos consideran las mejores prácticas, estándares, regulaciones, clasificaciones, software y otras herramientas. El uso de estas herramientas ayuda a establecer un enfoque coherente para practicar la implementación. La garantía valida la implementación con patrones de seguridad, diseños *secure-by-default* y, enfoques y mecanismos de protección conocidos
- Nivel 4: Formalizado. Un proceso bien establecido constituye la base para la implementación de las Prácticas, proporcionando soporte continuo y mejoras de seguridad. La garantía de la aplicación se centra en la cobertura de las necesidades de seguridad y el abordaje oportuno de cuestiones que parecen amenazar el sistema de interés. Para esta garantía, se aplica un enfoque más complejo que utiliza métodos semiformales o formales

[1] Este nivel se presenta con el objetivo de dar completitud al trabajo, pero no será utilizado de aquí en adelante.

Niveles de Alcance (*Scope*)

El SMM define tres niveles de Alcance para cada aspecto de seguridad, donde un nivel mayor significa un alcance más específico.

- Nivel 1: General. Este es el alcance más amplio. La práctica de seguridad se implementa en los sistemas y redes informáticas sin ninguna evaluación de su pertinencia para el sector específico de la IoT, los equipos utilizados, el software o los procesos que deben mantenerse. Las capacidades y técnicas de seguridad se aplican como en el entorno típico
- Nivel 2: Específico de la Industria. La práctica de seguridad se implementa teniendo en cuenta cuestiones específicas del sector industrial en consideración, particularmente las relativas a los componentes y procesos que son propensos a ciertos tipos de ataques, vulnerabilidades conocidas e incidentes que tuvieron lugar en dicho contexto
- Nivel 3: Específico del Sistema. La implementación de la práctica de seguridad está alineada con las necesidades organizativas específicas y los riesgos del sistema considerado, los límites de confianza identificados, los componentes, las tecnologías, los procesos y los escenarios de uso

De esta forma se puede reflejar, para cada Práctica, el estado respecto tanto a la Exhaustividad como en relación al Alcance, pudiéndose observar un ejemplo de ello en la Figura 3.14.

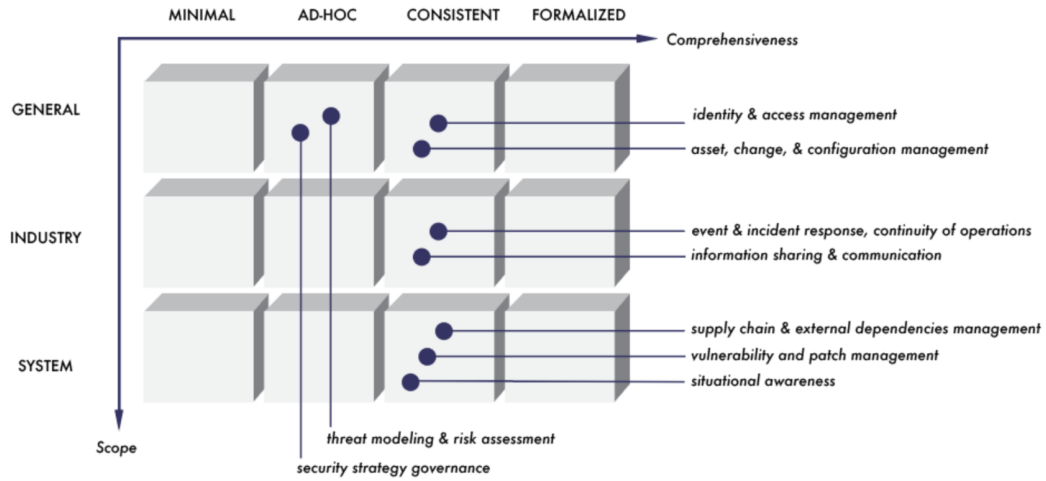


Figura 3.14: Ejemplo en dos dimensiones (Exhaustividad y Alcance) para algunas Prácticas del SMM. Fuente: [121]

Template para el SMM

No todos los sistemas, redes y dispositivos IoT requieren el máximo nivel ni en Exhaustividad ni en Alcance para todas las Dimensiones, Dominios y Prácticas, como se ejemplifica en la Figura 3.14.

El nivel de madurez objetivo del sistema en consideración queda determinado por el conjunto de todos los valores deseables de Exhaustividad y Alcance para cada Dimensión, Dominio y Práctica.

En caso de no disponer de la información suficiente para determinar los valores de Exhaustividad y Alcance para cada Práctica, se recomienda ir identificando valores para ellas de lo general a lo particular (de las Dimensiones a las Prácticas) a medida que las partes interesadas van ganando conocimiento del sistema de interés.

Como se puede apreciar en la Figura 3.15 el SMM ofrece un *template* en formato de tabla, donde se documenta para cada Práctica, para cada nivel de Exhaustividad y para cada nivel de Alcance, las consideraciones que se deberían cumplir en cada caso.

	<Practice Name>			
	Comprehensiveness Level 1	***Comprehensiveness Level 2***	***Comprehensiveness Level 3***	***Comprehensiveness Level 4***
Objective	<Objective Level 1>	<Objective Level 2>	<Objective Level 3>	<Objective Level 4>
General considerations	<List of Level 1 general considerations>	<List of Level 2 general considerations>	<List of Level 3 general considerations>	<List of Level 4 general considerations>
Sector-specific considerations	<List of sector considerations>			
System-specific considerations	<List of system considerations>			

Figura 3.15: *Template* para las Prácticas del SMM. Fuente: [121]

El documento *IoT Security Maturity Model: Description and Intended Use* ofrece un ejemplo que se muestra en las Figuras 3.16 y 3.17, para la Práctica "Modelado de Amenazas" en el sector industrial de equipamiento médico y para un sistema específico: un equipo portátil que recolecta información (signos vitales) de un paciente y la envía a un sistema ubicado en un hospital, datos que luego son compartidos utilizando la red del nosocomio.

Objetivo de madurez en seguridad y perfiles

El objetivo de madurez en seguridad es un documento donde se fijan los objetivos que establece el estado de madurez final para un sistema IoT. Dicho

	Practice: Threat Modeling of Medical Devices including a handheld that collects patient telemetry and a base station aggregates patient vitals and shares data across a hospital network.			
	Comprehensiveness Level 1	***Comprehensiveness Level 2***	***Comprehensiveness Level 3***	***Comprehensiveness Level 4***
Objective	Address general threats without regard for appropriateness	Perform vulnerability analysis to identify threats. Address in an ad-hoc manner	Describe and classify threats in an accurate (optionally formal) way	Reveal and clearly describe IT factors both known and specific that may put the system at risk
General considerations	- General security threats, e.g. sensitive data disclosure, DoS attacks, or infiltration with malware, are mentioned by business level documents	- Vulnerability assessment is performed for IT components. - Generally accepted vulnerability evaluation schemes (e.g., CVSS) are used.	- Security threats are classified according to the possibly vulnerable technology, exploitation method or attack pattern. - Generally accepted classifications like CAPEC or OWASP Top10 are used during threat analysis	- The security threats are validated against objectives set according to business needs. - The threat model is based upon the set of clearly identified security assumptions about system environment (including physical security), trustworthiness constraints and key actor's behavior. - The particular threats and attack vectors comprise the consistent hierarchical structure, including all identified security issues

Figura 3.16: *Template* para las Prácticas del SMM. Fuente: [121]

Industry-Specific Considerations	- Level 3 and higher: Note: FDA guidance can be interpreted to require that a medical device manufacturer reach or exceed a level 3 comprehensiveness in threat modeling as part of a pre-market submission. - The threat model takes into account FDA guidance for post-market management of cybersecurity in medical devices FDA requirements for pre-market submissions related to cybersecurity: *https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf* FDA post-market guidance on managing cybersecurity in medical devices: *https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf* - Level 4: threat model includes not only the device in isolation, but the medical environments in which the device will operate. - Level 4: threat model includes scenarios in which the device could allow its users to violate HIPAA standards (such as by leaking PII), and seeks to mitigate those opportunities.
Handheld Specific Considerations	- The handheld collects only anonymized patient telemetry data. Its exposed attack surfaces are Bluetooth LE, USB, and physical access.
Base station Specific Considerations	- The base station aggregates patient telemetry with PII, making the data it stores and transmits HIPAA relevant. Its exposed attack surfaces include Bluetooth LE, USB, Wi-Fi, Ethernet, and physical access.

Figura 3.17: *Template* para las Prácticas del SMM. Fuente: [121]

objetivo incluye un conjunto consistente de prácticas de seguridad, proveyendo una vista exhaustiva de seguridad para todas las partes interesadas. Dicha vista es un conjunto de objetivos y necesidades generales de seguridad y el propósito de cada práctica de seguridad.

En *IoT Security Maturity Model: Description and Intended Use* se proponen los siguientes pasos para establecer el objetivo y fijar las prioridades:

- *Establecer el objetivo* considerando el foco de cada Dimensión; a partir de allí se pueden establecer los niveles de Exhaustividad y Alcance para cada una de ellas. En este paso, los Dominios y las Prácticas heredan los niveles de su Dimensión. Esta es la primera visión del estado madurez objetivo, muy genérico por cierto
- *Considerar las necesidades* que son cubiertas en cada Dimensión de acuerdo al nivel de madurez de cada dimensión. A partir de lo anterior, las partes interesadas podrán determinar con mayor precisión los niveles de Exhaustividad y Alcance que cubren sus necesidades específicas, más allá de la línea base establecida
- *Clarificar el propósito* de cada Práctica de seguridad. Las priorizaciones a nivel de Dominio enfatizan las necesidades específicas de seguridad y las consideraciones de cada Práctica de seguridad clarifica cómo contribuye a cubrir esas necesidades. Disponer de los niveles de Exhaustividad y Alcance de cada Práctica de seguridad provee un mayor grado de detalle del nivel de madurez en seguridad objetivo y qué es necesario para lograr su cumplimiento

Una vez que el objetivo de madurez de seguridad está disponible, se puede utilizar en aplicaciones posteriores del SMM, para crear un perfil de destino o realizar una evaluación de estado de madurez actual.

Estado de madurez en seguridad actual

Se trata de un documento (con un formato similar al del objetivo de madurez en seguridad) que describe el nivel actual de madurez de las Prácticas implementadas para el sistema en cuestión. Su creación depende de la realización previa de una evaluación de seguridad y disponer de ambos documentos permite identificar los *gaps* entre uno y otro. El estado de madurez en seguridad actual es la descripción del estado de madurez en seguridad para el tipo específico de dispositivo, organización o sistema.

Análisis de *gap*

A partir de los documentos de estado de madurez en seguridad actual y estado de madurez en seguridad objetivo, se identifican los *gaps* entre ellos (en

Exhaustividad y en Alcance) y por lo tanto, las oportunidades de mejora. Las partes interesadas, tanto del negocio como técnicas, de manera conjunta y coordinada, deben establecer una hoja de ruta a recorrer para implantar las mejoras identificadas, y cómo medir el avance.

Diversas alternativas de visualización se proponen para apreciar el *gap* en cada Práctica de seguridad: mapa de calor, gráfico de barras o diagrama radar.

3.6.2. *IoT Security Maturity Model: Practitioner´s Guide*

A continuación se mencionan los aspectos más relevantes explicitados en el documento.

El Modelo de Madurez en Seguridad

Las organizaciones tienen diferentes necesidades y los diferentes sistemas necesitan diferentes fortalezas en los mecanismos de protección a considerar, donde la misma tecnología puede aplicarse con diferentes configuraciones y "sabores" para cubrir diferentes necesidades.

El modelo fomenta una colaboración eficaz y productiva entre las partes interesadas, tanto empresariales como técnicas. Los responsables de la toma de decisiones empresariales, los gestores de riesgos empresariales y los propietarios de sistemas de IoT, preocupados por una estrategia adecuada para implementar prácticas de seguridad maduras, pueden colaborar con los analistas, arquitectos, desarrolladores, integradores de sistemas y otras partes interesadas que son responsables de la implementación técnica.

Para impulsar una inversión adecuada, el SMM incluye componentes organizativos y tecnológicos. Las organizaciones usan el modelo para establecer su madurez de destino, comprender su madurez actual y determinar lo que deben hacer para pasar a un estado de madurez más alto.

Madurez en Seguridad vs. Seguridad

La madurez se trata de la eficacia, no del uso arbitrario de mecanismos. El SMM alinea la Exhaustividad (grado de profundidad, coherencia y garantía de las medidas de seguridad) y el Alcance (grado de ajuste a las necesidades de la industria o del sistema) de las necesidades de seguridad, con la inversión en las Prácticas apropiadas.

No todos los sistemas requieren la misma fuerza en los mecanismos o procedimientos de protección para cumplir con sus requisitos de seguridad. Las implementaciones de los mecanismos y procesos de seguridad se consideran maduras si se espera que sean eficaces para abordar los objetivos de la organización.

Dominios, Subdominios y Prácticas

En este documento se proponen algunos cambios en la terminología respecto a la utilizada en el documento *IoT Security Maturity Model: Description and Intended Use*, según se aprecia en la Figura 3.18 y que se mencionan a continuación:

- Las Dimensiones pasaron a denominarse Dominios
- Los Dominios pasaron a denominarse Subdominios
- El Subdominio "Estrategia y Gobernanza en Seguridad" pasó a llamarse "Estrategia y Gobernanza"
- El Subdominio "Gestión de Cambios y Configuración de los Activos" pasó a llamarse "Protección de los Activos"
- El Subdominio "Conciencia Situacional" pasó a llamarse "Conciencia de la Situación"
- El Subdominio "Respuesta a Incidentes y Continuidad de las Operaciones" pasó a llamarse "Respuesta a Eventos e Incidentes, Continuidad de las Operaciones"
- La Práctica "Gestión de Riesgos en la Cadena de Suministros del Producto" pasó a llamarse "Gestión de Riesgos en la Cadena de Suministros"
- La Práctica "Gestión de Dependencias de Terceras Partes" pasó a llamarse "Gestión de Dependencias de Servicios de Terceras Partes"
- La Práctica "Política y Modelo de Seguridad para Datos" pasó a llamarse "Política y Modelo de Protección para Datos"
- La Práctica "Auditado" pasó a llamarse "Práctica de Monitorizado"
- La Práctica "Comunicación e Intercambio de Información" pasó a llamarse "Conciencia de la Situación e Intercambio de Información"
- Se reorganizó la estructura jerárquica del SMM: las Prácticas se agruparon, vinculando ahora dos Prácticas con cada Subdominio

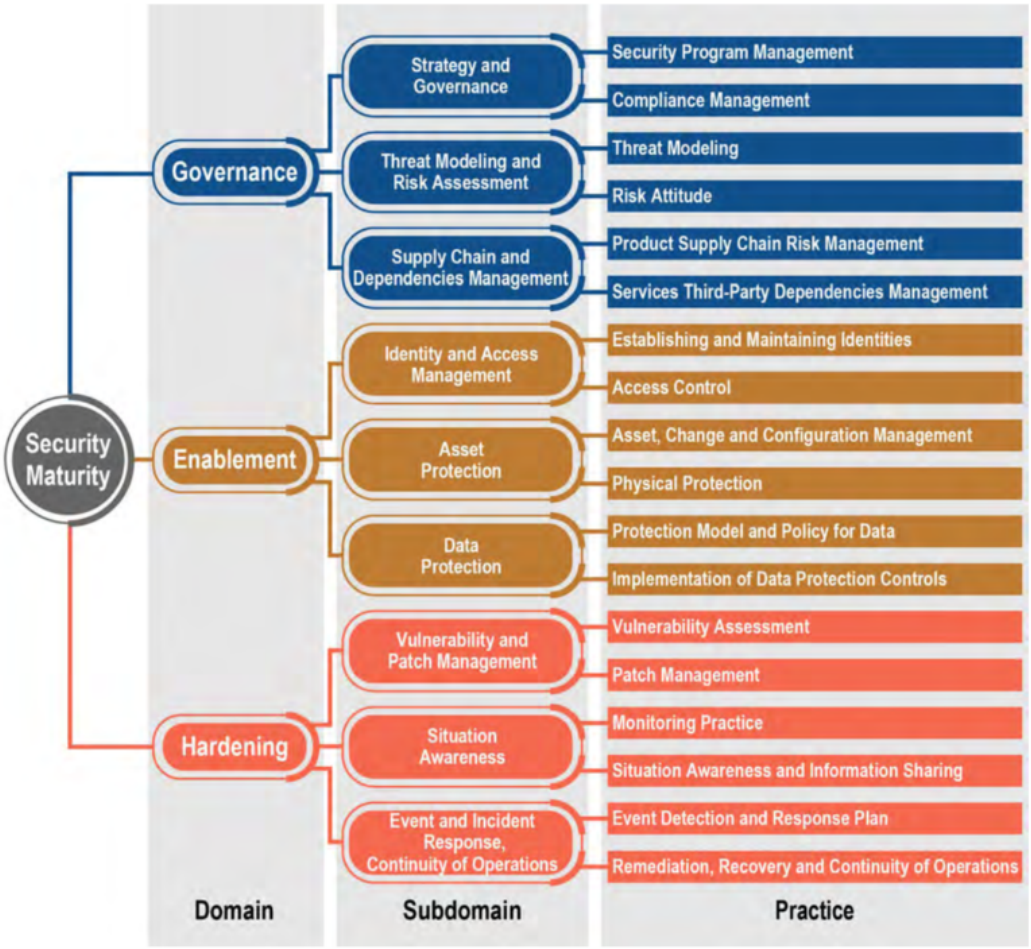


Figura 3.18: Jerarquía del Modelo de Madurez en Seguridad. Fuente: [113]

Template para el SMM

El *template* anterior o sea, el presentado en el documento *IoT Security Maturity Model: Description and Intended Use*, fue ligeramente modificado para contemplar:

Descripción de la práctica

Se explicita además que las características son lo que hay que hacer para alcanzar ese nivel y un campo para los indicadores del logro (ver Figura 3.19).

Extensibilidad

El modelo se puede extender tanto en el alcance de cada práctica (a la industria o al sistema) así como también con la adición de nuevos Subdominios y Prácticas (ver Figuras 3.20 y 3.21).

<Practice-Name>				
<Practice Description>				
	Comprehensiveness Level 1	**Comprehensiveness Level 2**	**Comprehensiveness Level 3**	**Comprehensiveness Level 4**
Objective	Objective Description	Objective Description	Objective Description	Objective Description
General considerations	Level Description	Level Description	Level Description	Level Description
	What needs to be done to achieve this level Considerations	**What needs to be done to achieve this level** Considerations	**What needs to be done to achieve this level** Considerations	**What needs to be done to achieve this level** Considerations
	Indicators of accomplishment Considerations	**Indicators of accomplishment** Considerations	**Indicators of accomplishment** Considerations	**Indicators of accomplishment** Considerations

Figura 3.19: Tabla *template* para el Modelo de Madurez en Seguridad. Fuente: [113]

<Practice-Name>				
<Practice Description>				
	Comprehensiveness Level 1	**Comprehensiveness Level 2**	**Comprehensiveness Level 3**	**Comprehensiveness Level 4**
Objective	<Objective Level 1>	<Objective Level 2>	<Objective Level 3>	<Objective Level 4>
General considerations	<List of Level 1 general considerations>	<List of Level 2 general considerations>	<List of Level 3 general considerations>	<List of Level 4 general considerations>
Industry-specific considerations	<List of industry specific considerations>			
System-specific considerations	<List of system specific considerations>			

Figura 3.20: Tabla *template* para el SMM incluyendo consideraciones específicas de la industria y el sistema. Fuente: [113]

Proceso para Aplicar el Modelo

Respecto al documento anterior (*IoT Security Maturity Model: Description and Intended Use*), en éste se incorpora la consideración del contexto de aplicación, previo a crear el objetivo de madurez o a realizar una evaluación de la madurez. Para ello, es necesario identificar si la evaluación se está realizando, por ejemplo, a una sistema completo, a un subsistema o a un dispositivo, y además si la organización involucrada es un proveedor de servicios, un contratista, o un cliente, lo que puede determinar que algunas prácticas se deban considerar como "no aplicable".

Creando el Objetivo de Madurez en Seguridad

El objetivo de madurez de seguridad se define cuando se hace referencia a la

<Practice-Name>				
<Practice Description>				
	Comprehensiveness Level 1	**Comprehensiveness Level 2**	**Comprehensiveness Level 3**	**Comprehensiveness Level 4**
Objective	<Objective Level 1>	<Objective Level 2>	<Objective Level 3>	<Objective Level 4>
General considerations	<List of Level 1 general considerations>	<List of Level 2 general considerations>	<List of Level 3 general considerations>	<List of Level 4 general considerations>
Industry-specific considerations	Industry-specific security needs (e.g., facilitating safety, keeping continuous execution etc.) Accepted and recommended approaches to the practice implementation Known constraints What needs to be done to achieve the specific level and the indicators for accomplishment for that level			
System-specific considerations	System description and connected industries System-specific security needs (e.g., facilitating safety, keeping continuous execution etc.) Recommended approaches to the practice implementation Known constraints What needs to be done to achieve the specific level and the indicators of accomplishments for that level			

Figura 3.21: Tabla *template* para el SMM incluyendo descripción e indicadores específicos de la industria y el sistema. Fuente: [113]

exhaustividad y el alcance de las prácticas de madurez de seguridad, pudiendo utilizar para ello el *template* en formato tabla antes referido.

Para crear el objetivo de madurez en seguridad se deben considerar tres pasos: determinar los niveles de Exhaustividad, determinar el Alcance y chequear la consistencia.

A los efectos de determinar los niveles de Exhaustividad, es necesario establecer un objetivo para cada uno de los Dominios, de manera consistente con el nivel de madurez que se desea alcanzar.

En lo que refiere al Alcance, es necesario considerar si existen requerimientos particulares en la industria en cuestión, que deban tenerse en cuenta como complemento a las consideraciones generales de cada Dominio, Subdominio y Práctica.

Finalmente, el chequeo de la consistencia implica que los valores impuestos para la Exhaustividad y el Alcance, para los Dominios, Subdominios y Prácticas directamente relacionadas no entren en contradicción entre sí, lo que ocurriría si por ejemplo el nivel de Exhaustividad de una Práctica fuera menor a la de su Subdominio superior.

El *Core* del SMM

Guías de Objetivos, Necesidades y Propósitos en el SMM

En el documento *IoT Security Maturity Model: Practitioner´s Guide* se proporciona una guía de los objetivos típicos a cumplir en cada Dominio del SMM (Gobernanza, Establecimiento y Fortalecimiento) en cada nivel de Exhaustividad. Acompañando a dicha guía, el artículo proporciona también una guía de las necesidades para cada uno de los Subdominios y para cada nivel del Exhaustividad. En un tercer y último nivel de granularidad, se ofrece la finalidad o propósito de cada Práctica, para cada nivel de Exhaustividad (1. Mínimo, 2. *Ad Hoc*, 3. Consistente y 4. Formalizado).

En la Sección 2.7 del Apéndice 2, se brinda el detalle de cada guía, ordenando en cada caso según los cuatro Niveles de Exhaustividad, desde Mínimo hasta Formalizado.

Aspectos a considerar al analizar un sistema

Se presenta un conjunto de factores a tener en cuenta al momento de aplicar el SMM a un sistema. Luego, ello es ejemplificado mediante tres casos de uso[1]:

- Una línea de embotellado inteligente basada en datos
- Un *gateway* automotriz que soporta actualizaciones *Over The Air* (OTA)
- Cámaras de seguridad residenciales

Los factores que los autores recomiendan considerar en el análisis de un sistema (nuevo o ya existente) son:

- Tamaño y cobertura
- Exposición
- Escenario de Amenazas
- Mejores Prácticas
- Experiencia

[1]Habiéndose identificado algunos errores algunos de los casos de uso, en lo que refiere al procedimiento a seguir al momento de aplicar el SMM, se entabló contacto con el equipo de trabajo vinculado a la elaboración del documento; uno de sus integrantes confirmó la existencia de los mismos y que se está trabajando en la elaboración de una versión corregida y mejorada del mismo; ésto, a juicio del autor, es una muestra clara de que la temática abordada en el presente trabajo está plena fase de maduración.

- Urgencia
- Impacto de Amenazas
- Restricciones
- Confianza
- Línea de tiempo
- Resultados esperados
- Dependencias

Una vez que se dispone de una descripción, clara y documentada, de todos los supuestos, objetivos y requisitos del sistema, se deberían priorizar los Dominios en base al nivel de Exhaustividad y al Alcance.

Finalmente, se deberían validar las necesidades de los Subdominios y los propósitos de las Prácticas, siendo la recomendación realizarse las siguientes preguntas, para cada uno de los Subdominios y para cada una de las Prácticas:

¿Cómo se pueden describir las necesidades de *Nombre_del_Subdominio*?

¿Cuál es el propósito de la *Nombre_de_la_Práctica*?

Luego que los estados *actual* y *objetivo* están definidos, la siguiente fase del proceso es que la organización identifique aquellas Prácticas que están por debajo del objetivo. Para ellas, la organización debería definir las acciones adicionales para que la Práctica llegue al estado objetivo. Además la organización deberá priorizar las acciones, contemplando un conjunto de consideraciones, como ser los costos asociados a: tiempo, recursos, económicos y financieros, cambios organizacionales e involucramiento de partes interesadas; la anterior no debe considerarse una enumeración taxativa. Con ello, la organización estará en condiciones de establecer una hoja de ruta que lleve el SMM al estado objetivo en las condiciones definidas.

3.6.3. *Extending the IIC IoT Security Maturity Model to Trustworthiness*

En el artículo *Extending the IIC IoT Security Maturity Model to Trustworthiness* [107], de la edición de septiembre de 2018 de la publicación *Journal of Innovation* del IIC, los autores mencionan que el SMM cubre solamente cuestiones de seguridad, y sugieren cómo puede ser extendido el modelo para considerar todos los aspectos de la confiabilidad. Con ello se pretende habilitar a las organizaciones a que utilicen el modelo extendido a los efectos de evaluar

su posición respecto a las diferentes características de la confiabilidad, o sea, *safety*, seguridad, fiabilidad, resiliencia y privacidad, y así poder determinar qué pasos dar y qué acciones tomar para mejorar en ellos, pudiendo determinar dónde invertir, en qué momento y a su vez analizar posibles impactos positivos y negativos de ellos entre sí, analizando de manera conjunta todas las características.

Para ello, en el artículo en cuestión se proponen algunas incorporaciones y algunos cambios al SMM Jerárquico original, de acuerdo a lo reflejado en la Figura 3.22, los que se mencionan a continuación[1]:

Se propone incorporar un cuarto Dominio, denominado *Institutional*, compuesto por tres Subdominios, a saber:

- *Culture*
- *Training*
- *Continuous Improvement and Learning*

Adicionalmente, se propone también agregar los siguientes Subdominios:

- *Performance Measurement and Metrics*, al Dominio *Governance*
- *Analysis and Design*, al Dominio *Enablement*
- *Verification and Validation*, al Dominio *Hardening*

Para ninguno de los nuevos Subdominios el artículo formaliza Prácticas asociadas.

Por otro lado, en el artículo se plantean cambios en los nombres de 2 Prácticas; ellos son:

- *Program Management* en lugar de *Security Program Management*
- *Supply Chain Management* en lugar de *Product Supply Chain Risk Management*

Dichos cambios son propuestos a manera de ejemplo de la dinámica de mejora que está presente en el SMM y a la vez, pretende mostrar que se podría proceder con el mismo espíritu con algunos de los otros nombres.

[1]La figura de referencia, extraída del artículo en consideración, no refleja algunos de los nuevos Subdominios propuestos. Por otro lado, los autores del artículo no proponen Prácticas asociadas a los nuevos Subdominios. Ésto, a juicio del autor de la tesis, es una muestra más de que la temática abordada en el presente trabajo está en fase de maduración.

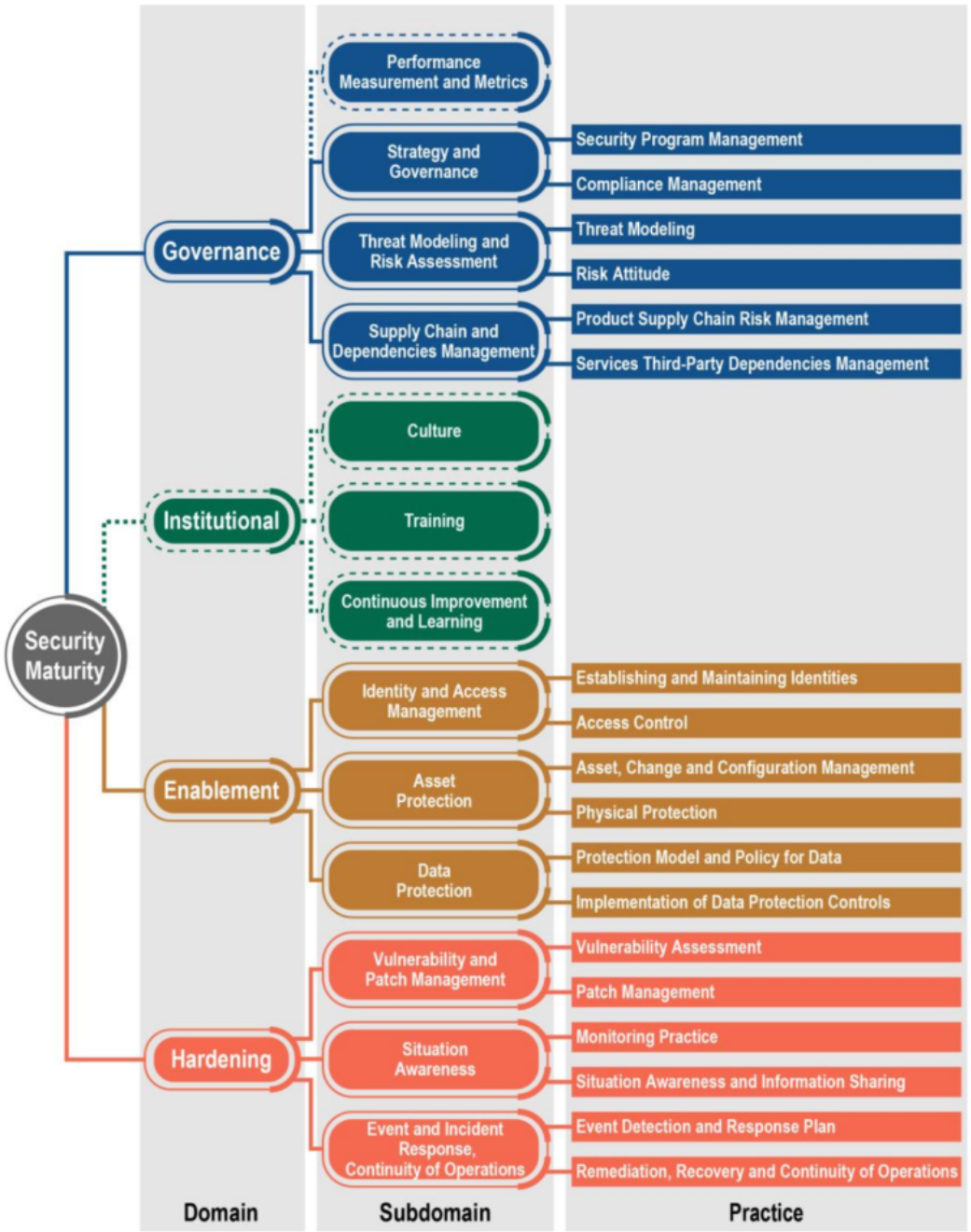


Figura 3.22: SMM revisado y extendido a la confiabilidad. Fuente: [107]

Por medio de la incorporación del dominio *Institutional*, se pretende reforzar el concepto que existen varias prácticas vinculadas a la confiabilidad que reflejan la cultura de la organización, el entrenamiento y la gestión del *staff* y, todo aquello que contribuye a mantener las mejores capacidades vinculadas a las características de la confiabilidad.

La propuesta de agregar el subdominio *Analysis and Design* pretende fortalecer la extrapolación del concepto de *privacy by design* a *trustworthiness by design* [170].

Añadiendo el Subdominio *Performance Measurement and Metrics* se busca disponer de métricas y medidas de rendimiento de las características asociadas a la confiabilidad.

Incorporar el subdominio *Verification and Validation* busca reflejar las prácticas de *safety* y fiabilidad para enmarcar, en una visión más general, las actividades de *testing*.

3.7. *Managing and Assessing Trustworthiness for IIoT in Practice*

Posteriormente el IIC publicó el documento denominado *The Industrial Internet of Things: Managing and Assessing Trustworthiness for IIoT in Practice* [120]. En esta sección se mencionarán los aspectos más relevantes abordados en el mismo vinculados a la temática de este trabajo.

Como ya se expresó anteriormente, la confiabilidad de un sistema queda definida mediante las cinco características mencionadas y descritas en la Sección 3.5.3 del presente Capítulo (*safety*, seguridad, fiabilidad, resiliencia y privacidad) e interactuando entre sí.

Debemos tener presente que, históricamente, no todas las características comenzaron a considerarse al mismo tiempo en los sistemas industriales, pudiéndose expresar que el orden de aparición, de acuerdo a lo documentado en [118] podría ser el siguiente: Fiabilidad, Resiliencia, *Safety*, Seguridad y Privacidad.

La gestión de la confiabilidad de un sistema IIoT implica entender las características referidas, definir objetivos y métricas, determinar qué evidencia es requerida para confirmar que las características están proveyendo lo que se espera para la operación del sistema, analizando las interrelaciones entre ellas y su impacto en el negocio y en las operaciones.

La rigurosidad de las evaluaciones y de las evidencias que sirvan para lograr la confianza en un sistema estarán fuertemente condicionadas por el contexto donde se encuentra y las consecuencias de las fallas del sistema.

Las consideraciones relativas a la confiabilidad deben cubrir tanto la infraestructura IT (también conocida como *office floor*), la infraestructura OT (también conocida como *shop floor*), los datos y las personas. Adicionalmente, las características tienen diferentes significados según si estamos en el contexto de IT o de OT. Por ejemplo, la fiabilidad en IT se enfoca más servicios y sistemas mientras que en OT lo hace en el equipamiento (máquinas). Esto hace que se deban considerar diferentes métricas para evaluar las características en IT y en OT.

Por otro lado, las interdependencias de las características de la confiabilidad se deben entender en dos dimensiones: entre ellas y en las realidades distintas de IT y OT.

Resulta innegable entonces la necesidad crucial del trabajo colaborativo y

continuo entre IT y OT, dado que la convergencia de información entre ambos "mundos" resulta un factor clave para el éxito de IIoT. Un ejemplo reciente de esa necesidad es un incidente de seguridad donde un *ransomware* (proveniente del "mundo" IT) afectó las operaciones de un servicio de gas natural ("mundo" OT) [280].

3.7.1. El negocio y la confiabilidad

En el contexto de la industria, existen algunos tópicos fundamentales vinculadas al negocio que tienen relación directa con la confiabilidad. Ellos son:

- Cumplimiento de Requerimientos
- Gestión de Riesgos
- Previsibilidad y Calidad del Rendimiento

El Cumplimiento de Requerimientos refiere al cumplimiento de leyes, normas y regulaciones, tanto específicas de la industria en cuestión como también gobernamentales y regionales. Ello es un requerimiento para el negocio pues impacta directamente en la venta de los productos, teniendo un valor de *marketing* relevante.

La Gestión de Riesgos es apoyada por diversos *frameworks* y guías existentes y en continua mejora y elaboración, con diferentes enfoques según el ámbito de aplicación. Una adecuada Gestión de Riesgos impactará positiva o negativamente en el negocio.

La Previsibilidad y Calidad del Rendimiento, por ejemplo en acuerdo con proveedores, permite impulsar la firma de acuerdos donde se establecen las condiciones esperadas de los servicios provistos y cómo proceder en caso de incumplimiento, como por ejemplo mediante *Service-Level Agreements* (SLAs), a través de los cuales se contempla el punto de vista de la eficiencia operacional y el cumplimiento adecuado de los objetivos de los sistemas.

Estos tres tópicos mencionados tienen relación con las características de la confiabilidad. En algunos casos la relación es (casi) directa, como puede ser entre las leyes y regulaciones y, *safety*, seguridad y privacidad. En otros casos, luego de un análisis más profundo se pueden identificar relaciones indirectas. Por otro lado, estos vínculos, y las fortalezas de los mismas, pueden ir cambiando a lo largo del tiempo.

Las fallas en el cumplimiento de los requerimientos mínimos o recomendados vinculados a la confiabilidad pueden implicar, entre otros, accidentes, daños en equipamiento, lesiones en las personas, violación de datos o información, retrasos o interrupciones en las operaciones. Ello puede implicar costos directos e indirectos (por ejemplo a través de multas, juicios, cierre de mercados, pérdida de imagen, mayores costos de seguros).

La implementación de medidas vinculadas a la confiabilidad tienen, en general, un costo directo identificable sin mayor esfuerzo; sin embargo, resulta más complejo identificar y medir el impacto de dichas medidas en las operaciones, donde 2 preguntas fundamentales no tienen respuesta inmediata: "¿qué medir?" y "¿cómo medir?" Las respuestas no son generales ni únicas y dependerán de cada sistema IIoT.

Como ya se ha comentado, es necesario comprender las interrelaciones entre las características de la confiabilidad y cómo ello se vincula con el negocio. Se debe entender entonces si una característica potencia o inhibe a otra y cuánto. Por otro lado, siempre se debe tener presente que un excesivo énfasis (más del necesario o requerido) en las características de la confiabilidad (lo que se traduce en costos), puede tener un impacto relevante en el negocio.

3.7.2. Análisis y Gestión de la Confiabilidad

Respecto al análisis y gestión de la Confiabilidad, en el documento *The Industrial Internet of Things: Managing and Assessing Trustworthiness for IIoT in Practice* se plantea la siguiente estrategia:

En primer lugar define un conjunto de conceptos que son la apoyatura para identificar, por un lado el estado actual de un sistema respecto a la confiabilidad y por otro, el estado deseado u objetivo.

Posteriormente, establece un proceso de evaluación y control de la confiabilidad, compuesto de dos fases, denominadas análisis de la confiabilidad del sistema y, evaluación y control, las que deben iterar entre sí hasta lograr el objetivo deseado.

Luego de planteada la estrategia, se presenta un caso concreto de aplicación, basado en un *testbed* implementado con el apoyo del IIC.

Finalmente, se discuten algunos aspectos que hacen a la gestión de la confiabilidad: el impacto de las diferentes decisiones tanto en el negocio como en la confiabilidad, la estrategia de abordaje para la gestión de la confiabilidad,

en lo que refiere a la estructura organizativa y funcional, la relevancia de utilizar como una herramienta de gestión más una matriz RACI (o RASCI), para finalizar con la importancia de identificar que el trabajo en confiabilidad no es un proyecto.

En la Sección 2.5 del Apéndice 2 se ahonda en todos los conceptos mencionados aquí.

Capítulo 4

Otras referencias e iniciativas vinculadas a la Industria 4.0

4.1. Introducción

Complementando el estudio del Estado del Arte al respecto de la I4.0 que se abordó en los dos primeros capítulos del presente trabajo, aquí se incursiona en otras referencias e iniciativas impulsadas por organizaciones y países, que se consideran que terminan de enriquecer y completar el cumplimiento del objetivo asociado a los 3 primeros capítulos del presente trabajo.

Este capítulo está organizado de la siguiente forma: las organizaciones consideradas son las identificadas como ENISA (*European Union Agency for Cybersecurity*) [61], NIST (*National Institute of Standards and Technology*) [190], IETF (*Internet Engineering Task Force*) [85], *Internet Society* [139] y la *IoT Security Foundation* (IoTSF) [153]. Siguiendo la secuencia mencionada, se irán explicitado sus aportes más relevantes respecto a la temática de este trabajo. Posteriormente, se explicitan las estrategias de Singapur (en el contexto de un plan nacional denominado *Smart Nation*), Japón (denominada *Society 5.0*) y China, para culminar con una mención a los planes respecto a la Industria 4.0 en diversos países, así como también la referencia a varios acuerdos existentes al respecto entre países y organizaciones con marcado interés en la Industria 4.0 y la Transformación Digital.

4.2. ENISA

Esta sección comienza brindando la definición de IoT elaborada por ENISA, para continuar con la mención y descripción de diferentes trabajos realizados por la agencia europea respecto a la seguridad en IoT. De acuerdo a su secuencia de aparición aquí, se detallan recomendaciones de seguridad para IoT tanto para el contexto de infraestructuras críticas como para *Smart Manufacturing*, para luego continuar con detalle de desafíos y recomendaciones en ciberseguridad en el ámbito de la Industria 4.0, y concluir con la mención a una herramienta disponible en línea que colabora, para algunas verticales del negocio, en la identificación de las buenas prácticas en materia de seguridad, las posibles amenazas involucradas y las referencias más relevantes identificadas, de acuerdo al análisis de ENISA reflejado en los trabajos referidos en las Secciones previas.

4.2.1. IoT

ENISA define IoT [64] como "*un ecosistema ciber-físico de sensores y actuadores interconectados, que habilita a la toma de decisiones inteligentes*".

Dicho ecosistema tiene la característica de ser pervasivo y tiende a estar presente en todos los aspectos del diario vivir, en áreas críticas y no críticas, como por ejemplo la industria, la energía, el transporte, la salud, las tiendas, el hogar y las ciudades, lo que ha impulsado la imposición de verticales de aplicación como las denominadas *Smart Homes*, *Smart Cities and Intelligent Public Transport*, *Smart grids*, *Smart Cars*, *Smart Airports*, *eHealth and Smart Hospitals*, entre otras.

4.2.2. *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*

ENISA elaboró el informe *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures* [57] con el objetivo de hacer disponibles recomendaciones de ciberseguridad de referencia para IoT con un enfoque en las infraestructuras críticas de la información, que abarcan instalaciones, redes, servicios y equipos de tecnología física y de la información.

Estas infraestructuras se consideran críticas porque su destrucción o perturbación podría tener consecuencias importantes para la salud, la seguridad y el bienestar económico de los ciudadanos, para el funcionamiento eficiente de las instituciones del Estado y las Administraciones Públicas, y para los propietarios de activos que hacen uso de la IoT para prestar sus servicios.

En este contexto, los términos *Industry 4.0* e IIoT son frecuente y legítimamente asociados a IoT focalizado en la digitalización de las industrias.

Elementos de IoT

A partir de la definición de IoT, existen un conjunto de elementos que dan forma al ecosistema referido, siendo ellos:

- Las cosas (*things*) o sea, todo objeto físico o virtual capaz de ser identificado e integrado en una red de comunicaciones
- La toma de decisiones inteligentes, con diferentes niveles de analítica y de independencia en las decisiones, lo que va de la mano en una visión global, con un incremento enorme en la cantidad de datos a manejar y analizar
- Los sensores y los actuadores; los primeros son aquellos que permiten monitorizar variables del medioambiente y del contexto donde opera el sistema IoT, operando a nivel físico o a nivel digital y generando datos que pueden ser procesados en tiempo real y/o almacenados para un procesamiento posterior, tanto local como remotamente, e incluso estando desatendidos. Los actuadores son las entidades encargadas de controlar un sistema o un mecanismo, ejecutando las decisiones que se toman a partir del análisis de los datos recolectados por los sensores. Por lo tanto, en una visión resumida, se puede afirmar que los sensores son los dispositivos de entrada, y los actuadores, los de salida
- Los sistemas embebidos IoT, según Figura 4.1, refiere a aquellos dispositivos que, además de integrar sensores y actuadores, contienen la capacidad de procesamiento de manera que la toma de decisiones se realiza localmente
- Las comunicaciones son un requerimiento que se contempla en función del propósito del sistema IoT en cuestión y de las restricciones que existan. Existe una plétora de protocolos disponibles, fundamentalmente para re-

des inalámbricas, cada uno con sus capacidades en cuanto a *performance*, QoS, resiliencia, seguridad y gestión. Es común encontrar en diferentes despliegues de sistemas IoT varios protocolos de comunicación intentando convivir

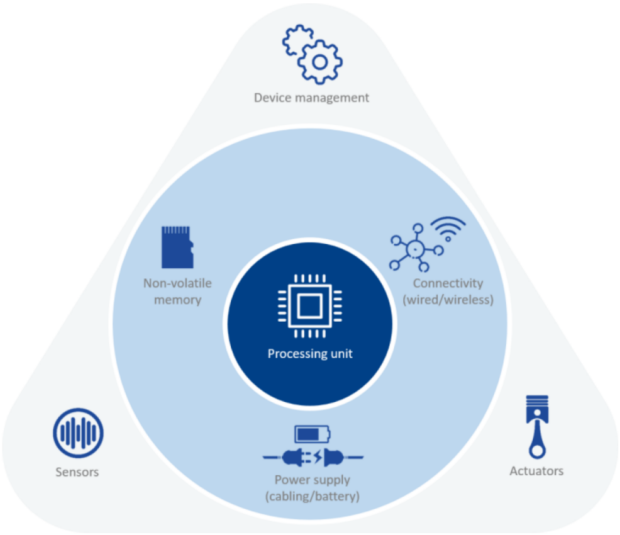


Figura 4.1: Sistema Embebido IoT. Fuente: [57]

Es importante destacar que el uso de la palabra Internet en *Internet of Things* no implica que la comunicación entre las *Cosas* se deba dar a través de dicha red. Con dicha palabra se intenta transmitir la idea de conectividad en general.

Consideraciones de Seguridad

Debido al aumento continuo de la cantidad de dispositivos IoT presentes, rodeándonos, siendo parte de cada día de nuestra vida, en diferentes ámbitos y cada vez de manera más natural, sumado a su capacidad de toma de decisiones, uno de los aspectos fundamentales a considerar es la seguridad de los mismos, ya que de verse afectada, ello podría impactar en las personas, en el resto de los seres vivos y en el medioambiente.

Por lo tanto, algunos de los aspectos vinculados a la seguridad que se deberían considerar con el objetivo de consolidar el ecosistema IoT son:

- Enorme superficie de ataque
- Dispositivos con recursos limitados

- Ecosistema complejo
- Fragmentación de estándares y regulaciones
- Despliegue generalizado
- Integración de seguridad
- Consideraciones de *safety*
- Costos bajos
- Falta de experiencia
- Actualizaciones de seguridad
- Programación insegura
- Responsabilidades poco claras

El estudio de la seguridad de IoT en un sentido horizontal se ve complejizado debido a que las medidas de seguridad y potencial impacto de las diferentes amenazas a las que se encuentra expuesto un activo (dispositivo), estarán condicionadas por su criticidad, la que dependerá del caso de uso, la aplicación en uso, y el escenario de uso. De todas formas, un enfoque horizontal permite definir una línea de base a considerar en cuanto a la seguridad en IoT, que luego puede ser complementada por el análisis para la vertical que se requiera.

Arquitectura

ENISA, luego de analizar diferentes arquitecturas elaboradas por diferentes organizaciones, propone un modelo de referencia de alto nivel en la que contempla cuatro ejes, a saber:

- Dispositivos
- Comunicaciones
- Plataforma en la nube, *backend* y servicios
- Casos de uso

con un eje transversal a los cuatro anteriores específico para la seguridad, donde explicita los siguientes mecanismos:

- Autenticación
- Autorización
- Control de acceso
- Disponibilidad

- Cifrado
- Integridad
- Comunicación segura
- No repudio

Este modelo de referencia es a los efectos de disponer de una herramienta que permita, de manera sistemática y coherente, identificar los activos a ser protegidos.

En las Secciones 3.1.1 y 3.1.2 del Apéndice 3 se dispone de información complementaria respecto a la presentada aquí.

4.2.3. *Good practices for Security of Internet of Things in the context of Smart Manufacturing*

ENISA condujo el estudio que culminó con la elaboración del documento denominado *Good practices for Security of Internet of Things in the context of Smart Manufacturing* [62], con el objetivo de abordar los desafíos de seguridad y privacidad relacionados con la evolución de los sistemas y servicios industriales precipitados por la introducción de las innovaciones asociadas a IoT. Los principales objetivos del trabajo fueron recopilar buenas prácticas para garantizar la seguridad de la IoT en el contexto de la Industria 4.0/*Smart Manufacturing*, al tiempo que se mapeaban los desafíos de seguridad y privacidad pertinentes, las amenazas, los riesgos y los escenarios de ataque. El objetivo del estudio es servir de punto de referencia para promover la colaboración en la Industria 4.0 y la Seguridad Industrial de la IoT en toda la Unión Europea y sensibilizar sobre las amenazas y riesgos pertinentes, centrándose en la "seguridad para el *safety*".

Este estudio describe las buenas prácticas para la ciberseguridad en la IoT aplicada en un entorno industrial. Debido al amplio panorama de las implementaciones de IoT, el mismo se centra en la IIoT y *Smart Manufacturing* pues se identifican como los elementos más representativos del panorama general de la Industria 4.0.

ENISA define la Industria 4.0 como "*un cambio de paradigma hacia cadenas de valor digitalizadas, integradas e inteligentes, que permiten la toma de decisiones en la producción de manera distribuida mediante la incorporación de nuevas tecnologías ciberfísicas como IoT*".

La Industria 4.0 conecta la producción con las tecnologías de la información y la comunicación. Combina los datos del usuario final con los datos de la máquina y permite que las máquinas se comuniquen entre sí. Como resultado, se ha hecho posible que los componentes y las máquinas administren la producción de forma autónoma y de una manera flexible, eficiente y ahorrando recursos. Sus beneficios incluyen, entre otros, una mayor calidad del producto, una mayor flexibilidad, tiempos de lanzamiento de productos más cortos, nuevos servicios y nuevos modelos de negocio.

ENISA define *Smart Manufacturing* como "*los procesos y sistemas de fabricación industrial de próxima generación basados en tecnologías emergentes de información y comunicación, en línea con la Industria 4.0, como la fabricación*

aditiva, la analítica avanzada y la integración IT/O".

Para lograr la innovación y las capacidades mejoradas deseadas, la Industria 4.0 y la *Smart Manufacturing* se benefician de diversas tecnologías, como se puede apreciar en la Figura 4.2, entre las que podemos mencionar:

- Dispositivos finales IIoT
- Comunicación M2M
- Analítica Big Data
- Robótica
- Inteligencia Artificial
- *Machine Learning*
- Mantenimiento Predictivo
- Monitorizado en tiempo real
- Analítica avanzada de pérdidas
- Computación en la nube
- Fabricación aditiva
- Realidad aumentada

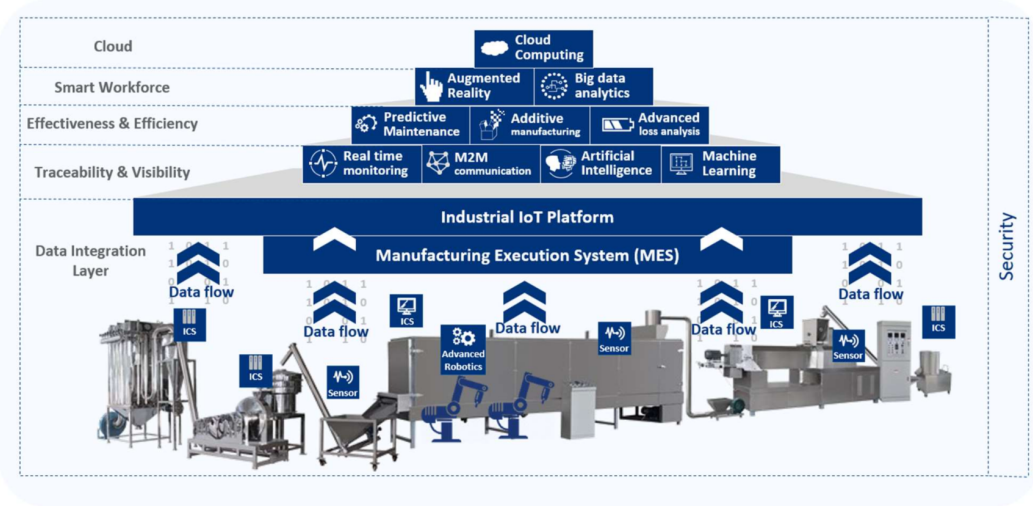


Figura 4.2: Capacidades de la Industria 4.0 y la *Smart Manufacturing*. Fuente: [62]

Como parte del trabajo, ENISA identificó los siguientes desafíos para la seguridad en el contexto de la I4.0 y de la *Smart Manufacturing*:

- Componentes vulnerables

- Gestión de procesos
- Incremento en la conectividad
- Convergencia IT/OT
- Complejidad de la cadena de suministros
- Sistemas de Control Industrial heredados
- Protocolos inseguros
- Factores humanos
- Funcionalidades no utilizadas
- Aspectos vinculados al *safety*
- Actualizaciones de seguridad
- Ciclo de vida seguro del producto

En la Sección 3.1.3 del Apéndice 3 se dispone de información complementaria respecto a la taxonomía de activos, taxonomía de amenazas, buenas prácticas recomendadas y una referencia al vínculo con el informe *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures.*

4.2.4. Ciberseguridad en la Industria 4.0

Con referencia a la Industria 4.0, ENISA elaboró el documento *Industry 4.0 - Cybersecurity Challenges and Recommendations* [63]; se trata de un compendio de desafíos y recomendaciones de alto nivel para cada uno de los diferentes grupos de partes interesadas identificados, a los efectos de promover la ciberseguridad en dicho ámbito.

Los cinco grupos de partes interesadas identificados se muestran en la Figura 4.3 y son:

- Expertos en seguridad (tanto del "mundo" IT como del "mundo" OT)
- Operadores de la Industria 4.0 (proveedores y fábricas)
- Reguladores
- Comunidad de estandarización
- Academia y centros de desarrollo e investigación

Los desafíos y las recomendaciones planteados se agrupan en tres categorías: personas, procesos y tecnología. Luego, se los vincula con los grupos de partes interesadas. A continuación se brinda un resumen de ello.

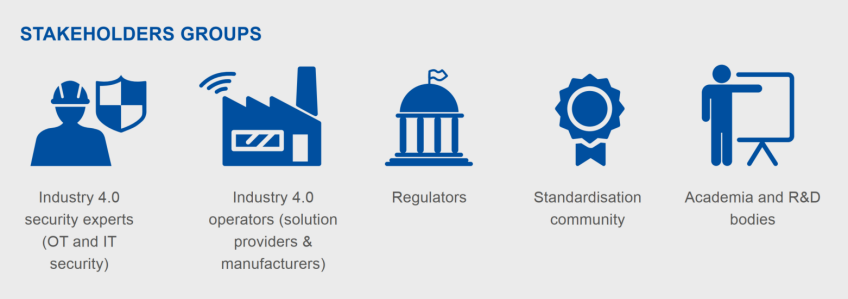


Figura 4.3: Grupos de Partes Interesadas. Fuente: [63]

Personas

Desafío: necesidad de fomentar y alinear la experiencia y concientización en seguridad en IT y OT.
Recomendación: promover el conocimiento cruzado en seguridad IT y OT.

Desafío: existencia de políticas organizacionales incompletas y rechazo a los fondos para seguridad.
Recomendación: promover incentivos económicos y administrativos para la seguridad de la Industria 4.0.

Procesos

Desafío: pobre definición de responsabilidades en la vida útil de los productos de la Industria 4.0.
Recomendación: clarificar las responsabilidades entre los diferentes actores.

Desafío: fragmentación en los estándares técnicos de seguridad para la Industria 4.0.
Recomendación: armonizar los esfuerzos vinculados a los estándares de seguridad de la Industria 4.0.

Desafío: complejidad en la gestión de la cadena de suministro.
Recomendación: elaborar un proceso de gestión segura de la cadena de suministro.

Tecnología

Desafío: interoperabilidad entre los dispositivos de la Industria 4.0, las plataformas y los *frameworks*.
Recomendación: establecer una línea de base para la interoperabilidad segura en la Industria 4.0.

Desafío: restricciones técnicas dificultan la seguridad en la Industria 4.0 y en la fabricación inteligente.
Recomendación: aplicar medidas técnicas para garantizar la seguridad en la Industria 4.0.

Grupos de Partes Interesadas y Recomendaciones

A continuación, para cada grupo de partes interesadas, se detallan las recomendaciones con las que deberían involucrarse directamente.

Expertos en seguridad (tanto del "mundo" IT como del "mundo" OT)

- Promover el conocimiento cruzado en seguridad IT y OT
- Elaborar un proceso de gestión segura de la cadena de suministro
- Establecer una línea de base para la interoperabilidad segura en la Industria 4.0
- Aplicar medidas técnicas para garantizar la seguridad en la Industria 4.0

Operadores de la Industria 4.0 (proveedores y fábricas)

- Promover el conocimiento cruzado en seguridad IT y OT
- Promover incentivos económicos y administrativos para la seguridad de la Industria 4.0
- Clarificar las responsabilidades entre los diferentes actores
- Elaborar un proceso de gestión segura de la cadena de suministro
- Establecer una línea de base para la interoperabilidad segura en la Industria 4.0

- Aplicar medidas técnicas para garantizar la seguridad en la Industria 4.0

Reguladores

- Clarificar las responsabilidades entre los diferentes actores
- Promover incentivos económicos y administrativos para la seguridad de la Industria 4.0
- Armonizar los esfuerzos vinculados a los estándares de seguridad de la Industria 4.0
- Establecer una línea de base para la interoperabilidad segura en la Industria 4.0

Comunidad de estandarización

- Armonizar los esfuerzos vinculados a los estándares de seguridad de la Industria 4.0
- Establecer una línea de base para la interoperabilidad segura en la Industria 4.0

Academia y centros de desarrollo e investigación

- Promover el conocimiento cruzado en seguridad IT y OT
- Establecer una línea de base para la interoperabilidad segura en la Industria 4.0

4.2.5. Herramienta de Buenas Prácticas para IoT e Infraestructuras *Smart*

ENISA tiene a disposición en [60] una herramienta de Buenas Prácticas para IoT e Infraestructuras *Smart* alineada con sus trabajos al respecto, y una guía de uso de la misma.

La herramienta tiene la intención de proporcionar a los operadores e industrias de IoT e Infraestructura *Smart* una guía rápida para hacer su propia evaluación de riesgos (identificar amenazas y priorizar áreas de seguridad de importancia) de acuerdo con las buenas prácticas de seguridad recomendadas por ENISA. La herramienta enumera las buenas prácticas de seguridad para IoT, la Industria 4.0 y, *smart cars*, *smart airports*, *smart hospitals*, y *smart cities*.

Para su uso, primero se debe seleccionar la temática de interés, desplegándose así las Mejores Prácticas, los Dominios de Seguridad al que corresponde cada una y el grupo de amenazas con el que se vincula. Además, aplicando los filtros que resulten relevantes (Categorías, Dominios, Amenazas y Referencias), se pueden obtener las Buenas Prácticas de interés específico.

En todos los casos, está disponible la posibilidad de acceder a las Referencias relevantes asociadas a cada Buena Práctica.

4.3. NIST

Esta sección comienza describiendo las consideraciones del NIST respecto a la gestión de riegos vinculados a la privacidad y la ciberseguridad, para culminar con un acercamiento a la propuesta de un *Framework* de Ciberseguridad que es referencia en la comunidad, con casos de aplicación concretos.

4.3.1. *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*

Como parte del trabajo del NIST respecto a la ciberseguridad en IoT, debemos mencionar la publicación *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*, NIST IR 8228 [184], cuyo propósito es entender y gestionar mejor los riesgos en cuanto a la ciberseguridad y a la privacidad asociados a los dispositivos IoT a lo largo de su ciclo de vida. En el documento referido no se abordan otros tipos de riesgos vinculados, por ejemplo a *safety*, fiabilidad y resiliencia.

Además, en la *NIST Special Publication* (SP) 800-82, *Guide to Industrial Control Systems (ICS) Security* [189], se ofrece una perspectiva desde OT respecto a los riesgos asociados ciberseguridad y la privacidad, con un tratamiento tangencial y parcial de los otras posibles fuentes de riesgos como las mencionadas en el párrafo anterior.

En la primera de las publicaciones mencionadas (NIST IR 8228), se presenta la Figura 4.4 que acompaña un resumen de las capacidades esperables a ser provistas por los dispositivos IoT, mencionándose la siguientes:

- Capacidades de transductor (sensor y/o actuador) o sea, de interactuar con el medio físico y servir de borde entre el ambiente físico y el ambiente digital
- Capacidades de interfaz, que habilitan las interacciones con el dispositivo, destacando tres tipos: interfaz de aplicación, interfaz con el usuario humano e interfaz de red
- Capacidades de apoyo, que comprende aquellas capacidades que proveen las funcionalidades que apoyan otras capacidades del dispositivo, como pueden ser gestión, ciberseguridad y privacidad

Respecto a los riesgos vinculados a la ciberseguridad y a la privacidad, se

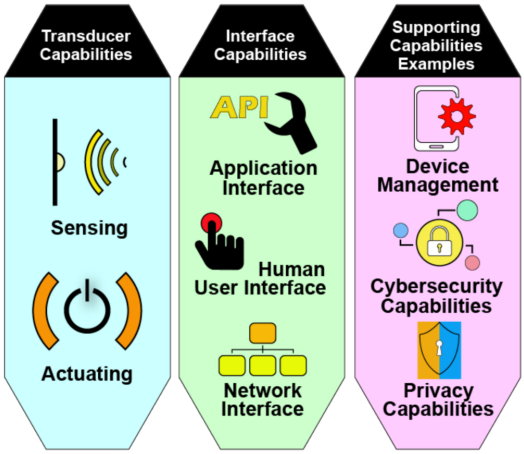


Figura 4.4: Capacidades de los dispositivos IoT. Fuente: [184]

identifica un solapamiento parcial de, por un lado los riesgos de la ciberseguridad que surgen a partir de comportamientos no autorizados de los sistemas y, por otro lado, los riesgos de la privacidad, que surgen a partir del uso no autorizado de la Información de Identificación Personal (PII, por su sigla en inglés); el solapamiento se identifica como la "Ciberseguridad de PII".

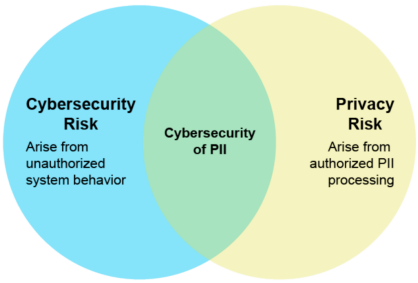


Figura 4.5: Ciberseguridad de PII. Fuente: [184]

Se identifican tres consideraciones de alto nivel que pueden afectar la gestión de los riesgos de la ciberseguridad y la privacidad para los dispositivos IoT, cuando son comparados con los dispositivos IT convencionales. Dichas consideraciones son:

- Muchos de los dispositivos IoT interactúan con el mundo físico de maneras en las que no lo hacen los dispositivos IT convencionales
- Muchos de los dispisitivos IoT no pueden ser accedidos, administrados o monitorizados de la misma forma que sí se puede con los dispositivos IT convencionales

- La disponibilidad, eficiencia y efectividad de las capacidades realativas a ciberseguridad y privacidad frecuentemente son distintas en los dispositivos IoT respecto a los dispositivos IT convencionales

En el mismo contexto, se identifican tres grandes objetivos para mitigar los riesgos asociados a la ciberseguridad y la privacidad en los dispositivos IoT, a saber:

- Protección de la Seguridad del Dispositivo
- Protección de la Seguridad de los Datos
- Protección de la Privacidad de los Individuos

El objetivo de Protección de la Seguridad del Dispositivo involucra mitigar riesgos en las siguientes áreas: Gestión de Activos, Gestión de Vulnerabilidades, Gestión de Accesos, Detección de Incidentes de Seguridad en los Dispositivos.

En segundo lugar, el objetivo de Protección de la Seguridad de los Datos involucra mitigar riesgos en las siguientes áreas: Protección de Datos y Detección de Incidentes de Seguridad en los Datos.

Finalmente, el objetivo de Protección de la Privacidad de los Individuos involucra mitigar riesgos en la siguientes áreas: Gestión del Flujo de Información, Gestión de Permisos para el Procesamiento de PII, Decisiones Informadas, Gestión de Datos No Asociados y Detección de Brechas de Privacidad.

En el documento se explicita, cómo las organizaciones esperan que los dispositivos IT convencionales mitigen los riesgos vinculados con la ciberseguridad y la privacidad, para cada uno de los objetivos y sus correspondientes áreas (y lo que se esperaría para cada una), qué implicaría ello para la organización, y los desafíos potenciales que ello plantea en el caso de aplicarse para los dispositivos IoT. En el trabajo se vincula cada desafío con los controles documentados en la *NIST Special Publication (SP) 800-53, Security and Privacy Controls for Information Systems and Organizations* [195] y también con la subcategoría correspondiente del *Framework for Improving Critical Infrastructure Cybersecurity* [188], también elaborado por el NIST, que se podría ver afectada (salvo para las áreas vinculadas a la Protección de la Privacidad de los Individuos).

Las expectativas identificadas para cada una de las áreas mencionadas, de cada uno de los 3 objetivos mencionados antes se detallan en la Sección 3.2.1 del Apéndice 3.

4.3.2. *Cybersecurity Framework*

A continuación se brinda una descripción de los aspectos fundamentales del *Framework* de Ciberseguridad del NIST, lo que será precedido de la mención a las acciones que lo motivaron.

Antecedentes

Podemos identificar tres documentos fundacionales que terminaron resultando en la elaboración por parte del NIST de la versión actual, la 1.1, de su *Cybersecurity Framework*. Ellos son:

- La *Executive Order 13636 - Improving Critical Infrastructure Cybersecurity* del año 2013 [269]
- La *Public Law No: 113-274 - Cybersecurity Enhancement Act of 2014* del año 2014 [40]
- La *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* del año 2017 [270]

Las Órdenes Ejecutivas y la Ley referidas indujeron al NIST a la elaboración del *Framework* en cuestión, en el entendido que las amenazas de seguridad cibernética explotan la mayor complejidad y conectividad de los sistemas de infraestructura crítica, lo que pone en riesgo la seguridad de la nación, su economía, la salud y la seguridad pública, en el entendido que la seguridad cibernética puede ser un componente importante y amplificador de la gestión general de riesgos de una organización. Si bien este documento se desarrolló para mejorar la gestión del riesgo de seguridad cibernética en la infraestructura crítica, el *Framework* puede ser utilizado por organizaciones en cualquier sector o comunidad. Este permite que las organizaciones, independientemente de su tamaño, grado de seguridad cibernética o sofisticación de seguridad cibernética, apliquen los principios y mejores prácticas de gestión de riesgos para mejorar la seguridad cibernética y la capacidad de recuperación.

El *Framework* ofrece una forma flexible de abordar la seguridad cibernética, lo que incluye el efecto de la seguridad cibernética en las dimensiones físicas, cibernéticas y de personas. Este es aplicable a organizaciones que dependen de la tecnología, ya sea que su enfoque de seguridad cibernética sea principalmente en TI, Sistemas de Control Industrial (ICS, por su sigla en inglés), Sistemas

Ciber Físicos (CPS, por su sigla en inglés) o dispositivos conectados en general, incluido IoT.

El *Framework*

El *Framework* elaborado está conformado por tres componentes primarios: el *Core*, los *Tiers* y los *Profiles*.

Core

Según se puede observar en la Figura 4.6, el *Core* busca resumir todo aquello que sirve como referencia común para todos los sectores con infraestructuras críticas. Consiste en actividades de ciberseguridad y Referencias Informativas, organizadas en función de resultados.

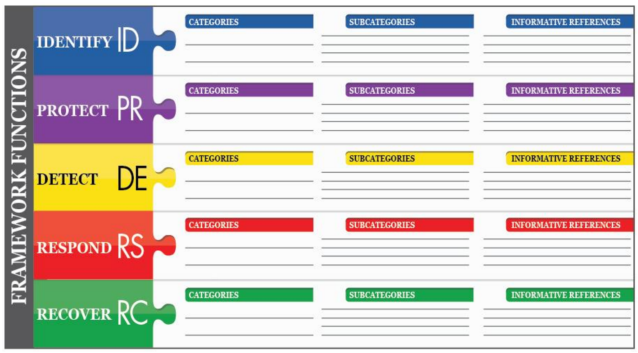


Figura 4.6: *Core del Framework*. Fuente: [188]

El *Core* consta de las 5 funciones concurrentes y continuas que se mencionan a continuación, y que se muestran en la Figura 4.7:

- Identificar
- Proteger
- Detectar
- Responder
- Recuperar

Estas funciones proporcionan una visión estratégica de alto nivel del ciclo de vida de la gestión del riesgo de ciberseguridad de una organización. Para cada función se identifican Categorías (un total de 23) y Subcategorías (un total de 108), que "matchean" resultados con Referencias Informativas de la comunidad, normas o estándares.

(a) Partes **(b)** Funciones

Figura 4.7: NIST - *Framework* de Ciberseguridad. Fuente: [186]

Tiers

Los *Tiers* proporcionan el contexto sobre cómo una organización ve los riesgos de ciberseguridad y los procesos vigentes para gestionarlos, identificándose con cuatro niveles:

- *Partial*
- *Risk Informed*
- *Risk Informed and Repeatable*
- *Adaptive*

A medida que se cambia de nivel, desde *Partial* hasta *Adaptive*, aumenta el grado de rigor y sofisticación en las prácticas de gestión de riesgos de ciberseguridad, se refleja cuán bien son integradas las decisiones de riesgo cibernético en otras vinculadas riesgos más amplias, y el grado en que la organización comparte y recibe información de ciberseguridad de terceros. La implementación exitosa del *Framework* se basa en lograr los resultados descritos en el *Profile* objetivo de la organización y no en la determinación del *Tier*.

Los *Tiers* no representan niveles de madurez ni se los debe tomar como una carrera hacia el *Adaptative*. Cada organización debe decidir qué *Tier* "matchea" mejor con sus necesidades y capacidades de gestión de riesgos. Las organizaciones deben determinar el nivel deseado, asegurándose de que el nivel seleccionado cumpla los objetivos de la organización, sea factible de implementar y reduzca el riesgo de ciberseguridad a niveles aceptables para ella.

Se identifican tres procesos transversales a los *Tiers* vinculados con la gestión de los riesgos, según se observa en la Figura 4.8; ellos son:

- Proceso de Gestión de Riesgo, que refiere a la funcionalidad y repetibilidad de la gestión de riesgos de ciberseguridad

- Programa de Gestión de Riesgo Integrado, que refiere a la medida en que la ciberseguridad se considera en decisiones más amplias de gestión de riesgos
- Participación Externa,que refleja grado en que la organización se beneficia por compartir o recibir información de terceros y permite monitorizar y gestionar los riesgos de la cadena de suministros

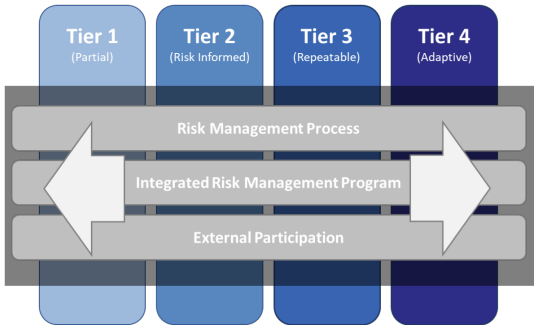


Figura 4.8: *Tiers*. Fuente: [183]

Profiles

Los *Profiles* son los resultados basados en las necesidades del negocio que la organización ha identificado para las Categorías y Subcategorías. Pueden servir para identificar el perfil actual y el perfil deseado en cuanto a la ciberseguridad, y establecer una hoja de ruta, con prioridades para "viajar" de uno a otro.

Los *Profiles* son la alineación de las Funciones, Categorías y Subcategorías a los requerimientos del negocio, la tolerancia al riesgo y a los recursos de la organización.

Como se pretende reflejar en la Figura 4.9, la implementación del *Framework* es una actividad coordinada que involucra flujos de información y decisiones a tres niveles:

- Ejecutivo (superior)
- Empresarial (o de Procesos)
- Implementación (u Operaciones)

El nivel Ejecutivo comunica al nivel Empresarial las prioridades de la misión, los recursos disponibles y la tolerancia general al riesgo. El nivel Empresarial utiliza la información como insumo en el proceso de gestión de riesgos

y a continuación, colabora con el nivel de Implementación para comunicar las necesidades del negocio y crear un perfil. El nivel de Implementación comunica el progreso de la implantación del perfil al nivel de Empresarial. El nivel Empresarial utiliza esta información para realizar una evaluación de impacto. El nivel Empresarial reporta de los resultados de esa evaluación de impacto al nivel Ejecutivo para informar el proceso general de gestión de riesgos de la organización y también al nivel de Implementación para la conciencia del impacto en el negocio.

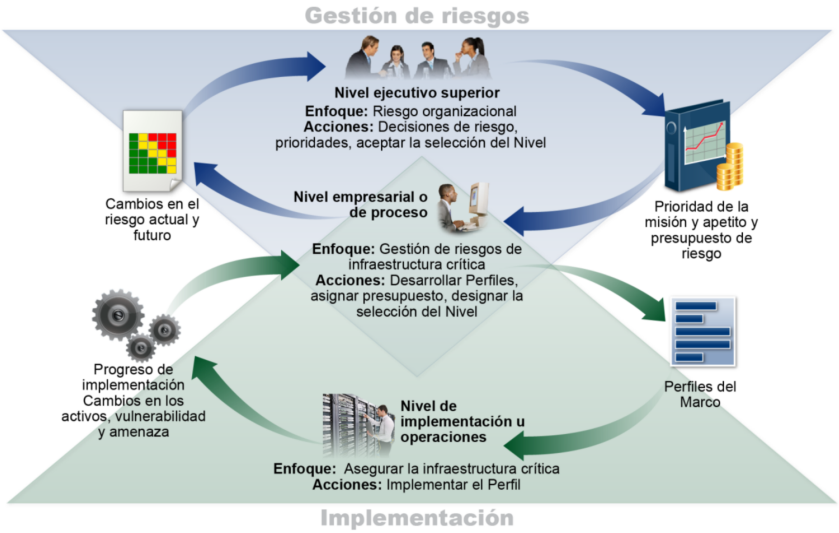


Figura 4.9: Gestión de Riesgos e Implementación. Fuente: [197]

En la Sección 3.2.2 del Apéndice 3 se mencionan y describen los usos posibles del *Framework* de ciberseguridad del NIST.

El *Framework* como fuente de referencia

El *Framework* descrito ha sido utilizado como referencia en diversos contextos [187], pudiendo citar algunos ejemplos concretos:

- Uruguay - AGESIC [3]
- Intel [137]
- Israel - INCD [198]

4.4. IETF

Esta sección comienza describiendo las consideraciones fundamentales respecto al estado del arte y los desafíos a la seguridad en IoT de acuerdo a la visión del IETF, para culminar con un acercamiento al concepto *Manufacturer Usage Descriptor* (MUD) el cual es considerado muy relevante por buena parte de la comunidad vinculada a IoT.

4.4.1. *Internet of Things (IoT) Security: State of the Art and Challenges*

La RFC 8576, *Internet of Things (IoT) Security: State of the Art and Challenges*, de categoría *Informational* [86], presenta un resumen de los aspectos más importantes relativos a la seguridad de IoT.

En dicho documento se define el concepto IoT como "*el uso de protocolos de Internet estándares para permitir la comunicación human-to-thing y thing-to-thing*"; señala además que IoT significa la interconexión de entidades y redes muy heterogéneas y con diferentes patrones de comunicación, como ser: *human-to-human* (H2H), *human-to-thing* (H2T), *thing-to-thing* (T2T), o *thing-to-things* (T2Ts).

Ciclo de Vida

En esta RFC se presenta una propuesta de ciclo de vida de las cosas de IoT, que se observa en la Figura 4.10, a las que identifica como "dispositivos informáticos que entienden y reaccionan al entorno en el que residen", a veces también denominadas como *smart objects* o *smart devices*. Para ello considera como referencia un hipotético sistema de Control y Automatización de Inmuebles (BAC, por su sigla en inglés), donde conviven diferentes nodos interconectados cumpliendo diversas funciones coordinadas en diferentes dominios, como ser calefacción, ventilación, iluminación, *safety*, entre otros, siendo muchos de esos dispositivos de recursos limitados.

En dicho escenario de referencia, la vida de la "cosa" comienza cuando es fabricada y, considerando la diversidad de funciones esperadas, es poco probable que todas sean provistas por el mismo fabricante, lo que hace que la interoprabilidad sea un tema muy relevante a considerar.

Luego de fabricados, los dispositivos son instalados e iniciados lo que inicia la fase operacional. Durante la misma, se requerirán actividades de mantenimiento, actualizaciones de software y realizar reconfiguraciones. Esto fase continuará hasta que el dispositivo sea retirado al final de su ciclo de vida, lo que puede significar su reemplazo por, quizás, otro u otros dispositivos con mejores funcionalidades. El dispositivo retirado puede ser reciclado para ser utilizado en otro contexto, comenzando así un nuevo ciclo de vida.

Dicho ciclo de vida podría considerarse algo simplificado, pues podría afirmarse que no comienza cuando se dispone del dispositivo fabricado (tangible), sino que comienza cuando se dispone de la última línea de código del software asociado. Por otro lado, también se debería considerar si dicho dispositivo es parte de una cadena de suministro previa a la instalación.

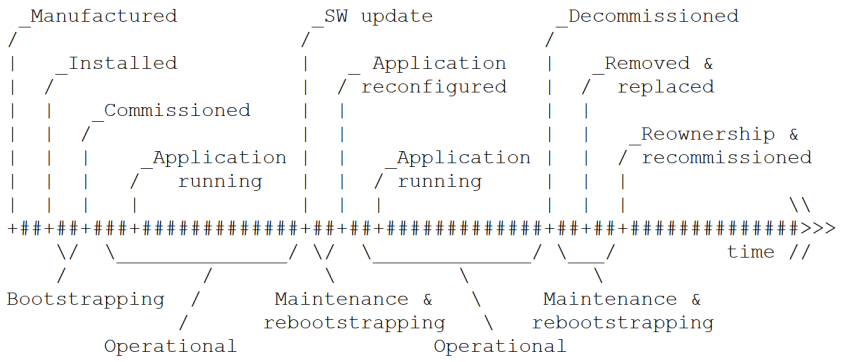


Figura 4.10: Ciclo de Vida de una *Thing* de IoT. Fuente: [86]

En la Sección 3.3.0.1 del Apéndice 3 se ahonda en más aspectos de seguridad para IoT considerados en la RFC 8576.

Desde la óptica de la privacidad, un usuario o dueño de un dispositivo IoT quisiera conocer el comportamiento del mismo: a qué se conecta y qué información se transfiere. Proporcionar dicha información a los usuarios de una manera comprensible es también un desafío. Esto se debe a que los dispositivos IoT no son solo restringidos en recursos en términos de su capacidad computacional, sino que también en términos de la interfaz de usuario disponible. Sumado a ello, la infraestructura de red donde se despliegan estos dispositivos varia significativamente de un entorno de usuario a otro. Por lo tanto, cuándo y cómo se implementa esta función de monitorizado de la privacidad sigue siendo un pregunta latente.

Un primer paso hacía disponibilizar ese monitorizado es lo que se conoce como *Manufacturer Usage Descriptor* (MUD), que se encuentra especificado

en la RFC 8520, *Manufacturer Usage Description Specification* [89]. La idea general del MUD es que el dispositivo IoT, durante su instalación, proporcione a la red donde se conectará, la ubicación del archivo MUD, el que contendrá la información necesaria para que la red conozca cuál es el comportamiento esperado del dispositivo, de acuerdo a lo expresado por quien creó el MUD *file*; dicho de otra forma, el archivo MUD indica los requerimientos de comunicaciones del dispositivo IoT. El monitorizado buscado, puede considerar esta información como una de las fuentes posibles para informar al usuario o dueño del dispositivo de eventuales apartamientos respecto a ese comportamiento esperado.

Desde un punto de vista conceptual y de acuerdo a lo expresado en la RFC 7452, *Architectural Considerations in Smart Object Networking* [83], los dispositivos IoT no son de propósito general, sino que cumplen un propósito específico, por lo tanto, no están destinados para todos los otros usos posibles, por lo que estos otros usos deberían estar prohibidos.

En la Sección 3.3.1 del Apéndice 3 se profundiza respecto al concepto MUD, contemplando la arquitectura involucrada, pruebas de concepto referenciales y herramientas disponibles para eventuales despliegues de la solución.

4.5. Internet Society

Esta sección comienza brindando la definición de IoT elaborada por la Internet Society, para continuar con la mención a dos trabajos: el primero de ellos, respecto a un *framework* orientado a la confianza en IoT y el segundo, un compendio de consideraciones relativas a la privacidad. El final de la sección se destina a documentar las iniciativas que la Internet Society impulsa en diversos países con el paradigma *multistakeholder*, con foco en el trabajo realizado en Canadá.

4.5.1. IoT

La *Internet Society* define a IoT [145] como "*un dispositivo que se puede conectar a Internet*"; luego menciona algunos ejemplos posibles de dispositivos IoT que ayudan a enriquecer una definición bastante (demasiado) general, como ser un *fitness tracker*, una cerradura y una lámpara de iluminación.

Respecto a IoT, el trabajo de la *Internet Society* está fuertemente dirigido a los dispositivos IoT y al involucramiento de las diferentes partes interesadas, especialmente a los ciudadanos, y en cuanto a la seguridad de los dispositivos IoT, su premisa es: "*Si queremos estar seguros, tenemos que estar dispuestos a hacer nuestra parte*".

Se afirma que muchos de los dispositivos IoT de hoy en día se introducen al mercado de manera apresurada y con poca consideración por las protecciones básicas de seguridad y privacidad, en lo que denominan "*insecurity by design*". Reafirman lo expresado al indicar que esto nos pone a todos en riesgo: de ser espiado involuntariamente o tener nuestros datos comprometidos o no poder mantener activada la alarma de nuestra propia casa. Incluso estos dispositivos podrían convertirse en parte de una red de *bots* que ataque a algunos servicios de Internet. Incluso, una cámara web insegura, junto con millones de otros dispositivos, podrían ser utilizado para atacar la red eléctrica de todo un país.

Vinculados a la temática, se destacan 2 documentos elaborados por la Internet Society, denominados *IoT Trust Framework* y *Policy Brief: IoT Privacy for Policymakers*.

El primero de ellos, abordado en la Sección 3.4.1 del Apéndice 3, realiza un acercamiento holístico a los aspectos de seguridad, privacidad y sostenibilidad, estando destinado a los consumidores de dispositivos IoT.

El segundo, documentado en la Sección 3.4.2 del Apéndice 3, profundiza en un aspecto fundamental de los dispositivos IoT: la privacidad.

4.5.2. Seguridad en IoT - El caso Canadá

La *Internet Society* en conjunto con el *Ministry of Innovation, Science and Economic Development (ISED)*, la *Canadian Internet Registration Authority* (CIRA), CANARIE y la *Canadian Internet Policy and Public Interest Clinic* (CIPPIC) se unieron para convocar a las partes interesadas, con el fin de elaborar recomendaciones para un conjunto de normas/políticas para asegurar el IoT en Canadá.

El trabajo del equipo multidisciplinario estuvo enfocado a los productos IoT a nivel del consumidor y guiado por los siguientes principios:

- La complejidad de la seguridad de IoT requiere un proceso orgánico *botton-up* para garantizar que los resultados aborden todos los desafíos y problemas existentes y potenciales. El enfoque debe ser fluido en la naturaleza, definido y refinado a través de la discusión con las partes interesadas
- Las normas técnicas armonizadas internacionalmente son clave para mejorar la seguridad de la IoT a largo plazo, pero son difíciles de hacer bien y toma tiempo. Es razonable que los enfoques de la seguridad de la IoT comiencen a nivel nacional mientras trabajan en colaboración con otros organismos nacionales, regionales e internacionales
- Debido a la inmediatez de los riesgos y el largo plazo involucrados en los desarrollos, así como también en las mejoras de las políticas marco y el desarrollo de normas internacionales, es importante comenzar a trabajar en la educación de los consumidores para que las empresas comiencen con la adopción de mejores prácticas que reduzcan los riesgos de la incorporación de dispositivos IoT por parte de aquellos

Ciertos aspectos de la seguridad de IoT están tan bien establecidos que se afirmaron como acciones de referencia que deben tomarse para mejorar la seguridad de IoT, considerando las siguientes:

- No deben existir contraseñas preestablecidas universales o fácilmente adivinadas

- Los datos deben transmitirse y almacenarse de forma segura mediante un cifrado seguro
- La recopilación de datos debe minimizarse solo a lo necesario para que un dispositivo funcione
- Los dispositivos deben ser capaces de recibir actualizaciones y parches de seguridad
- Los fabricantes de dispositivos deben notificar a los consumidores si hay una brecha de seguridad
- Los fabricantes de dispositivos deben asegurarse de que los consumidores puedan restablecer un dispositivo a la configuración de fábrica en caso de venta o transferencia del dispositivo

Luego de más de un año de trabajo, el resultado fue la elaboración del *Final Outcomes and Recommendations Report*, disponible en [142].

Grupos de Trabajo

A los efectos de organizar el trabajo del equipo multidisciplinario en el proyecto, se crearon tres grupos de trabajo:

- Resiliencia de la Red
- Etiquetado de los Dispositivos
- Educación y Concientización de los Consumidores

El grupo *Canadian Multistakeholder Process: Enhancing IoT Security* [141] casi logró el consenso para definir IoT como "*cualquier dispositivo expuesto a la red que no accesible históricamente, o cualquier dispositivo que transmita datos, a través de Internet, que generalmente carece de suficiente seguridad integrada para protegerse de causar o convertirse en una fuente de daño*". Al respecto de la definición, el consenso estuvo condicionado a que la misma esté sujeta a actualizaciones en función de los desarrollos tecnológicos que ocurran.

Resultados

Las consideraciones de seguridad generales más relevantes que resultaron del trabajo son las que se mencionan a continuación:

- Elevar el enfoque en los estándares de nivel internacional. Los estándares pueden proporcionar una orientación clara, comprobable y creíble sobre la implementación de la seguridad y la privacidad mediante el diseño en todas las jurisdicciones
- Continuar el desarrollo y la implementación del *Secured Home Gateway* en CIRA y el estándar *Manufacturer Usage Description* (MUD) en el IETF, con el fin de proporcionar enfoques a nivel de red para la resiliencia, que puedan abordar el desafío de dispositivos de bajo costo y de fabricación extranjera que no se adhieran a las normas de seguridad (que están diseñadas para dispositivos y empresas específicos)
- Continuar desarrollando una etiqueta amigable para el consumidor junto con los estándares internacionales. Se recomienda que una etiqueta combine "marcas de confianza" estáticas (como CE en Europa, *Kitemark* en el Reino Unido, CSA en Canadá) con un componente "vivo" como un código QR que puede transmitir información avanzada y actualizada de la seguridad del producto

4.5.3. Iniciativas similares en otros países

Esfuerzos similares a los llevados adelante por la *Internet Society* y Canadá, están en marcha en otros países, como ser Francia [147], Senegal [143] y Uruguay [152].

En el caso concreto de Uruguay, se elaboró un documento de propuestas sobre Seguridad en IoT [140], como resultado de un proceso de consulta y trabajo en modalidad *multistakeholder*.

4.6. *IoT Security Foundation*

La *IoT Security Foundation* (IoTSF) es una organización sin fines de lucro establecida para responder a la miríada de desafíos en cuanto a la seguridad, y que pregona la premisa *build secure, buy secure, be secure.*

En las próximas dos secciones se enumeran las publicaciones fundamentales elaboradas por la IoTSF y una autocertificación que ofrece a la comunidad.

4.6.1. Publicaciones

La IoTSF ha publicado numerosos documentos relacionados con la seguridad, con el objetivo de disponibilizar a la comunidad, en función de los diferentes roles que se asumen al momento de analizar la seguridad de los dispositivos IoT, los que autoidentifican como las mejores prácticas al respecto. En tal sentido, en [154] se puede acceder a las siguientes publicaciones:

- *IoT Security Compliance Framework*
- *Consumer IoT: Understanding the Contemporary Use of Vulnerability Disclosure : 2020 Progress Report*
- *Secure Design Best Practice Guides*
- *Can You Trust Your Smart Building?*
- *IoT Security Reference Architecture for the Healthcare Industry*
- *Use of Vulnerability Disclosure in Consumer Internet of Things Companies*
- *HOME IoT Security Architecture and Policy*
- *ENTERPRISE IoT Security Architecture and Policy*
- *IoT Cybersecurity: Regulation Ready - FULL Version Nov 2018*
- *IoT Cybersecurity: Regulation Ready - CONCISE Version Nov 2018*
- *Vulnerability Disclosure BPG*
- *Best Practice User Mark*

4.6.2. *Best Practice User Mark*

Las organizaciones que utilizan (siguen e implementan) la última versión (*Release* 2.1 - mayo 2020) del primero de los documentos mencionados, *IoT Security Compliance Framework* y la documentación de orientación asociada

proporcionada por la IoTSF, pueden hacer uso de la *Best Practice User Mark*, sin que implique costo alguno y sin necesidad de ser miembros de la IoTSF.

Para ello la IoTSF pone a disposición un cuestionario que tiene como objetivo registrar la evidencia requerida para la autocertificación ante el *Framework* en cuestión.

Dicho cuestionario permite determinar el nivel de apetito de riesgo (Básico, Medio, Alto) para el dispositivo en cuestión, respecto a las propiedades fundamentales de la seguridad: confidencialidad, integridad y disponibilidad. Ello determina que se seleccione una de las 5 Clases de Cumplimiento (identificada por los valores de 0 a 4).

Posteriormente, el cuestionarios aborda diversas cuestiones respecto a diferentes áreas consideradas de interés por parte de los autores, a saber:

- Proceso de Negocio
- Hardware del Dispositivo
- Software del Dispositivo
- Sistema Operativo del Dispositivo
- Interfaces del Dispositivo
- Autenticación y Autorización
- Cifrado y Gestión de Claves
- Interfaz Web para el Usuario
- Aplicación Móvil
- Privacidad
- Nube y Elementos de Red
- Producción Segura en la Cadena de Suministros
- Configuración
- Transferencia de la Propiedad del Dispositivo

4.7. *Smart Nation*

En esta sección se comienza brindando algunos argumentos que sustentan el porqué de la consideración particular de Singapur respecto a la Industria 4.0. Luego, se presenta el trabajo que se ha realizado en la nación del sureste asiático, referido al llamado Índice SIRI (*Smart Industry Readiness Index*) y las necesidades de mejoras al respecto que han identificado de manera empírica, luego de aplicarlo en diferentes ámbitos. La Sección culmina con una breve mención a la *Cyber Security Agency* de Singapur.

4.7.1. Industria 4.0 en Singapur

Es importante destacar que el país en cuestión es uno de los líderes mundiales en cuanto a la Transformación Digital, de acuerdo al Índice de Transformación Digital Asiático elaborado por *The Economist* [266, 54], estando también en los primeros lugares de los país donde es más fácil realizar negocios, de acuerdo al último reporte del Banco Mundial [271], siendo también líder en el último Reporte de Competitividad Global del Foro Económico Mundial, del año 2019 [288]. Lo anterior no hace más que justificar la necesidad de ser contemplado en el presente trabajo.

4.7.2. *Smart Industry Readiness Index*

Singapur se encuentra llevando adelante un plan de transformación del país a través de la iniciativa, denominada *Smart Nation* [259]. No obstante ello, las empresas estaban teniendo dificultades para identificar qué implicaba exactamente la Industria 4.0 para ellas. En noviembre de 2017, el *Economic Development Board* (EDB) de Singapur, en asociación con TÜV SÜD [272], lanzaron el Índice de Preparación de la Industria Inteligente [258], denominado *Smart Industry Readiness Index* (SIRI) [256], con el objetivo de ayudar a las empresas a evaluar las instalaciones de fabricación existentes, apoyar a las empresas en su proceso de transformación e impulsar la revolución de toda la industria. El Índice SIRI está diseñado de tal forma que puede ser aplicado desde las pequeñas y medianas empresas (SMEs, por su sigla en inglés) hasta las corporaciones multinacionales (MNCs, por su sigla en inglés).

Se podría resumir su utilidad indicando que mediante SIRI es posible responder, al menos, las siguientes preguntas: “¿Qué es la Industria 4.0 y cómo

puede beneficiarse de ella mi empresa?", "¿Por dónde empiezo?", "¿Cuáles son mis brechas hoy y dónde están las oportunidades mañana?". El Índice SIRI permite determinar cómo comenzar, escalar y mantener la transformación de una empresa hacia la Industria 4.0.

Para el desarrollo del Índice SIRI, además de considerar el apoyo de diferentes asesores especializados en la materia y las experiencias particulares de SMEs y MNCs, se utilizaron las siguientes referencias:

- El modelo RAMI 4.0
- El *Industrie 4.0 Maturity Index* [2] desarrollado por la *German Academy of Science and Engineering* (acatech)
- El *Bersin Model for Human Capital Development* [46] elaborado por Deloitte

Framework

De acuerdo a la información disponible en [257], el *framework* referencial del Índice SIRI, según se muestra en la Figura 4.11, está compuesto de 3 capas:

La capa superior, contempla los 3 aspectos fundamentales de la Industria 4.0, a los que denominan Bloques:

- Procesos
- Tecnología
- Organización

Estos tres Bloques se sustentan en 8 Pilares (capa intermedia):

- Operaciones
- Cadena de Suministro
- Ciclo de Vida del Producto
- Automatización
- Conectividad
- Inteligencia
- Preparación del Talento
- Gestión y Estructura

Por último, la capa inferior contempla 16 Dimensiones:

- Integración Vertical
- Integración Horizontal
- Ciclo de Vida del Producto Integrado
- Planta ("x3")
- Empresa ("x3")
- Instalación ("x3")
- Aprendizaje y Desarrollo de la Fuerza Laboral
- Competencia de Liderazgo
- Colaboración Inter e Intra Compañía
- Gobernanza y Estrategia

Debemos puntualizar que la dimensión Planta hace referencia al "*shop floor*" o sea, donde se lleva a cabo la producción y gestión de mercancías; la Empresa o *Enterprise*, es donde se llevan adelante las tareas administrativas; y la Instalación o *Facility* refiere al edificio físico o a los locales donde la producción tiene lugar.

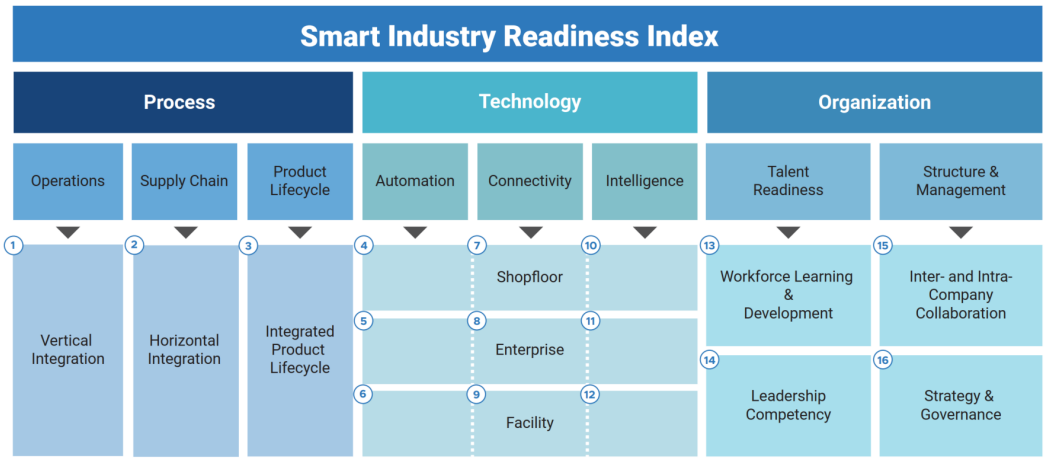


Figura 4.11: *Framework* SIRI. Fuente: [257]

Los 3 Bloques y los 8 Pilares se mapean con las 16 Dimensiones, que son las áreas de evaluación que debería utilizar la empresa para determinar su preparación actual para la Industria *Smart*.

4.7.3. Utilizando el Índice SIRI

A continuación veremos brevemente cómo utilizar el Índice SIRI y así pasar de los conceptos al valor para el negocio.

El Índice SIRI considera cuatro pasos pragmáticos que la empresa debe dar, siendo ellos los reflejados en la Figura 4.12:

- Aprender
- Evaluar
- Diseñar
- Ofrecer

lo que se conoce como el *framework* LEAD (*Learn, Evaluate, Architect and Deliver*).

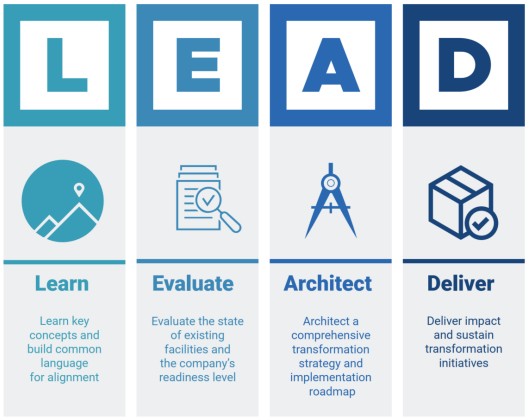


Figura 4.12: *Framework* LEAD. Fuente: [257]

Veamos a continuación las ideas principales detrás de cada paso.

El primer paso es Aprender los conceptos clave y construir un lenguaje común para estar alineados. Examinando los 3 Bloques, los 8 Pilares y las 16 Dimensiones, el Índice busca informar y educar mejor a las empresas sobre los conceptos básicos y los principios fundamentales de la Industria 4.0, incluyendo aspectos vinculados con el valor para el negocio; permite además establecer un lenguaje común entre las diversas partes interesadas necesarias para la transformación hacia la Industria 4.0.

El segundo paso consiste en Evaluar el estado de las instalaciones existentes y el nivel de preparación de la empresa para la Industria 4.0. Luego del primer paso (Aprender), las empresas deben poder identificar tres cosas: qué se evaluará (alcance), a quiénes se evaluará (partes interesadas) y cómo se evaluará (granularidad). La evaluación implica asignar a cada una de las 16 Dimensiones lo que se identifica como "Banda", con valores entre 0 y 5, utilizando para ello los siguientes Principios de Evaluación:

- El Índice proporciona una instantánea del estado actual de la instalación y no de su potencial en el futuro
- El Índice utiliza los conceptos de la Industria 4.0 como punto de referencia. También deben tenerse en cuenta, si procede, los conceptos y tecnologías industriales y de fabricación en el futuro
- Todas las dimensiones deben ser tomadas formalmente en consideración. La importancia y pertinencia de cada Pilar y Dimensión variará, dependiendo de las necesidades actuales y futuras de la empresa y de la naturaleza de la industria
- El enfoque no debe ser en lograr la Banda 5 en todas las Dimensiones. En su lugar, las empresas deben esforzarse por lograr una banda más alta basada en sus necesidades y aspiraciones empresariales específicas
- El Índice debe utilizarse de forma continua, en lugar de para una única evaluación

El tercer paso del *framework* LEAD implica Diseñar una estrategia de transformación integral y una hoja de ruta de implementación. En este tercer paso, las empresas pueden utilizar el Índice de dos maneras tangibles. En primer lugar, sirve como una lista de verificación para las empresas, ayudándolas a asegurarse de que todos los Bloques, Pilares y Dimensiones se consideran formalmente. Si bien la importancia relativa de cada dimensión puede variar, las empresas deben tener en cuenta todas las Dimensiones para garantizar que "todo el terreno esté cubierto". En segundo lugar, el Índice funciona como una guía de mejora paso a paso, desglosando y estableciendo los pasos intermedios del viaje de transformación hacia la Industria 4.0. Sin la orientación adecuada, muchas empresas tendrán dificultades para eliminar la brecha entre su estado actual y su visión de lo que quiere ser.

Finalmente, el cuarto paso es Ofrecer iniciativas de transformación que resulten de impacto y sostenibles. Una vez que una empresa ha llegado a su hoja de ruta de transformación, el siguiente paso es poner en marcha la infraestructura, los sistemas y los procesos adecuados, de manera alineada con esa hoja de ruta. Las empresas intentarán determinar el enfoque óptimo para lograr sus resultados en las diversas fases e iniciativas involucradas. Las estrategias de transformación también deben adaptarse y evolucionar continuamente, y por lo tanto las empresas deben considerar establecer equipos centrales y multifuncionales para ejecutar el seguimiento, evaluar el impacto e identificar

oportunidades futuras de mejora.

4.7.4. Herramienta de auto-diagnóstico

En el final del documento *The Smart Industry Readiness Index - Catalysing the transformation of manufacturing*, los autores ofrecen lo que identifican como *Assessment Tool: The 16 Dimensions*: un conjunto de tablas donde se establece, para cada combinación posible de Bloque, Pilar y Dimensión, con cual de las 6 Bandas posibles (etiqueta asociada a cada valor de 0 a 5) más se identifican, considerando las correspondientes Definiciones y Descripciones que acompañan a cada una.

En la Figura 4.13 se muestra un ejemplo para el caso "Tecnología - Inteligencia - Inteligencia en el *Shop Floor*", que se corresponde con el área 10 del *framework* SIRI.

A partir de dicha información, cada empresa dispondrá de un *snapshot* de su nivel de madurez respecto a la Industria 4.0 y habrá generado la denominada *Assessment Matrix Score* (AMS).

4.7.5. Matriz de Priorización

La Matriz de Evaluación (AMS) que resulta del análisis previo se debe acompañar de una segunda herramienta, conocida como la Matriz de Priorización, disponible en [255].

Dicha matriz ayuda a priorizar las Dimensiones SIRI, identificando aquellas que pueden ofrecer mayor impacto a la organización. Esta herramienta fue desarrollada con la colaboración de *McKinsey & Company*, Siemens, SAP y TÜV SÜD. A continuación ahondaremos en la utilidad de dicha matriz.

Framework TIER

Desde su lanzamiento, el Índice SIRI ha ayudado a muchas empresas a comprender mejor la Industria 4.0 y su valor potencial para sus instalaciones de fabricación. A pesar del aumento del conocimiento, la mayoría de las empresas seguían sin comprometerse en el desarrollo y ejecución de planes de acción, lo que pretende reflejar la Figura 4.14, exponiendo una brecha significativa entre el conocimiento y la implementación de las soluciones de la Industria 4.0

Technology Building Block | Intelligence Pillar | Shop Floor Intelligence Dimension			
Shop Floor Intelligence is the processing & analysis of data to optimize existing processes and create new applications, products, and services, within the location where the production and management of goods is carried out.			
Band		**Definition**	**Description**
0	None	OT & IT systems are not in use.	No electronic or digital devices are used.
1	Computerized	OT & IT systems execute pre-programmed tasks and processes.	Equipment, machinery and computer-based systems are able to perform tasks based on pre-programmed logic.
2	Visible	Computerized OT & IT systems are able to identify deviations.	Equipment, machinery and computer-based systems are able to notify operators of deviations from predefined parameters.
3	Diagnostic	Computerized OT & IT systems are able to identify deviations and diagnose potential causes.	Equipment, machinery and computer-based systems are able to notify operators of deviations, and provide information on the possible causes.
4	Predictive	Computerized OT & IT systems are able to diagnose problems and predict future states of assets and systems.	Equipment, machinery and computer-based systems are able to predict and notify operators of potential deviations, and provide information on the possible causes.
5	Adaptive	Computerized OT & IT systems are able to diagnose problems, predict future states and autonomously execute decisions to adapt to changes.	Equipment, machinery and computer-based systems are able to predict and diagnose potential deviations, and independently execute decisions to optimize performance and resource efficiency.

Figura 4.13: Ejemplo para Evaluación de las Dimensiones. Fuente: [257]

[55], y es allí donde la priorización de las Dimensiones, mediante la Matriz de Priorización, pretende ayudar a reducir ese *gap*.

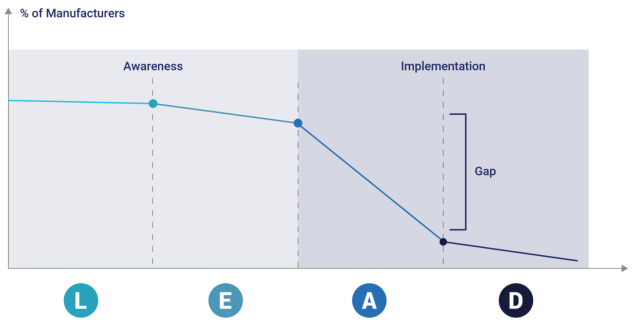


Figura 4.14: Industria 4.0 - *Gap* entre Conciencia e Implementación. Fuente:[255]

Una de las barreras más citadas para avanzar a la implementación es la falta de una estrategia eficaz. En un mundo de escasos recursos, sobrecarga de información y presiones para ofrecer resultados a corto plazo, una visión clara de la Industria 4.0 es esencial para que las empresas se adentren más allá de

los pilotos a pequeña escala y adopten proyectos realmente transformadores.

La priorización permite a las empresas identificar las áreas donde enfocarse pues son las que le generarán el mayor beneficio, impulsando la toma de decisiones basadas en información y la asignación efectiva de los recursos.

Por lo tanto, para que se avance a la implementación resulta vital responder algunas preguntas fundamentales, como ser, "¿cuáles son los elementos claves que mi empresa debe tener en cuenta?", "¿cómo podría mi empresa llevarlo a cabo de manera sistemática?" Para ello, se propone que la priorización tome en cuenta cuatro principios clave, reflejados en la Figura 4.15 lo que se conoce como el *Framework* TIER: acrónimo de *Today's State*, *Impact to Bottom Line*, *Essential Business Objetives* y *Reference to the Broader Community*.

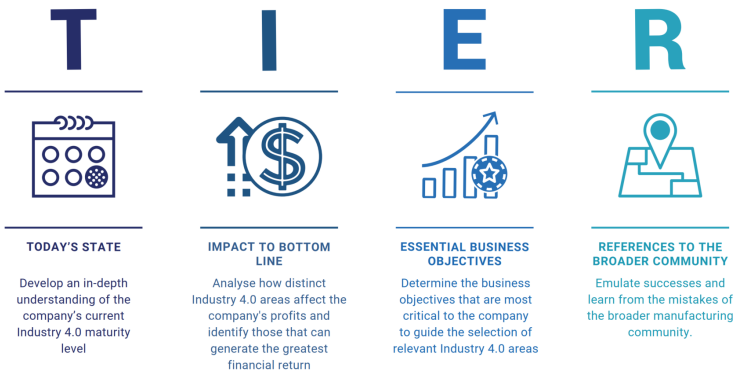


Figura 4.15: *Framework* TIER. Fuente: [255]

Con el principio Estado Actual (*Today's State*) se busca desarrollar una comprensión profunda del nivel de madurez actual de la Industria 4.0.

Mediante el principio Impacto en la Línea de Fondo (*Impact to Bottom Line*) se pretende determinar qué áreas impactan más directamente en los beneficios de la empresa e identificar aquellas que pueden generar el mayor rendimiento financiero.

El principio Objetivos Esenciales del Negocio (*Essential Business Objetives*) permite determinar los objetivos de negocio que son más críticos para la empresa, para así guiar la selección de las áreas relevantes de la Industria 4.0.

Finalmente, el principio Referencia a la Comunidad más Amplia (*Reference to the Broader Community*) busca emular los éxitos, compararse con los mejores y aprender de los errores de la comunidad de fabricación, en su sentido más amplio.

Para identificar en cada caso las Dimensiones de alta prioridad del Índice

SIRI, se propone una fórmula, denominada Matríz de Priorización, que considera tres factores claves: el costo, los KPIs principales, y la proximidad de la empresa al *Best-in-Class* de la industria en cuestión. Cada uno de dichos factores es ponderado de acuerdo a su influencia, como se verá más adelante.

Con el objetivo de desarrollar una transformación holística hacia la Industria 4.0, los autores recomiendan considerar al menos una Dimensión de cada Bloque, considerando para ello el Valor de Impacto asociado a cada una. El Valor de Impacto representa el beneficio relativo que una empresa obtendrá al progresar por una sola banda dentro de una Dimensión determinada del Índice. Al comparar los Valores de Impacto de las diferentes mejoras de la banda, los fabricantes podrán identificar cuantitativamente las Dimensiones específicas del Índice SIRI a las que se debe dar prioridad y las bandas precisas a las que aspirar.

Dicho Valor de Impacto se calcula como la suma de cada uno de los 3 factores mencionados anteriormente (Costo, KPI y Proximidad), ponderado cada uno de acuerdo a como se describe a continuación, según se observa en la Figura 4.16.

Figura 4.16: Fórmula de la Matriz de Priorización. Fuente: [255]

La Matriz de Priorización toma como insumos el *Score* de la Matriz de Evaluación, el Perfil de Costos e Ingresos, los KPIs y la Proximidad a ser el *Best-in-Class*.

El *Score* de la Matriz de Evaluación son los niveles de madurez en Industria 4.0 actual, representados por la Banda para cada una de las Dimensiones del Índice. Esto determina la línea base para la transformación de la empresa, y tener así contra qué compararse.

El Factor Costo de una Dimensión del Índice SIRI refleja el nivel de impacto que puede tener esa Dimensión en la *botton line* de la empresa. Las Dimensiones SIRI recomendadas deben incluir aquellas que entreguen el mayor beneficio

financiero a la empresa.

Para el Cálculo del Factor Costo de una Dimensión SIRI se requiere disponer del Perfil de Costos de la empresa y de la tabla de Grado de Relevancia (DOR, por su sigla en inglés) asociado.

El Perfil de Costo de una empresa refiere al desglose de sus costos expresado como porcentajes de sus ingresos. Se propone para ello desagregarlo en las siguientes 10 categorías:

- Servicios post-venta / Garantía
- Depreciación
- Trabajo
- Mantenimiento y Reparación
- Materias Primas y Materiales Fungibles
- Alquiler y Arrendamiento Operativo
- Investigación y Desarrollo
- Gastos de Venta, Generales y Administrativos
- Transporte y Distribución
- Ganancias Antes de Intereses e Impuestos

4.7.6. Indicadores Clave de Rendimiento

Los Indicadores Clave de Rendimiento (KPI, por su sigla en inglés) son medidas utilizadas para evaluar el éxito o la eficacia de una empresa en la consecución de sus objetivos empresariales clave y directivas estratégicas.

El Factor KPI de una Dimensión SIRI refleja el impacto que esa Dimensión puede tener en los objetivos de negocio esenciales de la empresa. Para ello se propone que se identifiquen los 5 KPIs fundamentales que reflejen el futuro deseado del negocio, y la tabla de Grado de Relevancia asociada.

La Matriz de Priorización considera 14 categorías de KPI organizados en 4 grupos, según se aprecia en la Figura 4.17:

- Productividad
- Calidad
- Flexibilidad
- Velocidad

A continuación se describirá brevemente cada uno de los grupos y se mencionarán los KPIs considerados.

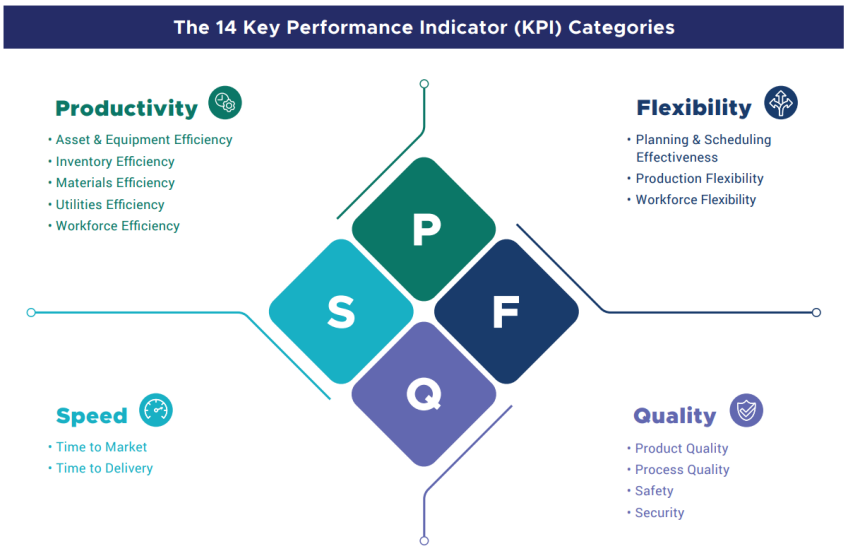


Figura 4.17: KPIs de la Matriz de Priorización. Fuente: [255]

Productividad

La Eficiencia es un concepto medible que es cuantitativamente determinado por la relación entre la salida útil y la entrada total. Significa un nivel de rendimiento o un estado deseado que proviene del uso de la menor cantidad de insumos, como el tiempo, la energía, los materiales, la mano de obra y el dinero, para lograr la mayor cantidad de producción.

Dentro de esta categoría se identifican 5 KPIs:

- KPI 1: Eficiencia de activos y equipamiento
- KPI 2: Eficiencia de la fuerza de trabajo
- KPI 3: Eficiencia de las utilidades
- KPI 4: Eficiencia del inventario
- KPI 5: Eficiencia de los materiales

Calidad

Los KPIs identificados dentro de esta categoría reflejan el deseo de una empresa de evitar defectos en su trabajo en proceso y en los productos terminados, así como fallas en sus productos después de la entrega del cliente. Buscan asegurarse que un fabricante pueda satisfacer las crecientes demandas

y expectativas de los clientes. Esto se debe a que un excelente rendimiento en estos KPIs no solo refuerza la confianza y la lealtad de los clientes, sino que también reduce los costos asociados con la remanufacturación o sustitución de productos defectuosos. Con el tiempo, esto establece una reputación más fuerte y una marca referente.

Dentro de esta categoría se identifican 4 KPIs:

- KPI 6: Calidad del Proceso
- KPI 7: Calidad del Producto
- KPI 8: *Safety*
- KPI 9: Seguridad

Flexibilidad

Una mayor flexibilidad en las operaciones de fabricación permite al fabricante adaptarse rápidamente a las cambiantes demandas de los consumidores y reducir el tiempo de inactividad en la reconfiguración de las líneas de producción.

Dentro de esta categoría se identifican 3 KPIs:

- KPI 10: Eficacia en la Planificación y en la Programación
- KPI 11: Flexibilidad en la Producción
- KPI 12: Flexibilidad en la fuerza de trabajo

Velocidad

Con el advenimiento de la 4RI, la creciente interconectividad de los sistemas, el auge de las nuevas tecnologías digitales y la analítica avanzada, están proporcionando a las empresas una visión más rica de sus productos, preferencias de los clientes y expectativas del mercado. Esto lleva en algunos casos a tiempos de vida del producto más cortos y a una mayor personalización del producto. El aumento de la velocidad de comercialización permite a un fabricante acceder un grupo más amplio de consumidores y maximizar las ventas.

Dentro de esta categoría se identifican 2 KPIs:

- KPI 13: *Time to Market* (TTM)
- KPI 14: *Time to Delivery* (TTD)

Los Grados de Relevancia (DOR, por su sigla en inglés) reflejan el impacto relativo que cada Dimensión SIRI tiene en un Costo o en una categoría KPI (DOR_C y DOR_K respectivamente). Los tres niveles considerados para DOR, son:

- 0: Insignificante
- 1: Bajo y/o Indirecto
- 3: Alto y/o Directo[1]

Respecto al Factor de Proximidad o sea, a la proximidad a ser *best-in-class*, el concepto se asocia al nivel de rendimiento actual más alto entre los fabricantes, y es el punto de referencia que otras empresas buscan cumplir o superar. Una empresa que sabe qué es lo mejor en su clase, puede identificar lo que es alcanzable, pudiendo fijar un punto de referencia y metas reales. Cuando las empresas saben dónde se encuentran en relación con los mejores de su clase, pueden articular mejor los fundamentos para embarcarse en la transformación en áreas específicas de la Industria 4.0.

Los descriptores de Banda del Índice proporcionan a las empresas amplios detalles para que puedan reconocer el perfil de una instalación de primera clase. Posteriormente, las empresas pueden determinar su proximidad a los mejores de su clase calculando la diferencia entre la Banda promedio de la mejor clase y su propia Banda a través de las 16 Dimensiones del Índice SIRI.

El Factor de Proximidad de una Dimensión SIRI refleja el *gap* entre el estado actual de la empresa y el *Best-in-Class*. Por lo tanto, se calcula como la diferencia entre el AMS y el *Best-In-Class Benchmark* (BIC).

El BIC de una industria se define como el rendimiento promedio del mejor 10 % de las empresas de esa industria, a lo largo de las 16 Dimensiones SIRI. Los creadores del Índice SIRI y la Matriz de Priorización definieron el BIC para 14 industrias, a saber: Aeroespacial, Automotriz, Electrónica, Energía y Química (derivados del petróleo, refinerías), Comidas y Bebidas, Fabricación

[1]El pasaje de 1 a 3 omitiendo el 2, tiene el objetivo de otorgar mayor peso al Factor/Dimensión en consideración.

en general, Logística, Petróleo y Gas (exploración y extracción), Maquinaria y Equipamiento, Tecnología Médica, Farmacéutica, Partes de Precisión, Semiconductores y, Textil, Ropa, Cuero y Calzado.

El trabajo relacionado con la Matriz de Priorización recomienda que se considere un horizonte de planificación de los negocios de la empresa que pondere los 3 factores claves considerados (Costo, KPI y Proximidad), según se presenta en la Tabla 4.1.

Horizonte planificado	**Factor Costo (W_C)**	**Factor KPI (W_K)**	**Factor Proximidad (W_P)**
Estratégico (3 a 5 años)	30 %	40 %	30 %
Táctico (1 a 2 años)	45 %	30 %	25 %
Operacional (3 a 6 meses)	60 %	20 %	20 %

Tabla 4.1: Distribución de ponderaciones según horizonte de planificación

En una consideración muy general, el horizonte Estratégico es referenciado por las MNCs, mientras que por otro lado, las SMEs y organizaciones con presencia regional apuntan al horizonte Táctico. Finalmente, y siempre hablando en términos generales, el horizonte Operacional es adoptado por empresas que tienen la presión de rápidamente obtener retornos financieros.

Por lo tanto y como ya se adelantó, la fórmula de la Matriz de Priorización que se considera es la siguiente:

$$\begin{gathered}\text{Valor de Impacto de la Dimensión SIRI}_i \\ = \\ W_C \text{ x } [DOR_C \text{ x Perfil de Costo}]_i \\ + \\ W_K \text{ x } [DOR_K \text{ x TopKPIs}]_i \\ + \\ W_P \text{ x } [\text{BIC - AMS}]_i\end{gathered}$$

En la Sección 3.5.1 del Apéndice 3 se presenta la Metodología de Cálculo propuesta para determinar el Valor de Impacto de cada Dimensión SIRI.

4.7.7. *Cyber Security Agency of Singapore*

Dicha Agencia [254] tiene la tarea de mantener *safe* y seguro al ciberespacio de dicho país, para así apuntalar la Seguridad Nacional, potenciar la Economía Digital y proteger el Estilo de Vida Digital. Para cumplir con lo anterior, entre otras actividades, es la organización *host* del SigCERT (*Computer Emergency Response Team*), colabora activamente en la elaboración de las leyes que hacen a su Misión, Visión y Objetivos, mantiene diversos programas, planes y publicaciones relacionadas con la *Cyber Safety* y la *Cyber Security*, y con el etiquetado vinculado a dispositivos IoT, entre otros.

La decisión de incluir esta mención a la CSA radica en que su trabajo referencia explícitamente varios de las tecnologías y conceptos que tienen directa relación con esta tesis.

4.8. *Society 5.0*

Japón se encuentra impulsando un plan para una sociedad superinteligente, la denominada Sociedad 5.0 [168] o la "Sociedad de la Imaginación" [275]. Se trata de un concepto de mayor alcance que la 4RI, ya que prevé transformar completamente el estilo de vida japonés al difuminar la frontera entre el ciberespacio y el espacio físico.

El término Sociedad 5.0 pretende fortalecer la existencia de una secuencia de sociedades previas,de la cual será el siguiente paso: Sociedad 1.0 ("Cazadores y Recolectores"), Sociedad 2.0 ("Agricultura"), Sociedad 3.0 ("Industria"), Sociedad 4.0 ("Información"), según se refleja en la Figura 4.18, de la *Japan Business Federation* (*Keidanren*) [166].

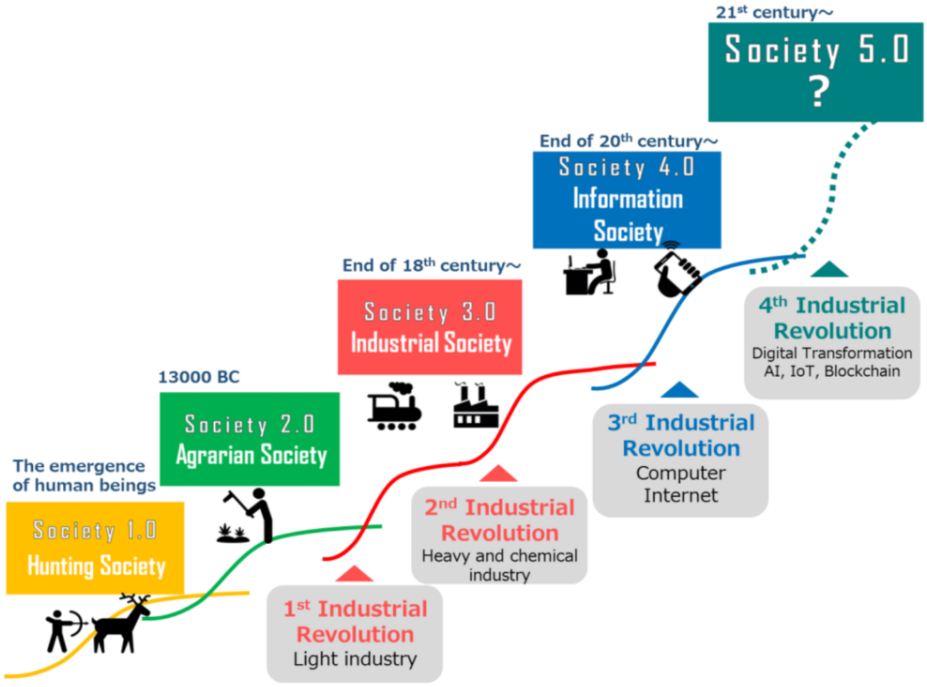


Figura 4.18: Keidanren - Evolución de la Sociedad. Fuente: [166]

Mediante el impulso de la Sociedad 5.0, a la que considera como inevitable y también como una oportunidad, la comunidad nipona impulsa la existencia de un sistema socio-económico sostenible, potenciado por diversas tecnologías, como ser, big data, inteligencia artificial, blockchain, biotecnologías y robótica. Si bien la transición a la Sociedad 5.0 se podría asimilar con la 4IR, la principal diferencia es que la primera hace foco en las personas y en una completa transformación en las forma de vivir. Considerando a las personas como el centro

de toda la transformación, se visualiza que la Sociedad 5.0 y los 17 Objetivos de Desarrollo Sostenible (SDG, según su sigla en inglés) [240, 276], que se pueden apreciar en la Figura 4.19, del Programa de las Naciones Unidas para el Desarrollo (UNDP, por su sigla en inglés), apuntan en la misma dirección [167].

Figura 4.19: PNUD - Objetivos de Desarrollo Sostenible. Fuente: [276]

De acuerdo a la visión que se tiene por parte de quienes impulsan la *Society 5.0*, el mundo está asistiendo a tres cambios importantes: el cambio tecnológico, el cambio económico y geopolítico, y el cambio de mentalidad; ellos se volverán más obvios y acelerados en el futuro. A medida que dichos cambios exacerban la incertidumbre en el mundo, también aumenta la sensación de inseguridad. Sin embargo, cada cambio también trae oportunidades y por ello, la Sociedad de la Imaginación, la Sociedad Creativa, es la clave para co-crear el futuro.

La Sociedad 5.0, comparada con la Sociedad 4.0, y según se muestra en las Figuras 4.20 y 4.21 obtenidas de [168], estará caracterizada por la resolución de los problemas, la creación de valor, la diversidad, la descentralización, la resiliencia, la sostenibilidad y la armonía con el medioambiente.

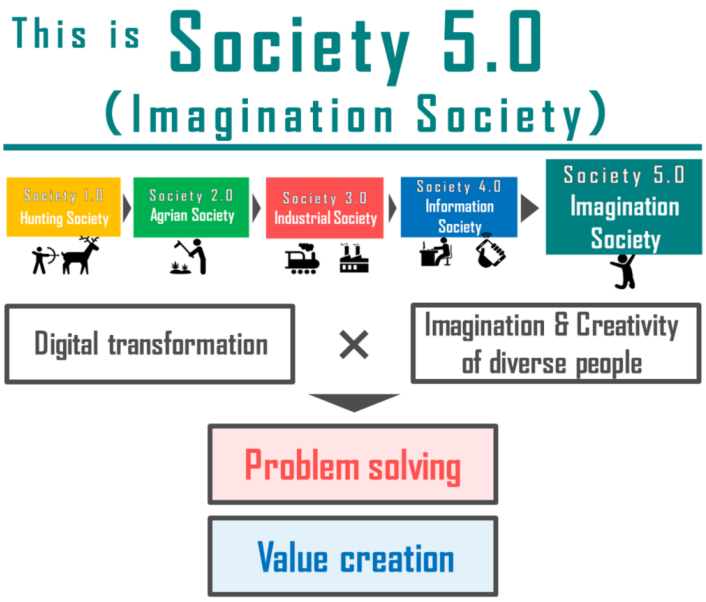


Figura 4.20: Sociedad 5.0 - Resolver Problemas y Crear Valor. Fuente: [166]

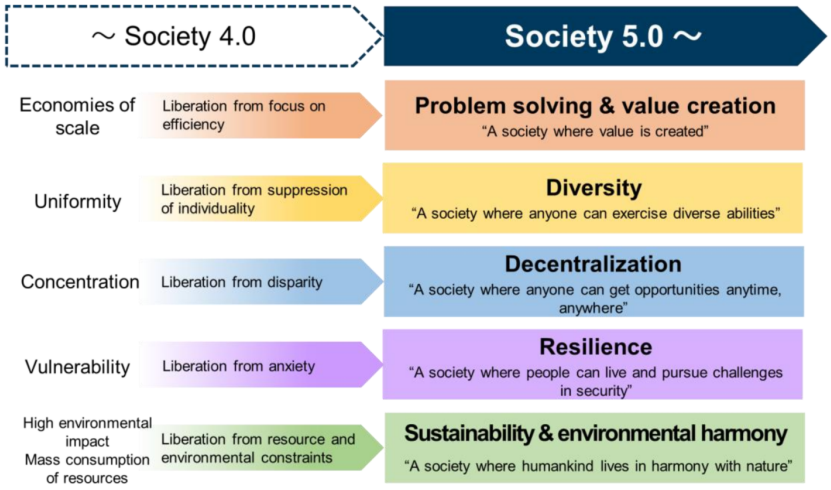


Figura 4.21: Sociedad 4.0 - Sociedad 5.0. Fuente: [166]

4.9. China

En esta sección se referencia a 2 trabajos vinculados a la temática, ambos impulsados por el gobierno chino. Dichas iniciativas se han ido complementando con otras que son mencionadas en la próxima y última sección del capítulo.

4.9.1. *Industrial Internet Architecture*

La elaboración del reporte *Industrial Internet Architecture* [6], publicado por la *Alliance of Industrial Internet* [32], estuvo a cargo de representantes de diversas organizaciones de China; el trabajo fue guiado por el *Ministry of Industry and Information Technology* (MIIT) y liderada por la *China Academy of Information and Communications Technology* (CAICT) [33]. La versión final del reporte (1.0), que tomó además como insumo la opinión de representantes de empresas, organizaciones y expertos de todo el mundo, se liberó en el año 2016 siendo sus autores e impulsores plenamente conscientes que se está frente a un documento referencial que sirve como guía para los diferentes ejes de trabajo que abarca el concepto Internet Industrial, a sabiendas de la inmadurez que existía y existe respecto a todo lo que implica dicho concepto.

Si bien tanto por el origen del mismo como por su contenido, se podría considerar como otra fuente referencial fundacional en la temática, los diferentes temas abordados son los mismos a los considerados en el conjunto de las referencias tenidas en cuenta en los capítulos anteriores del presente documento, por lo que su consideración podría aportar un enfoque o visión ligeramente distinto; dada la necesidad de acotar el presente trabajo, finalmente no fue incluido, lo que a juicio del autor no significa que no pueda llegar a ser considerado en un futuro. Es de destacar que la versión vigente sigue siendo la misma, y que no se identificaron iniciativas de actualización ni de su consideración de manera activa e intensa por parte del resto de la comunidad.

4.9.2. *National Intelligent Manufacturing Standard System Construction Guidelines*

El documento *National Intelligent Manufacturing Standard System Construction Guidelines*, publicado en el año 2015 [35], merece similares consideraciones a las puesta de manifiesto en el apartado anterior para la publicación *Industrial Internet Architecture*.

4.10. Otras iniciativas para el impulso de la Industria 4.0

En esta sección se brinda una lista de países y nombres de iniciativas nacionales tendientes a fomentar la Industria 4.0. Se complementa ello con la mención a diversos acuerdos multilaterales entre países y organizaciones, con el mismo objetivo. Si bien la enumeración no pretende ser taxativa, se explicitan las que están asociadas a países en su mayoría del primer mundo y que están siendo líderes en la temática, habiendo validado ésto mediante referencias y menciones cruzadas. En todos los casos, se acompaña con la/s referencia/s que permiten ahondar en la información respecto a cada una de las iniciativas.

4.10.1. Iniciativas identificadas

En el caso concreto de Europa, se identifican numerosas iniciativas nacionales, la mayoría de las cuales se encuentran referenciadas en [69].

Los países y las principales referencias a sus iniciativas son las indicadas en la Tabla 4.2.

País	Iniciativa	Referencia/s
Austria	Plattform Industrie 4.0	[14]
Bélgica	Made Different	[18]
Dinamarca	Manufacturing Academy of Denmark (MADE)	[50]
Eslovaquia	Industry4UM	[66]
Eslovenia	Digital Coalition	[67]
España	Industria Conectada 4.0	[68]
Francia	Industrie du futur	[72]
Hungría	IPAR 4.0 NTP (Industry 4.0 National Technology Platform)	[80]
Italia	Transizione 4.0	[163]
Lituania	Pramonė 4.0	[173]
Países Bajos	Smart Industry	[207]
Portugal	Indústria 4.0	[241]
Reino Unido	Digital Catapult	[243]
República Checa	Průmysl 4.0	[244]
Suecia	Produktion2030 (P2030)	[264]
Australia	Prime Minister's Industry 4.0 Taskforce	[13]
Nueva Zelanda	Industry 4.0 Hub	[200]
China	China Manufacturing 2025 - Internet + Collaborative Manufacturing	[33, 32, 36, 34]
Corea del Sur	I-KOREA 4.0	[41]
India	SAMARTH Udyog Bharat 4.0	[131, 130]
Indonesia	Making Indonesia 4.0	[132]
Israel	Industry 4.0	[162]

Tabla 4.2: Países e Iniciativas de Transformación digital

Existen además múltiples acuerdos multilaterales entre diferentes países y organizaciones con el objetivo de compartir experiencias y buscar caminos en común y sinergia para el desarrollo de la Industria 4.0, estando disponibles algunas de ellas en [225, 228, 211, 217, 218, 213, 212, 214, 215, 12, 216, 219, 119].

4.10.2. América Latina y el Caribe

En el caso de América Latina y el Caribe (ALC), se investigó respecto a iniciativas nacionales al respecto, en lo siguientes países: Argentina, Brasil, Chile, Colombia, México y Uruguay. En ninguno de ellos se identificó alguna estrategia con el mismo espíritu que las identificadas en los países de otras regiones mencionados. Ello no significa que no existan distintas inquietudes e iniciativas en diferentes organizaciones y actores sociales de ALC pero, por lo menos hasta ahora, sin una visión integral, sin una participación de todas las partes interesadas, o al menos la mayoría, y sin un plan de acción concreto para los próximos años.

Capítulo 5

Propuesta de adopción de la Industria 4.0

En este capítulo se presenta la propuesta de adopción de la Industria 4.0, con énfasis en la confiabilidad, objetivo del presente trabajo.

La presentación de la propuesta se estructura de la siguiente manera: en primer lugar se aborda el contexto mundial, regional y nacional respecto a las condiciones necesarias para una adopción exitosa de la Industria 4.0. Luego se presenta la propuesta de adopción, brindando en primer lugar una recomendación de uso de las diferentes referencias abordadas en el estudio del estado del arte, para proseguir con una enumeración de las Partes Interesadas y el rol que debería asumir cada una de ellas, continuando con la presentación del Modelo de Madurez en Confiabilidad (TMM, por su sigla en inglés) creado, que plasma en la propuesta el énfasis pretendido para la misma, para culminar con la propuesta de adopción propiamente, la que se acompaña de un Diagrama de Flujo que se proporciona como guía para su aplicación. Finalmente se presenta la aplicación de la propuesta a un ejemplo teórico de caso de uso.

5.1. El contexto mundial, regional y nacional

El estudio del Estado del Arte realizado con motivo del presente trabajo permitió confirmar que, la adopción exitosa de la Industria 4.0 por parte de una organización, se verá notoriamente facilitada si a nivel del país o región de influencia de la misma existe una estrategia al respecto claramente definida y en marcha, que involucre adecuadamente a todas las partes interesadas.

Por otro lado, no podemos desconocer que se ha comprobado empíricamente como ser con la experiencia de Singapur ("*Smart Nation*") en lo que refiere a la dificultad para definir una hoja de ruta de adopción de la Industria 4.0, y el despliegue de numerosos *testbed* asociados, o con los modelos referenciados en el Estado del Arte, las implementaciones amplias, concretas y en marcha de la Industria 4.0 todavía no han alcanzado el nivel de madurez deseado.

No podemos desconocer que la pandemia declarada este año debido a la COVID-19 y todavía vigente, ha inmerso a todos los países, sus sociedades, economías y culturas, en un realidad ni conocida ni imaginada, con la incertidumbre de saber cuál será la situación en los próximos meses y quizás años, tanto a nivel global, regional y de cada país, y desconociendo además cómo irá impactando en las evoluciones asociadas a la Industria 4.0. Se vislumbra que las distintas comunidades experimentarán diferentes grados de avance y adopción de la Industria 4.0 (con y sin pandemia), los que estarán fuertemente condicionados por las realidades económicas financieras, sociales y sanitarias (durante y post pandemia), sin desconocer que esas mismas realidades pueden acelerar adopciones, aunque sea parciales, que en otra situación podría dilatarse más en el tiempo [174, 71, 290, 222, 99, 115, 283].

Por otro lado, siendo ya una realidad que la 4IR significará un cambio que impactará en lo económico, en lo social y en lo cultural (en algunos casos, ya resulta tangible), resulta indispensable que cada país disponga y aplique una estrategia de adopción de la Industria 4.0, mediante lo que debería ser una política de estado.

En todos los casos de éxito identificados, con las variantes propias de cada realidad, incluso hasta culturales, existe una estrategia definida y en marcha, liderada por el gobierno de turno, pero con la fuerza de ser una política de estado. En la mayoría de los casos, se tratan de acciones coordinadas que están en marcha hace más 5 años, y que son ajustadas periódicamente con planes estratégicos ya definidos para los próximos 5 o 10 años.

Como se expresó al momento de documentar en el presente trabajo las distintas iniciativas para el impulso de la Industria 4.0, disponible en la Sección 4.10 del Capítulo 4, en el caso concreto de América Latina y el Caribe (sección 4.10.2), no se identificaron estrategias claras a nivel de los países para la adopción de la Industria 4.0. Como también se aclaró, ello no significa que no existan distintas inquietudes e iniciativas en diferentes organizaciones y actores sociales, pero sin la adecuada sinergia de todas las partes interesadas, sin un plan concreto, y sin el estado actuando como "sponsor", facilitador e impulsor de las acciones que han ido demostrando ser necesarias e imprescindibles; en ese contexto la suma de esfuerzos no será suficiente, y puede terminar desalentando las iniciativas fragmentadas; de ser así, los países de la región se verán rezagados respecto a la mayoría del resto de los países de otras regiones, en una tendencia peligrosa que ya se ha puesto de manifiesto en otros ámbitos tal como se indica por ejemplo en el Reporte *Doing Business 2020* del Banco Mundial [271]: "*las economías del África subsahariana y de América Latina y el Caribe siguen estando rezagadas en términos de reformas. Sólo dos economías del África subsahariana se sitúan entre las 50 primeras* (nota del autor de este trabajo: de un total de 190 países) *en la facilidad para hacer negocios; ninguna economía latinoamericana se posiciona en este grupo*" (sic). Esta es una muestra de las dificultades que habrá que sortear para impulsar la adopción de la Industria 4.0 en la región, ya que nada indica que sea una opción aceptable el no hacerlo.

Una consideración especial merece el factor tiempo. Las iniciativas vinculadas a la Industria 4.0 evaluadas a lo largo del trabajo existen desde hace bastante tiempo: entre 5 y 10 años. No podemos desconocer que la curva de aprendizaje que se han recorrido y las lecciones aprendidas generadas, permitirían acortar el tiempo de adopción de la Industria 4.0 en una realidad como la nuestra. A pesar de ello, existe un aspecto fundamental demandando que lo antes posible se ponga en marcha, para no dilatar más comenzar con dicha adopción: la formación de los ciudadanos en la Industria 4.0 y tecnologías vinculadas. En lo que refiere a la formación, algunos tiempos están impuestos por la propia esencia de la educación de las personas, y en algunos casos, la posibilidad de acortar tiempos resulta muy difícil. Cuanto antes se comience a recorrer el camino de la formación, antes estarán mejor preparados los ciudadanos y el país para los desafíos que implica la inevitable adopción en tiempo y forma 4IR.

En el caso de nuestro país y de acuerdo a los datos disponibles en el Informe de la Evolución de los Cotizantes [25] en su edición del año 2020 (con datos hasta el 2019) elaborado por el BPS, el 49,9 % de las empresas del sector privado (de un total de 206.710 para el año 2019) pertenecen al segmento de Mipymes[1] [2] y un 49,6 % corresponde a empresas del tipo "Patrón sin dependiente" (unipersonal). El 0,5 % restante atañe a empresas grandes.

En cuanto a la distribución de los puestos de trabajo por tamaño de empresa del sector privado en el Uruguay, y de acuerdo al mismo informe, las Mipymes ocupan el 58,9 % de los mismos[3] (de un total promedio mensual año para el 2019 de 1.015.852), mientras que a las unipersonales les atañe el 9,6 %, correspondiendo el 31,5 % restante a las empresas grandes.

[1] Se define microempresa a aquella que ocupa no más de 4 personas, pequeñas a las que ocupan no más de 19, medianas hasta 99 y grandes aquellas de 100 o más personas ocupadas, con consideraciones además de topes de ventas anuales -aspecto cuya consideración excede al presente trabajo- según Decreto N° 504/007 [128].

[2] Distribuyéndose de la siguiente forma: 33,6 % de empresas micro, 13,5 % de empresas pequeñas y 2,8 % de medianas empresas.

[3] Distribuyéndose de la siguiente forma: 15,7 % en las empresas micro, 22,2 % en las empresas pequeñas y 21,0 % en las medianas empresas.

5.2. La propuesta de adopción

5.2.1. Las referencias del Estado del Arte como insumo

A continuación se proponen los siguientes puntos focales identificados como la primera consideración a contemplar para cada uno de las referencias fundamentales abordadas en los Capítulos dedicados al estudio del estado del arte (Capítulos 2, 3 y 4), así como también en los Apéndices vinculados (Apéndices 1, 2 y 3).

El modelo de referencia RAMI 4.0 impulsado y desarrollado por la *Plattform Industrie 4.0*, pionera en el concepto *Industrie 4.0*, es una excelente referencia para todo análisis que hace a la fabricación, el ciclo de vida de los productos y la logística asociada. Por otro lado, el intenso trabajo y los importantes avances que se identifican en torno al concepto de *Asset Administration Shell* (AAS) hace que sea una referencia ineludible al momento de considerar la gestión de los activos (en su concepción más amplia). Finalmente, pero no por ello resulta menos importante, las continuas alianzas de trabajos que se realizan con organizaciones similares de otros países, están generando sinergias que a tener en cuenta al momento de considerar otras tecnologías, como por ejemplo robótica, considerando el trabajo conjunto con el RRI de Japón, y la relevancia de ser una de las fuentes para el desarrollo del Índice SIRI y la Matriz de Priorización de Singapur.

La Arquitectura de Referencia IIRA elaborada por el IIC, así como otros documentos referenciales impulsados por el consorcio (en concreto el IISF y el SMM) se identifican como fundacionales al momento de un análisis exhaustivo de los sistemas de la Internet Industrial, donde se contempla la necesaria interacción entre el negocio y la operación, y el especial énfasis en lo que refiere a la seguridad. El IIC ha sido fuerte impulsor del concepto de confiabilidad (*trustworthiness*), el cual ya ha sido adoptado por organizaciones similares, al haber identificado su relevancia para la adopción de la Industria 4.0. Por otro lado, el concepto de *Digital Twin*, si bien ya conocido desde hace varios años, ha cobrado gran relevancia en los últimos tiempos y el IIC se encuentra trabajando fuertemente para aprovechar todo su potencial, incluso a través de identificar la enorme cantidad de puntos en común que tiene con el AAS. Es de destacar que el trabajo del IIC relativo a la confiabilidad fue el que inspiró a la temática de esta tesis.

El trabajo llevado adelante por ENISA ha puesto a disposición de la comunidad un excelente material de referencia al momento de requerir Taxonomías de Activos y de Amenazas, así como también Buenas Prácticas a considerar a la hora de dotar de seguridad a los dispositivos IoT. Para ello ENISA abordó 2 escenarios: Infraestructuras Críticas de Información (CII) y Fabricación Inteligente.

En cuanto al NIST, su *Framework* de Ciberseguridad resulta una referencia fundamental, considerando además que se trata de una de las fuentes principales para la elaboración del Marco de Ciberseguridad de AGESIC.

Con respecto al IETF, brinda aportes significativos en cuanto a las consideraciones más relevantes vinculadas con el ciclo de vida de los dispositivos IoT y el MUD.

Internet Society focaliza fuertemente sus trabajos en la participación activa de diversas partes interesadas, y en particular de los ciudadanos, por lo que resulta una referencia ineludible al momento de que las mismas entran en consideración.

Las publicaciones elaboradas por la IoTSF ofrecen un conjunto muy amplio de aspectos a considerar a la hora de analizar la seguridad en el contexto de IoT, por lo que resultan una referencia muy atractiva por lo abarcativa de la misma.

Smart Nation, y en particular el Índice SIRI y la Matriz de Priorización significan un aporte muy completo y con sustento empírico que hace parte de la propuesta que aquí se presenta.

La Society 5.0 hace especial énfasis en cómo cada acción aporta a los Objetivos de Desarrollo Sostenible de las Naciones Unidas, por lo que al momento de su consideración en la propuesta, resulta una referencia fundamental.

5.2.2. Partes interesadas

En esta sección se aborda para cada una de las Partes Interesadas, los aspectos más relevantes a considerar a la hora de impulsar y sustentar la adopción de la Industria 4.0.

Al momento de identificar las Partes Interesadas, su importancia y sus necesidades al respecto, se propone considerar los siguientes grupos:

- Gobierno Nacional (y Gobiernos Locales)
- Industrias
- Proveedores
- Trabajadores
- Ciudadanos
- Organizaciones reguladoras
- Comunidad de estandarización
- Centros de Formación
- Centros de investigación, desarrollo e innovación

A continuación, para cada una de las Partes Interesadas, se brinda un resumen de los aspectos sustanciales que deben impulsar para la adopción de la Industria 4.0, en función de su rol en la sociedad.

Gobierno Nacional (y Gobiernos Locales)

Establecer el ámbito adecuado para convocar a todos las partes interesadas a los efectos de elaborar y mantener un Plan Estratégico Nacional de Adopción de la Industria 4.0, con carácter de política de estado.

Elaborar las leyes, regulaciones y reglamentaciones que brinden el marco necesario para una adecuada adopción del Plan Estratégico Nacional por parte de toda la sociedad, para el beneficio de todas las partes interesadas.

Ser el *sponsor*, facilitador e impulsor de todas las actividades que resulten del trabajo, del rol y las necesidades de todas las partes interesadas.

Impulsar en todas las partes interesadas actividades "customizadas" de concientización y sensibilización respecto a los beneficios de adoptar la Industria 4.0.

Articular en todo momento y de manera eficaz y eficiente los vínculos y necesidades de todas las partes interesadas.

Crear grupos de trabajo, verticales y horizontales, adecuadamente articulados, que involucren a todas las partes interesadas.

Considerar las acciones a emprender en el marco del Plan Estratégico Nacional contemplando siempre cómo impacta en los Objetivos de Desarrollo Sostenible del Programa de Desarrollo de las Naciones Unidas.

Fomentar en todo momento el espíritu crítico y participativo de todas las partes interesadas.

Realizar un seguimiento de las actividades que hacen al Plan Estratégico Nacional, mediante el uso de indicadores, a los efectos de concretar en los ámbitos adecuados, mejoras al mismo.

Fomentar la creación de *testbeds*.

Brindar beneficios tributarios y otras facilidades (económicas, financieras, logísticas) para la adopción de la Industria 4.0.

Monitorizar la realidad regional e internacional, identificando oportunidades de mejora al Plan. El enfoque propuesto implica mantener siempre activos al menos los siguientes ejes de observación y análisis: financiero, económico, cultural, social, negocio, medio ambiental, político y tecnológico.

Convocar a autoridades de gobiernos locales (departamentales, alcaldías) a que se sumen al desafío, enriqueciendo el Plan desde las óptica de sus realidades locales.

Bregar siempre para que el Plan Estratégico Nacional tenga como premisas la transparencia, la gestión de datos abiertos y el bienestar de los ciudadanos.

Industrias

Las industrias, las cámaras y asociaciones que las engloban, según las verticales del negocio, deben elaborar un Plan de Adopción de la Industria 4.0, sustentado en el Plan Estratégico Nacional correspondiente.

Identificar las flexibilidades necesarias en cada una de las verticales, según las realidades de cada empresa, para que cada una recorra "a su ritmo" el Plan de Adopción correspondiente.

Conocer, considerar y respetar las leyes, regulaciones, reglamentaciones, estándares y mejores prácticas, respecto a la Industria 4.0, que aplican a su ámbito de acción.

Considerar las experiencias y lecciones aprendidas de iniciativas similares en otros lugares.

Fomentar en sus trabajadores diversas actividades de formación necesaria para la adopción de la Industria 4.0.

Participar de los *testbeds* vinculados a su vertical de negocio.

Considerar su vínculo en el resto de las partes interesadas, para el beneficio de todos.

Contemplar los eventuales vínculos de negocio con partes interesadas de otros países, y sus realidades.

Realizar un seguimiento de las actividades que hacen al Plan de Adopción, mediante el uso de indicadores, a los efectos de concretar en los ámbitos adecuados, mejoras al mismo.

Proveedores

Los proveedores, las cámaras y asociaciones que las engloban, según las verticales del negocio, deben elaborar un Plan de Adopción de la Industria 4.0, sustentado en el Plan Estratégico Nacional.

Identificar las flexibilidades necesarias en cada una de las verticales, según las realidades de cada empresa, para que cada una recorra "a su ritmo" el Plan de Adopción correspondiente.

Conocer, considerar y respetar las leyes, regulaciones, reglamentaciones, estándares y mejores prácticas, respecto a la Industria 4.0, que aplican a su ámbito de acción.

Considerar las experiencias y lecciones aprendidas de iniciativas similares en otros lugares.

Fomentar en sus trabajadores diversas actividades de formación necesaria para la adopción de la Industria 4.0.

Participar de los *testbeds* vinculados a su vertical de negocio.

Considerar su vínculo en el resto de las partes interesadas, para el beneficio de todos.

Contemplar los eventuales vínculos de negocio con partes interesadas de otros países, y sus realidades.

Realizar un seguimiento de las actividades que hacen al Plan de Adopción, mediante el uso de indicadores, a los efectos de concretar en los ámbitos adecuados, mejoras al mismo.

Trabajadores

Participar de las actividades de formación vinculadas con su área laboral.

Considerar la reconversión en cuanto a horarios, tareas y condiciones laborales que conlleva la adopción de la Industria 4.0, como oportunidades de

mejora y bienestar, sin que ello menoscabe derechos adquiridos por ninguna de las partes involucradas.

Contemplar la necesidad de estar preparados para la dinámica en las tareas desarrolladas y todo lo que se derive de la innovación en los procesos de producción y del negocio.

Conocer, considerar y respetar las leyes, regulaciones, reglamentaciones, estándares y mejores prácticas, respecto a la Industria 4.0, que aplican a su ámbito de acción.

Considerar su vínculo en el resto de las partes interesadas.

Tener presente las experiencias y lecciones aprendidas de iniciativas similares en otros lugares.

Considerar su vínculo en el resto de las partes interesadas, para el beneficio de todos.

Contemplar los eventuales vínculos de negocio con partes interesadas de otros países, y sus realidades.

Ciudadanos

Preservar la privacidad de la información vinculada a todos los ciudadanos, y que siempre sea verificable la misma, considerando la misma como un derecho a ser respetado en todos los ámbitos.

Como consumidores, exigir la transparencia en cuanto a la gestión de los datos que los involucra en función de los servicios que utiliza.

Como consumidores, conocer, considerar y respetar las leyes, regulaciones, reglamentaciones, estándares y mejores prácticas, respecto a la Industria 4.0, que aplican a su rol.

Demandar la adecuada formación para los nuevos perfiles laborales que resultan de la adopción de la Industria 4.0 y su posterior evolución.

Instar siempre por el bienestar de todos los ciudadanos.

Considerar su vínculo en el resto de las partes interesadas, para el beneficio de todos.

Tener presente las experiencias y lecciones aprendidas de iniciativas similares en otros lugares.

Contemplar los eventuales vínculos con partes interesadas de otros países, y sus realidades.

Organizaciones reguladoras

Participar de las actividades de formación vinculadas con su área laboral.

Colaborar en la elaboración de las leyes, regulaciones y reglamentaciones que brinden el marco necesario para una adecuada inserción en toda la sociedad, tanto del Plan Estratégico Nacional como de los diferentes Planes de Adopción.

Conocer, considerar y respetar las leyes, regulaciones, reglamentaciones y mejores prácticas, respecto a la Industria 4.0, que aplican a su ámbito de acción.

Considerar su vínculo en el resto de las partes interesadas, para el beneficio de todos.

Tener presente las experiencias y lecciones aprendidas de iniciativas similares en otros lugares.

Contemplar los eventuales vínculos con partes interesadas de otros países, y sus realidades.

Regular conforme a los beneficios de las partes interesadas, asegurando los derechos y el bienestar de todos los ciudadanos.

Comunidad de estandarización

Participar en la elaboración de estándares y mejores prácticas, o en la mejora de los mismos, sin que necesariamente ello implique lograr la unanimidad, pero sí el consenso.

Participar de las actividades de formación vinculadas con su área laboral.

Conocer, considerar y respetar las leyes, regulaciones, reglamentaciones y mejores prácticas, respecto a la Industria 4.0, que aplican a su ámbito de acción.

Considerar su vínculo en el resto de las partes interesadas, para el beneficio de todos.

Tener presente las experiencias y lecciones aprendidas de iniciativas similares en otros lugares.

Contemplar los eventuales vínculos con partes interesadas de otros países, y sus realidades.

Trabajar en estándares y buenas prácticas conforme a los beneficios de las partes interesadas, asegurando los derechos y el bienestar de todos los ciudadanos.

Centros de Formación (y autoridades correspondientes)

Disponer de un Plan de Formación que permita concientizar, sensibilizar, educar y entrenar a todos los ciudadanos, en la temática de la Industria 4.0 y tecnologías vinculadas, durante toda la vida. El Plan de Formación debe ser lo suficientemente abarcativo para contemplar los diferentes niveles de la educación de los ciudadanos (inicial, primaria, secundaria, terciaria, maestría, doctorado, post-doctorado y técnica) y lo suficientemente flexible para, tanto el plan como los ciudadanos puedan adaptarse a la dinámica intrínseca a la Industria 4.0 y a las tecnologías vinculadas[1].

Impulsar la educación STEAM (*Science, Technology, Engineering, Art and Math*)[2].

Elaborar un Plan de Formación de Formadores, para cada uno los niveles de educación, contemplando la necesidad de recurrir al apoyo extranjero.

Implantar el Plan de Formación de Formadores.

Realizar un seguimiento de las actividades que hacen al Plan de Formación de Formadores, mediante el uso de indicadores, a los efectos de concretar en los ámbitos adecuados, mejoras al mismo.

Elaborar los Programas Educativos para cada uno de los niveles de educación de los ciudadanos.

Implantar los Programas Educativos elaborados.

Realizar un seguimiento de las actividades que hacen a los Programas Educativos, mediante el uso de indicadores, a los efectos de concretar en los ámbitos adecuados, mejoras al mismo.

Impulsar un Plan de Formación de Asesores referentes en la Industria 4.0 y en las tecnologías vinculadas, y asociado a un Plan de Retención de Talentos. Estos expertos pueden acompañar asesorando a las diferentes partes interesadas a adoptar adecuadamente la Industria 4.0 y las tecnologías vinculadas.

Realizar un seguimiento de las actividades que hacen a los Planes de Formación de Asesores y de Retención de Talentos, mediante el uso de indicadores, a los efectos de concretar en los ámbitos adecuados, mejoras a los mismos.

Impulsar un Plan de Formación de Auditores vinculados a la Industria 4.0.

Realizar un seguimiento de las actividades que hacen al Plan de Formación de Auditores, mediante indicadores, a los efectos de concretar en los ámbitos

[1]Una posible referencia al respecto son los resultados del proyecto identificado como "*Universities of the Future*" [277].

[2]Considerando el artículo de Bernard Marr denominado "*We Need STEAM, Not STEM Education, To Prepare Our Kids For The 4th Industrial Revolution*" [171].

adecuados, mejoras al mismo.

Conocer, considerar y respetar las leyes, regulaciones, reglamentaciones y mejores prácticas, respecto a la Industria 4.0, que aplican a su ámbito de acción.

Considerar su vínculo en el resto de las partes interesadas, para el beneficio de todos.

Tener presente las experiencias y lecciones aprendidas de iniciativas similares en otros lugares.

Contemplar los eventuales vínculos con partes interesadas de otros países, y sus realidades.

Centros de investigación, desarrollo e innovación

Fomentar la investigación en Industria 4.0 y tecnologías vinculadas.

Impulsar los desarrollos relacionados con la Industria 4.0 y tecnologías vinculadas.

Estimular los centros de innovación vinculados a la temática.

Posicionarse como centros de referencia para la Industria 4.0 y tecnologías vinculadas.

Instar a la creación de *testbeds*.

Conocer, considerar y respetar las leyes, regulaciones, reglamentaciones y mejores prácticas, respecto a la Industria 4.0, que aplican a su ámbito de acción.

Considerar su vínculo en el resto de las partes interesadas, para el beneficio de todos.

Tener presente las experiencias y lecciones aprendidas de iniciativas similares en otros lugares.

Contemplar los eventuales vínculos con partes interesadas de otros países, y sus realidades.

5.2.3. Modelo de Madurez en Confiabilidad

Habiéndose identificado a lo largo del trabajo la relevancia de la confiabilidad por ser una de las claves para el éxito en la adopción de la Industria 4.0, el centro de la propuesta es, partir del Modelo de Madurez en Seguridad (SMM) elaborado por el IIC [113, 121] y extenderlo a la confiabilidad, creando así un Modelo de Madurez en Confiabilidad (TMM, por su sigla en inglés). Para ello, se tomó como base el contenido del artículo *Extending the IIC IoT Security Maturity Model to Trustworthiness* [107] del IIC, al cual se le realizaron algunos cambios leves en los nombres de algunos Dominios, Subdominios y Prácticas, y fundamentalmente algunos agregados, como se verá más adelante.

Sumado a lo anterior, el trabajo asociado al Índice SIRI [257] y a la Matriz de Priorización [255], enriquece la propuesta del TMM en dos aspectos fundamentales: la definición de un conjunto de KPIs que han sido validados empíricamente y, también en base a la experiencia desarrollada en Singapur, la necesidad del concepto de Matriz de Priorización a los efectos de determinar por dónde y cómo comenzar a implantar la Industria 4.0.

El trabajo para elaborar la propuesta que aquí se presenta consistió entonces en, a partir del contenido del documento *Extending the IIC IoT Security Maturity Model to Trustworthiness*, y en particular, del diagrama de la Figura 3.22 ("Modelo SSM revisado y extendido para *trustworthiness*") disponible en el Capítulo 3, se elaboró el diagrama de *Trustworthiness Maturity Model* (TMM) que se observa en la Figura 5.1, el cual refleja el conjunto de Dominios, Subdominios y Prácticas propuesto.

Respecto al "Modelo SSM revisado y extendido para *trustworthiness*" [107], los cambios de nombres relevantes, y los agregados realizados para obtener el TMM propuesto, son los siguientes:

- Se considera la Práctica "Gestión del Programa de Confiabilidad", en lugar de "Gestión del Programa de Seguridad"
- Se incorpora la Práctica "Medidas"
- Se incorpora la Práctica "Métricas e Indicadores"
- Se incorpora la Práctica "Identificación e Impacto Interno"
- Se incorpora la Práctica "Impacto Externo"
- Se incorpora la Práctica "Desarrollo"
- Se incorpora la Práctica "Gestión del Capital Humano"
- Se incorpora la Práctica "Aprendizaje"

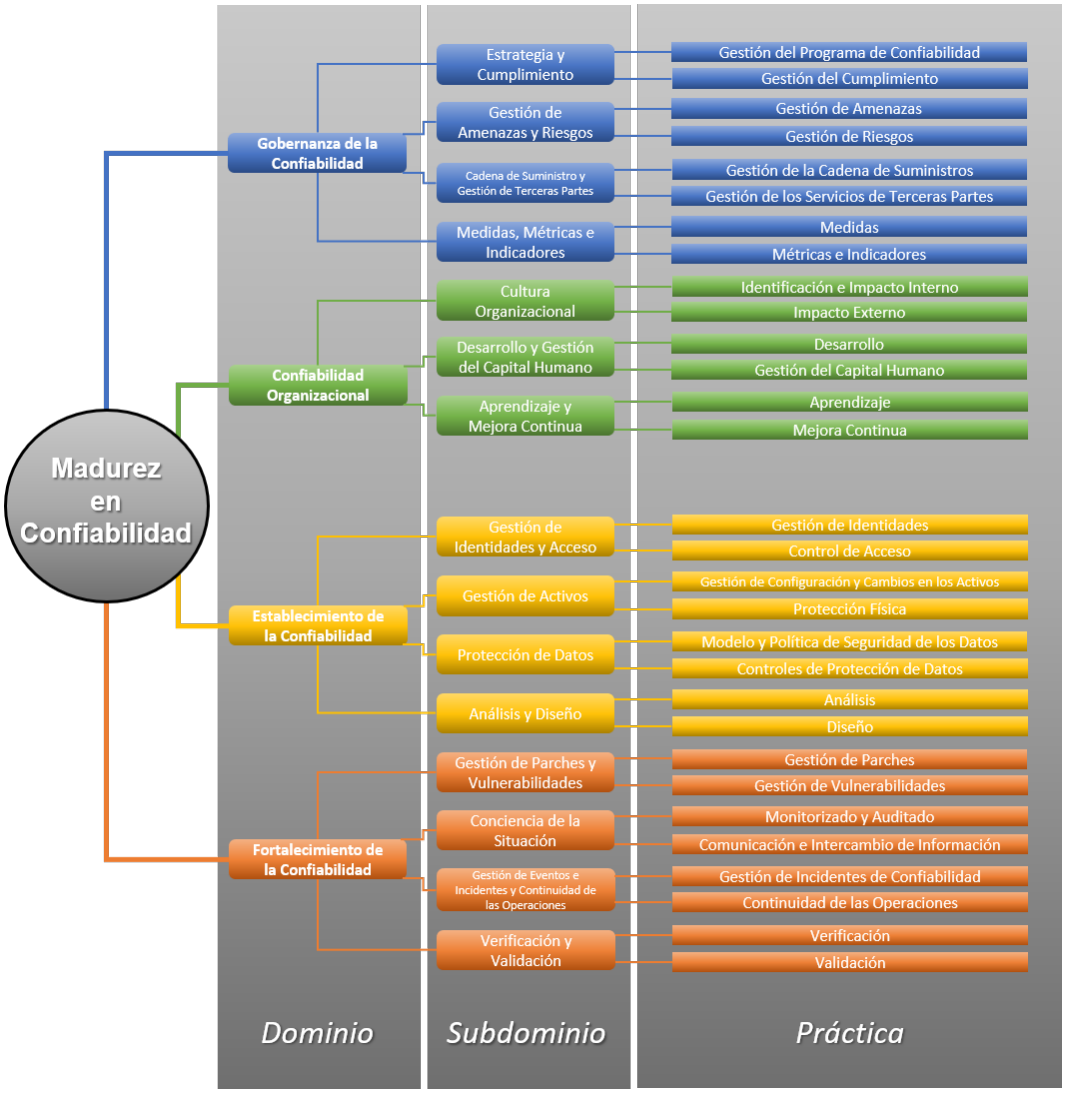


Figura 5.1: *Trustworthiness Maturity Model* (TMM)

- Se incorpora la Práctica "Mejora Continua"
- Se incorpora la Práctica "Análisis"
- Se incorpora la Práctica "Diseño"
- Se considera la Práctica "Monitorizado y Auditado" en lugar de la Práctica "Monitorizado"
- Se considera la Práctica "Gestión de Incidentes de Confiabilidad", en lugar de la Práctica "Detección de eventos y Plan de Respuesta"
- Se considera la Práctica "Continuidad de las Operaciones", en lugar de la Práctica "Remediación, Recuperación y Continuidad de Operaciones"
- Se incorpora la Práctica "Verificación"

- Se incorpora la Práctica “Validación”

Continuando con la Propuesta, luego de la evaluación realizada de acuerdo al mecanismo de uso del SMM elaborado por el IIC, se podrá identificar en qué aspectos hay distancias entre el estado actual y el estado deseado u objetivo.

Guías de Objetivos, Necesidades y Propósitos

Como se documentó en la Sección 3.6.2 del Capítulo 3, en el artículo *IoT Security Maturity Model: Description and Intended Use* [121] del IIC se proporciona una guía de los objetivos típicos a cumplir en cada Dominio del SMM (Gobernanza, Establecimiento y Fortalecimiento) en cada Nivel de Exhaustividad. Acompañando a dicha guía, el artículo proporciona también una guía de las necesidades para cada uno de los Subdominios, para cada Nivel del Exhaustividad. En un tercer y último nivel de granularidad, se ofrece la finalidad (o propósito) de cada Práctica, también para cada Nivel de Exhaustividad (1. Mínimo, 2. *Ad Hoc*, 3. Consistente y 4. Formalizado).

Como parte de la propuesta de este trabajo, y en la misma línea de la referencia citada en el párrafo anterior, se elaboró una guía de definición (o redefinición) de Objetivos (para cada uno de los Dominios), Necesidades (para cada uno de los Subdominios) y Propósitos (para cada una de las Prácticas), en función de los Niveles de Exhaustividad, y adaptadas al Modelo de Madurez en Confiabilidad propuesto.

Dicha guía se encuentra disponible en la Sección 4.1 del Apéndice 4. Dado lo extenso de este detalle se decidió ponerlo a disposición en un Apéndice del documento, sin que ello signifique que no sea parte sustancial de la propuesta.

Aspectos a considerar en cada Práctica

Para cada uno de las 30 Prácticas que componen el TMM, se elaboró un detalle con las consideraciones que se entienden necesarias para realizar una evaluación exhaustiva de cada una de ellas.

Dado lo extenso de este detalle, el mismo se encuentra disponible en la sección 4.2 del Apéndice 4, y nuevamente, sin que ello signifique que no sea parte sustancial de la propuesta.

5.2.4. La Propuesta

La propuesta considera que existe un Plan Estratégico Nacional de Adopción de la Industria 4.0, y propone el rol que debería asumir cada una de las Partes Interesadas (más adelante en la Sección 5.2.2 de este Capítulo) y la necesaria articulación entre las mismas, lo que podría ser parte del Plan en cuestión.

Posteriormente, plantea analizar si la propuesta de adopción es una consideración de un conjunto de organizaciones (Clúster) o de una única Organización; en el caso de ser un conjunto, el análisis deberá contemplar una heterogeneidad de situaciones y a su vez establecer una realidad de partida para cada Organización o Clúster, y diferentes objetivos a alcanzar en cada caso o grupos de casos y en qué momento. Entre otros aspectos, en ello influirá si se trata de un despliegue *brownfield* o *greenfield* y si el sistema que se pretende que adopte la Industria 4.0 es una parte o comprende a toda la Organización. De tratarse de un conjunto de organizaciones, la eventual heterogeneidad de las realidades podrá determinar la definición de Clústeres que agrupen organizaciones con situaciones y objetivos similares y abordar la adopción de la Industria 4.0 de cada Clúster de manera separada.

En cuanto a la estrategia de abordaje para el caso de Uruguay, la distribución de empresas por tamaño y de puestos de trabajo en cada tipo documentada en la Sección 5.1 de este Capítulo, es una tendencia que permanece desde hace más de 10 años. Ello puede significar que resulte muy frecuente la necesidad que el análisis asociado a la propuesta que aquí se plantea, incluso con el asesoramiento que se pudiera requerir, imponga que se realice a un conjunto de empresas del mismo ramo o tipo de actividad económica (vertical), y no a cada una de manera individual de manera de poder abatir costos y poder sumar las sinergias necesarias para lograr avances concretos, sin desconocer las consideraciones necesarias vinculadas por ejemplo a los planes de negocio de cada empresa o sus estructuras de costos, información que habitualmente es clasificada como reservada o confidencial.

En cualquiera de los tipos de despliegues, *brownfield* o *greenfield*, los modelos de referencia abordados, RAMI 4.0 (Sección 2.3 del Capítulo 3) e IIRA (Sección 3.4 del Capítulo 4), así como los conceptos asociados, serán referencia inevitable para todos los actores involucrados, para disponer de un lenguaje común a ser utilizado durante los desarrollos, las implantaciones y las puestas

en producción.

A continuación, y con el objetivo de poder identificar una hoja de ruta a ser seguida por la Organización (o el Clúster) de determinada rama industrial ("vertical"), el siguiente paso propuesto es aplicar el Índice SIRI y la Matriz de Priorización (Secciones 4.7.2 y 4.7.5 del Capítulo 4, respectivamente), a los efectos de identificar las Dimensiones de mayor impacto.

Si la rama industrial a la que pertenece la Organización (o el Clúster) no está contemplada claramente en el conjunto disponible en el contexto del Índice SIRI, se propone considerar las 2 que más se aproximen y realizar una combinación de ellas y avanzar en el análisis con dicha rama industrial combinada.

Otra alternativa podría ser realizar el análisis para cada una de las ramas industriales por separado y contrastar los resultados, lo que puede resultar en considerar más Dimensiones de mayor impacto. Esta estrategia requiere un mayor esfuerzo de diagnóstico y posteriormente de acción; los resultados obtenidos pueden ser más ricos y abarcativos frente a la primera estrategia, donde el mayor desafío para el diagnóstico se presenta al momento de ponderar cada rama industrial considerada.

Como siguiente paso, y teniendo ya identificadas las Dimensiones de mayor impacto, es posible asociarlas con los KPIs más relevantes (ver Sección 4.7.6 del Capítulo 4). A partir de ello, se propone la aplicación del Modelo de Madurez en Confiabilidad (TMM), el cual se encuentra documentado previa a ésta, la Sección 5.2.3, aunque no hubieran sido identificados los KPIs 8 y 9, *Safety* y Seguridad como parte de los más relevantes, para analizar el estado actual y las acciones a seguir para alcanzar el estado deseado.

Por otro lado, la vertical concreta a la que pertenece la Organización (o el Clúster) que se está analizando, por sus propias características, permitirán identificar aspectos concretos a ser contemplados para un adecuado análisis y así, definir una hoja de ruta hacia una adopción exitosa de la Industria 4.0.

Finalmente, se llegará a un conjunto de acciones a emprender a los efectos de llegar al estado deseado, existiendo estados intermedios de evaluación del avance de cada una de las actividades, posibles correcciones y cambios de rumbos, siendo recomendable también que de alcanzado el estado deseado, se vuelva a realizar el proceso a los efectos de determinar el próximo estado deseado, en un ciclo de mejora continua.

Dada la relevancia que significa para los estados y los ciudadanos que se trabaje en diferentes ámbitos para cumplir con los Objetivos de Desarrollo Sos-

tenible (ODS) y, considerando que la Industria 4.0 (Sección 2.1 del Capítulo 2), la Transformación Digital (Sección 3.2 del Capítulo 3) y la *Society 5.0* (Sección 4.8 del Capítulo 4) tienen como premisa impulsarlos desde el momento que el objetivo final es el bienestar de los ciudadanos, es importante poder identificar cómo esta propuesta de adopción de la Industria 4.0, está alineada a ello. En tal sentido, y tomando como base lo expresado en el documento *How Digital Transformation and IoT Can Contribute to the UN Sustainable Development Goals* [95], es parte de la propuesta que, a partir del Cuadro de Mando Integral (*The Balanced Scorecard* [247]) de cada organización, identificar qué ODSs son apuntalados con las acciones tomadas para la adopción de la Industria 4.0.

El resto del contenido del estudio del estado del arte incluido en el presente trabajo, y contemplando lo expresado en la Sección anterior, permite disponer de un conjunto de consideraciones lo suficientemente rico y amplio para abordar la determinación del estado actual en cuanto a la Confiabilidad y en general del Sistema y de la Organización, y las posibles estrategias para alcanzar el estado deseado, considerando además, la participación de las diferentes Partes Interesadas.

En la Figura 5.2 se muestra una representación esquemática de los bloques principales del Diagrama de Flujo que sirve como guía general para aplicar la Propuesta de Adopción de la Industria 4.0 para un Sistema u Organización. Los Diagramas de Flujo de cada uno de los bloques referidos, son mostrados en detalle en las Figuras 5.3, 5.4 y 5.5.

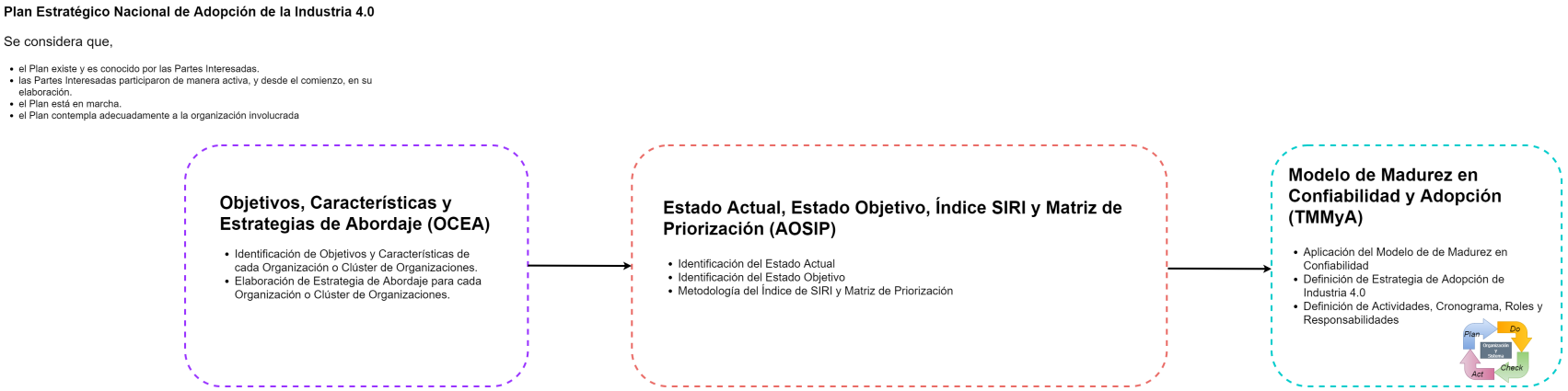


Figura 5.2: Propuesta de Adopción de la Industria 4.0 - Bloques del Diagrama de Flujo

Plan Estratégico Nacional de Adopción de la Industria 4.0

Se considera que,

- el Plan existe y es conocido por las Partes Interesadas.
- las Partes Interesadas participaron de manera activa, y desde el comienzo, en su elaboración.
- el Plan está en marcha.
- el Plan contempla adecuadamente a la organización involucrada

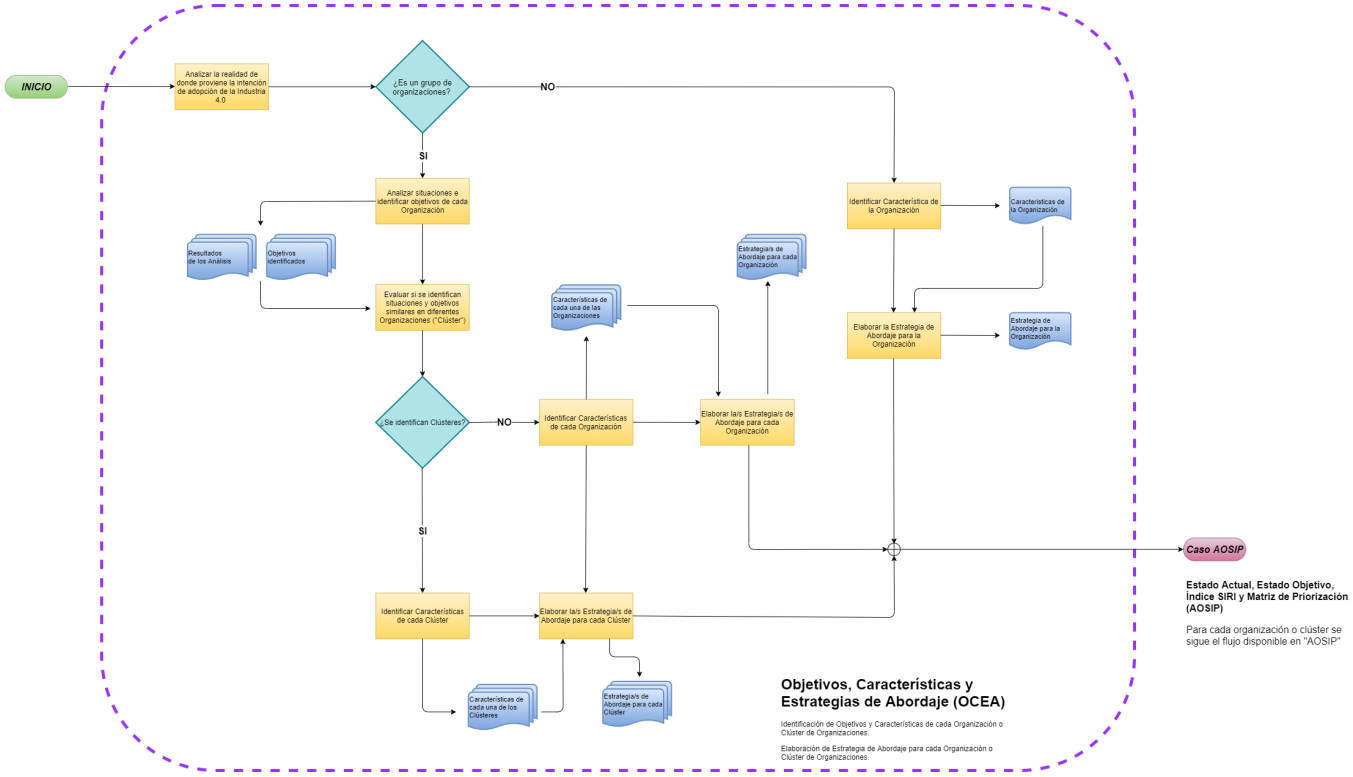


Figura 5.3: Propuesta de Adopción de la Industria 4.0 - Objetivos, Características y Estrategias de Abordaje

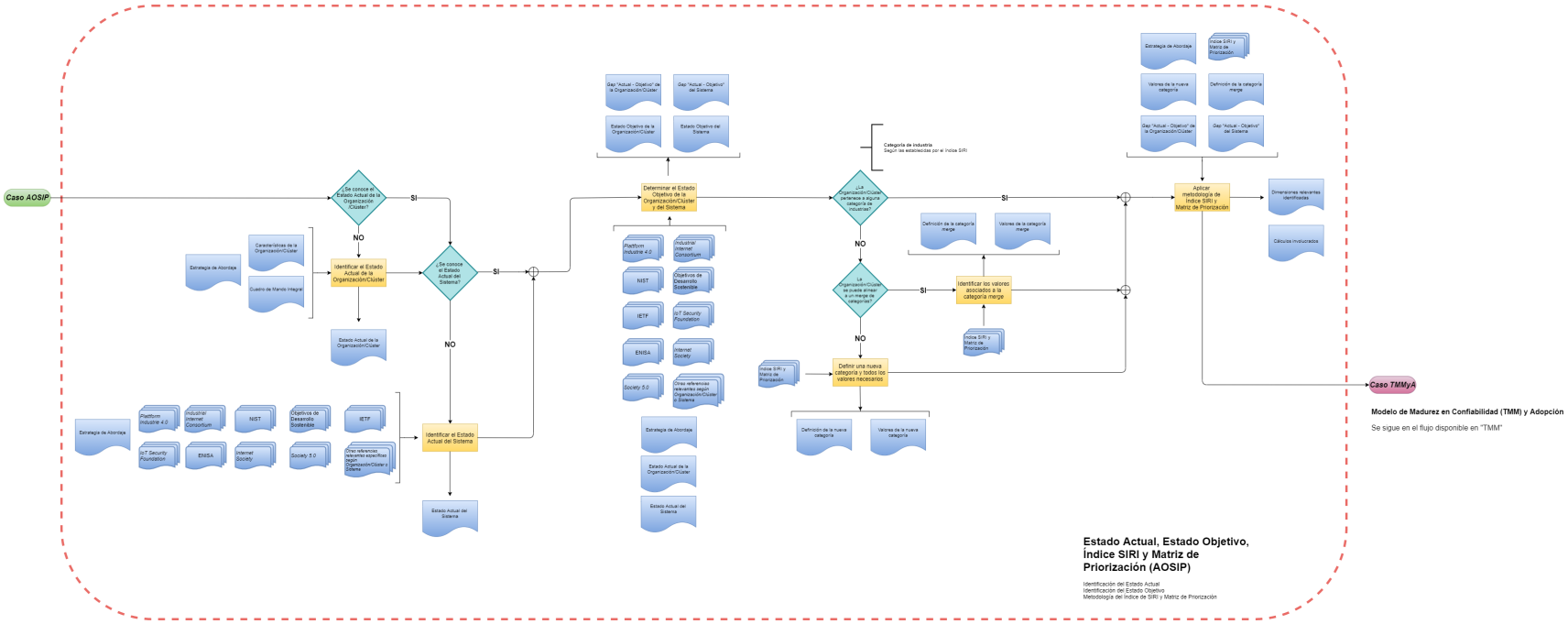


Figura 5.4: Propuesta de Adopción de la Industria 4.0 - Estado Actual, Estado Objetivo, Índice SIRI y Matriz de Priorización

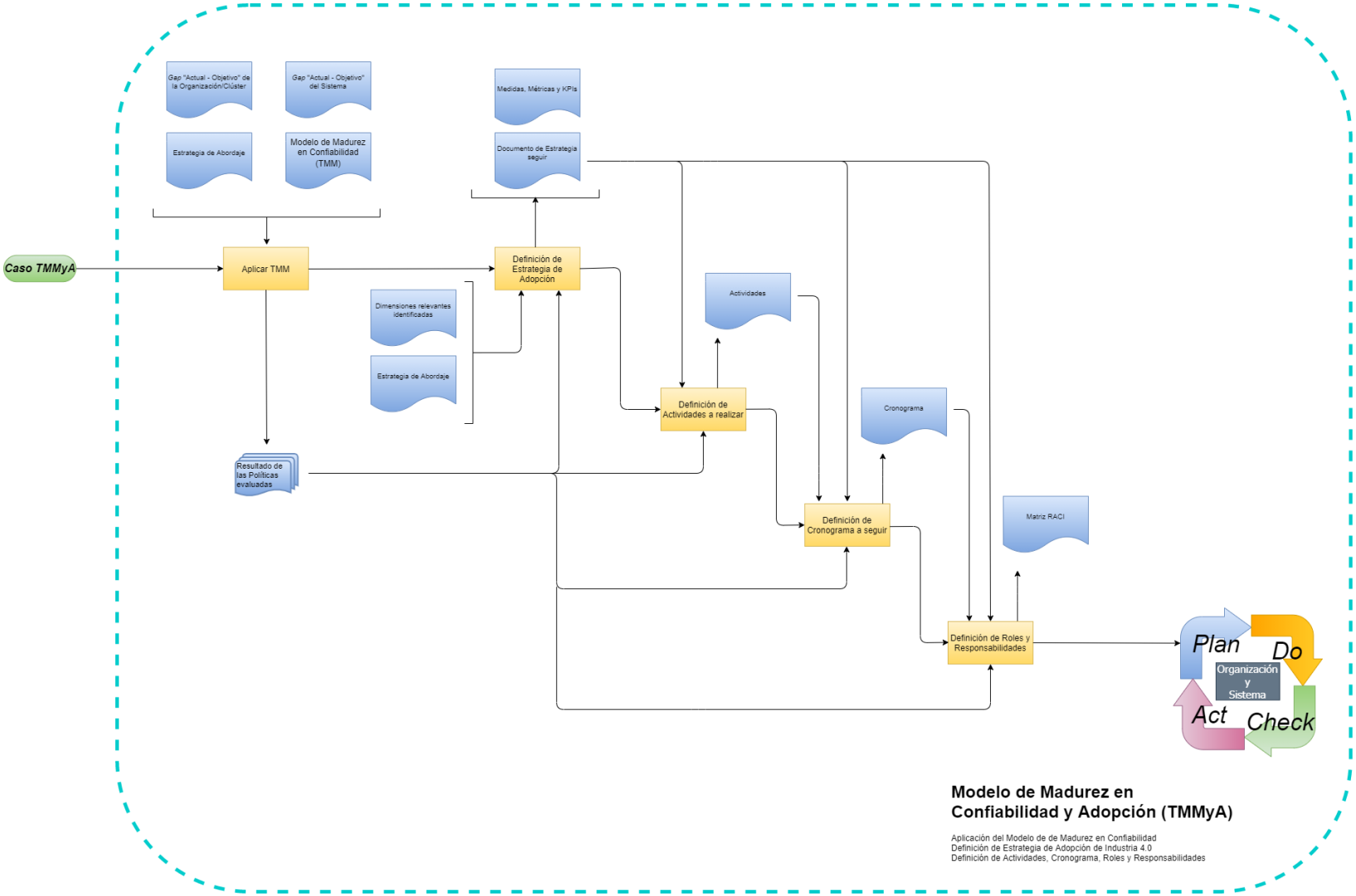


Figura 5.5: Propuesta de Adopción de la Industria 4.0 - Modelo de Madurez en Confiabilidad y Adopción

5.3. Caso de Uso

En esta sección se aplica la propuesta descrita en la Sección 5.2 de este Capítulo y se presentan los resultados obtenidos.

5.3.1. Gabinete de Dosificación Automatizado

La propuesta de adopción de la Industria 4.0 se aplicó de manera teórica al escenario que consistiría en la incorporación de un *Automated Dispensing Cabinet* (ADC) en un servicio de salud en nuestro país.

Un ADC (también conocido con otros nombres, como ser *Automated Dose Dispensing* o *Automated Dispensing Devices* o *Automated Drug Dispensed*, ADD) tiene como objetivo general mejorar la gestión de los medicamentos y la dosificación adecuada de las drogas en un sanatorio u hospital. Se trata de equipamiento desarrollado con los siguientes objetivos específicos:

- Mejorar la gestión del inventario de medicamentos y drogas
- Reducir costos de gestión y servicio
- Hacer más eficiente el tiempo de trabajo de las enfermeras (o *nurses*) y del personal de farmacia [20, 138]
- Velar por el *safety* y la calidad del cuidado de los pacientes

Con su adecuada incorporación a una institución de salud, se logra aumentar el nivel de satisfacción en las enfermeras y en los pacientes, y fundamentalmente cuidar la salud de estos últimos y disminuir el estrés laboral de las primeras, bajando los errores asociados por ejemplo a interpretaciones erróneas de prescripciones, dosificaciones incorrectas de drogas a suministrar, incumplimiento de horarios de toma de medicamentos, administración cruzada de medicamentos entre pacientes, no suministro de medicamentos, lo que en general se conoce como *Adverse Drug Event* (ADE) [208], siendo la mayoría de ellos evitables y considerando que los ADC contribuyen de manera relevante para disminuir los ADEs [273]. Además, su incorporación permite también disminuir de forma notoria los pedidos urgentes a farmacia y también los retornos de medicamentos a la misma. Ante una ocurrencia de un evento ADE, en promedio un paciente permanece casi 3 días más en el hospital, respecto a lo previsto inicialmente, lo que además las posibles consecuencias en lo que refiere a la salud, implica un costo relevante y eventualmente no previsto.

Las soluciones ADC *Best-in-Class* [202, 17] ofrecen un conjunto de características principales a ser consideradas como referencia:

- Control de acceso al uso de la solución
- Facilidad de uso
- Impresión de etiquetas a asociar a la dosificación
- Gestión remota dentro del mismo centro de salud
- Integración con otros sistemas[1] del prestador de salud
- Gestión del inventario de medicamentos y drogas
- Control del conteo de dosificaciones
- Registro de actividad
- Posibilidad de integrar soluciones similares instaladas en diferentes edificios
- Analítica de datos
- Manejo de medicamentos que requieren preservar cadena de frío
- Integración con farmacia central

La gestión de medicamentos en *loop* cerrado (*Closed Loop Medication Management*, CLMM) o *closed-loop Electronic Medication Management Systems* (EMMS) donde participen de manera integrada y coordinada los diferentes sistemas involucrados, contribuye a la reducción de los ADEs y otros errores, así como también a disminuir las ineficiencias vinculadas al proceso y por lo tanto también, los costos innecesarios en los que se puede incurrir en caso contrario. De todas formas, se debe tener presente que se deben disponer de los recursos necesarios para gestionar adecuadamente los inconvenientes que se pudieran presentar ante la implementación de soluciones de este tipo, y los beneficios concretos que aportan [268, 292]. El ejercicio que aquí se plantea, al tener un abordaje estrictamente teórico, puede que considere algunos aspectos de manera parcial y además, que se asuman algunas hipótesis no completamente validadas. En el caso de uso que se analiza aquí, se pone foco en la aplicación del Indice SIRI, de la Matriz de Priorización y por supuesto, del Modelo de Madurez en Confiabilidad (TMM). De todas formas, en función de las referencias utilizadas para la elaboración del mismo, a juicio del autor no invalida la

[1] Algunos ejemplos de dichos sistemas son: la Historia Clínica Electrónica (EHR), el Ingreso de Orden Médica Computarizada (CPOE), el Sistema de Soporte de Decisiones Clínicas (CDSS), la Administración de Medicamentos con Códigos de Barras (BCMA) y el Registro Electrónico de Administración de Medicamentos (eMAR). En todos los casos, se presentan las siglas asociadas a los nombres en inglés.

puesta a prueba de la propuesta que se documenta en la investigación [293]. En primer lugar se considera la hipótesis que está en marcha un Plan Estratégico Nacional de Adopción de la Industria 4.0, y que es conocido por todas las partes interesadas para este caso de uso. Como se expresó, se trata de una única organización y además, el sistema a incorporar comprende a una parte de la organización (hospital o nosocomio) el que ya está en funcionamiento, por lo que estamos en el contexto de un despliegue *brownfield*. La siguiente hipótesis considerada es que se conoce el Estado Actual de dicho hospital en cuanto a la gestión de medicamentos y dosificación de drogas, estando caracterizado por situaciones similares a las expresadas en las referencias [293, 44]. El Estado Objetivo también está caracterizado por alcanzar las mejoras contempladas en las mismas referencias así como también contemplando los factores a tener en cuenta, como ser los documentados en [262]. En lo que refiere a la categoría de industria a contemplar, se selecciona la Farmacéutica, lo que será considerado más adelante. De aquí en adelante, se procederá a aplicar la metodología que involucra al índice SIRI y a la Matriz de Priorización, con el objetivo final de identificar las Dimensiones SIRI de mayor impacto y por lo tanto, en las que hay que focalizar el esfuerzo. En la Tabla 5.1 se establece la correspondencia entre las diferentes Dimensiones del Índice SIRI y las siglas que serán utilizadas como su representación en las tablas que se presentan más adelante.

Dimensiones	Siglas
Procesos	
Vertical Integration	VI
Horizontal Integration	HI
Integrated Product Lifecycle	IPL
Tecnología	
Shop Floor Automation	SFA
Enterprise Automation	EA
Facility Automation	FA
Shop Floor Connectivity	SFC
Enterprise Connectivity	EC
Facility Connectivity	FC
Shop Floor Intelligence	SFI
Enterprise Intelligence	EI
Facility Intelligence	FI
Organización	
Workforce Learning & Development	WL&D
Leadership Competency	LC
Inter- & Intra- Company Collaboration	I&ICC
Strategy & Gobernance	S&G

Tabla 5.1: Sigla asociada a cada Dimensión

Siguiendo la metodología propuesta por el Índice SIRI, el primer paso es establecer el *Assessment Matrix Score* (AMS) para cada una de las Dimensiones, arrojando el resultado que se muestra en la Tabla 5.2.

Dimensiones	Procesos			Tecnología									Organización			
	VI	HI	IPL	SFA	EA	FA	SFC	EC	FC	SFI	EI	FI	WL&D	LC	I&ICC	S&G
AMS	1	1	1	1	0	2	1	1	0	0	1	0	0	1	0	1

Tabla 5.2: Hospital - *Assessment Matrix Score* (AMS)

Tomando como referencia la información disponible en [242, 11], se elaboró el Perfil de Costos (en las diferentes categorías consideradas), que se muestra en la Tabla 5.3.

Categorías	Costos
Aftermarket Services / Warranty	0.00
Depreciation	0.02
Labour	0.49
Maintenance & Repair	0.05
Raw Material & Consumables	0.31
Rental & Operative Lease	0.00
Research & Development	0.03
Selling, General & Administrative Expense	0.03
Transportation & Distribution	0.07
Utilities	0.00

Tabla 5.3: Hospital - Costo por Categoría

Tomando como base el ejemplo concreto documentado en [44], donde en diferentes escenarios en varios países el costo total asociado a la implantación del ADD se amortizó en un período de 4 o 5 años, para este ejercicio se establece un horizonte planificado del tipo Estratégico (3 a 5 años), lo que determina los siguientes valores, según la Tabla 4.1:

- Factor Costo (W_C) = 30 %
- Factor KPI (W_K) = 40 %
- Factor Proximidad (W_P) = 30 %

En función de la descripción del caso de uso, y teniendo en cuenta el Estado Objetivo fijado, de los 14 KPIs definidos en la Sección 4.7.6 se seleccionan los siguientes:

- Eficiencia del inventario
- *Safety*
- Calidad del Proceso
- Calidad del Producto
- Eficacia en la Planificación y en la Programación

Respecto a la industria, se concluye que la que mejor se adapta a este caso de uso es la Farmacéutica, presentando el perfil *Best-in-Class* BIC que se observa en la Tabla 5.4, de acuerdo a lo que se identifica en la Figura 3.15 del Apéndice 3.

Dimensiones	Procesos			Tecnología									Organización			
	VI	HI	IPL	SFA	EA	FA	SFC	EC	FC	SFI	EI	FI	WL&D	LC	I&ICC	S&G
BIC	4	3	3	3	2	3	4	4	4	4	3	4	4	4	4	4

Tabla 5.4: Industria Farmacéutica - *Best-in-Class* (BIC)

Eventualmente se podrían haber considerado otras opciones, como ser:

- Una combinación de los perfiles BIC de las industrias Farmacéutica y Tecnología Médica
- Definir un BIC específico

A partir de los DOR_C (Grado de Relevancia para los Costos) proporcionados en la tabla disponible en la Figura 3.13 del Apéndice 3 y de los Costos por Categoría plasmada en la Tabla 5.3, se calcula el Factor Costo para cada Dimensión SIRI, obteniéndose los resultados que se observan en la Tabla 5.5.

Dimensiones	Procesos			Tecnología									Organización			
	VI	HI	IPL	SFA	EA	FA	SFC	EC	FC	SFI	EI	FI	WL&D	LC	I&ICC	S&G
Factor Costo	2,63	1,31	0,48	1,83	0,61	1,83	0,87	0,49	0,87	2,57	1,37	1,95	1,87	2,04	2,22	2,10

Tabla 5.5: Hospital - Factor Costo

A partir de los DOR_K (Grado de Relevancia para los KPI) proporcionados en la tabla disponible en la Figura 3.14 del Apéndice 3 y de los 5 KPIs seleccionados, se calcula el Factor KPI para cada Dimensión SIRI, obteniéndose los resultados que se observan en la Tabla 5.6.

Dimensiones	Procesos			Tecnología									Organización			
	VI	HI	IPL	SFA	EA	FA	SFC	EC	FC	SFI	EI	FI	WL&D	LC	I&ICC	S&G
Factor KPI	11	8	4	12	10	7	5	6	3	13	10	7	9	9	9	5

Tabla 5.6: Hospital - Factor KPI

Considerando que la Proximidad se calcula como la diferencia, para cada Dimensión, entre el BIC asignado a la industria involucrada (en este reflejado en la Tabla 5.4), y el AMS (en este caso reflejado en la Tabla 5.2), el Factor Proximidad resultante es el que se muestra en la Tabla 5.7.

Dimensiones	Procesos			Tecnología									Organización			
	VI	HI	IPL	SFA	EA	FA	SFC	EC	FC	SFI	EI	FI	WL&D	LC	I&ICC	S&G
Factor Proximidad	3	2	2	2	2	1	3	3	4	4	2	4	4	3	4	3

Tabla 5.7: Hospital - Factor Proximidad

Luego de disponer de los tres Factores (Costo, KPI y Proximidad), con el objetivo de lograr una comparación más equitativa se procede a normalizar los mismos.

En la Tabla 5.8 se observan los valores normalizados del Factor Costo.

Dimensiones	Procesos			Tecnología									Organización			
	VI	HI	IPL	SFA	EA	FA	SFC	EC	FC	SFI	EI	FI	WL&D	LC	I&ICC	S&G
Factor Costo Normalizado	0,1050	0,0523	0,0192	0,0731	0,0244	0,0731	0,0347	0,0196	0,0347	0,1026	0,0547	0,0779	0,0747	0,0815	0,0887	0,0839

Tabla 5.8: Hospital - Factor Costo Normalizado

Los valores normalizados del Factor KPI aparecen reflejados en la Tabla 5.9.

Dimensiones	Procesos			Tecnología									Organización			
	VI	HI	IPL	SFA	EA	FA	SFC	EC	FC	SFI	EI	FI	WL&D	LC	I&ICC	S&G
Factor KPI Normalizado	0,0859	0,0625	0,0313	0,0938	0,0781	0,0547	0,0391	0,0469	0,0234	0,1016	0,0781	0,0547	0,0703	0,0703	0,0703	0,0391

Tabla 5.9: Hospital - Factor KPI Normalizado

En la Tabla 5.10 se observan los valores normalizados del Factor Proximidad.

Dimensiones	Procesos			Tecnología									Organización			
	VI	HI	IPL	SFA	EA	FA	SFC	EC	FC	SFI	EI	FI	WL&D	LC	I&ICC	S&G
Factor Proximidad Normalizado	0,0652	0,0435	0,0435	0,0435	0,0435	0,0217	0,0652	0,0652	0,0870	0,0870	0,0435	0,0870	0,0870	0,0652	0,0870	0,0652

Tabla 5.10: Hospital - Factor Proximidad Normalizado

A partir de los Factores Normalizados y las ponderaciones correspondientes al horizonte de planificación Estratégico, se obtienen los Valores de Impacto para cada Dimensión SIRI, presentados en la Tabla 5.11.

Dimensiones	Procesos			Tecnología									Organización			
	VI	HI	IPL	SFA	EA	FA	SFC	EC	FC	SFI	EI	FI	WL&D	LC	I&ICC	S&G
Valores de Impacto	0,0854	0,0537	0,0313	0,0725	0,0516	0,0503	0,0456	0,0442	0,0459	0,0975	0,0607	0,0713	0,0766	0,0721	0,0808	0,0603

Tabla 5.11: Hospital - Valores de Impacto

Finalmente, observando los Valores de Impacto obtenidos, seleccionamos el más alto de cada Bloque (Procesos, Tecnología y Organización) y además, el más alto de los 13 Valores de Impacto restantes. De esta forma, los seleccionados son:

- Bloque Procesos: **0,0854** - Corresponde a la Dimensión *Vertical Integration* (VI)

- Bloque Tecnología: **0,0975** - Corresponde a la Dimensión *Shop Floor Intelligence* (SFI)
- Bloque Organización: **0,0808** - Corresponde a la Dimensión *Inter- & Intra- Company Colaboration* (I&ICC)
- **0,0766** - Corresponde a la Dimensión *Workforce Learning & Development* (WL&D) del Bloque Organización

Por lo tanto, a partir de los Valores de Impacto obtenidos, las Dimensiones SIRI de mayor impacto son:

- *Vertical Integration* - Procesos
- *Shop Floor Intelligence* - Tecnología
- *Workforce Learning & Development* - Organización
- *Inter- & Intra- Company Colaboration* - Organización

En la Tabla 5.12 se ofrece una vista unificada de los valores reflejados en las tablas anteriores, que permitieron finalmente identificar las Dimensiones SIRI de mayor impacto para el caso de uso analizado.

Dimensiones	Procesos			Tecnología									Organización			
	VI	HI	IPL	SFA	EA	FA	SFC	EC	FC	SFI	EI	FI	WL&D	LC	I&ICC	S&G
Factor Costo	2,63	1,31	0,48	1,83	0,61	1,83	0,87	0,49	0,87	2,57	1,37	1,95	1,87	2,04	2,22	2,10
Factor KPI	11	8	4	12	10	7	5	6	3	13	10	7	9	9	9	5
Factor Proximidad	3	2	2	2	2	1	3	3	4	4	2	4	4	3	4	3
Factor Costo Normalizado	0,1050	0,0523	0,0192	0,0731	0,0244	0,0731	0,0347	0,0196	0,0347	0,1026	0,0547	0,0779	0,0747	0,0815	0,0887	0,0839
Factor KPI Normalizado	0,0859	0,0625	0,0313	0,0938	0,0781	0,0547	0,0391	0,0469	0,0234	0,1016	0,0781	0,0547	0,0703	0,0703	0,0703	0,0391
Factor Proximidad Normalizado	0,0652	0,0435	0,0435	0,0435	0,0435	0,0217	0,0652	0,0652	0,0870	0,0870	0,0435	0,0870	0,0870	0,0652	0,0870	0,0652
AMS	1	1	1	1	0	2	1	1	0	0	1	0	0	1	0	1
Valores de Impacto	0,0854	0,0537	0,0313	0,0725	0,0516	0,0503	0,0456	0,0442	0,0459	0,0975	0,0607	0,0713	0,0766	0,0721	0,0808	0,0603

Tabla 5.12: Hospital - Compendio de valores

De acuerdo a los resultados obtenidos, si los recursos y la atención se focalizan en las Dimensiones *Vertical Integration*, *Shop Floor Intelligence*, *Workforce Learning & Development* y *Inter- & Intra- Company Colaboration*, en particular en lo que refiere al ADD en cuestión (y los otros sistemas con los que se integre), se dispondrá de una analítica de datos y un procesamiento de los productos involucrados, en este caso la gestión de las medicamentos y la dosificación de la drogas, con mayor eficiencia y menor tasa de ADEs, lo cual se verá reflejado de manera directa a los 5 KPIs seleccionados.

La Dimensión *Vertical Integration* impacta directamente en los procesos relacionados con la gestión de medicamentos y dosificación de drogas, los que implicará ajustar los existentes e incluso, elaborar nuevos, de manera de contemplar no solo el proceso concreto de gestión y dosificación sino que también aquellos que tienen que ver con la logística, el mantenimiento de la ADD (reactivo, preventivo y predictivo), el relacionado a la evaluación de la satisfacción de los usuarios y aquellos involucrados con el entrenamiento de todas las partes involucradas. A su vez, la nueva tecnología permitirá que a nivel de la Dirección se disponga de información en tiempo real del uso del ADD y poder compararlo con la situación previa a su incorporación así como también con la evolución en otros nosocomios que por el momento no han incorporado una solución similar, lo que a futuro, puede brindar los argumentos necesarios para justificar su compra e incorporación.

La Dimensión *Shop Floor Intelligence* está directamente relacionada con la incorporación de tecnología (el ADD) y la integración con otros sistemas ya existentes. Poner foco en esta Dimensión, con la adecuada instalación, configuración y puesta en producción del ADD, apuntalará la reducción de los errores humanos, liberará tiempo de estos que se podrán destinar a otras tareas no (tan) rutinarias, bajará el nivel de estrés de las personas directamente involucradas, permitirá mantener un seguimiento más cercano y exacto de stock y de toda la logística asociada, pudiendo incorporar al procesos a los proveedores tanto de medicamentos y drogas como los directamente relacionados con el producto ADD.

La Dimensión *Workforce Learning & Development* será una apoyatura transversal a todo el proceso asociado a la adecuada adopción de la solución

ADD, mediante la consecución de implantar un programa planificado de formación, alineado al negocio, con retención de talentos, que mantenga motivado al personal y con la proactividad necesaria para que los cambios que ocurran en la organización sean aceptados y acompañados. Necesariamente se deberá trabajar también en un plan de reconversión laboral, donde las personas asuman nuevos roles, con nuevos desafíos, con el objetivo de lograr un trabajo de mayor calidad y más motivador.

La Dimensión *Inter- & Intra- Company Colaboration* resulta fundamental para la adecuada adopción del ADD. El éxito en la adopción estará fuertmente ligado a que tanto las diferentes partes interesadas dentro de la organización así como también las de fuera de la organización pero directamente involucradas, promuevan su adopción, participando activamente desde el comienzo del proceso y aportando cada uno desde su rol, todo aquello que sea necesario para que se cumpla el objetivo. La participación colaborativa e interdisciplinaria de los involucrados resulta indispensable para ello. Asimismo, esto puede determinar que se requieran definiciones y ejecutar acciones que hasta ese momento no se habían identificado como necesarias, las que adecuadamente impulsadas y aplicadas, redundará en un beneficio para todos.

Respecto a los Objetivos de Desarrollo Sostenible (ODS), la incorporación del ADD promueve directamente los siguientes:

- 3. Salud y Bienestar
- 8. Trabajo Decente y Crecimiento Económico
- 9. Industria, Innovación e Infraestructura

Si además, la solución de ADD a incorporar y la empresa que la produce cumple con requisitos vinculados a la reducción de la huella medioambiental, al reciclado y disposición final adecuado de materiales involucrados tanto en su fabricación como en su mantenimiento, al uso eficiente de la energía, a no realizar actividades que dañen la capa de Ozono, también se promueven los siguientes ODSs:

- 12. Producción y Consumo Responsables
- 13. Acción por el Clima
- 15. Vida de Ecosistemas Terrestres

De acuerdo a lo que se expresó anteriormente, *Safety* es uno de los KPIs seleccionados. De todas formas, si ni ese ni Seguridad se hubieran elegido, la realidad de la Industria 4.0 hace que resulte muy difícil (por no decir imposible) que no se considere necesario analizar la Confiabilidad de cualquier sistema a implantar, más allá de los matices a contemplar al momento de definir la exhaustividad requerida en el análisis.

Por lo tanto, de acuerdo a la propuesta de adopción y en lo que refiere específicamente a la Confiabilidad, la aplicación del Modelo de Madurez en Confiabilidad (TMM) presentado en la Sección 5.2.3 permite identificar los aspectos a considerar, con el objetivo que la incorporación del ADD al nosocomio cumpla con los requisitos que forman parte de la hoja de ruta que impone el TMM para este caso.

A continuación se brinda un detalle de los aspectos a tener en cuenta para cada una de las Prácticas consideradas en el TMM para el Caso de Uso en cuestión, evaluando cada una de ellas en función de lo expresado al respecto en el Apéndice 4, donde se ofrece una referencia muy amplia para cada Práctica.

Práctica Gestión del Programa de Confiabilidad

Se debe contar con un Programa de Confiabilidad para el ADD y por lo tanto, con los 5 programas que lo componen, adecuadamente articulados. En este caso en particular, cobran especial relevancia 2 de ellos: el Programa de *Safety* y el Programa de Privacidad; a ellos que habrá que destinar especial atención y recursos para su elaboración, aprobación, difusión y mejora.

Los restantes 3 Programas (Seguridad, Fiabilidad y Resiliencia) también deben ser contemplados, por lo que se requiere su elaboración, aprobación, difusión y mejora

Práctica Gestión del Cumplimiento

La incorporación de una solución ADD y su integración con otros sistemas ya existentes en el nosocomio, requiere conocer, entender y cumplir las normas, mejores prácticas, regulaciones y estándares aplicables. En tal sentido, una enumeración no taxativa (pues excede al alcance de este trabajo) de referencias para las mismas es la siguiente:

- Documento *Guidelines for the Safe Use of Automated Dispensing Cabinets* del ISMP [133].
- Documento *Targeted Medication Safety Best Practices for Hospitals* del ISMP [134].
- Documento *Best Practice for the Automated Dose Dispensing (ADD) Process and Care and Safety of Patients* del EDQM [267].
- *Standard Health Level Seven International (HL7)* [79].
- Guía de Protección de Datos en Salud, de AGESIC [4].
- Recomendaciones para el tratamiento de datos personales ante la situación de emergencia sanitaria nacional, de AGESIC [5].
- *Automated Dispensing Cabinets* de *KLAS Research* [169].

Práctica Gestión de Riesgos

Se debe realizar un análisis de Gestión de Riesgos asociados a la incorporación del ADD, su interconexión con otros sistemas, el intercambio de información y su funcionamiento. A partir de ello se identificará qué riesgos gestionar y cómo, y cuales asumir.

Práctica Gestión de Amenazas

Se deben identificar las principales amenazas a las que está expuesto el ADD, directa e indirectamente, así como las personas directamente vinculadas a su operativa y mantenimiento, analizando también cómo actuar en caso de materializarse.

Práctica Gestión de la Cadena de Suministros

Se debe contemplar tanto a los proveedores de la solución ADD como también a los proveedores de los medicamentos y demás insumos para que el producto funcione de acuerdo a lo esperado. En todos los casos se debe mantener vigente un SLA, un NDA y eventualmente, un TDA.

En el caso de los proveedores de la solución ADD, deben asegurar, al menos:

- Stock de repuestos
- Soporte técnico
- Tiempos de respuesta y resolución de problemas
- Formación adecuada del soporte técnico
- Actualizaciones de software/firmware

- Información respecto a vulnerabilidades, paliativos y parches
- Solución de monitorizado
- Si la solución ADD es proporcionada por más de un proveedor, deben quedar claramente delimitadas las responsabilidades, y formalizada por escrito por las partes involucradas, debiéndose cubrir todos los componentes (hardware, software, gestión) de la solución.

En el caso de los proveedores de los medicamentos (y drogas) se debe disponer de una trazabilidad de los mismos en todo momento, de las personas involucradas así como también se debe mantener un inventario y flujo de medicamentos conocido y con la posibilidad de detectar desvíos.

En el caso del resto de los proveedores (por ejemplo, lectores de código de barras, impresora de código de barras o de etiquetas) se deben requerir aspectos similares a los mencionados para los proveedores de la solución ADD.

Práctica Gestión de los Servicios de Terceras Partes
Se deben identificar todas las terceras partes que no forman parte de la cadena de suministros. Para cada uno de ellos se debe identificar y registrar su rol y sus responsabilidades, así como la trazabilidad completa de sus acciones. En todos los casos se debe mantener vigente un SLA, un NDA y eventualmente, un TDA.

Práctica Medidas
Es necesario identificar las medidas a obtener que resulten necesarias para a partir de ellas (de su procesamiento), llegar a métricas y KPIs relevantes. Qué medir puede cambiar en función de las necesidades del negocio.

Práctica Métricas e Indicadores
Es necesario identificar las métricas y los KPIs que resulten relevantes para a partir de ellos comparar el estado actual con el estado objetivo y determinar así, acciones a tomar. Incluso es posible que se identifique la necesidad de considerar nuevos KPIs. En el caso de uso considerado, los KPIs deben poder "decirnos" cosas relevantes respecto a:

- Eficiencia del inventario
- *Safety*
- Calidad del Proceso

- Calidad del Producto
- Eficacia en la Planificación y en la Programación
- La Satisfacción del Cliente o Usuario
- La Calidad de los Procesos
- La Satisfacción de los empleados
- El Rendimiento Funcional
- Privacidad

En tal sentido, una referencia que puede ser un buen punto de partida para identificar KPIs específicos relevantes es [291].

En dicha referencia se consideran los siguientes KPIs:

- Al menos el xx % de las órdenes médicas del nosocomio son abastecidas mediante ADC
- Recolección segura de medicamentos (umbral de errores por cada 100 pacientes día)
- Administración de medicamentos correctos (umbral de errores por cada 100 pacientes día)
- Almacenamiento seguro de medicamentos (autenticación fuerte)
- Mejora de la eficiencia del trabajo (reducción medida en cantidad de *Full-Time Equivalent* - FTE en un período de tiempo, tanto para enfermeras como para el personal de farmacia)
- Mejora del proceso de reabastecimiento (reducción en los tiempos involucrados)
- Inventario (mantenimiento en tiempo real un xx % del tiempo de funcionamiento)
- Reducción del malgasto de fondos (reducción de costos en un xx % en un período de tiempo respecto a la situación previa a la implantación del ADC)
- eficiente, oportuno y preciso Facturación
- Al menos un xx % de los medicamentos disponen de código de barras

Práctica Identificación e Impacto Interno

El nosocomio debe tener identificada su cultura organizacional y el impacto interno de la misma, a los efectos de considerar una readecuación de la misma.

Práctica Impacto Externo
El nosocomio debe tener identificada su cultura organizacional y el impacto externo de la misma, a los efectos de considerar una readecuación de la misma.

Práctica Desarrollo
La incorporación del ADD trae de la mano la necesidad de impulsar actividades de Concientización, Sensibilización, Capacitación, Educación y Entrenamiento que permitan que las diferentes personas involucradas tengan la certeza que la aparición del ADD no es una amenaza a su fuente laboral o a sus ingresos, y sí es una oportunidad para reconvertirse y adaptarse a una nueva realidad laboral, donde no se menoscaben sus derechos y donde además, se logre una reconversión laboral que implique una mejor calidad laboral y una satisfacción de las personas por el cambio.

Práctica Gestión del Capital Humano
Es fundamental que la incorporación del ADD esté acompasado por un plan de evaluación por desempeño alineado a la Práctica de Desarrollo de manera que los esfuerzos realizados al respecto por las personas, puedan tener un retorno mediante reconocimientos que ayudan a fidelizar al personal y a la retención de los talentos, en este caso, para las personas vinculadas a los procesos donde el ADD impacta.

Práctica Aprendizaje
Se deben identificar y fomentar aquellas actividades, formales e informales, que hagan parte de la cultura organizacional los paradigmas de "aprender a aprender", "aprender a desaprender" y "aprender y desaprender toda la vida".

Práctica Mejora Continua
La organización debe fomentar entre las personas vinculadas a los procesos donde el ADD impacta a que sea parte de actividad laboral la identificación de oportunidades de mejora, ofreciendo además canales amigables para los planteos al respecto, considerando todas las propuestas recibidas y siempre otorgando *feedback* y agradeciendo el interés.

Práctica Gestión de Identidades
Deben detallarse claramente las identidades que necesariamente deben ser defi-

nidas tanto en ADD como en todos los sistemas con los que interactúa. También deben estar claramente identificadas las identidades de las entidades que por diversas razones deben acceder al mismo a su lugar de acción. Las identidades definidas deben ser periódicamente revisadas para validar la pertinencia de su existencia.

Práctica Control de Acceso
Se debe establecer los mecanismos de control de acceso al ADD y a los sistemas con los que se relaciona directamente, permitiendo solo acceso necesario, sin que ello esté atado al cargo dentro de la organización, y si a su rol. Debe existir un sistema de trazabilidad asociado y mecanismos de bloqueos y alertas en caso de detectarse (de manera automática) situaciones sospechosas.

Práctica de Gestión de Configuración y Cambio en los Activos
Se debe mantener un versionado de configuraciones del ADD, debidamente respaldado, así como también un Plan de Gestión de Cambios, donde se deben contemplar todos los aspectos que resultan necesarios para una adecuada realización de los mismos, contemplando *rollbacks*.

Práctica Protección Física
Se debe dotar al sitio donde se instala el ADD (y al perímetro del mismo) de sistemas de protección física (y ambiental) y con las alarmas correspondientes.

Práctica Modelo y Política de Seguridad de los Datos
El nosocomio debe contar con un Modelo de Política de Seguridad de los Datos que sea el *template* para las restantes políticas relacionadas. Esto es insumo para todo el ciclo de vida del ADD, desde la especificación de requerimientos, pasando por la selección del equipamiento a instalar, su instalación, su integración con otros sistemas del nosocomio, su puesta en producción, su uso, y hasta su remoción y disposición final. Se deben considerar los datos en todos sus estados (en reposo, en tránsito o en uso) y, dadas las características del sistema en cuestión, la privacidad y la integridad requieren especial atención.

Práctica Controles de Protección de Datos
Los activos de información vinculados con el ADD deben tener un dueño que establezca qué protección se le debe brindar a los datos (en reposo, en tránsito

o en uso) y un custodio que determine el cómo, con el aval del primero. Ello debe ser auditado periódicamente.

Práctica Análisis
Esta práctica puede tener sentido en el caso que se deba analizar alternativas de integración del ADD con otros sistemas, o funcionalidades específicas requeridas, y que las mismas no estén disponibles.

Práctica Diseño
Esta práctica puede tener sentido en el caso que se deba diseñar la integración del ADD con otros sistemas, o desarrollar funcionalidades requeridas, y que las mismas no estén disponibles.

Practica Gestión de Parches
El sistema ADD se debe mantener al día en cuanto a los parches que aseguran su correcto funcionamiento. Para ello el vínculo con el proveedor del ADD debe contemplar la disponibilidad de los mismos en tiempo y forma, en incluso en caso que el propio nosocomio identifique la necesidad de un parche no contemplado por el fabricante del ADD. Aquí se aplica el Plan de Gestión de Cambios.

Práctica Gestión de Vulnerabilidades
Los administradores del sistema ADD se deben mantener al día en cuanto a las vulnerabilidades del sistema ADD y sus componentes, así como también del potencial impacto en caso de ser explotadas. El fabricante debe ser una fuente de información proactiva o reactiva temprana tanto de las vulnerabilidades como de los parches que las resuelven, o al menos que oficien de *workaround* temporalmente. Aquí se aplica el Plan de Gestión de Cambios.

Práctica Monitorizado y Auditado
El sistema ADD debe ofrecer un sistema de monitorizado acorde a la criticidad del mismo, que ofrezca un servicio de alertas tempranas y que no permita que existan acciones sobre el mismo o propias que no puedan ser auditadas y trazadas de manera completa.

Práctica Comunicación e Intercambio de Información
Los administradores del ADD, su proveedor, el fabricante y los mismos actores relacionados con los otros sistemas del nosocomio con el cual el ADD se relaciona, deben establecer canales de comunicación fluidos y confiables, a través de los cuales se intercambie información que resulte útil para estar mejores preparados ante amenazas o vulnerabilidades que podrían ser explotadas y afectar al ADD. De la misma forma, se debe disponer de contactos con la comunidad de poseedores de soluciones similares, sean o no del mismo proveedor o fabricante.

Práctica Gestión de Incidentes de Confiabilidad
Se debe disponer de un procedimiento de gestión de incidentes de confiabilidad al cual recurrir en caso que se presente en el ADD alguna situación que requiera su tratamiento como tal.

Práctica Continuidad de las Operaciones
Se debe disponer de un plan de continuidad de operaciones el que se accione en caso de ocurrir una falla del ADD que sea catalogada como desastre.

Práctica Verificación
El sentido de esta práctica está íntimamente ligado a las Prácticas de Análisis y Diseño.

Práctica Validación
El sentido de esta práctica está íntimamente ligado a la Práctica de Diseño.

Disponiendo de las Dimensiones identificadas a través del Índice SIRI y la Matriz de Priorización, así como también de las consideraciones que se explicitaron para cada una de las Prácticas del Modelo de Madurez en Confiabilidad, es momento para fijar una Estrategia de Abordaje para poner en práctica la propuesta de adopción del sistema ADD. La estrategia debe determinar los objetivos a lograr, los indicadores medir el nivel de avance hacia los mismos, las actividades y tareas a desarrollar, el cronograma a seguir, los roles y las responsabilidades. Para esto último, resulta sumamente útil definir una matriz RACI que contemple cada una de las actividades y tareas definidas.

Disponiendo de lo expresado en el párrafo anterior, ya contamos con el Plan de acción (*Do*), el que hay que llevar a la práctica (*Do*), para luego verificar (*Check*) y actuar (*Act*); estamos así en el ciclo de mejora continua.

Para el caso de uso planteado aquí, varias de las Prácticas son un insumo para el momento de establecer los requisitos del ADD a incorporar, así como el tipo de servicio asociado, y otras pueda que no tengan sentido. Ello no significa que pierda validez el modelo, sino que por el contrario, muestra la flexibilidad que ofrece, dado que quizás en la "primera vuelta"de ciclo esa sea la situación, pero en la siguiente, por los propios requerimientos del nosocomio o de los reguladores por ejemplo, algunas de las prácticas pueden cobrar una relevancia que no tenían, pudiendo ocurrir lo contrario con otras. Esto muestra que el trabajar en la Confiabilidad de un sistema no es un proyecto, es un viaje sin fin.

Capítulo 6

Consideraciones finales, conclusiones y trabajo futuro

En el último capítulo del trabajo, se incluyen 3 secciones: consideraciones finales vinculadas a la temática del trabajo, las conclusiones del mismo y propuestas de trabajo futuro.

6.1. Consideraciones finales

En esta sección se abordan algunos aspectos que tienen directa relación la temática del trabajo realizado.

6.1.1. CPS e IoT

Los conceptos Sistemas Ciberfísicos (CPS) e Internet de las Cosas (IoT), tienen orígenes distintos pero definiciones superpuestas, y ambos se refieren a las tendencias en la integración de capacidades digitales, incluida la conectividad de red y la capacidad de cómputo, con los sistemas y dispositivos físicos. Respecto a si son denominaciones de los mismo, o uno es un subconjunto del otro, la publicación *Cyber-Physical Systems and Internet of Things* del NIST, disponible en [185], documenta el análisis de diferentes definiciones y características asociadas a cada uno de los conceptos y la evolución de los mismos a lo largo del tiempo para concluir, entre otras cosas, que las definiciones de CPS e IoT son convergentes a lo largo del tiempo incluyendo un énfasis común en los sistemas híbridos de interacción de componentes digitales, analógicos,

físicos y humanos en sistemas diseñados para funcionar a través de la física y la lógica integradas.

6.1.2. Coexistencia de los modelos de referencia

Desde hace varios años, existen esfuerzos para identificar similitudes y diferencias entre los diferentes modelos de referencia fundamentales para la comunidad, así como entre los principales conceptos involucrados en cada uno, buscando caminos para alinearlos y dotar de interoperabilidad a quienes opten por uno u otro, o por un *mix* de ellos. En otros casos, documentos técnicos de elaboración conjunta pretenden reflejar también los puntos de conexión entre los diferentes modelos y conceptos. En ese sentido, diversos trabajos se han realizado al respecto, siendo algunos ejemplos de ello:

- *Architecture Alignment and Interoperability* [96]
- *Alignment Report for Reference Architectural Model for Industrie 4.0/ Intelligent Manufacturing System Architecture* [260]
- *Usage View of Asset Administration Shell* [231]
- *Usage View "Seamless and Dynamic Engineering of Plants"* [220]
- *Digital Twin and Asset Administration Shell Concepts and Application in the Industrial Internet and Industrie 4.0* [97]

6.1.3. Alcance del trabajo

Para llevar adelante el análisis del Estado del Arte en la temática, de la miríada de organizaciones e iniciativas existentes, las seleccionadas son a juicio del autor, las más relevantes; las razones se habrán podido deducir a partir de los capítulos anteriores del trabajo y en particular, en función de lo expuesto en el C apítulo 5. De todas formas, resulta completamente válido que algunas no se consideren (tan) relevantes y además, que se identifique alguna/s otra/s que se debería/n haber considerado. Es más, quizás si se realizara este mismo trabajo o uno similar eventualmente perfilado a algunas de las propuestas de trabajo futuro, el conjunto seleccionado sería distinto, al menos parcialmente. Ello también es una muestra más de la dinámica que está teniendo la temática en la comunidad, por diferentes factores: inexperiencia, lecciones aprendidas, nuevas alianzas económicas, participación activa de las diferentes partes interesadas, nuevas alianzas estratégicas, tendencias tecnológicas, entre otras.

6.2. Conclusiones

A lo largo del trabajo realizado se logró completar un estudio amplio y profundo del estado del arte de la Industria 4.0, contemplando durante el mismo los principales conceptos involucrados así como también los trabajos fundacionales que han elaborado las organizaciones que están liderando la Transformación Digital en la Industria. A través del estudio realizado se identificó que la estrategia del negocio se vincula cada vez más con la visión táctica y operacional, en un lazo cerrado que debe beneficiar a todas las Partes Interesadas.

Como parte del estudio realizado, quedó claramente identificada la importancia de la confiabilidad en cualquier proceso de adopción de la Industria 4.0, en cualquier vertical de aplicación así como también tanto para una Organización completa como para un Sistema específico. Imponer el concepto de confiabilidad implica dejar de manifiesto la relevancia de las características que la componen, a saber: seguridad, *safety*, privacidad, resiliencia y fiabilidad. Estas características no hacen más que reafirmar su importancia cuando se aborda una propiedad intrínseca de la Industria 4.0 o la Internet Industrial: la convergencia IT-OT.

El análisis del rol de las Partes Interesadas permitió identificar la relevancia que algunas de las organizaciones consideradas durante el estudio del estado del arte le dan a los clientes, a los usuarios y en definitiva, a los ciudadanos, quedando de manifiesto que si se logra el bienestar de ellos, se habrá logrado el objetivo fundamental, lo que también se plasma al momento de ser una recomendación identificada: que siempre se busque emparejar las mejoras que se logran mediante la Transformación Digital con los Objetivos de Desarrollo Sostenible sustentados por las Naciones Unidas. Nuevamente, cumplir con este objetivo tiene como componentes ineludibles a las características de la confiablidad.

El trabajo realizado abordó la elaboración de una propuesta de adopción de la Industria 4.0 enfocada en la confiabilidad, que tuvo como objetivo fundamental hacer coexistir de manera armoniosa las consideraciones más relevantes que se fueron identificando durante el estudio del estado del arte. La propuesta elaborada, que contempla particularmente un Modelo de Madurez en Confiabilidad, también fruto de este trabajo, y que ofrece un Diagrama de Flujo asociado, el que colabora para su mejor entendimiento y aplicación, cumple con el objetivo mencionado en el párrafo anterior. A su vez, la propuesta tam-

bién cumple con otros objetivos planteados inicialmente: su versatilidad para adaptarse a diferentes realidades organizacionales y además, que sea parte de un proceso de mejora continua, característica que resulta ineludible en cualquier estrategia de adopción de una Transformación Digital.

Culminando con el trabajo, se aplicó de forma teórica la propuesta elaborada a un caso de uso teórico, lo que permitió confirmar en un primer ejercicio que es viable su consideración, sin desconocer que se aplicó con algunas simplificaciones coyunturales y que es recomendable y necesario que durante la maduración de la misma se puedan generar nuevas versiones, que se enriquezcan con lecciones aprendidas y visiones de otros actores involucrados.

Sobre el final del cuerpo principal del presente documento se presentan varias líneas de trabajo futuro que no hacen más que demostrar que la temática involucra diversas áreas de investigación, desarrollo e innovación.

En los Anexos del documento, se presenta un importante volumen de información que complementa la contenida en el cuerpo principal, así como también un Anexo dedicado exclusivamente a herramientas de hardware y software, que también son fuente para identificar posibles líneas de trabajo futuro.

Concluyendo, el trabajo realizado permitió confirmar que estamos frente a una temática muy relevante y abarcadora, y que todo hace indicar que su consideración debería ser algo ineludible por las industrias, los estados y los ciudadanos. El producto aquí documentado puede ser una herramienta útil al momento de considerar la adopción de la Industria 4.0, en el marco de lo que debería ser una política de estado.

6.3. Trabajo futuro

Aquí se incluyen algunas propuestas de trabajo futuro vinculadas con la temática abordada en la tesis.

6.3.1. Modelo de Madurez en Confiabilidad (TMM)

Se mencionan posibles trabajos futuros que pueden involucrar al TMM propuesto.

Mejorar el TMM

Mejorar el TMM aquí propuesto considerando, por ejemplo, como insumo el trabajo que al respecto el IIC viene haciendo con respecto a la confiabilidad, y su posible utilización en casos concretos.

Ampliar el TMM

El TMM se elaboró intencionalmente con un perfil horizontal. La comunidad ya se encuentra explorando la elaboración de perfiles del SMM orientados a verticales específicas, por lo que un posible trabajo futuro, que podría complementar y enriquecer a éste, podría ser elaborar Modelos de Madurez en Confiabilidad orientados a determinadas verticales del negocio.

Validar el TMM

Realizar un análisis del TMM, eventualmente basado en Métodos Formales, con el objetivo de verificar con la rigurosidad correspondiente su validez, o en su defecto identificar las mejoras necesarias a aplicarle para que sea válido formalmente.

Herramienta de gestión y simulación

Desarrollar una herramienta que ayude a quien desee aplicar el TMM, a realizar el seguimiento del trabajo, registrar las decisiones y lecciones aprendidas. La misma herramienta podría ser de utilidad para simular el uso del TMM en determinado contexto o para analizar el estado actual de una organización al respecto. Además, el trabajo podría contemplar la integración con otros sistemas ya disponibles en la organización, tanto en el *shop floor* como en el *office floor*.

6.3.2. *Digital Twin - Administration Shell*

A lo largo del trabajo se plasmó la relevancia del concepto de *Digital Twin* (principalmente impulsado por el IIC) así como también la del concepto *Administration Shell* (AS) o *Asset Administration Shell* (AAS), ambos cruciales para la I4.0. En ambos casos, se trata de conceptos y tecnologías involucradas que resultan fundamentales para el despliegue de la Industria 4.0. Un posible trabajo futuro propuesto es investigar, desarrollar e implementar casos de uso donde se pueda evaluar el potencial de los conceptos *Digital Twin* y AS/AAS.

6.3.3. *Manufacturer Usage Descriptor* (MUD)

En este trabajo se identificó que el MUD actualmente se posiciona como una solución que ofrecería la dinámica que demanda el despliegue seguro de dispositivos IoT en diferentes ámbitos. Investigar, desarrollar e implementar casos de uso donde se pueda evaluar el potencial de dicha tecnología podría ser un trabajo futuro de sumo interés.

6.3.4. Planes de Formación

Como se mencionó antes en el documento, y en particular al momento de describir el rol de las partes interesadas en el contexto de la propuesta realizada, la formación de los ciudadanos es un pilar para la adecuada adopción de la Industria 4.0. Por lo expresado, sería muy relevante que un trabajo futuro sea el colaborar con la elaboración de los Planes de Formación relacionados con la Industria 4.0 y tecnologías vinculadas, en las áreas de influencia de la Universidad de la República.

6.3.5. Tecnologías vinculadas a la Industria 4.0

Existen numerosas tecnologías vinculadas a la Industria 4.0 y a la DX [103, 105], en las cuales se identifica un potencial muy relevante, pero por el momento, no siempre adecuadamente analizado, dimensionado y explotado. Ejemplos de ellas son: *big data*, *machine learning*, inteligencia artificial, 5G, analítica de datos, robótica, *time sensitive networking* y *blockchain*. Una posible trabajo futuro (o un conjunto de trabajos) de sumo interés sería investigar el verdadero impacto y el potencial de las diferentes tecnologías vinculadas con la Industria 4.0 y la DX.

6.3.6. Protocolos de red vinculados a la Industria 4.0

Una gran cantidad de protocolos, tanto del "mundo" IT como del "mundo" OT (y de la convergencia de ellos), se han desarrollado o mejorado con motivo de la 4IR y de la Industria 4.0. Varios de ellos han sido mencionados a lo largo del presente trabajo. Una posible trabajo futuro podría contemplar el análisis de los mismos, tanto del punto de vista de sus prestaciones en diferentes ámbitos de aplicación, así como también, respecto a los servicios de seguridad que proporcionan.

6.3.7. Indicadores Clave de Rendimiento (KPIs)

Una adecuada definición de los KPIs a considerar, tanto en cantidad como en calidad, impacta directamente en la adecuada toma de decisiones estratégicas por parte de las organizaciones. Históricamente las organizaciones han tenido una tendencia a utilizar decenas de KPIs, lo que termina abrumando con información, la mayoría de escaso valor, a los tomadores de decisiones, y a su vez queda oculta la información que sí es importante. Investigar cuáles son los KPIs más relevantes para las diferentes verticales del negocio en la Industria 4.0. es un desafío por demás cautivante como trabajo futuro, considerando también su relación directa con mas medidas y las métricas, e incluso cuando en la comunidad se trabaja en poder estandarizar esta temática.

6.3.8. Mantenimiento Predictivo

En lo que refiere al mantenimiento de los diferentes componentes de los sistemas de producción, otros sistemas vinculados y hasta de los productos, se observa una evolución desde el mantenimiento reactivo al predictivo, pasando por el proactivo y el planificado. El "sabor" predictivo resulta extremadamente tentador para las empresas y los usuarios pues tiene un fuerte impacto en la eficiencia de los procesos de producción y en el bienestar de los consumidores. Investigar los beneficios del mantenimiento preventivo, identificar formas de medir los beneficios y estrategias para implementarlo, es un posible trabajo futuro de interés para la comunidad.

6.3.9. *Zero Trust Security*

Diversos factores, algunos puestos de manifiesto durante este trabajo, están haciendo que el paradigma del perímetro de seguridad, donde existen zonas claramente delimitadas (por ejemplo *inside*, *outside* y DMZ) y que a partir de ello podemos pensar en zonas seguras y zonas inseguras, ya no sea (tan) cierto. Es así que ha surgido un nuevo paradigma de seguridad denominado *Zero Trust* [199, 45], donde el modelo del perímetro, a veces conocido como el "modelo del castillo y la fosa" ya no aplica y sí adquiere vigencia el modelo de "cero confianza hasta que se demuestre lo contrario" o también identificado como "*never trust, always verify*", en el sentido de poder validar en todo momento *qué/quién utiliza qué cosa, cómo y cuándo*, antes de que cualquier acción pueda ocurrir.

APÉNDICES

Apéndice 1

RAMI 4.0 - Ampliación de conceptos vinculados al modelo

1.1. *Administration Shell*

La *Administration Shell* (AS) es la implementación del *Digital Twin* en I4.0 [235], concepto que se aborda en la Sección 3.3 del Capítulo 3. Con *Digital Twin* nos referimos a la representación digital del activo físico, y eventualmente también a un modelo de simulación. Con la AS integramos los activos al mundo de la información. Es lo que convierte al activo en un componente I4.0, siendo su representación digital. La AS registra datos del ciclo de vida del activo y los convierte en información. La información asociada puede ser accedida como Vistas y los servicios del *Component Manager* pueden ser accedidos vía APIs.

Estructura básica

En su consideración más general, y como se puede observar en las Figuras 1.1 y 1.2, la AS está dividida en dos bloques: *DF Header* y *DF Body*, componiendo lo que se denomina el *Digital Factory* (DF).

DF Header

El *DF Header* contiene la información para identificar el activo y su uso, en lo que refiere a sus capacidades.

DF Body

En el *DF Body* es donde se almacena la información del activo. Es la portadora de la información.

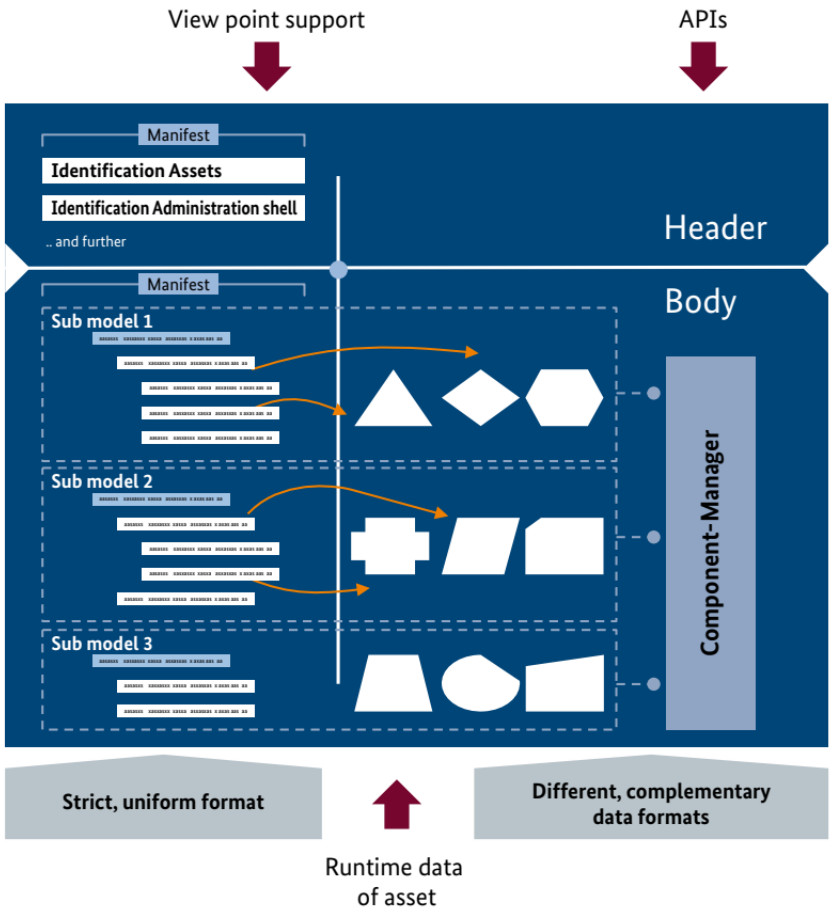


Figura 1.1: Estructura básica de la *Administration Shell*. Fuente: [230]

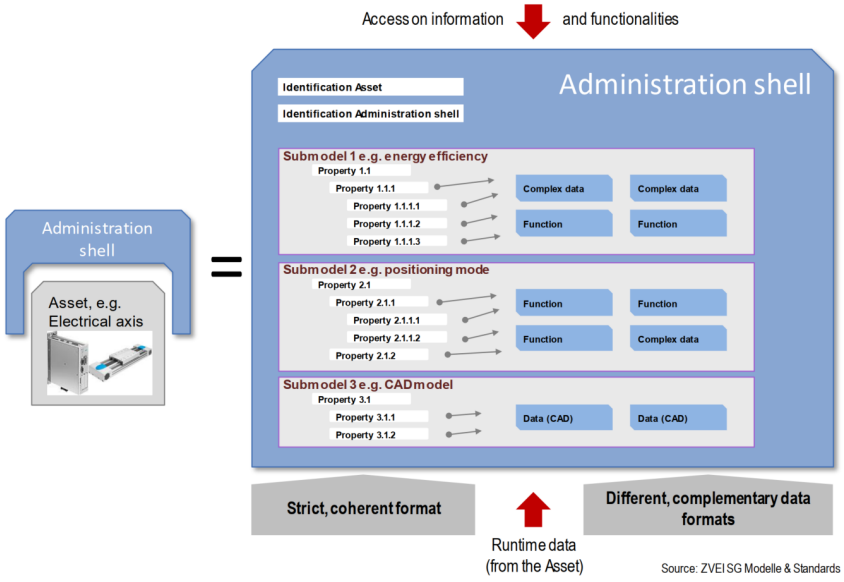


Figura 1.2: Otra visión de la estructura básica de la AS. Fuente: [49]

Modelos parciales

La AS contiene modelos parciales [233, 234] separados, con propiedades y funciones de diferentes dominios, y cada uno con su propio plan de actualizaciones. Los modelos son creados de acuerdo al modelo RAMI 4.0 mientras que las propiedades y funciones respetan una semántica definida.

Cada AS puede, teóricamente, contener cualquier número de modelos parciales, lo que se ejemplifica en la Figura 1.3. Cada modelo parcial mantiene una estructura jerárquica de propiedades vinculada a propiedades y funciones. Los modelos parciales son especificados por expertos en el área temática del dominio en cuestión. Cada modelo parcial especifica propiedades (ver Figura 1.4), datos y funciones de acuerdo a reglas para el *header* y el *body*.

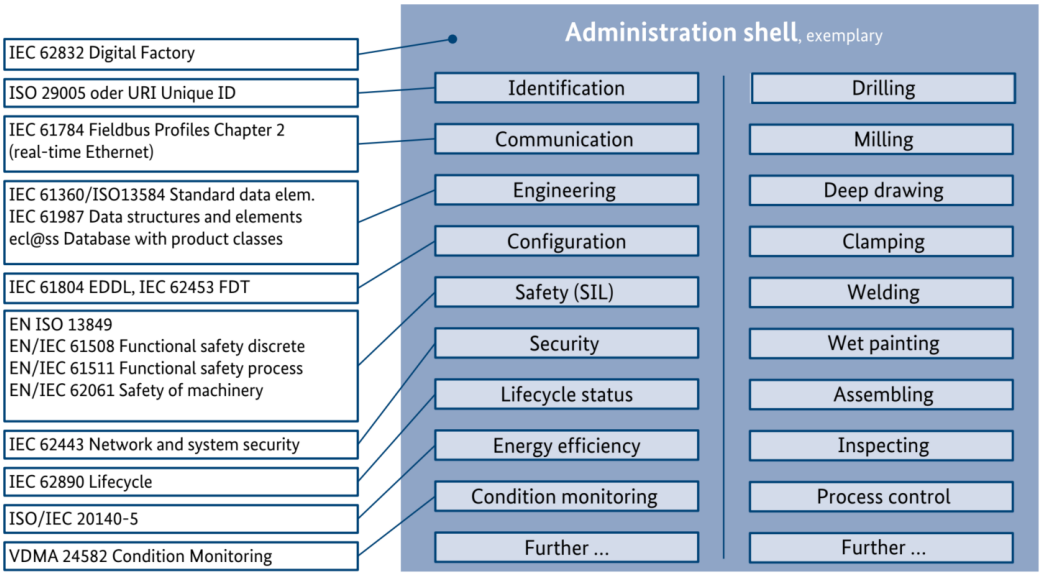


Figura 1.3: Ejemplo de *Administration Shell* con varios submodelos. Fuente: [230]

Existe un conjunto de vistas básicas que son obligatorias para todos los modelos parciales. Otras vistas pueden ser creadas de acuerdo a las necesidades que se identifiquen.

Propiedades

Existen cuatro clases de propiedades, a saber:

Básicas

Aquellas que son obligatorias y se encuentran estandarizadas para todas las AS.

Mandatorias

Las que son obligatorias y se encuentran estandarizadas para modelos parciales de las AS.

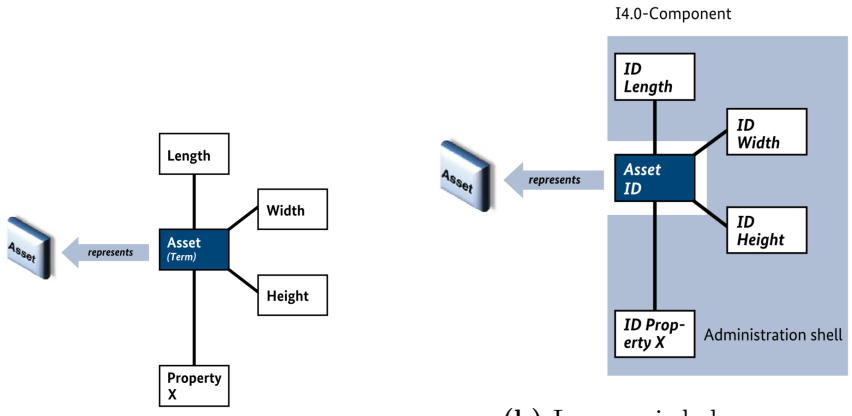
Opcionales

Refiere a las propiedades estandarizadas pero no mandatorias para Aquellas que son obligatorias y se encuentran estandarizadas para todas las AS.

Libres

Propiedades de los modelos parciales de las AS, como por ejemplo aquellas específicas del fabricante, que no están ni estandarizadas ni son obligatorias. Debe ser posible utilizar las propiedades y otros elementos de información de la AS tanto para Tipos como para Instancias. Las propiedades deben poder enumerarse y organizar de manera jerárquica, pueden referenciar a otras propiedades, incluso en otras AS, y también pueden referenciar a datos y funciones de la AS.

Las propiedades deben cumplir aspectos de seguridad de la información para la disponibilidad graduada, integridad, confidencialidad, visibilidad y autenticidad.



(a) Las propiedades permiten caracterizar a los activos en el mundo físico

(b) Las propiedades son almacenadas con su ID en la *Administration Shell* del Componente I4.0

Figura 1.4: Propiedades de los activos. Fuente: [230]

Gestión de la *Administration Shell*

Mediante el *Component Manager* y el *Manifest* la información contenida en la AS es organizada y administrada.

Component Manager

El *Component Manager* permite gestionar la información almacenada y ofrece la posibilidad de realizar *queries* de la misma. Es el enlace entre los servicios técnicos de TI del componente I4.0 que provee acceso externo a la información de la representación, y las funcionalidades técnicas del activo.

Organiza el direccionamiento e identificación de la AS y del activo. Adicionalmente, organiza la administración y el acceso a los recursos del componente I4.0 y se encarga de la protección adecuada respecto al uso del activo.

Manifest

El *Manifest* contiene la información obligatoria del componente I4.0, incluyendo cómo conectarse a activo mediante la identificación apropiada. Se trata de una tabla de contenidos identificable únicamente, con toda la información, datos y funciones de la AS, y la información externamente accesible. Contiene información que puede ser públicamente conocida a los efectos de implementar un sistema I4.0 con la adecuada protección para su uso. El *Manifest* de la AS gestiona los elementos de información en la forma de propiedades, y la propia AS puede incluir datos y funcionalidades técnicas.

Identificadores

Tanto las AS como los activos son identificables unívocamente todo el tiempo, como se muestra en la Figura 1.5. Ello asegura que se pueda establecer la conexión entre ellos incluso si encuentran en repositorios digitales distribuidos o adjuntos, incluso por parte de diferentes participantes de un proceso.

La vida de la *Administration Shell*

Durante la fase de ingeniería es que se planifican las funcionalidades, por ejemplo, un motor con un cierto par y altura del eje. Algunas propiedades del motor se incorporarán en la AS. En un paso siguiente, se elige un Tipo de motor específico de un fabricante, y se agregará más información sobre ese tipo de motor a la AS. El fabricante del motor puede entregar un componente para simular el motor y poder realizar cálculos asociados. Luego, previo a la puesta en marcha, se ordenará el motor, por lo que el Tipo de motor se convierte en una Instancia del motor con un número de serie y datos específicos para ese motor individual. La AS se enriquece de nuevo. Los parámetros de funcionamiento (temperatura, vibraciones, tiempo de trabajo, etc.) se miden durante

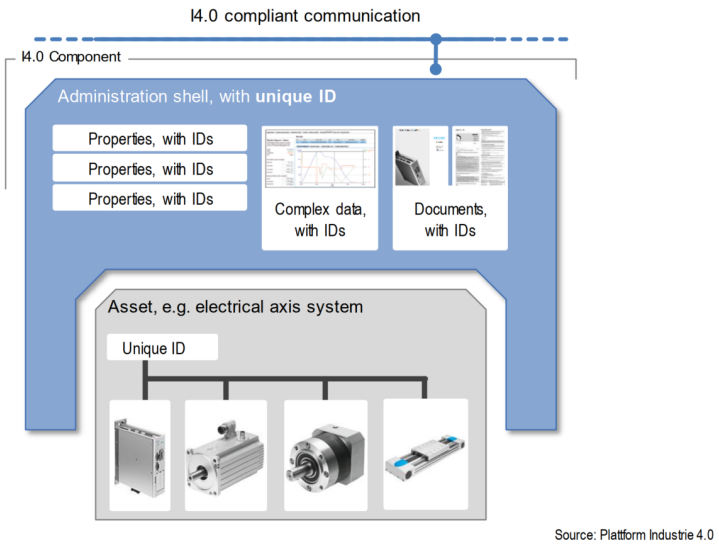


Figura 1.5: Identificador Único para la Administration Shell. Fuente: [230]

el funcionamiento del motor. Esto también se puede registrar en la AS. El mantenimiento se realiza en el motor, y también se puede registrar en la AS. Después del final de la vida útil, el motor se reemplaza con uno nuevo. Este cambio y toda la información sobre el nuevo Tipo e Instancia del motor se puede registrar también. La información en la AS se puede intercambiar entre todos los socios en una cadena de valor: proveedores, socios de ingeniería, integradores de sistemas, operadores y socios de servicio.

La AS incluye información relevante par representar al activo y sus funcionalidades técnicas (rol) o sea, aquello que realiza o debería realizar en un sistema. Provee al mundo de información con datos del activo (o activos), de manera estructura de acuerdo al modelo RAMI 4.0.

Ella puede estar almacenada en el propio activo al que representa, o puede estar distribuida en uno o más sistemas TI, según se puede apreciar en la Figura 1.6.

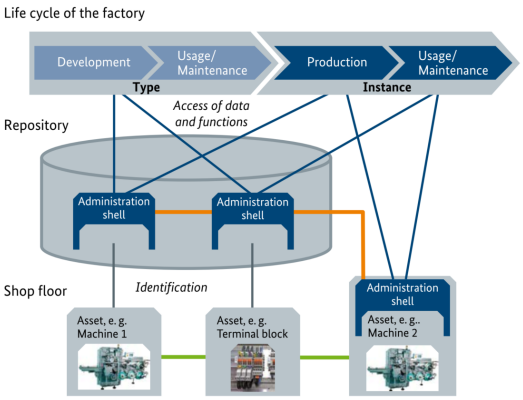


Figura 1.6: Opciones de disponibilidad de la *Administration Shell*. Fuente: [230]

Formas de los componentes I4.0

Un activo puede tener más de una AS, como se representa en la Figura 1.7.

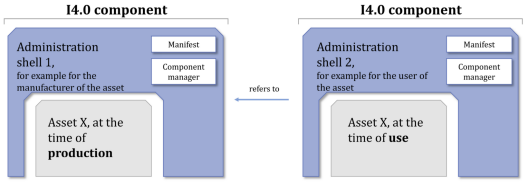


Figura 1.7: Un activo - múltiples *Administration Shells*. Fuente: [49]

Por otro lado, también es posible que una AS represente a varios activos, como lo muestra la Figura 1.8.

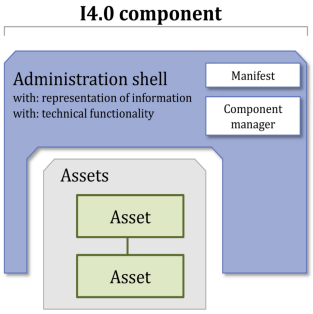


Figura 1.8: Representación de múltiples activos Fuente: [49]

Varios componentes I4.0 relacionados pueden constituir un componente I4.0, como se observa en la Figura 1.9.

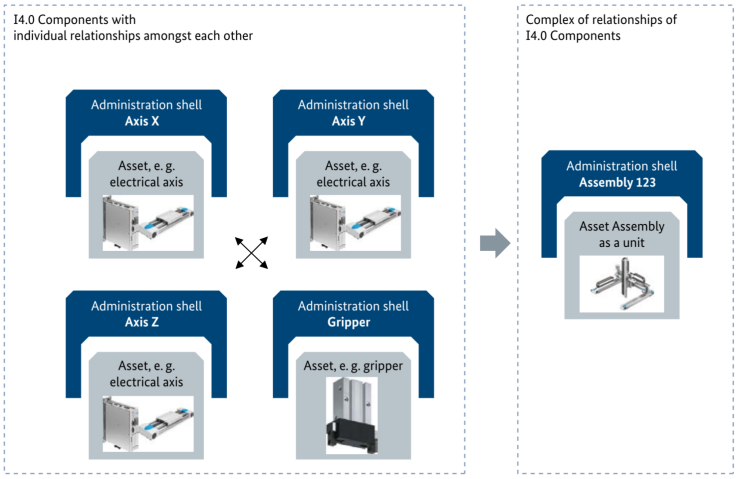


Figura 1.9: Varios Componentes I4.0 relacionados - un Componente I4.0. Fuente: [230]

Propiedad de anidado

Como se observa en la Figura 1.10 cualquier componente I4.0 puede consistir de otros componentes I4.0, lo que conoce como componentes I4.0 lógicamente anidados, incluso con la posibilidad que los componentes anidados sean accedidos desde fuera.

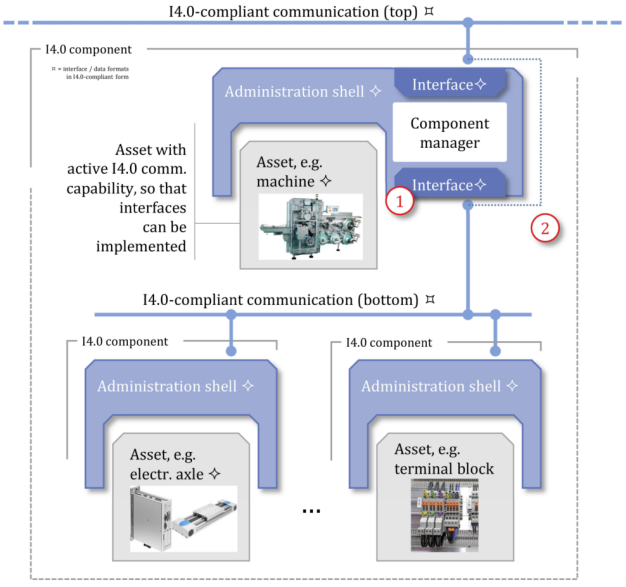


Figura 1.10: Anidado de componentes. Fuente: [49]

Propiedad de encapsulado

De acuerdo a lo que muestra a manera de ejemplo la Figura 1.11, un componente I4.0 debería ser capaz de establecer todas las conexiones necesarias con un sistema I4.0 (1 en la figura). Sin embargo, las conexiones no deben dar lugar a ninguna restricción en su funcionalidad principal (2 en la figura). Las comunicaciones pueden tener lugar a través de una sola conexión (3 en la figura).

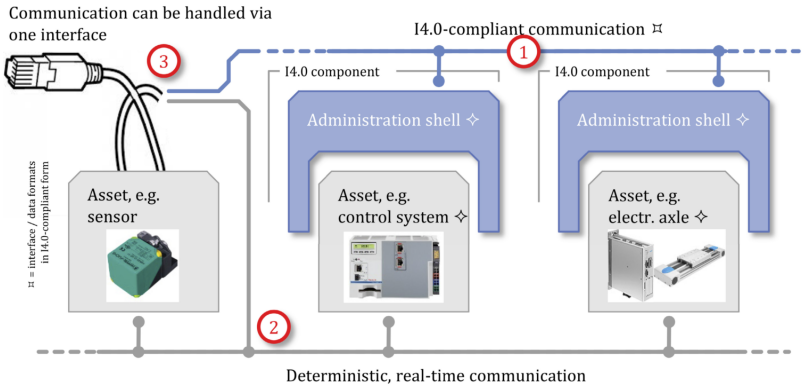


Figura 1.11: Encapsulado de componentes. Fuente: [49]

Apéndice 2

Industrial Internet Consortium

En este apéndice se amplia la información vinculada a diferentes aspectos referenciados en el Capítulo 3.

2.1. *Digital Twin*

Si bien el concepto de *Digital Twin* (DT) como tal apareció en el año 2003, existen ejemplos previos donde el concepto utilizado fue mismo, siendo quizás el ejemplo más famoso, el espejado o emparejamiento del Apolo 13 que realizó [209] el Departamento de Investigación de la NASA en sus instalaciones, a los efectos de definir qué acciones se debían tomar para salvar la vida de los astronautas que se encontraban en él.

Un DT [98, 104, 122] comprende datos, modelos computacionales e interfaces de servicio, según se ejemplifica en la Figura 2.1. Los datos contenidos en el DT son relativos a la entidad y son aquellos requeridos por los modelos con el objetivo de representar y entender sus estados y comportamientos. Pueden ser datos de todo el ciclo de vida de la entidad, de su fase de desarrollo, de su fase de producción, de su fase de operación e incluso de su fase de fin de su vida útil. Adicionalmente puede contener datos del negocio como por ejemplo, registro de transacciones.

Los modelos refieren a aquellos que son requeridos para describir, entender y predecir los estados operacionales de la entidad y sus comportamientos, así como también determinar acciones basadas en la lógica del negocio. A través de las interfaces de servicio las aplicaciones industriales u otros DTs pueden acceder a sus datos y a sus capacidades (invocar a sus modelos).

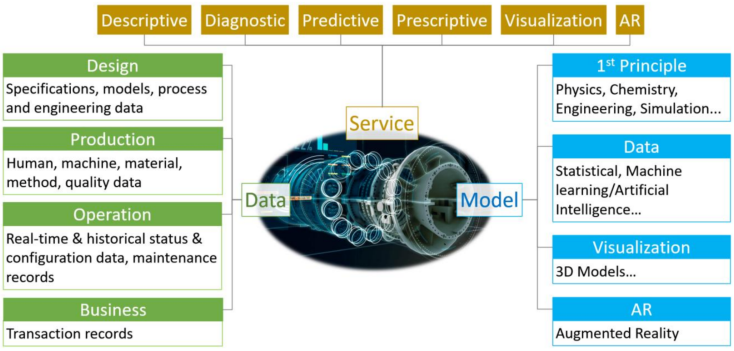


Figura 2.1: Digital Twin. Fuente: [98]

De esta forma, con un DT podemos describir, simular y predecir el estado y el comportamiento de su contraparte del mundo real, ya sea basado en los resultados de la analítica o en los datos en tiempo real, y así responder buscando optimizar su funcionamiento y de esa forma también, que ello aporte a la optimización del resto de los procesos en los que participa.

En la concepción más general, se pueden componer el DT de una entidad a partir de la adecuada combinación (ensamblado) de los DTs que la constituyen, pudiéndose comenzar desde el *Discrete Digital Twin*, que se podría asociar con la entidad atómica que provee valor por si misma sin necesidad de ser dividida.

Se pueden distinguir tres tipos de ensamblados: Jerárquico, por Asociación y *Peer-to-Peer*.

En el ensamblado Jerárquico, un conjunto de DTs se ensamblan para componer otro DT y éste, se ensambla con otros con el mismo objetivo, pudiéndose repetir la idea. En el ensamblado por Asociación, los DTs se asocian reflejando lo que ocurre entre las entidades de las cuales son gemelos. Finalmente, en el ensamblado *Peer-to-Peer*, se trata de DTs que representan entidades del mismo tipo realizando la misma tarea.

Los DT son una forma de combatir los silos de información relacionada con las entidades a lo largo de su vida útil. Uno de los mayores desafíos al respecto es permitir el intercambio de información entre los DTs, la cual puede llegar en cualquier momento y en cualquier formato.

Algunos aspectos técnicos a tener en cuenta para el desarrollo, despliegue y mantenimiento de los DTs son el modelado, la incorporación y el sincronizado de la información, las APIs para interactuar con otros componentes, la conectividad, el despliegue y la interoperabilidad.

La Internet Industrial y la Fabricación Inteligente se pueden ver como un

movimiento entrelazado en el contexto de la transformación digital industrial. Ello comprende la incorporación de nuevas tecnologías en conjunción con el uso de los datos y la información de los procesos y sistemas de fabricación con el objetivo de aumentar la productividad, la flexibilidad, la calidad, reducir los costos, mejorar la calidad de vida y cuidar el medioambiente.

Para conseguir lo anterior, es necesario que se acceda a la información necesaria y en el momento oportuno para tomar las decisiones adecuadas en tiempo y forma. Es así que en este contexto se puede identificar tres ciclos de optimización controlados por los datos, a saber: el Ciclo de las Operaciones, el Ciclo del Negocio y el Ciclo del Control de las máquinas.

Una adecuada implementación de estos ciclos de optimización es clave para una adecuada adopción de la Industrial Internet y avanzar así a la Fabricación Inteligente.

Para ello, se requiere de datos, analítica y aplicaciones actuando de la siguiente manera:

Los datos provienen de fuentes muy diversas, de equipos y sistemas, tanto en OT como en IT. La analítica (modelos) permite analizar los datos recolectados y la información generada a partir de ellos para saber respecto a los procesos de producción y otros asociados (logística, ventas), poder conocer qué va a ocurrir, cuándo, y poder tomar decisiones al respecto, progresando de lo descriptivo a lo diagnóstico, predictivo y prescriptivo, lo que incrementa la complejidad de la analítica demandada, al hacerla más profunda, pero a su vez resulta en una analítica más amplia, pasando de analizar cada entidad a analizar los procesos. Finalmente, las aplicaciones permiten que la lógica del negocio transforme las ideas que surgen de la analítica en decisiones y acciones dirigidas a las personas o a los propios dispositivos.

Un DT no es un *proxy* para un dispositivo y tampoco es una interfaz de comandos o *shell* para un dispositivo. Es un medio para visualizar un dispositivo y emular lo que podría suceder operativamente. La arquitectura debe permitir al usuario responder las preguntas de "qué pasaría si..." a partir de datos reales de sistemas en ejecución. Por lo tanto, es algo que va bastante más allá de la simulación, pudiendo abarcar también las fases de diseño, desarrollo, despliegue y servicio.

El paradigma DT, al igual que cualquier avance tecnológico con algún componente de conectividad, incrementa el número de vulnerabilidades (o superficie de ataque) y el potencial impacto de ello se ve amplificado por el nivel de

despliegue real y/o previsto y el ámbito donde ocurre.

2.2. *Viewpoints* en detalle

En esta sección se brinda una descripción más detallada de los *viewpoints* de la IIRA.

2.2.1. Punto de Vista del Negocio

El punto de vista del negocio enmarca la visión, los valores y los objetivos de las partes interesadas del negocio en el establecimiento de un sistema IIoT en su contexto empresarial y regulatorio.

Los asuntos de interés orientados al negocio, como el valor empresarial, el retorno esperado de la inversión, el costo de mantenimiento y el pasivo del producto, deben evaluarse al considerar un sistema IIoT como una solución a los problemas empresariales.

Los tomadores de decisión del negocio y otras partes interesadas tienen una Visión del futuro de la organización y la dirección que deben seguir sus negocios. La percepción de la Visión por parte de las partes interesadas se denominan Valores. Los Objetivos Claves son los resultados medibles, de alto nivel, que permite cuantizar si el sistema brinda lo que se espera de él. Las Capacidades Fundamentales refieren a las especificaciones de alto nivel del sistema, las que se deben brindar sin depender de cómo se implementan. De los Objetivos Claves se derivan las Capacidades Fundamentales.

A los efectos de determinar el cumplimiento de los objetivos del negocio, también se debe considerar el cumplimiento de las características del sistema.

2.2.2. Punto de Vista del Uso

El punto de vista del uso está vinculado con cómo el sistema IIoT realiza las capacidades claves identificadas en el Punto de Vista del Negocio. El Punto de Vista del Uso describe las actividades (cómo es usado el sistema) que coordinan varias unidades de trabajo sobre varios componentes del sistema. Las actividades sirven de guía para el diseño, la implementación, el desarrollo, la operación y la evolución del sistema IIoT.

Cada actividad tendrá un "disparador" (Condiciones de Inicio), estará integrada por un conjunto de tareas coordinadas y tendrá restricciones (Características del Sistema) que se deberán preservar durante la ejecución de las tareas y luego de alcanzar el nuevo estado.

En el Capítulo 5 de la IIRA se presenta un modelado de los diferentes conceptos involucrados en este Punto de Vista y cómo se relacionan, siendo ellos: tarea, actividad, rol, parte y sistema.

2.2.3. Punto de Vista Funcional

El avance de las TIC de los últimos años se pueden aplicar a la Internet Industrial para transformar drásticamente los sistemas de control industrial en dos temas principales: el aumento de la autonomía colaborativa local y el incremento de la optimización del sistema a través del orquestado global.

El aumento de la autonomía colaborativa local implica que, con el crecimiento del poder computacional embebido, aumenta la capacidad analítica local que considere no solo los aspectos físicos sino que también el entorno. Ello hace que se migre de la automatización a la autonomía. Sumado a ello, la ubicuidad de la conectividad facilita la colaboración entre los sistemas.

El incremento de la optimización del sistema a través del orquestado global significa que a partir de los datos colectados por diferentes sensores y con la analítica aplicada adecuadamente, la información obtenida puede ser llevada al nivel del negocio y tomarse allí las decisiones que tiendan a la optimización de las operaciones de manera orquestada.

Con el objetivo de analizar adecuadamente el punto de vista funcional, se introduce el concepto de Dominio Funcional. Esta descomposición en cinco dominios funcionales reafirma la relevancia de cada uno de ellos y las diferentes prioridades según la vertical industrial. Los Dominios Funcionales se describen a continuación.

Dominios Funcionales

Los cinco Dominios Funcionales, como se puede apreciar en la Figura 2.2, son:

- Control
- Operaciones

- Información
- Aplicación
- Negocio

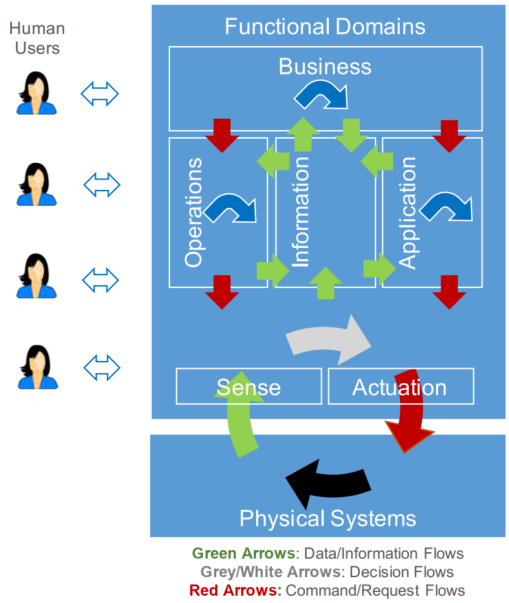


Figura 2.2: Dominios Funcionales. Fuente: [110]

Los flujos de datos y los flujos de control fluyen entre los dominios funcionales.

Los ejercicios de orquestado, coordinación y control tienen diferente granularidad y ciclos de tiempo en cada dominio funcional.

A continuación se describe cada uno de los Dominios Funcionales.

Dominio de Control

El Dominio de Control es un dominio funcional para implementar los Sistemas de Control Industrial (ICS, por su sigla en inglés). Básicamente comprende la lectura de datos mediante los sensores, el aplicado de reglas y poder ejercer el control sobre el sistema físico mediante actuadores. Esto requiere en general alta precisión y resolución. Son sistemas que generalmente se encuentran cerca del componente físico sobre el que actúan; en general, el acceso físico a ellos no es sencillo y la seguridad física es relevante.

Como lo muestra la Figura 2.3, es posible realizar una descomposición funcional del Dominio de Control, con diferentes niveles de complejidad y sofisticación según el sistema o el componente en cuestión.

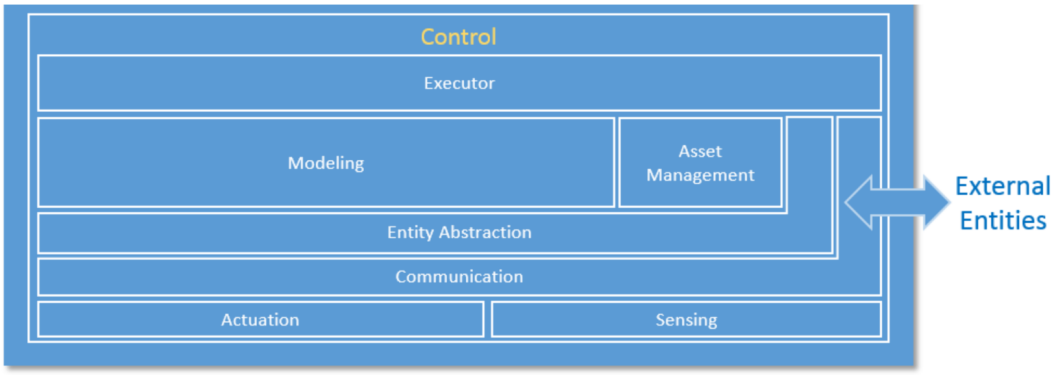


Figura 2.3: Descomposición Funcional del Dominio de Control. Fuente: [110]

Las siete funciones que se identifican en el Dominio de Control son:

- "Sensado"
- Actuación
- Comunicación
- Abstracción de la entidad (a través de una Representación Virtual)
- Modelado
- Gestión del Activo
- Ejecutor

El "Sensado" es función encargada de la lectura de los datos desde los sensores. La Actuación es la función que escribe señales de datos o control al actuador. La Comunicación conecta con sensores, actuadores, controladores, *gateways* y otros sistemas; en general existen requerimientos de calidad de servicio como ser *jitter*, retardo, ancho de banda, fiabilidad y resiliencia. La Representación Virtual se encarga de gestionar la semántica utilizada para los mensajes que son intercambiados entre los elementos del sistema. El Modelado trata con el entendimiento de los estados, condiciones y comportamientos de los sistemas bajo control y otros sistemas con los que interactúa. La complejidad del modelado depende del sistema en cuestión y puede incluir consideraciones analíticas para la toma de decisiones en tiempo real. A la función de modelado puede estar asociada una subfunción de gestión de los datos. La Gestión del Activo incluye, entre otras responsabilidades, operaciones de gestión del sistema de control, configuración, actualización de software/firmware y otras operaciones a lo largo del ciclo de vida del sistema. El Ejecutor se encarga de impactar la lógica de control para el entendimiento de los estados, condiciones

y comportamiento del sistema bajo control y su entorno, de acuerdo a los objetivos de control. Es el responsable de asegurar que las políticas que están a su alcance se apliquen, considerando también las Características del Sistema ("transversales").

Dominio de Operaciones

El Dominio de Operaciones es el dominio funcional encargado de gestionar y operar el dominio de control. Se encarga de tareas de aprovisionamiento, gestión, monitorizado y optimización de los sistemas en el dominio de control, y no solo restringuido a la planta física, sino que también considerando diferentes plantas, fletes, clientes y recursos de logística. Esto habilita el agregado de valor tanto desde la visión del negocio como también desde el cliente.

En el Dominio de Operaciones también es posible realizar una descomposición funcional donde, a través del dominio de control se brinde apoyo a varios clientes.

Como se observa en la Figura 2.4 las cinco funciones identificadas son:

- Aprovisionamiento y Despliegue
- Gestión del Activo
- Monitorizado y Diagnóstico
- Pronóstico
- Optimización

La función de Aprovisionamiento y Despliegue es en sí el conjunto de funciones requeridas para configurar, iniciar, registrar, realizar un seguimiento del activo, desplegar y retirar el activo de las operaciones. La Gestión del Activo incluye el conjunto de funciones que permiten dar comandos a los activos a través de los sistemas de control, y en el sentido inverso conocer la reacción a los mismos; en algunos casos, puede requerir la incorporación de capacidades adicionales(cómputo, almacenamiento, conectividad) al activo. El Monitorizado y Diagnóstico habilita la detección y predicción de problemas que pueden ocurrir. Busca monitorizar en tiempo real indicadores claves de la salud del activo, realizar un diagnóstico de la causa e informar, ayudando así a reducir los tiempos de respuesta. El Pronóstico consiste en el conjunto de funciones que proporcionan un análisis predictivo del sistema IIoT; a partir de un histórico de datos vinculados al activo y de un proceso analítico adecuado, tiene como

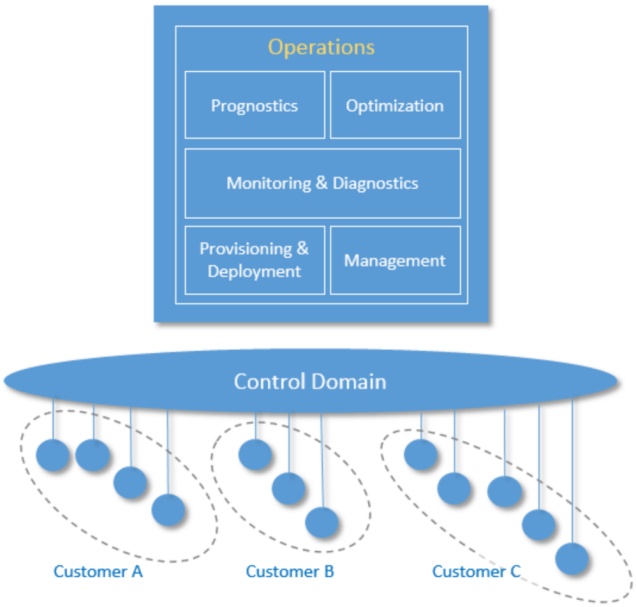


Figura 2.4: Descomposición Funcional del Dominio de Operaciones. Fuente: [110]

objetivo identificar potenciales problemas antes que ocurran y brindar recomendaciones para mitigarlos. La Optimización tiene como objetivo mejorar la fiabilidad y el rendimiento del activo, reduciendo el consumo de energía, incrementando la disponibilidad e informando cómo el activo es utilizado.

Las funciones de Diagnóstico, Pronóstico y Optimización requieren de actividades analíticas con volúmenes importantes de datos e información, por lo tanto, un enfoque adecuado es usar o compartir estas funcionalidades que están disponibles en el Dominio de Información.

En la Figura 2.5 se pueden observan las funciones de los dominios de la Información, de Aplicación y del Negocio. A continuación se describirá brevemente cada uno de ellos.

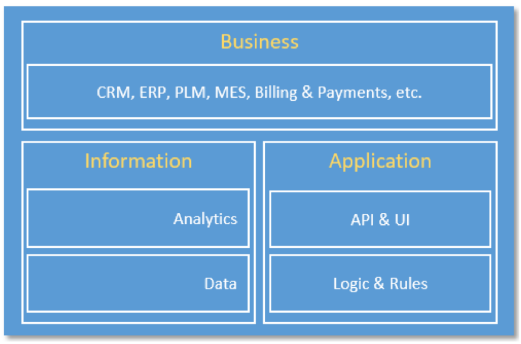


Figura 2.5: Dominios de Información, Aplicación y Negocio. Fuente: [110]

Dominio de Información

Se trata de un dominio destinado a gestionar y procesar datos. Representa el conjunto de funciones destinadas a recopilar datos de varios dominios, de manera más significativa del Dominio de Control, y así transformar, conservar y modelar o analizar esos datos para adquirir inteligencia de alto nivel sobre el sistema en general.

La recolección y el análisis de datos de este dominio complementa a lo que ocurre en el Dominio de Control; en éste, el uso primordial es el control inmediato del sistema, mientras que en el Dominio de Información lo es la toma de decisiones, la optimización de las operaciones del sistema en su conjunto y poder tener una visión de más largo plazo de mejora del sistema. Los componentes que implementan estas funciones pueden no estar ubicados junto, ni cerca, de sus contrapartes del Dominio de Control.

En el Dominio de la Información podemos identificar dos funciones: Datos y Analíticas.

La función de Datos incluye: ingresado de datos de sensores y operaciones, calidad de los datos, transformación sintáctica, transformación semántica, persistencia, almacenamiento y distribución. Las modalidades para la gestión de los datos pueden ser tanto *offline* (*batch*) como *online* (*real time*), e incluso combinadas. Es notoria la necesidad de contemplar los mecanismos más adecuados de protección de los datos.

La función de Analíticas incluye, de manera general, el modelado y el procesado adecuado de los datos. En este caso, los modos *offline* (*batch*) y *online* (*streaming*) son posibles. En el primero de los modos mencionados (*offline*), la salida puede tener más sentido para el Dominio del Negocio mientras que en el segundo (*online*), para el Dominio de las Aplicaciones, dada las características de la información generada y para quién tiene más relevancia el valor de la misma.

Dominio de Aplicación Representa la colección de funciones que implementan las funcionalidades específicas del negocio, así como las APIs y las interfaces de usuario que las aplicaciones exponen para su consumo y para que se pueda interactuar con ellas.

Dominio del Negocio

El Dominio del Negocio representa las funciones empresariales que soportan

los procesos del negocio y de procedimiento que un sistema IIoT debe integrar para permitir las operaciones deseadas, *end-to-end*, de los sistemas IIoT.

Ejemplos de esas funciones se pueden traducir en sistemas como *Enterprise Resource Planning* (ERP), *Customer Relationship Management* (CRM), *Product Lifecycle Management* (PLM), *Manufacturing Execution System* (MES) y *Human Resource Management* (HRM). Puede contemplar también la gestión de activos, la gestión del ciclo de vida del servicio, los sistemas de facturación y pago, y los sistemas de planificación y programación del trabajo.

2.2.4. Punto de Vista de Implementación

Este Punto de Vista tiene que ver con los aspectos que hacen a la implementación de las capacidades y la estructura del sistema IIoT. Involucra las tecnologías y sistemas requeridos para implementar las funciones y actividades dictadas por los Puntos de Vista Funcional y de Uso.

La selección de la arquitectura del sistema IIoT y de las tecnologías a utilizar está guiada por el Punto de Vista del Negocio, considerando aspectos como costos, restricciones de *time-to-market*, estrategias empresariales, aspectos regulatorios y perspectiva de evolución tecnológica.

Además, la implementación deberá tener en cuenta también los requerimientos del sistema y particularmente aquellas características claves del mismo.

El Punto de Vista de Implementación deberá entonces describir, al menos, los siguientes aspectos: arquitectura del sistema IIoT (componentes, topología), descripción técnica de los componentes (interfaces, protocolos, comportamientos), mapas de implementación (de Uso a Funcional, de Funcional a Implementación y, de Características Claves del Sistema).

2.3. Ejemplos de Patrones de Arquitectura

La IIRA presenta tres patrones referenciales, que por supuesto admiten variantes; ellos están elaborados en base a experiencias reales de despliegue de sistemas IIoT, que pueden utilizarse como punto de partida para elaborar la arquitectura del sistema en cuestión.

Los Patrones de Arquitectura identificados son:

- Tres Niveles (*Three-Tier*)

- Gestión y Conectividad en el Borde mediante *Gateway*
- Bus de Datos en Capas

Los dos últimos se pueden considerar variantes del primero.

Los tres niveles considerados en el primer patrón de arquitectura mencionado, *Three-Tier*, según se puede apreciar en la Figura 2.6, son: *Edge*, *Platform* y *Enterprise*.

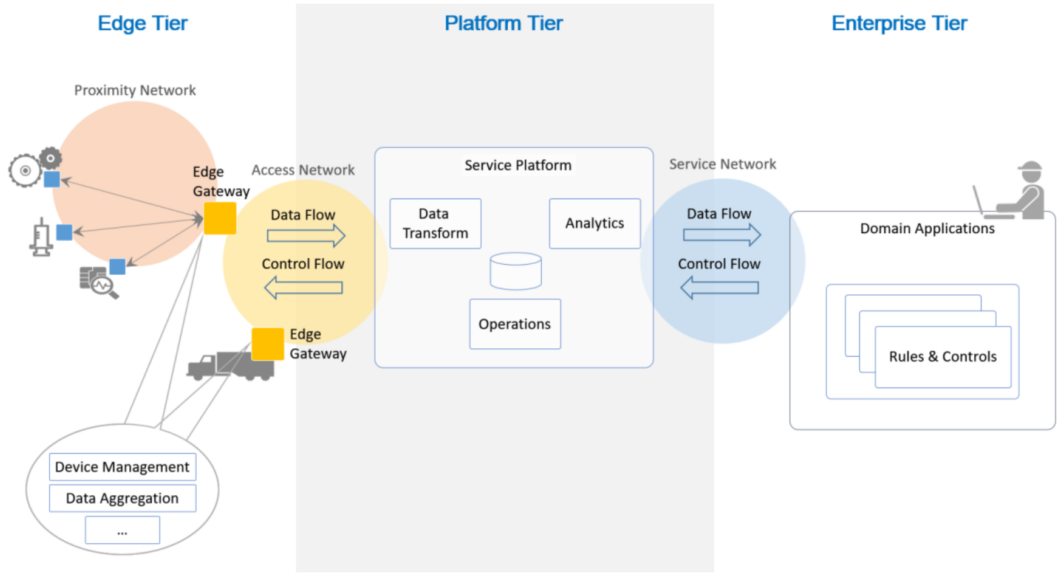


Figura 2.6: Patrón de Arquitectura *Three-Tier*. Fuente: [110]

El nivel *Edge* colecta datos de los nodos de la periferia utilizando red de proximidad. El nivel *Platform* recibe, procesa y reenvía comandos de control desde el nivel *Enterprise* al nivel *Edge*. Además, consolida los procesos y analiza los datos que vienen de los otros niveles y provee funciones de gestión de dispositivos y activos en general. Incluye además tareas de analítica. Finalmente, el nivel *Enterprise* implementa aplicaciones específicas de los dominios, sistemas de decisión, y allí se proveen las interfaces para los usuarios finales. Este nivel recibe flujos de datos de los otros dos niveles y genera comandos de control para ellos también.

Como se muestra en la Figura 2.7, es posible además, realizar un mapeo de la arquitectura de Tres Niveles con los dominios funcionales del Punto de Vista Funcional, lo que conduce, sin excesiva rigurosidad, a que el Dominio de Control se mapea principalmente con el nivel *Edge*, los Dominios de Operaciones y de Información se mapean con el nivel *Platform*, y los Dominios

de Aplicación y Negocio se mapean con el nivel *Enterprise*. Una vez más, es importante resaltar que esto se debe tomar como una referencia y no como una guía que imponga restricciones a la hora de diseñar la arquitectura del sistema IIoT.

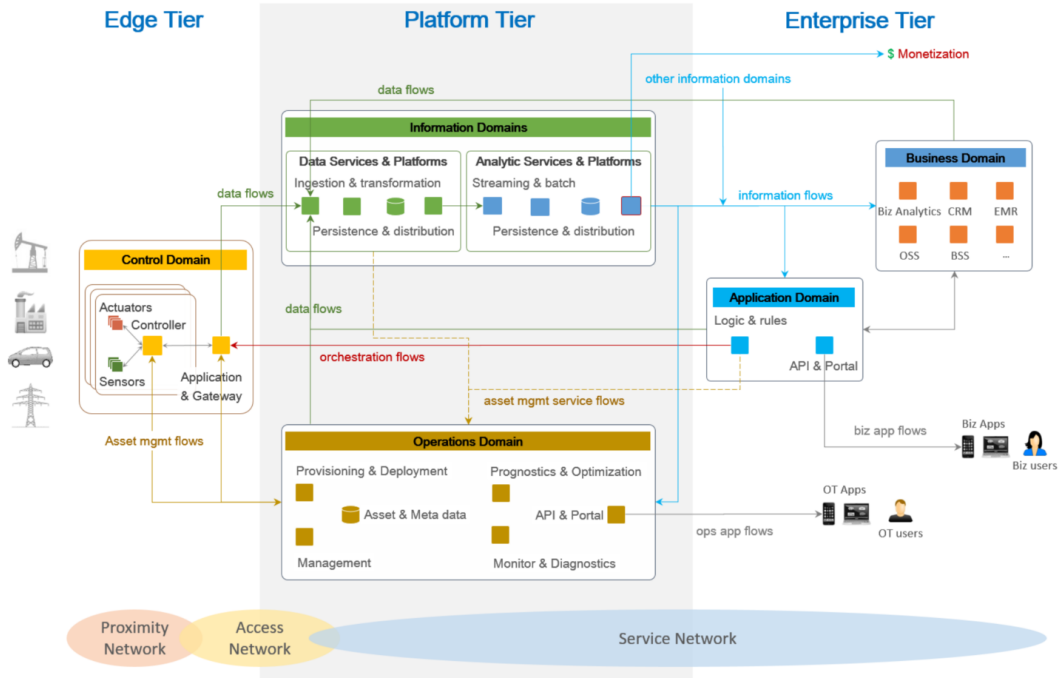


Figura 2.7: Mapeo del patrón *Three-Tier* con los Dominios Funcionales. Fuente: [110]

El segundo patrón de arquitectura mencionado, denominado Gestión y Conectividad en el Borde mediante *Gateway*, y de acuerdo a la Figura 2.8, implica la existencia de una solución de conectividad local en el *Edge* del sistema IIoT, que oficia de *bridge* desde y hacia la WAN, ofreciendo la posibilidad de aislar eventuales complejidades y además, brindando eventuales soluciones no disponibles, como por ejemplo, relacionadas con la seguridad de las comunicaciones.

Finalmente, el patrón de arquitectura de Bus de Datos en Capas, según se observa en la Figura 2.9, puede proporcionar comunicaciones de datos punto a punto de baja latencia, seguras y punto a punto a través de capas lógicas del sistema. Es más útil para los sistemas que deben administrar interacciones directas entre aplicaciones en planta, como el control, la supervisión local y el análisis perimetral.

La federación de estos sistemas en un "sistema de sistemas" permite aplicaciones complejas, a escala de Internet, potencialmente basadas en la nube,

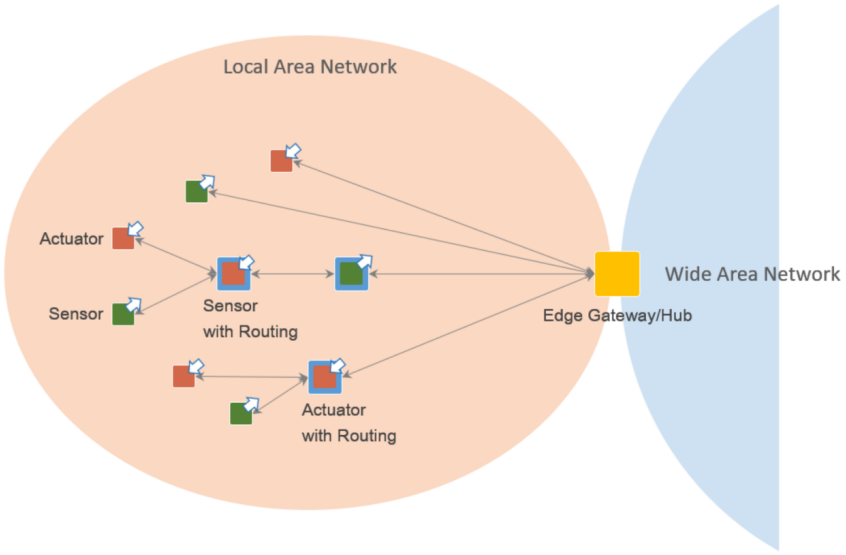


Figura 2.8: Patrón de Arquitectura con *Gateway*. Fuente: [110]

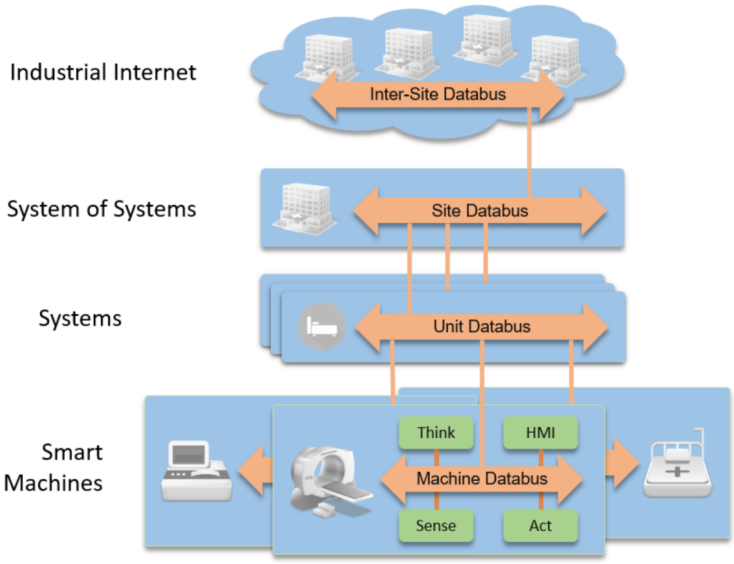


Figura 2.9: Patrón de Arquitectura de Bus de Datos en Capas. Fuente: [110]

con supervisión, control y poder de analítica. La Figura 2.10 ejemplifica este concepto.

La incorporación de adaptadores (*Databus Gateways*) entre capas permiten separar y conectar dominios de seguridad, o actuar como puntos de interfaz para integrar sistemas heredados o protocolos diferentes.

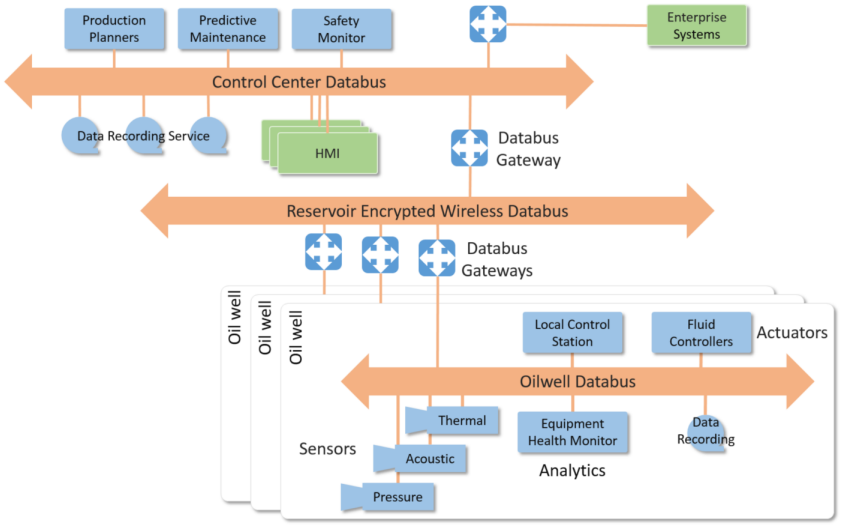


Figura 2.10: Patrón de Arquitectura de Modelo Federado. Fuente: [110]

2.4. Gestión de riesgos

En el contexto de la temática abordada en este trabajo, mantener el valor del negocio requiere salvaguardar la inversión empresarial en sistemas IIoT y proteger del riesgo a sus operaciones.

Los elementos de riesgo de seguridad abordan la probabilidad de que ocurra un evento incluyen amenazas y actores que pueden intentar explotar las vulnerabilidades del sistema a menos que se desplieguen contramedidas para mitigar el riesgo. Las amenazas pueden ser inadvertidas (provenientes de peligros no identificados) o intencionales (provenientes de atacantes).

Varios elementos de riesgo definen el impacto de un evento, incluido el valor del activo, los daños a la reputación, los posibles problemas de responsabilidad y eventuales problemas físicos y de seguridad, como consecuencia de la mala operación de los procesos físicos.

Como no es factible eliminar todo riesgo de un sistema, se lo debe gestionar para que las inversiones en seguridad se equilibren con los efectos de resultados indeseables. Para gestionar los riesgos, la organización debe evaluarlos periódicamente, decidir en qué partes del programa de seguridad invertir, desplegar y revaluar periódicamente tanto los riesgos como la eficacia del programa.

El riesgo de seguridad se puede abordar de varias maneras:

- Evitándolo
- Mitigándolo

- Transfiriéndolo
- Aceptándolo

El evitado de los riesgos busca eliminar el riesgo por completo para evitar toda exposición. A menudo, el evitado completo del riesgo sólo se puede lograr mediante la eliminación de la funcionalidad que lo causa.

La mitigación de los riesgos se traduce en implementar medidas compensatorias para reducir el impacto de una amenaza inevitable. La mitigación es la estrategia más aplicable cuando no se puede lograr la prevención de lo riesgos. Por ejemplo, se implementa con un enfoque sistemático para la seguridad del software, la auditoría y la gestión de parches.

Respecto a la transferencia del riesgo (a un tercero), lo más común es en forma de seguro, donde el riesgo es aceptado por el tercero a cambio de un pago. La transferencia es una técnica común para incidentes de alto impacto y baja frecuencia que tienen costos de mitigación inaceptablemente altos.

La aceptación de riesgos no reduce el riesgo; simplemente significa que uno lo acepta. Esta estrategia se aplica generalmente cuando el costo de la mitigación excede el costo de un incidente adverso en caso de materializarse.

El Riesgo Residual, que se debe seguir gestionando, es el riesgo que queda luego que se adoptaron las contramedidas de acuerdo a cómo se abordó.

La toma de decisiones empresariales eficaces es un componente importante de los programas de seguridad industrial. Los riesgos asociados a la seguridad, así como los costos y beneficios de las diferentes posturas defensivas, deben comunicarse eficazmente a los responsables de la toma de decisiones empresariales, especialmente porque con frecuencia no están familiarizados con la temática.

Programas de Seguridad

Los programas de seguridad abarcan una amplia gama de tecnologías y actividades esenciales para una postura de seguridad completa y sólida. Por ejemplo, el NIST, en su publicación *Framework for Improving Critical Infrastructure Cybersecurity* [186], y que se describe en la Sección 4.3.2 del Capítulo 4, identifica cinco actividades esenciales:

- Identificar
- Proteger

- Detectar
- Responder
- Recuperar

En este modelo, la gestión de riesgos es principalmente un proceso empresarial, mientras que la implementación es técnica y operativa. El proceso de implementación proporciona insumos de activos, vulnerabilidad y experiencia para el proceso de gestión de riesgos, y el proceso de gestión de riesgos proporciona prioridades, decisiones políticas y presupuestarias para el proceso de implementación.

Evaluación de Riesgos

El IIC define el riesgo en el negocio como el efecto de la incertidumbre en los objetivos y define el riesgo en seguridad de la información como el potencial que una amenaza explote alguna/s vulnerabilidad/es de un activo o grupos de activos y así causar daño a la organización. Como vemos, en el contexto de seguridad de la información se utiliza el concepto de amenaza en lugar del término incertidumbre.

Las amenazas más comúnmente discutidas provienen de atacantes maliciosos que desean interrumpir un sistema, robar información o causar daño o miedo, pero incluso un sistema adecuadamente asegurado debe tener en cuenta fallas en el entorno operativo, como ser condiciones medioambientales o climáticas extremas. El término amenaza, entonces, debe interpretarse en términos generales para incluir cualquier influencia o incidente que pueda interferir con el uso normal y previsto del sistema considerado.

Si bien no es práctico anticipar todas las posibles amenazas, un fuerte modelo de seguridad que contemple cambios en el entorno operativo puede mitigar el impacto de muchas situaciones no planificadas.

La identificación de las amenazas y sus consecuencias requiere una comprensión del sistema general y de su implementación. Los elementos de un sistema IIoT o los servicio expuestos a posibles ataques, se denominan Superficie de Ataque. El crecimiento en el número de dispositivos, de tecnologías y el aumento de la complejidad asociada (incluso fruto de la hiperconectividad) aumentan la Superficie de Ataque y las vulnerabilidades del sistema, aumentando así el riesgo.

Cada uno de los elementos (sistema/s, servicio/s) puede ser vulnerable a través de un Vector de Ataque: un mecanismo por el cual puede tener lugar un ataque. Los Vectores de Ataque incluyen, entre otros, ataques físicos, a las redes, contra el software, a los operadores y, a las cadenas de suministro de los elementos que componen el sistema. Cada industria tiene un conjunto específico de Vectores de Ataque, al igual que cada clase de tecnología. El impacto de cada tipo de ataque depende de las prioridades del negocio, del diseño y del sistema.

Los enfoques para enumerar las amenazas cibernéticas y los métodos de ataque incluyen listas de Vectores de Ataque pudiendo citar como referencias a OWASP [206], y a STRIDE [176] si hablamos de identificar y modelar amenazas. Es importante destacar que STRIDE ya no es mantenido por Microsoft, habiendo desarrollado una nueva solución que lo contempla y amplia, denominada *Microsoft Security Development Lifecycle* (SDL) [175] con la herramienta *Threat Modeling Tool* [177] como su *core*.

2.5. Análisis y Gestión de la Confiabilidad

En esta sección se documenta la estrategia propuesta en el *white paper Managing and Assessing Trustworthiness for IIoT in Practice* [120] para realizar un adecuado análisis y gestión de la Confiabilidad, así como otros aspectos relevantes vinculados a ello.

2.5.1. Definiciones

A continuación se define un conjunto de conceptos que son la apoyatura para identificar, por un lado el estado actual de un sistema respecto a la confiabilidad y por otro, el estado deseado u objetivo.

Criterio de Confiabilidad
Indicador de confiabilidad de un componente o subsistema en el contexto de un sistema IIoT, para una característica particular de la confiabilidad.

Interpretación de la Confiabilidad
El conjunto de todos los Criterios de Confiabilidad establecidos para todos los componentes o subsistemas del sistema IIoT.

Métrica de Confiabilidad
Una forma de estandarizar las medidas, que se deriva de estas y permite reunir evidencia acerca de un Criterio de Confiabilidad o varios. Puede ser cualitativa o cuantitativa.

Vector de Evaluación de Confiabilidad (*TA-vector*)
El conjunto de las Métricas de Confiabilidad definidas para interpretar la Confiabilidad de un sistema.

Objetivo de Confiabilidad
El objetivo definido para una Métrica de Confiabilidad.

Vector Objetivo de Confiabilidad (*TT-vector*)
Define el objetivo de Confiabilidad para cada métrica que aparece en el Vector de Evaluación de Confidencialidad.

***Key Performance Indicators* (KPIs)**
Los Indicadores Claves de Rendimiento son métricas que aplican a las operaciones de un negocio, desde las operaciones y logísitica, hasta aspectos financieros y objetivos estratégicos. Si bien generalmente no son métricas de confiabilidad, sí se pueden ver afectadas por las consideraciones de implementación de la confiabilidad.

Factor de Cambio
Cualquier cambio intencional en el sistema con el objetivo de afectar la Interpretación de la Confiabilidad o una mejora en el resultado de las métricas. Los cambios pueden ser en procesos, políticas, configuración, operación, de arquitectura, entre otros.

Implementación de Confiabilidad
Los dos vectores definidos antes (*TA-vector* y *TT-vector*) son utilizados para evaluar y realizar un seguimiento en el tiempo de la confiabilidad de un sistema y sus partes, y deberían reflejar el nivel de confianza que la organización tiene en los datos (evidencia) reflejada en los vectores. Además, dichos vectores son herramientas para evaluar el impacto de la confiabilidad en el negocio y en las operaciones, y como herramienta de ajuste a dicho impacto mientras se satisfacen los objetivos de confiabilidad.

Por lo tanto, en su concepción más general, al evaluar la confiabilidad de un sistema se deben identificar los Criterios de Confiabilidad relevantes para cada una de sus características, los que determinan la Interpretación de la Confiabilidad del Sistema. Luego, a partir de identificar y asociar Objetivos a cada Criterio, se deben determinar las métricas vinculadas a cada Criterio (puede existir más de una métrica para un mismo Criterio) de cada Interpretación y así determinar los valores que componen el *TA-vector*, que son los valores de cada una de esas métricas. Disponiendo de los rangos y cotas objetivos de cada métrica, se cuenta con el *TT-vector*. Asimismo, se deben identificar los Factores de Cambio para cada uno de los criterios, los que tienen sus propias métricas que permiten evaluar su efectividad en contribuir al criterio con el que se vincula, y eventualmente el impacto, positivo o negativo en otros.

La gestión de la Confiabilidad implica entonces superar (en el mejor de los casos, siempre) el desafío que el *TA-vector* se encuentre dentro del volumen (determinado por el *TT-vector*) que queda definido en la representación espa-

cial de 5 dimensiones (*safety*, fiabilidad, seguridad, privacidad y resiliencia). Esta representación espacial es realizable si, por ejemplo, los valores de rangos y cotas de cada métrica de cada característica se pueden combinar y resumir de una manera convincente en dos valores (máximo y mínimo) que determinan los umbrales de los objetivos de la Característica en cuestión.

2.5.2. Proceso de Evaluación y Gestión de la Confiabilidad

El proceso de evaluación y gestión de la confiabilidad de un sistema se puede ver como la composición de dos fases: Análisis de la Confiabilidad y, Evaluación y Control. A continuación se describen cada una de ellas.

Análisis de la Confiabilidad

El análisis de la confiabilidad implica realizar las siguientes acciones:

Definir una Interpretación de la Confiabilidad del sistema incluyendo criterios específicos del sistema para cada una de las Características de la confiabilidad que son relevantes para dicho sistema y sus componentes, y determinar la calidad de la evidencia requerida para cada Característica, para estar en el nivel deseado.

Definir métricas para cada Criterio de la Interpretación de la Confiabilidad. Esto conduce a la definición del *TA-vector*.

Definir rangos aceptables o umbrales para cada métrica definida. Esto conduce a la definición del *TT-vector*.

Identificar factores que pueden influenciar en los valores del vector de Confiabilidad o en los niveles de confianza necesarios para los componentes del vector. Esto conduce a la definición de los Factores de Cambio.

Identificar métricas y KPIs específicos del negocio y las operaciones para evaluar el impacto de la confiabilidad.

Identificar dependencias entre los Criterios de Confiabilidad y listar los posibles impactos en el negocio y en las operaciones. Preservar evidencias sobre ésto es fundamental para confirmar (o no), con la rigurosidad apropiada, las consecuencias de los desvíos respecto a lo esperado.

Evaluación y Control

La evaluación y control implica realizar las siguientes acciones:

Implementar las métricas y las herramientas de monitorizado para la interpretación de la confiabilidad.

Medir el sistema en operación y generar valores para el *TA-vector*.

Ajustar los factores para controlar el *TA-vector* y llevarlo a valores aceptables, de acuerdo al *TT-vector*, mientras se monitorizan los costos asociados y el impacto en el negocio.

Ajustar prioridades en el caso que existan conflictos en el *TT-vector*, los costos involucrados en lograr las condiciones de confiabilidad deseadas y las métricas y KPIs objetivos pera el rendimiento del negocio y las operaciones.

Iterar entre ambas fases, Análisis de Confiabilidad y, Evaluación y Control, hasta que el *TA-vector* alcanza la situación deseada y al mismo tiempo se satisfagan los objetivos de rendimiento del negocio y de las operaciones.

2.5.3. Interacciones en la Confiabilidad y el impacto en el negocio y en las operaciones

Cuando se sigue el proceso de Análisis, Evaluación y Control, el efecto de los criterios y de los factores de cambio en el rendimiento del negocio y de las operaciones debe ser evaluado. Para ello se deben seleccionar y definir indicadores del negocio y de las operaciones (métricas y KPIs) que serán afectadas, positiva o negativamente, por los objetivos de confiabilidad y los factores de cambio.

Por otro lado, los criterios de confiabilidad se pueden afectar entre sí, y ello también debe ser analizado para eventualmente tomar decisiones al respecto.

Como forma de fijar la idea de las posibles interacciones referidas antes, se documenta a continuación un ejemplo extraído de un caso concreto, denominado FOVI (*Factory Operations Visibility and Intelligence*) [124]; se trata de un sistema "*brownfield*" de la empresa Fujitsu Limited, desarrollado en conjunto con Cisco Systems, en el ámbito de los *testbeds* de IIC.

En el ejemplo referido, uno de los Criterios de *safety* identificado fue "*evitar daños por estrés en las personas que utilizan determinado equipamiento*"; la métrica definida fue "*cantidad de daños / 3 meses*". El Factor de Cambio identificado para este criterio fue "*detectar situaciones o condiciones de riesgo*

y reducir la frecuencia de manipulación de las máquinas involucradas por parte del personal", lo que se puede traducir en "*enlentecer el ritmo de trabajo en la línea de ensamblado*". Del conjunto de Indicadores de Rendimiento (PI, por su sigla en inglés), en particular se identifica que el Factor de Cambio propuesto, considerando el PI "*productividad de la cadena de ensamblado*", impacta negativamente en la productividad (rendimiento de las operaciones) e impacta también negativamente en los ingresos (rendimiento del negocio). A su vez, impacta positivamente en la previsibilidad en cuanto a los tiempos de producción y entregas (rendimiento de las operaciones) y también impacta positivamente en los gastos de atención médica y costos de seguros asociados (rendimiento del negocio). Estas interacciones se pueden apreciar en la Figura 2.11.

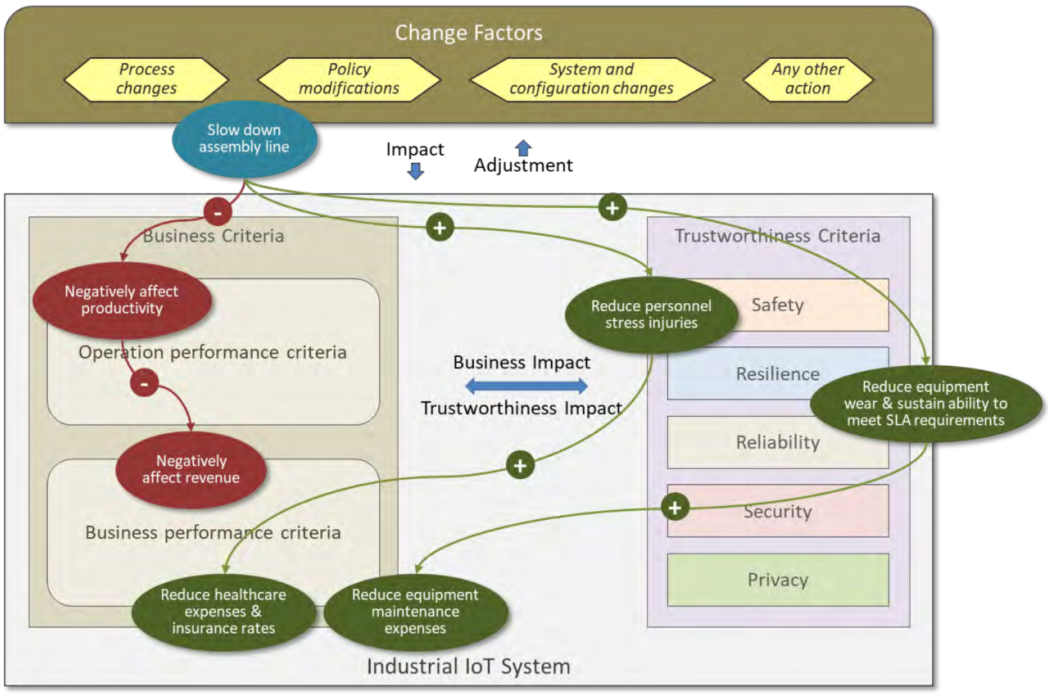


Figura 2.11: Ejemplo de análisis de Confiabilidad y Negocio. Fuente: [120]

En la Figura 2.12 se refleja el concepto de Espacio de Confiabilidad definido por Métricas, para el caso de 3 dimensiones.

2.5.4. Gestionando los Objetivos de la Confiabilidad

Siempre debemos tener presente que las interpretaciones de la confiabilidad varían de un sistema a otro, según la región, según los países y según la vertical

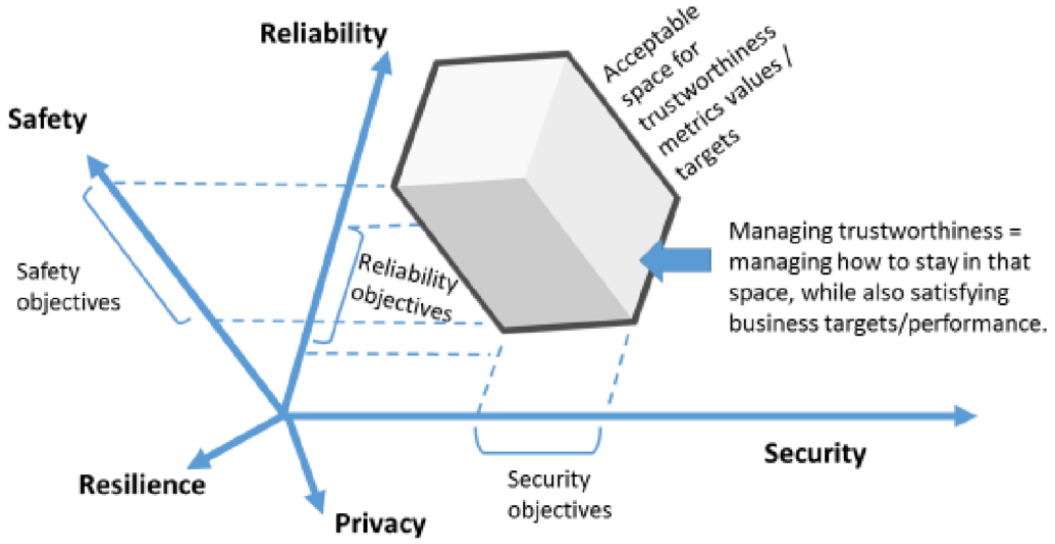


Figura 2.12: Ejemplo de Espacio de Confiabilidad definido por Métricas. Fuente: [126]

industrial.

Si fuera posible resumir el conjunto de métricas de cada característica de la confiabilidad en un valor, se podría elaborar un diagrama de radar donde representar la situación actual, la situación objetivo y el mínimo no negociable. Dicho diagrama podría ser el primer paso para determinar los pasos a dar para recorrer, de ser necesario, el camino desde lo actual a lo mínimo (si corresponde) y desde lo mínimo al objetivo. Cada característica de la confiabilidad tiene su propio camino, con sus propias restricciones técnicas y financieras, y sus propios tiempos. Es altamente probable que los caminos se crucen y se afecten positiva o negativamente. Para que el avance ocurra, todo ello se debe analizar en una visión lo más holísitica posible, y de manera continua.

2.5.4.1. La estrategia de gestión *middle-out*

Se considera que la estrategia *middle-out*, que resulta de una combinación de las estrategias *botton-up* y *top-down*, es la más adecuada para el trabajo multidisciplinario (interdisciplinario) que caracteriza a IIoT, y así definir una estrategia de Gobernanza de la Confiabilidad. En esa línea, se recomienda la existencia de:

- Un Equipo multisciplinario destinado a Gestionar las tareas vinculadas a la Confiabilidad

- Un Comité de Dirección de Confiabilidad
- Un Programa de Confiabilidad
- Un Líder del Comité y del Programa
- Un *Sponsor* del Comité y del Programa

A los efectos de gestionar el proyecto de implantación del Programa de Confiabilidad, es recomendable recurrir a una Matriz RACI (en la Figura 2.13 se presenta un ejemplo) o RASCI[1], donde en un primer nivel de detalle podemos identificar cinco tareas que coinciden con las cinco características de la confiabilidad. *A posteriori*, se puede desglosar cada una de ellas para obtener un mayor nivel de detalle.

Tasks	Corporate	Finance	OT	IT	Security	Operation	Business	Legal
Security	C	C	R	R	RA	R	I	C
Safety	C	C	R	I	C	RA	C	I
Reliability	I	C	RA	I	C	R	I	I
Resilience	I	C	RA	I	C	R	C	I
Privacy	I	C	R	R	R	C	C	RA

Figura 2.13: Ejemplo de Matriz RACI para Confiabilidad. Fuente: [120]

2.5.5. El "viaje" de la Confiabilidad

Las preocupaciones acerca de establecer la confianza en que un sistema IIoT cumple con los requisitos de la confiabilidad deben abordarse durante todo el ciclo de vida del sistema. Esto significa que la confiabilidad de IIoT no es un proyecto, con un inicio y un final, sino que es un viaje sin fin, que debe ser impulsado a través de un Programa de Confiabilidad establecido. Es posible ahondar en el concepto a partir del artículo *IoT Trustworthiness is a Journey and NOT a Project* [117] publicado en la edición de septiembre de 2018 del *Journal of Innovation* del IIC.

[1]Roles:
R: *Responsible* o Responsable. Este rol corresponde a quien efectivamente realiza la tarea.
A: *Accountable* o Aprobador. Este rol se responsabiliza de que la tarea se realice y es el que debe rendir cuentas sobre su ejecución. Sólo puede existir uno por tarea.
S: *Support* o Apoyo. Son recursos asignados al R para la consecución de la tarea.
C: *Consulted* o Consultado. Este rol posee alguna información o capacidad necesaria para realizar la tarea.
I: *Informed* o Informado. Este rol debe ser informado sobre el avance y los resultados de la ejecución de la tarea.

2.6. IISF - Puntos de Vista Funcional y de Implementación

En esta sección se describen en detalle los Puntos de Vista Funcional y de Implementación del IIRA [110] de acuerdo a lo especificado en el IISF [111], y la interacción entre ellos.

2.6.1. Introducción

Una implementación de un sistema IIoT debe proporcionar seguridad de extremo a extremo, desde el perímetro (*edge*) hasta la nube (*cloud*). Esto incluye el *hardening* de los *endpoints*, la protección de las comunicaciones, la administración y el control de políticas y actualizaciones, y el uso de analítica y acceso remoto para administrar y supervisar todo el proceso de seguridad.

Idealmente, la seguridad y la conciencia situacional en tiempo real deben abarcar los subsistemas de IT y OT sin interferir con ninguno de los procesos de negocio. La seguridad debe integrarse en el diseño y los riesgos deben evaluarse desde el inicio, en lugar de intentar "atornillar" la seguridad como una idea posterior.

Las implementaciones "desde cero" (ambiente conocido como *greenfield*) que utilizan las tecnologías más actuales y seguras no siempre son factibles. Dado que la vida media de un sistema industrial es actualmente de unos 20 años (NIST), a menudo la tecnología debe involucrarse en torno a un conjunto existente de sistemas heredados (ambiente conocido como *brownfield*) que son difíciles de cambiar.

Como no existe una sola "mejor manera" de implementar la seguridad y lograr un comportamiento adecuadamente seguro, los bloques de construcción tecnológicos deben apoyar una estrategia de defensa en profundidad que realice un mapeo de los niveles de defensa lógicos a las herramientas y técnicas de seguridad.

Los sistemas IIoT tienen recursos limitados y a su vez necesitan cumplir con diversos requisitos, como la seguridad del sistema y, por ejemplo, la ejecución en tiempo real. Es posible que estos factores no permitan implementar todas las medidas y controles de seguridad en su máxima expresión, en consonancia a como lo requiere la estrategia de defensa en profundidad.

2.6.2. Punto de Vista Funcional

El Punto de Vista Funcional, desde la óptica de la seguridad y como se muestra en la Figura 2.14, está conformado por 6 bloques, organizados en 3 capas.

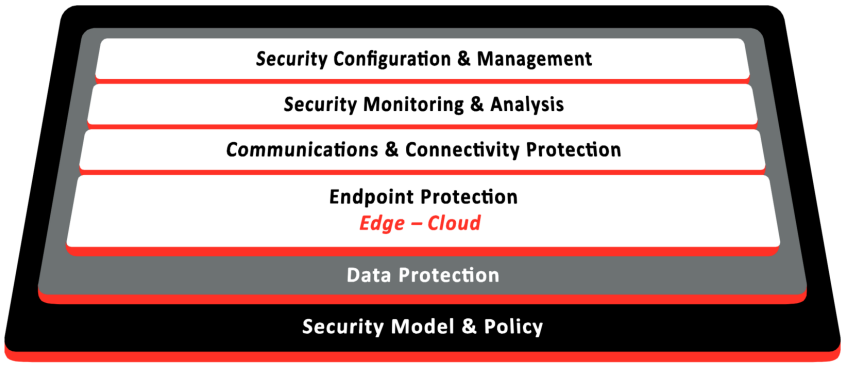


Figura 2.14: Punto de Vista Funcional del *Framework* de Seguridad. Fuente: [111]

La capa superior contiene 4 funciones:

- Protección del *Endpoint*
- Protección de las Comunicaciones y de la Conectividad
- Monitorizado y Análisis de la Seguridad
- Gestión y Configuración de la Seguridad

Esta capa superior se sustenta en la capa de Protección de los Datos la que a su vez se sustenta en la capa de Modelo y Política de Seguridad.

En la Figura 2.15 se visualiza, para un sistema IIoT, cómo se vinculan *end-to-end* el IISF y el Punto de Vista Funcional del IIRA.

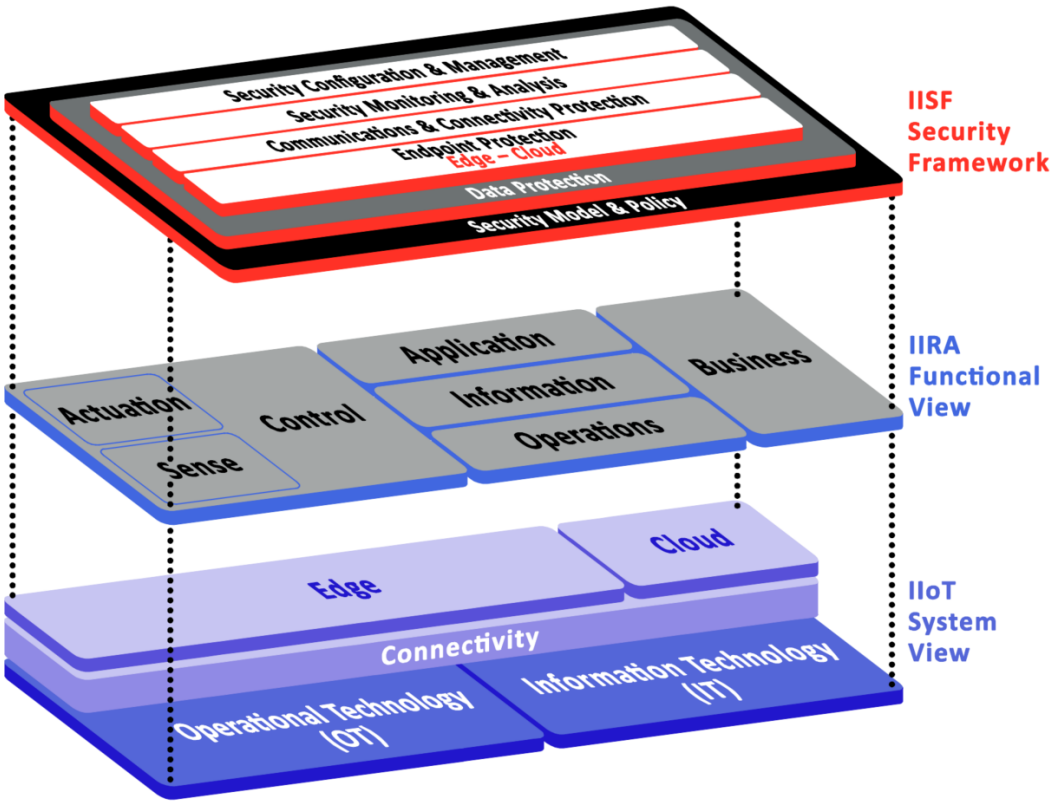


Figura 2.15: Vista Funcional IIRA y *Framework* IISF. Fuente: [111]

Protección de los bloques

A continuación se describirá cada uno de los 6 bloques mencionados.

Protección del *Endpoint*

Los *Endpoints* son cualquier elemento de un sistema IIoT que tiene capacidades de poder de cómputo y de comunicaciones, y que expone capacidades funcionales. Los mecanismos de seguridad deberían ser aplicados a los *endpoints* dependiendo de su función específica, de los requerimientos de seguridad y teniendo presente las restricciones de hardware y software.

La función de Protección del *Endpoint* está conformada por 9 bloques organizados en 3 capas, según se puede observar en la Figura 2.16.

La capa superior contiene 7 funciones:

- Seguridad Física del *Endpoint*
- Raíz de Confianza del *Endpoint*

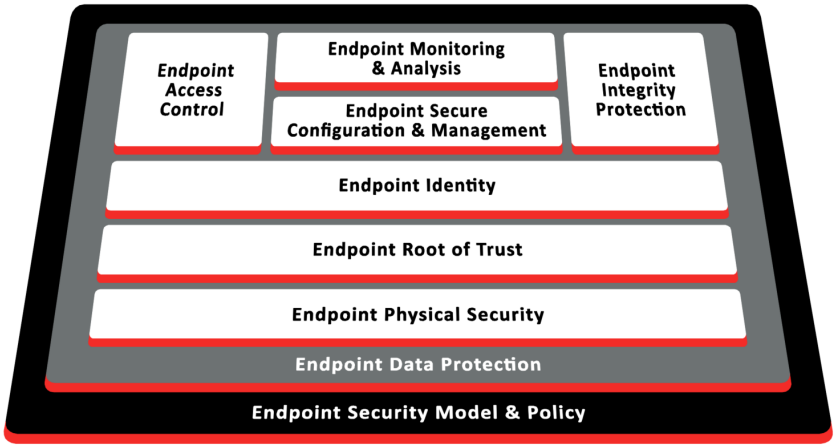


Figura 2.16: Descomposición Funcional de la protección del *Endpoint*. Fuente: [111]

- Identidad del *Endpoint*
- Control de Acceso al *Endpoint*
- Protección de Identidad del *Endpoint*
- Monitorizado y Análisis del *Endpoint*
- Gestión y Configuración de la Seguridad del *Endpoint*

Esta capa superior se sustenta en la capa de Protección de los Datos del *Endpoint*, la que a su vez tiene su apoyatura en la capa de Modelo y Política de Seguridad del *Endpoint*.

En el IIC ha disponibilizado el *white paper* denominado *Endpoint Security Best Practices* [106], que complementa la información al respecto proporcionada en el IISF.

Protección de las Comunicaciones y de la Conectividad

Como se observa en la Figura 2.17 la función de Protección de las Comunicaciones y de la Conectividad está conformada por 8 bloques organizados en 3 capas.

La capa superior contiene 6 funciones:

- Seguridad Física de las Conexiones
- Protección de la Comunicación entre los *Endpoints*
- Protección del Flujo de Información
- Protección Criptográfica

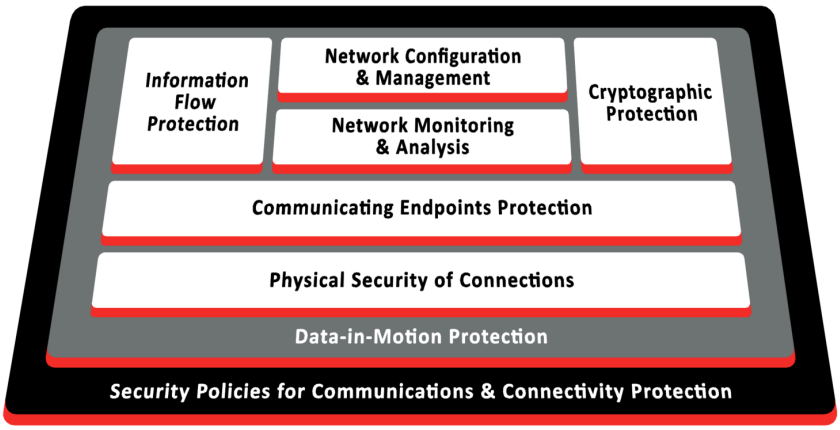


Figura 2.17: Descomposición Funcional de la protección de la Conectividad y Comunicaciones. Fuente: [111]

- Monitorizado y Análisis de la Red
- Gestión y Configuración de la Seguridad de la Red

Esta capa superior se sustenta en la capa de Protección de los Datos en Movimiento (DIM, *Data-In-Motion*) la que a su vez tiene su apoyatura en la capa de Políticas de Seguridad para la Protección de las Comunicaciones y de la Conectividad.

Monitorizado y Análisis de la Seguridad

La función de Monitorizado y Análisis de la Seguridad está conformada por 5 bloques organizados en 3 capas, de acuerdo a lo que se refleja en la Figura 2.18.

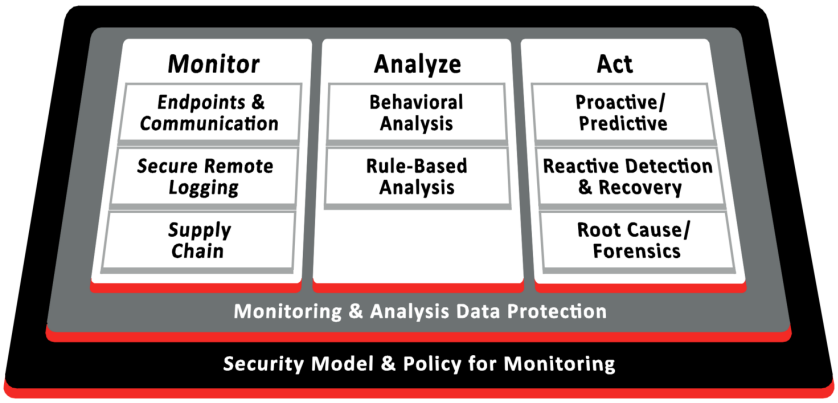


Figura 2.18: Monitorizado y Analisis de la Seguridad. Fuente: [111]

La capa superior contiene 3 funciones:

- Monitorizar
- Analizar
- Actuar

Esta capa superior se sustenta en la capa de Protección del Monitorizado y Análisis de los Datos, la que a su vez tiene su apoyatura en la capa de Modelo y Política de Seguridad para el Monitorizado.

La función de Monitorizar considera 3 fuentes principales:

- Comunicaciones y *Endpoint*
- *Logging* Remoto Seguro
- Cadena de Suministro

La función de Analizar contempla 2 tipos de análisis:

- de Comportamiento
- Basado en Reglas

Finalmente, la función Actuar identifica 3 tipos:

- Proactivo/Predictivo
- Deteccción reactiva y Recuperación
- Causa raíz/Forense

Gestión y Configuración de la Seguridad

Según se observa en la Figura 2.19 la función de Gestión y Configuración de la Seguridad está conformada por 8 bloques organizados en 3 capas.

- Modelo de Seguridad para el Control de Cambios
- Gestión de la Seguridad Operacional
- Gestión de la Seguridad
- Configuración y Gestión de las Comunicaciones
- Configuración y Gestión de los *Endpoints*
- Gestión de la Identidad de los *Endpoints*

Esta capa superior se sustenta en la capa de Protección de los Datos de Configuración y Gestión, la que a su vez tiene su apoyatura en la capa de Modelo y Política de Seguridad para la Gestión de los Cambios.

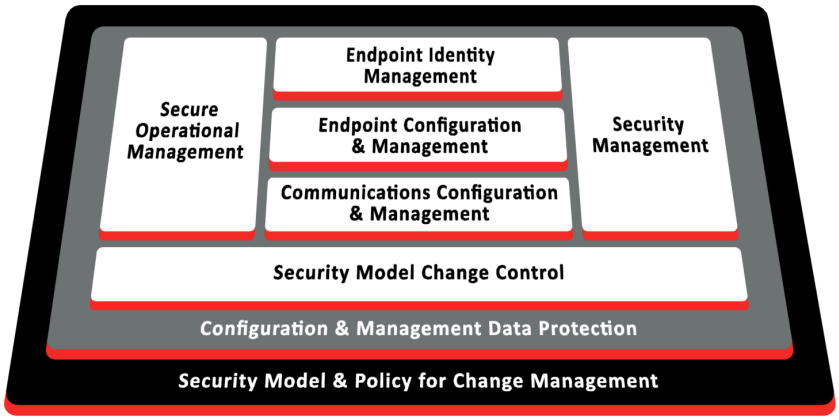


Figura 2.19: Gestion y Configuracion de la Seguridad. Fuente: [111]

Protección de los Datos

Los datos son "pervasivos" en los sistemas IIoT. Cada conjunto de datos tiene un ciclo de vida diferente, tiempo de relevancia y riesgo potencial asociado con su compromiso. La amenaza puede resultar de su modificación, interceptación o duplicación. Los efectos de los ataques en los datos varían de un cambio inmediato en el comportamiento del sistema a un comportamiento negativo más sutil en el futuro.

En el marco de la seguridad y según se observa en la Figura 2.20, se propone descomponer las consideraciones funcionales en 8 bloques organizados en 3 capas.

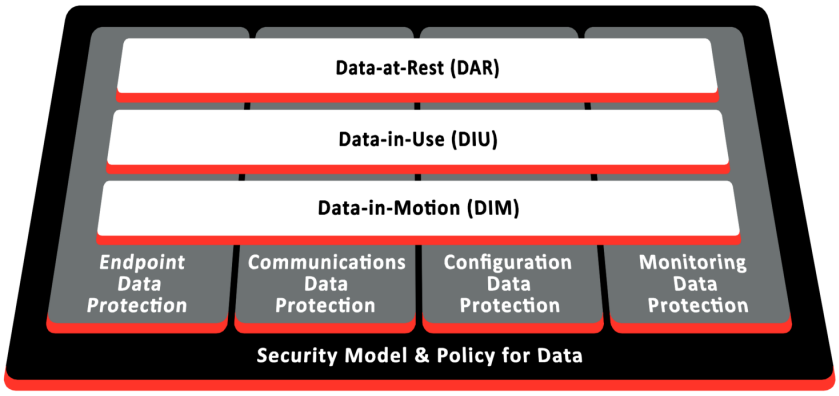


Figura 2.20: Protección de Datos. Fuente: [111]

La capa superior contiene 3 funciones:

- Datos en Movimiento (DIM)

- Datos en Uso (*Data-in-Use*, DIU)
- Datos Almacenados (*Data-at-Rest*, DAR)

La capa inmediata inferior refleja los diferentes tipos de datos a proteger, a saber, datos asociados a:

- *Endpoints*
- Comunicaciones
- Configuraciones
- Monitorizado

Finalmente, existe una función en la capa que sustenta a la anterior, denominada Modelo y Política de Seguridad para los Datos.

Modelo y Política de Seguridad

Esta función comprende los niveles de seguridad regulatorios, organizativos y a nivel de máquina. La Política de Seguridad describe los objetivos de seguridad del sistema; el Modelo de Seguridad es una representación formal de las políticas de seguridad aplicadas en el sistema. Varios modelos de seguridad pueden ser aplicables en un sistema, y el alcance de estos modelos puede abordar diferentes funciones de seguridad o dominios de seguridad dentro de él. El Modelo y la Política de Seguridad abarcan todos los aspectos de seguridad del sistema, incluido cómo proteger los *endpoints*, las comunicaciones y los datos. También define lo que se debe monitorizar, analizar y recuperar, y quién y cómo puede realizar cambios en todos los aspectos del sistema.

Las 9 funciones que brinda el Modelo y Política de Seguridad, según se aprecia en la Figura 2.21, son:

- Análisis de Amenazas al Sistema
- Objetivos de Seguridad del Sistema
- Política de Seguridad
- Modelo de Seguridad
- Política de Seguridad para la Protección de los Datos
- Política de Seguridad para los *Endpoints*
- Política de Seguridad para las Comunicaciones y la Conectividad
- Política de Seguridad para el Monitorizado y el Análisis

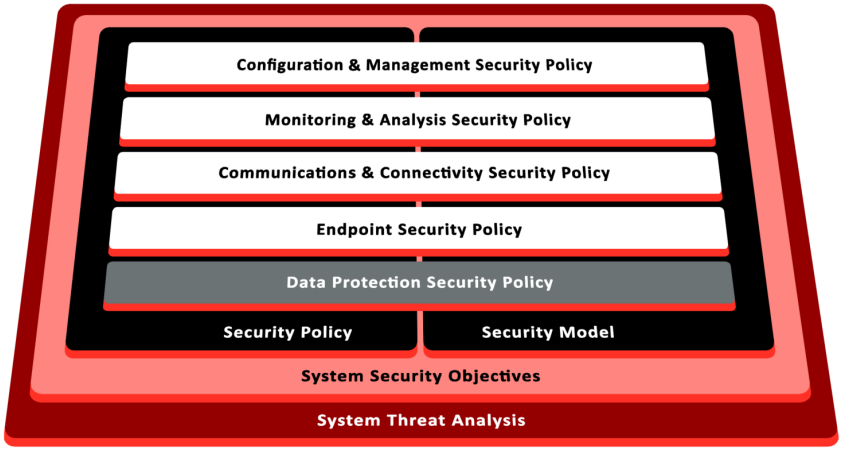


Figura 2.21: Modelo y Política de Seguridad. Fuente: [111]

- Política de Seguridad para la Configuración y la Gestión

Dichas funciones se organizan en 4 capas, donde, viajando desde la capa inferior a la superior, encontramos las siguientes funciones: la primera función mencionada en la capa de más abajo, la segunda función en la segunda capa, las 2 siguientes en la tercera capa y las 5 restantes en la capa superior.

2.6.3. Del Punto de Vista Funcional al Punto de Vista de Implementación

Como se describió antes, el Punto de Vista Funcional, desde la óptica de la seguridad, está conformado por 6 bloques funcionales, a saber: Protección del *Endpoint*, Protección de las Comunicaciones y de la Conectividad, Monitorizado y Análisis de la Seguridad, Gestión y Configuración de la Seguridad, Protección de los Datos y, Modelo y Política de Seguridad.

Estas funciones son la guía para implementar seguridad *end-to-end* en los sistemas IIoT en el contexto de la confiabilidad. Un conjunto de principios de diseño de seguridad deben guiar las capacidades y técnicas empleadas en el Punto de Vista de Implementación, para cada implementación.

El *Framework* IISF referencia al trabajo *The Protection of Information in Computer Systems* [279] donde se identifican 8 principios de diseño a ser considerados al momento de pensar en proteger la información almacenada en un sistema. Ellos son:

- Economía del mecanismo

- Defectos a prueba de fallas
- Mediación completa
- Diseño abierto
- Separación de privilegios
- Mínimo privilegio
- Mecanismo menos común
- Aceptabilidad psicológica

En los capítulos 8, 9 y 10 del IISF, se mencionan y analizan varias técnicas posibles para proteger los *Endpoints*, las Comunicaciones y la Conectividad y además, algunas estrategias para dotar de seguridad al Monitorizado y el Análisis y, a la Configuración y la Gestión.

Respecto a la Protección de los *Endpoints*, se abordan las posibles vulnerabilidades y amenazas que pueden afectar a los *endpoints*, tanto a nivel físico, de hardware, de software, de aplicaciones, de *boot*, de configuración, de gestión, de datos, de identidad, de control de acceso, de integridad, entre otros, y las posibles consideraciones al respecto.

En relación a la Protección de las Comunicaciones y la Conectividad, el nivel de protección requerido depende de las amenazas al intercambio de datos e información. Esta información puede ser, entre otros, debida a actualizaciones de sensores, datos de telemetría, comandos, alarmas, eventos, registros, cambios de estado o actualizaciones de configuración. En lo que refiere a técnicas criptográficas, se abordan los aspectos de autenticación (mutua), la confidencialidad, la integridad y la "frescura" de los datos. Se consideran los despliegues en ambientes *brownfield*, la separación de los canales de datos, control y gestión, se realiza la mención a algunos de los protocolos más relevantes, la segmentación de las redes, la incorporación de *gateways* y el filtrado en diferentes capas del modelo de referencia, *firewalls* y el Control de Acceso a la Red (NAC, por su sigla en inglés).

El IIC ha elaborado el *IIoT Connectivity Framework* (IICF) [109] con el que pretende brindar una estrategia de abordaje ordenada a la enorme cantidad de posibilidades de conectividad que se ofrece en IIoT. Allí propone un *Framework* de Conectividad, una Guía para la Evaluación de diferentes *frameworks* y tecnologías de conectividad, en concordancia con los Puntos de Vista de la IIRA (Negocio, Uso, Funcional y de Implementación), y culmina con una mención y descripción de algunos estándares, en concreto, se hace referencia a

los siguientes: DDS, HTTP, OPC UA, oneM2M, TCP, UDP, CoAP y MQTT.

En los Anexos del IICF se plasman algunos ejemplos de Guías de Evaluación, según el siguiente orden:

- Anexo A: DDS
- Anexo B: UPC UA
- Anexo C: oneM2M
- Anexo D: HTTP
- Anexo E: CoAP
- Anexo F: MQTT

En el artículo *A Practical Guide to Using the Industrial Internet Connectivity Framework* [116], los autores ofrecen una guía, alineada con el IICF, con las cuestiones que a su entender son las más relevantes a considerar al momento de seleccionar una tecnología de conectividad.

Con respecto al Monitorizado y Análisis, es relevante destacar que el monitorizado de la seguridad agrega y almacena una variedad de tipos de datos de la ejecución de los sistemas IIoT, lo que permite el análisis de los compromisos pasados, los eventos de seguridad actuales y la predicción de riesgos futuros; por otro lado, las herramientas analíticas de seguridad proporcionan comentarios útiles a la organización a través de parámetros adecuados para la visualización de alto nivel.

Los parámetros de monitorizado son más valiosos cuando se relacionan directamente con las preocupaciones relativas a la seguridad de una organización y son priorizados por las partes interesadas. Deben representar condiciones bien definidas y entendidas por aquellos que deben tomar acciones. Los aspectos abordados incluyen, la prevención, la detección, análisis y respuesta de un incidente, los tipos de análisis y monitorizado (forense, en curso y predictivo), los tipos de analíticas a aplicar (por comportamiento o por reglas), los datos a recolectar y consideraciones por ejemplo en cuanto a la privacidad, desde dónde y el caso particular de los despliegues *brownfield*.

Finalmente, en lo que refiere a Gestión y Configuración, los cambios en el entorno y el descubrimiento de nuevas vulnerabilidades y amenazas requerirán actualizaciones de la política, el firmware y el software, por lo que las características de seguridad de un sistema IIoT deben ser configurables y manejables, y no definidas estáticamente. Además, las versiones implementadas deben controlarse, configurarse y gestionarse cuidadosamente.

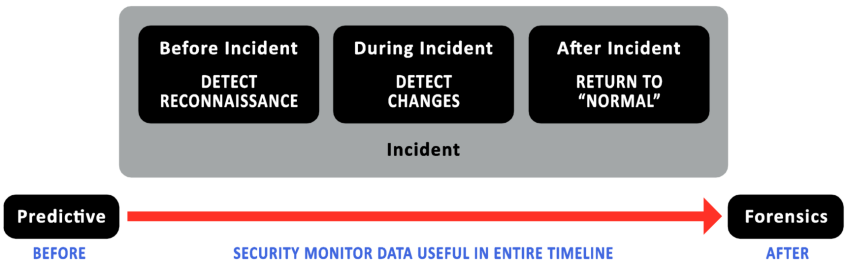


Figura 2.22: Monitorizado de la Seguridad - Incidentes. Fuente: [111]

Los informes periódicos de cumplimiento de seguridad suelen ser obligatorios y ciertamente aconsejables. Las configuraciones de red y *endpoints* deben analizarse periódicamente para informar de las desviaciones respecto a todas las políticas relevantes y para informar respecto al cumplimiento.

En el *Framework* IICF Se hace especial hincapié en la distinción entre Gestión Operacional Segura y Gestión de la Seguridad. Por un lado, se hace hincapié en que son actividades distintas, cada una con sus propios procesos de control y a su vez, que deben existir procesos de Monitorizado tanto Operacional como de Seguridad.

2.7. Niveles de Exhaustividad

Como se comentó en la Sección 3.6.2 el Capítulo 3, el documento *IoT Security Maturity Model: Practitioner´s Guide* se proporciona una guía de los objetivos típicos a cumplir en cada Dominio del SMM (Gobernanza, Establecimiento y Fortalecimiento) en cada nivel de Exhaustividad. Acompañando a dicha guía, el artículo proporciona también una guía de las necesidades para cada uno de los Subdominios y para cada nivel del Exhaustividad. En un tercer y último nivel de granularidad, se ofrece la finalidad o propósito de cada Práctica, para cada nivel de Exhaustividad.

De acuerdo a como se detalló en la Sección 3.6.1 del Capítulo 3 los niveles de Exhaustividad considerados son:

- 1. Mínimo
- 2. *Ad Hoc*
- 3. Consistente
- 4. Formalizado

A continuación se expresan los niveles de Exhaustividad para cada Dominio, Subdominio y Práctica del SMM.

2.7.1. Dominio Gobernanza

1. Establecer una base general para consideraciones de seguridad
2. Establecer medidas de seguridad de referencia
3. Facilitar la implementación de capacidades de seguridad
4. Establecer una estructura de gobernanza con procesos claros asociados

Subdominio Estrategia y Gobernanza

1. Objetivos de visión, alcance y seguridad
2. Mejores prácticas más apropiadas
3. Enfoques y estándares reconocidos
4. Apoyo consistente a los procesos del negocio, legales, operacionales y de otros temas

Práctica Gestión del Programa de Seguridad

1. Describir la provisión general de seguridad
2. Referencia a los objetivos de seguridad más relevantes y cómo son abordados
3. Cobertura de los tópicos generales de los estándares de gestión de la seguridad reconocidos
4. Implementar una planificación clara, una provisión oportuna y el control de las actividades de seguridad

Práctica Gestión del Cumplimiento

1. Ser conscientes de los facilitadores de cumplimiento
2. Considerar algunos requisitos opcionales de cumplimiento para la implementación
3. Implementar requisitos de cumplimiento obligatorios
4. Supervisar la evolución de los requisitos estándar para el cumplimiento

Subdominio Modelado de Amenazas y Evaluación de Riesgos

1. Revisión del panorama actual de amenazas
2. Entendimiento de las vulnerabilidades del sistema y la tecnología
3. Descripción completa de los riesgos relevantes
4. Enfoque holístico y sistemática de la gestión de riesgos

Práctica Modelado de Amenazas

1. Referir a los problemas generales de seguridad de TI como amenazas
2. Identificar y describir las amenazas de manera *ad hoc*
3. Describir y clasificar las amenazas de una manera precisa (opcionalmente de manera formal)
4. Revelar y describir claramente los factores de TI conocidos y específicos que pueden poner el sistema en riesgo

Práctica Actitud frente al Riesgo

1. Definir informalmente la noción de riesgo
2. Diferenciar la importancia de los riesgos
3. Medir y gestionar adecuadamente los riesgos
4. Utilizar un marco y procesos de gestión de riesgos

Subdominio Gestión de Cadena de Suministros y Dependencias Externas

1. Chequeo de reputación de proveedores y contratistas
2. Garantía de seguridad de los artefactos de la cadena de suministros
3. Certificados y otras garantías provistos por autoridades de confianza
4. Control de exposición a posibles daños desde proveedores y contratistas

Práctica Gestión de Riesgos en la Cadena de Suministros de Productos

1. Monitorizar parches y vulnerabilidades para los componentes suministrados
2. Implementar algunas pruebas de seguridad para los componentes suministrados
3. Obtener certificados u otras garantías de seguridad para los componentes esenciales
4. Aplicar una política de gestión de riesgos para la cadena de suministros

Práctica Gestión de Dependencias para los Servicios de Terceras Partes

1. Monitorizar la reputación de los contratistas
2. Proporcionar la calidad de los servicios a través de acuerdos contractuales
3. Obtener evidencia de terceras partes respecto a la calidad del
4. Aplicar una política de gestión de confiabilidad uniforme a los contratistas

2.7.2. Dominio Establecimiento

1. Permitir el uso de los controles de seguridad disponibles
2. Implementar controles de seguridad de acuerdo con los escenarios de uso conocidos
3. Emplear tanto mecanismos integrados como adicionales para cubrir los riesgos conocidos
4. Establecer el proceso para abordar los riesgos por los mejores medios disponibles

Subdominio Gestión de Identidades y Accesos

1. Apoyar a las entidades elementales para el escenario de uso básico

2. Diferenciar a los actores para los escenarios de acceso general
3. Emplear las mejores prácticas para apoyar escenarios de acceso sofisticados
4. Protección integral contra los riesgos relacionados con el acceso no autorizado

Práctica Establecimiento y Mantenimiento de Identidades

1. Mantener una o varias cuentas de la misma forma o muy similar
2. Administrar las identidades de varios grupos de personas, sistemas o cosas
3. Apoyar una amplia gama de identidades aprovechando los mecanismos automatizados
4. Mantener y controlar el uso de identidades de personas, sistemas y cosas a lo largo de su ciclo de vida

Práctica Control de Acceso

1. Sólo restringir la posibilidad de acceso a los sistemas a agentes externos
2. Considerar el rol del sujeto y controlar los derechos de acceso
3. Utilizar políticas de control de acceso disponibles con un adecuado nivel de garantía
4. Mantener un esquema de autorización estrictamente alineado a las necesidades y restricciones del negocio

Subdominio Protección de Activos

1. Trazabilidad del uso de los activos físicos y digitales
2. Monitorizado de los activos sobre la base de casos de uso
3. Gestión y protección de los activos de diversos tipos
4. Garantía de cumplimiento de las políticas de gestión de activos

Práctica Gestión de Configuración y Cambios de los Activos

1. Seguir los cambios no frecuentes en los activos y las configuraciones
2. Seguir algunas reglas específicas para gestionar posibles cambios a los sistemas
3. Mantener procedimientos de gestión de cambio para los activos y/o las configuraciones
4. Regular el proceso del ciclo de vida de los activos, desde el aprovisionamiento hasta el reemplazo, incluyendo cambios de emergencia

Práctica Protección Física

1. En general se limita el acceso a los activos físicos
2. "Customizar" las restricciones de acceso considerando tiempo y forma de acceso físico
3. Control de acceso físico automático y ajustable utilizando *tokens* de identidad específicos
4. Abordar todos los aspectos de la seguridad física y *safety*, prevenir robos y garantizar un funcionamiento *safety* y continuo

Subdominio Protección de Datos

1. Mantenimiento general de la confidencialidad e integridad de los datos
2. Un mayor nivel de garantía para algunos datos
3. Implementación de políticas y métodos reconocidos para la protección de los datos
4. Garantía de la protección de la información crítica del negocio, en tránsito y almacenada

Práctica Modelo de Seguridad y Política de Datos

1. Declarar que los datos deberían ser protegidos frente a accesos no autorizados
2. Definir una categorización simple de los datos y las restricciones apropiadas
3. Definir el enfoque particular y los roles/atributos para controlar el acceso a los datos
4. Categorizar y proteger consistentemente los datos de acuerdo a los requerimientos de las partes interesadas

Práctica Implementación de Controles de Protección de los Datos

1. Aprovechar los controles de protección integrados (SO, red, servicios)
2. Configurar controles integrados y asegurarse de que su uso se ajuste a los objetivos de protección de datos
3. Apoyar la correcta aplicación de los controles de datos de acuerdo con las normas reconocidas
4. Garantizar la protección necesaria de cada elemento de datos tanto en tránsito como en reposo

2.7.3. Dominio Fortalecimiento

1. Aplicar las prácticas reconocidas de higiene cibernética
2. Mejorar la protección del sistema de acuerdo con sus necesidades y prioridades
3. Emplear los métodos y herramientas bien reconocidos que permitan la confiabilidad
4. Establecer el proceso continuo de apoyo a los objetivos de la confiabilidad

Subdominio Gestión de Vulnerabilidades y Parches

1. Mantener los sistemas actualizados y menos propensos a ataques
2. Aplicar una política de actualización regular para los componentes críticos
3. Actualizaciones automatizadas configuradas específicamente para el caso
4. Planificación de un proceso de actualizaciones regulares y considerando escenarios de emergencia para eventos críticos del tipo *zero-day*

Práctica Evaluación de Vulnerabilidades

1. Considerar si las vulnerabilidades ampliamente conocidas son relevantes para el sistema
2. Comprobar si los componentes especificados son propensos a ataques
3. Obtener una evaluación objetiva de terceros respecto a vulnerabilidades y exposiciones
4. Realizar inspecciones de seguridad de manera regular, personalizadas y profundas

Práctica Gestión de Parches

1. Considerar los avisos de seguridad emitidos por los proveedores e instalar los parches apropiados
2. Comprobar que los componentes especificados están protegidos contra los ataques más probables
3. Establecer procedimientos de actualización automática siempre que sea posible
4. Implantar una política para el sistema con el objetivo de garantizar la protección continua contra ataques conocidos

Subdominio Conciencia Situacional

1. Mantener una conciencia mínima de eventos relacionados con la seguridad
2. Atención específica a algunos tipos de eventos de seguridad
3. Supervisión integral y intercambio regular de información relacionada con la seguridad
4. Proporcionar y gestionar toda la información relevante para los aspectos de confiabilidad

Práctica de Monitorizado

1. Ocasionalmente chequear los *logs* del sistema a los efectos de realizar diagnósticos
2. Periódicamente chequear eventos que indiquen qué tan adecuadamente se ejecutan los procesos críticos
3. Recopilar y analizar información relevante para la seguridad, tanto con herramientas integradas como específicamente diseñadas
4. Actuar como catalizador y generador de capacidad para la protección continua del sistema

Práctica Intercambio de Información y Conciencia de Situación

1. Obtener alguna información externa relevante en base a una estrategia no formal
2. Habilitar al personal a que consistentemente utilice fuentes externas de información relevante
3. Realizar intercambios de información con autoridades y con la comunidad
4. Establecer comunicaciones bidireccionales con foco en situaciones *zero-day* e incidentes en la industria

Subdominio Respuesta a Eventos e Incidentes, Continuidad de las Operaciones

1. Chequeo de la recuperación de los sistemas luego de los incidentes
2. Aseguramiento de la recuperación de los componentes de los sistemas o procesos
3. Procedimiento de recuperación automática siempre que sea posible y que se tengan informes adecuados
4. Respuesta rápida ante incidentes y reducción de daños a la empresa tanto

por medios técnicos como organizativos

Práctica Detección de Eventos y Plan de Respuesta

1. Definir eventos específicos y acciones básicas para reaccionar a ellos
2. Proveer una guía aplicada a componentes críticos y cómo detectar y responder a los incidentes
3. Establecer las bases para la ejecución automática de los procedimientos de respuesta
4. Crear controles para detectar incidentes, asignarlos para ser investigados y escalarlos de ser necesario

Práctica Remediación, Recuperación, y Continuidad de las Operaciones

1. Brindar las instrucciones básicas para la recuperación del sistema
2. Manejar incidentes conocidos y comprobar si el sistema está completamente recuperado
3. Permitir la ejecución automática de procedimientos de corrección y recuperación
4. Apoyar una combinación de medidas técnicas y organizativas que faciliten la rápida recuperación del sistema

Apéndice 3

Complemento a la información relativa a ENISA, NIST, IETF y *Smart Nation*

En este apéndice se brinda información que amplia y complementa la documentada en el Capítulo 4.

3.1. ENISA

En las siguientes secciones se complementa la información brindada en la Sección 4.2 del Capítulo 4 referida al trabajo de ENISA.

3.1.1. Taxonomía de Activos - Dispositivos IoT en CII

Tomando como base el modelo de referencia *Baseline Security Recommendations for IoT* (Figura 3.1) en el contexto de *Critical Information Infrastructures* (CII), ENISA propone identificar grupos de activos y activos a ser protegidos, según se observa en la Figura 3.2. Es importante destacar que dado el enfoque horizontal de la propuesta, el nivel y tipo de protección a brindar a un determinado activo, dependerá del caso de uso, de la aplicación usada y del escenario de uso del ecosistema IoT.

Los grupos de activos considerados son:

- Dispositivos IoT (hardware, software, sensores, actuadores)

- Otros dispositivos del ecosistema IoT (dispositivos con interfaz con las cosas, dispositivos para gestionar las cosas, sistemas embebidos)
- Comunicaciones (redes, protocolos)
- Infraestructura (routers, gateways, fuentes de alimentación, activos de seguridad)
- Plataforma y *backend* (servicios web, infraestructura y servicios en la nube)
- Toma de decisiones (minería de datos, datos computados y procesados)
- Aplicaciones y servicios (analítica y visualización de datos, gestión de red y dispositivos, uso de dispositivos)
- Información (almacenada, en tránsito, en uso)

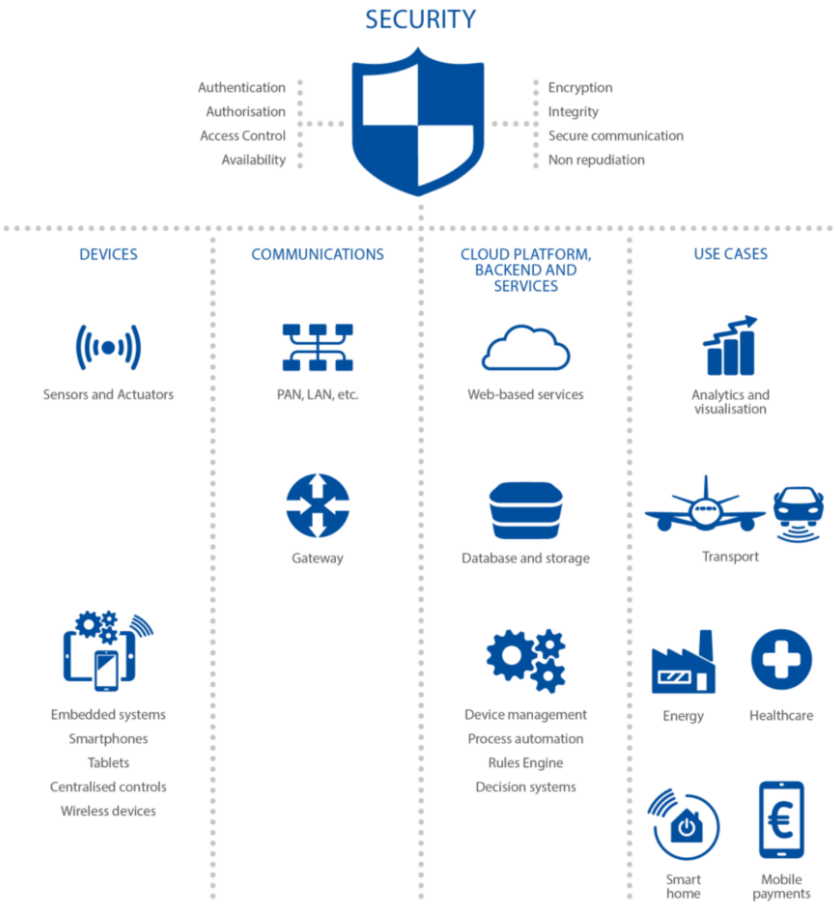


Figura 3.1: Modelo de Referencia de Alto Nivel para IoT. Fuente: [57]

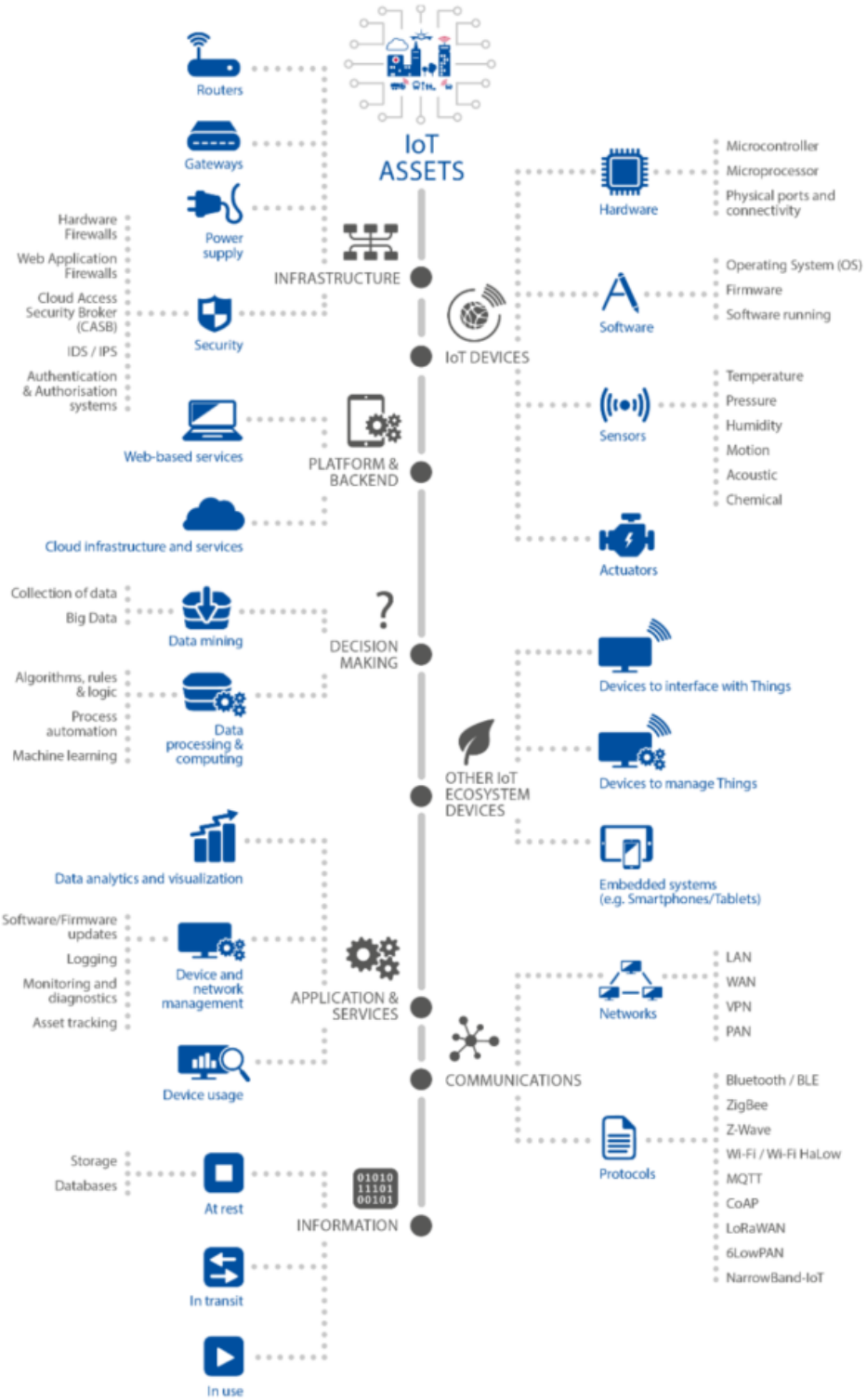


Figura 3.2: Taxonomía de Activos. Fuente: [57]

3.1.2. Análisis de Riesgos y Amenazas - Dispositivos IoT en CII

En esta sección se determinan y enumeran las principales amenazas de seguridad, vulnerabilidades, factores de riesgo y escenarios de ataque que afectan a los dispositivos y redes de IoT, tomando los diferentes niveles de importancia y criticidad de los expertos entrevistados para cada escenario de amenaza, riesgo y ataque en consideración.

Incidentes de seguridad

El número de amenazas de seguridad que tienen como objetivo los dispositivos IoT ha ido creciendo en los últimos años y nada hace pensar en un cambio en la tendencia, y sí, en un aumento más acelerado, potenciado ello principalmente por la cantidad de dispositivos disponibles y por no ser actualmente la seguridad una consideración relevante a momento de ser diseñados.

Sólo a manera de ejemplo, podemos mencionar a la botnet Mirai [281] como la responsable de varios incidentes de seguridad que ocurrieron en los años 2016 y 2017, y que pusieron de manifiesto parte del impacto que puede significar explotar algunas de las vulnerabilidades del ecosistema IoT.

Taxonomía de amenazas

En el contexto del trabajo de ENISA, se presenta una taxonomía de amenazas en el ecosistema de IoT, reflejada en la Figura 3.3, identificando las siguientes categorías:

- Abuso/Actividades maliciosas
- Escucha/Interceptación/Secuestro
- Interrupción
- Daño/Pérdida de activos IT
- Fallas/Malfuncionamiento
- Desastres
- Ataques físicos

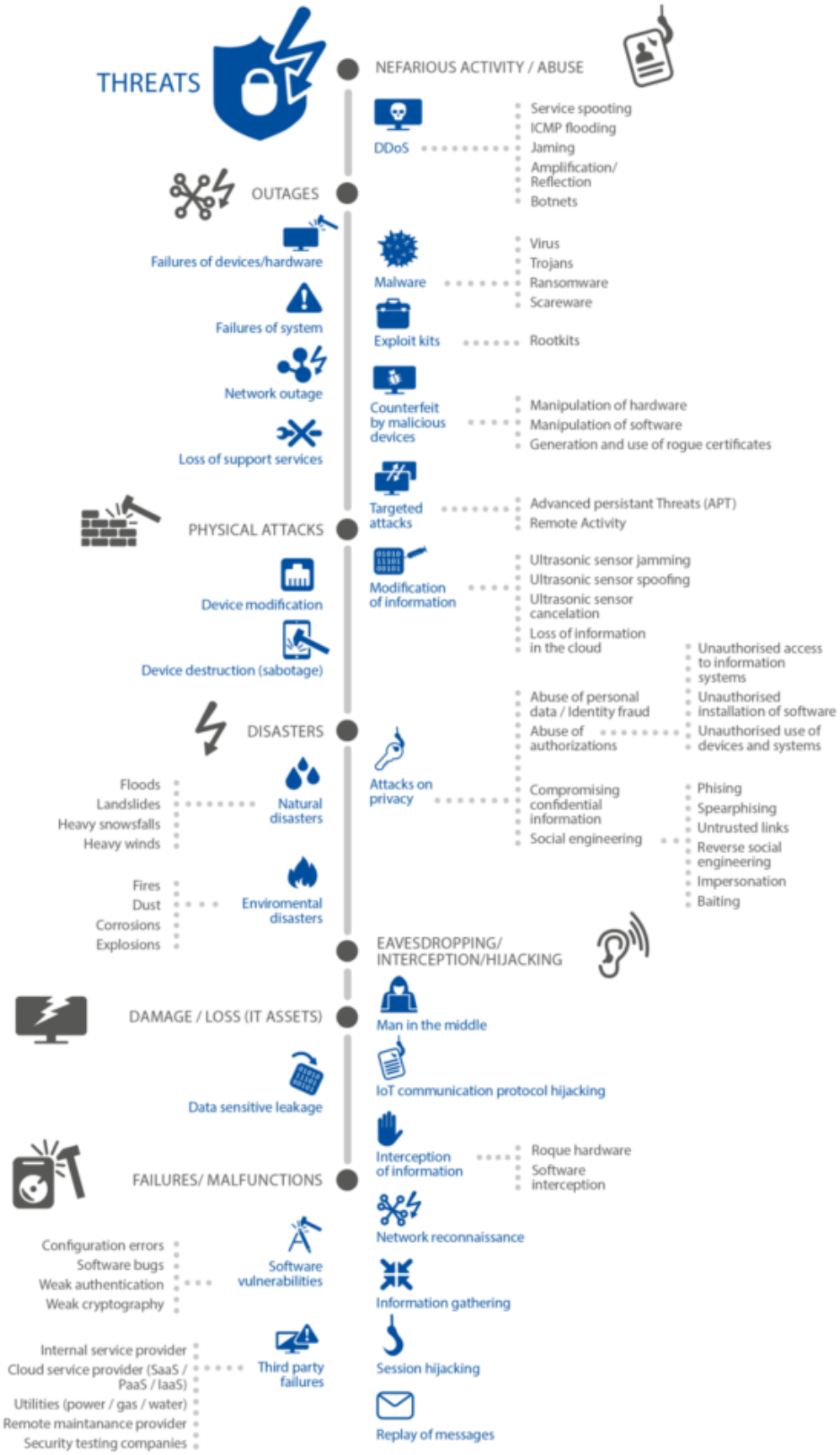


Figura 3.3: Taxonomía de Amenazas. Fuente: [57]

Cada categoría se desglosa en una lista no exhaustiva de amenazas y a su vez, se brinda una enumeración no taxativa de los potenciales activos afectados, de acuerdo al modelo de referencia utilizado. Esta taxonomía es acompañada por la mención y breve descripción de 10 ejemplos de escenarios de ataques en IoT. En el documento *Baseline Security Recommendations for IoT*, 3 de los escenarios fueron considerados como los más críticos (recordando que se trata de un enfoque horizontal):

- El sistema de administración de IoT es comprometido
- Manipulación de valores en dispositivos IoT
- Botnet/Inyección de comandos

Para cada uno ellos, el referido documento brinda un detalle de: impacto, partes interesadas involucradas, riesgo de efecto cascada, *gaps* y desafíos, contramedidas posibles y detalles técnicos adicionales. En todos los casos se citan referencias de casos reales, investigaciones o ejercicios que complementan la información que se brinda.

Medidas de seguridad y Buenas Prácticas - Dispositivos IoT

A partir del análisis de numerosas fuentes referenciadas en el documento, se identifica un conjunto de medidas de seguridad y buenas prácticas, organizadas en Dominios de Seguridad, que son aplicables en diversos ambientes de IoT, ya que la estrategia de abordaje de este trabajo siempre ha sido en el sentido horizontal.

Los Dominios considerados son:

- Gobernanza de la Seguridad de los Sistemas de Información y Gestión de Riesgos
- Gestión del Ecosistema
- Arquitectura de la Seguridad IT
- Administración de la Seguridad IT
- Gestión de identidades y acceso
- Mantenimiento de la Seguridad IT
- Seguridad Física y Ambiental
- Detección
- Gestión de Incidentes de Seguridad Informáticos

- Continuidad de Operaciones
- Gestión de Crisis

Las medidas seleccionadas para componer la línea base de seguridad para IoT, respetan la siguiente notación:

GP-XX-YY

Donde,

GP proviene de *Good Practices*.

XX puede ser PS (*PolicieS*), OP (*Organisational, People and Process measures*) o TM (*Technical Measures*).

YY es un número de dos dígitos.

Cada una de las Buenas Prácticas mencionadas, son vinculadas (en anexos al documento en cuestión) con las amenazas mencionadas antes así como también con los dominios considerados, ofreciéndose además referencias donde profundizar al respecto de cada una.

A continuación se enumeran las Buenas Prácticas, segregadas en las siguientes Categorías: Políticas, Medidas Organizacionales, para las Personas y los Procesos, y Medidas Técnicas.

Políticas

El primer conjunto de 12 medidas corresponde a políticas que en general se focalizan en la seguridad de la información, la que debe ser adecuada a la actividad de la organización que se esté analizando.

Las 12 medidas son distribuidas en 4 grupos de Buenas Prácticas, a saber:

- *Security by design*
- *Privacy by design*
- Gestión de Activos
- Identificación y Evaluación de Riesgos y Amenazas

Medidas Organizacionales, para las Personas y los Procesos

Se identifican 14 medidas distribuidas en 5 grupos de Buenas Prácticas, siendo ellos:

- Soporte EOL

- Soluciones probadas
- Gestión de vulnerabilidades y/o incidentes de seguridad
- Entrenamiento y Concientización en seguridad de los recursos humanos
- Vinculos con terceras partes

Medidas Técnicas

Se identifican 57 medidas distribuidas en los siguientes 15 grupos de Buenas Prácticas:

- Seguridad del hardware
- Gestión de confianza y de la integridad
- Seguridad y Privacidad fuerte por defecto
- Protección de los datos y cumplimiento de las normas
- Fiabilidad y *Safety* de los sistemas
- Software seguro / Actualizaciones de firmware
- Autenticación
- Autorización
- Control de acceso – Seguridad física y ambiental
- Criptografía
- Comunicaciones seguras y confiables
- Servicios de red e interfaces seguras
- Manejo seguro de entrada/salida
- Registro
- Monitorizado y auditado

Análisis de *gaps*

Este análisis de *gaps* refiere a identificar el espacio entre el estado actual y el estado deseado respecto a la ciberseguridad en IoT. De la misma forma resulta relevante identificar los pasos necesarios para cerrar dichos *gaps*, o dicho en otras palabras, cómo movernos del estado de inmadurez actual, en cuanto a seguridad en IoT, a un estado maduro.

Es importante aclarar que al referirse a seguridad, se están englobando más conceptos que la seguridad como tradicionalmente se la conoce en el mundo

IT, contemplando además conceptos como *safaety*, privacidad, resiliencia y fiabilidad.

El trabajo de ENISA identificó 6 *gaps* principales:

- Fragmentación en las regulaciones y enfoques de seguridad existentes
- Ausencia de concientización y conocimiento
- Diseño y/o desarrollo inseguro
- Ausencia de interoperabilidad entre dispositivos IoT, plataformas y *frameworks*
- Falta de incentivos económicos
- No existencia de una gestión adecuada del ciclo de vida de los productos

Recomendaciones de alto nivel para mejorar la ciberseguridad en IoT

Las 7 recomendaciones de alto nivel que resultaron del trabajo son las siguientes:

- Promover el armonizado de las regulaciones e iniciativas de seguridad en IoT
- Aumentar la concientización respecto a la necesidad de ciberseguridad en IoT
- Definir lineamientos para el desarrollo seguro de hardware y software de IoT durante todo el ciclo de vida
- Lograr consensos para la interoperabilidad en el ecosistema IoT
- Promover incentivos económicos y administrativos vinculados a seguridad en IoT
- Establecer una gestión segura del ciclo de vida de los productos IoT y de los servicios
- Clarificar las responsabilidades de las diferentes partes interesadas en el ecosistema IoT

3.1.3. Taxonomía de Activos - *Smart Manufacturing*

Con el objetivo de disponer de una taxonomía de activos de la I4.0/*Smart manufacturing*, en el trabajo *Good Practices for Security of Internet of Things in the context of Smart Manufacturing* ENISA los clasifica en los siguientes grupos (ver Figura 3.4):

- Dispositivos finales IIoT (Sensores, Actuadores, *Safety Instrumented Systems* (SIS))
- ICS (PLCs, RTUs, DCS, SCADA, HMI)
- Redes de comunicación y componentes (Routers, IIoT Gateways, Switches, Access Points, Firewalls, Redes, Protocolos, Fuentes de Alimentación)
- Información (Datos de Operación y Producción, Información de dispositivos, Información de usuarios)
- Algoritmos de toma de decisiones (Inteligencia Artificial y *Machine Learning*)
- Servicios de Computación en la Nube
- Analítica de Big Data
- Robótica
- Monitorizado en tiempo real y herramientas de seguridad (SIEM, IDS/IPS)
- Software y licencias (Programas, Sistemas Operativos, Aplicaciones móviles, Antivirus (Antimalware), Firmware)
- Servidores y Sistemas (Historians, Servidores de Aplicación, Servidores de Bases de Datos, Sistemas de Operaciones Empresariales (ERP, CRM, etc.), MES)
- Dispositivos móviles (Tablets, Smartphones)
- Personal (operadores, Personal de Mantenimiento, Terceras partes)

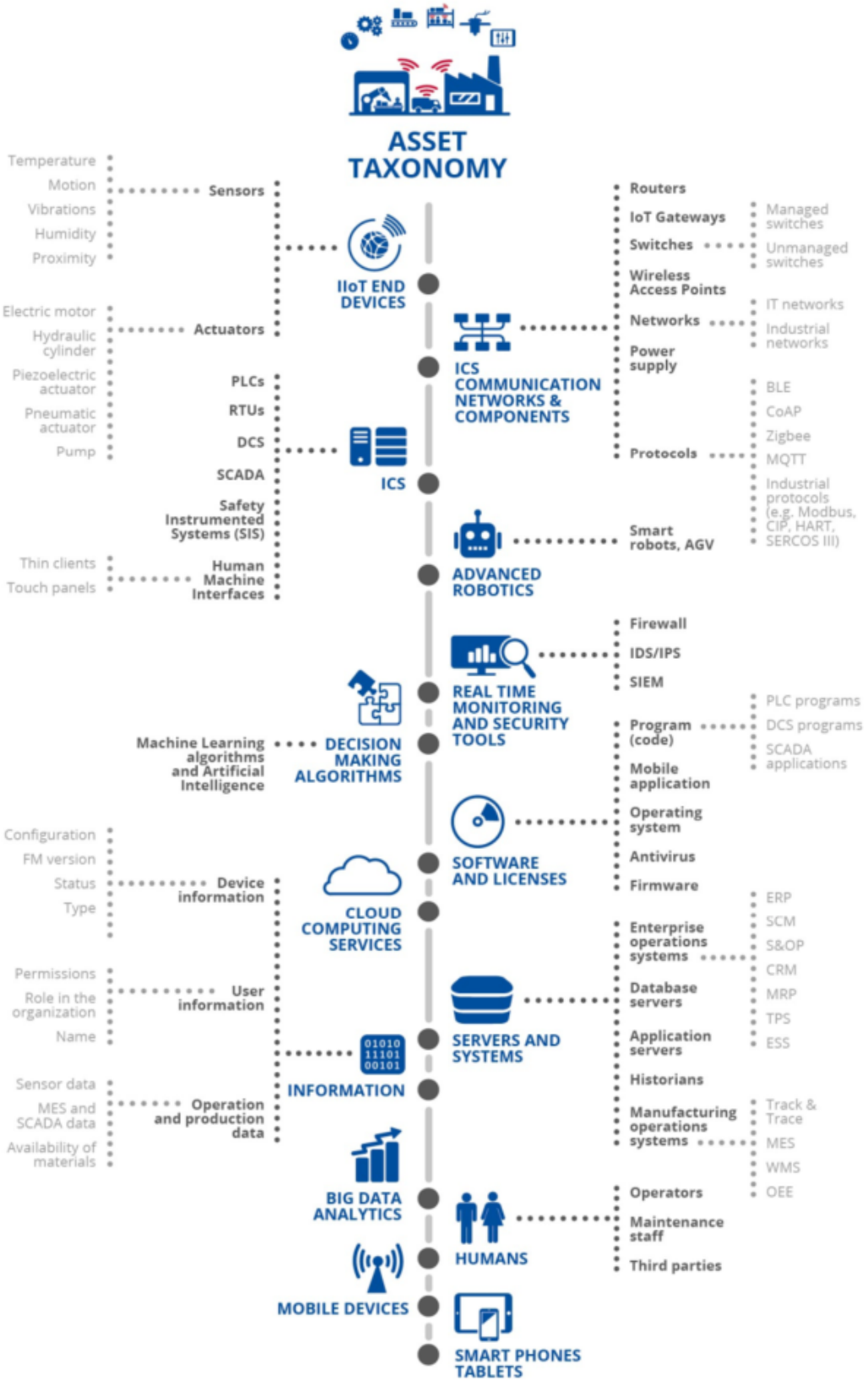


Figura 3.4: Taxonomía de Activos. Fuente: [62]

3.1.4. Taxonomía de Amenazas - *Smart Manufacturing*

Además de las amenazas relacionadas con las tecnologías de IoT, es probable que las empresas de *Smart Manufacturing* y de la I4.0 se vean afectadas por otras amenazas, que son típicas en los entornos de OT e IT [165].

Como parte del trabajo de ENISA se identificaron las siguientes categorías (ver Figura 3.5):

- Abusos/Actividades maliciosas
- Escuchsa/Interceptación/Secuestros
- Ataques físicos
- Daños no intencionales (accidentes)
- Fallas/Malfuncionamiento
- Interrupciones
- Legal
- Desastres

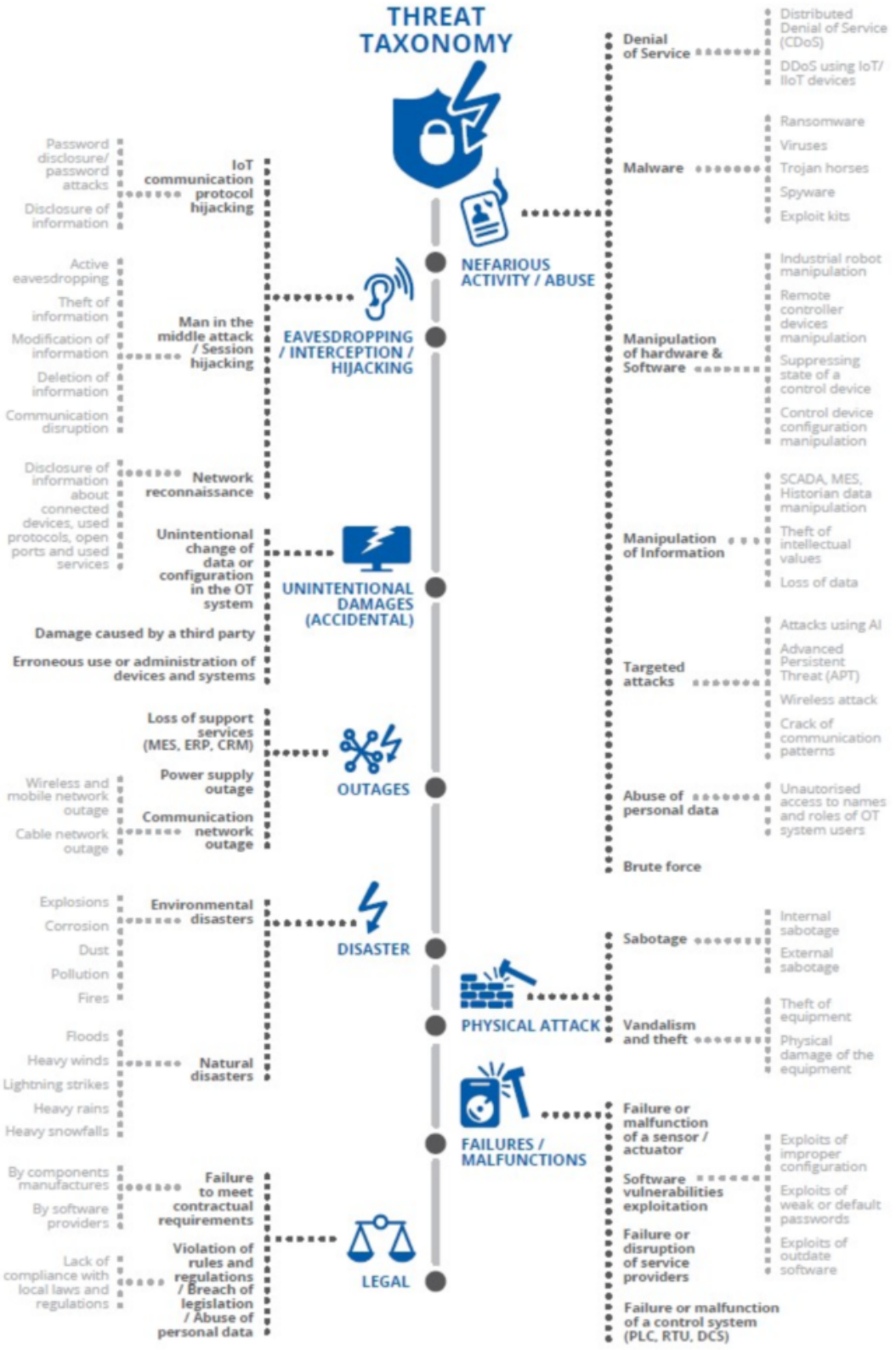


Figura 3.5: Taxonomía de Amenazas. Fuente: [62]

Medidas de seguridad y Buenas Prácticas - *Smart Manufacturing*

A partir del análisis de numerosas fuentes referenciadas en *Good Practices for Security of Internet of Things in the context of Smart Manufacturing*, se identifica un conjunto de medidas de seguridad y buenas prácticas, organizadas en 20 Dominios de Seguridad, los que fueron ordenados clasificándolos en 3 Grupos, los que se pueden observar en la Figura 3.6:

- Políticas
- Prácticas Organizacionales
- Prácticas Técnicas

Figura 3.6: Buenas Prácticas. Fuente: [62]

Las Medidas seleccionadas para componer las Buenas Prácticas, respetan la siguiente notación:

XX-YY

Donde,

XX puede ser PS (Políticas), OP (Prácticas Organizacionales) o TM (Prácticas Técnicas).

YY es un número de dos dígitos.

Cada una de las Buenas Prácticas mencionadas, son vinculadas (en anexos del documento en cuestión) con las amenazas mencionadas antes, así como

también con los dominios considerados, ofreciéndose además referencias donde profundizar al respecto de cada una.

A continuación se enumeran las Buenas Prácticas, segregadas en los siguientes Grupos: Políticas, Prácticas Organizacionales y Prácticas Técnicas.

Políticas

El primer conjunto de 12 medidas corresponde a políticas que en general se focalizan en la seguridad de la información, la que debe ser adecuada a la actividad de la organización.

Se identifican 24 medidas distribuidas en 4 grupos de Buenas Prácticas:

- *Security by design*
- *Privacy by design*
- Gestión de Activos
- Gestión de Riesgos y Amenazas

Prácticas Organizacionales

Se identifican 27 medidas distribuidas en 6 grupos de Buenas Prácticas:

- Ciclo de vida de los *endpoints*
- Arquitectura de Seguridad
- Manejo de Incidentes
- Gestión de vulnerabilidades
- Entrenamiento y Concientización
- Gestión de terceras partes

Medidas Técnicas

Se identifican 59 medidas distribuidas en 10 grupos de Buenas Prácticas:

- Gestión de confianza y de la integridad
- Seguridad en la nube
- Continuidad del Negocio y Recuperación
- Seguridad M2M
- Protección de los datos

- Actualizaciones de software/firmware
- Control de acceso
- Redes, Protocolos y Cifrado
- Monitorizado y Auditado
- Gestión de las configuraciones

Relación con el documento *Baseline Security Recommendations for IoT*

Sobre la base de los criterios de la función empresarial, el IoT se puede dividir en IoT para el consumidor, que incluye plataformas de productos inteligentes conectados que agregan valor a un cliente individual e, IoT industrial, que corresponde a conectividad de la máquina que aumenta el rendimiento de los activos, la calidad del producto, así como la trazabilidad y la responsabilidad, como se representa en la Figura 3.7.

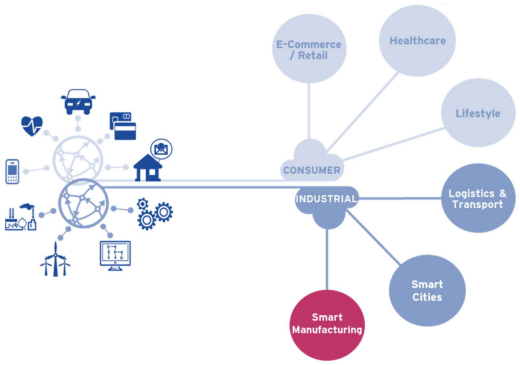


Figura 3.7: Dispositivos IoT del consumidor e IIoT. Fuente: [62]

El concepto de IIoT está asociado con el IoT centrado en la digitalización de las industrias. IoT en general es un concepto mucho más amplio que incluye una variedad de productos de consumo, mientras que IIoT es específico para IoT utilizado en entornos OT. Caracterizados por las similitudes en términos de tecnología, los sistemas IoT suelen estar más centrados en la usabilidad que en el *safety*. Sin embargo, los sistemas IIoT deben cumplir los requisitos de seguridad específicos de los entornos OT, lo que resulta en diferencias en términos de los impulsores de negocio y características propias.

3.2. NIST

En las siguientes secciones se complementa la información brindada en la Sección 4.3 del Capítulo 4 referida al trabajo de NIST.

3.2.1. Mitigación de Riesgos

Como se indicó en la Sección 4.3.1 del Capítulo 4, se identifican 3 grandes objetivos para mitigar los riesgos asociados a la ciberseguridad y la privacidad en los dispositivos IoT: Protección de la Seguridad del Dispositivo, Protección de la Seguridad de los Datos y Protección de la Privacidad de los Individuos. A continuación, para cada uno de los objetivos se detallan las áreas que comprende y las expectativas en cada una:

Protección de la Seguridad del Dispositivo A continuación se enumeran los principales desafíos para cumplir con el objetivo de proteger la seguridad del dispositivo.

Gestión de Activos

- El dispositivo tiene incorporado un identificador único
- El dispositivo se puede integrar con sistemas corporativos de gestión de activos
- El dispositivo puede proveer a la organización suficiente visibilidad de sus características
- El dispositivo, o su fabricante, puede informar a la organización de todo el software y servicios externos que utiliza, como ser software corriendo en él o descargado desde la nube

Gestión de Vulnerabilidades

- El fabricante puede proveer parches o actualizaciones para todo el software y firmware a lo largo de toda su vida útil
- El dispositivo posee una funcionalidad integrada que le permite gestionar de manera segura la configuración, las actualizaciones y parches o, puede integrarse a sistemas de gestión de vulnerabilidades con prestaciones similares

- El dispositivo soporta el uso de *scanners* de vulnerabilidades o posee la funcionalidad integrada de identificación y reporte de vulnerabilidades

Gestión de Acceso

- El dispositivo puede identificar unívocamente a cada usuario o dispositivo, y procesar los intentos de accesos lógicos a él
- El dispositivo puede ocultar en el display los caracteres de las contraseñas cuando la misma es ingresada
- El dispositivo puede autenticar a cada usuario o dispositivo, y procesar los intentos de accesos lógicos a él
- El dispositivo puede utilizar autenticadores y mecanismos de autenticación existentes en la empresa
- El dispositivo puede para cada usuario, dispositivo o proceso, restringir al mínimo necesario los privilegios de acceso
- El dispositivo puede frustrar los intentos de obtener acceso no autorizado, y esta característica se puede configurar o deshabilitar para evitar interrupciones no deseadas en la disponibilidad. Posibles ejemplos de ello son: bloquear o deshabilitar una cuenta cuando hay demasiados intentos de autenticación fallidos consecutivos, retrasar los intentos de autenticación adicionales después de intentos fallidos y bloquear o finalizar sesiones inactivas
- El dispositivo tiene controles de seguridad física incorporados para protegerse de manipulaciones

Detección de Incidentes

- El dispositivo puede registrar los eventos de operación y seguridad
- El dispositivo puede integrarse a sistemas de gestión de registros de la empresa
- El dispositivo puede facilitar la detección de potenciales incidentes mediante controles internos o externos, como ser IPS, utilidades antimalware y mecanismos de control de integridad de archivos
- El dispositivo puede soportar actividades de análisis de eventos e incidentes

Protección de la Seguridad de los Datos A continuación se enumeran los principales desafíos para cumplir con el objetivo de proteger la seguridad de los datos.

Protección de Datos

- El dispositivo puede prevenir accesos no autorizados a todos los datos sensibles en sus dispositivos de almacenamiento
- El dispositivo tiene un mecanismo de disponibilidad de los datos a través de respaldos seguros
- El dispositivo puede prevenir accesos no autorizados a todos los datos sensibles transmitidos desde él hacia la red

Protección de la Privacidad de los Individuos A continuación se enumeran los principales desafíos para cumplir con el objetivo de proteger la privacidad de los individuos.

Gestión de Datos No Asociados

- El dispositivo funciona en un entorno de identidad federado tradicional
- Existen interfaces tradicionales para la interacción de los individuos con el dispositivo
- Hay suficiente control centralizado para aplicar los requisitos regulatorios o las políticas a la PII

Gestión del Flujo de Información

- Existe el suficiente control centralizado para gestionar la PII

3.2.2. Cómo utilizar el *Framework* de Ciberseguridad

Se identifican 6 grandes usos:

- Revisión básica de prácticas de ciberseguridad
- Establecimiento o mejora de un programa de ciberseguridad
- Comunicación de requisitos de ciberseguridad a las partes interesadas
- Decisiones de compra
- Identificación de oportunidades para referencias informativas nuevas o revisadas
- Metodología para proteger la privacidad y las libertades civiles

A continuación se describe brevemente cada uno de ellos.

Revisión básica de prácticas de ciberseguridad

El *Framework* puede ser utilizado para comparar las actividades de seguridad cibernética actuales de una organización con las establecidas en el *Core* del *Framework*. Mediante la creación de un Perfil Actual, las organizaciones pueden examinar en qué medida están logrando los resultados descritos en las Categorías y Subcategorías principales, alineadas con las cinco Funciones de alto nivel: Identificar, Proteger, Detectar, Responder y Recuperar. De esta forma la organización puede concluir si está gestionando la ciberseguridad de una manera adecuada o si puede o requiere mejorar; en el último caso, puede establecer un Plan de Acción para lograrlo.

Establecimiento o mejora de un programa de ciberseguridad

Una serie de pasos ilustran cómo una organización podría utilizar el *Framework* para crear un nuevo programa de seguridad cibernética o mejorar un programa existente. Estos pasos deben repetirse según sea necesario en un plan de mejora continua de la ciberseguridad.

Los pasos son:

- Priorización y Alcance
- Orientación
- Crear un Perfil Actual

- Realizar una Evaluación de Riesgos
- Crear un Perfil Objetivo
- Determinar, Analizar y Priorizar Brechas o *Gaps*
- Implementar Plan de Acción

Es aconsejable que la organización identifique qué pasos repetir y con qué frecuencia a los efectos de aumentar los beneficios resultantes de sus prácticas de ciberseguridad.

Comunicación de requisitos de ciberseguridad a las partes interesadas

El *Framework* proporciona un lenguaje común para comunicar los requisitos entre las partes interesadas interdependientes responsables de la entrega de productos y servicios esenciales de la infraestructura crítica.

La comunicación es especialmente importante entre todas las partes interesadas dentro de las cadenas de suministro. Las cadenas de suministro son conjuntos de recursos y procesos complejos, distribuidos globalmente e interconectados entre múltiples niveles de las organizaciones.

Las cadenas de suministro comienzan con el suministro de productos y servicios y se extienden desde el diseño, desarrollo, fabricación, procesamiento, manejo y entrega de productos y servicios hasta el usuario final. Dadas estas relaciones complejas e interconectadas, la Gestión del Riesgo de la Cadena de Suministro (SCRM, por su sigla en inglés) es una función organizativa crítica.

la SCRM cibernética aborda tanto el efecto de la ciberseguridad que una organización tiene en las partes externas como el efecto de ciberseguridad que las partes externas tienen en una organización.

Un objetivo principal de la SCRM cibernética es identificar, evaluar y mitigar los productos y servicios que pueden contener una funcionalidad potencialmente maliciosa, son falsificados o son vulnerables debido a malas prácticas de fabricación y desarrollo dentro de la cadena de suministro cibernética. La SCRM cibernética puede incluir las siguientes actividades:

- Determinar los requisitos de ciberseguridad para los proveedores
- Promulgar requisitos de ciberseguridad mediante un acuerdo formal (por ejemplo, contratos)

- Comunicar a los proveedores cómo se verificarán y validarán esos requisitos de ciberseguridad
- Verificar que los requisitos de ciberseguridad se cumplan a través de una variedad de metodologías de evaluación
- Gobernar y administrar las actividades anteriores

Decisiones de compra

Dado que un Perfil Objetivo del *Framework* es una lista priorizada de requisitos de ciberseguridad de la organización, los Perfiles Objetivo pueden utilizarse para informar las decisiones sobre la compra de productos y servicios. El objetivo debe ser tomar la mejor decisión de compra entre múltiples proveedores, dada una lista cuidadosamente determinada de requisitos de ciberseguridad. Una vez que se compra un producto o servicio, el Perfil también se puede utilizar para rastrear y abordar el riesgo residual de ciberseguridad.

Identificación de oportunidades para referencias informativas nuevas o revisadas

El *Framework* se puede utilizar para identificar oportunidades de mejora para normas, pautas o prácticas nuevas o revisadas en las que referencias informativas adicionales ayudarían a las organizaciones a abordar las necesidades emergentes. Una organización que implementa una Subcategoría determinada o desarrolla una nueva Subcategoría podría descubrir que hay pocas Referencias Informativas, si las hay, para una actividad relacionada, y colaborar en su desarrollo.

Metodología para proteger la privacidad y las libertades civiles

La privacidad y la ciberseguridad tienen una fuerte conexión. Las actividades de ciberseguridad de una organización también pueden crear riesgos para la privacidad y las libertades civiles cuando se usa, recopila, procesa, mantiene o divulga información personal. Algunos ejemplos incluyen: actividades de ciberseguridad que resultan en la recopilación o retención excesiva de información personal; la divulgación o uso de información personal no relacionada con actividades de ciberseguridad, las actividades de mitigación de la ciberseguridad

que dan lugar a la denegación de servicios u otros impactos potencialmente adversos similares, incluidos algunos tipos de detección o monitorizado de incidentes que pueden inhibir la libertad de expresión o asociación.

Los siguientes procesos y actividades pueden considerarse como un medio para abordar las implicaciones de la privacidad y las libertades civiles mencionadas anteriormente:

- Gobernanza del riesgo de ciberseguridad
- Enfoques para identificar, autenticar y autorizar a las personas a acceder a los activos y sistemas de la organización
- Conciencia y acciones formativas
- Detección de actividad anómala y monitorizado de sistemas y activos
- Actividades de respuesta, incluido el intercambio de información u otros esfuerzos de mitigación

El carácter voluntario y flexible de este *Framework* le otorga la característica de ser efectivo en cuanto a costos y además, puede ser utilizado por las organizaciones para dar prioridad a las actividades de ciberseguridad ajustándose a su presupuesto.

El *Cybersecurity Framework* incluye un Anexo conteniendo 2 tablas: en la primera se indican las Funciones y las Categorías y en la segunda, se describen las Categorías y las Subcategorías, y además se listan las Referencias Informativas y en particular, las secciones de ellas que son relevantes para cada Subcategoría. Las Figuras 3.8 y 3.9 son ejemplos respectivos de ello.

Identificador único de función	Función	Identificador único de categoría	Categoría
ID	Identificar	ID.AM	Gestión de activos
		ID.BE	Entorno empresarial
		ID.GV	Gobernanza
		ID.RA	Evaluación de riesgos
		ID.RM	Estrategia de gestión de riesgos
		ID.SC	Gestión del riesgo de la cadena de suministro
PR	Proteger	PR.AC	Gestión de identidad y control de acceso
		PR.AT	Conciencia y capacitación
		PR.DS	Seguridad de datos
		PR.IP	Procesos y procedimientos de protección de la información
		PR.MA	Mantenimiento
		PR.PT	Tecnología protectora
DE	Detectar	DE.AE	Anomalías y eventos
		DE.CM	Vigilancia continua de seguridad
		DE.DP	Procesos de detección
RS	Responder	RS.RP	Planificación de respuesta
		RS.CO	Comunicaciones
		RS.AN	Análisis
		RS.MI	Mitigación
		RS.IM	Mejoras
RC	Recuperar	RC.RP	Planificación de recuperación
		RC.IM	Mejoras
		RC.CO	Comunicaciones

Figura 3.8: Funciones y Categorías. Fuente: [188]

Función	Categoría	Subcategoría	Referencias informativas
IDENTIFICAR (ID)	**Gestión de activos (ID.AM):** Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos empresariales se identifican y se administran de forma coherente con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización.	**ID.AM-1:** Los dispositivos y sistemas físicos dentro de la organización están inventariados.	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Las plataformas de software y las aplicaciones dentro de la organización están inventariadas.	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: La comunicación organizacional y los flujos de datos están mapeados.	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: Los sistemas de información externos están catalogados.	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Los recursos (por ejemplo, hardware, dispositivos, datos, tiempo, personal y software) se priorizan en función de su clasificación, criticidad y valor comercial.	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Los roles y las responsabilidades de la seguridad cibernética para toda la fuerza de trabajo y terceros interesados	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03

Figura 3.9: Ejemplo de Categoria, Subcategorias y Ref. Informativas. Fuente: [188]

3.2.3. Referencias Informativas para la elaboración del *Framework*

Las seis Referencias Informativas consideradas en el *Framework* son:

- NIST SP 800-53 Rev. 4 [194]
- ISO/IEC 27001:2013 [159]
- COBIT 5 [157]
- CIS CSC [37]
- ISA 62443-2-1:2009 [156]
- ISA 62443-3-3:2013 [155]

El *Framework* habilita a que se incorporen otras Referencias Informativas. En la Figura 3.10 se muestra un ejemplo de Referencias Informativas asociadas a algunas de las Subcategorías del *Framework*.

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Figura 3.10: Ejemplo de Subcategorías. Fuente: [183]

3.3. IETF

En las siguientes secciones se complementa la información brindada en la sección 4.4 del Capítulo 4 referida al trabajo del IETF .

3.3.0.1. Otras consideraciones de la RFC 8576

En los siguientes párrafos se incluyen otros aspectos de la RFC 8576 que resultan relevantes para la temática del trabajo.

Condiciones para la seguridad en IoT

Si bien se reconoce que la seguridad es un tema clave en cualquier sistema de comunicación, es una requerimiento aún más crítico en los despliegues IoT, por las razones que se enumeran a continuación:

- Un sistema IoT comprometido no sólo puede hacer peligrar la seguridad y la privacidad de un usuario, sino que además, puede causar daños físicos
- Un sistema IoT vulnerable significa que un atacante puede alterar alguna funcionalidad de algún dispositivo de algún fabricante, afectando no solamente su imagen sino que también puede implicar la difusión de información de alto valor
- El impacto de un ataque a un sistema IoT puede ir más allá de un dispositivo o sistema aislado, pudiendo alcanzar otros dispositivos y sistemas no considerados, siendo ejemplo de ello los ataques de DDoS

Amenazas a la seguridad y Gestión de Riesgos

A continuación se transcriben las diversas amenazas identificadas en la RFC 8576 que pueden comprometer un dispositivo en particular o toda una red, considerando no sólo aquellas que pueden afectar los protocolos de Internet y además, que la criticidad puede estar condicionada por el escenario donde se despliega el sistema IoT:

- Código/software vulnerable
- Amenaza a la privacidad
- Clonado de cosas

- Sustitución maliciosa de cosas
- Ataque de Eavesdropping
- Ataque de *Man-in-the-Middle*
- Ataques al Firmware
- Extracción de información privada
- Ataque al *routing*
- Elevación de privilegios
- Ataques de DoS

Metodologías a contemplar

Los diferentes dispositivos son y serán fabricados y desplegados en ambientes muy diversos, habiendo sido auditados en cuanto a la seguridad de diferente formas y con rigurosidades dispares, y estarán sujetos a diferentes amenazas, cambiantes y nuevas, muchas de las cuales surgirán luego del despliegue de los sistemas IoT vulnerables a ellas. En esta RFC se identifican diversas metodologías que de ser utilizadas, pueden ayudar a manejar los desafíos mencionados, ellas son:

- Realizar un *Business Impact Analysis* (BIA) evaluando las consecuencias de la pérdida de algunos de los atributos básicos de la seguridad (del sistema o entidad IoT): confidencialidad, integridad y disponibilidad. El resultado del BIA puede ser un input relevante al momento de considerar la seguridad en el diseño.
- Realizar un *Risk Assessment* (RA), pues analiza las amenazas a la seguridad de un sistema IoT considerando la probabilidad y el impacto, clasificando cada uno según niveles predefinidos, debiendo ser mitigados aquellos de riesgo moderado y alto.
- Realizar una *Privacy Impact Assessment* (PIA), dado que ayuda a identificar la *Personally Identifiable Information* (PII) que es reunida, procesada y utilizada por un sistema IoT. Esto ayuda a identificar los cumplimientos de los requerimientos legales y a reconocer los riesgos por la pérdida de la PII.

Los BIA, RA y PIA deberían ser realizados durante la creación de un nuevo sistema IoT, o durante el despliegue de algún *upgrade*. En general se

recomienda que se realicen periódicamente considerando nuevos casos de uso y/o amenazas.

Estado del Arte

En la RFC 8576 se mencionan y analizan brevemente los protocolos y estándares de IoT basados en IP y, algunos protocolos y soluciones de seguridad basados en IP. Además, se enumeran algunas de las organizaciones que trabajan en la elaboración de guías destinadas a desarrolladores y la comunidad en general, para construir dispositivos y servicios IoT seguros. Las mencionadas son:

- *Global System for Mobile Communications Association (GSMA) IoT security guidelines*
- *Broadband Internet Technical Advisory Group (BITAG) IoT Security and Privacy Recommendations*
- *United Kingdom Department for Digital, Culture, Media and Sport (DCMS)*
- *Cloud Security Alliance (CSA) New Security Guidance for Early Adopters of the IoT*
- *United States Department of Homeland Security (DHS)*
- *National Institute of Standards and Technology (NIST)*
- *Open Web Application Security Project (OWASP)*
- *IoT Security Foundation*
- *National Highway Traffic Safety Administration (NHTSA)*
- *"Best Current Practices for Securing Internet of Things (IoT) Devices"*
- *European Union Agency for Network and Information Security (ENISA)*
- *Internet Society Online Trust Alliance*

Desafíos para un IoT Seguro

Luego de analizar más de cerca los diversos desafíos de seguridad en las características operativas y técnicas de IoT, y de discutir cómo los protocolos de seguridad de Internet que existentes hacen frente a ellos a lo largo del ciclo de vida del dispositivo, se identificaron los siguientes 11 aspectos a considerar:

- Restricciones y comunicaciones heterogéneas

- Arranque de un dominio de seguridad
- Desafíos operacionales
- Actualización segura de software y agilidad criptográfica
- Fin de la vida del dispositivo
- Verificación del comportamiento del dispositivo
- *Testing*
- Resistencia cuántica
- Protección de la privacidad
- Consideraciones de ingeniería reversa
- Operación confiable

Con el foco en los objetivos del presente trabajo, a continuación se hará énfasis en algunos de los desafíos mencionados.

La heterogeniedad que resulta de acoplar redes con restricciones de recursos e Internet, significa en sí mismo un desafío. Los despliegues IoT frecuentemente son *lossy* y con canales de bajo ancho de banda. Por otro lado, los dispositivos IoT en general presentan restricciones en términos de CPU, memoria y energía; ello impacta directamente en la selección de los protocolos apropiados para utilizar en el dominio IoT.

Las restricciones características de los dispositivos IoT los hace blanco de ataques que se centran en el agotamiento de recursos, y en algunos casos (por ejemplo en las comunicaciones T2T) la detección de un ataque se realiza "a hecho consumado", por ejemplo, ante una indisponibilidad.

La creación de un dominio de seguridad a partir de un conjunto de dispositivos IoT no asociados anteriormente es una operación clave en el ciclo de vida de una cosa en una red IoT. En esa línea, se trabaja actualmente en identificar mecanismos para disponer de un *bootstrapping* seguro en IoT. Una línea de trabajo al respecto, aunque actualmente discontinuada en dicho ámbito, es el *draft* del IETF denominado *Secure IoT Bootstrapping: A Survey* [91].

En dicho *draft* se define *bootstrapping* como el proceso por el cual el estado de un dispositivo, un subsistema, una red o una aplicación cambia de no operativo a operativo; en este caso es un dispositivo que, como se afirmó antes, frecuentemente tiene restricciones de recursos. A título general, en algunos contextos el término *onboarding* se utiliza como sinónimo de *bootstrapping*. Además, se mencionan y describen diferentes métodos que pueden aplicables para el *bootstrapping* de dispositivos IoT, considerando aspectos vinculados a

la autenticación, la autorización y el intercambios de claves.

3.3.1. *Manufacturer Usage Descriptor*

Si bien el nombre hace referencia al fabricante, la concepción debe ser más amplia, y debemos considerar que el MUD puede ser proporcionado también por un integrador de componentes IoT, o por un proveedor de servicios.

Un MUD está compuesto de una URL donde se localiza la descripción, ella en sí misma (y cómo interpretarla) y una forma de obtener dicha descripción por parte del sistema de gestión local donde se está instalando el dispositivo IoT.

El MUD queda determinado a partir de la combinación de los casos de uso de un dispositivo IoT con las comunicaciones que se requieren para ello [87].

Arquitectura MUD

La arquitectura MUD estaría compuesta, en su visión más general, por cuatro componentes (se acompaña cada uno con al menos un ejemplo concreto):

- La cosa (dispositivo IoT)
- El dispositivo de red (router, switch, access point)
- El MUD *Manager* (AAA server, radius)
- El MUD *File Server* (web server)

En la Figura 3.11 se puede encontrar una referencia al proceso MUD. La secuencia de pasos para el uso del MUD es la siguiente: El dispositivo de red obtiene la MUD URL emitida por "la cosa", la informa al MUD *Manager* y éste obtiene desde el MUD *File Server* el MUD *file* (la política recomendada por el "*manufacturer*") y su firma, realizada mediante *Cryptographic Message Syntax* (CMS) [84]. El MUD *Manager* valida la firma y analiza la URL contra algún servicio de reputaciones (por ejemplo, vía DNS), interpreta la información disponible en el MUD *file* y la traslada a configuraciones apropiadas en los elementos de la red (ACLs y/o reglas de *firewalls* y/o reglas de flujos de datos); las políticas son removidas cuando el dispositivo se desconecta de la red.

Las reglas del MUD file pueden limitar tanto el tráfico Norte/Sur como también el tráfico Este/Oeste.

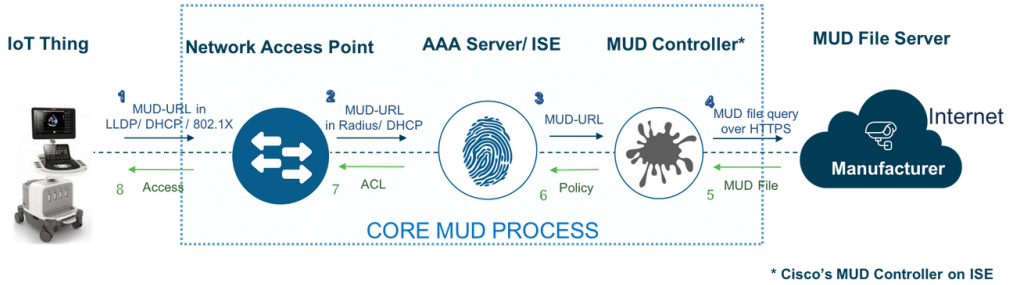


Figura 3.11: Flujo del proceso MUD de CISCO. Fuente: [38]

La MUD URL (que debe utilizar el esquema *https*) permite clasificar el tipo de dispositivo y localizar el archivo con la política a aplicar. Las posibles opciones identificadas para informarla, son:

- como una opción de DHCP (específicamente, la 161)
- como una extensión de un certificado X.509 en un proceso basado en el protocolo IEEE 802.1X
- utilizando el protocolo *Link Layer Discovery Protocol* (LLDP, IEEE 802.1AB)

El estándar propone que el archivo MUD sea una instancia de modelo YANG que se ha serializado en JSON [93, 92, 94, 88].

Si bien se identifica al concepto MUD con control de acceso, hay otros usos posibles, como por ejemplo la posibilidad de describir condiciones de calidad de servicio requeridas o deseadas.

Pruebas de Concepto del MUD

En el marco de su trabajo para identificar cómo mitigar los ataques DDoS basados en IoT [179], el *National Cybersecurity Center of Excellence* (NCCoE) del NIST, ha elaborado el borrador final del *Securing Small Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)*, SP 1800-15 [193].

Esta guía práctica está destinada a mostrar a los desarrolladores y fabricantes de dispositivos de IoT, a los desarrolladores y fabricantes de equipos de red, y a los proveedores de servicios que emplean componentes compatibles

con MUD, cómo integrar y usar MUD y otras herramientas para satisfacer los requerimientos de seguridad de los usuarios de IoT. En la publicación *Securing Small-Business and Home Internet of Things (IoT) Devices - Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)* [192], se describen cuatro implementaciones MUD, con diferentes grados de avance, utilizando productos y soluciones de diferentes proveedores y colaboradores.

3.4. Internet Society

En esta sección se reflejan los conceptos fundamentales de 2 artículos referenciales de la Internet Society en relación a IoT.

3.4.1. *IoT Trust Framework*

La Internet Society elaboró un documento denominado *Top Tips for Consumers: Internet of Things Security and Privacy* donde reúne un conjunto de consejos (*tips*) genéricos relativos a seguridad y privacidad destinados a los consumidores [151] y, a partir del trabajo de la *Online Trust Alliance* (OTA), una inciativa de la *Internet Society*, y en el marco del *OTA IoT Trust Framework* [148], han elaborado el *IoT Trust by Design*, que es identificado también como *OTA IoT Trust Framework Summary*.

El *IoT Trust Framework* se caracteriza por dos aspectos que son destacados por sus autores como únicos:

- Abarca cuestiones de seguridad, privacidad y sostenibilidad a largo plazo (ciclo de vida)
- Aborda holísticamente todo el ecosistema

El *Framework* incluye una lista de principios a considerar agrupados en 8 categorías:

- Autenticación
- Cifrado
- Seguridad
- Actualizaciones
- Privacidad
- Divulgaciones
- Control
- Comunicaciones

Garantizar niveles adecuados de seguridad y privacidad para los productos y servicios de IoT es una responsabilidad colectiva. Los principios del *Framework* pueden ser utilizados por una amplia gama de partes interesadas para cumplir su función en la protección de los usuarios e Internet, identificando las siguientes:

- Proveedores de IoT y su cadena de suministro
- Canales de distribución
- Responsables de la formulación de políticas y organismos gubernamentales
- Organizaciones de pruebas de consumidores y revisión de productos
- Consumidores y empresas

En lo que refiere a la responsabilidad colectiva, la *Internet Society* invoca el concepto de Seguridad Colaborativa [144], en el entendido que la gente es la que en última instancia mantiene a Internet unida. El desarrollo de Internet se ha basado en la cooperación y la colaboración voluntarias. La cooperación y la colaboración siguen siendo los factores esenciales para la prosperidad y el potencial de Internet.

En ese sentido, se identifican cinco aspectos clave para la seguridad colaborativa:

- Fomentar la confianza y proteger las oportunidades
- Responsabilidad Colectiva
- Propiedades y valores fundamentales
- Evolución y consenso
- Piense globalmente, actúe localmente

El *Internet of Things (IoT) Trust Framework* [146] está divido en cuatro grandes áreas:

- Principios de Seguridad
- Credenciales y Acceso de Usuarios
- Privacidad, Divulgación y Transparencia
- Notificaciones y Mejores Prácticas Relacionadas

El *Framework* incluye un conjunto de 40 principios estratégicos necesarios para ayudar a proteger los dispositivos IoT y sus datos cuando se envían y durante todo su ciclo de vida. En él se menciona la necesidad de divulgaciones completas que deben proporcionarse antes de la compra del producto, políticas relativas a la recopilación y uso compartido de datos, así como los términos y condiciones de la aplicación de parches de seguridad después de la garantía. Las actualizaciones de seguridad son esenciales para maximizar la protección

de los dispositivos IoT cuando se descubren vulnerabilidades y los ataques evolucionan. Además, el *Framework* proporciona recomendaciones para que los fabricantes mejoren la transparencia y la comunicación con respecto a la capacidad de actualización de los dispositivos y una serie de cuestiones relacionadas con la privacidad de los datos. Sirviendo como una guía de evaluación de riesgos para desarrolladores, compradores y minoristas, el *Framework* es la base para futuros programas de certificación de IoT.

3.4.2. *Policy Brief: IoT Privacy for Policymakers*

En este artículo elaborado por la Internet Society [149], se afirma que los dispositivos conectados socavan un principio fundamental de la privacidad: la capacidad de mantener los contextos separados entre sí como elegimos. Esto es especialmente significativo en el caso de los dispositivos IoT domésticos y portátiles, debido a las fuertes presunciones de privacidad que asociamos con los contextos del hogar y el cuerpo.

El ámbito principal del trabajo es la IoT del consumidor, aunque muchas de las consideraciones y recomendaciones que en él se plasman se pueden aplicar de forma más amplia.

La privacidad es un factor clave en las relaciones de confianza. Cuando divulgamos datos a otros, estamos (implícitamente o de otra manera) confiando en que no los utilicen de manera que entren en conflicto con nuestros intereses.

En el dominio de IoT, por lo tanto, la privacidad conlleva fuertes implicaciones de confianza, transparencia y control: es fundamental para las personas poder controlar cómo se comparte la información recopilada por sus dispositivos IoT y determinar quién tiene acceso a los datos de los dispositivos de su hogar, en su automóvil y en su persona.

También resulta relevante conocer con claridad sobre cómo se recopila, usa y comparte la información sobre las personas con otras personas, cuán identificable es uno cuando se realizan actividades en línea o fuera de línea y tener la capacidad de controlar la huella digital.

La privacidad es un valor social e individualista: apoya y empodera a las personas con la opción de retirarse de la mirada y de las interacciones con otras a voluntad, y es el derecho al respeto por su espacio personal, para crear soledad y reserva respecto a los demás.

De acuerdo con este derecho a la privacidad, las personas deben poder dis-

frutar de los beneficios de la IoT del consumidor, ya sea con el menor riesgo de privacidad posible, o después de haber hecho un juicio claro e informado sobre el riesgo y el beneficio. La confianza de los consumidores en IoT puede afectar potencialmente a la confianza de los consumidores en general, y finalmente también a la confianza en la red Internet.

La IoT se caracteriza por una serie de factores:

- Escala, en lo que refiere al número creciente de dispositivos IoT
- Proximidad, relacionado con la intimidad, por la cantidad cada vez mayor de dispositivos portátiles e implantados "cerca de las personas"
- Ubicuidad, debido al despliegue masivo de IoT en espacios públicos y privados
- Conexión, dado que muchos de los dispositivos IoT tienden a estar siempre conectados, o están en momentos que los usuarios no lo saben

Estos factores tienen un impacto en la privacidad pues hacen que sea más fácil que el individuo sea:

- Identificado
- Seguido
- Perfilado
- Influenciado

IoT amplifica los desafíos de privacidad existentes y crea otros nuevos. Por ejemplo, el aumento de la escala de sensores y la proximidad crea el potencial para el monitorizado continuo de las actividades, comportamientos, habla, salud y emociones de las personas. El IoT hará que las personas sean más identificables en espacios públicos y privados.

Los dispositivos IoT están conectados, pero no necesariamente son "inteligentes". Debido a que los dispositivos son "tontos", los datos que recopilan a menudo se procesan en otro lugar. A su vez, tiende a proliferar la cantidad de productos y servicios de IoT "en silos", motiva en parte por la falta de estandarización, de interoperabilidad y de reducir el TTM.

IoT reduce los espacios privados en general. La combinación de las tendencias anteriores (escala y proximidad del sensor, monitorizado continuo, aumento de la identificación y la "ruptura de las paredes del hogar") apunta a una posible disminución en la capacidad de las personas para encontrar lugares privados de reserva y soledad en general.

La protección de la privacidad es un pilar clave que apoya la confianza en IoT y nuestras interacciones con ella. La confianza en los actores clave de IoT (proveedores de servicios, empresas de infraestructura, minoristas, gobiernos y fabricantes) es necesaria para aprovechar los beneficios de las próximas oleadas de dispositivos conectados. La privacidad es un aspecto fundamental de la construcción de esa confianza. Los dispositivos IoT recopilarán una serie de nuevos datos y comportamientos personales: los consumidores deben confiar en que los custodios de estos datos los tratarán adecuadamente, y disponer de las pruebas de ello cuando así lo requieran. En ausencia de esta confianza, las personas no aceptarán dispositivos IoT, temerosos de que sus datos sean inseguros o se compartan de forma inapropiada.

Principios rectores recomendados

Mejorar el control de usuario
Mejorar el control significativo del usuario de los dispositivos y servicios de IoT y la administración de los datos que recopilan.

Mejorar la transparencia y la notificación
La información a los usuarios debe mejorar la transparencia y el control al ser claros, precisos, pertinentes y adecuadamente detallados.

Mantener el ritmo con la tecnología
Actualizar las leyes y políticas de privacidad para reflejar el nuevo mundo de sensores omnipresentes y monitorizado continuo.

Fortalecer el enfoque de múltiples partes interesadas para la privacidad de IoT
Abordar la diversidad de los riesgos y beneficios de la IoT, ampliando la gama de participantes en el debate sobre la gobernanza de la IoT.

Los autores afirman que estamos en un momento crítico en el que tenemos que tomar medidas para garantizar que los beneficios de IoT superen los riesgos de privacidad, pero eso requerirá un esfuerzo colaborativo de todas las partes interesadas, incluidos los responsables políticos, los fabricantes y los consumidores, para que las oportunidades representados por IoT se desarrollan de manera sostenible y responsable.

3.5. *Smart Nation* - Índice SIRI - Matriz de Priorización

Aquí se presenta la Metodología de Cálculo de la Matriz de Priorización propuesta en la referencia *The Prioritisation Matrix* del EDB de Singapur [255].

3.5.1. Metodología de Cálculo

El objetivo es obtener de la organización analizada las entradas necesarias para la Matriz de Priorización. Los pasos a seguir para aplicar la Metodología son los que se muestran en la Tabla 3.1.

En la Figura 3.12 se dispone de la referencias a considerar respecto al Horizonte de Planificación, requerido al momento de ejecutar el paso 4 de la Metodología de Cálculo.

Weightage Distribution according to Planning Horizon

Planning Horizon	Cost Factor (W_c)	KPI Factor (W_k)	Proximity Factor (W_p)
Strategic (3 – 5 years)	30%	40%	30%
Tactical (1 – 2 years)	45%	30%	25%
Operational (3 – 6 months)	60%	20%	20%

Figura 3.12: *Horizonte de Planificación.* Fuente: página 29 de [255]

La Metodología de Cálculo propuesta involucra la utilización de 4 tablas diferentes[1]:

- *Degree of Relevance (Cost)* - DOR_C. Ver Figura 3.13.
- *Degree of Relevance (KPI)* - DOR_K. Ver Figura 3.14.
- *Industry Best-in-Class (BIC) Benchmarks.* Ver Figura 3.15.
- *Summary.* Ver Figura 3.16.

[1]Las tablas que se muestras corresponden a un Caso de Estudio ilustrativo considerado en [255].

Paso	Acciones
1	En la tabla *Summary* (Figura 3.16), en la sección *Priorisation Matrix Results*, en la fila *Assessment Matrix Score*, ingresar el *Score* de la Matriz de Evaluación (valor de cada Banda), para cada uno de las 16 Dimensiones del Índice SIRI. Realizar el mismo proceso en la fila *Assessment Matrix Score* de la Tabla *Industry Best-in-Class (BIC) Benchmarks* (Figura 3.15).
2	En la tabla *Degree of Relevance (Cost)* (Figura 3.13), en la columna *Input*, ingresar el Perfil de Costos desagregado porcentualmente en las 10 categorías contempladas y respecto a los ingresos anuales totales.
3	En la tabla *Degree of Relevance (KPI)* (Figura 3.14), en la columna *Input*, seleccionar los 5 KPIs más relevantes de las 14 posibles, ingresando un "1" en ellos, y un "0" en los restantes.
4	En la tabla *Summary* (Figura 3.16), en la sección *Weightages*, definir un Horizonte de Planificación (Operacional, Táctico o Estratégico), lo que determinará las ponderaciones a ser aplicadas a cada uno de los 3 Factores (Costo, KPI y Proximidad), W_{Cost}, W_{KPI} y $W_{Proximidad}$ respectivamente. Para ello se debería considerar la propuesta de la Figura 3.12.
5	En la tabla *Industry Best-in-Class (BIC) Benchmarks*(Figura 3.15), en la columna *Input*, seleccionar el tipo de industria.
6	En la tabla *Degree of Relevance (Cost)* (Figura 3.13), para cada Dimensión SIRI, multiplicar cada valor DOR_C por el valor correspondiente en la columna *Input* para las 10 categorías de costos y sumar los valores obtenidos, obteniendo así, para cada Dimensión, su Factor Costo en la fila correspondiente.
7	En la tabla *Degree of Relevance (KPI)* (Figura 3.14), para cada Dimensión SIRI, multiplicar cada valor DOR_K por el valor correspondiente en la columna *Input* para los 14 KPIs y sumar los valores obtenidos, obteniendo así, para cada Dimensión, su Factor KPI en la fila correspondiente.
8	En la tabla *Industry Best-in-Class (BIC) Benchmarks* (Figura 3.15), para cada Dimensión SIRI, restar el valor de la fila *Assessment Matrix Score* al de la industria seleccionada y colocar el resultado en la fila *Proximity Factor*. Si el resultado es negativo, colocar "0".
9	Traslade a la respectivas filas de la tabla *Summary* (Figura 3.16), en la sección *Impact Value*, los valores obtenidos para los Factores Costos, KPI y Proximidad. En cada caso, sume y complete la columna **Total**.
10	En la tabla *Summary* (Figura 3.16), en la sección *Normalised Factors*, complete cada celda el resultado de dividir el valor de la celda correspondiente ("Factor-Dimensión") por el valor de la celda de la columna **Total** que corresponda.
11	En la fila *Impact Value* de la sección *Priorisation Matrix Results* de la tabla *Summary* (Figura 3.16), complete cada celda de cada Dimensión con el resultado de la suma ponderada de los Factores normalizados.
12	En la tabla *Summary* (Figura 3.16) y para cada Bloque (Procesos, Tecnología y Organización), seleccione la Dimensión que haya obtenido el Valor de Impacto más alto. Adicionalmente, de las restantes 13 Dimensiones, seleccione también aquella con el Valor de Impacto más alto.

Tabla 3.1: Metodología de Cálculo. Fuente: [255]

De esta forma, habiendo recorrido secuencialmente los 12 pasos detallados en la Tabla 3.1 se habrán identificado las 4 Dimensiones que resultan de mayor impacto para la organización y es hacia donde se deberían enfocar los esfuerzos, los recursos y la atención, para recorrer adecuadamente la hoja de ruta hacia la madurez en la Industria 4.0.

Degree of Relevance (Cost)																
Cost Categories	Input	Process			Technology									Organisation			
		Vertical Integration	Horizontal Integration	Integrated Product Lifecycle	Shop Floor Automation	Enterprise Automation	Facility Automation	Shop Floor Connectivity	Enterprise Connectivity	Facility Connectivity	Shop Floor Intelligence	Enterprise Intelligence	Facility Intelligence	Workforce Learning & Development	Leadership Competency	Inter- & Intra-Company Collaboration	Strategy & Governance
Aftermarket Services / Warranty	0.00	0	1	3	0	3	0	0	1	0	0	3	0	1	1	1	1
Depreciation	0.03	1	0	0	0	0	0	1	0	1	1	0	1	0	1	0	1
Labour	0.24	3	0	0	3	0	3	1	0	1	3	0	3	3	3	3	3
Maintenance & Repair	0.01	3	1	1	1	1	1	1	1	1	3	1	3	3	1	1	1
Raw Material & Consumables	0.38	3	3	1	1	1	1	1	1	1	3	3	1	0	1	1	1
Rental & Operating Lease	0.00	1	1	0	1	1	1	1	1	1	1	1	1	0	1	0	1
Research & Development	0.05	1	1	3	0	3	0	0	1	0	0	3	0	3	1	3	3
SG&A	0.17	1	3	1	0	3	0	0	1	0	0	3	0	3	3	3	3
Transporation & Distribution	0.03	0	3	0	0	1	0	0	1	0	0	3	0	1	1	3	1
Utilities	0.05	1	1	0	1	1	3	1	1	1	1	1	3	0	1	0	1
Cost Factor		2.19	1.85	0.71	1.16	1.13	1.26	0.71	0.69	0.71	1.97	1.95	1.31	1.44	1.78	1.86	1.88

Figura 3.13: *Degree of Relevance (Cost).* Fuente: página 38 de [255]

Degree of Relevance (KPI)																	
KPI Categories	Input	Process			Technology									Organisation			
		Vertical Integration	Horizontal Integration	Integrated Product Lifecycle	Shop Floor Automation	Enterprise Automation	Facility Automation	Shop Floor Connectivity	Enterprise Connectivity	Facility Connectivity	Shop Floor Intelligence	Enterprise Intelligence	Facility Intelligence	Workforce Learning & Development	Leadership Competency	Inter- & Intra-Company Collaboration	Strategy & Governance
Asset & Equipment Efficiency	0	3	1	0	3	1	3	3	1	3	3	1	3	1	1	1	1
Workforce Efficiency	1	3	3	3	3	3	3	1	1	1	3	3	3	3	3	3	3
Utilities Efficiency	0	1	0	0	1	0	3	1	0	3	1	0	3	1	1	1	1
Inventory Efficiency	1	3	3	0	3	3	0	1	1	0	3	3	0	1	1	1	1
Materials Efficiency	0	3	0	3	1	1	0	1	1	0	3	3	0	1	1	1	1
Process Quality	1	3	1	1	3	3	3	1	1	1	3	3	3	3	3	3	1
Product Quality	0	3	1	3	3	1	1	1	1	1	3	1	1	3	1	3	1
Safety	0	1	0	0	3	0	3	1	0	1	3	0	3	1	3	1	1
Security	0	1	1	1	0	0	0	3	3	3	1	1	1	3	3	1	3
Planning & Scheduling Effectiveness	1	1	3	0	0	3	0	1	3	0	1	3	0	1	1	1	1
Production Flexibility	0	3	1	0	3	0	1	3	0	1	3	0	1	1	3	1	3
Workforce Flexibility	1	3	1	1	1	1	1	3	1	3	3	1	3	3	3	3	3
Time to Market	0	0	0	3	0	3	0	0	3	0	0	3	0	1	3	1	3
Time to Delivery	0	3	3	0	3	3	1	3	3	1	3	3	1	1	3	3	1
KPI Factor		13	11	5	10	13	7	7	7	5	13	13	9	11	11	11	9

Figura 3.14: *Degree of Relevance (KPI).* Fuente: página 39 de [255]

Industry Best-In-Class (BIC) Benchmarks																	
SIRI Industry Classification	Input	Process			Technology									Organisation			
		Vertical Integration	Horizontal Integration	Integrated Product Lifecycle	Shop Floor Automation	Enterprise Automation	Facility Automation	Shop Floor Connectivity	Enterprise Connectivity	Facility Connectivity	Shop Floor Intelligence	Enterprise Intelligence	Facility Intelligence	Workforce Learning & Development	Leadership Competency	Inter- & Intra-Company Collaboration	Strategy & Governance
Aerospace		3	3	3	2	3	2	4	4	2	3	3	2	3	3	3	3
Automotive		3	4	4	2	3	2	4	4	2	3	3	2	4	4	4	4
Electronics	X	4	4	3	3	3	2	4	4	3	5	4	4	4	4	4	4
Energy & Chemicals (Downstream)		4	3	3	3	3	3	4	4	4	4	3	4	4	4	4	4
Food & Beverages		4	3	3	3	3	3	4	4	4	3	2	2	4	4	4	4
General Manufacturing		4	4	4	3	3	2	4	4	2	3	3	2	4	4	4	4
Logistics		2	4	3	3	4	3	4	4	4	2	3	2	3	3	3	3
Machinery & Equipment		3	4	4	2	2	2	4	4	2	2	3	2	3	3	4	3
Medical Technology		4	4	3	4	3	2	4	4	2	3	2	2	4	4	4	4
Oil & Gas (Upstream)		2	3	3	2	2	2	2	3	2	2	3	2	2	2	2	2
Pharmaceuticals		4	3	3	3	2	3	4	4	4	4	3	4	4	4	4	4
Precision Parts		3	3	3	3	3	2	4	4	2	2	2	2	3	3	3	3
Semiconductors		4	4	3	3	3	3	4	4	4	3	3	2	4	4	4	4
Textiles, Clothing, Leather & Footwear		3	4	4	2	3	2	4	4	2	3	3	2	3	4	4	4
Assessment Matrix Score		1	1	2	1	1	0	0	2	0	1	2	0	2	1	2	1
Proximity Factor		3	3	1	2	2	2	4	2	3	4	2	4	2	3	2	3

Figura 3.15: *Industry Best-in-Class (BIC) Benchmarks.* Fuente: página 40 de [255]

Summary Table

$$\text{Impact Value} = [\,W_{cost} \cdot \text{Cost Factor}_N\,] + [\,W_{KPI} \cdot \text{KPI Factor}_N\,] + [\,W_{Proximity} \cdot \text{Proximity Factor}_N\,]$$

Dimension	Process			Technology									Organisation				
	Vertical Integration	Horizontal Integration	Integrated Product Lifecycle	Shop Floor Automation	Enterprise Automation	Facility Automation	Shop Floor Connectivity	Enterprise Connectivity	Facility Connectivity	Shop Floor Intelligence	Enterprise Intelligence	Facility Intelligence	Workforce Learning & Development	Leadership Competency	Inter-/Intra-Collaboration	Strategy & Governance	Total
Cost Factor	2.19	1.85	0.71	1.16	1.13	1.26	0.71	0.69	0.71	1.97	1.95	1.31	1.44	1.78	1.86	1.88	22.6
KPI Factor	13	11	5	10	13	7	7	7	5	13	13	9	11	11	11	9	155
Proximity Factor	3	3	1	2	2	2	4	2	3	4	2	4	2	3	2	3	42
Normalised Factors																	
Cost Factor_N	0.0969	0.0819	0.0314	0.0513	0.0500	0.0558	0.0314	0.0305	0.0314	0.0872	0.0863	0.0580	0.0637	0.0788	0.0823	0.0832	
KPI Factor_N	0.0839	0.0710	0.0323	0.0645	0.0839	0.0452	0.0452	0.0452	0.0323	0.0839	0.0839	0.0581	0.0710	0.0710	0.0710	0.0581	
$\text{Proximity Factor}_N$	0.0714	0.0714	0.0238	0.0476	0.0476	0.0476	0.0952	0.0476	0.0714	0.0952	0.0476	0.0952	0.0476	0.0714	0.0476	0.0714	
Weightages																	
Planning Horizon			Strategic	W_{Cost}		0.3		W_{KPI}		0.4			$W_{Proximity}$		0.3		
Prioritisation Matrix Results																	
Assessment Matrix Score	1	1	2	1	1	0	0	2	0	1	2	0	2	1	2	1	
Impact Value	0.0840	0.0744	0.0295	0.0555	0.0628	0.0491	0.0561	0.0415	0.0438	0.0883	0.0737	0.0692	0.0618	0.0734	0.0674	0.0696	

Figura 3.16: *Summary.* Fuente: página 41 de [255]

Apéndice 4

Modelo de Madurez en Confiabilidad

De acuerdo a como se detalló en la Sección 5.2.3 del Capítulo 5 los niveles de Exhaustividad considerados son:

- 1. Mínimo
- 2. *Ad Hoc*
- 3. Consistente
- 4. Formalizado

A continuación se expresan los niveles de Exhaustividad para cada Dominio, Subdominio y Práctica del Modelo de Madurez en Confiabilidad.

4.1. Niveles de Exhaustividad

A continuación, para cada uno de sus Dominios, Subdominios y Prácticas del Modelo de Madurez en Confiabilidad (TMM), se describe la consideración para cada uno.

4.1.1. Dominio Gobernanza de la Confiabilidad

1. Establecer una base general para las consideraciones de confiabilidad
2. Establecer medidas de confiabilidad de referencia
3. Facilitar la implementación de capacidades de confiabilidad

4. Establecer una estructura de gobernanza de confiabilidad, con procesos claros asociados a seguridad, *safety*, resiliencia, fiabilidad y privacidad, y vinculados de manera consistente

Subdominio Estrategia y Cumplimiento

1. Objetivos de visión, alcance y confiabilidad
2. Mejores prácticas más apropiadas
3. Enfoques y estándares reconocidos
4. Apoyo consistente a los procesos del negocio, legales, operacionales y de otros temas

Práctica Gestión del Programa de Confiabilidad

1. Describir la provisión general de confiabilidad
2. Referencia a los objetivos de confiabilidad más relevantes y cómo son abordados
3. Cobertura de los tópicos generales de los estándares de gestión de la confiabilidad reconocidos
4. Implementar una planificación clara, una provisión oportuna y el control de las actividades de confiabilidad

Práctica Gestión del Cumplimiento

1. Ser conscientes de los facilitadores de cumplimiento
2. Considerar algunos requisitos opcionales de cumplimiento para la implementación
3. Implementar requisitos de cumplimiento obligatorios
4. Supervisar la evolución de los requisitos estándar para el cumplimiento

Subdominio Gestión de Riesgos y Amenazas

1. Revisión del panorama actual de amenazas
2. Entendimiento de las vulnerabilidades del sistema y la tecnología
3. Descripción completa de los riesgos relevantes
4. Enfoque holístico y sistemática de la gestión de riesgos

Práctica Gestión de Amenazas

1. Referir a los problemas generales de seguridad de TI como amenazas
2. Identificar y describir las amenazas de manera ad hoc

3. Describir y clasificar las amenazas de una manera precisa (opcionalmente de manera formal)
4. Revelar y describir claramente los factores de TI conocidos y específicos que pueden poner el sistema en riesgo

Práctica Gestión de Riesgos

1. Definir informalmente la noción de riesgo
2. Diferenciar la importancia de los riesgos
3. Medir y gestionar adecuadamente los riesgos
4. Utilizar un marco y procesos de gestión de riesgos

Subdominio Cadena de Suministro y Gestión de Terceras Partes

1. Chequeo de reputación de proveedores y contratistas
2. Garantía de confiabilidad de los artefactos de la cadena de suministros
3. Certificados y otras garantías provistos por autoridades de confianza
4. Control de exposición a posibles daños desde proveedores y contratistas

Práctica Gestión de la Cadena de Suministros

1. Monitorizar parches y vulnerabilidades para los componentes suministrados
2. Implementar algunas pruebas de seguridad para los componentes suministrados
3. Obtener certificados u otras garantías de seguridad para los componentes esenciales
4. Aplicar una política de gestión de riesgos para la cadena de suministros

Práctica Gestión de los Servicios de Terceras Partes

1. Monitorizar la reputación de los contratistas
2. Proporcionar la calidad de los servicios a través de acuerdos contractuales
3. Obtener evidencia de terceras partes respecto a la calidad del servicio
4. Aplicar una política de gestión de confiabilidad uniforme a los contratistas

Subdominio Medidas, Métricas e Indicadores

1. Ocasionalmente realizar algunas medidas a los efectos de analizar ciertas métricas e indicadores no definidos formalmente
2. Periódicamente realizar algunas medidas y generar algunas métricas, a los

efectos de analizar la situación de algunos indicadores vinculados a la confiabilidad, definidos formalmente
3. Sistemáticamente recopilar mediciones relevantes para la confiabilidad, tanto con herramientas integradas como específicamente diseñadas, generar las métricas correspondientes y analizar la situación en cuanto a los KPIs más relevantes, definidos formalmente
4. Mantener un proceso continuo, revisado y mejorado, de medición de todo lo relevante respecto a la confiabilidad, elaboración de métricas y valoración de todos los indicadores relacionados con la confiabilidad y formalizados en la organización

Práctica Medidas

1. Ocasionalmente se realizan algunas medidas
2. Periódicamente se realizan algunas medidas que pueden vincularse con la confiabilidad
3. Sistemáticamente recopilar algunas mediciones relevantes para la confiabilidad, utilizando herramientas de IT/OT
4. Proceso de medición, revisado y mejorado, de todo lo relevante respecto a la confiabilidad, sustentado en herramientas de IT/OT

Práctica Métricas e Indicadores

1. Generación ocasional de algunas métricas e indicadores no definidos formalmente
2. Generación periódica de algunas métricas e indicadores definidos formalmente que tienen relevancia para evaluar la confiabilidad
3. Generación sistemática de las métricas y KPIs relevantes para la confiabilidad, mediante el uso de herramientas IT/OT
4. Proceso, revisado y mejorado, de generación sistemática de todas las métricas y KPIs relevantes para la confiabilidad, mediante el uso de herramientas IT/OT

4.1.2. Dominio Confiabilidad Organizacional

1. Disponer de referencias básicas sin un plan de difusión
2. Implementar un plan de difusión para las referencias básicas

3. Facilitar los métodos y las herramientas para contar con un plan completo
4. Establecer el proceso de mejora continua del plan de confiabilidad organizacional

4.1.2.0.1. Subdominio Cultura Organizacional

1. Visión informal de la cultura de la organización sustentada en las creencias de las mayorías y/o de las jerarquías
2. En las situaciones más comunes la cultura percibida es verificada
3. A partir de aplicar un proceso reconocido se conoce la cultura organizacional
4. Existe un proceso continuo mediante el cual toda la organización se impregna de la cultura organizacional [58, 59]

Práctica Identificación e Impacto Interno

1. La organización intuye, en base a la situaciones más comunes, cuál es su cultura organizacional
2. Contrasta con situaciones similares para identificar su cultura organizacional
3. Mediante una metodología formal, ha identificado su perfil actual de cultura organizacional, el impacto y interno y la cultura deseada
4. Mediante una metodología formal, ha evolucionado a la cultura deseada y dispone de un proceso contínuo de mejora y fortalecimiento

Práctica Impacto Externo

1. Acciones no coordinadas y parciales permiten deducir el impacto externo de su cultura organizacional
2. Existen acciones coordinadas para identificar el impacto externo
3. Se dispone de un plan para evaluar el impacto externo
4. La organización cuenta con un proceso que evalúa el impacto externo y de manera formal identifica acciones para potenciar lo positivo y mitigar lo negativo

Subdominio Desarrollo y Gestión del Capital Humano

1. Existen iniciativas personas no coordinadas ni completas que en general cubren los aspectos fundamentales
2. Los aspectos fundamentales son cubiertos mediante actividades no planificadas
3. Existe un proceso en marcha que cubre los requisitos de las mejores prácti-

cas aplicables
4. Se dispone de un proceso completo de mejora continua, con medidas planificadas y reactivas tempranas

Práctica Desarrollo

1. Se intenta que el personal ya cuente con la formación y las habilidades blandas necesarias
2. La mayoría del personal dispone de la formación y habilidades blandas mínimas para las tareas que desempeña
3. Detalle de la formación y habilidades blandas necesarias para cada perfil del personal, y cumplimiento del mismo
4. Proceso bien establecido de mejora continua de la formación y habilidades blandas de todo el personal

Práctica Gestión del Capital Humano

1. Proceso informal de evaluación de competencias
2. Instancias formales y periódicas de evaluación y devolución, con prácticas de retención de talentos
3. Proceso de evaluación, devolución y recompensa, y proceso de captación y retención de talentos
4. Procesos bien establecido de mejora continua con identificación de diferenciales sustanciales

Subdominio Aprendizaje y Mejora Continua

1. Se apoyan actividades básicas
2. Se identifican los requerimientos particulares y se cubren las necesidades más comunes
3. Se dispone de un proceso de seguimiento basado en las mejores prácticas para identificar las necesidades
4. Existe un plan de mejora continua focalizado en la evaluación, el seguimiento y la recompensa

Práctica Aprendizaje

1. Se fomentan actividades de aprendizaje
2. Plan básico que fomenta actividades de aprendizaje y evaluación
3. Herramienta que sustenta el aprendizaje continuo, fomentando actividades

según las necesidades
4. Existe un plan bien establecido que fomenta los paradigmas “aprender a aprender”, “aprender a desaprender” y “aprender y desaprender toda la vida”

Práctica Mejora Continua
1. Ocasionalmente se identifican mejoras a productos o procesos
2. Periódicamente se identifican mejoras a productos o procesos, a partir de cuestiones básicas
3. A partir de una estrategia coordinada, se realizan instancias formales para identificar mejoras a productos o procesos
4. Existe un plan bien establecido para identificar mejoras a productos o procesos, o nuevos productos o nuevos procesos

4.1.3. Dominio Establecimiento de la Confiabilidad

1. Realizar el uso de los controles de confiabilidad disponibles
2. Implementar controles de confiabilidad de acuerdo con los escenarios de uso conocidos
3. Emplear tanto mecanismos integrados como adicionales para cubrir los riesgos conocidos
4. Establecer el proceso para abordar los riesgos por los mejores medios disponibles

Subdominio Gestión de Identidades y Accesos
1. Apoyar a las entidades elementales para el escenario de uso básico
2. Diferenciar a los actores para los escenarios de acceso general
3. Emplear las mejores prácticas para apoyar escenarios de acceso sofisticados
4. Protección integral contra los riesgos relacionados con el acceso no autorizado

Práctica Gestión de Identidades
1. Mantener una o varias cuentas de la misma forma o muy similar
2. Administrar las identidades de varios grupos de personas, sistemas o cosas
3. Apoyar una amplia gama de identidades aprovechando los mecanismos automatizados

4. Mantener y controlar el uso de identidades de personas, sistemas y cosas a lo largo de su ciclo de vida

Práctica Control de Acceso

1. Sólo restringir la posibilidad de acceso a los sistemas a agentes externos
2. Considerar el rol del sujeto y controlar los derechos de acceso
3. Utilizar políticas de control de acceso disponibles con un adecuado nivel de garantía
4. Mantener un esquema de autorización estrictamente alineado a las necesidades y restricciones del negocio

Subdominio Gestión de Activos

1. Trazabilidad del uso de los activos físicos y digitales
2. Monitorizado de los activos sobre la base de casos de uso
3. Gestión y protección de los activos de diversos tipos
4. Garantía de cumplimiento de las políticas de gestión de activos

Práctica Gestión de Configuración y Cambios en los Activos

1. Seguir los cambios no frecuentes en los activos y las configuraciones
2. Seguir algunas reglas específicas para gestionar posibles cambios a los sistemas
3. Mantener procedimientos de gestión de cambio para los activos y/o las configuraciones
4. Regular el proceso del ciclo de vida de los activos, desde el aprovisionamiento hasta el reemplazo, incluyendo cambios de emergencia

Práctica Protección Física

1. En general se limita el acceso a los activos físicos
2. Customizar las restricciones de acceso considerando tiempo y forma de acceso físico
3. Control de acceso físico automático y ajustable utilizando *tokens* de identidad específicos
4. Abordar todos los aspectos de la seguridad física y *safety*, prevenir robos y garantizar un funcionamiento safety y continuo

Subdominio Protección de Datos

1. Mantenimiento general de la confidencialidad, integridad y disponibilidad de los datos
2. Un mayor nivel de garantía para algunos datos
3. Implementación de políticas y métodos reconocidos para la protección de los datos
4. Garantía de la protección de la información crítica del negocio, en tránsito, almacenada y en uso

Práctica Modelo y Política de Seguridad de los Datos

1. Declarar que los datos deberían ser protegidos frente a accesos no autorizados
2. Definir una categorización simple de los datos y las restricciones apropiadas
3. Definir el enfoque particular y los roles/atributos para controlar el acceso a los datos
4. Categorizar y proteger consistentemente los datos de acuerdo a los requerimientos de las partes interesadas

Práctica Controles de Protección de los Datos

1. Aprovechar los controles de protección integrados (SO, red, servicios)
2. Configurar controles integrados y asegurarse de que su uso se ajuste a los objetivos de protección de datos
3. Apoyar la correcta aplicación de los controles de datos de acuerdo con las normas reconocidas
4. Garantizar la protección necesaria de cada elemento de datos tanto en tránsito como en reposo

Subdominio Análisis y Diseño

1. Se tiene una idea general de su relevancia
2. Consideración de los aspectos fundamentales a considerar para las situaciones más comunes
3. Lista exhaustiva de aspectos y contextos a evaluar en las etapas fundamentales de cada fase
4. Proceso formal de evaluación de todos los aspectos y contextos, con las posibles decisiones en cada caso

Práctica Análisis

1. Análisis de requisitos obligatorios y deseables en cuanto a factibilidad, costos y tiempos
2. Impacto por incumplimiento o retraso en algunos de los requisitos obligatorios y deseables
3. Se dispone de un proceso de análisis donde además se contempla las premisas que "desde el inicio funciona bien" y "sin necesidades inmediatas de readecuación"
4. Existe un plan bien establecido con una herramienta de seguimiento del proceso de análisis y mejoras basadas en lecciones aprendidas

Práctica Diseño

1. Se dispone de un plan de diseño parcial
2. Durante el mismo se consideran sólo los aspectos más relevantes del análisis
3. Se consideran los requisitos de las mejores prácticas, reglamentos y normativas, con herramientas de apoyo para todo el proceso
4. Existe un plan bien establecido que brinda un apoyo de mejora continua a todo el proceso, considerando el ciclo de vida del producto, y que genera lecciones aprendidas

4.1.4. Dominio Fortalecimiento de la Confiabilidad

1. Aplicar las prácticas reconocidas de *trustworthiness-by-design*
2. Mejorar la protección del sistema de acuerdo con sus necesidades y prioridades
3. Emplear los métodos y herramientas bien reconocidos que permitan la confiabilidad
4. Establecer el proceso continuo de apoyo a los objetivos de la confiabilidad

Subdominio Gestión de Parches y Vulnerabilidades

1. Mantener los sistemas actualizados y menos propensos a ataques
2. Aplicar una política de actualización regular para los componentes críticos
3. Actualizaciones automatizadas configuradas específicamente para el caso
4. Planificación de un proceso de actualizaciones regulares y considerando escenarios de emergencia para eventos críticos del tipo *zero-day*

Práctica Gestión de Parches

1. Considerar los avisos de seguridad emitidos por los proveedores e instalar los parches apropiados
2. Comprobar que los componentes especificados están protegidos contra los ataques más probables
3. Establecer procedimientos de actualización automática siempre que sea posible
4. Implantar una política para el sistema con el objetivo de garantizar la protección continua contra ataques conocidos

Práctica Gestión de Vulnerabilidades

1. Considerar si las vulnerabilidades ampliamente conocidas son relevantes para el sistema
2. Comprobar si los componentes especificados son propensos a ataques
3. Obtener una evaluación objetiva de terceros respecto a vulnerabilidades y exposiciones
4. Realizar inspecciones de seguridad de manera regular, personalizadas y profundas

Subdominio Conciencia Situacional

1. Mantener una conciencia mínima de eventos relacionados con la seguridad
2. Atención específica a algunos tipos de eventos de seguridad
3. Supervisión integral y intercambio regular de información relacionada con la seguridad
4. Proporcionar y gestionar toda la información relevante para los aspectos de confiabilidad

Práctica Monitorizado y Auditado

1. Ocasionalmente chequear los logs del sistema a los efectos de realizar diagnósticos
2. Periódicamente chequear eventos que indiquen qué tan adecuadamente se ejecutan los procesos críticos
3. Recopilar y analizar información relevante para la seguridad, tanto con herramientas integradas como específicamente diseñadas
4. Actuar como catalizador y generador de capacidad para la protección continua del sistema

Práctica Comunicación e Intercambio de Información

1. Obtener alguna información externa relevante en base a una estrategia no formal
2. Habilitar al personal a que consistentemente utilice fuentes externas de información relevante
3. Realizar intercambios de información con autoridades y con la comunidad
4. Establecer comunicaciones bidireccionales con foco en situaciones *zero-day* e incidentes en la industria

Subdominio Gestión de Eventos e Incidentes y Continuidad de las Operaciones

1. Chequeo de la recuperación de los sistemas luego de los incidentes
2. Aseguramiento de la recuperación de los componentes de los sistemas o procesos
3. Procedimiento de recuperación automática siempre que sea posible y que se tengan informes adecuados
4. Respuesta rápida ante incidentes y reducción de daños a la empresa tanto por medios técnicos como organizativos

Práctica Gestión de Incidentes de Confiabilidad

1. Definir eventos específicos y acciones básicas para reaccionar a ellos
2. Proveer una guía aplicada a componentes críticos y cómo detectar y responder a los incidentes
3. Establecer las bases para la ejecución automática de los procedimientos de respuesta
4. Crear controles para detectar incidentes, asignarlos para ser investigados y escalarlos de ser necesario

Práctica Continuidad de las Operaciones

1. Brindar las instrucciones básicas para la recuperación del sistema
2. Manejar incidentes conocidos y comprobar si el sistema está completamente recuperado
3. Permitir la ejecución automática de procedimientos de corrección y recuperación
4. Apoyar una combinación de medidas técnicas y organizativas que faciliten la rápida recuperación del sistema

Subdominio Verificación y Validación

1. Testings básicos a muestras no siempre representativas sin asegurarse el descarte o corrección ante incumplimientos
2. Testings básicos a muestras representativas con descarte o correcciones ante incumplimientos
3. Los testings a realizar, las muestras a considerar y las acciones a tomar se basan en las regulaciones y mejores prácticas de la industria
4. Existe un proceso bien establecido que incorpora la mejora continua al *testing*

Práctica Verificación

1. Revisiones básicas en todas las fases del diseño
2. En cada fase, las revisiones contemplan los casos de uso más comunes
3. Una herramienta sustenta el seguimiento de las revisiones en cada fase, considerando las mejores practicas y las regulaciones pertinentes
4. Un plan de mejora continua bien establecido, con generación de lecciones aprendidas, permite guía todo el diseño

Práctica Validación

1. Revisiones básicas para verificar que se creó el producto deseado
2. Revisiones exhaustivas que siguen un checklist predefinido
3. Proceso de revisión basado en las mejores prácticas, normas y reglamentos aplicables, con informes finales
4. Plan bien establecido, completo y en mejora continua que revisa completamente (cualitativa y cuantitativamente) el producto para validar (o no) el producto, generando reportes y lecciones aprendidas

4.2. Evaluación de las Prácticas

4.2.1. Consideraciones generales

Las evaluaciones de las diferentes Prácticas que se proponen implican que deben estar a disposición del equipo evaluador las evidencias que sustenten lo afirmado y/o documentado respecto a la Práctica en cuestión. El nivel de exigencia en cuanto a las evidencias que se pueden solicitar debería ser directamente proporcional al nivel de madurez exigido o esperado. Para cada Práctica, se plantean diversos aspectos que de cumplirse de manera completa, se estaría en el Nivel de Exhaustividad más alto de acuerdo a lo expresado en la Sección 5.2.3 del Capítulo 5. Se debe tener presente que el no cumplimiento de alguno de los aspectos no necesariamente puede implicar bajar de nivel de Exhaustividad, si se trata de algo que carece de sentido para el sistema IIoT analizado, lo que debe ser acompañado de la justificación correspondiente.

4.2.2. Vínculo entre las Prácticas

En la descripción de los aspectos a considerar en las diferentes prácticas, se podrán encontrar menciones a aspectos de otras prácticas, lo que refuerza el concepto de que lograr una visión integral de las mismas, otorga a la aplicación del modelo la consistencia necesaria.

4.2.3. Consideraciones propuestas para cada una de las Prácticas

A continuación, para cada una de las Prácticas del modelo TMM se mencionan las consideraciones a tener en cuenta.

Práctica Gestión del Programa de Confiabilidad

La práctica de gestión de programas de confiabilidad es vital para la planificación clara y la provisión oportuna de las actividades de confiabilidad, el control sobre el proceso y los resultados, y el procedimiento óptimo de toma de decisiones para el cumplimiento de las demandas relacionadas con la confiabilidad.

El Programa de Confiabilidad se compone a su vez de cinco programas, a saber: Programa de Seguridad, Programa de *Safety*, Programa de Resiliencia,

Programa de Fiabilidad y Programa de Privacidad, los que se deben ejecutarse de manera paralela, con diferentes "intensidades" según el tipo de industria, el tipo de sistema y los objetivos de mejora en el nivel de madurez impuesto en la organización en cuestión. A su vez, se debe tener presente que así como ya sabemos que las características de la confiabilidad se pueden potenciar entre sí, y también contraponer, ello se podrá ver reflejado -o deberá resolverse- en los programas correspondientes.

Para la evaluación del nivel de madurez en la Práctica de Gestión del Programa de Confiabilidad se debe analizar, por un lado, el nivel de madurez de cada uno de los cinco programas y por otro, el grado de articulación entre todos ellos.

Se debe recordar que el modelo de madurez que se plantea tiene un fuerte enfoque horizontal, lo que hace que, en principio, todos los programas tengan igual relevancia. Si el modelo es aplicado a alguna vertical en particular, allí sí podrá cobrar mayor relevancia alguno/s de ello/s frente a los restantes.

Evaluación del Programa de Seguridad

La evaluación debe estar fuertemente regida por el principio de *security by design*, considerando al menos, los siguientes aspectos: La seguridad (ciberseguridad) en IIoT debe tratarse como un ciclo de mejora continua y no como un proyecto.

La seguridad debe ser considerada desde el comienzo mismo de todo proceso involucrado con el sistema IIoT que se está evaluando.

Debe ser considerada la normativa local e internacional que sea aplicable.

La mejora continua debe ser aplicada en cada paso del ciclo de vida de desarrollo del sistema (SDLC, por su sigla en inglés) o sea, desde el análisis hasta la disposición final del producto.

Implementación de mecanismos de *fail-secure* en el sistema, susbsistemas, sistemas embebidos asociados y producto.

Implementación de mecanismos de seguridad en todos los componentes del sistema, adaptados a sus capacidades y a su relevancia, considerando premisas básicas como ser: principio de mínimo privilegio, principio de necesidad de saber, autenticación, autorización, registro de actividades, deshabilitar configuraciones no necesarias y recomendaciones de *hardening* asociadas a la tecnología y al proveedor.

Difusión adecuada a cada una de las partes interesadas de los consideraciones

de seguridad de la organización, del sistema y del producto.
Realización periódica y planificada de análisis de amenazas y riesgos, identificando prestaciones de seguridad necesarias, como oportunidades de mejora a partir de lecciones aprendidas o de avances tecnológicos o de procesos.
Disposición de certificaciones asociadas.
Plan en marcha de concientización, sensibilización, entrenamiento, capacitación y aprendizaje en aspectos de seguridad.
Asegurar que el diseño por ahorro de consumo no compromete la seguridad.
Análisis y consideración del impacto del programa en los cuatro programas restantes.
Inclusión de un ítem respecto a la seguridad en todo documento que se elabore, donde se expliciten las consideraciones al respecto, si corresponde.

Evaluación del Programa de *Safety*

La evaluación debe estar fuertemente regida por el principio de *safety by design*, considerando al menos, los siguientes aspectos: El *safety* debe tratarse como un ciclo de mejora contínua y no como un proyecto.
El *safety* debe ser considerada desde el comienzo mismo de todo proceso involucrado con el sistema IIoT que se está evaluando.
Safety implica la protección de la vida y la salud de los seres vivos, así como también, la protección del medioambiente.
Debe ser considerada la normativa local e internacional que sea aplicable.
La mejora continua debe ser aplicada en cada paso del ciclo de vida de desarrollo del sistema (SDLC) o sea, desde el análisis hasta la disposición final del producto.
Implementación de mecanismos de fail-safe en el sistema, susbsistemas, sistemas embebidos asociados y en el producto.
Implementación de mecanismos de *safety* en todos los componentes del sistema que corresponda, considerando premisas básicas como ser: identificación clara y completa de todas las consideraciones de *safety*de cada componente, conocimiento de las mismas por parte de las personas vinculadas directamente, condiciones de trabajo no riesgosas conocidas, entendidas y respetadas, planes de emergencia elaborados, evaluados, aprobados y prontos para ser ejecutados en caso de requerirse.
Difusión adecuada a cada una de las partes interesadas de los consideraciones de *safety* de la organización, del sistema y del producto.

Disposición de certificaciones asociadas.
Realización periódica y planificada de verificación y validación de las medidas de *safety* a los efectos de evaluar el cumplimiento de la normativa, de los requerimientos de diseño e identificar las prestaciones de *safety* necesarias, como oportunidades de mejora a partir de lecciones aprendidas o de avances tecnológicos o de procesos.
Plan en marcha de concientización, sensibilización, entrenamiento, capacitación y aprendizaje en aspectos de *safety*.
Análisis y consideración del impacto del programa en los cuatro programas restantes.
Inclusión de un ítem respecto a *safety* en todo documento que se elabore, donde se expliciten las consideraciones al respecto, si corresponde.

Evaluación del Programa de Resiliencia

La evaluación debe estar fuertemente regida por el principio de *resilience by design*, considerando al menos, los siguientes aspectos: La resiliencia [29, 28] debe tratarse como un ciclo de mejora continua y no como un proyecto.
La resiliencia debe ser considerada desde el comienzo mismo de todo proceso involucrado con el sistema IIoT que se está evaluando.
Identificación de los servicios o prestaciones críticas que el sistema debe seguir proveyendo en presencia de perturbaciones.
Plan en marcha de detección de eventos y condiciones adversas afectarán al sistema o a sus componentes o al producto.
Plan en marcha para que el sistema, los componentes o el producto responda de manera adecuada a las distorsiones detectadas, y poder recuperarse rápidamente de ello.
Plan en marcha de concientización, sensibilización, entrenamiento, capacitación y aprendizaje en aspectos de resiliencia.
Plan en marcha de análisis y *testing* de resiliencia contemplando la identificación de condiciones de estrés y condiciones de falla, para disponer de modelos de resiliencia y predicciones.
Plan en marcha de gestión de la cadena de suministro de componentes o servicios en lo que refiere a su resiliencia y su impacto en el sistema que está siendo evaluado.
Plan en marcha de seguimiento de fallas, documentando qué, porqué, dónde, cuándo y cómo falló, para la elaboración de recomendaciones para corregir y

prevenir fallas futuras ("lecciones aprendidas").
Realización periódica y planificada de verificación y validación de las medidas de resiliencia a los efectos de evaluar el cumplimiento de la normativa, de los requerimientos de diseño e identificar las prestaciones de resiliencia necesarias, como oportunidades de mejora a partir de lecciones aprendidas o de avances tecnológicos o de procesos.
Debe ser considerada la normativa local e internacional que sea aplicable.
Difusión adecuada a cada una de las partes interesadas de los consideraciones de resiliencia de la organización, del sistema y del producto.
Disposición de certificaciones asociadas.
Análisis y consideración del impacto del programa en los cuatro programas restantes.
Inclusión de un ítem respecto a la resiliencia en todo documento que se elabore, donde se expliciten las consideraciones al respecto, si corresponde.

Evaluación del Programa de Fiabilidad

La evaluación debe estar fuertemente regida por el principio de *reliability by resign*, considerando al menos, los siguientes aspectos: La fiabilidad debe tratarse como un ciclo de mejora continua y no como un proyecto.
La fiabilidad debe ser considerada desde el comienzo mismo de todo proceso involucrado con el sistema IIoT que se está evaluando.
Plan en marcha de identificación de los requerimientos de fiabilidad, tanto para el sistema que está siendo evaluado, como para sus componentes, y para el producto.
Plan en marcha de concientización, sensibilización, entrenamiento, capacitación y aprendizaje en aspectos de fiabilidad.
Plan en marcha de análisis y *testing* de fiabilidad contemplando la identificación de condiciones de estrés y condiciones de falla, para disponer de modelos de fiabilidad y predicciones.
Plan en marcha de gestión de la cadena de suministro de componentes o servicios en lo que refiere a su fiabilidad y su impacto en el sistema que está siendo evaluado.
Plan en marcha de seguimiento de fallas, documentando qué, porqué, dónde, cuándo y cómo falló, para la elaboración de recomendaciones para corregir y prevenir fallas futuras ("lecciones aprendidas").
Realización periódica y planificada de verificación y validación de las medidas

de fiabilidad a los efectos de evaluar el cumplimiento de la normativa, de los requerimientos de diseño e identificar las prestaciones de fiabilidad necesarias, como oportunidades de mejora a partir de lecciones aprendidas o de avances tecnológicos o de procesos.
Debe ser considerada la normativa local e internacional que sea aplicable. Difusión adecuada a cada una de las partes interesadas de los consideraciones de fiabilidad de la organización, del sistema y del producto.
Disposición de certificaciones asociadas.
Análisis y consideración del impacto del programa en los cuatro programas restantes.
Inclusión de un ítem respecto a la fiabilidad en todo documento que se elabore, donde se expliciten las consideraciones al respecto, si corresponde.

Evaluación del Programa de Privacidad

La evaluación debe estar fuertemente regida por el principio de *privacy by design*, considerando al menos, los siguientes aspectos: La privacidad debe tratarse como un ciclo de mejora continua y no como un proyecto.
La privacidad debe ser considerada desde el comienzo mismo de todo proceso involucrado con el sistema IIoT que se está evaluando.
Debe ser considerada la normativa local e internacional que sea aplicable.
La mejora continua debe ser aplicada en cada paso del ciclo de vida de desarrollo del sistema (SDLC, por su sigla en inglés) o sea, desde el análisis hasta la disposición final del producto.
Implementación de mecanismos de privacidad en todos los componentes del sistema que corresponda, considerando premisas básicas como ser: qué datos son considerados, con qué fin, minimizar los datos personales que se gestionan, brindar la protección adecuada a dichos datos, permitir al dueño de los datos auditar el uso y protección de los datos, así como también, la eliminación comprobada de los mismos, revisión periódica de permisos de accesos a los datos, y gestión de dichos permisos.
Difusión adecuada a cada una de las partes interesadas de las consideraciones de privacidad de la organización, del sistema y del producto.
Disposición de certificaciones asociadas.
Realización periódica y planificada de análisis de impacto en la privacidad (PIA, por su sigla en inglés), a los efectos de evaluar el cumplimiento de la normativa e identificar las prestaciones de privacidad necesarias. Plan en marcha

de concientización, sensibilización, entrenamiento, capacitación y aprendizaje en aspectos de privacidad.
Análisis y consideración del impacto del programa en los cuatro programas restantes.
Inclusión de un ítem respecto a la privacidad en todo documento que se elabore, donde se expliciten las consideraciones al respecto, si corresponde.

Evaluación del grado de articulación entre los cinco programas
La evaluación debe considerar la existencia de los análisis y consideraciones correspondientes en cada uno de los cinco programas, y la consistencia y coherencia entre ellos.

Práctica Gestión del Cumplimiento
La práctica de gestión del cumplimiento se impone cuando existen requisitos para el cumplimiento de los estándares o buenas prácticas de confiabilidad.
La evaluación del cumplimiento de esta práctica debe contemplar, al menos, los siguientes aspectos: Identificación, entendimiento y correcta consideración de la normativa y regulación local e internacional que corresponda, así como estándares y buenas prácticas, que deban ser consideradas para la adecuada implementación y mejora de los cinco programas que componen la práctica Gestión del Programa de Confiabilidad.
Revisión periódica para identificar nuevas versiones de la normativa y regulación, así como estándares y buenas prácticas aplicables.
Revisión periódica para identificar nueva normativa y regulación, así como estándares y buenas prácticas aplicables.
Revisión periódica para identificar obsolescencia en la normativa y regulación, así como en los estándares y las buenas prácticas aplicadas.
Plan de análisis de la necesidad de readecuaciones internas a la organización en caso modificaciones relacionadas con la normativa y regulaciones, así como estándares y buenas prácticas aplicables.
Elaboración y mantenimiento de contratos con terceras partes involucradas, de acuerdo con los cinco programas que componen la Práctica Gestión del Programa de Confiabilidad.
Plan de análisis de la necesidad de readecuaciones internas a la organización en caso de modificaciones en los contratos con terceras partes, o incumplimientos.
Plan de seguimiento de las expectativas de los clientes o usuarios.

Plan de análisis de la necesidad de readecuaciones internas a la organización en caso de identificarse expectativas de los clientes o usuarios que se consideren relevantes, en lo que refiere a los cinco programas que componen la Práctica Gestión del Programa de Confiabilidad y su cumplimiento.

Práctica Gestión de Riesgos

La evaluación de esta práctica debe considerar, al menos, los siguientes aspectos: La gestión de riesgos debe ser un proceso continuo.

Comprender claramente el uso de cada componente del sistema IIoT y el entorno de acción.

Disponer de una política general y de políticas específicas de gestión de riesgos.

Disponer de un procedimiento general y de procedimientos específicos de gestión de riesgos.

Contar con un plan en marcha de evaluación de riesgos, tanto cualitativo como cuantitativo, técnico y procedural, que considere las interdependencias entre los ambientes y sistemas IT y OT.

Disponer de una categorización de los riesgos identificados.

Definir el tratamiento a realizar a cada riesgo identificado.

Implementar los controles identificados como más adecuados para manejar los riesgos.

Integrar la gestión de riesgos con otros procesos de la organización, como ser gestión de cambios, gestión de incidentes y la gestión de vulnerabilidades.

Implementar dos estrategias combinadas de abordaje para la gestión de riesgos: top-down y *botton-up*, lo que como ya se mencionó se conoce como *middle-out*. La primera estrategia es desde la perspectiva del negocio y la segunda es desde la perspectiva de las personas y los activos, intrínsecamente más granular que la primera.

Considerar otras partes interesadas en la gestión de riesgos: proveedores, contratistas, vendendores, para promover que la confianza permee en todos los actores.

Práctica Gestión de Amenazas

La evaluación de esta práctica debe considerar, al menos, los siguientes aspectos: Plan en marcha para identificar amenazas, que considere las interdependencias entre los ambientes y sistemas IT y OT.

Acceso a diferentes fuentes de información de amenazas considerando como

posibles objetivos tanto a los sistemas y sus componentes, como también a las personas.
Sistema de *Threat Intelligence* implantado y en uso en la organización.
Análisis del impacto en caso de materializarse las amenazas.

Práctica Gestión de la Cadena de Suministros
La evaluación de esta práctica debe considerar, al menos, los siguientes aspectos: Se dispone de una política y un procedimiento que sustenta los requerimientos, a ser considerados como parte de la evaluación de los contratistas y proveedores, en cuanto a las características de la confiabilidad, antes del establecer algún vínculo con ellos.
Las características de la confiabilidad están consideradas en los vínculos, formales e informales, con los contratistas y proveedores.
Antes del comienzo del vínculo con un contratista o proveedor, se formaliza el vínculo mediante un contrato que, además de las condiciones que regirán la cooperación, se contemplan cuestiones como Acuerdo de Nivel de Servicio (SLA, por su sigla en inglés) y Acuerdo de Confidencialidad (NDA, por su sigla en inglés); este último se podría extrapolar a Acuerdo de Confiabilidad (TDA, por su sigla en inglés).
Se dispone de herramientas y procesos documentados para el monitorizado de toda la cadena de suministros (*end-to-end*), en un contexto de demandas dinámicas, que permiten detectar en tiempo real situaciones anómalas o no deseadas, y reaccionar a ello con eficiencia y eficacia.
Existen identificadores únicos para todos los elementos que integran la cadena de suministro, sin lugar a ambigüedades, e incluso identificadores "vivos" (*live labels*) durante el ciclo de vida del producto o de los componentes del sistema.
Se cuenta con una gestión en tiempo real de la demanda y un inventario optimizado.
Se dispone de los mecanismos de comunicación con otras organizaciones del sector, proveedores, contratistas y clientes o usuarios, para el intercambio de información vinculada a las características de la confiabilidad.

Práctica Gestión de los Servicios de Terceras Partes
La evaluación de esta práctica debe considerar, al menos, los siguientes aspectos: Se dispone de una política y un procedimiento que sustenta los requerimientos a ser considerados como parte de la evaluación de los *partners* y otras

terceras partes, en cuanto a las características de la confiabilidad, antes del establecer algún vínculo con ellos.
Las características de la confiabilidad están consideradas en los vínculos, formales e informales, con los *partners* y otras terceras partes.
Antes del comienzo del vínculo con un *partner* u otra tercera parte, se formaliza el vínculo con un contrato que, además de las condiciones que regirán la cooperación, se contemplan cuestiones como Acuerdo de Nivel de Servicio (SLA, por su sigla en inglés) y Acuerdo de Confidencialidad (NDA, por su sigla en inglés); este último se podría extrapolar a Acuerdo de Confiabilidad (TDA, por su sigla en inglés).
Se dispone de un plan en marcha, basado en políticas, procedimientos y documentos de gestión, que contempla los controles de acceso (físico o virtual) de *partners* y terceras partes al sistema o componentes, el plan de actividad previamente acordado, el registro de la actividad, el manejo de imprevistos, las ventanas de trabajo, la disponibilidad y condiciones de acceso, y las acciones permitidas.
Se aplica el principio de mínimo privilegio para todos los accesos.

Práctica Medidas

La organización implementa la estrategia que contempla *TA-vector* y *TT-vector* de acuerdo a lo mencionado en 2.5.2, en particular, para el caso de esta práctica, la obtención de los *TA-vector* que fueron definidos en el marco de un proceso de medición, revisado y mejorado, de todo lo relevante respecto a la confiabilidad.

Práctica Métricas e Indicadores

La organización implementa la estrategia que contempla *TA-vector* y *TT-vector* de acuerdo a lo mencionado en 2.5.2, en particular, para el caso de esta práctica, la obtención de los *TT-vector* que fueron definidos en el marco de un proceso, revisado y mejorado, de generación sistemática de todas las métricas y KPIs relevantes para la confiabilidad, mediante el uso de herramientas IT/OT
Los KPIs seleccionados son aquellos que proporcionan a los ejecutivos información significativa para la toma de decisiones
A los efectos de la selección de los KPIs, se referencian las siguientes fuentes y consideraciones:

- Los KPIs del Índice SIRI, documentados en la sección 4.7.6

- Los KPIs referidos en la Figura 4.1
- Los KPIs al menos deben contemplar:
  - La Satisfacción del Cliente o Usuario
  - La Calidad de los Procesos
  - La Satisfacción de los empleados
  - El Rendimiento Funcional
- Los KPIs relevantes según la vertical en consideración
- La cantidad adecuada de KPIs es aquella que no abruma en volumen de información a ser considerada por los ejecutivos para la toma de las decisiones estratégicas y a su vez, considera todos los aspectos importantes del negocio

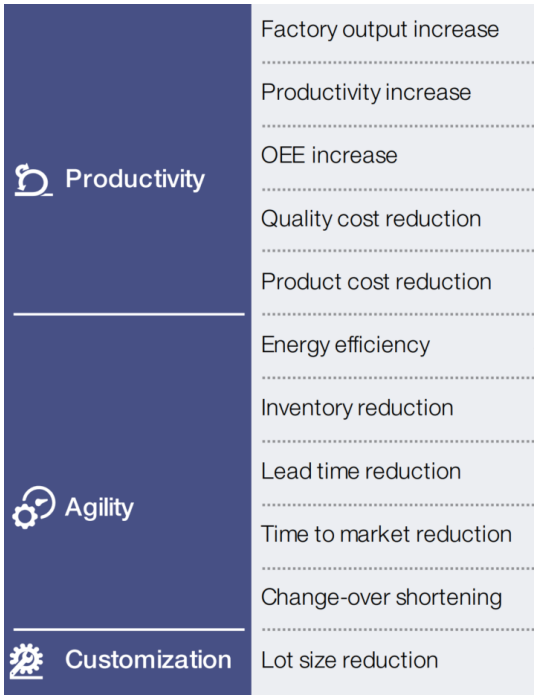


Figura 4.1: Ejemplos de KPIs del *World Economic Forum*. Fuente [287]

Práctica Identificación e Impacto Interno

La organización, mediante una metodología formal, ha identificado su perfil actual de cultura organizacional [201].

La organización, mediante una metodología formal, ha identificado el impacto interno de su perfil actual de cultura organizacional.

La organización, mediante una metodología formal, y considerando el impacto

interno y externo de su cultura organizacional actual, ha identificado su perfil deseado de cultura organizacional.
La organización, mediante una metodología formal, ha identificado las acciones para alcanzar su perfil deseado de cultura organizacional.
La organización, mediante un plan formal, trabaja con todo su *staff*, y con las estrategias adecuadas en cada caso, para, por un lado, afianzar las fortalezas de su cultura organizacional, y por otro para combatir las debilidades.

Práctica Impacto Externo

La organización, mediante un método formal, ha identificado el impacto externo de su perfil actual de cultura organizacional.
La organización, mediante un plan formal, difunde externamente y con las estrategias adecuadas, las fortalezas de su cultura organizacional actual y las mejoras a sus debilidades actuales, incluso contemplando el "viaje" hacia la cultura organizacional deseada, donde eventualmente involucra a las partes externas en el proceso.

Práctica Desarrollo

Existe en la organización un plan de desarrollo del conocimiento, revisado y actualizado periódicamente, que incentiva, facilita y premia la realización de actividades de Concientización, Sensibilización, Capacitación y Educación, que signifiquen una superación personal, profesional y de la organización.
Existe también un plan de desarrollo de habilidades blandas, revisado y actualizado periódicamente, que incentiva, facilita y premia la realización de actividades vinculadas al fortalecimiento de las habilidades blandas del *staff*, que signifiquen una superación personal, profesional y de la organización.
Ambos planes contemplan los roles y las responsabilidades actuales y próximas de los diferentes integrantes del *staff*. Ambos planes contemplan las cinco características de la confiabilidad.
Ambos planes contemplan los conceptos fundamentales de la Industria 4.0.
La organización cuenta con un plan de *networking* con las diferentes partes interesadas externas (otras empresas del sector, proveedores, contratistas, socios, clientes, usuarios, organizaciones relevantes nacionales e internacionales) para fomentar el desarrollo del conocimiento y de habilidades blandas.

Práctica Gestión del Capital Humano

Existe en la organización un plan de evaluación por competencias, revisado y actualizado periódicamente, que evalúa a cada integrante del *staff* en función de las competencias asociadas a su formación, su rol y las actividades de desarrollo en las que ha participado, y donde se registran las fortalezas y oportunidades de mejora, para la toma de diferentes acciones, entre ellas, la instancia de devolución a la persona.

Existe también un plan de captación y retención de talentos, revisado y actualizado periódicamente donde, por un lado se identifican aquellas personas que pueden incorporarse al *staff* y ofrecer un diferencial en la organización, y por otro lado se realiza un seguimiento permanente del *staff* de la organización y se brindan diversos canales de comunicación, a través de los cuales se puedan identificar de manera temprana, disconformidades o necesidades que pueden desencadenar el abandono de la organización; esto con el objetivo de determinar, si corresponde, la estrategia a seguir para intentar impedirlo.

Ambos planes contemplan las cinco características de la confiabilidad.

Ambos planes contemplan los conceptos fundamentales de la Industria 4.0.

Cualquier integrante del *staff*, antes de asumir algún rol o responsabilidad, dispone de las competencias necesarias para llevarlo adelante adecuadamente.

La organización cuenta con un plan de *networking* con las diferentes partes interesadas (otras empresas del sector, proveedores, contratistas, socios, clientes, usuarios, organizaciones relevantes nacionales e internacionales) para mejorar el plan de evaluación de competencias y el plan de captación y retención de talentos.

Ambos planes contemplan también las diferentes generaciones de trabajadores y lo que resulta más relevante, en general, para cada una de ellas. A continuación se brinda como referencia una enumeración no taxativa de dichas generaciones: Generación Z, Millenials, Generación X y *Boomers*.

Práctica Aprendizaje

La organización dispone de un plan de aprendizaje mediante un proceso que fomenta a los integrantes del *staff* a incursionar en actividades, formales e informales, donde se incentiva el desarrollo de dicho potencial, e incluso a incorporar los paradigmas de "aprender a aprender", "aprender a desaprender" y "aprender y desaprender toda la vida".

Práctica Mejora Continua

La organización dispone de un plan de mejora continua, tanto en lo técnico como en lo humano [43], que le permite a los integrantes del *staff*, con la asistencia de las herramientas adecuadas, determinar mejoras necesarias y factibles a, productos ya en poder de los usuarios (parches, actualizaciones) así como también para producir nuevas versiones de dichos productos, o desarrollar otros tipos de productos, a partir de las lecciones aprendidas, las demandas de los clientes, el estado del arte, la identificación de nuevas líneas de negocios, entre otros.

Práctica Gestión de Identidades

Esta práctica ayuda a identificar y establecer restricciones respecto a qué entidades tienen acceso a qué sistemas y con qué privilegios.

Considerar el acceso a cada uno de los sistemas, contemplando además que dichos sistemas pueden ser la conjunción de diferentes componentes embebidos, cada uno con sus capacidades y restricciones.

Revisar periódicamente los derechos de acceso de cada una de las entidades a cada uno de los sistemas (y sus componentes) y, al requerirse, terminarlos tan pronto como sea posible; algunos posibles casos que requieren terminar algún derecho de acceso son: en el caso de empleados, después del cambio de rol o al no pertenecer más a la empresa o ante investigaciones administrativas o legales en las que estuviese implicado; en el caso de otras partes interesadas, ante la culminación del vínculo formal o cambios en el mismo y, en el caso de otras entidades, ante su cambio de rol, nuevas definiciones o modificaciones. En algunos casos las terminaciones puede llegar a requerirse que se ejecuten antes que ocurra el cambio que las motiva.

Considerar los roles y responsabilidades de las personas integrantes de los equipos de respuesta a incidentes de confiabilidad, tanto en el mundo IT como en el mundo OT, de los sistemas utilizados por dichos equipos, y los privilegios de accesos a los sistemas de la organización.

Considerar los roles y responsabilidades de las personas encargadas de la seguridad física.

Considerar la gestión de identidades directamente relacionadas con los accesos físicos a las diferentes áreas de la organización.

Práctica Control de Acceso

La implementación de la práctica de control de acceso permite a una empresa limitar el acceso a los recursos solo a las identidades específicas que requieren acceso, y solo en el nivel específico necesario para cumplir los requisitos de la organización.

Se controla el acceso remoto segregado a los sistemas estrictamente necesarios, con los mínimos privilegios que se requieran, y definiendo condiciones previas al acceso, durante y después, que permitan el monitorizado de lo que se está realizando y la trazabilidad de todas las acciones que tuvieron lugar. Se debe asegurar que en todo momento está identificada de manera unívoca la entidad que accede. Los accesos remotos deberían estar, por defecto, deshabilitados.

Todos los sistemas (y componentes) cuentan con al menos un nivel mínimo de autenticación acorde a su rol y relevancia en la organización.

Se considera que los accesos con ciertos privilegios a determinados sistemas (y componentes) pueden llegar a ser habilitadores del acceso a otros sistemas (o componentes) lo que podría no ser conveniente, o no sería contemplado si se analizara este último sistema por sí solo.

Se implementan sistemas de autenticación de múltiples factores en los sistemas (y componentes) que lo permiten.

No existen contraseñas por defecto en ningún sistema (o componente) de la organización.

Se dispone de una política de contraseñas de acceso a los diferentes sistemas (y componentes) que contempla, al menos: fortaleza, complejidad, cambio periódico, histórico y recuperación.

Siempre se aplica el principio del menor privilegio al momento de otorgar privilegios a los usuarios y a las entidades.

Existe una adecuada definición de roles y responsabilidades, con los privilegios de acceso convenientemente definidos y aprobados.

No existen usuarios genéricos compartidos. En caso de ser necesario por restricciones de la tecnología involucrada, se complementa la autenticación con controles compensatorios adicionales que permite identificar unívocamente la entidad involucrada.

Se implementan mecanismos de bloqueos ante determinada cantidad de intentos de acceso fallidos, discriminando por sistemas (y componentes), y se implementan las alertas correspondientes.

Se implementan mecanismos de control de acceso físico a las diferentes áreas,

y las alertas correspondientes en caso de intentos fallidos.

Práctica de Gestión de Configuración y Cambios en los Activos
Establece los tipos de cambios permitidos, cuándo y en qué condiciones se pueden realizar los mismos, los procesos de aprobación y cómo controlar los escenarios de cambios de emergencia.
Se dispone de una herramienta que permite gestionar los activos de la organización.
La herramienta de gestión de activos permite realizar descubrimiento y actualización dinámica, identificando las características principales y particulares de los activos.
Se cuenta con un inventario actualizado, completo y consistente de los activos físicos y digitales de la organización, así como la criticidad de los mismos.
El inventario identifica, para cada activo, el dueño y el custodio, lo cual es conocido por ellos, así como también las responsabilidades asociadas. El inventario permite registrar un histórico de situaciones relevantes para cada activo.
Se mantiene un repositorio actualizado y completo con versiones de software, firmware y sistemas operativos de los sistemas (y componentes), vinculado con el inventario.
La administración de los sistemas (y componentes) se realiza a través de canales de comunicación seguros.
La gestión de los sistemas (y componentes) se realiza a través de una red dedicada exclusivamente a ello, a la que también se conectan los sistemas utilizados para dicha gestión.
Se dispone de una política y un procedimiento de Gestión de Cambios de Activos, que contempla altas, bajas y modificaciones de activos en la organización, en relación a los aspectos a considerar antes, durante y después de la actividad planificada, con una fuerte componente de gestión de riesgos, las autorizaciones requeridas, y la acción frente a imprevistos.
El despliegue de un nuevo sistema, o el cambio de uno ya existente, se realiza siempre de acuerdo a una política y un procedimiento de Gestión de Cambios de Activos existente.
Se dispone de una política y un procedimiento de Gestión de Cambios de Emergencia de Activos, que contempla altas, bajas y modificaciones de activos en la organización, en relación a los aspectos a considerar antes, durante y después de la actividad planificada, las autorizaciones requeridas y la acción frente a

imprevistos.
Los cambios de emergencia se realizan siempre de acuerdo a la política y el procedimiento de Gestión de Cambios de Emergencia de Activos existente.
Se dispone de un mecanismo (sustentado en una o más herramientas) para la gestión de las configuraciones de los sistemas (y componentes) para realizar el seguimiento de los cambios y que permite volver al estado previo.
Se dispone para cada sistema (y componentes) de una estrategia de *hardening* proporcionada por el proveedor/fabricante/representante o en su defecto elaborada por terceras partes o por la propia organización, debidamente actualizada, que se aplica en todo momento.
Existe un plan de respaldos aprobado y en marcha, sustentando en una política y en un procedimiento, que se revisa periódicamente.
El plan de respaldos se adecua a los diferentes tipos de sistemas (y componentes), en lo que refiere a medio de almacenamiento, lugar, frecuencia y tipo de respaldo.
El plan de respaldos está en sintonía con las prioridades del negocio, y se prueba respetando lo preestablecido, y actuando en función de los resultados de las pruebas.
Toda actualización de software o firmware es precedida de un chequeo de integridad del código exitoso, y su obtención se realiza por un canal seguro y desde una fuente confiable.
Toda actualización de software o firmware es precedida de su testeo exitoso en un ambiente controlado que represente lo más fielmente posible las condiciones reales.
Las actualizaciones automáticas son realizadas previa validación mediante un análisis de riesgos.
Las actualizaciones que son realizadas por terceras partes se rigen por las mismas condiciones que aquellas que son realizadas por la organización. Para aquellos sistemas o componentes en los que no es posible realizar actualizaciones, se identifican medidas compensatorias tendientes a mitigar los problemas que se podrían presentar.
Para aquellos sistemas o componentes en los que no es posible realizar actualizaciones y con medidas compensatorias, se realiza un análisis de riesgos con el objetivo de identificar cómo gestionarlos.

Práctica Protección Física

Aborda la seguridad física de las instalaciones y el *safety* vinculado, considerando los sistemas (y componentes), las personas y el medioambiente, para prevenir robos y garantizar el funcionamiento seguro y en las condiciones esperadas de los equipos.

Se dispone de los controles de acceso físico a las diferentes áreas, con los mecanismos más adecuados para cada caso.

Se dispone de los mecanismos de monitorizado/supervisión/alertas/alarmas en caso de actitudes sospechosas o de incidentes vinculados a accesos físicos, fomentando siempre la proactividad o en su defecto la reactividad temprana.

Se dispone de un plan en marcha de seguridad física y *safety* para las áreas físicas, sustentado en, al menos, una política y un procedimiento.

Todas las áreas físicas disponen de las medidas de seguridad y de *safety* acordes a la normativa vigente y aplicable, en función de los activos que se encuentran en ellas y de las mejores prácticas al respecto.

Todas las personas, previo al acceso a cualquier área, han explicitado que conocen y entienden todas las condiciones necesarias vinculadas a la seguridad física y el *safety* para la circulación o permanencia en la misma, y las consecuencias de no hacerlo.

Todas las personas respetan en todo momento durante la circulación o permanencia en un área, las condiciones para poder hacerlo.

Ningún sistema (o componente) se incorpora a la organización sin que previamente se conozcan de manera completa, y se comprendan sin lugar a dudas, las condiciones de operación que se recomiendan en cuanto a seguridad física y *safety*.

Durante todo el ciclo de vida de un sistema (o componentes) se evalúan las condiciones de seguridad física y *safety*, tanto en momentos de operación así como también en instancias de mantenimiento.

Ningún sistema (o componente) se pone en situación de disposición final sin antes asegurarse que se respetan todas las condiciones al respecto de seguridad física y *safety*.

El diseño de las redes de datos, tanto de IT como de OT, contemplan las mejores prácticas respecto a: topología jerárquica, zonas, segmentación, microsegmentación, aislamiento de redes, tratamiento de flujos de tráfico, filtrado, uso de protocolos conocidos y probados, con prestaciones de seguridad y sustentados en estándares y recomendaciones de la comunidad y, separación de

tráficos de datos, control y gestión.

Práctica Modelo y Política de Seguridad de los Datos
Identifica las diferentes categorías de datos que existen y considera los objetivos específicos de seguridad y las reglas para la protección de los datos en cada una de ellas. Se contemplan los datos en todo su ciclo de vida y en los diferentes estados que pueden ser encontrados: en reposo, en tránsito o en uso. Se contemplan los datos considerando también el ámbito de uso: negocio, IT, OT, etc. Se tienen en consideración las leyes, regulaciones, normas, estándares y mejores prácticas aplicables y que correspondan al ámbito en el que se debe dotar de seguridad a los datos. Se dispone de un Modelo de Política de Seguridad de los Datos con el cual están alineadas todas las políticas vinculadas.

Práctica Controles de Protección de Datos
Describe los mecanismos adecuados para la protección de las diferentes categorías de datos, en cuanto a confidencialidad, integridad y disponibilidad.
Se dispone de una política y un procedimiento, para la protección de los datos en reposo, volátiles y no volátiles (DAR).
Se dispone de una política y un procedimiento para la protección de los datos en tránsito (DIM).
Se dispone de una política y un procedimiento, para la protección de los datos en uso (DIU).
Los datos son categorizados (a partir de un análisis de riesgos) según el nivel su nivel de criticidad y en función de ello se definen las medidas de seguridad con los cuales protegerlos de manera de alcanzar el nivel de seguridad requerido.
El acceso de terceras partes a los datos requeridos siempre se hace considerando los principios de mínimo privilegio y de necesidad de saber.
El procesamiento de la información personal es anonimizada.
Una referencia al respecto se puede encontrar en [101].

Práctica Análisis
Se dispone de un plan de análisis de productos cuyos resultados se aplican durante el proceso de definición y diseño.
En el plan de análisis se consideran, al menos, los siguientes aspectos:
Se identifican los requisitos obligatorios que debe cumplir el producto, fundamentalmente determinados por exigencias regulatorias, normas, leyes naciona-

les e internacionales y condiciones de ingreso al mercado.
Se identifican los requisitos deseables que debería cumplir el producto, fundamentalmente determinados por el negocio y por la demanda (oculta o no) de los potenciales clientes.
Se analiza la factibilidad de cumplir con cada uno de los requisitos obligatorios y deseables, tanto desde la óptica de los costos involucrados (aspectos financieros y económicos), por la eventual necesidad de ajustes o incorporaciones tecnológicas, necesidades de formación del personal o cambios en los procesos, así como también de los tiempos que insumiría cumplir con ellos, y el impacto en el negocio (asociado al TTM).
El análisis contempla también cuál sería el impacto de retrasar el cumplimiento de algún requisito, incluso considerando en qué momento del tiempo de vida del producto se planifica cumplirlo y qué tan complejo resultará en esa circunstancia poner en marcha la configuración para su cumplimiento. La complejidad puede estar asociada a aspectos, por ejemplo como: tiempos y costos involucrados, afectación de alguna funcionalidad del dispositivo durante la configuración y la potencial molestia para el cliente durante el proceso.
El análisis considera también como premisa de trabajo que el producto debe salir al mercado bien "desde el inicio", sin la necesidad ya identificada que a corto o mediano plazo se deba realizar una readecuación del mismo.
Se dispone de un plan de análisis para los sistemas cuyos resultados se aplican durante todo el proceso de desarrollo y diseño, o adecuación de uno existente, que será utilizado para la elaboración de un producto o para su monitorizado y gestión durante su ciclo de vida.
En el plan de análisis se consideran, al menos, los mismos aspectos mencionados en el plan de análisis de productos, adaptados a sistemas.

Práctica Diseño

Se dispone de un plan de diseño de productos que se aplica durante todo el proceso de definición y diseño de un producto, y que toma como insumo los resultados del plan de análisis asociado.
En el plan de diseño se toman en cuenta, al menos, los siguientes aspectos:
Para el diseño se consideran cada uno de los resultados obtenidos en el plan de análisis asociado.
Se analiza en conjunto con quienes participaron en el plan de análisis asociado, todo potencial o real incumplimiento de los resultados del plan de análisis y

se decide cómo seguir.
Se dispone de un plan de diseño de sistema que se aplica durante todo el proceso de desarrollo y diseño de un sistema, o adecuación de uno existente, que será utilizado para la elaboración de un producto o para su monitorizado y gestión durante su ciclo de vida, y que toma como insumo los resultados del plan de análisis asociado.

Práctica de Gestión de Parches
La práctica clarifica cuándo y con qué frecuencia aplicar los parches de software y firmware, establece procedimientos a seguir con parches de emergencia y propone mitigaciones adicionales en el caso de acceso restringido al sistema u otros problemas relacionados con la aplicación de los parches.
Se dispone de una política y un procedimiento de Gestión de Parches, que reúne los aspectos a considerar antes, durante y después de la actividad de aplicación de un parche, con una fuerte componente de gestión de riesgos, las autorizaciones requeridas, y la acción frente a imprevistos.
Se dispone de una política y un procedimiento de Gestión de Parches de Emergencia, respecto a los aspectos a considerar antes, durante y después de la aplicación del parche, las autorizaciones requeridas y la acción frente a imprevistos.
Se dispone de un mecanismo (sustentado en una o más herramientas) para la gestión de las configuraciones de los sistemas (y componentes) para realizar el seguimiento de los parches aplicados y que permite volver al estado previo a la aplicación.
Toda instalación de parches es precedida de un chequeo de integridad exitoso del código, y su obtención se realiza por un canal seguro y desde una fuente confiable.
Toda instalación de parches es precedida de su testeo exitoso en un ambiente controlado que represente lo más fielmente posible a las condiciones reales.
Las instalaciones automáticas de parches son realizadas previa validación mediante un análisis de riesgos.
Las instalaciones que son realizadas por terceras partes se rigen por las mismas condiciones que aquellas realizadas por la organización.
Para aquellos sistemas o componentes en los que no es posible realizar instalaciones de parches, se identifican medidas compensatorias tendientes a mitigar los problemas que se podrían presentar.

Para aquellos sistemas o componentes en los que no es posible realizar instalaciones de parches y con medidas compensatorias, se realiza un análisis de riesgos con el objetivo de identificar cómo gestionarlos.

Práctica de Gestión de Vulnerabilidades

Esta práctica ayuda a identificar vulnerabilidades, determinar el riesgo en que cada vulnerabilidad pone a la organización y desarrollar un plan de corrección priorizado.

Se dispone y está en marcha un proceso de gestión de vulnerabilidades sustentando en herramientas de escaneo automáticas y manuales, para su identificación.

La tarea de identificación de vulnerabilidades se acompaña por la revisión periódica de las fuentes de difusión de vulnerabilidades de los activos de la organización.

Las herramientas automáticas, antes de su uso, fueron analizadas a los efectos de evaluar el riesgo de afectar los procesos de producción de la organización.

Se dispone y está en marcha un proceso de priorización de vulnerabilidades, según el impacto que significaría para la organización en caso de ser explotadas.

Se dispone y está en marcha un plan de resolución de vulnerabilidades, que puede contemplar paliativos o soluciones.

Los técnicos de IT y de OT participan y colaboran activamente en los procesos de identificación y priorización de vulnerabilidades.

Las vulnerabilidades identificadas son informadas en tiempo y forma a las partes interesadas en pro de evitar que sean explotadas.

Se dispone de un programa de recompensa (*bug bounty program*) por identificación e información en tiempo y forma de vulnerabilidades identificadas, sin que dicha actividad signifique riesgo alguno para la organización y sus procesos.

Los proveedores, contratistas, socios y otras terceras partes están obligados formalmente a informar en tiempo y forma de las vulnerabilidades identificadas en los sistemas y componentes que motivan el vínculo con la organización.

Existe un plan en marcha de pruebas de penetración a realizarle a los sistemas nuevos, que considera pruebas en fábrica (FAT, por su sigla en inglés) y pruebas en planta (SAT, por su sigla en inglés).

Existe un plan en marcha de pruebas de penetración a realizarle periódicamen-

te a los sistemas ya existentes.
Existe un plan en marcha de pruebas de penetración a realizarle a los sistemas ya existentes que han sido actualizados.

Práctica Monitorizado y Auditado
La práctica de monitorizado se utiliza para supervisar el estado del sistema (y componentes) o productos, identificar anomalías y ayudar en la resolución de problemas.
Se dispone de registros (*logs*) que permiten conocer la actividades de las diferentes entidades en los diversos sistemas (y componentes) y productos.
Se dispone de una herramienta que permite la correlación de los registros de los diferentes sistemas (y componentes) y productos.
Existe un plan en marcha para el análisis periódico preestablecido de los registros y/o de los resultados de las correlaciones automáticas y manuales, con el objetivo de identificar anomalías.
Los registros se mantienen por tiempos establecidos previo a su generación.
Se realizan revisiones periódicas preestablecidas de los privilegios de acceso a los diferentes sistemas (y componentes) y productos, o ante cambios significativos.
Se realizan revisiones periódicas preestablecidas de las configuraciones de los diferentes sistemas (y componentes) y productos, o ante cambios significativos.
Se realizan monitorizados en tiempo real de los sistemas (y componentes) y productos.

Práctica Comunicación e Intercambio de Información
Esta práctica interna, entre pares de la industria y otras organizaciones con intereses similares, ayuda a todos a estar mejor preparados para responder, por ejemplo a las amenazas. Compartir información sobre amenazas, vulnerabilidades, mejores prácticas, colabora para mantener los sistemas (y los componentes) y productos actualizados, reduciendo el riesgo que se materialicen las amenazas, y en caso de ocurrir, responder antes y mejor, otorgando resiliencia a los procesos de producción y al negocio.
Se dispone de una herramienta que permite la gestión de la información vinculada a la práctica.
Se dispone de un plan en marcha que realiza la difusión adecuada, a la interna de la organización, de toda aquella información vinculada a amenazas,

vulnerabilidades y mejores prácticas que pueden servir como insumo para tomar acciones de configuración en los sistemas (y componentes) y productos, y también para la formación del *staff* de la organización.
Se dispone de un plan en marcha que realiza la difusión adecuada, a la externa de la organización (partes interesadas posibles: contratistas, socios, proveedores, clientes, organismos reguladores, gobierno), de toda aquella información vinculada a amenazas, vulnerabilidades y mejores prácticas que pueden servir como insumo para tomar acciones de configuración en otros sistemas (y componentes) y productos, y también para la formación de la comunidad.
Una difusión adecuada implica contemplar, al menos, qué, cuándo, cómo y a quiénes se difunde.
Existe un plan de recepción de información desde el exterior de la organización la que puede ser un insumo para los planes de difusión a la interna de la organización y también hacia el exterior de la misma.

Práctica Gestión de Incidentes de Confiabilidad
Permite asignar para su gestión los incidentes de confiabilidad detectados, y eventualmente escalarlos, con el objetivo de responder adecuadamente.
También debe incluir un plan de comunicaciones para compartir información de manera adecuada y oportuna con las partes interesadas, así como también, establecer un plan de lecciones aprendidas para evitar que los incidentes vuelvan a ocurrir.
Se dispone y aplica de un conjunto de políticas, procedimientos, mejores prácticas y lecciones aprendidas, para la gestión de incidentes de confiabilidad.
Se dispone de un equipo de personas destinado a la gestión de incidentes de confiabilidad vinculados a IT.
Se dispone de un equipo de personas destinado a la gestión de incidentes de confiabilidad vinculados a OT.
Los equipos de gestión de incidentes de confiabilidad de IT y OT participan y colaboran activamente en la gestión de los incidentes de confiabilidad.
Se dispone de herramientas para la gestión de los incidentes de confiabilidad.
Se dispone de herramientas para detectar eventos e incidentes de confiabilidad.
Se dispone de procedimientos de gestión de incidentes de confiabilidad.
El conjunto de políticas, procedimientos, mejores prácticas y lecciones aprendidas, se revisa periódicamente con el objetivo de identificar mejoras a realizar.
Se dispone del contacto con otros equipos de gestión de incidentes de confia-

bilidad (o seguridad) y con otras organizaciones vinculadas a la temática, con las cuales poder interactuar para compartir experiencias y resolver incidentes de manera colaborativa.

Práctica Continuidad de las Operaciones

La implementación de esta práctica permite a la organización recuperarse lo antes posible de un desastre y continuar con el negocio.

Se dispone de un Plan de Recuperación de Desastres (DRP, por su sigla en inglés) aprobado y en marcha.

Se dispone de un Plan de Continuidad del Negocio (BCP, por su sigla en inglés) aprobado y en marcha.

El Plan de Recuperación de Desastres se prueba periódicamente y se ajusta en función de las lecciones aprendidas.

El Plan de Continuidad del Negocio se prueba periódicamente y se ajusta en función de las lecciones aprendidas.

Práctica Verificación

Esta práctica permite que la organización pueda realizar revisiones de un diseño a los efectos de comprobar que se está creando bien el producto, de acuerdo a los requerimientos y especificaciones consideradas. Es una práctica focalizada en el proceso de diseño y puede tener lugar en diferentes fases del mismo.

Se dispone de un proceso de verificación que considera el proyecto de diseño, compuesto por sus diferentes fases, las pruebas a realizar en cada uno, los resultados obtenidos y cómo proceder con los errores o defectos identificados.

El proceso puede ser aplicable tanto a un sistema como a cada uno de sus componentes o a un producto.

El proceso contempla tanto las consideraciones de la organización como también las del cliente.

Práctica Validación

Esta práctica permite que la organización pueda probar que se creó el producto adecuado, de acuerdo a las necesidades de la parte interesada.

Es una práctica focalizada en el producto diseñado, cuando concluye el mismo.

Se dispone de un proceso de validación donde están definidas el conjunto de pruebas a realizar al producto, con el objetivo de demostrar que fue diseñado cumpliendo con lo que el cliente quiere.

El proceso puede ser aplicable tanto a un sistema como a cada uno de sus componentes o a un producto.
El proceso contempla tanto las consideraciones de la organización como también las del cliente.

Apéndice 5

Soluciones de hardware y software para la Industria 4.0

En este Apéndice se mencionan algunas de las soluciones identificadas que pueden ser de utilidad para llevar adelante la gestión de una organización que adopta la Industria 4.0, o investigar y desarrollar en algunas de los conceptos mencionados a lo largo del documento.

El espíritu de brindar esta información es intentar dotar al trabajo de completitud, a sabiendas que este no era uno de los objetivos de la tesis, en función de lo cual se ponderó el esfuerzo destinado a este punto.

La mención de cada una de las soluciones se acompaña de una referencia que permita profundizar en sus prestaciones[1].

Las soluciones se presentan en orden alfabético.

5.1. *Administration Shell* de un Activo (AAS)

A continuación se mencionan y referencian algunas implementaciones *open source* activas en la comunidad. En todos los casos, siguen la especificación *Details of the Asset Administration Shell* [223, 224], aunque puede variar a qué versión de la misma.

[1]Las principales soluciones de *cloud* existentes contemplan siempre a IoT como parte de su negocio y por lo tanto, es una componente más de su portafolio de servicios. Las referencias aquí son aquellas que explícitamente refieren a IIoT, sin que ello implique que las restantes no puedan ser consideradas al momento de evaluar la pertinencia o no de su utilización.

5.1.1. AASX Package Explorer

AASX [78] es una herramienta *open source* impulsada por la *Plattform Industrie 4.0* y ZVEI, con la que se puede crear y editar AAS en los formatos JSON y XML.

5.1.2. BaSyx

BaSyx [52] ofrece un middleware de conectividad entre dispositivos y un SDK para el desarrollo de AAS, entre otras prestaciones. Es soportada por las empresas Bosch y Fraunhofer, además de otros colaboradores individuales.

5.1.3. i40-aas

i40-aas [250] es un desarrollo a cargo de de SAP que provee un sistema basado en Dockers que implementan RAMI 4.0, incluyendo AAS.

5.1.4. PyI40AAS

PyI40AAS [248] es una implementación en Python 3 de la AAS, desarrollado por la *RWTH Aachen University*.

5.2. BIS

Businees Integration Suite (BIS) [26], desarrollado y mantenido por Seeburger [253], es una plataforma que permite integrar las aplicaciones, procesos y transacciones de una empresa.

5.3. Bosch

En lo que refiere a la Industria 4.0, Bosch [24] ofrece diversas soluciones, siendo algunas de ellas Nexeed [23] y ctrlX AUTOMATION [246].

La familia de productos Nexeed permite gestionar de manera integrada el proceso de producción con la logística asociada, la gestión de materiales, la operativa y la productividad, entre otras funcionalidades.

CtrlX AUTOMATION, desarrollada e impulsada por Rexroth [245], tiene como objetivo hacer realidad la Fábrica del Futuro mediante una solución 360,

escalable, abierta [274] y con *performance* que permita aportar dinámica y flexibilidad a las decisiones y ofrecer la solución que mejor se adapta a los requerimientos.

5.4. Eclipse Ditto

Es un *backend* que permite la gestión de dispositivos IoT [53].

5.5. Eclipse IoT

Eclipse IoT [51] es una solución *open source* para IoT y para la Industria 4.0 [51]. A través de numerosos proyectos, con diferente nivel de madurez, Eclipse IoT ofrece implementaciones para OPC UA, MQTT, PPMP, oneM2M, desarrollos de PLCs, gateways de IoT, firmado de código, autenticación y autorización, configuración y gestión de dispositivos, actualizaciones de software, gestión de eventos, almacenamiento de datos, gestión de datos, creación y gestión de *Digital Twins*, entre otros.

5.6. ERP5

ERP5 [65] es un ERP *open-source* ERP escrito en Python. Es parte del *stack* de software desarrollado y mantenido por Nexedi [181] que también incluye a Wendelin [284] para Big Data & Machine Learning y SlapOS [261] para despliegue en la nube y orquestado.

5.7. Fiware for Industry

Fiware for Industry [70] ofrece una amplia gama de tecnologías vinculadas al despliegue, el desarrollo y la integración de soluciones para la Industria 4.0.

5.8. General Electric Digital Twin Framework

GENIX [75] es una solución en la nube que permite la creación de DT para representar un activo, un sistema integrado de activos o una flota de ellos,

pudiendo conocer su estado y sus rendimientos, aprovechando advertencias tempranas y las predicciones.

5.9. Giers 4.0

Giers 4.0 [76] es una plataforma multifuncional desarrollada por microtom [178]. Está diseñada principalmente para los fabricantes con el fin de ayudarles a gestionar eficientemente sus procesos, prevenir tiempos de inactividad imprevistos y detectar problemas o incoherencias en un proceso de orden de trabajo o en la infraestructura. También ayuda a la TI de fabricación a administrar equipos que requieren alta disponibilidad y tiempos de respuesta rápidos y, por último, pero no menos importante, combina datos empresariales con datos de producción en una interfaz fácil de usar.

5.10. Intel

Intel ofrece numerosas soluciones para la IoT Industrial y para diferentes sectores de la Industria 4.0 [136].

5.11. IMPROVE 4.0

IMPROVE [129] es una solución de software desarrollada y mantenida por NeXT [182] que puede ser aplicada en diferentes áreas de los procesos industriales, como ser: producción, mantenimiento, logísitica, seguridad, *safety*, monitorizado, automatización y control calidad.

5.12. Kaa

Kaa [164] también es una plataforma de IoT industrial, que funciona como un gestor de aplicaciones en la nube para instalaciones de producción industriales conectadas, agnóstica al hardware y al transporte, lo que le permite integrarse fácilmente con una amplia variedad de sensores, controladores, máquinas y puertas de enlace de dispositivos con el fin de soportar fácilmente cualquier infraestructura industrial existente.

5.13. Kafka

Kafka [8], desarrollado por la Apache Software Foundation [9] es una plataforma de *streaming* de eventos distribuidos de código abierto, utilizada para *data pipelines* de alto rendimiento, análisis de *streaming*, integración de datos y aplicaciones de misión crítica, que permite el procesamiento de grandes volúmenes de datos en tiempo real de una manera confiable, escalable y flexible.

5.14. Linutronix

Linuxtronix [172] es una solución desarrollada para disponer de un ambiente linux de grado industrial, considerando entre otros aspectos: seguridad, adaptación a diferentes arquitecturas, ser liviano y contemplando el requerimiento de tiempo real.

5.15. MUD

A continuación se mencionan algunas de las herramientas e implementaciones disponibles para la realización de investigaciones y despliegues basados en MUD.

5.15.1. IoT Hub

Desarrollo de una aplicación para móviles, financiado por Intel, para la gestión segura de los dispisitivos IoT instalados en el hogar [135].

5.15.2. IoT Hub

MUD Manager en fase de desarrollo, a cargo del NIST, para analizar y perfilar dispositivos IoT [191].

5.15.3. MUD Maker

Herramientas en línea provistas por Cisco (e IETF) para crear y visualizar archivos MUD [90].

5.15.4. MUD Manager

MUD Manager implementado por Cisco [39].

5.15.5. MUD tools

MUD Manager para componentes CableLabs [27].

5.15.6. MUDGEE

Herramienta desarrollada en la Universidad de Nueva Gales del Sur (Australia), para crear archivos MUD a partir de trazas de tráfico *pcap* [278].

5.15.7. Pre-certificación en seguridad de dispositivos IoT

Automatización del entorno de pruebas de seguridad de pre-certificación de IoT basado en el MUD [56].

5.15.8. Soft MUD

Se trata de la investigación del NIST acerca de cómo implementar MUD en switches SDN que soportan OpenFlow [196].

5.16. NEXCOM

El *IoT Automation Solutions* (IAS) *Business Group* de NEXCOM [180] ofrece un conjunto de soluciones para el despliegue de la Industria 4.0, comprendiendo, entre otras: automatización, robótica, conectividad e integración con diversos servicios en la nube.

5.17. Optiware

Optiware [203] ofrece soluciones de Gestión de Activos Empresariales (EAM), denominada API PRO [10], y de Efectividad General del Equipamiento (OEE), identificada como AXXOS [16].

5.18. Oracle IoT Digital Twin

Su implementación permite gestionar tres pilares: *Virtual Twin*, *Predictive Twin* y *Twin Projections* [204].

5.19. PI System

La solución PI System [210] de OsiSoft [205] (recientemente adquirida por AVEVA [15])permite integrar datos de diversas fuentes, almacenarla, procesarla e integrarla para una adecuada toma de decisiones.

5.20. SAP

SAP [249] ofrece un portafolio muy amplio de soluciones para el despliegue de la Industria 4.0. Una primera referencia al respecto se puede encontrar en [251].

5.21. Seebo

Seebo [252] está diseñado para predecir y prevenir pérdidas de producción basadas en procesos en la fabricación, utilizando la Inteligencia Artificial Basada en Procesos.

5.22. Telit

Telit ofrece diversas plataformas con diferentes funcionalidades [265], destacándose entre ellas las denominadas *deviseWISE* y *secureWISE* por estar focalizadas para ambientes IIoT.

5.23. ThingWorx

PTC ofrece *ThingWorx* [252], una plataforma de soluciones para IIoT, la que entre numerosas prestaciones, permite integrase con Microsoft Azure.

5.24. Wipro

Wipro [285] se especializa en diferentes áreas, entre ellas ciberseguridad, y ha desarrollado soluciones bajo el principio de *Security by Design* y considerando también la seguridad *chip to cloud* [286].

Lista de tablas

Lista de figuras

Bibliografía

[1] *ABB. Digital twin – a key software component of Industry 4.0.* URL: https://new.abb.com/news/detail/11242/digital-twin-a-key-software-component-of-industry-40. Última visita: nov 2020.

[2] *ACATECH. Industrie 4.0 Maturity Index – Managing the Digital Transformation of Companies.* URL: https://en.acatech.de/publication/industrie-4-0-maturity-index-managing-the-digital-transformation-of-companies/. Última visita: nov 2020.

[3] *AGESIC. Marco de Ciberseguridad.* URL: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco-ciberseguridad. Última visita: nov 2020.

[4] *AGESIC. Unidad Reguladora y de Control de Datos Personales. Guía de Protección de Datos en Salud.* URL: https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-de-proteccion-de-datos-en-salud. Última visita: nov 2020.

[5] *AGESIC. Unidad Reguladora y de Control de Datos Personales. Recomendaciones para el tratamiento de datos personales ante la situación de emergencia sanitaria nacional.* URL: https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/recomendaciones-para-tratamiento-datos-personales-ante-situacion. Última visita: nov 2020.

[6] *AII. Industrial Internet Architecture - Version 1.0.* URL: http://en.aii-alliance.org/uploadfile/2017/0309/20170309.pdf. Última visita: nov 2020.

[7] *ANSI. IEC/PAS 63088 Ed. 1.0 en:2017 - Smart Manufacturing - Reference Architecture Model Industry 4.0 (RAMI4.0).* URL: https://

webstore.ansi.org/Standards/IEC/IECPAS63088Eden2017. Última visita: nov 2020.

[8] *Apache Kafka*. URL: https://kafka.apache.org/. Última visita: nov 2020.

[9] *Apache Software Foundation*. URL: https://www.apache.org/. Última visita: nov 2020.

[10] *API PRO*. URL: https://optiware.com/products/api-pro-eam/. Última visita: nov 2020.

[11] *Asociación Uruguaya de Contabilidad y Presupuesto Públicos (ASUCYP). Ariel Rodríguez. Salud Pública en Uruguay. Evolución del Gasto Presupuestal. Estructura y Financiamiento. Período 2000-2015. Informe elaborado el año 2016*. URL: http://asucyp.org.uy/wp-content/uploads/2016/07/Presentacion-Colegio.pdf. Última visita: dic 2020.

[12] *Association of Southeast Asian Nations (ASEAN). ASEAN Declaration on Industrial Transformation to Industry 4.0*. URL: https://asean.org/asean-declaration-industrial-transformation-industry-4-0/?highlight=4.0. Última visita: nov 2020.

[13] *Australia. Industry 4.0*. URL: https://www.industry.gov.au/funding-and-incentives/industry-40. Última visita: nov 2020.

[14] *Austria. Association Industry 4.0 Austria - The Platform for Smart Production*. URL: https://plattformindustrie40.at/. Última visita: nov 2020.

[15] *AVEVA*. URL: https://www.aveva.com/en/. Última visita: nov 2020.

[16] *AXXOS*. URL: https://optiware.com/products/axxos-oee/. Última visita: nov 2020.

[17] *BD. BD Pyxis MedStation ES*. URL: https://www.bd.com/en-us/offerings/capabilities/medication-and-supply-management/medication-and-supply-management-technologies/pyxis-medication-technologies/pyxis-medstation-es-system. Última visita: dic 2020.

[18] *Bélgica. Made Different*. URL: http://www.madedifferent.be/en. Última visita: nov 2020.

[19] *Ben Purvis, Yong Mao & Darren Robinson. Three pillars of sustainability: in search of conceptual origins.* URL: https://doi.org/10.1007/s11625-018-0627-5. Última visita: nov 2020.

[20] *BioMed Central (BMC). Riikka Metsämuuronen, Hannu Kokki, Toivo Naaranlahti, Minna Kurttila & Reeta Heikkilä. Nurses´ perceptions of automated dispensing cabinets – an observational study and an online survey.* URL: https://bmcnurs.biomedcentral.com/articles/10.1186/s12912-020-00420-2. Última visita: nov 2020.

[21] *BITKOM.* URL: https://www.bitkom.org/EN. Última visita: nov 2020.

[22] *BMBF. Federal Ministry of Education and Research.* URL: https://www.bmbf.de/en/index.html. Última visita: nov 2020.

[23] *BOSH. Nexeed Industrial Application System: towards the Factory of the Future.* URL: https://www.bosch-connected-industry.com/de/en/index. Última visita: nov 2020.

[24] *BOSH. Towards a Connected Industry with Bosch.* URL: https://www.bosch.com/products-and-services/connected-products-and-services/industry-4-0/. Última visita: nov 2020.

[25] *BPS. Evolución de los cotizantes.* URL: https://www.bps.gub.uy/1940/evolucion-de-los-cotizantes.html. Última visita: nov 2020.

[26] *Business Integration Suite.* URL: https://www.seeburger.com/platform/industrial-iot-industry-4-0/. Última visita: nov 2020.

[27] *CableLabs. MUD Tools.* URL: https://github.com/cablelabs/micronets-mud-tools. Última visita: nov 2020.

[28] *Carnegie Mellon University. Software Engineering Institute - Blogs - Scoping IT & OT Together When Assessing an Organization's Resilience.* URL: https://insights.sei.cmu.edu/insider-threat/2018/11/scoping-it-ot-together-when-assessing-an-organizations-resilience.html. Última visita: nov 2020.

[29] *Carnegie Mellon University. Software Engineering Institute - Blogs - System Resilience - Parts 1 .. 7.* URL: https://insights.sei.cmu.edu/author/donald-firesmith/. Última visita: nov 2020.

[30] *CEN CENELEC. Smart grids.* URL: https://www.cencenelec.eu/standards/Sectorsold/SustainableEnergy/SmartGrids/Pages/default.aspx. Última visita: nov 2020.

[31] *CHERNOBYLWEL.COMe. La historia de Chernobyl.* URL: https://www.chernobylwel.com/es/la-historia-de-chernobil. Última visita: nov 2020.

[32] *China. Alliance of Industrial Internet.* URL: http://en.aii-alliance.org/. Última visita: nov 2020.

[33] *China. China Academy of Information and Communications Technology.* URL: http://www.caict.ac.cn/english/. Última visita: nov 2020.

[34] *China. China-Britain Business Council - Made in China 2025.* URL: http://www.cbbc.org/resources/other-cbbc-reports/made-in-china-2025/made-in-china-2025-(free-to-all)/. Última visita: nov 2020.

[35] *China. National Intelligent Manufacturing Standard System Construction Guidelines.* URL: https://www.dke.de/resource/blob/929020/7080b1667308545c088901b39a111756/manufacturing-guidelines-data.pdf. Última visita: nov 2020.

[36] *China. Standarization Administration of the P.R.C.* URL: http://www.sac.gov.cn/sacen/. Última visita: nov 2020.

[37] *CIS. Center for Internet Security.* URL: https://www.cisecurity.org/. Última visita: nov 2020.

[38] *Cisco. Manufacturer Usage Descriptions - DEVNET.* URL: https://developer.cisco.com/site/mud/. Última visita: nov 2020.

[39] *Cisco. MUD Manager.* URL: https://github.com/CiscoDevNet/MUD-Manager. Última visita: nov 2020.

[40] *Congress USA. Cybersecurity Enhancement Act of 2014 - Public Law 113–274 113th Congress.* URL: https://www.congress.gov/113/plaws/publ274/PLAW-113publ274.pdf. Última visita: nov 2020.

[41] *Corea del Sur. Ministry of Science and ICT.* URL: https://msit.go.kr/english/main/main.do. Última visita: nov 2020.

[42] *CSA. Corporate Sustainability Assessment.* URL: https://www.spglobal.com/esg/csa/. Última visita: nov 2020.

[43] *Dean Yeong. Continuous Improvement: A Simple Glance of What Lifelong Learning Really Means.* URL: https://deanyeong.com/continuous-improvement/. Última visita: nov 2020.

[44] *Débora de-Carvalho, José Luiz Alvim-Borges, Cristiana Maria Toscano. Impact assessment of an automated drug-dispensing system in a tertiary hospital.* URL: https://www.scielo.br/pdf/clin/v72n10/1807-5932-clin-72-10-629.pdf. Última visita: nov 2020.

[45] *Defense Innovation Board - USA. The Road to Zero Trust (Security).* URL: https://innovation.defense.gov/Portals/63/Templates/Updated%5C%20Meeting%5C%20Documents/DIB%5C_Zero%5C%20Trust%5C%20Whitepaper%5C_190709.pdf. Última visita: nov 2020.

[46] *Deloitte. Bersin by Deloitte.* URL: https://www2.deloitte.com/bd/en/pages/human-capital/topics/bersin-by-deloitte.html. Última visita: nov 2020.

[47] *Deloitte. Industry 4.0 and the digital twin.* URL: https://www2.deloitte.com/us/en/insights/focus/industry-4-0/digital-twin-technology-smart-factory.html. Última visita: nov 2020.

[48] *Digital Cooperation - UN. The age of digital interdependence.* URL: https://digitalcooperation.org/wp-content/uploads/2019/02/ISOC-HLPDC-contribution-Final-1.pdf. Última visita: nov 2020.

[49] *DIN. DIN SPEC 91345 - Reference Architecture Model Industrie 4.0 (RAMI4.0).* URL: https://www.din.de/en/wdc-beuth:din21:250940128. Última visita: nov 2020.

[50] *Dinamarca. MADE - Manufacturing Academy of Denmark.* URL: https://en.made.dk/. Última visita: nov 2020.

[51] *Eclipse IoT.* URL: https://iot.eclipse.org/. Última visita: nov 2020.

[52] *Eclipse. BaSyx.* URL: https://projects.eclipse.org/projects/technology.basyx. Última visita: nov 2020.

[53] *Eclipse. ditto.* URL: https://www.eclipse.org/ditto/. Última visita: nov 2020.

[54] *EDB Singapore. Singapore tops the Asian Digital Transformation Index.* URL: https://www.edb.gov.sg/en/news-and-events/insights/innovation/singapore-tops-the-asian-digital-transformation-index.html. Última visita: nov 2020.

[55] *EDB Singapore. SIRI Assessor Programme launched to scale industrial transformation.* URL: https://www.edb.gov.sg/en/news-and-events/news/siri-assessor-programme-launched-to-scale-industrial-transformation.html. Última visita: nov 2020.

[56] *Eindhoven University of Technology. Automation of IoT pre-certification security testing environment based on the Manufacturing Usage Description, Gangurde, C.A., Master Thesis.* URL: https://research.tue.nl/en/studentTheses/automation-of-iot-pre-certification-security-testing-environment-. Última visita: nov 2020.

[57] *ENISA. Baseline Security Recommendations for IoT.* URL: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot. Última visita: nov 2020.

[58] *ENISA. Cyber Security Culture in organisations.* URL: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations. Última visita: nov 2020.

[59] *ENISA. Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity.* URL: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity. Última visita: nov 2020.

[60] *ENISA. ENISA Good practices for IoT and Smart Infrastructures Tool.* URL: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool. Última visita: nov 2020.

[61] *ENISA. European Union Agency for Cybersecurity.* URL: https://www.enisa.europa.eu/. Última visita: nov 2020.

[62] *ENISA. Good Practices for Security of Internet of Things in the context of Smart Manufacturing.* URL: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot. Última visita: nov 2020.

[63] *ENISA. Industry 4.0 - Cybersecurity Challenges and Recommendations.* URL: https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations. Última visita: nov 2020.

[64] *ENISA. Internet of Things (IoT).* URL: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot. Última visita: nov 2020.

[65] *ERP5. Most Powerful Open Source ERP.* URL: https://www.erp5.com/. Última visita: nov 2020.

[66] *Eslovaquia. Industry4UM.* URL: https://industry4um.sk/. Última visita: nov 2020.

[67] *Eslovenia. Digital Coalition.* URL: https://www.digitalna.si/en. Última visita: nov 2020.

[68] *España. Industria Conectada 4.0.* URL: https://www.industriaconectada40.gob.es/. Última visita: nov 2020.

[69] *European Commission - Digital transformation monitor. National initiatives.* URL: https://ec.europa.eu/growth/tools-databases/dem/monitor/category/national-initiatives. Última visita: nov 2020.

[70] *Fiware for Industry. FIWARE Technologies enabling Industry 4.0.* URL: https://www.fiware4industry.com/. Última visita: dic 2020.

[71] *Forbes. How Can Industry 4.0 Help Manufacturers During COVID-19?* URL: https://www.forbes.com/sites/sap/2020/09/08/how-can-industry-40-help-manufacturers-during-covid-19/?sh=240a304131ea. Última visita: nov 2020.

[72] *Francia. Alliance industrie du futur.* URL: http://www.industrie-dufutur.org/. Última visita: nov 2020.

[73] *GAIA-X. A Federated Data Infrastructure for Europe.* URL: https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html. Última visita: nov 2020.

[74] *Gartner. Gartner Identifies the Top 10 Strategic Technology Trends for 2019.* URL: https://www.gartner.com/en/newsroom/press-releases/2018-10-15-gartner-identifies-the-top-10-strategic-technology-trends-for-2019. Última visita: nov 2020.

[75] *GE - General Electric. Project Digital Twin Framework.* URL: https://www.ge.com/research/project/digital-twin-framework. Última visita: nov 2020.

[76] *Gears 4.0.* URL: https://www.microtom.com/products/smart-manufacturing. Última visita: nov 2020.

[77] *Germany - The Federal Government. The High-Tech Strategy 2025.* URL: https://www.hightech-strategie.de/en/. Última visita: nov 2020.

[78] *GitHub. Relationships between I4.0 Components – Composite Components and Smart Production.* URL: https://github.com/admin-shell/aasx-package-explorer. Última visita: nov 2020.

[79] *Health Level Seven International (HL7).* URL: https://www.hl7.org/. Última visita: nov 2020.

[80] *Hungría. The Industry 4.0 National Technology Platform.* URL: https://www.i40platform.hu/en. Última visita: nov 2020.

[81] *IEC. Factory of the future.* URL: https://www.iec.ch/whitepaper/pdf/iecWP-futurefactory-LR-en.pdf. Última visita: nov 2020.

[82] *IEC. IEC 62890:2020 - Industrial-process measurement, control and automation - Life-cycle-management for systems and components.* URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/criteria-industrie-40-products.html. Última visita: nov 2020.

[83] *IETF. Architectural Considerations in Smart Object Networking.* URL: https://www.rfc-editor.org/info/rfc7452. Última visita: nov 2020.

[84] *IETF. Cryptographic Message Syntax (CMS).* URL: https://www.rfc-editor.org/info/rfc5652. Última visita: nov 2020.

[85] *IETF. Internet Engineering Task Force.* URL: https://ietf.org/. Última visita: nov 2020.

[86] *IETF. Internet of Things (IoT) Security: State of the Art and Challenges - RFC 8576.* URL: https://www.rfc-editor.org/info/rfc8576. Última visita: nov 2020.

[87] *IETF. Journal - Managing the Internet of Things – It's All About Scaling.* URL: https://www.ietfjournal.org/managing-the-internet-of-things-its-all-about-scaling/. Última visita: nov 2020.

[88] *IETF. JSON Encoding of Data Modeled with YANG.* URL: https://www.rfc-editor.org/info/rfc7951. Última visita: nov 2020.

[89] *IETF. Manufacturer Usage Description Specification.* URL: https://www.rfc-editor.org/info/rfc8520. Última visita: nov 2020.

[90] *IETF. MUD Maker.* URL: https://www.mudmaker.org/. Última visita: nov 2020.

[91] *IETF. Secure IoT Bootstrapping: A Survey - draft-sarikaya-t2trg-sbootstrapping-09.* URL: https://tools.ietf.org/html/draft-sarikaya-t2trg-sbootstrapping-09. Última visita: nov 2020.

[92] *IETF. The JavaScript Object Notation (JSON) Data Interchange Format.* URL: https://www.rfc-editor.org/info/rfc8259. Última visita: nov 2020.

[93] *IETF. The YANG 1.1 Data Modeling Language.* URL: https://www.rfc-editor.org/info/rfc7950. Última visita: nov 2020.

[94] *IETF. YANG Data Model for Network Access Control Lists (ACLs).* URL: https://www.rfc-editor.org/info/rfc8519. Última visita: nov 2020.

[95] *IIC & IoT Alliance Australia. How Digital Transformation and IoT Can Contribute to the UN Sustainable Development Goals.* URL: https://www.iotaustralia.org.au/2020/06/23/iotnewsglobal/iotaa-iic-white-paper-pushes-iot-for-sustainability/. Última visita: dic 2020.

[96] *IIC & Plattform Industrie 4.0. Architecture Alignment and Interoperability.* URL: https://www.iiconsortium.org/press-room/02-06-18.htm. Última visita: nov 2020.

[97] *IIC & Plattform Industrie 4.0. Digital Twin and Asset Administration Shell Concepts and Application in the Industrial Internet and Industrie 4.0.* URL: https://www.iiconsortium.org/pdf/Digital-Twin-and-Asset-Administration-Shell-Concepts-and-Application-Joint-Whitepaper.pdf. Última visita: dic 2020.

[98] *IIC. A Short Introduction to Digital Twins.* URL: https://www.iiconsortium.org/news/joi-articles/2019-November-JoI-A-Short-Introduction-to-Digital-Twins.pdf. Última visita: nov 2020.

[99] *IIC. COVID-19: Industry Impact and Response.* URL: https://www.iiconsortium.org/coronavirus-industry-impact.htm. Última visita: dic 2020.

[100] *IIC. Cybersecurity Considerations for Digital Twin Implementations.* URL: https://www.iiconsortium.org/news/joi-articles/2019-November-JoI-Cybersecurity-Considerations-for-Digital-Twin-Implementations.pdf. Última visita: nov 2020.

[101] *IIC. Data Protection Best Practices White Paper.* URL: https://www.iiconsortium.org/press-room/07-22-19.htm. Última visita: nov 2020.

[102] *IIC. Digital Transformation.* URL: https://www.iiconsortium.org/digital-transformation/. Última visita: nov 2020.

[103] *IIC. Digital Transformation in Industry White Paper.* URL: https://www.iiconsortium.org/pdf/Digital%5C_Transformation%5C_in%5C_Industry%5C_Whitepaper%5C_2020-07-23.pdf. Última visita: dic 2020.

[104] *IIC. Digital Twin Architecture and Standards.* URL: https://www.iiconsortium.org/news/joi-articles/2019-November-JoI-Digital-Twin-Architecture-and-Standards.pdf. Última visita: nov 2020.

[105] *IIC. Distributed Ledgers in IIoT.* URL: https://www.iiconsortium.org/pdf/Distributed%5C_Ledgers%5C_in%5C_IIoT%5C_White%5C_Paper%5C_2020-07-22.pdf. Última visita: dic 2020.

[106] *IIC. Endpoint Security Best Practices.* URL: https://www.iiconsortium.org/press-room/03-12-18.htm. Última visita: nov 2020.

[107] *IIC. Extending the IIC IoT Security Maturity Model to Trustworthiness.* URL: https://www.iiconsortium.org/news/joi-articles/2018-Sept-JoI-Extending-the-IIC-Security-Maturity-Model-to-Trustworthiness.pdf. Última visita: nov 2020.

[108] *IIC. IIC Overview.* URL: https://www.iiconsortium.org/pdf/IIC-one-pager-2020-01-24.pdf. Última visita: nov 2020.

[109] *IIC. IIoT Connectivity Framework.* URL: https://www.iiconsortium.org/IICF.htm. Última visita: nov 2020.

[110] *IIC. Industrial Internet Reference Architecture.* URL: https://www.iiconsortium.org/IIRA.htm. Última visita: nov 2020.

[111] *IIC. Industrial Internet Security Framework.* URL: https://www.iiconsortium.org/IISF.htm. Última visita: nov 2020.

[112] *IIC. Industry Leadership Council.* URL: https://www.iiconsortium.org/industry-leadership-councils.htm. Última visita: nov 2020.

[113] *IIC. IoT Security Maturity Model: Practitioner´s Guide.* URL: https://www.iiconsortium.org/smm.htm. Última visita: nov 2020.

[114] *IIC. Journal of Innovation - November 2019 - The Road to Digital Transformation.* URL: https://www.iiconsortium.org/news/joi-articles/2019-November-JoI-Whats-New-at-the-IIC.pdf. Última visita: nov 2020.

[115] *IIC. Journal of Innovation - November 2020 - IOT Enabling Rapid Response to COVID and Future Pandemics.* URL: https://www.iiconsortium.org/press-room/11-17-20.htm. Última visita: dic 2020.

[116] *IIC. Journal of Innovation - September 2017.* URL: https://www.iiconsortium.org/news/journal-of-innovation-2017-sept.htm. Última visita: nov 2020.

[117] *IIC. Journal of Innovation: September 2018.* URL: https://www.iiconsortium.org/news/journal-of-innovation-2018-sept.htm. Última visita: nov 2020.

[118] *IIC. Journal of Innovation: September 2018 - Trustworthiness in Industrial System Design.* URL: https://www.iiconsortium.org/news/joi-articles/2018-Sept-JoI-Trustworthiness-in-System-Design-Wibu-Systems.pdf. Última visita: nov 2020.

[119] *IIC. Liaisons.* URL: https://www.iiconsortium.org/liaisons.htm. Última visita: nov 2020.

[120] *IIC. Managing and Assessing Trustworthiness for IIoT in Practice.* URL: https://www.iiconsortium.org/press-room/07-29-19.htm. Última visita: nov 2020.

[121] *IIC. Press Release - IIC IoT Security Maturity Model: Description and Intended Use.* URL: https://www.iiconsortium.org/press-room/04-09-18.htm. Última visita: nov 2020.

[122] *IIC. Shades of Digital Twinning.* URL: https://www.iiconsortium.org/news/joi-articles/2019-November-JoI-Shades-of-Digital-Twinning.pdf. Última visita: nov 2020.

[123] *IIC. Steering Committee.* URL: https://www.iiconsortium.org/steering-committee-overview.htm. Última visita: nov 2020.

[124] *IIC. Testbed - Factory Operations Visibility & Intelligence (FOVI).* URL: https://hub.iiconsortium.org/fovi. Última visita: nov 2020.

[125] *IIC. The Industrial Internet of Things Volume G2: Key System Concerns.* URL: https://www.iiconsortium.org/pdf/Industrial_Internet_of_Things_Volume_G2-Key_System_Concerns_2018_08_07.pdf. Última visita: nov 2020.

[126] *IIC. Using Metrics in the Industrial IoT Data Value Chain to Drive Trustworthiness.* URL: https://www.iiconsortium.org/news/joi-articles/2018-Sept-Trustworthiness-Metrics-Value-Chain-FujitsuNokia.pdf. Última visita: nov 2020.

[127] *IIC. Working Groups.* URL: https://www.iiconsortium.org/working-committees.htm. Última visita: nov 2020.

[128] *IMPO. Decreto N° 504/2007.* URL: https://www.impo.com.uy/bases/decretos/504-2007/. Última visita: nov 2020.

[129] *IMPROVE 4.0.* URL: https://mynext.it/industry-4-0/?lang=en. Última visita: nov 2020.

[130] *India. Department for Promotion of Industry and Internal Trade.* URL: https://dipp.gov.in/. Última visita: nov 2020.

[131] *India. SAMARTH Udyog Bharat 4.0 - A Industry 4.0 initiative of DHI, Ministry of HI & PE, Government of India.* URL: https://www.samarthudyog-i40.in/. Última visita: nov 2020.

[132] *Indonesia. Dokumen Peta Jalan Making Indonesia 4.0.* URL: https://kemenperin.go.id/. Última visita: nov 2020.

[133] *Institute for Safe Medication Practices (ISMP). Guidelines for the Safe Use of Automated Dispensing Cabinets.* URL: https://www.ismp.org/resources/guidelines-safe-use-automated-dispensing-cabinets. Última visita: nov 2020.

[134] *Institute for Safe Medication Practices (ISMP). Targeted Medication Safety Best Practices for Hospitals.* URL: https://www.ismp.org/guidelines/best-practices-hospitals. Última visita: nov 2020.

[135] *Intel. IoT Hub.* URL: https://www.seone-park.com/iot-hub. Última visita: nov 2020.

[136] *Intel. IoT Industrial (IIoT) y tecnología de la automatización.* URL: https://www.intel.la/content/www/xl/es/internet-of-things/industrial-iot/overview.html. Última visita: dic 2020.

[137] *Intel. The Cybersecurity Framework in Action: An Intel Use Case.* URL: https://www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/cybersecurity-framework-in-action-use-case-brief.pdf. Última visita: nov 2020.

[138] *International of Nursing Studies. Colección Elsevier. Disponible en Portal Timbó. Alison Craswell et al. The impact of automated medicine dispensing units on nursing workflow: A cross-sectional study.* URL: https://doi.org/10.1016/j.ijnurstu.2020.103773. Última visita: nov 2020.

[139] *Internet Society.* URL: https://www.internetsociety.org/es/. Última visita: nov 2020.

[140] *Internet Society. AGESIC - Seguridad IoT.* URL: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/seguridad-iot. Última visita: nov 2020.

[141] *Internet Society. Canadian Multistakeholder Process: Enhancing IoT Security.* URL: https://www.internetsociety.org/events/canadian-multistakeholder-process-enhancing-iot-security/. Última visita: nov 2020.

[142] *Internet Society. Canadian Multistakeholder Process: Enhancing IoT Security Final Outcomes and Recommendations Report.* URL: https://www.internetsociety.org/resources/doc/2019/enhancing-iot-security-final-outcomes-and-recommendations-report/. Última visita: nov 2020.

[143] *Internet Society. Collaborative Governance Leaders, Canada, and Senegal Exchange Notes on IoT Security Frameworks.* URL: https://www.internetsociety.org/blog/2018/07/collaborative-governance-leaders-canada-and-senegal-exchange-notes-on-iot-security-frameworks/. Última visita: nov 2020.

[144] *Internet Society. Collaborative Security.* URL: https://www.internetsociety.org/collaborativesecurity/. Última visita: nov 2020.

[145] *Internet Society. Internet of Things (IoT).* URL: https://www.internetsociety.org/iot/. Última visita: nov 2020.

[146] *Internet Society. Internet of Things (IoT) Trust Framework v2.5.* URL: https://www.internetsociety.org/resources/doc/2018/iot-trust-framework-v2-5/. Última visita: nov 2020.

[147] *Internet Society. La Internet Society apoya la seguridad del IoT en Francia.* URL: https://www.internetsociety.org/es/news/comunicados-de-prensa/2019/la-internet-society-apoya-la-seguridad-del-iot-en-francia/. Última visita: nov 2020.

[148] *Internet Society. OTA IoT Trust Framework.* URL: https://www.internetsociety.org/iot/trust-framework/. Última visita: nov 2020.

[149] *Internet Society. Policy Brief: IoT Privacy for Policymakers.* URL: https://www.internetsociety.org/policybriefs/iot-privacy-for-policymakers/. Última visita: nov 2020.

[150] *Internet Society. Submission: High-Level Panel on Digital Coordination Consultation.* URL: https://digitalcooperation.org/wp-content/uploads/2019/02/ISOC-HLPDC-contribution-Final-1.pdf. Última visita: nov 2020.

[151] *Internet Society. Top Tips for Consumers: Internet of Things Security and Privacy.* URL: https://www.internetsociety.org/resources/doc/2018/top-tips-for-consumers-internet-of-things-security-and-privacy/. Última visita: nov 2020.

[152] *Internet Society. Uruguay se suma a los países que toman acciones para fortalecer la seguridad de dispositivos IoT.* URL: https://www.internetsociety.org/es/blog/2019/06/uruguay-joins-others-taking-action-to-strengthen-iot-security/. Última visita: nov 2020.

[153] *IoT Security Foundation.* URL: https://www.iotsecurityfoundation.org/. Última visita: nov 2020.

[154] *IoTSF. IoT Security Foundation Publications.* URL: https://www.iotsecurityfoundation.org/best-practice-guidelines/. Última visita: nov 2020.

[155] *ISA. ANSI/ISA-62443-3-3 (99.03.03)-2013 Security for industrial automation and control systems Part 3-3: System security requirements and security levels.* URL: https://www.isa.org/products/ansi-isa-62443-3-3-99-03-03-2013-security-for-indu. Última visita: nov 2020.

[156] *ISA. ISA–62443-2-1–2009 Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program.* URL: https://www.isa.org/products/isa-62443-2-1-2009-security-for-industrial-automat. Última visita: nov 2020.

[157] *ISACA. COBIT 5.* URL: https://www.isaca.org/resources/cobit/cobit-5%5C#sort=relevancy. Última visita: nov 2020.

[158] *ISO. ISO/CD 23247-1 - Digital Twin manufacturing framework — Part 1: Overview and general principles - Under development.* URL: https://www.iso.org/standard/75066.html. Última visita: nov 2020.

[159] *ISO. ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements.* URL: https://www.iso.org/standard/54534.html. Última visita: nov 2020.

[160] *ISO. ISO/IEC/IEEE 42010:2011 - Systems and software engineering - Architecture description.* URL: https://www.iso.org/standard/50508.html. Última visita: nov 2020.

[161] *ISO/IEC. JETI - Standardization for emerging technologies and innovations.* URL: https://jtc1info.org/technology/jeti/. Última visita: nov 2020.

[162] *Israel. Start-Up Nation Central - Industry 4.0.* URL: https://www.startupnationcentral.org/sector/industry-4-0/. Última visita: nov 2020.

[163] *Italia. Transizione 4.0.* URL: https://www.mise.gov.it/index.php/it/transizione40. Última visita: nov 2020.

[164] *Kaa. Industrial IoT Platform.* URL: https://www.kaaproject.org/industrial-automation. Última visita: dic 2020.

[165] *Kaspersky Lab ICS CERT. More than 50 % of organizations attacked by ExPetr (Petya) cryptolocker are industrial companies.* URL: https://ics-cert.kaspersky.com/alerts/2017/06/29/more-than-50-percent-of-organizations-attacked-by-expetr-petya-cryptolocker-are-industrial-companies/. Última visita: nov 2020.

[166] *Keidanren. Japan Business Federation.* URL: https://www.keidanren.or.jp/en/. Última visita: nov 2020.

[167] *Keidanren. Keidanren SDGs.* URL: https://www.keidanrensdgs-world.com/. Última visita: nov 2020.

[168] *Keidanren. Society 5.0.* URL: https://www.keidanren.or.jp/en/policy/2018/095.html. Última visita: nov 2020.

[169] *KLAS Research. Automated Dispensing Cabinets.* URL: https://klasresearch.com/compare/automated-dispensing-cabinets/25. Última visita: nov 2020.

[170] *KPMG. Trustworthy by design - November 2019 - A practical guide to organisational trust.* URL: https://assets.kpmg/content/dam/kpmg/au/pdf/2019/trustworthy-by-design-organisational-trust-guide.pdf. Última visita: nov 2020.

[171] *Linkedin. We Need STEAM, Not STEM Education, To Prepare Our Kids For The 4th Industrial Revolution - Bernard Marr.* URL: https://www.linkedin.com/pulse/we-need-steam-stem-education-prepare-our-kids-4th-industrial-marr/. Última visita: nov 2020.

[172] *Linuxtronix.* URL: https://linutronix.de/en/. Última visita: nov 2020.

[173] *Lituania. PLATFORM 'PRAMONĖ 4.0' STRUCTURE.* URL: https://industrie40.lt/platform-pramone-4-0-structure/. Última visita: nov 2020.

[174] *McKinsey & Company. Industry 4.0: Reimagining manufacturing operations after COVID-19.* URL: https://www.mckinsey.com/business-functions/operations/our-insights/industry-40-reimagining-manufacturing-operations-after-covid-19. Última visita: nov 2020.

[175] *Microsoft. Security Development Lifecycle (SDL).* URL: https://www.microsoft.com/en-us/securityengineering/sdl/. Última visita: nov 2020.

[176] *Microsoft. The STRIDE Threat Model.* URL: https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN. Última visita: nov 2020.

[177] *Microsoft. Threat Modeling.* URL: https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling. Última visita: nov 2020.

[178] *Microtom*. URL: https://www.microtom.com/products/smart-manufacturing. Última visita: nov 2020.

[179] *National Cybersecurity Center of Excellence (NCCoE). Mitigating IoT-Based DDoS*. URL: https://www.nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos. Última visita: nov 2020.

[180] *NEXCOM*. URL: https://www.nexcom.com/applications/DetailByDivision/-the-solutions-to-industry-4-0. Última visita: nov 2020.

[181] *Nexedi. Flexibility for your business*. URL: https://www.nexedi.com/. Última visita: nov 2020.

[182] *NeXT*. URL: https://mynext.it/?lang=en. Última visita: nov 2020.

[183] *NIST. An Introduction to the Components of the Framework*. URL: https://www.nist.gov/cyberframework/online-learning/components-framework. Última visita: nov 2020.

[184] *NIST. Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks - NIST IR 8228*. URL: https://csrc.nist.gov/publications/detail/nistir/8228/final. Última visita: nov 2020.

[185] *NIST. Cyber-Physical Systems and Internet of Things - SP - 1900-202*. URL: https://www.nist.gov/publications/cyber-physical-systems-and-internet-things. Última visita: nov 2020.

[186] *NIST. Cybersecurity Framework*. URL: https://www.nist.gov/cyberframework. Última visita: nov 2020.

[187] *NIST. Cybersecurity Framework - Success Stories*. URL: https://www.nist.gov/cyberframework/success-stories. Última visita: nov 2020.

[188] *NIST. Cybersecurity Framework Version 1.1*. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. Última visita: nov 2020.

[189] *NIST. Guide to Industrial Control Systems (ICS) Security - SP 800-82 Rev. 2*. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf. Última visita: nov 2020.

[190] *NIST. National Institute of Standards and Technology*. URL: https://www.nist.gov/. Última visita: nov 2020.

[191] *NIST. NCCoE MUD Profiling for IoT- MUDPI*. URL: https://github.com/usnistgov/MUDPI. Última visita: nov 2020.

[192] *NIST. NIST Special Publication 1800-15A, 1800-15B and 1800-15C - Preleminary Draft.* URL: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/iot-ddos-nist-sp1800-15-preliminary-draft-v2.pdf. Última visita: nov 2020.

[193] *NIST. Securing Small Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD) - SP 1800-15(Draft).* URL: https://csrc.nist.gov/publications/detail/sp/1800-15/draft. Última visita: nov 2020.

[194] *NIST. Security and Privacy Controls for Federal Information Systems and Organizations - SP 800-53 Rev. 4.* URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final. Última visita: nov 2020.

[195] *NIST. Security and Privacy Controls for Information Systems and Organizations - SP 800-53 Rev. 5(Draft).* URL: https://csrc.nist.gov/publications/detail/nistir/8228/final. Última visita: nov 2020.

[196] *NIST. Soft MUD: Implementing Manufacturer Usage Descriptions on OpenFlow SDN Switches.* URL: https://github.com/usnistgov/nist-mud. Última visita: nov 2020.

[197] *NIST. Spanish Translation of the NIST Cybersecurity Framework V1.1.* URL: https://www.nist.gov/document/frameworkesmellrev20181102mncleanpdf. Última visita: nov 2020.

[198] *NIST. Sucess Story: Israel National Cyber Directorate (INCD). Cyber Defense Methodology for the Organization.* URL: https://www.nist.gov/cyberframework/success-stories/israel-national-cyber-directorate. Última visita: nov 2020.

[199] *NIST. Zero Trust Architecture.* URL: https://csrc.nist.gov/publications/detail/sp/800-207/final. Última visita: nov 2020.

[200] *Nueva Zelanda. Callaghan Innovation - Industry 4.0 Hub.* URL: https://www.callaghaninnovation.govt.nz/industry-4. Última visita: nov 2020.

[201] *OCAI. Organizational Culture Assessment Instrument online.* URL: https://www.ocai-online.com/. Última visita: nov 2020.

[202] *Omnicell. Omnicell XT Automated Dispensing Cabinets.* URL: https://www.omnicell.co.uk/products/omnicell-xt-automated-dispensing-cabinets. Última visita: dic 2020.

[203] *Optiware*. URL: https://optiware.com/. Última visita: nov 2020.

[204] *Oracle. Oracle IoT Digital Twin Implementation*. URL: https://docs.oracle.com/en/cloud/paas/iot-cloud/iotgs/oracle-iot-digital-twin-implementation.html. Última visita: nov 2020.

[205] *OSISoft*. URL: https://www.osisoft.es/pi-system/. Última visita: nov 2020.

[206] *OWASP. OWASP Internet of Things*. URL: https://owasp.org/www-project-internet-of-things/. Última visita: nov 2020.

[207] *Países Bajos. Smart Industry*. URL: https://www.smartindustry.nl/. Última visita: nov 2020.

[208] *Patient Safety Netowork (PSNet). Agency for Healthcare Research and Quality (AHRQ). Medication Errors and Adverse Drug Events*. URL: https://psnet.ahrq.gov/primer/medication-errors-and-adverse-drug-events. Última visita: dic 2020.

[209] *Philips. The rise of the digital twin: how healthcare can benefit*. URL: https://www.philips.com/a-w/about/news/archive/blogs/innovation-matters/20180830-the-rise-of-the-digital-twin-how-healthcare-can-benefit.html. Última visita: nov 2020.

[210] *PI System*. URL: https://www.osisoft.es/pi-system/. Última visita: nov 2020.

[211] *Platform Industrie 4.0 and the Robot Revolution and Industrial IoT Initiative (RRI). Revitalizing Human-Machine Interaction for the Advancement of Society*. URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/acatech-i40-revitalizing-human-machine-interaction.html. Última visita: nov 2020.

[212] *Plattform Industrie 4.0 & Industrie du Futur. Plattform Industrie 4.0 and Industrie du Futur: Common List of Scenarios*. URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/plattform-i40-und-industrie-du-futur-scenarios.html. Última visita: nov 2020.

[213] *Plattform Industrie 4.0 & Industrie du Futur. Plattform Industrie 4.0 and Industrie du Futur: Joint working program 2017 for Convergence in standardization*. URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/plattform-i40-und-industrie-du-futur-joint-programme.html. Última visita: nov 2020.

[214] *Plattform Industrie 4.0 and G20. Digitising Manufacturing in the G20 – Initiatives, Best Practice and Policy Approaches.* URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/g20-documentary.html. Última visita: nov 2020.

[215] *Plattform Industrie 4.0 and Industry 4.0 Taskforce of the Australian Prime Minister. German-Australian Cooperation on Industrie 4.0.* URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Dossiers/international-cooperations.html. Última visita: nov 2020.

[216] *Plattform Industrie 4.0 and Robot Revolution & Industrial IoT Iniciative. Facilitating International Cooperation for Secure Industrial Internet of Things/Industrie 4.0.* URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/Secure-Industrial-Internet-of-Things.html. Última visita: nov 2020.

[217] *Plattform Industrie 4.0 and Smart Industry. Joint Agreement between Plattform Industrie 4.0 and the Smart Industry Program of the Netherlands.* URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/smart-industry-nl-agreement.html. Última visita: nov 2020.

[218] *Plattform Industrie 4.0, Industrie du Futur and Piano Industria 4.0. Shared Action Plan Industrie du Futur / Industrie 4.0 / Industria 4.0 in France – Germany – Italy.* URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/shared-actionplan-fr-de-it.html. Última visita: nov 2020.

[219] *Plattform Industrie 4.0, Industrie Du Futur and Robot Revolution & Industrial IoT Iniciative. Maps of IoT use case in Germany, France and Japan.* URL: https://www.jmfrri.gr.jp/english/430.html. Última visita: nov 2020.

[220] *Plattform Industrie 4.0, SCI4.0, RRI & VDI/VDE-GMA. Usage View Seamless and Dynamic Engineering of Plants.* URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/usage-view-seamless-and-dynamic-engineering-of-plantsx.html. Última visita: dic 2020.

[221] *Plattform Industrie 4.0. Asset Administration Shell - Reading Guide.* URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/Asset%5C_Administration%5C_Shell%5C_Reading%5C_Guide.html. Última visita: dic 2020.

[222] *Plattform Industrie 4.0. Corona and the Consequences.* URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/Corona%5C_Thesen.html. Última visita: dic 2020.

[223] *Plattform Industrie 4.0. Details of the Asset Administration Shell Part 1 - Version 3.* URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/Details_of_the_Asset_Administration_Shell_Part1_V3.html. Última visita: nov 2020.

[224] *Plattform Industrie 4.0. Details of the Asset Administration Shell Part 2 - Version 3.* URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/Details_of_the_Asset_Administration_Shell_Part2_V1.html. Última visita: nov 2020.

[225] *Plattform Industrie 4.0. International cooperation.* URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Dossiers/international-cooperations.html. Última visita: nov 2020.

[226] *Plattform Industrie 4.0. Position Paper 2030 Vision for Industrie 4.0.* URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/Positionspapier%5C%20Leitbild%5C%20(EN).html. Última visita: nov 2020.

[227] *Plattform Industrie 4.0. Progress Report 2019.* URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/2019-progress-report.html. Última visita: nov 2020.

[228] *Plattform Industrie 4.0. Recommendations of the Trilateral Cooperation between France, Italy and Germany on Digitalising the European Manufacturing Industry.* URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/Positionspapier-EU-TriKop.pdf. Última visita: nov 2020.

[229] *Plattform Industrie 4.0. Reference Architectural Model Industrie 4.0 (RAMI4.0) - An Introduction.* URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/rami40-an-introduction.html. Última visita: nov 2020.

[230] *Plattform Industrie 4.0. Relationships between I4.0 Components – Composite Components and Smart Production.* URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/hm-2018-relationship.html. Última visita: nov 2020.

[231] *Plattform Industrie 4.0. Standarization Council Industrie 4.0, RRI & VDI/VDE. Usage Viewpoint of Asset Administration Shell.* URL: https://www.jmfrri.gr.jp/english/document/library/1110.html. Última visita: nov 2020.

[232] *Plattform Industrie 4.0. Structure and Organization of the Plattform Industrie 4.0.* URL: https://www.plattform-i40.de/PI40/Navigation/EN/ThePlatform/Structure-Organization/structure-organization.html. Última visita: nov 2020.

[233] *Plattform Industrie 4.0. Submodel Templates of the Asset Administration Shell - Generic Frame for Technical Data for Industrial Equipment in Manufacturing (Version 1.1).* URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/Submodel%5C_templates-Asset%5C_Administration%5C_Shell-Technical%5C_Data.html. Última visita: dic 2020.

[234] *Plattform Industrie 4.0. Submodel Templates of the Asset Administration Shell - ZVEI Digital Nameplate for industrial equipment (Version 1.0).* URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/Submodel%5C_templates-Asset%5C_Administration%5C_Shell-digital%5C_nameplate.html. Última visita: dic 2020.

[235] *Plattform Industrie 4.0. The Asset Administration Shell: Implementing digital twins for use in Industrie 4.0.* URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/VWSiD%5C%20V2.0.html. Última visita: nov 2020.

[236] *Plattform Industrie 4.0. The platform's working groups.* URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Dossiers/working-groups.html. Última visita: nov 2020.

[237] *Plattform Industrie 4.0. What is Industrie 4.0?* URL: https://www.plattform-i40.de/PI40/Navigation/EN/Industrie40/WhatIsIndustrie40/what-is-industrie40.html. Última visita: nov 2020.

[238] *Plattform Industrie 4.0. Which criteria do Industrie 4.0 products need to fulfil? Guideline 2019.* URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/criteria-industrie-40-products.html. Última visita: nov 2020.

[239] *Plattform Industrie 4.0. Which criteria do Industrie 4.0 products need to fulfil? Guideline 2019.* URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/criteria-industrie-40-products.html. Última visita: nov 2020.

[240] *PNUD. Objetivos de Desarrollo Sostenible.* URL: https://www.undp.org/content/undp/es/home/sustainable-development-goals.html. Última visita: nov 2020.

[241] *Portugal. Indústria 4.0.* URL: https://www.iapmei.pt/Paginas/Industria-4-0.aspx. Última visita: nov 2020.

[242] *Presidencia de la República. Oficina de Planeamiento y Presupuesto. Administración de Servicios de Salud del Estado (ASSE). Recursos período 2004-2018. Informe elaborado el año 2018.* URL: https://transparenciapresupuestaria.opp.gub.uy/sites/default/files/expo_motivos/2018-salud-asse-recursos.htm. Última visita: dic 2020.

[243] *Reino Unido. Digital Catapult.* URL: https://www.digicatapult.org.uk/. Última visita: nov 2020.

[244] *República Checa. Průmysl 4.0.* URL: https://www.prumysl-4.cz/. Última visita: nov 2020.

[245] *rexroth. A Bosh Company.* URL: https://www.boschrexroth.com/en/xc/. Última visita: nov 2020.

[246] *rexroth. A Bosh Company. ctrlX AUTOMATION.* URL: https://apps.boschrexroth.com/microsites/ctrlx-automation/en/. Última visita: nov 2020.

[247] *Robert S. Kaplan and David P. Norton. The Balanced Scorecard: Translating Strategy into Action.* URL: https://www.hbs.edu/faculty/Pages/item.aspx?num=8831. Última visita: dic 2020.

[248] *RWTH Aachen University. PyI40AAS.* URL: https://git.rwth-aachen.de/acplt/pyi40aas. Última visita: dic 2020.

[249] *SAP.* URL: https://www.sap.com/. Última visita: nov 2020.

[250] *SAP. i40-aas*. URL: https://github.com/SAP/i40-aas. Última visita: nov 2020.

[251] *SAP. Industry 4.0 Solutions*. URL: https://www.sap.com/products/supply-chain-management/industry-4-0.html. Última visita: nov 2020.

[252] *Seebo*. URL: https://www.seebo.com/why-seebo/. Última visita: nov 2020.

[253] *SEEBURGER Business Integration*. URL: https://www.seeburger.com/. Última visita: nov 2020.

[254] *Singapore Cyber Security Agency*. URL: https://www.csa.gov.sg/. Última visita: doc 2020.

[255] *Singapore Economic Development Board (EDB). The Prioritisation Matrix*. URL: https://siri.gov.sg/docs/default-source/default-document-library/the-prioritisation-matrix.pdf. Última visita: nov 2020.

[256] *Singapore Economic Development Board (EDB). The Singapore Smart Industry Readiness Index*. URL: https://siri.gov.sg/. Última visita: nov 2020.

[257] *Singapore Economic Development Board (EDB). The Smart Industry Readiness Index - Catalysing the transformation of manufacturing*. URL: https://siri.gov.sg/docs/default-source/default-document-library/the-smart-industry-readiness-index.pdf. Última visita: nov 2020.

[258] *Singapore Manufacturing Consortium - SIMCO. Inspiring trust in the physical and digital world*. URL: http://www.singaporemanufacturingconsortium.com/. Última visita: nov 2020.

[259] *Singapore. Transforming Singapore Through Technology*. URL: https://www.smartnation.sg/. Última visita: nov 2020.

[260] *Sino-German Standardisation Cooperation Commission. Alignment Report for Reference Architectural Model for Industrie 4.0 / Intelligent Manufacturing System Architecture*. URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/hm-2018-manufacturing.html. Última visita: nov 2020.

[261] *SlapOS. Edge Cloud Computing and Orchestation*. URL: https://slapos.nexedi.com/. Última visita: nov 2020.

[262] *Society of Hospital Pharmacists of Australia (SHPA). Factors to consider for the implementation of Automated Pharmacy Distribution Systems in Hospitals and Health Services.* URL: https://www.shpa.org.au/sites/default/files/uploaded-content/website-content/Fact-sheets-position-statements/automation_practice_update.pdf. Última visita: dic 2020.

[263] *Sputnik News. La tragedia de Bophal.* URL: https://mundo.sputniknews.com/reportajes/201912061089557624-la-tragedia-de-bhopal-el-mayor-desastre-industrial-que-sego-miles-de-vidas-en-un-instante/. Última visita: nov 2020.

[264] *Suecia. Strategic innovation programme for sustainable production in Sweden.* URL: https://produktion2030.se/en/. Última visita: nov 2020.

[265] *Telit. IoT & M2M Modules, Platforms, and Connectivity Products.* URL: https://www.telit.com/m2m-iot-products/%5C#iot-platforms. Última visita: dic 2020.

[266] *The Economist and Telstra. The Asian Digital Transformation Index 2018.* URL: http://connectedfuture.economist.com/article/asian-digital-transformation-index-2018/. Última visita: nov 2020.

[267] *The European Directorate for the Quality of Medicines & HealthCare. Best Practice for the Automated Dose Dispensing (ADD) Process and Care and Safety of Patients.* URL: https://www.edqm.eu/en/news/new-automated-dose-dispensing-add-guidelines. Última visita: nov 2020.

[268] *The Pharmaceutical Journal. Adoption of closed loop medicines administration into the NHS.* URL: https://www.pharmaceutical-journal.com/news-and-analysis/opinion/blogs/adoption-of-closed-loop-medicines-administration-into-the-nhs/20206864.blog. Última visita: dic 2020.

[269] *The White House - President Barack Obama -USA. Executive Order – Improving Critical Infrastructure Cybersecurity.* URL: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity. Última visita: nov 2020.

[270] *The White House - USA. Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.* URL: https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/. Última visita: nov 2020.

[271] *The World Bank. Doing Business 2020.* URL: https://www.doingbusiness.org/en/reports/global-reports/doing-business-2020. Última visita: nov 2020.

[272] *TÜV SÜD. Inspiring trust in the physical and digital world.* URL: https://www.tuvsud.com/en/-/media/global/pdf-files/brochures-and-infosheets/tuvsud-corp-brochure-en-lr.pdf?la=en%5C&hash=41CDA99A82188987EB3424E6AEA87959. Última visita: nov 2020.

[273] *U.S. Department of Health & Human Services. The Office of Disease Prevention and Health Promotion (ODPHP). Adverse Drug Events.* URL: https://health.gov/our-work/health-care-quality/adverse-drug-events. Última visita: dic 2020.

[274] *Ubuntu blog. Bosch Rexroth adopts Ubuntu Core and snaps for app-based ctrlX AUTOMATION platform.* URL: https://ubuntu.com/blog/bosch-rexroth-adopts-ubuntu-core-and-snaps-for-app-based-ctrlx-automation-platform. Última visita: nov 2020.

[275] *UNESCO. Japan pushing ahead with Society 5.0 to overcome chronic social challenges.* URL: https://en.unesco.org/news/japan-pushing-ahead-society-50-overcome-chronic-social-challenges. Última visita: nov 2020.

[276] *United Nations. Sustainable Development Knowdledge Platform.* URL: https://sustainabledevelopment.un.org/. Última visita: nov 2020.

[277] *Universities of the Future. Project Results.* URL: https://universitiesofthefuture.eu/comunication/. Última visita: nov 2020.

[278] *University of New South Wales. MUDGEE Tool.* URL: https://iotanalytics.unsw.edu.au/mudprofiles. Última visita: nov 2020.

[279] *University of Virginia, Department of Computer Science. The Protection of Information in Computer Systems.* URL: http://www.cs.virginia.edu/~evans/cs551/saltzer/. Última visita: nov 2020.

[280] *US-CERT - CISA. Alert (AA20-049A) - Ransomware Impacting Pipeline Operations.* URL: https://www.us-cert.gov/ncas/alerts/aa20-049a. Última visita: nov 2020.

[281] *Usenix. Understanding the Mirai Botnet.* URL: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf. Última visita: nov 2020.

[282] *VDMA.* URL: https://www.vdma.org/en/der-vdma. Última visita: nov 2020.

[283] *WEF. The Great Reset.* URL: https://www.weforum.org/great-reset/. Última visita: dic 2020.

[284] *Wendelin. Data Lake Sharing Platform.* URL: https://www.wendelin.io/. Última visita: nov 2020.

[285] *Wipro.* URL: https://www.wipro.com/. Última visita: nov 2020.

[286] *Wipro. Security by Design.* URL: https://www.wipro.com/engineeringNXT/industry-4-0-security-engineering/. Última visita: nov 2020.

[287] *World Economic Forum. Fourth Industrial Revolution: Beacons of Technology and Innovation in Manufacturing.* URL: https://www.weforum.org/whitepapers/fourth-industrial-revolution-beacons-of-technology-and-innovation-in-manufacturing. Última visita: nov 2020.

[288] *World Economic Forum. Global Competitiveness Report 2019: How to end a lost decade of productivity growth.* URL: https://www.weforum.org/reports/how-to-end-a-decade-of-lost-productivity-growth. Última visita: nov 2020.

[289] *World Economic Forum. The Global Risks Report 2020.* URL: https://www.weforum.org/reports/the-global-risks-report-2020. Última visita: nov 2020.

[290] *World Economic Forum. These 7 tech investments are critical to building 'intelligent factories' after COVID-19.* URL: https://www.weforum.org/agenda/2020/09/7-tech-investments-that-will-make-factories-more-resilient-after-covid-19/. Última visita: nov 2020.

[291] *Wu Tuck Seng, Deputy Director & Head, Pharmacy Department, National University Hospital (NUH), Singapore. Introduction of Closed Loop Medication Management System for Inpatient Services in Singapore.* URL: https://www.fing.edu.uy/owncloud/index.php/s/z2hJ3qGTDZgNg8u. Última visita: dic 2020.

[292] *Wu Yi Zheng, Valentina Lichtner, Bethany A. Van Dort & Melissa T. Baysari. The impact of introducing automated dispensing cabinets, barcode medication administration, and closed-loop electronic medication management systems on work processes and safety of controlled medications in hospitals: A systematic review.* URL: http://www.sciencedirect.com/science/article/pii/S155174112030406X. Última visita: dic 2020.

[293] *Wu Yi Zheng, Valentina Lichtner, Bethany A. Van Dort and Melissa T. Baysari - The impact of introducing automated dispensing cabinets, barcode medication administration, and closed-loop electronic medication management systems on work processes and safety of controlled medications in hospitals: A systematic review.* URL: https://www.sciencedirect.com/science/article/pii/S155174112030406X. Última visita: nov 2020.

[294] *ZVEI.* URL: https://www.zvei.org/en/. Última visita: nov 2020.