Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

MAESTRÍA EN CIBERDEFENSA Y CIBERSEGURIDAD

TESIS DE MAESTRÍA

Propuesta metodológica para una evaluación en ciberseguridad enfocada a dispositivos *IoT* en un entorno de transformación digital.

AUTOR: ING. LUISA FERNANDA VECINO DAZA

DIRECTOR: MAG. DANIEL PERLES

BUENOS AIRES, ARGENTINA – NOVIEMBRE 2023

i. RESUMEN.

La presente tesis pretende realizar, en primer lugar, una investigación y análisis del estado del arte referente a los dispositivos *IoT*, industria 4.0, marcos de referencia, estándares y evaluaciones de ciberseguridad enfocados a *IoT* en la actualidad, teniendo en cuenta el crecimiento notorio en la adquisición e incorporación de estos dispositivos durante los últimos años en diferentes áreas, para evaluar los aspectos de la ciberseguridad en esta materia.

El aumento en la incorporación de sensores y diversas tecnologías en distintos dispositivos de uso común (domótica, *wearables*, *Smart Cities*, *IIoT*, IoMT, industria 4.0, entre otros) supone también el aumento en el número de fabricantes y proveedores de estos. Es aquí, en donde esta investigación busca exponer las ventajas, desventajas, usos, funcionalidades y configuraciones de estos dispositivos, con el fin de demostrar, que, si bien son útiles en el día a día de sus usuarios, son también la puerta a ciberataques de gran escala debido a las vulnerabilidades de seguridad que ofrece como tal el dispositivo y la ausencia de soporte por parte de algunos fabricantes. Asimismo, de la mano con esta investigación, se busca relacionar la incorporación de estos dispositivos, específicamente en la industria 4.0, evaluando su impacto dentro de las pequeñas y grandes empresas a través de una evaluación completa de ciberseguridad con foco en dispositivos *IoT*.

Una vez concluida esta investigación, se analizará el panorama actual en cuanto a seguridad en dispositivos *IoT*, industria 4.0 y los diferentes marcos y estándares para una adecuada evaluación de ciberseguridad en entornos empresariales, para lograr tomar esto como referencia y lograr relacionar ambas temáticas.

Finalmente, volcar toda la información recolectada y analizada para el desarrollo de una propuesta para evaluación de la ciberseguridad en dispositivos *IoT* en la industria 4.0 a través del desarrollo de una matriz de riesgos, un plan de trabajo y de una serie de consideraciones enfocadas al buen uso de dispositivos *IoT* en entornos empresariales, esto con el fin de brindar una guía para la evaluación de la ciberseguridad con foco a dispositivos *IoT* dentro de pequeñas y grandes empresas a través de la implementación de controles de seguridad, recomendaciones, buenas prácticas e instrucciones para el uso correcto de dispositivos *IoT*.

ii. ABSTRACT.

This project aims to perform, firstly, an investigation and analysis of the state of the art concerning IoT devices, Industry 4.0, frameworks, standards, and Cybersecurity assessments focused on IoT today, considering the notorious growth in the acquisition and incorporation of these devices during the last years in different areas, in order to evaluate the Cybersecurity aspects in this matter.

The increase in the inclusion of sensors and various technologies in different devices of common use (home automation, wearables, Smart Cities, IIoT, IoMT, Industry 4.0, among others) also means an increase in the number of manufacturers and suppliers of these devices. It is here, where this research seeks to expose the advantages, disadvantages, uses, functionalities, and configurations of these devices, in order to demonstrate that, although they are useful in the daily lives of their users, they are also the door to large-scale cyberattacks due to security vulnerabilities provided by the device and the lack of support from some manufacturers. Also, in conjunction with this research, we seek to relate the incorporation of these devices, specifically in Industry 4.0, assessing their impact on small and large companies through a comprehensive Cybersecurity assessment focused on IoT devices.

Once this research is completed, we will analyze the current security landscape in IoT devices, Industry 4.0 and the different frameworks and standards for an adequate Cybersecurity assessment in business environments, in order to take this as a reference and manage to relate both topics.

Finally, to overturn all the information collected and analyzed for the purpose of developing of a proposal for the Cybersecurity assessment in IoT devices in Industry 4.0 through the development of a risk matrix, a work plan and a series of considerations focused on the proper use of IoT devices in enterprise environments, in order to provide a guide for the evaluation of Cybersecurity focused on IoT devices in small and large companies through the implementation of security controls, recommendations, best practices and instructions for the proper use of IoT devices.

iii. DEDICATORIAS.

A mis padres y hermanos, quienes me motivaron y brindaron su apoyo durante la realización de esta tesis impulsando mi crecimiento académico y profesional.

iv. AGRADECIMIENTOS.

En primer lugar, agradezco a mi director de tesis, Mtr. Daniel Perles, por su paciencia y apoyo a lo largo del desarrollo de esta tesis con sus correcciones, recomendaciones y acompañamiento.

Agradezco también a cada uno de los docentes que contribuyeron a mi formación durante la realización de esta maestría con su conocimiento y dedicación, principalmente al Dr. Roberto Uzal y al Ing. Carlos Amaya. Asimismo, a cada uno de mis compañeros de cohorte ya que sus conocimientos en las diferentes áreas de formación y experiencia laboral contribuyeron a mi crecimiento académico y adopción de nuevos conocimientos.

Finalmente, a mi familia, amigos y compañeros de trabajo que estuvieron motivándome durante la realización de esta tesis ya que quiero compartir principalmente con ellos esta nueva meta alcanzada, gracias por estar en los momentos más importantes.

v. ÍNDICE.

vi. ÍNDICE DE TABLAS.

vii. ÍNDICE DE FIGURAS.

viii. ABREVIATURAS Y ACRÓNIMOS.

AMQP	*Advanced Message Queuing Protocol* / Protocolo avanzado de colas de mensajes
AS	Accesos Sensitivos
B2B	*Business to Business* / Negocio a negocio
B2C	*Business to Consumer* / Negocio a cliente
BDM	*Business Decision Maker* / Tomadores de decisiones en las áreas de negocio)
BYOD	*Bring your Own Device* / Trae tu propio dispositivo
BYOW	*Bring Your Own Wearable* / Trae tu propio vestible
C&C	Comando y Control
CIoT	*Internet of Consumer Things* / Internet de las cosas del consumidor
CoAP	*Constrained Application Protocol* / Protocolo de aplicación restringida
CVE	*Common Vulnerabilities and Exposures* / Vulnerabilidades y riesgos comunes
DDOS	*Distributed Denial of Services* / Denegación de servicios distribuida
DDS	*Data Distribution Service* / Servicio de distribución de datos
DRP	*Disaster Recovery Plan* / Plan de recuperación de desastres
ERP	*Enterprise Resource Planning* / Planificación de recursos empresariales
FDA	*U.S. Food and Drug Administration* / Administración de Alimentos y Medicamentos de E.E.U.U
FI	*Fill-ins* / A completar
HTTP	Protocolo de transferencia de hipertexto
HVAC	*Heating, Ventilating, Air Conditioned* / Calefacción, Ventilación, Aire acondicionado
IA	Inteligencia Artificial
IaaS	*Internet as a Service* / Internet como servicio
IIoT	*Internet of Industrial Things* / Internet industrial de las cosas
IoE	*Internet of Everything* / Internet de todo
IoMT	*Internet of Medical Things* / Internet de las cosas médicas
IoRT	*Internet of Robotic Things* / Internet de las cosas robóticas
IoT	*Internet of Things* / Internet de las cosas

IP *Internet Protocol* / Protocolo de internet

ISACA *Information Systems Audit and Control Association* / Asociación de auditoría y control de sistemas de información

ISO *International Organization for* Standardization / Organización internacional para la estandarización

IT *Information Technology* / Tecnología de la información

ITDM *Information Technology Decision Maker* / Tomadores de decisiones en el área de tecnología de la información

KPI *Key Performance Indicator* / Indicador clave de rendimiento

M2M *Machine to machine* / Máquina a máquina

MP *Major Projects* / Principales proyectos

MQTT *Message Queuing Telemetry Transport* / Cola de mensajes Transporte de telemetría

NFC *Near Field Communication* / Comunicación de campo cercano

NFT *Non-Fungible Token* / Ficha no fungible

OT *Operation Technology* / Tecnología de la operación

OWASP *Open Web Application Security Project* / Proyecto abierto de seguridad de las aplicaciones web

P2P *Peer-to-peer* / Cliente a cliente

QW *Quick Wins* / Ganancias rápidas

RFID *Radio Frequency Identification* / Identificación por radiofrecuencia

SaaS *Software as a Service* / Programa informático como servicio

SDK Kit de desarrollo de *software*

SLA *Service Level Agreement* / Acuerdo de nivel de servicio

SNMP Protocolo simple de administración de red

SoD *Segregation of Duties* / Segregación de funciones

TIC Tecnologías de la Información y las Comunicaciones

TT *Thankless Tasks* / Trabajos poco apreciados

UPnP *Universal Plug and Play* / Enchufar y usar universal.

VAR *Video Assistant Referee* / Árbitro asistente de video

VLAN Redes de área local virtuales

VOIP *Voice Over IP* / Voz sobre IP

VPN *Virtual Private Network* / Red privada virtual

XML Lenguaje de marcado extensible

XMPP *Extensible Messaging and Presence Protocol* / Protocolo extensible de mensajería y presencia

1) INTRODUCCIÓN.

Esta tesis tiene como objeto en primer lugar una profunda investigación referente a Internet de las Cosas (*IoT*, por sus siglas en inglés), conceptos básicos, estándares, regulaciones, tecnologías, casos de uso, ventajas y desventajas. Posteriormente, se profundizará en Internet de las Cosas dentro de un entorno empresarial, específicamente en empresas en proceso de transformación digital e Industria 4.0, para finalmente, indagar respecto a las diferentes evaluaciones de ciberseguridad en las empresas y marcos de referencia llevados a cabo en la actualidad para dar lugar a una propuesta de evaluación de ciberseguridad enfocada en dispositivos *IoT* en entornos empresariales.

A través de esta investigación y desarrollo de la propuesta mencionada anteriormente, se busca mejorar los procedimientos actuales dentro de las grandes empresas siendo estás las que pueden representar mayores consecuencias al verse víctimas de un ciberataque. Si bien, el enfoque de esta tesis es Internet de las Cosas al ser una tecnología que se encuentra en constante y rápido crecimiento en diferentes entornos, esta tesis propone una evaluación de ciberseguridad en ambientes empresariales que tenga en cuenta los distintos factores y riesgos alrededor de los diferentes vectores de ataque dentro de un enfoque de ciberseguridad.

Como beneficiarios de esta tesis se encuentra cualquier usuario de dispositivos *IoT* que desee conocer y mantener un uso seguro para la protección de su información o información de terceros. Adicionalmente, el desarrollo de una matriz de riesgos, manual de buenas prácticas y recomendaciones, se enfoca en los entornos empresariales en los cuales se han adoptado dispositivos *IoT* dentro de los diferentes procesos de la compañía y se desea mantener un control constante respecto a la seguridad de estos, entendiendo que mal uso o falta de control sobre estos puede significar la puerta de entrada a un ciberataque de gran escala y con grandes consecuencias.

Dentro de los conceptos claves de esta tesis, se encuentra la terminología relacionada con Internet de las Cosas tales como Internet Industrial de las Cosas, Internet del Todo, Internet Médico de las Cosas o Internet de las Cosas del Consumidor. También, se presentan conceptos relacionados a los casos de uso de *IoT*, así como domótica, Industria 4.0 y *Smart Cities*. Finalmente, se mencionan diferentes tecnologías relacionadas como 5G, Inteligencia Artificial, *Machine Learning*, *Big Data, Edge Computing*, entre otros.

Dentro de las metodologías de investigación de esta tesis, se presentan el método histórico a través de la búsqueda de antecedentes y proyecciones realizadas respecto a la

inducción de *IoT* en diferentes entornos, también, esta investigación pretende ser de tipo aplicada ya que busca desarrollar una propuesta que sea de utilidad, basado en la investigación teórica realizada previamente.

La estructura capitular de esta tesis inicia con la definición de conceptos claves en torno a Internet de las Cosas, antecedentes, ventajas, desventajas, arquitectura, ecosistemas, regulaciones, seguridad y privacidad de dispositivos *IoT*. Posteriormente, se presenta la inducción de *IoT* en las empresas a través del Internet Industrial de las Cosas (*IIoT*, por sus siglas en inglés), Industria 4.0, transformación digital y vectores de ataque en entornos empresariales. También, se dedica un capítulo a la investigación de la situación actual de las diferentes auditorias en ciberseguridad, marcos de referencia y regulaciones actuales. Finalmente, una vez realizada esta investigación, se presenta el desarrollo de la propuesta la cual se compone de un plan de trabajo, un manual de recomendaciones y buenas prácticas y una matriz de controles, todo esto enfocado a *IoT* y ciberseguridad en entornos empresariales.

2) PLANTEAMIENTO DEL PROBLEMA.

Esta tesis tiene como fin investigar los diferentes aspectos que amenazan la seguridad en los dispositivos *IoT*, sin dejar de lado su importancia y beneficios, pero haciendo énfasis en los diferentes riesgos que incluyen la seguridad por defecto y la responsabilidad del usuario. Es bien sabido que la adopción por parte de usuarios, empresas y gobiernos de dispositivos *IoT* ha estado en constante crecimiento. La conexión entre estos objetos inteligentes y sus usuarios implica un alto intercambio de todo tipo de información, sensible y no sensible, lo cual supone una potente amenaza y vulnerabilidad a los datos. Si bien la cantidad y disponibilidad de dispositivos *IoT* es creciente, no sucede lo mismo con el trabajo de seguridad implementado en los mismos, lo cual deja la mayor parte de responsabilidad sobre la seguridad de estos dispositivos del lado del usuario más que del proveedor.

Asimismo, la inclusión de estos dispositivos *IoT* en entornos empresariales, tanto para uso personal como institucional, puede automatizar y facilitar muchas tareas diarias, pero en varios casos, se deja de lado de seguridad de estos al no tener un control constante sobre ellos o no ejercer buenas prácticas desde el momento de su incorporación.

Es posible que el aumento en la demanda de dispositivos *IoT* motive a diferentes empresas a crear necesidades en los usuarios a través del desarrollo de objetos inteligentes que realicen casi cualquier tarea del día a día. Si bien esto no es malo, se podría pensar que del gran número de proveedores que surgen para dispositivos *IoT*, en muchos casos su objetivo principal no es garantizar la seguridad de los datos del usuario, sino generar ingresos económicos. En un futuro próximo, el aumento en la demanda y la inclusión de dispositivos *IoT* por parte de usuarios del común, empresas y gobiernos, lleva a la creación y auge en temas como la domótica y la industria 4.0 la cual supone la potenciación de *IIoT* y *Smart Cities*, por lo cual cada persona debe estar educada y capacitada para convivir en un entorno totalmente *Smart* ya que adquiera o no por su cuenta alguno de estos dispositivos para su beneficio, igualmente su entorno empleará estos dispositivos para brindar soluciones día a día, por lo cual, se quiera o no es una realidad para la cual cada persona debe tener conocimiento y conciencia respecto a la información que comparte, dónde y cómo lo hace.

Teniendo en cuenta que estos dispositivos se encuentran presentes tanto en los usuarios del común (en su mayoría), como en las organizaciones y gobiernos, es hoy casi

impensable prescindir de estos equipos, lo cual tampoco es lo ideal. Con una buena seguridad estos dispositivos pueden proporcionar al usuario datos importantes para toma de alguna decisión personal o técnica, así como también pueden ofrecer predicciones o recomendaciones personalizadas para mejorar su experiencia con la herramienta.

En el caso de las empresas, las cuales están actualmente casi dependiendo de estos equipos, las consecuencias se encuentran a un nivel más crítico debido al alcance y manejo de información por parte de dispositivos *IoT*. Por un lado, es algo bueno ya que facilitan las tareas de los operadores sin comprometer el funcionamiento de la organización, pero, por otro lado, sin una buena revisión en la seguridad de cada uno de estos equipos, podrían representar la oportunidad para un atacante de obtener todos los datos que se comparten y posteriormente realizar cualquier tipo de ataque a la víctima, ya sea un *ransomware*, robo de datos, *DDOS*, *man-in-the-middle*, ingeniería social, entre otros.

Por otro lado, surgen también dispositivos acordes a cualquier situación actual que vienen a reemplazar objetos comunes por objetos inteligentes. Tal es el caso del termómetro inteligente Kinsa[1] llamado *Smart Ear,* el cual se conecta al celular por *bluetooth* a través de una aplicación móvil manteniendo informado al usuario de su temperatura y de acuerdo con estos resultados realiza monitoreos, predicciones y da recomendaciones. Si bien su objetivo principal suple la misma función del termómetro convencional, es bastante atractivo saber que se tiene un control permanente gracias a los datos que ofrece la aplicación y más aún cuando este dispositivo aparece en medio de la pandemia Covid-19 aprovechando el miedo social por contraer el virus. No está mal el uso de este dispositivo, de hecho, puede ser de gran utilidad para muchos usuarios, pero, tanto en este como en cualquier otro dispositivo *IoT* es importante siempre preguntarse a quién le estamos proporcionando nuestros datos, especialmente en un momento en que la diferencia entre un dato considerado *sensible* y uno *no sensible* es mínima. Entender esto es el principio de todo, y es lo que se pretende lograr a través de esta tesis. Conocer el valor de nuestra información y cómo la compartimos, es clave para mantenerse seguro en la red.

Como se mencionó anteriormente, el número de proveedores para dispositivos *IoT* crece considerablemente día a día, según Gartner[2], en el 2020 hubo cerca de 21.000 millones de objetos inteligentes recopilando y transmitiendo datos para el desarrollo de sus funciones. Esto hace bastante difícil encontrar un estándar o herramienta universal *IoT* que

[1] Compañía Estadounidense dedicada al desarrollo de herramientas para el sector salud.
[2] Empresa líder en consultoría e investigación sobre tecnologías de la información.

ayude a controlar las configuraciones de seguridad de cada uno de estos dispositivos. Incluso, si esta herramienta existiera, no se puede dejar de lado o restar importancia al papel del usuario, si bien un producto puede garantizar seguridad a través de su modelo de desarrollo, sigue siendo vulnerable si no se tiene un uso adecuado.

El primer paso para lograr un uso responsable en los usuarios de dispositivos *IoT*, sean personas del común, empresas o gobiernos, es la educación. Si se tiene claro el valor de la información, las consecuencias de un uso deliberado de estos objetos y las vulnerabilidades a las que nos exponemos al hacer uso de estos, será más fácil tomar medidas conscientes y responsables al manipular cualquier dispositivo *IoT*, es por esto, que esta tesis pretende exponer cada una de las ventajas y desventajas de diferentes tipos de objetos inteligentes, para posteriormente brindar directrices e instrucciones para hacer más segura la interacción usuario-objeto principalmente en entornos empresariales. El fin no es evitar la adquisición de dispositivos *IoT* en ningún entorno, entendemos que son objetos que no buscan la adaptación a ellos por parte de los usuarios, al contrario, buscan facilitar tareas cotidianas, se trata de fomentar un uso responsable bajo los conceptos de la ciberseguridad.

Proteger a los usuarios y las organizaciones de amenazas cibernéticas es una prioridad, por lo cual una vez definido esto, se pretenden brindar aportes referentes al buen uso y buenas prácticas en dispositivos y sistemas *IoT* teniendo como finalidad concientizar a quien opere sobre los mismos en un entorno empresarial a través de la implementación de controles enfocados a la ciberseguridad en dispositivos *IoT* y buenas prácticas.

3) OBJETIVOS.

Objetivo general:

Exponer las limitaciones de seguridad en dispositivos *IoT* y el panorama actual en cuanto a guías, estándares y marcos de referencia para la evaluación de ciberseguridad enfocada a dispositivos *IoT* en un contexto de transformación digital para posteriormente desarrollar una propuesta de plan de trabajo, recomendaciones y matriz de controles que brinde herramientas básicas de conocimiento y monitoreo, y promueva la concientización frente al buen uso de dispositivos *IoT* principalmente con el fin de mejorar la seguridad en los mismos y prevenir ciberataques a causa de malas prácticas dentro de un entorno empresarial.

Objetivos específicos:

- Realizar una investigación referente a los antecedentes y estado del arte de dispositivos *IoT* y su evolución hasta la actualidad en cuanto a seguridad, innovación, regulaciones, riesgos y vulnerabilidades para entender si este aspecto ha sido una mejora o, por el contrario, ha pasado a segundo plano arriesgando los datos de sus usuarios.

- Conocer los diferentes vectores, aplicaciones, campos y arquitecturas en las que se hace uso de dispositivos *IoT* para entender las ventajas que trae su implementación, así como también sus desventajas para proponer mejoras en estas debilidades por el lado del proveedor y presentar ideas de buenas prácticas acordes al usuario final.

- Comparar las diferentes normativas referentes a la mejora o estandarización de la seguridad para dispositivos *IoT*, con el fin de brindar una conclusión que ayude a la supervisión y/o mejora de la seguridad al usuario de dispositivos *IoT*, por parte de sus fabricantes.

- Comparar las diferentes normativas referentes a la mejora o estandarización de la seguridad para dispositivos *IoT* a través de evaluaciones de ciberseguridad en empresas en la actualidad.

- Indagar respecto a la relación entre los desarrollos llevados a cabo para la creación de dispositivos *IoT* y comparar esto con estándares, metodologías o marcos de referencia orientados el desarrollo seguro de objetos inteligentes, tales como el *OWASP Top 10* para *IoT*.

- Desarrollar una propuesta para la evaluación de la ciberseguridad en dispositivos *IoT* para empresas en un contexto de transformación digital a través del desarrollo de una matriz de controles, un plan de trabajo y de una serie de consideraciones enfocadas al buen uso de dispositivos *IoT* en entornos empresariales.

4) HIPÓTESIS.

Actualmente, existen más dispositivos *IoT* interconectados que seres humanos, esto nos da una idea de la cantidad de datos que viajan por la red cada segundo. Si bien, estos dispositivos han traído grandes beneficios a las personas, empresas y gobiernos automatizando sus labores diarias, realizando predicciones para mejorar otras tareas, o, en conclusión, facilitando el día a día de sus usuarios, muchos fabricantes han comenzado a desarrollar un sinnúmero de dispositivos inteligentes que satisfagan la demanda de estos objetos que crece a pasos agigantados, lo negativo de este fenómeno es que los fabricantes se están enfocando en desarrollar dispositivos que realicen tareas específicas dejando de lado la seguridad de los mismos, siendo esto visible en fallas básicas como la transferencia de datos en texto plano o la solicitud de permisos innecesarios para el funcionamiento de ciertos dispositivos.

El problema no es la inclusión de estos objetos en el mercado, mucho menos el uso de los mismos, es la falta de implementación de medidas de seguridad en el desarrollo de estos dispositivos lo realmente preocupante, si bien estos objetos cumplen su labor de facilitar o automatizar la tarea del usuario, sin una buena barrera de seguridad, este dispositivo por mínima que sea la tarea que realice, puede representar la puerta de entrada para cualquier tipo de ciberataque. Es por esto que, la seguridad en dispositivos *IoT* debe ser el primer eslabón en su desarrollo, debe garantizar la protección de los datos de sus usuarios sin importar el tipo de dispositivo ya que una falta de cifrado de datos, la falta de actualizaciones periódicas o alguna otra mínima brecha en la seguridad del dispositivo puede llevar a ataques desde una estafa por ingeniería social a un usuario del común, hasta un *ransomware* a una gran compañía.

Por otro lado, la seguridad no puede ser totalmente responsabilidad del proveedor, los usuarios de dispositivos *IoT* deben conocer la importancia de sus datos, cómo y con quién los comparten pensando siempre en el peor escenario para así mantener un tomar acciones seguras. Lo ideal es educar usuarios inteligentes para el uso de objetos inteligentes.

Esta problemática se encuentra presente en cada entorno en donde se encuentre algún dispositivo *IoT*, pero es mayormente preocupante en un entorno empresarial, teniendo en cuenta que su inclusión representa el desarrollo de tareas cruciales dentro de la organización y una falla en las mismas puede derivar en problemas de gran escala, por lo

cual una serie de controles, buenas prácticas y recomendaciones son cruciales en estos entornos.

Teniendo en cuenta la problemática anteriormente mencionada y el enfoque de esta tesis, durante del desarrollo de la misma, se pretenden señalar los distintos riesgos a los que las empresas actualmente se encuentran expuestas al contar con baja seguridad en dispositivos *IoT*, esto se logra demostrar gracias a recursos como encuestas realizadas por compañías reconocidas, también, se realiza una investigación sobre las distintas herramientas, proveedores, regulaciones, *frameworks* y demás material relacionado con *IoT* en las empresas para evidenciar la falta de contenido enfocado a este ámbito desde la concientización, legalización y estandarización para las empresas, aunque también, se presentan distintos proyectos y herramientas útiles para mejorar la seguridad de los objetos inteligentes en las empresas.

Esta tesis pretende concientizar a los diferentes usuarios de dispositivos *IoT* respecto a las mejores prácticas y recomendaciones para el uso de estos objetos y prevenir ciberataques a través de estos. Principalmente, pretende ofrecer las bases para mantener un monitoreo constante dentro de las empresas a través de un manual de buenas prácticas, recomendaciones y una matriz de riesgos que reúna los controles necesarios para prevenir y detectar diferentes ciberataques principalmente a través de los dispositivos *IoT* dispuestos en el entorno laboral.

Se espera que el desarrollo de esta investigación, así como el aprovechamiento de las herramientas propuestas, sirvan como base para las empresas en proceso de transformación digital para robustecer sus procesos y prevenir ciber-ataques gracias al mayor control y monitoreo de sus dispositivos, a la concientización y al desarrollo de nuevas y mejores prácticas dentro de sus procesos.

5) MARCO TEÓRICO.

El abordaje de esta tesis se realiza desde una perspectiva social, legal, técnica y tecnológica. Se propone realizar una tesis de enfoque cualitativo ya que "utiliza la recolección de datos sin medición numérica para descubrir o afinar preguntas de investigación en el proceso de interpretación" (Hernández Sampieri, Fernández-Collado, & Baptista Lucio, 2018). Asimismo, se pretende realizar una investigación exploratoria en cuanto a la inducción de la tecnología de Internet de las Cosas en diferentes ecosistemas tales como empresariales, infraestructuras críticas, salud, *Smart Cities*, entre otros, ya que este tipo de investigación se ajusta al propósito de esta tesis siendo uno de sus objetivos lo definido en el libro *Metodología de la investigación* "Los estudios exploratorios sirven para familiarizarnos con fenómenos relativamente desconocidos, obtener información sobre la posibilidad de llevar a cabo una investigación más completa respecto de un contexto particular, investigar nuevos problemas, identificar conceptos o variables promisorias, establecer prioridades para investigaciones futuras, o sugerir afirmaciones y postulados" (Hernández Sampieri, Fernández-Collado, & Baptista Lucio, 2018). A partir de esto, se pretende indagar en cuanto a la situación actual respecto a las regulaciones, estándares, normas y marcos de referencias actuales asociadas a *IoT* y, asimismo, las soluciones ofrecidas en el mercado principalmente a empresas, respecto a evaluaciones de ciberseguridad enfocadas a *IoT*.

Para el desarrollo de esta tesis, se tomaron como fuentes y referencias grandes empresas con trayectoria y reconocimiento tecnológico tales como INCIBE (Instituto Nacional de Ciberseguridad en España), *OWASP*, *NIST, MIT, ISO,* además de algunas consultoras, gobiernos y proveedores cuyo trabajo relacionado a *IoT* fue objeto de estudio dentro de esta tesis.

5.1INTRODUCCIÓN Y SEGURIDAD EN DISPOSITIVOS *IoT*

Durante el desarrollo de este capítulo, se pretende abordar de manera general cada aspecto relacionado a dispositivos *IoT* desde el punto de vista de la Ciberseguridad. Se explicará su propósito, funcionamiento, ventajas, desventajas, ecosistemas, arquitectura, vectores, así como también algunos antecedentes en los cuales se evidencia cómo estos

dispositivos a los que se les deja de lado su seguridad y correcta configuración llegaron a representar la base para el desarrollo de ataques cibernéticos a gran escala, afectando no solamente sistemas digitales sino también objetos físicos. También, se indagará respecto a las diversas regulaciones, legislaciones y marcos legales alrededor del uso de dispositivos *IoT* a nivel mundial en la actualidad, también, se dedicará una parte de este capítulo a indagar sobre los distintos marcos de referencia, protocolos, estándares y vectores de ataque con el fin de conocer las principales vulnerabilidades de estos dispositivos en los diferentes campos de uso.

El objetivo general de este capítulo es dar a conocer las grandes ventajas de los dispositivos *IoT* en la actualidad cuando son utilizados correctamente, así como también, evidenciar las falencias en cuanto a su protección y seguridad tanto por parte de los proveedores como de sus usuarios, las cuales que pueden llevar a la creación de vulnerabilidades en entornos empresariales, institucionales, personales, entre otros, al no tener un correcto uso y control de estos.

5.1.1 QUÉ ES Y CÓMO FUNCIONA UN DISPOSITIVO *IoT*

Existen diversas definiciones respecto a la tecnología *IoT*, de acuerdo con el rol, sector o tipo de usuario, una definición puede variar de otra. En primer lugar, de acuerdo con el *IoT-GSI*[3], *IoT* se define como "*IoT* puede concebirse como una infraestructura global de la sociedad de la información, que permite ofrecer servicios avanzados mediante la interconexión de objetos (físicos y virtuales) gracias a la inter-operatividad de tecnologías de la información y la comunicación (*TIC*) presentes y futuras"[4].

Asimismo, Oracle, por ejemplo, la define como "El *Internet of Things* (*IoT*) describe la red de objetos físicos (cosas) que llevan sensores integrados, *software* y otras tecnologías con el fin de conectar e intercambiar datos con otros dispositivos y sistemas a través de Internet. Estos dispositivos abarcan desde objetos domésticos cotidianos hasta sofisticadas herramientas industriales."

Estas definiciones, junto con algunas dadas por importantes instituciones, coinciden en que *IoT* hace referencia a objetos con componentes como sensores integrados que tienen

[3] *Internet of Things – Global Standards Initiative*
[4] Recomendación ITU-T Y.2060 (06/2012). "Serie Y: Infraestructura mundial de la información, aspectos del protocolo internet y redes de la próxima generación"

la capacidad de conectarse con otros dispositivos para intercambiar datos y tomar decisiones independientemente de la interacción humana. Estos dispositivos trabajan de la mano con diversas tecnologías y plataformas permitiendo la recolección y análisis de datos desde las direcciones IP de todos los dispositivos interconectados.

IoT hace referencia no solamente a la interconexión entre dispositivos a través de Internet, se trata de una tecnología que reúne personas, procesos y datos para así poder hacer una integración entre entornos físicos y digitales.

Dentro del entorno de dispositivos *IoT* se puede hacer una segregación en dos grandes grupos, en primer lugar, los dispositivos inteligentes, los cuales se pueden interconectar a través de estándares como *wifi, Zigbee, bluetooth*, entre otros. Algunos ejemplos de estos dispositivos son los *Smart TVs*, *HVACs*[5], cafeteras inteligentes, dispositivos de iluminación o alarma.

Por otro lado, se encuentran los dispositivos de detección, que son aquellos que cuentan con sensores y actuadores que permiten el monitoreo de parámetros como la intensidad de la luz, humedad o temperatura.

Estos dispositivos envían toda su información a través de puertas de enlace, los cuales se encargan de procesar la información capturada por los sensores y es enviada posteriormente a la nube, la cual actúa como unidad de procesamiento y de almacenamiento.

IoT surge con la idea de un mundo conectado, por lo cual se encuentra presente en la cotidianidad así lo entendamos o no. Actualmente se habla de *Smart Cities*, domótica, industria 4.0 y algunas tecnologías como *Big Data*, inteligencia artificial (IA), *Machine Learning* o conectividad en la nube y todo esto hace parte de la tecnología *IoT* ya que siguen el mismo principio de conectividad en diferentes campos.

La combinación de estas tecnologías llegó a definirse en algún momento como *IoE* (*Internet of Everything*), aunque posteriormente, este término fue utilizado por Clive Longbottom, cofundador y director de Quocirca, una empresa de investigación y análisis con foco en el mercado europeo, quien utilizó este término para referirse a los datos provenientes de dispositivos *IoT* dentro de una organización, esto sin hacer diferencia entre dispositivos inteligentes personales o institucionales, sino como un conjunto de *IoT*.

Los dispositivos *IoT*, comparten componentes con los computadores tradicionales, estos son el *hardware*, sistema operativo, *software* y redes de comunicación. En el caso de

[5] *HVACs* hace referencia por sus siglas en inglés a la calefacción (*Heating*), ventilación (*Ventilating*) y aire acondicionado (*Air Conditioned*).

los dispositivos inteligentes, adicional al *hardware* que contiene transistores y al *firmware* que enlaza este con el sistema operativo, permite la interacción con los demás componentes. Adicional, se establecen diferentes reglas o instrucciones que condicionan al dispositivo a realizar ciertas tareas o tomar ciertas decisiones de acuerdo con las diferentes circunstancias.

Adicional a los componentes tradicionales, lo que realmente hace la diferencia en un dispositivo *IoT*, son los sensores, datos, redes de comunicación y servicios en la nube.

Estos sensores son los encargados de detectar distintos eventos en el ambiente y enviar esta información a los demás dispositivos, la funcionalidad de estos componentes se potencia al integrarse con las demás funcionalidades de *IoT*.

Los datos incluyen toda la información que el dispositivo recibe y maneja de acuerdo con las instrucciones configuradas en su *software*. Los servicios en la nube proveen la combinación de programas y datos a los cuales se puede acceder desde Internet.

A través de la tecnología *M2M* o *Machine-to-machine*, *IoT* permite que los dispositivos conectados a una misma red interactúen compartiendo datos para realizar tareas sin necesidad de un intermediario, este tipo de comunicación es utilizado principalmente con fines de automatizar pequeños espacios, como casas u oficinas ya que comparten cantidades mínimas de información, por ejemplo, en bombillos inteligentes, cerraduras o interruptores que realizan funciones básicas como encendido y apagado.

Pero además de este modelo de comunicación, *IoT* ofrece también la conexión machine-to-*Cloud*, ya que los proveedores mantienen sus datos en la nube de tal forma que la máquina debe comunicarse con ella para recibir los datos y actuar de acuerdo con lo solicitado, lo cual supone una posible brecha de seguridad al no tener en cuenta la comunicación entre el dispositivo y el api del proveedor en la nube. Este tipo de comunicación se encuentra presente en termostatos o *Smart TVs*, los cuales interactúan con bases de datos en la nube para analizarlos y tomar decisiones.

También, existen las arquitecturas *machine-to-gateway* (dispositivo a puerta de enlace) en donde la puerta de enlace funciona como intermediario entre el dispositivo y la nube, ya que funciona como *software* de aplicación brindando seguridad a la comunicación a través de protocolos. Este modelo se encuentra presente en los dispositivos de entrenamiento o monitores de salud y similares.

Finalmente, *Back-End Data-Sharing*, en donde se intercambian datos a través del *back-end*, es decir, es posible exportar, modificar y analizar datos provenientes de dispositivos inteligentes desde un servicio en la nube u otras fuentes.

El Internet de las Cosas también llamado *Internet de Todo* (o *IoE*, *Internet of Everything* por sus siglas en inglés) por *Cisco* y otras empresas, agrupa personas, datos, procesos y objetos, y estos entre sí se relacionan de distintas formas. Esto significa, que además de la comunicación *M2M* o máquina a máquina, también se presentan relaciones *P2P* o persona a persona y de igual manera de máquina a datos.

Cada uno de estos aspectos es de vital importancia dentro de la definición de Internet de las Cosas o Internet de Todo. En un contexto empresarial en el que las personas se encuentran conectadas, la información llega a la persona o el objeto indicado en el momento preciso, los objetos se encuentran conectados entre sí a través de Internet y los datos brindan información valiosa para la toma de decisiones, es posible aumentar la productividad de los empleados, mejorar los procesos, brindar calidad en la atención al cliente, innovar y aprovechar los recursos, entre otras ventajas.

Actualmente, la inducción de dispositivos *IoT* se encuentra en aumento ya que estos objetos representan innovación, automatización, optimización y avance en distintos campos tales como la industria de la salud, transporte, *retail* o venta minorista, agricultura, farmacéutica, entre otros, además del consumidor común.

Internet de las cosas logra además unificar la tecnología de la información (IT) con la tecnología de las operaciones (OT) al estar presente tanto en el área industrial como en el área de los procesos o negocios dando lugar a la transformación digital e industrial, conocida también como industria 4.0.

De acuerdo con el propósito de un dispositivo *IoT*, pueden converger múltiples tecnologías como 5G, *blockchain*, la nube, inteligencia artificial, *Big Data*, entre otros, las cuales ayudan a la recopilación y análisis de datos desde los diferentes nodos y puertas de enlace *IoT*.

Internet de las cosas es un término que abarca diversos ecosistemas, por lo cual se ha dado lugar a la creación de nuevos términos de acuerdo con su campo de uso y aplicaciones, por ejemplo, *CIoT* para hacer referencia al Internet de las cosas del consumidor, *IIoT* para Internet de las cosas industrial, *IoRT* para Internet de las cosas robóticas o *IoMT* para Internet de las cosas de dispositivos médicos por nombrar algunos ejemplos, la realidad es que *IoT* ha dado lugar a nuevos términos para explicar diferentes formas de uso de Internet de las Cosas.

Dentro de Internet de las Cosas del Consumidor (*CIoT*) se encuentran varias aplicaciones que surgen de las necesidades y el día a día de las personas, se conectan a través de Internet para recopilar y analizar datos de acuerdo con parámetros como

ubicación, temperatura, entre otros, y, normalmente son controladas y monitoreadas desde una *tablet* o *Smartphone*, este es el caso de los *wearables*, objetos inteligentes para el hogar, la salud, *fitness*, servicios al consumidor, vehículos, entre otros.

Por otro lado, existe desde hace muchos años una serie de objetos que no se encuentran conectados a Internet, no cuentan con una dirección IP, pero son utilizados en ámbitos principalmente industriales o *Smart Cities*, se trata de dispositivos para el control y monitoreo de la energía, transporte, agricultura, seguridad, *Smart Grid*, entre otros. Estos dispositivos al ser reemplazados o modernizados pasan a formar parte del ecosistema de Internet Industrial de las Cosas (*IIoT*).

Es claro que los dispositivos *IoT* hacen uso de tecnologías bastante sofisticadas y desarrolladas, además de manejar datos, aspectos y decisiones en muchos casos sensitivos, esto es totalmente opuesto al nivel de seguridad y privacidad que ofrecen en su mayoría bajo una fachada de seguridad física, velocidad e innovación.

El Internet de las cosas robóticas (*IoRT*) si bien no es un término muy popular, es bastante utilizado principalmente en entornos industriales. Este término, ideado por *ABI research*[6] en su publicación El *Internet de las cosas robóticas* define este término como el momento en el cual "los dispositivos inteligentes pueden monitorear eventos, fusionar datos de sensores de una variedad de fuentes, usar *inteligencia* para determinar el mejor curso de acción y luego actuar para controlar o manipular objetos en el mundo físico y, en algunos casos, mientras se mueven físicamente a través de ese mundo. La incorporación del aspecto robótico en el *IoT* más amplio transforma el panorama actualmente dominado por los modelos de negocios construidos sobre la interacción pasiva en relaciones dinámicas y físicas entre el mundo digital y físico."[7]

Si bien, *IoT* se considera una de las tecnologías emergentes que avanza con mayor fuerza debido a la expansión de la conectividad en Internet o al bajo costo de los sensores, también se encuentra con algunas barreras dentro del mercado tales como problemas de implementación y por supuesto la falta de seguridad y privacidad en sus dispositivos. *IoT* ha venido tomando lugar en el mercado de las tecnologías no solo debido a la adopción de estos dispositivos en ambientes industriales o dando lugar a lo que hoy se conoce como domótica o *Smart Cities*, también, *IoT* aparece para eliminar las barreras antes existentes entre las tecnologías de la información y tecnologías de la operación, comúnmente

[6] Equipo mundial de analistas que ayuda a las organizaciones a alcanzar la transformación digital a través de investigaciones, conocimientos prácticos y orientación estratégica.
[7] https://www.abiresearch.com/press/the-internet-of-robotic-things-iort-greatly-expand/

conocidas como *IT* y *OT*, respectivamente, gracias a componentes como actuadores o sensores, comienzan a converger estas tecnologías.

Básicamente este concepto propone llevar *IoT* al siguiente nivel mediante la optimización de sensores, mejora en los sistemas de monitoreo y la capacidad de integrar datos de otros sensores, estos dispositivos tendrán la capacidad de fusionar distintos datos, analizarlos y tomar de forma independiente decisiones y realizar determinadas acciones dentro de un rango predefinido, de esta forma, este dispositivo podrá operar no sólo en el mundo digital, sino también, en el mundo físico.

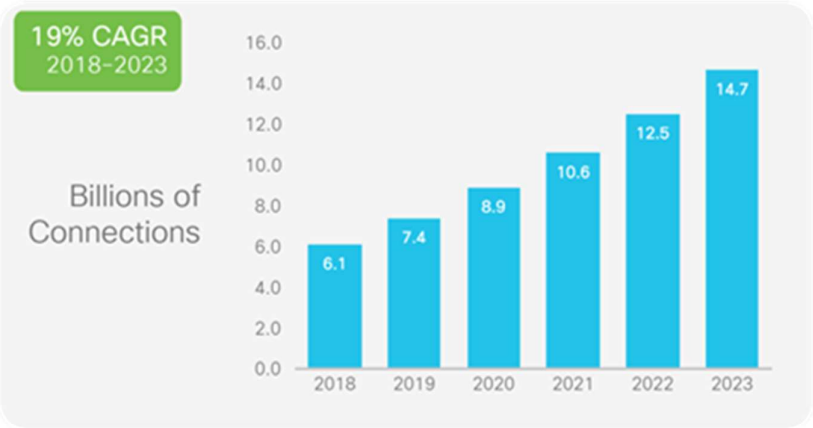
En resumen, los componentes de IoRT son tres, en primer lugar, un dispositivo inteligente con capacidad de monitoreo y datos de sensores de otras fuentes. En segundo lugar, la capacidad de análisis del dispositivo de acuerdo con los eventos que está monitoreando y los diferentes datos a los que tiene acceso. Finalmente, en tercer lugar, la fusión de diferentes datos (de origen e incorporados) junto con inteligencia, lo cual permite le permite al dispositivo determinar acciones para tomar control de objetos en el mundo físico.

Como se mencionó anteriormente, es un término no muy popular hoy en día pero es una realidad, principalmente en el entorno industrial donde se hace uso de ro*bots* dentro de los procesos de fabricación, logística, almacenamiento, entre otros, estos ro*bots* colaborativos o también llamados *cobots* son aquellos ro*bots* que trabajan de la mano de los empleados para brindar soporte en tareas repetitivas, existen también los ro*bots* industriales los cuales están diseñados para realizar tareas específicas sin intervención humana.

De acuerdo con el Informe Anual de Internet (2018 – 2023) de *Cisco*[8], se espera que para el año 2023 existan cerca de 14.7 mil millones de conexiones de dispositivos M2M como se indica en la **Figura 1**, lo cual significa que habrá 1.8 conexiones para cada miembro de la población mundial en este año.

[8] Compañía líder en la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.

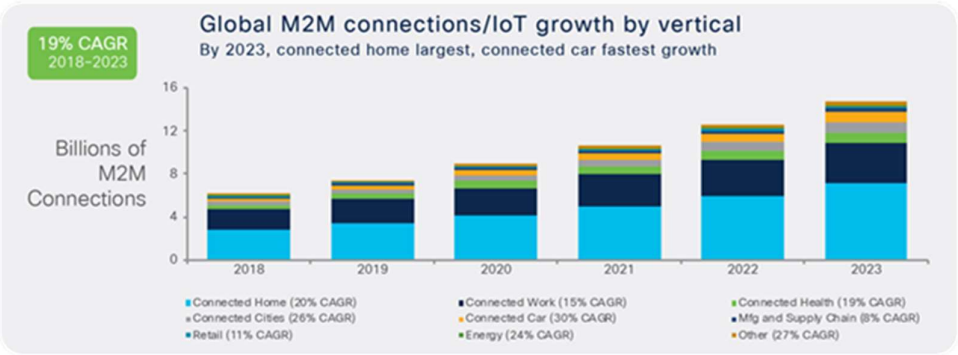
Figura 1. *Crecimiento global de conexiones M2M*



Nota. Tomado de *Global M2M connection growth*, por *Cisco* Annual Internet Report, 2018–2023, 2020, *Cisco* (https://www.*Cisco*.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html)

También, de acuerdo con este mismo informe, se estima que para el año 2023 la mayor parte de las conexiones sean por dispositivos para la automatización del hogar, seguridad, vigilancia, electrodomésticos y aplicaciones de monitoreo. Por otro lado, los carros inteligentes se ubican como la categoría con mayor crecimiento, seguido por la conectividad de ciudades inteligentes, tal como se evidencia en la **Figura 2.**

Figura 2. *Crecimiento global de conexiones M2M por industrias*



Nota. Tomado de *Global M2M connection growth by industries*, por *Cisco* Annual Internet Report, 2018–2023, 2020, *Cisco* (https://www.*Cisco*.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html)

Cisco asegura en su reporte también, que, si bien hoy en día la mayor parte del tráfico de conexiones vienen de dispositivos de usuario final tales como *Smartphone*s, *Smart* TVs o computadores, la cantidad de tráfico aumentará más rápido que el número de conexiones debido al crecimiento en el desarrollo de numerosos dispositivos *IoT* en diferentes industrias, los cuales van a requerir una menos latencia y mayor ancho de banda.

Este reporte indica que la expansión global de *IoT* es un hecho. De acuerdo con el informe *Señales de IoT* de *Microsoft*[9], "el 91 por ciento de los responsables de la toma de decisiones en materia de *IoT* manifestó haber implementado la tecnología en 2020 frente a un 85 por ciento que había respondido afirmativamente en 2019. Además, ocho de cada 10 indicaron tener un proyecto en fase de utilización (frente a los siete de cada diez del año precedente)."

5.1.2 ANTECEDENTES

El término *Internet de las Cosas* se atribuye al británico Kevin Ashton quien en 1999 lo empleó para hacer referencia a los dispositivos que podían conectarse a Internet haciendo uso de sensores.

Según el Grupo de Soluciones Empresariales para Internet de *Cisco* (IBSG), *IoT* marcó su inicio durante el 2008 y 2009, momento en el que existían más dispositivos conectados a Internet, que personas en el mundo. A partir de ese momento, ha crecido considerablemente llegando a verse en prácticamente cualquier industria, lo cual tiene sentido ya que *IoT* tiene también como objetivo, ser masivo.

Si bien, hoy en día podemos ver *IoT* en cualquier parte, esta tecnología aún se encuentra en proceso de innovación, todo lo que se puede construir y facilitar a partir de este paradigma se encuentra en constante evolución. Cada día se desarrollan nuevos objetos, protocolos, surgen nuevos proveedores con soluciones innovadoras, y esto no solamente con la idea de satisfacer la demanda o innovar, también sucede ya que *IoT* logra interactuar con otras tecnologías tales como *Cloud*, *blockchain*, *Big Data*, *Machine Learning* o inteligencia artificial; esta integración de tecnologías hace que *IoT* crezca a pasos agigantados dentro de la sociedad.

Un ejemplo de ataques mediante *IoT* y tal vez el más sonado es el del *botnet Mirai*, entendiendo un *botnet* como un conjunto de dispositivos en una red, llamados *bots* o *zombies* los cuales son infectados por un *malware* y controlados de forma remota.

[9] Multinacional tecnológica que tiene como objeto el desarrollo, fabricación, entrega de licencias y producción de *software* y *hardware* electrónico.

Un *botnet* puede realizar distintos tipos de ataques como los de *DDOS*, infectar dispositivos o utilizarse para la minería de bitcoins[10].

El objetivo del *botnet Mirai* son los dispositivos *IoT*, principalmente *routers* o enrutadores, cámaras *IP*, impresoras, grabadoras de video, entre otros. En 2016, esta *botnet* recopiló cerca de 24000 dispositivos *IoT* con los cuales logró afectar los servidores del proveedor alemán de servicios *DNS* Dyn, uno de los proveedores más importantes de nombres de dominio para empresas. Se calcula que la *botnet* infectó cerca de 380000 equipos en 164 países viéndose afectadas compañías como *Twitter*, *GitHub*, Paypal, Visa, Spotify, BBC, The New York Times, *Amazon*, entre otros.

El propósito del *botnet Mirai* era principalmente coordinar ataques *DDOS* infectando dispositivos *IoT*, además de localizar y comprometer nuevos equipos para aumentar su red. El *malware* dentro de los *bots* que se encontraban comandados por un servidor de comando y control remoto contaba con un directorio de 62 usuarios y contraseñas comunes y por defecto con las cuales intentaba acceder a los distintos dispositivos. Una vez logrado el acceso, *Mirai* infectaba estos dispositivos y a través de la comunicación con el servidor de Comando y Control se daba lugar al ataque. *Mirai* podía ejecutar distintos tipos de ataque *DDOS*, entre ellos inundación *HTTP* en donde se envían varias solicitudes *HTTP* pretendiendo ser reales, *SYN flood* siendo este un tipo de denegación de servicios en donde se inicia la conexión a un servidor pero no se finaliza, entre otros ataques.

Poco después del ataque, el código fuente de este *botnet* fue publicado en *GitHub*[11] y actualmente se encuentra disponible al público y se han identificado diversas variantes de este *botnet* en las cuales se han actualizado la lista de credenciales y en casos como la cepa *Torii*, descubierta por Avast, contaba con nuevos componentes de vigilancia y su objetivo no era coordinar ataques *DDOS* sino robar información.

En 2014, se había registrado actividad del *malware Gafgyt* también conocido como *BASHLITE*, el cual explotaba vulnerabilidades conocidas en *routers* de pequeñas empresas conocidas como *SOHO* (*Small office/Home office* o pequeñas empresas/trabajo desde casa) y posteriormente efectuaba ataques *DDOS*.

Similar a *Mirai*, se han encontrado otros *malware* enfocados al ataque de dispositivos *IoT* como es el caso del *malware Hajime* que construye una cadena de *bots*

[10] Criptomoneda o moneda virtual y sistema de pago descentralizado utilizado para adquirir productos y servicios.
[11] Plataforma para la creación y alojamiento de código para colaboración y control de versiones.

P2P buscando puertos *Telnet* abiertos, este fue descubierto en 2016 y a la fecha aún no se conoce el objetivo del mismo.

También, en 2017 apareció el *malware Persirai* el cual tiene como objetivo las cámaras *IP* el cual busca puertos *UPnP* (*Universal Plug and Play* por sus siglas en inglés) abiertos, el objetivo una vez vulneradas las cámaras es conectarlas a un servidor de comando y control para conectar el dispositivo vulnerado a una red de *bots* con el fin de provocar un ataque *DDOS*.

Posteriormente, el 27 de noviembre de 2017, la compañía enfocada en encontrar *botnet*s, 360 NetLab, reportó el *malware Satori* el cual también vulneraba dispositivos para realizar ataques *DDOS*, recientemente, en 2018, se descubrió una nueva variante de *Satori* la cual afecta la plataforma de minería *Claymore* y su función era reemplazar las credenciales del propietario con las del atacante.

Otro caso bastante conocido en cuanto a ataques cibernéticos es el del gusano *Stuxnet*, este ataque ocurrido en enero del 2010 en la planta nuclear de Natanz en Irán, es llamado también como el primer ciberataque al mundo físico. Según Symantec, firma de seguridad cibernética, la inducción del virus en la planta nuclear fue a través de una USB infectada, una vez dentro de la red de la planta, el gusano ubicó el *software* encargado de controlar las máquinas centrifugadoras, esto ya que, *Stuxnet* fue creada con el objetivo de espiar y reprogramar los sistemas SCADA[12]. Una vez ubicado el *software* que controlaba las centrifugadoras, hizo que estas giraran a gran velocidad durante aproximadamente 15 minutos y luego volvieran a su velocidad normal, posteriormente, un mes después, desaceleró las centrifugadoras durante aproximadamente 50 minutos. Este comportamiento se repitió durante varios meses en distintas ocasiones. Este comportamiento después de un tiempo llevó a la autodestrucción de las máquinas, cerca de 1000 máquinas las cuales representaban el 20% de las centrifugadoras, quedaron fuera de servicio.

Este gusano estaba programado para ubicar el *PLC* (Controlador lógico programable) encargado de del control de velocidad de las máquinas, en caso de no contar con los requisitos específicos, *Stuxnet* no hacía nada en estos equipos. *Stuxnet* logró no ser detectado ya que utilizaba una firma digital que simulaba ser legítima por lo cual Windows no detectó este virus.

El o los responsables de este virus no se conoce a la fecha, aunque se tienen sospechas de tratarse de un sabotaje al programa nuclear de Irán.

---

[12] Sistema de supervisión, control y adquisición de datos comandado en remoto utilizado en entornos industriales.

Los anteriores ejemplos de ataques perpetrados a través de dispositivos *IoT* demuestran que, en muchos casos, la vulnerabilidad se debe a dispositivos *IoT* con baja o nula seguridad que son utilizados como puerta de entrada a grandes ataques.

Dentro de otros ejemplos de ataques a través de dispositivos *IoT* se encuentra el espionaje que se realizaba a través de la muñeca infantil *Cayla* la cual fue prohibida en Alemania, también las vulnerabilidades de seguridad encontradas en los marcapasos fabricados por los laboratorios *Abbott*[13] (anteriormente *St. Jude Medical*) o en casos más recientes, las noticias de acceso no autorizado en los automóviles eléctricos *Tesla*[14].

Cayla, al estar conectada a internet entra a ser parte del ecosistema *IoT*. Esta muñeca infantil fue acusada de espionaje al grabar permanentemente las conversaciones que los niños tenían con ella, sometiéndolos a una vigilancia permanente, además de no estar bajo ninguna norma de protección de datos.

De acuerdo con la *BBC*[15], el 6 de diciembre de 2016 el Centro de Información sobre la privacidad electrónica de E.E.U.U, el Centro para la Democracia Digital, la Campaña por una Infancia Libre de Comerciales y la Unión de Consumidores presentaron una queja hacía *Genesis Toys* y *Nuance Communications*, proveedores del *software* de este juguete.

De acuerdo con expertos en ciberseguridad que estudiaron el funcionamiento de *Cayla*, la muñeca recopila una serie de información personal de los niños y su entorno, partiendo por lo más básico, para vincular un dispositivo móvil a *Cayla*, la aplicación no pide ningún tipo de emparejamiento, además de permitir la conexión a varios metros de distancia. Además, este dispositivo cuenta con un micrófono con el cual se conecta a través de *bluetooth* para interactuar con las personas, a través de esto logra capturar todo tipo de conversaciones en todo momento.

En esta muñeca fue encontrada una falla tecnológica que permitía vulnerar este dispositivo. Respecto a esto no se recibió solución o una respuesta contundente ya que los proveedores del *software* afirman que se trata de un caso aislado.

Adicionalmente, se afirma que la muñeca a través de sus frases pregrabadas hacia marketing a Disney, mencionando sus películas y parques temáticos siendo este un problema de irregularidades publicitarias.

---

[13] Farmacéutica Estadounidense que ofrece productos de nutrición, herramientas de diagnóstico, dispositivos médicos y productos farmacéuticos.

[14] Empresa Estadounidense fabricante de automóviles liderada por Elon Musk.

[15] El *British Broadcasting Corporation* es un reconocido servicio público de radio y televisión en Reino Unido.

Finalmente, se descubrió también que los fabricantes pueden cambiar sus términos y condiciones en cualquier momento, ampliando la brecha de vulnerabilidades en estos dispositivos.

Lo que se definió al final de esta publicación e investigación, fue recomendar a los padres desconectar la muñeca cuando no se esté utilizando y mantener los dispositivos móviles asociados actualizados y protegidos con contraseñas robustas. Aunque también, en otros casos se tomaron medidas más radicales, como en Alemania en donde en febrero de 2017 fue prohibida la venta de esta muñeca bajo el riesgo de espionaje y se ordenó a los padres que la adquirieron, destruirla.

En casos similares de juguetes para niños definidos como peligrosos para niños al ser interactivos con riesgo de comprometer la privacidad de los menores se encuentra el robot i-Que, de los mismos proveedores de *Cayla*, *Hello Barbie* de *Mattel*, *Furby Connect*, *CloudPets*, entre otros.

Durante 2017, la Administración de alimentos y medicamentos de E.E.U.U (FDA por sus siglas en inglés) encontró que 465.000 marcapasos fabricados por *Abbott* se encontraban vulnerables y por lo cual deberían actualizar su *firmware*.

Esta noticia resulta bastante preocupante ya que, aunque no se hizo pública la forma explícita en la que un atacante podría vulnerar estos dispositivos médicos, resulta bastante alarmante pensar siquiera en la posibilidad de que una persona ajena pueda controlar este tipo de dispositivos en un paciente.

Afortunadamente, si bien se encontró esta vulnerabilidad en seis modelos diferentes de marcapasos *Abbott*, no se registraron casos de hackeo en dispositivos fuera del laboratorio, de igual forma en su momento se llevó a cabo una demanda y posteriormente *Abbott* tuvo que publicar e instalar una actualización en el *firmware* de estos dispositivos.

A principios de 2022, un joven alemán de 19 años aseguró hackear más de 25 carros *Tesla* en 13 países diferentes a través de un fallo de seguridad en el *software* sobre el cual hizo publicaciones en *Twitter* y detalló a más profundidad en su blog bajo un artículo llamado *¿Cómo tuve acceso a más de 25 Tesla alrededor del mundo? Por Accidente. Y curiosidad,* en donde inicia su narrativa aclarando que la vulnerabilidad encontrada no era de la infraestructura de *Tesla* directamente sino de errores causados por los dueños de los autos, adicionalmente narra cómo llegó a descubrir esta vulnerabilidad hoy publicada como CVE-2022–23126 y da una extensa e interesante explicación de su proceso antes de encontrar el fallo de seguridad, lo cual se dio de casualidad ya que se encontraba auditando una compañía en Francia, también las diversas comunicaciones e

información compartida respecto a esto con los terceros afectados y finalmente el seguimiento que se dio y las acciones llevadas a cabo posterior a la publicación de lo encontrado.

Colombo afirmó que podía encender el sonido del auto, las luces, bloquearlo o desbloquearlo, verificar si el conductor se encontraba presente y además conocer la ubicación exacta de carro, velocidad máxima, estilo de conducción entre otros datos. *NVD*[16] describe que la vulnerabilidad *CVE-2022–23126* "permite a los atacantes abrir las puertas de los vehículos *Tesla*, iniciar la conducción sin llave e interferir en el funcionamiento del vehículo en ruta. Esto ocurre porque un atacante puede aprovechar el acceso de inicio de sesión de *Grafana*[17] para obtener un token para las llamadas a la *API* de *Tesla*."

En su artículo *Colombo* afirma que el problema de seguridad se centraba en el *TeslaMate* ya que esta plataforma es la que almacena la información confidencial necesaria para vincularse al auto, también afirma que intentó notificar a los propietarios de los *Tesla* vulnerados, pero no lo logró y finalmente comunicó la falla a *Tesla* quienes a los pocos días lanzaron el parche dando solución a la falla.

Los ejemplos de vulnerabilidades en dispositivos *IoT* son múltiples y siguen surgiendo día a día, lo cual seguirá sucediendo mientras no exista una regulación sobre seguridad en estos dispositivos, y del lado de proveedor se tomen las precauciones necesarias para mantener seguros sus dispositivos.

Tal como el ejemplo de los autos *Tesla* vulnerados, el acceso a los datos personales de los usuarios se debe a que ellos mismos no protegen su información confidencial a través de claves robustas o herramientas como el *2FA* o segundo factor de autenticación, acciones como estas son las que les dan ventaja a los hackers para vulnerar fácilmente distintos dispositivos tomando control sobre ellos o accediendo a información que no deberían.

Actualmente existe un buscador de dispositivos, dentro de los cuales se encuentran los *IoT*, bastante conocido llamado *Shodan* el cual ha sido clasificado como peligroso debido a la cantidad de información que contiene. Este buscador se encarga de indexar todos los dispositivos y servidores conectados a internet a través de un escaneo por

---

[16] Base de datos nacional de vulnerabilidades de E.E.U.U (*NVD* por sus siglas en inglés) es un proyecto del gobierno de Estados Unidos que contiene listas de los diferentes controles, errores, fallos de seguridad, nombres de productos y métricas de gran impacto.

[17] Herramienta de *software* libre que permite la visualización y ejecución de análisis de datos a través de distintas métricas.

diferentes puertos y clasificarlos brindando información bastante completa de los mismos (ubicación geográfica, *ISP, CVEs*[18] asociadas, puertos, servicios, entre otros), esto si bien puede ser una ventaja, por ejemplo, en trabajos de auditoría, puede representar también un gran vector de ataque al ser utilizado como fuente para encontrar equipos a vulnerar.

5.1.3 VENTAJAS Y DESVENTAJAS EN DISPOSITIVOS *IoT*

IoT supone una mejora en la calidad de vida de las personas, se basa en la eficiencia y la rapidez. Actualmente es posible hacer de cualquier objeto común un objeto inteligente agregándole ciertas funcionalidades que le permitan la interacción y la comunicación con otros dispositivos *IoT*, aprendiendo y compartiendo datos que ayuden al usuario. A partir de todos los datos que entregamos a nuestros dispositivos *IoT*, se pueden generar estadísticas o predicciones que pueden ayudar a la toma de decisiones que representen una ventaja sobre nosotros, reducción de costos o tiempo, por ejemplo.

Adicionalmente, muchas aplicaciones pueden funcionar como complemento de objetos convencionales, por ejemplo, en el caso de la seguridad, existen alarmas, cerraduras, sensores y otros objetos *IoT* que combinados con las medidas tradicionales pueden reforzar la seguridad de una casa u oficina.

A gran escala, combinando *IoT* con redes como la actual 5G, se podría pensar en el concepto de *Smart Cities*, lo cual trae inmensas ventajas en la sociedad. A través del despliegue de diversos dispositivos *IoT* es posible mejorar los servicios que se ofrecen, tales como iluminación, transporte, recogida de basuras, tránsito, agua, alumbrado, entre otros. Tener ciudades conectadas, recolectando datos, los cuales pueden ser analizados para la toma de decisiones, puede repercutir en asuntos globales tales como la sustentabilidad, lo cual de la mano de *IoT* podría utilizarse en la detección temprana de desastres naturales en los que se puedan tomar medidas preventivas o reactivas, también en el control de emisiones para reducir la contaminación.

En fin, el buen uso de dispositivos *IoT* trae consigo grandes ventajas que suponen la mejora en la calidad de vida de sus usuarios, ya sea como individuos, empresas, gobiernos o ciudades enteras.

---

[18] *Common Vulnerabilities and Exposures*, por sus siglas en inglés. *CVE* hace referencia a la clasificación sobre vulnerabilidades de seguridad conocidas.

Un mal uso o desconocimiento en la manipulación de estos dispositivos *IoT* puede traer grandes problemas de seguridad y privacidad, las cuales son las principales desventajas de estos objetos. Al ser dispositivos menos controlados, protegidos y encontrarse activos 24/7, por lo general, pueden convertirse en dispositivos puente para el desarrollo de un ataque cibernético como un *ransomware*, phishing o hacer parte de un ejército de *bots* para un ataque *DDOS*.

Dado que estos dispositivos, a diferencia de *tablet*s, computadores o celulares, no cuentan con antivirus, antispyware o anti*malware*, y por lo general no reciben actualizaciones de seguridad, es necesario tomar medidas y realizar una buena configuración antes de conectarlo a una red y hacer uso de este. Estas medidas deben tomarse no sólo sobre el dispositivo sino también sobre la red misma, más aún teniendo en cuenta el fenómeno de Shadow *IoT*, el cual al no ser controlado pueden convertirse en precursores o facilitadores de una gran brecha de seguridad.

En cuanto a la privacidad, es importante estudiar al fabricante, conocer qué servicios solicita y desactivar aquellos que no sean necesarios para el desarrollo de sus tareas. También, revisar las políticas de privacidad, teniendo en cuenta que entre más dispositivos *IoT* se encuentren en comunicación, más datos se transmitirán, los cuales pueden revelar información referente a hábitos, salud, búsquedas, seguridad, entre otros. Si el fabricante no cuenta con una robusta política de privacidad, es probable que estos datos puedan ser vendidos a otras empresas, y entonces, los dispositivos *IoT* además de facilitarnos las tareas diarias, pueden convertirse en objetos de espionaje.

De acuerdo con el informe *Señales de IoT* realizado por *Microsoft* en 2020, dentro de los principales beneficios de *IoT* en las empresas, de acuerdo con los encuestados, se encuentra el aumento en el rendimiento (86 %) y la eficiencia (79 %) ya que las empresas utilizan *IoT* principalmente para aumentar la eficiencia operativa y productiva. Las empresas encuestadas indican también que *IoT* les permite ser más productivos (47%), reduce errores humanos (44%) lo cual contribuye a la calidad de la empresa, y en menor medida, los encuestados manifiestan que *IoT* les permite hacer nuevos tipos de ofrecimientos a los clientes (37%) y también les abre las puertas a nuevas vías de ingresos (34%) de acuerdo con la **Figura 3.**

Por otro lado, existe también una serie de obstáculos indicados por los encuestados para hacer un mayor uso de *IoT* en sus empresas. Tal como se indica en la **Figura 4**, dentro de los principales obstáculos se encuentran la carencia de recursos internos, la complejidad y los problemas técnicos. Encabezando la lista se encuentra la continuidad en la

implementación de la solución de *IoT* existente (33%), seguido por la búsqueda de soluciones a problemas actuales (31%). También, los encuestados manifestaron preocupación por la privacidad de sus consumidores (26%) además de insuficiencia en la formación sobre cómo implementar el *IoT* (26%), falta de conocimientos técnicos (26%), falta de información (24%) y, en menor medida, se encuentra la negativa a almacenar datos en la nube pública (20%).

Figura 3. *Beneficios del IoT en las empresas*

Nota. Tomado de *Beneficios del IoT* (p.15), por *Microsoft*, 2020, *Microsoft* (https://azure.*Microsoft*.com/mediahandler/files/resourcefiles/*IoT*-signals/es-es/*IoT*%20Signals_Edition%202_Spanish.pdf)

Figura 4. *Obstáculos para utilizar más el IoT*

Nota. Tomado de *Obstáculos para utilizar más el IoT* (p.17), por *Microsoft*, 2020, *Microsoft* (https://azure.*Microsoft*.com/mediahandler/files/resourcefiles/*IoT*-signals/es-es/*IoT*%20Signals_Edition%202_Spanish.pdf)

Además de los problemas de seguridad anteriormente mencionados respecto a dispositivos *IoT*, también hay un tema importante el cual representa una fuerte desventaja de estos objetos inteligentes, y es que debido a la falta de estandarización técnica en *IoT*, muchas veces se presentan problemas de incompatibilidad entre dispositivos lo cual limita su correcto funcionamiento.

5.1.4 ARQUITECTURA

Dentro de una arquitectura general de *IoT* se deberían tener en cuenta las siguientes capas: física, capa de conectividad y unidades de procesamiento, *Edge Computing*, *Cloud*, aplicaciones, gestión de datos y seguridad. Dicha arquitectura reúne los dispositivos físicos, *hardware*, *software*, protocolos, estándares de red, métodos de cifrado, transporte, almacenamiento, tratamiento y aplicaciones de los datos, así como también la seguridad en general.

Como se mencionó anteriormente, en la actualidad casi cualquier objeto convencional puede convertirse en dispositivo *IoT* si es dotado de funcionalidades para la

interacción y comunicación con Internet y/u otros dispositivos. Es por esto por lo que su ecosistema incluye objetos inteligentes como sensores, relojes, tenis que cuentan pasos, *wearables*, *Smart* TVs, alarmas, cámaras de videovigilancia, neveras, lavadoras, cafeteras, candados, persianas, luces, entre muchos más.

Dentro de una arquitectura *IoT* es importante tener en cuenta cada momento desde la captura de información por parte del dispositivo hasta el almacenamiento, procesamiento y análisis de los datos en la nube.

En el nivel inicial de cualquier arquitectura *IoT* se encuentran los sensores y/o actuadores los cuales supervisan y controlan, respectivamente, los distintos procesos a llevar a cabo. Dependiendo el dispositivo, en algunos casos un sensor puede recopilar información que necesite la participación del actuador, por ejemplo para el control de temperatura o ajuste de potencia, por lo que el proceso de envío de información para su análisis y posterior recepción para llevar a cabo la tarea suele suponer latencia, para esto, se hace uso de los dispositivos de sistema en módulo (SOM) el cual actúa muy cerca del proceso que se controla y es llamado *procesamiento en el borde* permitiendo que la tarea se lleve a cabo sin retraso.

En otra instancia de la arquitectura *IoT* se encuentra el sistema de adquisición de datos (*DAS* por sus siglas en inglés) el cual se encarga de recoger la información obtenida por los sensores del dispositivo transformándolos a formato digital, filtrándolos y comprimiéndolos ya que la cantidad de datos recibida dependiendo el dispositivo puede ser masiva.

Posteriormente, estos datos son comprimidos una vez más antes de pasar al centro de datos o a la nube, esto hace parte de la fase de preprocesamiento de datos, en esta fase suele ser muy útil el uso de aprendizaje automático, para mejorar el proceso continuamente sin esperar instrucciones desde el centro de datos o nube una vez fueron procesados.

Finalmente, una vez se recopilan los datos en el lugar donde se almacenarán y analizarán, se utilizan diferentes herramientas para gestionar estos datos provenientes de distintos dispositivos, siendo ayuda para la toma de decisiones, monitoreo, identificar patrones o para tener una visión global del funcionamiento de los mismos de acuerdo con las necesidades de cada usuario.

5.1.5 CASOS DE USO DE *IoT*

Los entornos *IoT* se podrían resumir en tres grandes grupos: Consumo (*CIoT* o Internet de las cosas del consumidor), Industria (*IIoT* o Internet Industrial de las Cosas) y *Smart Cities* (también considerada parte de *IIoT*) aunque en algunos casos de uso, estos grupos se pueden llegar a superponer.

De acuerdo con el informe *Señales de IoT* de *Microsoft*, la mayor implementación de *IoT* se encuentra en los sectores de comercio minorista (94%), energía (94%), fábricas (93%) y salud (89%), también, todos estos sectores cuentan con más del 20% de sus proyectos *IoT* en fase de utilización tal como se indica en la **Figura 5**.

Figura 5. *Implementación y valor del IoT por sector*

	TOTAL	Fábricas	Salud	Comercios	Energía
% DE ADOPTANTES DEL IoT	91 %	93 %	89 %	94 %	94 %
% DE PROYECTOS EN FASE DE UTILIZACIÓN	25 %	23 %	25 %	26 %	26 %
PLAZO PARA ALCANZAR FASE DE UTILIZACIÓN EN MESES (MEDIANA)	12	12	12	12	13
CREEN QUE ES VITAL PARA LA EMPRESA	90 %	93 %	87 %	92 %	90 %
PREVÉN UTILIZAR EL IoT MÁS DE AQUÍ A 2 AÑOS	64 %	67 %	58 %	58 %	55 %

Nota. Tomado de *Implementación y valor del IoT* (p.11), por *Microsoft*, 2020, *Microsoft* (https://azure.*Microsoft*.com/mediahandler/files/resourcefiles/*IoT*-signals/es-es/*IoT*%20Signals_Edition%202_Spanish.pdf)

Dentro de los ecosistemas que han adoptado *IoT* dentro de sus procesos, es común también la implementación de otras tecnologías como Inteligencia Artificial o *Big Data* para aumentar la eficiencia, mejorar la experiencia de usuario, reducción de tiempos, entre otras ventajas.

Como parte de las desventajas u obstáculos en la inclusión de *IoT* en entornos empresariales pueden encontrarse la falta de presupuesto, falta de recurso humano capacitado para llevar a cabo la implementación o también la complejidad que representa en algunos casos la inducción de esta tecnología en procesos ya estandarizados.

En los últimos años el sector de la salud ha venido incorporando tecnologías *IoT* en sus procesos. Teniendo en cuenta que es un sector donde sus procesos requieren un máximo de cuidado, la inclusión de nuevas tecnologías es una gran ventaja tanto para el usuario, como para el sector como tal. Gracias a la automatización de distintos procesos es posible mejorar predicciones, mantener un control y seguimiento de personal e inventario, supervisión continua y remota de los pacientes, aumento en la seguridad, mayor exactitud en los datos, entre otros.

En conclusión, independientemente del tipo de industria, la inclusión de *IoT* en los procesos representa que los mismos sean más seguros y eficientes, es importante para ello mantener un monitoreo constante, buenas prácticas y una excelente implementación ya que es el punto de partida al desarrollo de esta estrategia. Actualmente, debido a la pandemia Covid-19, muchas empresas se vieron obligadas a incorporar nuevas tecnologías que garanticen el buen funcionamiento de sus procesos, esto ayuda a mantener la eficiencia y productividad de los mismos obteniendo grandes ventajas sin redoblar esfuerzos.

Adicional a estos casos de uso descritos anteriormente, *IoT* se puede encontrar en diferentes entornos más, en los cuales se aplican distintas tecnologías para implementar soluciones tecnológicas que ayudan a la mejora de los procesos y las operaciones. Dentro de estos entornos se encuentra *retail*, manufactura, OT, salud, ganadería, entre otros.

5.1.5.1 *CIoT* – INTERNET DE LAS COSAS DEL CONSUMIDOR

Dentro de Internet de las Cosas del Consumidor, se agrupan entornos como la salud, objetos inteligentes personales o la domótica.

Dentro del ámbito de la salud se encuentran objetos para uso no solo de los pacientes sino también de los profesionales y los establecimientos, tales como, contenedores de medicina inteligentes, también, es posible mantenerse al corriente sobre la

salud de un paciente a través de dispositivos de monitoreo y seguimiento del estado y la ubicación.

Como objetos de uso personal se encuentran los *wearables*, relojes inteligentes, dispositivos de salud personal, asistentes de voz o dispositivos *fitness*, entre otros.

En la domótica, se incluyen aquellos objetos inteligentes integrados dentro del hogar o pequeños entornos (*Smart* home), tales como electrodomésticos, asistentes de voz, aplicaciones de seguridad, sistemas de electricidad, sensores de temperatura, movimiento, calor, entre otros.

Actualmente, todos estos dispositivos dentro del Internet de las cosas del consumidor enfrentan una serie de desafíos con el fin de aumentar su popularidad y presencia en el mercado.

Dentro de estos desafíos se encuentra la posibilidad de brindar más funciones sin depender totalmente del *Smartphone*, sin limitar su eficiencia y otras funcionalidades, también, una mayor adopción de dispositivos *IoT* requiere una mejora en su seguridad para poder implementar estos objetos sin comprometer información importante, lo cual da lugar también al tema de uso y protección de datos.

5.1.5.2 *IIoT* – INTERNET INDUSTRIAL DE LAS COSAS

Dentro de la industria *IoT* se encuentra la ganadería, hostelería, *retail*, el sector salud, la agricultura, manufactura, construcción, educación, entretenimiento, transporte, comercio, chips de geolocalización, entre otros. En este entorno por lo general se manejan gran cantidad de dispositivos *IoT* dentro de una misma red, por lo cual la criticidad de la información y las medidas de seguridad deben ser prioridad.

Independientemente del tipo de industria, la inclusión de *IoT* en los procesos busca optimizar las operaciones, aumentar la eficiencia, productividad y seguridad las mismas. *IoT* puede integrarse con otras tecnologías con el fin de sacar el mayor provecho de los datos para detectar patrones, mejorar la toma de decisiones, aumentar la productividad y en algunos casos también mejorar la experiencia de usuario.

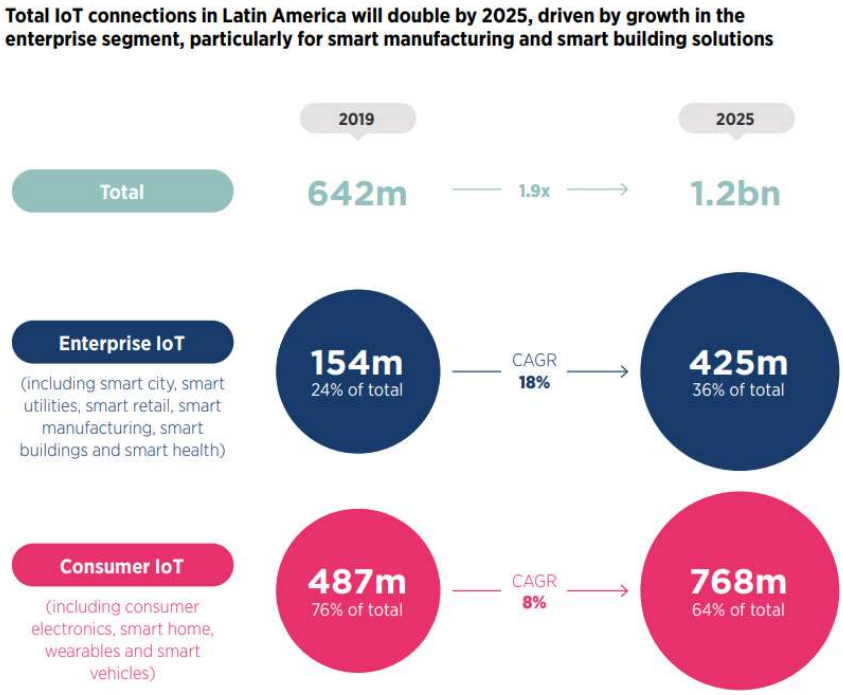
De acuerdo con el Informe sobre Economía Móvil emitido por *GSMA* en 2020, refleja que las empresas y gobiernos han adoptado nuevas tecnologías como *IoT* durante la

pandemia Covid-19 con el fin de no dejar estancar la economía y mejorar a resiliencia y eficiencia en sus operaciones.

GSMA afirma que para 2025 se estiman cerca de 24 mil millones de conexiones *IoT* a nivel global, debido a la rápida adopción de las empresas a las soluciones que los llevan a la transformación digital.

También, tal como se observa en la **Figura 6**, *GSMA* afirma que en Latinoamérica se llegarán a alcanzar cerca de 1.2 mil millones de conexiones para 2025 gracias al aumento en la oferta de mercado *IoT* por parte de grandes empresas como Telecom[19], Nokia[20], AT&T[21], entre otros. Además, ciudades como Medellín, Santiago, Buenos Aires y Sao Paulo están implementando iniciativas de *Smart Cities* a través de la implementación de *IoT*.

Figura 6. *Crecimiento de IoT en Latinoamérica para 2025*



Nota. Tomado de *Total IoT connections in Latin America will double by 2025, driven by growth in the enterprise segment, particularly for Smart manufacturing and Smart building solutions* (p.24), por *GSMA*, 2020, *GSMA* (https://www.*GSMA*.com/mobileeconomy/wp-content/uploads/2020/12/*GSMA*_MobileEconomy2020_LATAM_Eng.pdf)

[19] *Telecom Argentina S.A.* es una compañía de origen argentino dentro del área de las telecomunicaciones.
[20] *Nokia Corporation* es una multinacional fundada en Finlandia dentro del área de las telecomunicaciones.
[21] *AT&T, Inc.* es una multinacional estadounidense dentro del área de las telecomunicaciones.

Finalmente, *GSMA* menciona los principales startups de *IoT* en Latinoamérica, entre las mencionas se encuentran:

- Tecrea: Solución *IoT* para el seguimiento por *GPS* y emisión de alertas en tiempo real relacionadas con el ganado.
- Neltume: Solución *IoT* para ayudar a los agricultores a mantener control de los pesticidas e infestaciones de polillas.
- CitySense: Solución *IoT* para monitorear la calidad del aire y mantener seguimiento del nivel de criminalidad, también ayuda a las empresas a identificar potenciales mercados gracias al conteo de multitudes.
- Sensorbox: Solución *IoT* que predice, monitorea e informa diferentes fallas con las fuentes de energía ayudando a reducir las pérdidas empresariales por los cortes de luz.
- Jooycar: Solución *IoT* que monitorea y detecta patrones de conducción ofreciendo las rutas óptimas y emitiendo informes de mantenimiento para los carros conectados.
- Babybe: Solución *IoT* que a través de un colchón inteligente conecta a las madres con sus bebés prematuros imitando los latidos y la respiración de la madre.
- Firecity: Solución *IoT* que interconecta los sistemas de alarma de incendios en tiempo real, notificando a los propietarios y el departamento de bomberos en el caso de alguna emergencia.
- ChoppUp: Solución *IoT* que ayuda a reducir el desperdicio de cerveza en bares y restaurantes a través del monitoreo remoto de los datos de los dispensadores.

En Argentina surge también la Cámara Argentina de *IoT*[22] la cual busca ayudar al mercado local, detectar aspectos legales y regulatorios en cuanto a *IoT*, potenciar el crecimiento de las industrias que adoptan *IoT* en sus procesos, brindar seminarios, cursos, talleres, entre otros, relacionados a esta nueva tecnología contribuyendo a la capacitación

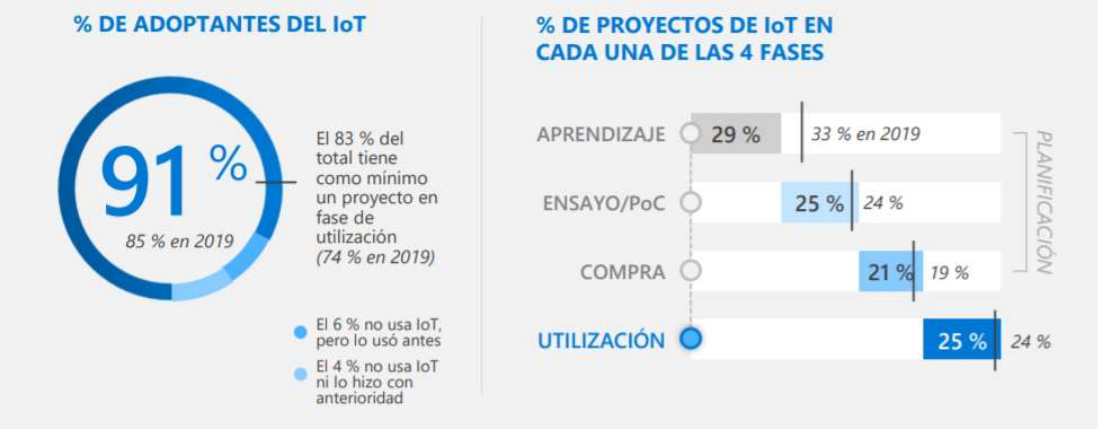
[22] Organización sin ánimo de lucro creada con el objetivo de promover el desarrollo del ecosistema de empresas y organizaciones vinculadas a *IoT* en Argentina y difundir los avances de esta industria a nivel local.

de las empresas e individuos, entre otros objetivos para impulsar la adopción de *IoT* en Argentina.

De acuerdo con el informe de *Microsoft* mencionado anteriormente, *Señales de IoT* entre 2019 y 2020 hubo un crecimiento del 6% en la incorporación de dispositivos *IoT* en ambientes empresariales, el 83% de estas empresas tienen como mínimo un proyecto en la última fase de proyecto, la cual es la fase de utilización, esto representa un 9% más respecto al año anterior.

Existen cuatro fases entre las cuales se clasifican los proyectos de *IoT*, estas son, aprendizaje, ensayo/PoC (prueba de concepto), compra y utilización. Al momento del informe de *Microsoft*, en 2020 el 29% de los proyectos *IoT* en las empresas encuestadas se encontraban en la fase inicial, es decir, la fase de aprendizaje y un 25% en fase final o fase de utilización, representando un 1% más que el año anterior, tal como se ilustra en la **Figura 7.**

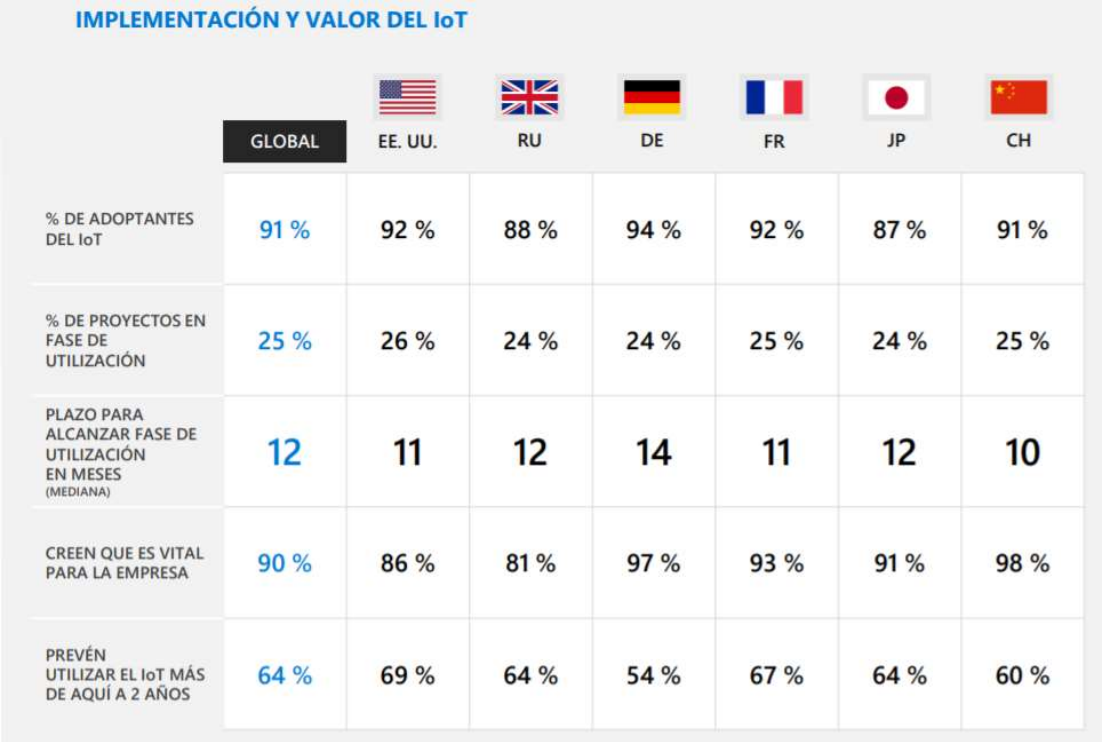
Figura 7. *Porcentaje de adoptantes del IoT.*



Nota. Tomado de *% de adoptantes del IoT* (p.8), por *Microsoft*, 2020, *Microsoft* (https://azure.*Microsoft*.com/mediahandler/files/resourcefiles/*IoT*-signals/es-es/*IoT*%20Signals_Edition%202_Spanish.pdf)

A nivel global, *Microsoft* asegura que, en Alemania, Estados Unidos y Francia encabezan la lista de países con mayor número de empresas que implementan el Internet de las Cosas, además, todos los países objeto de esta encuesta, detallados en la **Figura 8,** cuentan con más del 20% de los proyectos *IoT* en fase de utilización.

Figura 8. *Implementación y valor del IoT a nivel global*



IMPLEMENTACIÓN Y VALOR DEL IoT

	GLOBAL	EE. UU.	RU	DE	FR	JP	CH
% DE ADOPTANTES DEL IoT	91 %	92 %	88 %	94 %	92 %	87 %	91 %
% DE PROYECTOS EN FASE DE UTILIZACIÓN	25 %	26 %	24 %	24 %	25 %	24 %	25 %
PLAZO PARA ALCANZAR FASE DE UTILIZACIÓN EN MESES (MEDIANA)	12	11	12	14	11	12	10
CREEN QUE ES VITAL PARA LA EMPRESA	90 %	86 %	81 %	97 %	93 %	91 %	98 %
PREVÉN UTILIZAR EL IoT MÁS DE AQUÍ A 2 AÑOS	64 %	69 %	64 %	54 %	67 %	64 %	60 %

Nota. Tomado de *Implementación y valor del IoT* (p.10), por *Microsoft*, 2020, *Microsoft* (https://azure.*Microsoft*.com/mediahandler/files/resourcefiles/*IoT*-signals/es-es/*IoT*%20Signals_Edition%202_Spanish.pdf)

Sobre este caso de uso se profundizará en el capítulo 5.2.1.

5.1.5.3 *SMART CITIES*

Finalmente, las ciudades conectadas o *Smart Cities*, pueden mejorar considerablemente la calidad de vida dentro de la sociedad, gracias a que la cantidad de datos que recopilan pueden ser tratados a través de *Big Data* para la generación de reportes que ofrezcan soluciones a gran escala, ya sea en el transporte, alumbrado, medio ambiente, seguridad, gas, agua, alcantarillado, basuras, tráfico, entre otros. También, benefician al ciudadano ofreciéndole información real, a tiempo, útil y diversa.

Las personas suelen estar más familiarizadas con proyectos de *Smart Cities* ya que sus aplicaciones son más cercanas a sus usuarios, por ejemplo, en infraestructura, transporte, sustentabilidad, salud, prevención de desastres, servicios públicos, seguridad, entre otros.

Actualmente, en cuanto a infraestructura, es común ver edificios inteligentes en los cuales se incorporan dispositivos para vigilancia, control de temperatura, iluminación, mantenimiento y servicio al cliente, esto ayuda a facilitar la gestión y automatización de los edificios, optimizando la calidad de servicio de las instalaciones, reduciendo costes y mejorando la asignación de los recursos.

De acuerdo con el tipo de instalación, es posible encontrar proveedores especializados, ya que, por ejemplo, la adecuación para un edificio de oficinas es distinto a un hospital o un aeropuerto, así que, según el tipo de infraestructura, existe un área de foco que podría ser seguridad, sistemas, mecánica, eléctrica entre otros.

Como se mencionó anteriormente, varias ciudades en Latinoamérica han adoptado soluciones *IoT* para transformarse en *Smart City*. En San Nicolás de los Arroyos, ubicado en la provincia de Buenos Aires, en Argentina, se desplegaron gracias a Telefónica diferentes soluciones *IoT* con el fin de mejorar la calidad de vida de sus habitantes y transformarse en una ciudad inteligente. Se implementó un sistema de conectividad móvil para ayudar a gestionar su flota de vehículos y su personal. Dentro del celular de los empleados y los vehículos, se conectaron rastreadores *GPS* para conocer la ubicación en tiempo real de sus vehículos, ayudando a optimizar las rutas, reducir la probabilidad de accidentes y disminuir costos en combustible y mantenimiento.

Esto ha mejorado la eficiencia del proceso de recolección de basuras, ya que con el rastreador *GPS*, es posible conocer y publicar las rutas de los camiones en tiempo real alertando a los ciudadanos para que saquen los residuos en el momento oportuno ayudando a reducir malos olores y el desorden.

A medida que aumenta la conexión de los distintos elementos de la ciudad, se tiene mayor acceso a diferentes datos que finalmente contribuyen a mejorar la calidad de vida de los habitantes y a gestionar y tomar mejores decisiones por parte del gobierno.

Otro caso de uso de *Smart Cities*, podría ser el de Glasgow al implementar tecnologías *IoT* para controlar dinámicamente la calidad del aire. En 2013, a través de *Innovate UK*[23], Glasgow recibió una alta inversión en infraestructura digital para su proceso de transformación en *Smart City*, entre ellos se destacan el alumbrado público inteligente, demostrador eficiente de energía para conocer información sobre cortes y comportamiento de la energía, también, se realizó una integración inteligente en el servicio de transporte masivo entre otras implementaciones. El objetivo de esta tesis es reducir

[23] Agencia Nacional de Innovación en Reino Unido

costos, mejorar la calidad de vida de sus habitantes y sentar un precedente respecto a las ventajas de integrar tecnología y datos para mejorar la calidad de los negocios, habitantes y visitantes.

Alrededor del mundo, muchos países están impulsando la transformación a *Smart Cities* de varias ciudades, este es el caso de España en donde Barcelona es una de las ciudades inteligentes más avanzadas de Europa, también, Singapur está dentro de las ciudades más inteligentes y avanzadas del mundo, al igual que estas, otras ciudades como Londres, Melbourne o Copenhague están avanzando en su desarrollo digital. Como se mencionó en el capítulo anterior, Latinoamérica cuenta también con varias ciudades que ya están avanzando en su transformación digital.

5.1.6 ECOSISTEMAS TECNOLÓGICOS *IoT*

IoT también es un término general para una amplia gama de tecnologías y servicios subyacentes, que dependen de los casos de uso y, a su vez, forman parte de un ecosistema tecnológico más amplio dentro de los cuales se encuentran 5G, *Cloud*, *Big Data*, *IA, IT/OT*, Realidad virtual, Realidad aumentada, *Blockchain*, *Edge Computing*, *Fog Computing, NFT, RFID*, entre otros.

De acuerdo con *IBM*[24], relacionar una tecnología como *Blockchain* con el Internet de las Cosas puede traer bastantes beneficios respecto a seguridad, de acuerdo con una publicación en su sitio web, *IBM* destaca como principales beneficios generar confianza, reducir costos y agilizar procesos. También, dentro de las diferentes aplicaciones destaca el transporte de carga, seguimiento y cumplimiento de componentes y el registro de datos de mantenimiento operativo.

Big Data es la tecnología que más presente se encuentra en los proyectos de *IoT* ya que estos generan gran cantidad de datos que una vez ordenados y analizados, permiten la toma de decisiones de forma manual o automática.

La integración de Inteligencia Artificial en dispositivos *IoT*, permite la transformación de los datos adaptándose a las distintas soluciones.

Gracias a *Blockchain*, al igual que en otras tecnologías, se podría mejorar la seguridad de los dispositivos *IoT*. Los modelos de *Fog*, *Edge* y *Cloud computing* pueden

[24] *International Business Machines Corporation*, empresa multinacional tecnológica estadounidense.

ser muy útiles también para algunas soluciones *IoT*, por ejemplo, los carros autónomos ya que toman decisiones y acción a partir de factores internos, externos y datos recopilados.

5G es una tecnología que llega a favorecer a *IoT* especialmente en el entorno de *Smart Cities*, ya que es posible acceder con mayor rapidez a aplicaciones que contienen gran cantidad de datos provenientes de los distintos dispositivos inteligentes interconectados entre sí.

5.1.7 MARCO LEGAL: LEGISLACIÓN DE *IoT* A NIVEL MUNDIAL

Es claro que la tecnología avanza mucho más rápido que el derecho, por lo cual la innovación llega sin ser controlada mediante normas o legislaciones.

En el caso de *IoT* son muchas las discusiones que se han llevado a cabo en diferentes países respecto a si debería legislarse o no esta tecnología, en algunos casos se han creado regulaciones, mientras que en otros no lo ven necesario mientras exista una política de protección de datos o se puedan aplicar las leyes de protección de privacidad en Internet para dispositivos *IoT*.

El tema de legislar *IoT* se ha puesto en discusión debido también a la destinación de recursos que realizan los diferentes gobiernos cada año para promover el desarrollo de estos dispositivos dado su posicionamiento en el mercado.

El 28 de septiembre de 2018, se aprobó en California la ley SB-327 que entró en vigor el pasado 01 de enero de 2020 mediante la cual se buscan establecer requisitos de seguridad para todos los dispositivos *IoT* que se vendan en este Estado. Esta ley exige que cada dispositivo cuente con una contraseña única que lo identifique o que se solicite al usuario que antes de usar el dispositivo cambie la contraseña por defecto. Esta ley se diferencia de la actual ley de protección de datos ya que se centra en la protección del dispositivo, y, por ende, protege al usuario. Si bien es una ley bastante flexible para los fabricantes de objetos inteligentes, es el primer paso para que en Estados Unidos y otros países se comience a pensar en la creación de una ley para dispositivos *IoT* que contemple medidas robustas que garanticen la seguridad y privacidad de los datos de los usuarios de objetos interconectados.

En Reino Unido entró en vigor el 27 de enero de 2020 una ley con tres requisitos que busca garantizar que los dispositivos *IoT* que se vendan en los países que lo conforman se encuentren protegidos de ataques cibernéticos. El primer requisito hace referencia a las contraseñas, estas deben ser únicas para cada dispositivo y no pueden ser reiniciables a una configuración de fábrica. El segundo requisito exige que se tenga un punto de contacto al cual los usuarios puedan reportar incidentes de seguridad y el proveedor tome medidas frente a esto. Finalmente, el tercer requisito pide especificar cuál será el tiempo mínimo en que los fabricantes lanzarán actualizaciones sobre sus dispositivos.

Esta ley no es el primer paso que se da en pro de la securización de dispositivos *IoT*, ya que en 2018 Reino Unido creó un código que busca garantizar la seguridad durante el proceso de diseño de dispositivos *IoT*, por lo cual la reciente norma llega como un complemente a este código. También, en enero de 2020, se publicó una norma con 30 verificaciones creada por la Fundación IoT Security[25] (*IoTSF*, por sus siglas en inglés) y la Asociación Internacional de Educadores en Ciencias Médicas[26] (*IAMSE*, por sus siglas en inglés) en donde buscan certificar aquellos dispositivos que cumplan con estos 30 requerimientos de seguridad.

El Ministerio de Infraestructura y Tecnología de China destina sumas considerables cada año a la promoción del desarrollo de dispositivos *IoT*, su inversión en esta infraestructura supera la de Europa y Estados Unidos siendo China un país referente en el mercado *IoT*. En cuanto a su legislación, China tiene una ley en la cual se garantiza la seguridad de la información, la protección de datos y la protección de derechos sobre propiedad intelectual.

Durante 2017, la Secretaría de *TICs* o tecnologías de la información y las comunicaciones, en Argentina realizó una *Consulta pública sobre Internet de las Cosas* en la cual se reunieron empresas, cámaras, academias y consultoras con el fin de obtener información, propuestas y opiniones respecto a la creación de políticas públicas o regulaciones en infraestructura *IoT*. En conclusión, la mayor parte de estos entes coinciden en que la creación de normas para *IoT* es prematuro en innecesario, por lo cual el estado no debería regular esto, pero coinciden en que el gobierno debe incentivar al desarrollo y crecimiento de los sectores vinculados a *IoT*.

Es posible crear leyes, normas y estándares que garanticen la seguridad y privacidad en dispositivos *IoT*, pero esto es solamente una parte. Legislar no garantiza la

[25] Organización sin fines de lucro dedicada a impulsar la excelencia en seguridad.
[26] Consorcio internacional enfocado en servicios de educación en ciencias médicas de la salud.

seguridad de los datos mientras estos dispositivos no sean usados correctamente por sus usuarios, por lo cual un desarrollo seguro, la creación de estándares y leyes debe ir de la mano con medidas de concientización y educación para sus consumidores, así se puede garantizar un buen desarrollo y uso que logren crear una robusta barrera de seguridad frente ataques cibernéticos.

En el 2020, el congreso de Estados Unidos aprobó una ley llamada *Ley de mejora de la ciberseguridad en Internet de las cosas* la cual detalla en el sitio web del congreso de E.E.U.U que "Este proyecto de ley exige que el Instituto Nacional de Normas y Tecnología (*NIST*) y la Oficina de Gestión y Presupuesto (*OMB*) tomen medidas específicas para aumentar la ciberseguridad de los dispositivos de Internet de las Cosas (*IoT*).". Esta ley obliga a *NIST* que diseñe normas y directrices donde se detallen los requisitos mínimos de ciberseguridad para los objetos *IoT* bajo el uso o control del gobierno federal. Esto debe incluir temas de ciclo de vida seguro, aplicación de parches, gestión de sesiones, entre otros temas. Asimismo, la adquisición de un nuevo dispositivo *IoT* debe pasar por un proceso de cumplimiento de las normas y directrices establecidas, solamente se exceptúan dispositivos en caso de ser necesarios para la seguridad nacional, para fines investigativos o si se comprueba que el dispositivo cuenta con métodos alternativos de ciberseguridad eficaces.

Sumado a la iniciativa de Estados Unidos, en 2021 entró en vigor la Ley de Internet de las Cosas en Brasil. De acuerdo con el Ministerio de ciencia, tecnología e innovación de Brasil, esta ley "reduce a cero las tasas de inspección, de instalación y de funcionamiento de los sistemas de comunicación entre máquinas". Esta ley tiene una vigencia de cinco años y se afirma que ayudará a acelerar el crecimiento del PIB de Brasil trayendo grandes ganancias para el país en temas económicos.

Otra ventaja de la implementación de esta ley es que ayudará a las empresas a avanzar a un entorno de Industria 4.0, también ayudará a las personas del común a facilitar el día a día gracias a la inducción de la tecnología *IoT* en las ciudades mejorando la calidad de vida de sus habitantes.

En febrero de 2022, fue publicada la versión final de la norma ISO/IEC 27002:2022 referente a seguridad de la información, ciberseguridad y protección de la privacidad ofreciendo un catálogo de controles de referencia sobre seguridad de la información.

En esta nueva versión, se refuerzan controles ya existentes además de incluir controles nuevos sobre inteligencia de amenazas, eliminación de información, enmascaramiento de datos, actividades de monitoreo, entre otros para conformar un set de

93 controles clasificados en organizacionales, físicos, tecnológicos y controles de personas. Si bien el catálogo de controles es bastante amplio y hace referencia a diferentes tecnologías como *Big Data* o computación en la nube, aún no se profundiza en controles sobre internet de las cosas.

Debido al gran volumen de datos que generan los dispositivos *IoT*, es necesario garantizar la seguridad para sus usuarios a través estándares y protocolos tal como existe en Internet, esto reduciría en gran medida la preocupación por las personas y las empresas a caer en un ciberataque a través de alguno de sus dispositivos y también, ayudaría a comenzar a confiar más en estos, despreocupándose de estar en una constante vigilancia ya que hay garantía en la seguridad de los permisos dados a sus dispositivos *IoT* y los datos que estos manejan.

5.1.8 SEGURIDAD Y PRIVACIDAD DE DISPOSITIVOS *IoT*

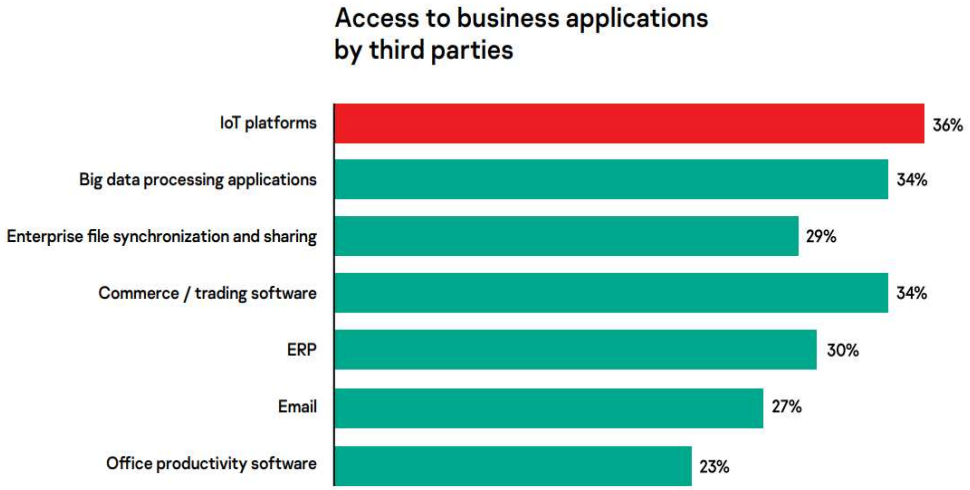
El principal problema actual de los dispositivos *IoT* son la seguridad y privacidad de sus datos, esto en gran medida debido a como se mencionó en el capítulo anterior, no hay una estandarización en los protocolos de esta tecnología.

Teniendo en cuenta que los dispositivos *IoT* son unos de los mayores generadores de datos, es necesario prestar atención a la seguridad, disponibilidad y confidencialidad de los mismos, especialmente ya que esta tecnología se encuentra en constante crecimiento debido a la gran adopción por parte de personas, gobiernos y empresas dentro de sus servicios o su día a día con el fin de agilizar sus procesos o mejorar su calidad de vida.

De acuerdo con un estudio realizado por Gartner en el 2018 sobre seguridad en dispositivos *IoT*, cerca del 20% de las organizaciones han detectado un ataque a través de *IoT* en los tres años anteriores. De igual forma, como se observa en la **Figura 9** en el reporte *Beneficios y desafíos de IoT en el negocio* realizado por *Kaspersky*[27] en 2020, 36% de las compañías admiten que terceros han ingresado a sus plataformas *IoT*, este porcentaje supera incluso a otros elementos de la infraestructura del negocio tales como *software* productivo de oficina (23%), correo electrónico (27%) o *ERPs* (30%). De acuerdo con esto, *Kaspersky* afirma que los ingresos por parte de terceros hacia las aplicaciones deberían ser considerados dentro de los términos y condiciones de seguridad de los datos.

[27] Compañía internacional dedicada a la seguridad informática.

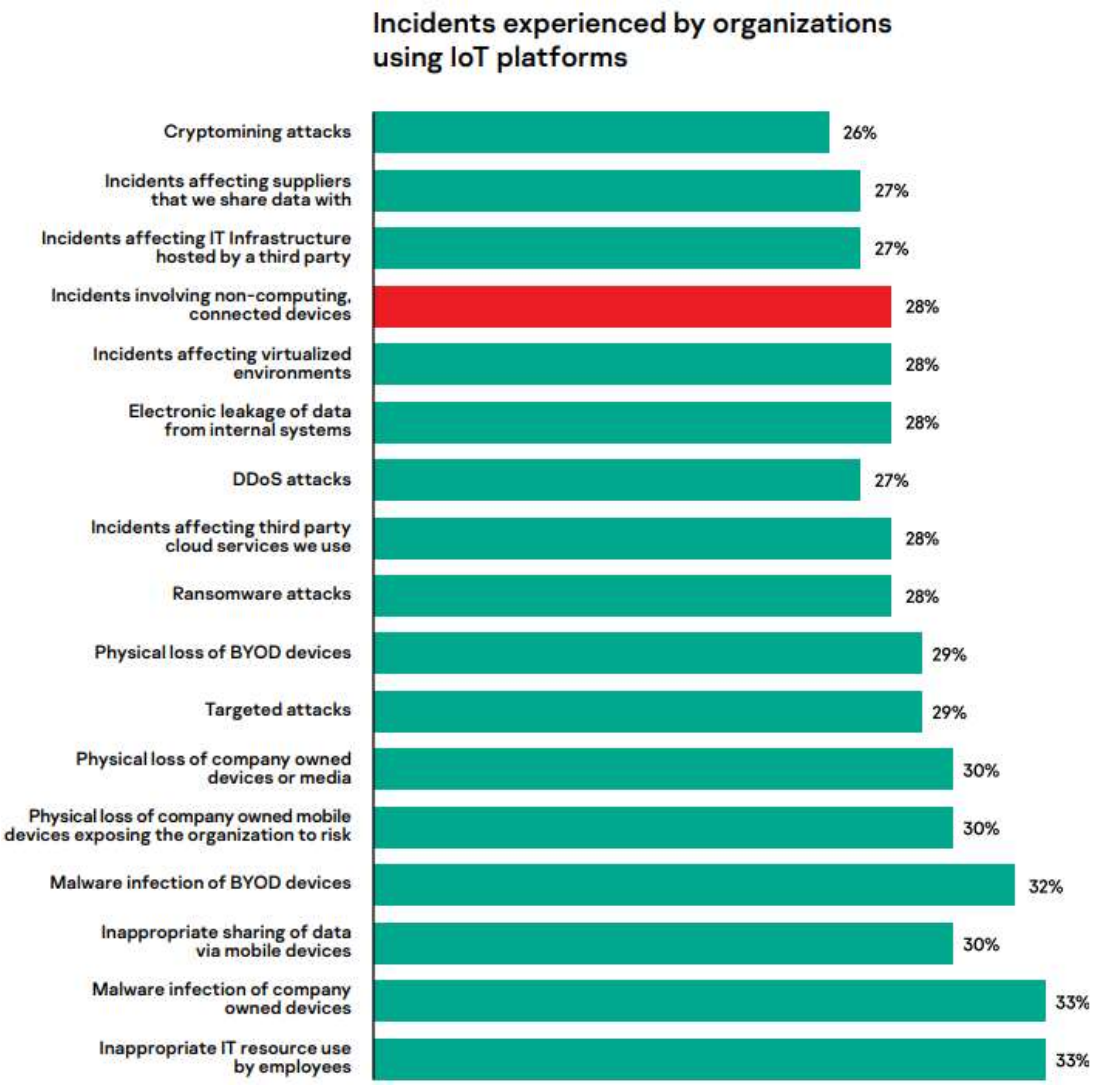
Figura 9. *Acceso a las aplicaciones del negocio por parte de terceros*



Nota. Tomado de *What business applications are accessed by third parties, Kaspersky Global Corporate IT Security Risks Survey 2019* (p.8), por *Kaspersky*, 2020, *Kaspersky* (https://media.*Kaspersky*daily.com/wp-content/uploads/sites/85/2020/05/21102818/2020_*Kaspersky_IoT*_report.pdf)

Adicionalmente, dentro de este reporte, *Kaspersky* analiza los incidentes presentados en compañías con plataformas *IoT*, dentro de este estudio se analizan incidentes hacia dispositivos conectados sean informáticos o no, donde los primeros cuentan con un porcentaje menor, entre ellos están los incidentes relacionados a minería de criptomonedas (26%), transferencia de datos entre proveedores (27%) o incidentes de infraestructura relacionado a terceros (27%) mientras que los incidentes en dispositivos no informáticos conectados representan el 28% tal como se refleja en la **Figura 10**.

Figura 10. *Incidentes ocurridos en empresas con plataformas IoT*



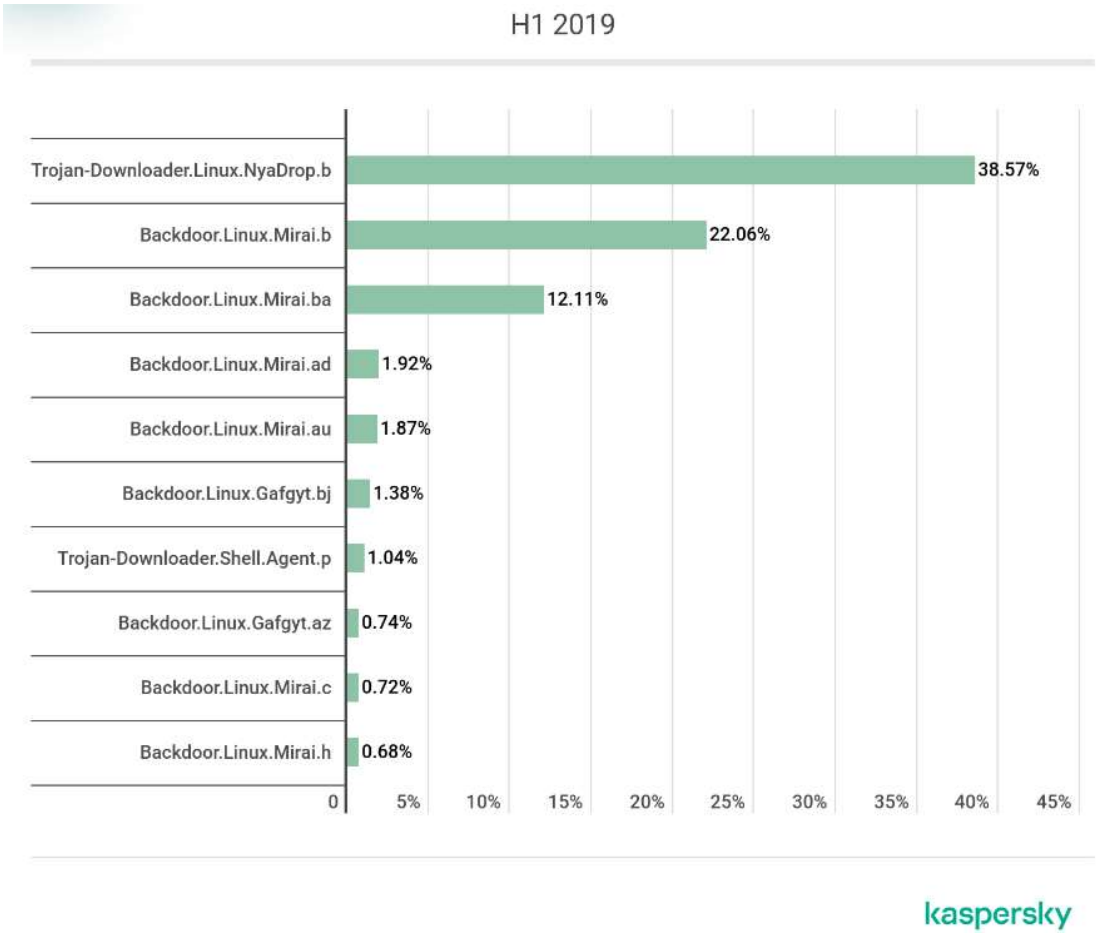
Nota. Tomado de *What incidents are experienced by organizations using IoT platforms, Kaspersky Global Corporate IT Security Risks Survey 2019* (p.9), por *Kaspersky*, 2020, *Kaspersky* (https://media.*Kaspersky*daily.com/wp-content/uploads/sites/85/2020/05/21102818/2020_*Kaspersky_IoT*_report.pdf)

En 2019, *Kaspersky* publicó un reporte llamado *IoT: a malware story,* en el cual realiza un análisis de los diferentes *malware* conocidos creados para atacar dispositivos *IoT*, afirma que el principal problema de estos objetos inteligentes es que es imposible por parte del usuario, instalar algún tipo de *software* de seguridad.

En este reporte, tal como se muestra en la **Figura 11**, se listan los principales *malware* que amenazan *IoT* durante el primer semestre de 2018 y 2019 en donde los primeros lugares los ocupan modificaciones del *malware Mirai* mencionado anteriormente, el cual está dirigido a dispositivos con servicio *Telnet* desactivado, esto debido a que el

código original se encuentra público hace varios años y es posible modificarlo a conveniencia.

Figura 11. *Top 10 amenazas primer semestre 2019*



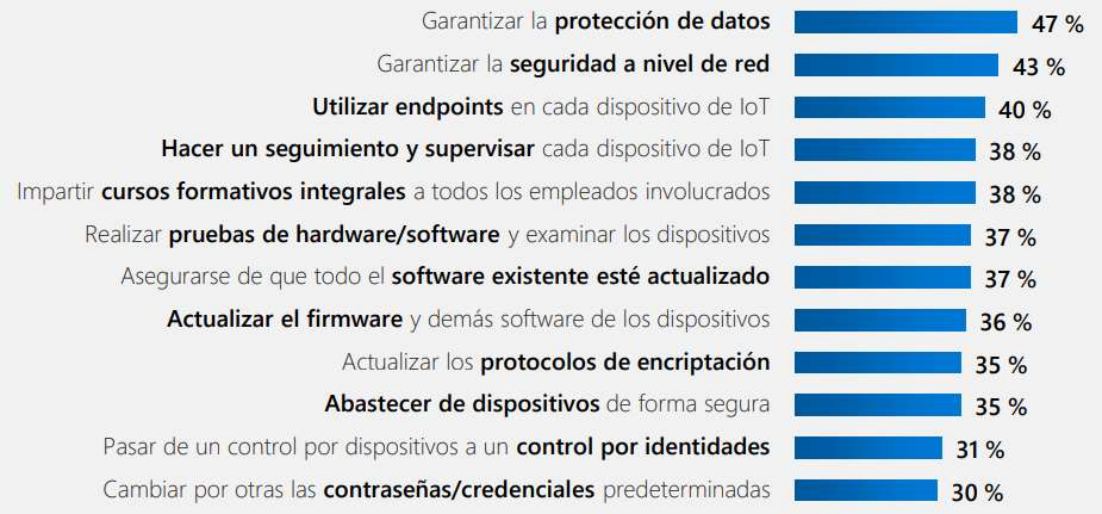
Nota. Tomado de *TOP 10 IoT threat verdicts, first half of 2019,* por *Kaspersky*, 2019, *Kaspersky* (https://securelist.com/*IoT*-a-*malware*-story/94451/)

La seguridad de cualquier tipo de dispositivo *IoT* debe ser una prioridad para sus usuarios, muchas veces esto no es así ya que hay desconocimiento sobre los alcances de un dispositivo infectado en donde en el mayor de los casos y el menos grave puede ser el de ser infectado para utilizarse como *botnet* en un ataque *DDOS*, pero en escenarios de mayor complejidad, un dispositivo *IoT* puede ser vulnerado y utilizarse para realizar actividades criminales por parte del atacante o realizar espionaje para posteriormente chantajear a la víctima, finalmente, el dispositivo vulnerado puede terminar siendo destruido siendo esta también una grave consecuencia.

En el reporte *Señales de IoT* de *Microsoft* mencionado anteriormente, se afirma que las empresas encuestadas tienen en cuenta distintos factores de seguridad al implementar *IoT* en sus procesos y a la gran mayoría (97%) les preocupa que la inducción de estos

dispositivos pueda desencadenar en brechas de seguridad. Como se ilustra en la **Figura 12**, los principales factores en tema de seguridad que preocupan a las empresas son la protección de los datos (47%), la seguridad a nivel de red (43%) y el uso de *endpoints* en cada dispositivo *IoT* (40%), así como en menor medida se encuentran el abastecimiento de dispositivos de forma segura (31%) o el cambio de contraseñas por defecto (30%).

Figura 12. *Principales preocupaciones de las empresas al implementar IoT*



Nota. Tomado de *Principales preocupaciones de seguridad en materia de IoT* (p.18), por *Microsoft*, 2020, *Microsoft* (https://azure.*Microsoft*.com/mediahandler/files/resourcefiles/*IoT*-signals/es-es/*IoT*%20Signals_Edition%202_Spanish.pdf)

Tal como se mencionó en el capítulo 5.1.7, en el 2018 se aprobó la ley SB-327 la cual entró en vigor en 2020 y hace referencia a la seguridad en los dispositivos *IoT*. Respecto a esto, la ley se enfoca en la seguridad desde el dispositivo y aplica a todos los dispositivos móviles que se conectan de manera directa o indirecta a internet a través de una dirección IP o *bluetooth* y sean vendidos en el Estado de California. Ya que la ley va dirigida a los dispositivos inteligentes, las librerías o los *SDKs* (*Software Development Kits*, por sus siglas en inglés) no aplican en esta regulación.

Adicional a la regulación SB-327 de California y los distintos *Frameworks*[28] sobre los cuales se profundizará en el siguiente capítulo, distintas instituciones y grupos han tomado la falta de privacidad y seguridad en dispositivos *IoT* como casos de estudio para emitir recomendaciones y buenas prácticas que ayuden a los usuarios a proteger sus dispositivos y sus datos.

[28] Marcos de referencia.

En pasado 28 de julio de 2021, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI[29]), emitió un comunicado en el cual advierte a los usuarios sobre los distintos riesgos de vincular dispositivos domésticos a Internet, alertando que sus datos pueden estar en peligro de no contar con una buena configuración de seguridad, indicando que el uso de estos datos por parte de terceros puede concluir en un seguimiento para obtener patrones de conducta o consumo, o como forma de extorsión dependiendo quien logre acceder a la información privada.

La *IoT Security Foundation*[30], emitió en el 2018 el reporte *IoT Cybersecurity*: *Regulation Ready*, en el cual resume y analiza quince políticas de diferentes países en las cuales destaca las distintas regulaciones y en algunos casos, incongruencias, entre las mismas en cuanto a la protección de datos dependiendo el área y el país, concluyendo que efectivamente hace falta la estandarización de normativas enfocadas a la protección y seguridad de los dispositivos inteligentes, si bien otras leyes pueden ser usadas para penalizar la falta de seguridad y privacidad en datos personales, no existe una ley como tal que garantice la seguridad de un dispositivo inteligente en cada una de sus etapas. Además, este documento muestra que, en algunos casos, como en la industria de los juguetes inteligentes, aún con leyes que protegen a los menores, se han presentado varios casos en donde los dispositivos son vulnerados y por consiguiente son prohibidos o destruidos, la respuesta por parte de algunos proveedores, en lugar de mejorar la seguridad de sus productos, es no vender sus dispositivos en Estados Unidos o la Unión Europea.

Finalmente, así como la baja o nula seguridad en los dispositivos *IoT* es aprovechada por terceros a través de herramientas como *Shodan*, existe también una cuenta dentro de la red social *Twitter*, llamada *@internetofshit* la cual expone dispositivos que carecen de seguridad o esta es muy mala, o también dispositivos que son desarrollados con funcionalidades absurdas alertando a sus seguidores y compartiendo datos de este tipo dentro de su comunidad.

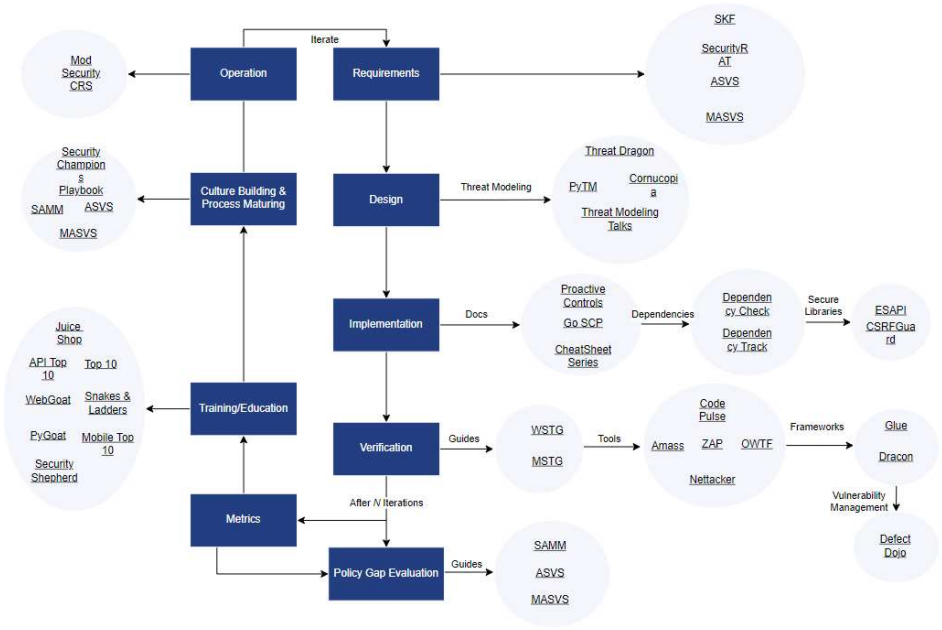
5.1.8.1 *OWASP TOP 10*

[29] Organismo constitucional autónomo en México encargado del cumplimiento del derecho al acceso a la información pública y la protección de datos personales.
[30] Organización sin ánimo de lucro enfocada en mejorar la seguridad de los dispositivos *IoT*.

El Proyecto de Seguridad de Aplicaciones Web Abiertas (*OWASP*, por sus siglas en inglés) es una organización sin ánimo de lucra que es trabaja en búsqueda de una mejora en la seguridad del *software*. Esta comunidad desarrolla diversos proyectos tanto de desarrollo como de documentación, y, en conjunto cuenta con miles de miembros. Gracias a su trabajo, ha logrado gran reconocimiento desde su inicio como fundación en 2004 y actualmente es considerada un referente en cuanto a herramientas, guías, educación, contactos, entre otras actividades, para desarrolladores y demás interesados en mejorar la seguridad de los sistemas.

Como se comentó anteriormente, *OWASP* ha desarrollado distintos proyectos los cuales en su sitio web se encuentran mapeados en un diagrama de ciclo de vida de desarrollo de *software* **(Figura 13)** con el fin de ayudar a los desarrolladores a identificar el proyecto más acorde al ciclo de vida de sus sistemas.

Figura 13. *Mapeo del Ciclo de Vida del Desarrollo de Software vs. Proyectos OWASP*



Nota. Tomado de *Application Security Wayfinder,* por *OWASP*, 2023, *OWASP* (https://*OWASP*.org/projects/)

Actualmente, *OWASP* cuenta con un total de 261 proyectos, los cuales se encuentran clasificados en tres categorías:

- Proyectos insignia: Hace referencia a los proyectos que han demostrado tener un valor estratégico para la comunidad *OWASP* y para la seguridad de los sistemas.

- Proyectos de laboratorio: Hace referencia a los proyectos que han presentado un entregable que ha sido revisado por *OWASP*.
- Proyectos de incubadora: Hace referencia a proyectos que aún se encuentran en etapa de desarrollo.

Los proyectos *OWASP* cuentan con su sitio web, correo electrónico y canal en *Slack*[31]. También, la mayoría de ellos publican su contenido en la *GitHub*. Estos proyectos pueden ser desarrollados por desarrolladores, técnicos, referentes en seguridad de la información y está abierto también a cualquier persona que desee un apoyo para presentar, desarrollar y/o probar una idea relacionada a mejorar la seguridad del *software*.

Tal vez el proyecto más conocido de *OWASP* es el *OWASP Top 10*, el cual se ha convertido en un standard para desarrolladores, auditores y demás grupos en el entorno tecnológico ya que esta tesis resume los diez riesgos de seguridad más críticos para las aplicaciones. Esta tesis es sugerida como punto de inicio en el desarrollo de proyectos o revisión de estos ya que da una idea amplia sobre la seguridad del sistema que se está revisando o desarrollando.

OWASP cuenta también con algunos proyectos relacionados con Internet de las Cosas, entre ellos se encuentran:

- *OWASP IoT Security Verification Standard* o Norma de verificación de la seguridad del *IoT* de *OWASP*
- *OWASP Internet of Things* o Internet de las cosas de *OWASP*
- *OWASP Internet of Things top 10* o Top 10 Internet de las cosas de *OWASP*

Según el proyecto *OWASP IoT top 10*, se encuentran definidas actualmente 10 vulnerabilidades para *IoT*. Este listado busca guiar a los desarrolladores de objetos inteligentes para incluir la seguridad en la creación de sus dispositivos inteligentes. A continuación, se detalla el Top 10 de vulnerabilidades para dispositivos *IoT* según *OWASP*.

1. Contraseñas débiles, codificadas o fáciles de adivinar.
2. Servicios de red inseguros.
3. Interfaces inseguras en el ecosistema.

[31] *Slack* es un sistema de mensajería utilizado por las empresas para mantener comunicación con sus equipos e impulsar sus negocios.

4. Falta de mecanismos de actualizaciones seguras.
5. Uso de componentes inseguros u obsoletos.
6. Insuficiente protección de la privacidad.
7. Transferencia de datos y almacenamiento inseguro.
8. Falta de soporte de seguridad en los dispositivos.
9. Configuraciones por defecto inseguras.
10. Falta de robustecimiento físico.

5.1.8.2 VULNERABILIDADES

Los dispositivos *IoT* presentan grandes vulnerabilidades en cuanto a seguridad y privacidad, el hecho de contener información sensible y privada del usuario y estar conectados a Internet ya significa un riesgo. Es por esto que hay que prestar atención a la configuración de seguridad en los dispositivos *IoT* antes de hacer uso de estos ya que una falta de protección o control puede llevar a un robo de información, un daño en el dispositivo o espionaje.

Dentro de las vulnerabilidades de *IoT*, una práctica común que hace uso de dispositivos mal configurados o desatendidos es el uso de estos como *botnet*s. Tal vez el caso más conocido es el del *botnet Mirai* durante octubre de 2016. Este *malware* realizaba un escaneo de puertos, específicamente *Telnet*, ingresaba con usuario y clave por defecto del fabricante y una vez había ingresado, incluía dicho dispositivo en su ejército de *bots* para el desarrollo de un ataque *DDOS* el cual afectó gran parte de la costa este de Estados Unidos.

Mirai no es el único caso, se han dado a conocer otros *malware* como *Pesirai*, *Demonbot, Gafgyt, Bushido* o *Rift* los cuales hacían uso también de vulnerabilidades en dispositivos *IoT* y llegaron a realizar ataques en Estados Unidos, Reino Unido, Malasia y Países Bajos.

Otra gran vulnerabilidad presente a nivel empresarial a partir de dispositivos *IoT* es aquella conocida como *IoT* en la sombra o *Shadow IoT*. Este fenómeno aparece afectando las redes empresariales desde que las compañías decidieron implementar la modalidad *BYOD (Bring Your Own Device*) en donde los empleados podían hacer uso de sus dispositivos personales para conectarse a la red empresarial y realizar su trabajo. Es así

como varios *Smartphone*s y computadores personales comenzaron a generar tráfico en las redes de las compañías en donde no se tenía un control sobre los dispositivos que se conectaban a ella, a lo cual se le denominó *Shadow IT*.

Con la aparición de dispositivos *IoT* y la gran adopción por parte de los usuarios, este fenómeno *Shadow IT* se transformó a Shadow *IoT* ya que ahora no solamente se conectaban teléfonos inteligentes y computadores a la red empresarial, sino también *Smart TVs,* asistentes de voz, *wearables*, dispositivos de domótica, entre otros.

Este fenómeno se ha ido convirtiendo en un gran problema de seguridad para las compañías, ya que, en la mayoría de los casos, los equipos de seguridad y tecnología informática no tienen control sobre los dispositivos para uso personal que se conectan a la red empresarial. El gran problema es que estos dispositivos *IoT* presentan graves problemas de seguridad, ya que se limitan a realizar una o dos tareas y dejan de lado la seguridad, por lo cual muchos transmiten datos en texto plano, sin hacer uso de protocolos como SSL, así que, al tener al menos un dispositivo de este tipo conectado a la red empresarial puede significar una brecha de seguridad que puede traer infección de *malware*, espionaje, robo de datos, acceso a la red o incluso hacer uso de estos dispositivos para convertirlos en *botnet*s y llevar a cabo un ataque *DDOS*.

Las empresas necesitan dar prioridad a este problema especialmente ahora que la adopción de dispositivos *IoT* es mayor y se encuentra en rápido crecimiento. Es necesario contar con políticas que prohíban o controlen la conexión de dispositivos personales a la red empresarial, que cuenten con comunicaciones cifradas y más importante aún, capacitar a los empleados en el uso de estos, tener usuarios inseguros lleva a una empresa a ser insegura.

5.1.8.3 VECTORES DE ATAQUE *IoT*

La inclusión de *IoT* tiene múltiples ventajas las cuales han sido descritas a lo largo de este documento, pero también puede traer algunas consecuencias si no se gestionan de forma correcta. En empresas en un entorno de Industria 4.0, por ejemplo, el Internet de las Cosas se puede ver dentro de procesos de automatización a nivel general o de tecnología operativa (OT), lo cual, de acuerdo con la cantidad de procesos y el tamaño de los recursos, puede representar gran cantidad de dispositivos *IoT* y dispositivos *IIoT* implementados, lo cual aumenta el nivel de vulnerabilidad de la compañía.

La inclusión de estos dispositivos bien sea en espacios generales como operacionales, deja una brecha de control y monitoreo en espacios que anteriormente no representaban un riesgo en cuanto a ciberseguridad, usualmente, al ser dispositivos que no realizan tareas de mayor dificultad, no se les presta la debida atención que merecen incluso desde el momento de su incorporación, esto sin duda, como cualquier dispositivo inteligente sin la correcta configuración y seguimiento, puede convertirse en la puerta de entrada para un ataque de gran escala sobre los distintos procesos de la compañía ya que estos dispositivos pueden estar conectados a servidores críticos o estar recopilando información sensible.

En un entorno empresarial, el primer paso antes incluso de la inclusión de dispositivos *IoT* o *IIoT*, es la preparación. Se debe conocer el dispositivo, configurarlo de manera adecuada y preparar un espacio para el control y monitoreo de este.

Los dispositivos *IoT* suelen incluir características las cuales son necesarias para su correcto funcionamiento, pero también pueden ser aprovechadas para actividades maliciosas. Un ejemplo de estas características es la recopilación de datos los cuales podrían contener información sensitiva que puede verse comprometida si no es protegida correctamente.

El proyecto *OWASP*, mencionado en capítulos anteriores, dentro de Internet de las Cosas ha definido las áreas de superficie de ataque en donde pueden existir amenazas o vulnerabilidades. En primer lugar, se encuentran los dispositivos, según *OWASP*, este es el medio principal por el cual inician los ataques, esto se puede deber a *firmware*s obsoletos, configuraciones predeterminadas inseguras, falta de actualizaciones, problemas con la interfaz web o vulnerabilidades desde los servicios de red.

En segundo lugar, se encuentran los canales de comunicación, *OWASP* considera que estos pueden representar una puerta de ataque ya que los protocolos utilizados para la conexión de dispositivos *IoT* entre sí pueden ser inseguros afectando la comunicación y los dispositivos. Adicionalmente, los ataques de red convencionales como *man-in-the-middle*, *DDOS* o suplantación de identidad pueden encontrarse también dentro de las redes de comunicación entre dispositivos *IoT*.

Finalmente, en tercer lugar, *OWASP* incluye las aplicaciones web y el *software* relacionado a *IoT* ya que estos pueden verse comprometidos con el fin de realizar un robo de credenciales o falsificar actualizaciones incluyendo *malware* en los mismos comprometiendo los dispositivos.

De acuerdo con estas áreas de ataque definidas por *OWASP*, los dispositivos *IoT* pueden verse comprometidos desde el dispositivo físico como tal, como desde sus componentes (*hardware*/*software*), por lo cual la seguridad de los dispositivos inteligentes debe estar presente desde el momento de su fabricación hasta el mantenimiento de estos, sumado a un buen uso por parte de los usuarios y constantes actualizaciones por parte de los proveedores asegurando que el dispositivo en un todo sea tanto seguro como funcional.

5.1.8.4 INFRAESTRUCTURA DE SERVICIOS *IoT*

La comunicación entre dispositivos *IoT* se realiza a través de conexiones de red, en algunos casos puede ser *Wifi* o *LoraWan*, pero la mayoría de las conexiones se realizan a través de las redes móviles 3G, 4G y 5G.

Adicionalmente, existen actualmente varios protocolos que permiten también la comunicación entre dispositivos inteligentes, estos deben tener en cuenta las características y propósito de los distintos dispositivos ya que en una misma comunicación pueden intervenir dos o más de estos, un protocolo adecuado debe soportar la mayor cantidad de dispositivos interconectados haciendo uso de la menor cantidad de recursos posibles para garantizar la interoperabilidad y dar respuesta a tiempo a cada solicitud. También, los dispositivos interconectados a pesar de contar con características distintas deben poder comunicarse entre sí en todo momento, para lo cual el protocolo que garantiza dicha comunicación debe asegurar que los dispositivos interconectados se encuentren accesibles, finalmente y no menos importante, se debe garantizar la seguridad en la comunicación teniendo en cuenta que estos dispositivos están compartiendo información muchas veces sensible que se encuentra expuesta en la red. En resumen, una buena infraestructura de redes *IoT* debe garantizar escalabilidad, concurrencia, accesibilidad y seguridad.

Como se mencionó anteriormente, es necesario identificar el tipo de dispositivos a interconectar ya que esto será importante para definir los protocolos de comunicación. En el caso de dispositivos de corto alcance, es decir, dispositivos en donde los datos no viajarán a distancias muy largas, por ejemplo, en entornos como casas u oficinas, se hace uso de tecnologías como *Bluetooth*, *Wifi*, *Zigbee*, *Z-wave* o NFC, entre otros.

Bluetooth es una tecnología con un máximo de alcance de 10 metros que permite el envío y recepción de señales de voz y datos a alta velocidad.

Wifi puede alcanzar una cobertura entre los 15 y 46 metros, pero no es la mejor opción teniendo en cuenta que puede presentar problemas de velocidad y calidad de la transmisión.

Zigbee tienen un alcance de entre 10 y 20 metros, pero reducen considerablemente su rendimiento si hay varios dispositivos conectados, por otro lado, *Z-wave* puede considerarse una mejor opción ya que al tener un mayor alcance, de hasta 100 metros de distancia, puede representar menos problemas en la comunicación.

NFC puede ser el que menos alcance tenga entre las tecnologías acá mencionadas, estos protocolos ofrecen una comunicación entre dispositivos a 4 centímetros o menos, cuentan con una configuración sencilla y bajas velocidades de conexión.

En el caso de distancias más grandes, se puede hacer uso de redes de bajo consumo, conocidas como *LPWAN* por sus siglas en inglés que permiten una comunicación de hasta 15 kilómetros de distancia, entre ellas se encuentran las redes 4G, 5G, *LoraWan, Sigfox, Cat-0, Cat-1 o NB-IoT* entre otros.

Las redes 4G y próximamente 5G para dispositivos *IoT*, proveen bajos niveles de latencia en la comunicación y representan una opción más viable que el *Wifi* debido a que cuentan con mayor estabilidad en la conexión.

El protocolo *LoraWan* ofrece una conexión entre dispositivos a una distancia de hasta 20 kilómetros y una capacidad de interconectar hasta un millón de dispositivos con bajas probabilidades de interferencia.

Sigfox es una red de alta cobertura (hasta 20 kilómetros en campo abierto y 1.5 kilómetros en zona urbana) y bajo costo ya que fue diseñada para transmitir comunicaciones de baja velocidad a través de un ancho de banda muy estrecha el cual facilita la conexión entre grandes distancias. Actualmente esta tecnología tiene cobertura en 60 países en todo el mundo dentro de los que se encuentran Argentina, Brasil, Colombia, España, Canadá, Rusia, Namibia, Japón, entre otros.

De acuerdo con el modelo *TCP/IP*[32], cada capa cuenta con protocolos definidos para la comunicación entre dispositivos. El modelo *TCP/IP* cuenta con 4 capas, capa de acceso a la red, Internet, transporte y aplicación y dentro de las mismas funcionan los siguientes protocolos:

[32] Protocolo de Control de Transmisión/Protocolo de Internet: es un modelo de referencia o estándar que tiene como propósito la comunicación de distintos dispositivos a través de protocolos de red logrando la interconexión de estos.

- Capa de Acceso a la red: A este nivel se encuentran algunas tecnologías mencionadas anteriormente como *bluetooth*, NFC, *Wifi*, *Z-wave*, *Zigbee* y algunas más como Ethernet la cual se considera la opción menos costosa ya que se trata de una conexión por cable que garantiza la conectividad con bajos niveles de latencia. LTE es un protocolo para comunicaciones inalámbricas entre dispositivos móviles. El protocolo PLC provee conexión a través de cables eléctricos por donde envía y recibe información y permite el control de un dispositivo *IoT* a través de este. Otro protocolo a nivel físico es el de Identificación por radiofrecuencia o *RFID* por sus siglas en inglés, el cual se usa para monitoreo y seguimiento de etiquetas inteligentes o chips que se instalan en ciertos objetos con el fin de conocer su identificación de forma remota.

The Helium Blog, un sitio web que publica noticias y artículos relacionados con tecnología, realizó una comparativa entre distintos protocolos de Internet de las Cosas, como se ilustra en la **Figura 14** y las mismas fueron comparadas con base en categorías como frecuencia, velocidad de datos, rango, consumo de energía y costo. Este análisis permite identificar la mejor tecnología de acuerdo con el tipo de dispositivo y su accesibilidad.

Figura 14. *Comparativa entre tecnologías en la Capa de Comunicación*

Technology	Frequency	Data Rate	Range	Power Usage	Cost
2G/3G	Cellular Bands	10 Mbps	Several Miles	High	High
Bluetooth/BLE	2.4Ghz	1, 2, 3 Mbps	~300 feet	Low	Low
802.15.4	subGhz, 2.4GHz	40, 250 kbps	> 100 square miles	Low	Low
LoRa	subGhz	< 50 kbps	1-3 miles	Low	Medium
LTE Cat 0/1	Cellular Bands	1-10 Mbps	Several Miles	Medium	High
NB-IoT	Cellular Bands	0.1-1 Mbps	Several Miles	Medium	High
SigFox	subGhz	< 1 kbps	Several Miles	Low	Medium
Weightless	subGhz	0.1-24 Mbps	Several Miles	Low	Low
Wi-Fi	subGhz, 2.4Ghz, 5Ghz	0.1-54 Mbps	< 300 feet	Medium	Low
WirelessHART	2.4Ghz	250 kbps	~300 feet	Medium	Medium
ZigBee	2.4Ghz	250 kbps	~300 feet	Low	Medium
Z-Wave	subGhz	40 kbps	~100 feet	Low	Medium

Nota. Tomado de *802.15.4 Wireless for Internet of Things Developers,* por Vidales, Mike, 2017, 16 de mayo. The Helium Blog (https://blog.helium.com/802-15-4-wireless-for-internet-of-things-developers-1948fc313b2e)

- Capa de Internet: En esta capa se encuentra el protocolo de Internet (IP, por sus siglas en inglés) en sus versiones IPv4 e IPv6. También, se puede encontrar el protocolo 6LoWPAN que como su nombre lo indica, es un protocolo de red de área personal que se usa principalmente en dispositivos con capacidad de procesamiento limitada y baja potencia.

- Capa de Transporte: En esta capa se encuentran el protocolo de control de transmisión (TCP, por sus siglas en inglés) el cual es el usado mayormente para conexiones con Internet proveyendo comunicaciones entre servidores; en este protocolo, se prioriza la calidad sobre el tiempo, es decir, es más importante que los paquetes lleguen completos, aunque exista latencia. Por otro lado, se encuentra el protocolo de diagramas de usuario (UDP, por sus siglas en inglés) el cual permite comunicaciones a través de direcciones IP, en este caso, a diferencia del protocolo TCP, se prioriza el tiempo sobre la calidad, es decir que aumenta la velocidad de transferencia, aunque exista pérdida de datos durante el proceso de transmisión.

- Capa de Aplicación: Algunos de los protocolos que operan en esta capa son:

    - Protocolo avanzado de colas de mensajes (*AMQP - Advanced Message Queuing Protocol*): protocolo de mensajería que permite la comunicación entre aplicaciones, se caracteriza por su escalabilidad y fiabilidad.
    - Protocolo de aplicación restringida *(CoAP - Constrained Application Protocol):* protocolo diseñado para que los dispositivos de baja capacidad puedan comunicarse sin problema, este protocolo permite también la transferencia de documentos el cual se ejecuta a través de *UDP* o protocolo de datagramas de usuario.
    - Servicio de distribución de datos *(DDS - Data Distribution Service):* este protocolo punto a punto permite la activación de pequeños dispositivos y conectarse a redes de alto rendimiento, este protocolo

aumenta la confiabilidad y al mismo tiempo reduce la complejidad y optimiza la implementación de los dispositivos.

- Cola de mensajes Transporte de telemetría *(MQTT - Message Queue Telemetry Transport):* protocolo de mensajería que permite la comunicación entre dispositivos en conexiones de bajo ancho de banda y ubicaciones remotas aprovechando al máximo el ancho de banda y cuidando la batería.
- Protocolo simple de administración de redes *(SNMP – Simple Network Management Protocol):* protocolo que permite la transferencia de datos entre dispositivos de red, se encuentra dentro del conjunto de protocolos *TCP/IP*. Este protocolo permite el monitoreo y administración de los dispositivos y es uno de los protocolos más utilizados dentro de la capa de aplicación.
- Protocolo de transferencia de hipertexto *(HTTP - Hypertext Transfer Protocol)*: este protocolo trabaja también sobre *TCP/IP* y tiene una arquitectura de tipo solicitud-respuesta en donde el cliente realiza la solicitud y espera que el servidor establezca la conexión, procese y devuelva una respuesta. En este protocolo, cliente y servidor son conscientes de la existencia del otro, solamente al momento de la conexión.
- Protocolo extensible de mensajería y comunicación de presencial *(XMPP - Extensible Messaging and Presence Protocol):* Este protocolo de mensajería es basado en *XML* (lenguaje de marcado extensible), originalmente era *P2P*, pero fue adoptado a *M2M* para el intercambio de mensajes *XML*, es considerado un protocolo bastante seguro y flexible además de ser utilizado por grandes compañías como *Facebook* o *WhatsApp*.

Figura 15. *Comparativa de protocolos IoT*

Protocol	Transport	Messaging	2G,3G,4G (1000's)	LowPower and Lossy (1000's)	Compute Resources	Security	Success Stories	Arch
CoAP	UDP	Rqst/Rspnse	Excellent	Excellent	10Ks/RAM Flash	Medium - Optional	Utility field area ntwks	Tree
Continua HDP	UDP	Pub/Subsrb Rqst/Rspnse	Fair	Fair	10Ks/RAM Flash	None	Medical	Star
DDS	UDP	Pub/Subsrb Rqst/Rspnse	Fair	Poor	100Ks/RAM Flash +++	High-Optional	Military	Bus
DPWS	TCP		Good	Fair	100Ks/RAM Flash ++	High-Optional	Web Servers	Client Server
HTTP/ REST	TCP	Rqst/Rspnse	Excellent	Fair	10Ks/RAM Flash	Low-Optional	Smart Energy Phase 2	Client Server
MQTT	TCP	Pub/Subsrb Rqst/Rspnse	Excellent	Good	10Ks/RAM Flash	Medium - Optional	IoT Msging	Tree
SNMP	UDP	Rqst/Response	Excellent	Fair	10Ks/RAM Flash	High-Optional	Network Monitoring	Client-Server
UPnP		Pub/Subscrb Rqst/Rspnse	Excellent	Good	10Ks/RAM Flash	None	Consumer	P2P Client Server
XMPP	TCP	Pub/Subsrb Rqst/Rspnse	Excellent	Fair	10Ks/RAM Flash	High-Manditory	Rmt Mgmt White Gds	Client Server
ZeroMQ	UDP	Pub/Subscrb Rqst/Rspnse	Fair	Fair	10Ks/RAM Flash	High-Optional	CERN	P2P

Nota. Tomado de *Comparativa de protocolos IoT,* por Aprendiendo Arduino, 2018, 17 de noviembre. Aprendiendo Arduino (https://aprendiendoarduino.wordpress.com/category/coap/)

5.1.8.5 ESTÁNDARES Y NORMATIVA *IoT*

Actualmente existen una serie de regulaciones o estándares de cumplimiento aplicables a *IoT*, si bien no es tan amplio el catálogo de estos como en otras tecnologías un poco más conocidas, igualmente son de gran ayuda para conocer, identificar y prevenir los distintos riesgos dentro del Internet de las Cosas.

Probablemente el estándar más conocido es el ISO con sus diferentes normas aplicables a *IoT*, pero además de esta, hay otras regulaciones más definidas y publicadas las cuales serán abordadas dentro de este capítulo.

En 2018 la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) publicaron la norma ISO/IEC 30141 Internet de las Cosas (*IoT*), la cual detalla la Arquitectura de Referencia donde reúne diseños y un set de mejores prácticas dentro de la industria. Comienza explicando las principales características de la tecnología de Internet de las Cosas y posteriormente, proponiendo modelos conceptuales que tienen como propósito el desarrollo de sistemas *IoT* confiables, seguros y robustos. Este estándar se encuentra dirigido tanto a desarrolladores como a organizaciones, ya que las herramientas que proporciona esta norma tienen como fin definir si un dispositivo *IoT* puede catalogarse como seguro de acuerdo con una serie de

pasos y recomendaciones. La creación de este estándar dio también lugar a varias normas más tales como:

- ISO/IEC 30149: Aporta una metodología para la implementación de servicios y sistemas *IoT* garantizando su confiabilidad.
- ISO/IEC 30161-1: Lista los requisitos de la plataforma de intercambio de datos *IoT* para varios servicios *IoT*.
- ISO/IEC 30165: Adicional a lo detallado en la norma ISO/IEC 30161-1, aporta una guía para implementar sistemas *IoT* en tiempo real.
- ISO/IEC 21823: Esta norma se divide en tres partes, en primer lugar, ofrece un marco de referencia para la interoperabilidad entre dispositivos *IoT*, en segundo lugar, detalla los requisitos para ello y, en tercer lugar, presenta una serie de normas para facilitar el intercambio de información a gran escala entre dispositivos *IoT*.
- ISO/IEC 27400 e ISO/IEC 27402: Estas normas son tal vez las más generales y conocidas, ambas detallan los principios de internet de las cosas dándole un enfoque al ecosistema de la domótica en la norma ISO/IEC 27402.

Otra serie de estándares *IoT* fue propuesto por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, por sus siglas en inglés), dentro de ellas se encuentran:

- IEEE P1451.99 - Norma para la armonización de los dispositivos y sistemas del Internet de las cosas (*IoT*): Esta norma propone un método para interoperabilidad y seguridad de los mensajes a través de la red para que distintos dispositivos puedan comunicarse exitosamente sin importar la tecnología de comunicación que se está utilizando.
- IEEE P1912 - Norma para el marco de privacidad y seguridad de los dispositivos inalámbricos de consumo: Esta norma presenta una escala de privacidad aplicable a los datos definidos como información personal que están siendo recolectados por los dispositivos para su posterior procesamiento y uso entre aplicaciones. Los datos presentados en la escala de privacidad brindan a desarrolladores y usuarios de dispositivos *IoT* las diferentes herramientas y características para implementar una correcta configuración de privacidad en estos dispositivos, enfocado a los datos personales. Esta norma es extensible a otras tecnologías diferentes a Internet de las Cosas.

- IEEE P2413-2019 - Norma IEEE para un marco arquitectónico para el Internet de las cosas (*IoT*): Esta norma brinda una arquitectura para *IoT* enfocada a ecosistemas como la salud, transporte, entre otros, en los cuales la interoperabilidad es considerada crítica.

5.1.8.6 PRINCIPALES PROVEEDORES DE *IoT*

Existen actualmente gran variedad de proveedores *IoT* aun cuando esta es considerada aún una tecnología relativamente nueva, como se mencionó anteriormente, el principal foco debe ser la seguridad en cada una de las etapas de desarrollo de dispositivos inteligentes, siguiendo algún marco de referencia y cumpliendo con las normas y estándares recomendadas dentro de esta tecnología, adicionalmente, la responsabilidad del proveedor no termina con el desarrollo del producto, este debe asegurar asistencia y actualizaciones permanentes garantizando la seguridad y confiabilidad de sus dispositivos y la información que los mismos recogen y utilizan.

Los principales proveedores ofrecen también plataformas de gestión de dispositivos (DMP, por sus siglas en inglés) dentro de las cuales se revisan temas como actualizaciones de *firmware*, alertas, métricas y parches de seguridad.

Dentro de los principales proveedores y empresas con plataformas *IoT* en el mercado se encuentran *Amazon*, *Microsoft*, Huawei, AT&T, *Cisco*, Ericsson, Telefónica, Vodafone, Sierra Wireless, Verizon, entre otros.

Realizando una rápida búsqueda en algunos sitios web de los más conocidos comercios electrónicos, por la palabra *Smart* se visualizó que la oferta de productos inteligentes es exageradamente amplia, por ejemplo, en el caso de *Amazon* se encontraron más de 80.000 resultados, en Mercado Libre Argentina se encontraron 59.820 resultados y el *EBay* más de 850.000 dentro de los cuales se encuentran principalmente relojes, cerraduras, celulares, termostatos, juguetes, asistentes de voz, cámaras, impresoras, bombillos, monitores, entre otros.

Como se observa en la **Tabla 1**, los principales proveedores dentro de *IoT* cuentan con un amplio portafolio de productos y soluciones en donde se encuentran no solamente dispositivos sino también plataformas para la gestión de los mismos, garantizando la seguridad, disponibilidad y confiabilidad de los datos que interactúan dentro de los

distintos productos. Es posible observar también, que la mayoría de los productos ofrecidos por los proveedores objeto de estudio, se enfocan en grandes industrias como la salud, transporte o vehicular, aportando soluciones que ayudan a la recolección y análisis de datos, así como también en la reducción de tiempo y tareas cotidianas. Por otro lado, por ejemplo, *Microsoft* a través de su plataforma *Cloud Microsoft* Azure, ofrece soluciones en temas actuales de gran importancia como la sustentabilidad, promoviendo el cuidado del ecosistema a partir de productos que ayudan a la reducción de emisión de gases, monitoreo de la calidad del agua y evitar el desperdicio de los recursos.

Se observa también, que muchos de los proveedores incluidos en la comparativa, hacen mención de *Cellular IoT*, esto hace referencia a una forma de conectar los distintos dispositivos haciendo uso de una misma red tal como los *Smartphone*s esto ayudando a reducir la latencia y el uso de energía.

Tabla 1. *Comparativa entre proveedores IoT. (Elaboración propia)*

PROVEEDOR	CASA MÁTRIZ	FUNDACIÓN	CANTIDAD EMPLEADOS	PORTAFOLIO
Ericsson	Estocolmo, Suecia	1876	101.322+	*IoT Accelerator, Connected Cars*
Telefónica	Madrid, España	1924	104.150+	Gestión de la movilidad, Industria 5.0, Espacios Inteligentes, Monitorización y Gestión Energética, Soluciones Publicitarias.
Microsoft	Redmond, Washington, USA	1975	221.000+	*Microsoft Azure: Connect, monitor, and control devices with secure, scalable, and open edge-to-Cloud solutions, IoT Security, IIoT, IoT for Sustainability, IoT for safer workplaces.*
AT&T	Delaware, Estados Unidos	1983	203.000+	*Networks, platforms, connected cars, asset management, professional services*
Verizon	New York, USA	1983	188.200+	*Connected fleet and field services, Connected assets, Smart Cities and communities, Connected commerce, IoT Security Credentialing, ThingSpace for IoT, IoT, Marketplace, IoT for small business*
Cisco	San Jose, CA	1984	65.225+	*Cisco Industrial Ethernet Switching Portfolio, Cisco Industrial, Router and Gateway Portfolio, Cisco Ultra-Reliable Wireless Backhaul, Industrial Wireless Access Points, Cisco Utility and Field Area Networking Portfolio, Cisco Solution for LoraWan, Cisco Industrial IoT, Embedded Networks Portfolio, Cybersecurity, Connectivity management, Edge Computing, Cisco IOx, Cisco IoT Validated Designs, Featured Design Guides, Cisco IoT Solutions, Cisco Industrial IoT Portfolio*
Vodafone	Newbury, Reino Unido	1984	96.506+	*IoMT, Connected Cars, Banking Finance, Retail, Smart Cities, Logistics, Utilities, Agriculture.*
PTC	Boston, Massachusetts	1985	5.001-10.000	*Industrial IoT-Build, Develop, & Deploy Smart connected solutions.*
Huawei	Shenzhen, China	1987	195.000+	*Smart Cities, Connected Cars, Internet of Elevator, Internet of Smart Building, Big Data analytics.*
ScienceSoft	McKinney, Texas, USA	1989	200-500	*IoT consulting, IoT development, IoT Analytics, IoT Solutions (IIoT, IoMT, Smart Cities, Smart/Connected Products, IoT Applications in*

				Retail), Remote Servicing Software.
ARM	Cambridge, Cambs	1990	1.700+	*Connectivity Management, Device Management, & Data Management.*
Sierra Wireless	Richmond, Canadá	1993	1.007+	*2G, 3G and 4G embedded modules and gateways, seamlessly integrated with its secure Cloud and connectivity services.*
Amazon	Bellevue, Washington, USA	1994	1.468.000+	*Secure device connectivity, management, storage, and analytics*
HQ Software	USA & Europe	2001	50-100	*IIoT, Agriculture IoT, Connected Cars, IoMT, Smart Cities.*
iTechArt	New York, USA	2002	3.515	*IoT application development, MVP development, IoT customization, Data Analytics, Third-Party Integration.*
Oxagile	New York, USA	2005	350+	*End-To-End IoT logistics solutions, Industry 4.0 and agriculture, Healthcare IoT, Connected Living, Next-Gen Useer Gadgets, IoT in sports, IoT-fueled marketing, Connected Cars.*
R-Style Lab	San Fran*Cisco*, CA	2006	51-200	*Wearables, Crafting embedded software for Smart devices and electronics, networking, M2M communication, Smart connectivity, device-to-app data exchange, OTA firmware updates.*
Innowise Group	Warsaw, Poland	2007	1.001-5.000	*Custom IoT software development, IoT web app development, IoT mobile app development, IoT dashboards development, IoT hardware solutions, IoT developers outstaffing.*
SumatoSoft	Boston, USA	2012	51-200	*Fridge Sensors, Fitness Tracking System*
Google	Menlo Park, California, USA	1998	47.756+	*Cloud IoT (Servicio de administración, integración y conexión de dispositivos IoT).*
Philips	Eindhoven, Países Bajos	1891	114.188+	*IoMT, sensores, actuadores, Cellular IoT, embedded softwar development, small signal analog procesing, ultra-low power solutions, accelerate new product introductions, architecting in digital IoT ecosystems, conectivity solutions, RF antenna design & integration, system test & verification, Wi-fi module reference design.*
SAP	Walldorf, Alemania	1972	100.330+	*SAP Leonardo portfolio IoT "It is an innovative portfolio of IoT (Internet of Things) solutions to help you extend your digital core (SAP S/4 HANA) with adaptive (Machine Learning) applications, Big Data applications and connectivity to imagine and implement new business processes, new business models and most importantly, new possibilities in human life. The main drivers for Leonardo are, IoTs, Machine Learning and Artificial Intelligence." (Tomado de: https://business-services-technologies.com/services/sap-leonardo-portfolio-IoT/)*
IBM	Armonk (Nueva York), USA	1911	377.757+	*Enterprise asset management, facilities management, systems engineering. IoT for blockchain cold chain, Connected cars analytics, Real-time performance analysis, real-time motor monitor.*

Finalmente, al momento de elegir un proveedor, es necesario tener en cuenta diferentes aspectos, como su reputación, soporte, escalabilidad, estrategias de recuperación

de desastres (copias de respaldo, *SLAs, KPIs*), actualizaciones constantes de *firmware*, calidad, seguridad, interoperabilidad, entre otros.

5.2*IoT* EN LAS EMPRESAS

Si bien el internet de las cosas es una tecnología emergente que viene tomando bastante fuerza en distintos ambientes, muchas empresas no se arriesgan a incorporarla en gran medida dentro de sus procesos, si bien son conocidas las ventajas, existe el miedo y el escepticismo frente a un nuevo modo de operar y los riesgos que siempre conllevan. Por otro lado, puede darse la incorporación en gran medida a través de sensores, actuadores o dispositivos que hacen uso de esta tecnología, pero no existe consciencia de su uso y por consiguiente no se toman los controles, normas o medidas necesarias para la optimización de estos. De acuerdo con el sitio web *Chakray*, internet de las cosas es hoy en día una realidad dentro de empresas bastante conocidas. Dentro de los mayores casos de éxito de inclusión de Internet de las Cosas en las empresas, *Chakray* destaca la cadena de gimnasios más grandes del mundo *Fitness First*, la cual, de la mano de su director de sistemas de información o *CIO* por sus siglas en inglés, Ed Hutt, está enfocada a ser un gimnasio digital que busca estar en constante interacción con el usuario, cuidando y aumentando su comunidad y promoviendo un estilo de vida saludable.

Por otro lado, el director de *IT* de *Virgin Atlantic Airways*[33], *David Bulman*, fue el encargado de lograr que todas las piezas de las aeronaves Boeing 787 se encuentren conectadas a la red. Gracias a esto, es posible mantener un monitoreo del vuelo incrementando su seguridad, se estima que estos aviones generan cerca de medio terabyte de datos por trayecto.

Como ejemplos adicionales, está el aumento en la línea de producción de la fábrica en México de *Stanly Black and Decker* en donde gracias a la inclusión de la tecnología *RFID* se pudo monitorear y brindar soporte en poco tiempo a sus empleados dentro de la instancia de producción aumentando la calidad de sus productos optimizando tiempos. También, en los parques temáticos de *Disney World* se incorporó también la tecnología *RFID* en sus *MagicBands*, a través de las cuales se reducen tiempos de espera, se recibe

[33] Aerolínea perteneciente al grupo *Virgin*.

información en tiempo real y se obtienen beneficios propios de la compañía mejorando la experiencia del usuario.

Como estas compañías, se encuentran muchos más casos de éxito en donde *IoT* combinado con otras tecnologías, ha logrado contribuir a la calidad de los productos, la mejora del negocio y por consiguiente brindar mejores productos o servicios a sus usuarios.

5.2.1 INTERNET DE LAS COSAS EN LAS EMPRESAS

Una de las aplicaciones principales de Internet de las Cosas es la industria, esta tecnología, al igual que el concepto básico de *IoT*, agrupa personas, datos y sistemas a través de sensores, redes, *software* que haciendo uso de analíticas, automatización y algoritmos, logran conectar personas en todo momento ya sea en un ambiente laboral o personal, mejorando la calidad y seguridad de los servicios y las operaciones.

Dentro del *IIoT* se encuentran la industria de la energía, salud, manufactura, minas, *retail*, transporte, agricultura, *Smart Cities*, entre otras, básicamente cualquier industria en la cual se integren IT y OT, hace parte de *IIoT*. Actualmente, *IIoT* es considerado el segmento más importante y beneficiado dentro de Internet de las Cosas, incluso por encima del *CIoT* o Internet de las Cosas del Consumidor.

IIoT se encuentra estrechamente relacionado con Industrias 4.0, si bien, todas las aplicaciones de Internet de las Cosas dentro de la Industria 4.0 son variables de *IIoT*, no todos los casos de uso de Internet Industrial de las Cosas hacen referencia a industrias catalogadas como Industria 4.0.

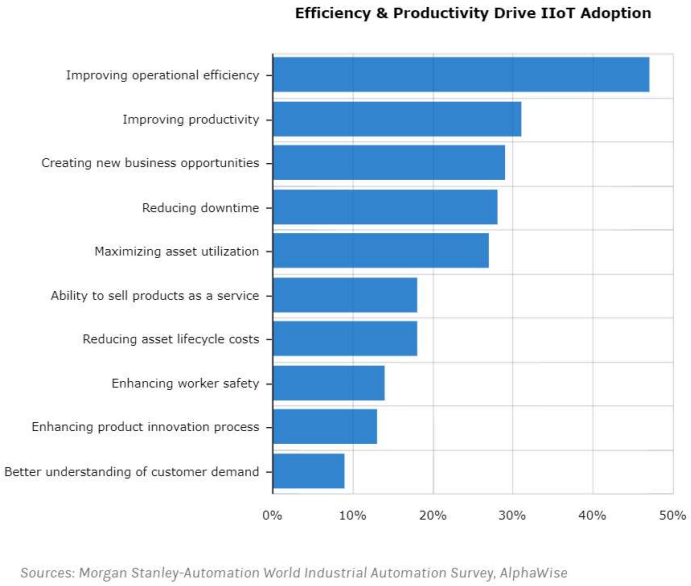
Algunos de estos casos de uso pueden referirse a iluminación inteligente, soluciones de tráfico, agricultura, control de basuras, prevención y detección de desastres naturales, monitoreo y seguridad, redes inteligentes, entre otras aplicaciones que se pueden observar en entornos de *Smart Cities*, refinerías de petróleo, ganadería, centros de salud y demás entornos industriales.

De acuerdo con una encuesta realizada en el 2015 por *Morgan Stanley*[34] y la revista *Automation World*[35] a cerca de 200 ejecutivos de automatización, los principales impulsos

[34] Multinacional financiera estadounidense con principal actividad como agente de bolsa y banco de inversiones.
[35] Editorial especializada en temas relacionados con la tecnología, *software* y dispositivos de automatización industrial.

para la adopción de *IIoT* son la mejora en la eficiencia operacional (47%) y la productividad (31%), por el contrario, en menor importancia se encuentran mejorar el proceso de innovación de productos (13%) y un mejor entendimiento en la demanda del consumidor (9%) tal como se muestra en la **Figura 16.**

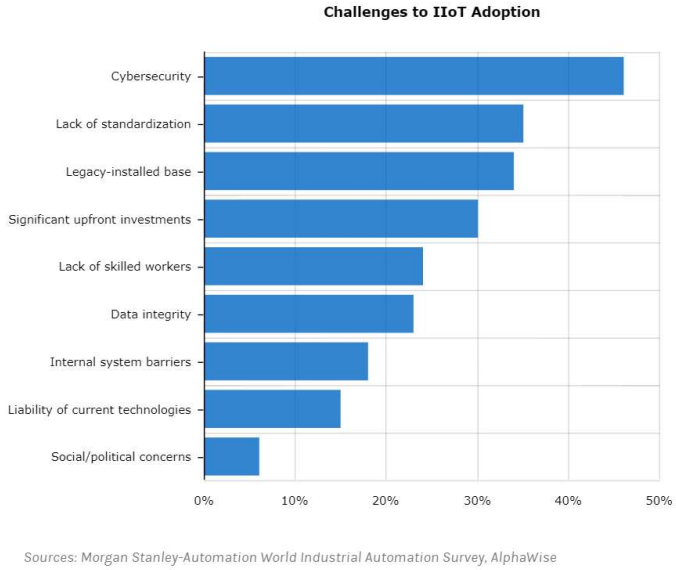
Figura 16. *La eficiencia y la productividad impulsan la adopción de IIoT*



Nota. Tomado de *Efficiency & Productivity Drive IIoT Adoption,* por Morgan Stanley Research, 2016. Morgan Stanley Research (https://www.morganstanley.com/ideas/industrial-internet-of-things-and-automation-robotics)

Dentro de esta misma encuesta, se ubicó en el primer lugar Ciberseguridad (46%) como la mayor preocupación de la adopción de *IIoT* según los ejecutivos encuestados y en último lugar se encuentran las cuestiones sociales y políticas (6%) como se ilustra en la **Figura 17.**

Figura 17. *Retos dentro de la adopción de IIoT*



Nota. Tomado de *Challenges to IIoT Adoption,* por Morgan Stanley Research, 2016. Morgan Stanley Research (https://www.morganstanley.com/ideas/industrial-internet-of-things-and-automation-robotics)

Esto demuestra que la preocupación respecto a la seguridad y la privacidad en dispositivos *IIoT* no es solamente de parte del consumidor, sino también del fabricante, de igual manera, se debe tener en cuenta que garantizar la seguridad en estos dispositivos inteligentes requiere de soluciones robustas para la protección de los datos, también, implica un enfoque en cada parte del proceso, desde la autenticación en el dispositivo y la seguridad de las aplicaciones hasta métodos de respuesta a incidentes, garantías y resiliencia.

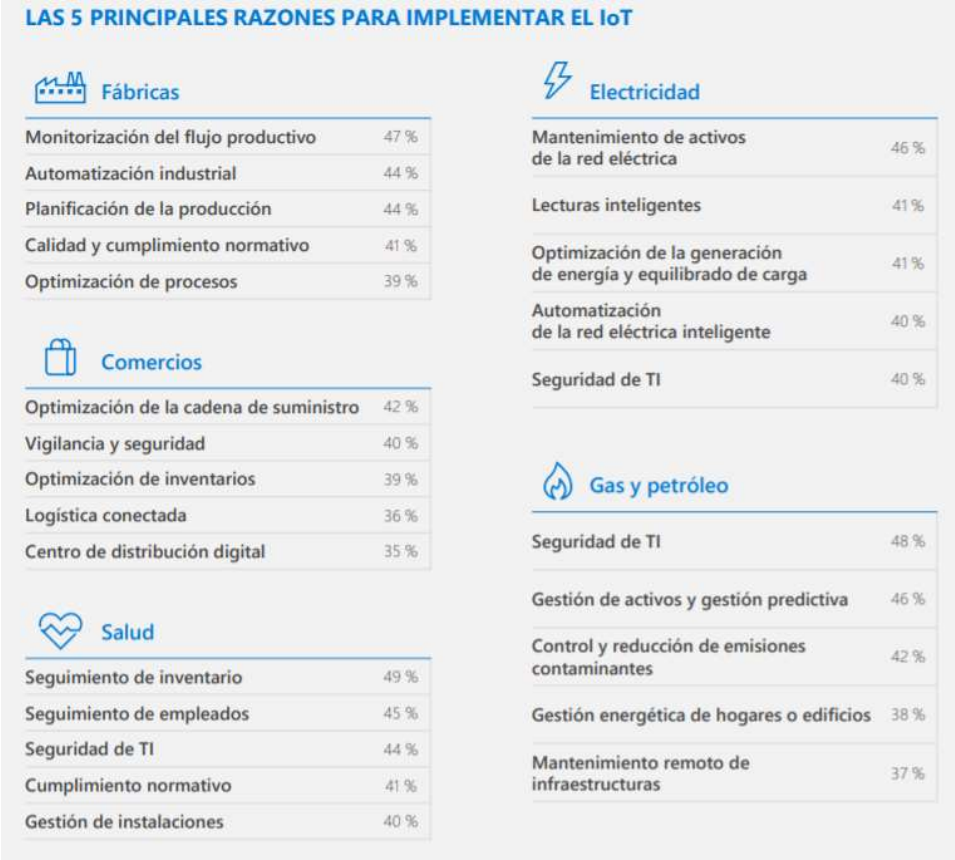
La idea de incluir Internet de las Cosas en la industria se refiere a una mejora en los procesos, aumentar la eficiencia, disminuir la pérdida de tiempo, reducir costos, mantener una comunicación en tiempo real para el mantenimiento o la toma de decisiones oportuna entre otros beneficios.

En la encuesta realizada por *Microsoft* en 2020 a diferentes desarrolladores *BDM* (tomadores de decisiones en las áreas de negocio) e *ITDM* (tomadores de decisiones en el área de IT) que trabajan para grandes empresas (más de 1000 empleados), se les consultó sobre las principales razones para implementar *IoT* en sus empresas de acuerdo con el sector al cual pertenecen.

Como se indica en la **Figura 18**, en las fábricas la principal razón es la monitorización del flujo productivo (47%), seguido por la automatización industrial (44%) y la planificación de la producción (44%). En el sector eléctrico, encabeza la lista el

mantenimiento de activos de la red eléctrica (46%) seguido por las lecturas inteligentes (41%) y en igual medida la optimización de la generación de energía y equilibrado de carga (41%). Dentro de los comercios, predomina como razón principal para implementar *IoT*, la optimización de la cadena de suministro (42%) además de la vigilancia y seguridad (40%). Para el sector de gas y petróleo, la razón principal es la seguridad de las tecnologías de información (48%) seguido por la gestión de activos y gestión predictiva (46%). Finalmente, en el sector salud se impone el seguimiento de inventario (49%), además del seguimiento de empleados (45%) y la seguridad de TI (44%).

Figura 18. *Las 5 principales razones para implementar el IoT*



Nota. Tomado de *Las 5 principales razones para implementar el IoT* (p.14), por *Microsoft*, 2020. *Microsoft* (https://azure.*Microsoft*.com/mediahandler/files/resourcefiles/*IoT*-signals/es-es/*IoT*%20Signals_Edition%202_Spanish.pdf)

De acuerdo con este estudio, algunas de las razones comunes entre sectores para la implementación de *IoT* son la seguridad de las tecnologías de información y el monitoreo de los distintos activos, pero por encima o por debajo de estas razones, se encuentran algunas propias de la actividad del negocio ya que de acuerdo con esto ciertos desarrollos o necesidades son más críticos que los de una empresa de otro sector.

Dentro de *IIoT* convergen otras tecnologías, por ejemplo, gracias al *Big Data* es posible hacer una evaluación y seguimiento de los datos que transmiten los distintos dispositivos con el fin de mejorar los procesos, gracias a los sensores integrados en los dispositivos inteligentes, es posible brindar información a quienes operan los distintos procesos respecto a la toma de decisiones basados en alertas tempranas, prevención y detección de incidentes, aumento o disminución en los tiempos de producción de acuerdo a las necesidades del negocio y demás acciones que logren asegurar la integridad de los procesos.

5.2.2 INDUSTRIA 4.0 E INDUSTRIA 5.0

El proceso de transformación económica, social y tecnológica que se presentó en Inglaterra a finales del siglo XVIII con la invención de la máquina de vapor fue lo que dio lugar a la Revolución Industrial, esta fue evolucionando, dando lugar posteriormente a la segunda revolución industrial con la llegada de la producción en masa a finales del siglo XIX dando lugar al capitalismo ya que, a mayor producción, mayor consumo. Durante las décadas de los 70s y 80s (Siglo XX), se hablaba ya de chips y algo de digitalización, lo cual dio lugar a la Tercera Revolución Industrial, treinta años después, en 2011 llegó la cuarta revolución industrial, también llamada Industria 4.0, la cual hace referencia a la transformación digital de las industrias, en donde se incluye la automatización de los procesos mediante la adopción de nuevas tecnologías que llevan a la optimización de tiempos, toma de decisiones, reducción de costos y errores y simplificación de los procesos.

Además del Internet de las cosas y el Internet Industrial de las cosas, principalmente, la industria 4.0 incluye la adopción de nuevas tecnologías como la nube, *Big Data*, inteligencia artificial y ro*bots*, entre otros.

El concepto de transformación digital hace referencia al cambio en la operatividad de los procesos como se conocen tradicionalmente, y el paso a un ambiente más tecnológico y digital pasando de una producción en masa a una producción más personalizada de los procesos.

El Internet de las cosas representa una porción muy grande e importante dentro de la transformación digital de las empresas ya que, gracias a la implementación de objetos inteligentes en los procesos industriales, se puede mantener un monitoreo constante a

través de alertas y métricas que permiten solucionar problemas en tiempo real, optimizar tiempos y responder asertivamente al público ofreciendo la mejor calidad en sus productos o servicios.

La inclusión de las nuevas tecnologías y la gran variedad de plataformas digitales y productos y servicios en el mercado, han cambiado el hábito de los consumidores y, por consiguiente, la forma en que estos productos y servicios se presentan al usuario. Esto lo podemos ver en el rápido aumento en la eficiencia de tecnologías como la nube o de diferentes productos que constantemente se encuentran lanzando mejoras que prometen mayor eficiencia y reduce tiempos al usuario siendo también productos intuitivos de cada vez más fácil uso, asimismo, la forma en que los servicios o las empresas ofrecen sus productos también ha cambiado, la atención presencial era la única forma de adquirir o conocer productos o servicios hace unos años, actualmente, gracias a la conectividad y los servicios que ofrecen las redes sociales, sistemas de gestión, la implementación de *Bots* y otras plataformas digitales enfocadas a empresas, es mucho más fácil tener un contacto directo con el usuario con el fin de resolver dudas, brindar soluciones o vender productos/servicios en un tiempo casi inmediato.

La industria 4.0 o transformación digital supone, como su nombre lo indica, una transformación en los hábitos, lo cual, apoyado con un avance tecnológico, ha llevado a una rápida adopción a nuevas tecnologías y costumbres y, por consiguiente, a la Industria 5.0 de la cual se comenzó a hablar en 2021.

Anteriormente, expertos en transformación digital pensaban que la quinta revolución industrial estaría presentándose en el 2029 aproximadamente, el hecho de que actualmente ya se esté mencionando incluso cuando aún no todas las personas se encuentran familiarizadas con la transformación digital o algunas de las nuevas tecnologías, significa que hubo una gran adopción por gran parte de la sociedad a los cambios que trajo la Industria 4.0, sumado a esto, la aceleración de la digitalización que trajo consigo la pandemia en 2020 donde tanto las empresas como las personas se vieron obligadas a cambiar completamente sus rutinas y la forma de realizar sus procesos y por consiguiente, la forma de llevar su día a día.

La falta de presencialidad no podía suponer la desaparición de las empresas, estas debieron adaptarse y la forma de estar presentes al usuario fue a través de la conectividad, incorporando o aumentando la inclusión de nuevas tecnologías en sus compañías, esto se vio tanto en grandes como medianas y pequeñas empresas, además de otro tipo de ambientes como gobiernos o escuelas que también tuvieron que adaptarse incluyendo

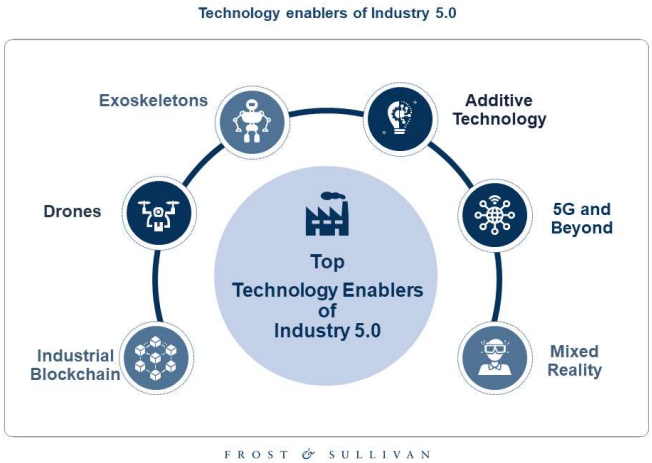
nuevas tecnologías para mantenerse presente en su misión sin verse muy afectados por la situación sanitaria del momento.

Todo esto muestra la rápida adopción de la tecnología en diferentes ecosistemas y la interacción con las personas, la cual incluso después de la pandemia se mantuvo y siguió creciendo, por lo cual actualmente ya se escucha hablar de una quinta revolución industrial, esta, a diferencia de la Industria 4.0 vuelve a darle un lugar protagónico al humano, no a la máquina.

La firma estadounidense de consultoría Frost & Sullivan, definió industria 5.0 como "un modelo del siguiente nivel de industrialización caracterizado por el retorno de la mano de obra a las fábricas, la producción distribuida, las cadenas de suministro inteligentes y la hiperpersonalización, todo ello con el objetivo de ofrecer una experiencia de cliente a medida una y otra vez." (Frost & Sullivan, 2019), según esta definición, la producción dará prioridad a las necesidades y gustos del cliente, creando productos personalizados lo cual no será problema para las empresas ya que tendrán a la mano tecnologías como ro*bots* que minimizarán el problema de producción en masa, esto lo harán fábricas inteligentes que luego enviarán el producto a fábricas convencionales en donde la mano de obra humana le dará la personalización final y necesaria a cada producto, siendo este un proceso híbrido en igual medida entre humanos y tecnologías, afirma Frost & Sullivan.

La compañía afirma también que si bien la cuarta revolución industrial trajo consigo nuevas tecnologías, lideradas por el *IoT*, esta quinta revolución sobresaldrá también con tecnologías no tan exploradas o utilizadas actualmente como *blockchain* industrial, drones, tecnología aditiva (como impresión 3D, 5G, metaversos, entre otros como se ilustra en la **Figura 19**.

Figura 19. *Principales facilitadores tecnológicos en la Industria 5.0*



Nota. Tomado de *Technology enablers of industry 5.0,* por Frost & Sullivan, 2019. Frost & Sullivan (https://www.frost.com/frost-perspectives/industry-5-0-bringing-empowered-humans-back-to-the-shop-floor/)

Según la Comisión Europea, en su documento *Industria 5.0. Hacia una industria europea sostenible, centrada en el ser humano y resiliente*, explica cómo la industria 5.0 logrará una relación pareja entre la sociedad y la industria europea siendo la quinta revolución industrial un beneficio para el trabajador, más que una amenaza. Afirma también, que no entienden la Industria 5.0 como un remplazo o una continuación de la 4.0, más bien como "el resultado de un ejercicio de prospectiva, una forma de enmarcar cómo coexistirán la industria europea y las tendencias y necesidades sociales emergentes. Como tal, la Industria 5.0 complementa y amplía las características distintivas de la Industria 4.0." (De Nul, Petridis, & Breque, 2021).

Finalmente, la industria 5.0 busca volver a darle el lado humano a los procesos y productos finales, esto también debido a que, si bien estamos en un mundo mucho más digitalizado y virtual cada día, dentro de esa misma virtualidad se busca algo de realidad, esto lo podemos ver en los juegos, aplicaciones e incluso lo que últimamente se conoce como *metaverso* que es un entorno que relaciona la virtualidad con la realidad. De la mano de esta realidad dentro del mundo digital, también se buscan experiencias más personalizadas, lo que da lugar al otro principio de la quinta revolución industrial, la customización de los productos. Todo esto va dando lugar a lo que en John Von Neumann[36] en 1957 llamó *Singularidad* y más adelante tomó mayor popularidad como *Singularidad tecnológica* que hace referencia al momento en el cual las máquinas alcanzarán y superarán la inteligencia humana.

[36] Matemático y Físico Húngaro considerado uno de los matemáticos más importantes del siglo XX.

5.2.3 ADOPCIÓN DE *IoT* EN LAS EMPRESAS

Tal como se detalló al inicio del presente capítulo, *IoT* es una realidad dentro de grandes, medianas y pequeñas empresas que buscan optimizar sus procesos y brindar una mejor experiencia de usuario.

Son innumerables casos de éxito y se encuentran en diferentes sectores de mercado, esto se debe a que el Internet de las cosas beneficia a la conectividad y gestión entre el usuario y la empresa, además de los ejemplos mencionados en la introducción del presente capítulo se encuentran también los siguientes:

La compañía Rolls Royce[37] encontró que existe cierta dificultad en la reparación de los motores de diferentes máquinas (aérea, marina, minería, entre otros) debido a la poca visibilidad en sus ciclos de uso y mantenimiento, asimismo, teniendo en cuenta la relevancia de los motores dentro de cualquier tipo de maquinaria, la compañía resolvió que para tener un monitoreo constante y por consiguiente realizar el mantenimiento necesario minimizando siniestros, debía incorporar sensores en sus motores los cuales ayudarían a rastrear su ubicación y producirían información relacionada a su uso y estado. Los datos que emiten estos rastreadores son enviados a las áreas de soporte a través de una aplicación web y a una aplicación móvil a la cual el cliente puede acceder a información de la ubicación y estado de los rastreadores de su motor. El diseño y desarrollo por parte de Rolls Royce en conjunto con el equipo Central de Tecnología *IoT* de Singapur los llevó a conseguir el premio Sir Henry Royce por Tecnología e Innovación en los negocios.

La innovación que trae la adopción de *IoT* en productos y procesos no tiene límite. En 2015 la compañía *Diageo*[38], en asociación con *Thin Film Electronics*[39], presentaron su innovador producto en el Congreso Mundial de Móviles[40] en Barcelona, se trata de la botella inteligente Johnnie Walker etiqueta azul, la cual contiene sensores impresos, como se observa en la Figura 20, que hacen uso de la tecnología *NFC* los cuales al ser leídos envían información a la aplicación móvil del producto, esto representa no solo una innovación en cuanto a integración de tecnología *IoT* con productos alimenticios sino

[37] Empresa británica de tecnología industrial líder en producción de motores aeronáuticos.
[38] Empresa británica dedicada a la fabricación y distribución de bebidas alcohólicas.
[39] Empresa noruega de fabricación de microbaterías.
[40] Congreso anual celebrado en Barcelona (España) enfocado a la comunicación móvil.

también una evolución del código QR[41] el cual puede ser copiado o modificado fácilmente y en algunos casos difícil de leer. La incorporación de sensores impresos en la botella de whisky no solamente brinda información al cliente sobre el producto, también, brinda a la compañía información de gran valor en cuanto a estrategias de marketing la cual es útil para tomar decisiones y conocer hábitos de consumo de sus clientes.

Figura 20. *Botella Inteligente Johnnie Walker Blue Label*

Nota. Tomado de *Johnny Walker lanza botella inteligente,* por The Food Tech, 2015, 12 de marzo. The Food Tech (https://thefoodtech.com/historico/johnny-walker-lanza-botella-inteligente/)

En el sector energético, la compañía *British Gas*[42] desarrolló *Hive*, una serie de soluciones que permiten administrar la energía del hogar de forma fácil y eficiente ofreciendo productos como termostatos, conectores, sensores, luces y demás objetos inteligentes que integran el ecosistema de la domótica.

En Colombia, un *startup* modelo *B2B*[43] (*Business to Business*, por sus siglas en inglés) llamado *TechnoApes* ofrece soluciones a otras empresas en cuanto a automatizaciones en procesos como el control de inventarios, reconocimiento de imágenes, estrategias de ventas, entre otros, a través de etiquetas *RFID* y tecnología *blockchain*, dentro de estas empresas se encuentran Adidas[44], *LATAM Cargo*[45], *Smart Fit*[46], *Mario Hernández*[47], *IBM*, entre otros.

---

[41] *Quick Response*, evolución del código de barras.
[42] Empresa británica dedicada a proveer energía y servicios para el hogar en Reino Unido.
[43] Modelo de negocio en el cual las empresas dirigen sus productos y/o servicios a otras empresas para facilitar el desarrollo de sus actividades.
[44] Multinacional Alemana dedicada a la fabricación de indumentaria y equipamiento deportivo.
[45] Aerolínea dedicada al transporte de carga de Brasil.

Como ejemplo más reciente, para el mundial de fútbol Qatar 2022, Adidas diseñó la pelota del campeonato llamada *Al Rihla*, la cual contenía un sensor en su interior, como se observa en la **Figura 21**, con el fin de identificar posiciones irregulares dentro del campo, también recopilar información relacionada con la velocidad de la pelota, su orientación y fuerza gravitacional enviando un alrededor de 500 paquetes de datos por segundo a la central, lo cual permitía obtener información exacta e inmediata sobre el balón al momento de ser golpeado.

Esta pelota fue sometida a diversas pruebas las cuales incluían túneles de viento e incluso análisis de rendimiento en distintas canchas de fútbol realizadas por varios futbolistas, entre ellos el actual campeón del mundo Lionel Messi.

Figura 21. *Pelota oficial del mundial de fútbol Qatar 2022.*

Nota. Tomado de *La pelota contiene en su interior un sensor de Unidad de Medición Inercial,* por Adidas, 2022. Meteored (https://www.meteored.com.ar/noticias/actualidad/la-pelota-del-mundial-de-qatar-2022-usa-inteligencia-artificial-imu-al-rihla-offside-lautaro-martinez-argentina-mexico.html)

La implementación de esta tecnología viene de años atrás, en el mundial Rusia 2018 se incorporó el sistema de video arbitraje (VAR, por sus siglas en inglés) y en Qatar 2022 combinando *IoT* con IA se ha desplegado un total de 12 cámaras que permiten captar con exactitud los movimientos de la pelota y las posiciones de los jugadores y enviar a través del chip incorporado información exacta relevante para el correcto desarrollo del juego.

---

[46] Red de gimnasios líder en América Latina.
[47] Casa de moda Colombiana enfocada en el diseño de productos en cuero de lujo.

Como se ha mencionado anteriormente, no es posible depender totalmente del trabajo de la máquina y en esta ocasión era completamente necesario la integración humana para hacer de este un desarrollo *semiautomático*, si bien la tecnología *AIoT*, (como se le llama a la integración de *IoT* con *AI*) recopila información útil, exacta y difícil de conseguir por el humano de forma precisa e inmediata, este debe utilizarla para la toma de decisiones y corrección de errores especialmente en situaciones que pueden generar polémica como fue en el caso del partido Argentina vs. Arabia Saudita en la fase de grupos del mundial de fútbol **(Figura 22).** Si bien la tecnología funciona correctamente, es necesaria la intervención humana para no depender totalmente de los datos recopilados si los mismos no se ajustan al resultado esperado al momento de desarrollar dicha tecnología.

Figura 22. *Resultado VAR en partido Argentina vs. Arabia Saudita en Mundial de Fútbol Qatar 2022*

Nota. Tomado de *Lautaro Martinez convierte un gol que fue posteriormente invalidado,* por @ArchivoVAR, 2022. Meteored (https://www.meteored.com.ar/noticias/actualidad/la-pelota-del-mundial-de-qatar-2022-usa-inteligencia-artificial-imu-al-rihla-offside-lautaro-martinez-argentina-mexico.html)

Como se observa con los ejemplos detallados anteriormente, la inclusión de *IoT* se encuentra presente en diferentes industrias, según *Kaspersky*, el mayor incremento de *IoT* se ha visto en el sector hotelero (pasó del 53% en 2018 a un 63% en 2019) aunque teniendo en cuenta la positiva y rápida adopción de los usuarios a esta tecnología, estas estadísticas se encuentran en constante crecimiento a pesar de las diferentes vulnerabilidades a las cuales se encuentran expuestas varias de las soluciones ofrecidas en el mercado.

Es por esto por lo que las empresas deben tener en cuenta una serie de recomendaciones y buenas prácticas al momento de adoptar la tecnología *IoT* en sus productos y/o procesos, si bien trae grandes y numerosos beneficios, puede asimismo traer grandes consecuencias si no se hace un análisis completo antes, durante y después de su implementación. Esta tesis, pretende ayudar a las empresas en este análisis a través de una serie de controles que se pueden implementar para prevenir o detectar errores de seguridad desde Internet de las Cosas, también ofrece una serie de recomendaciones y buenas prácticas en torno a la inclusión de la tecnología *IoT* en empresas en proceso de transformación digital.

5.2.4 VECTORES DE ATAQUE *IoT* EN LAS EMPRESAS

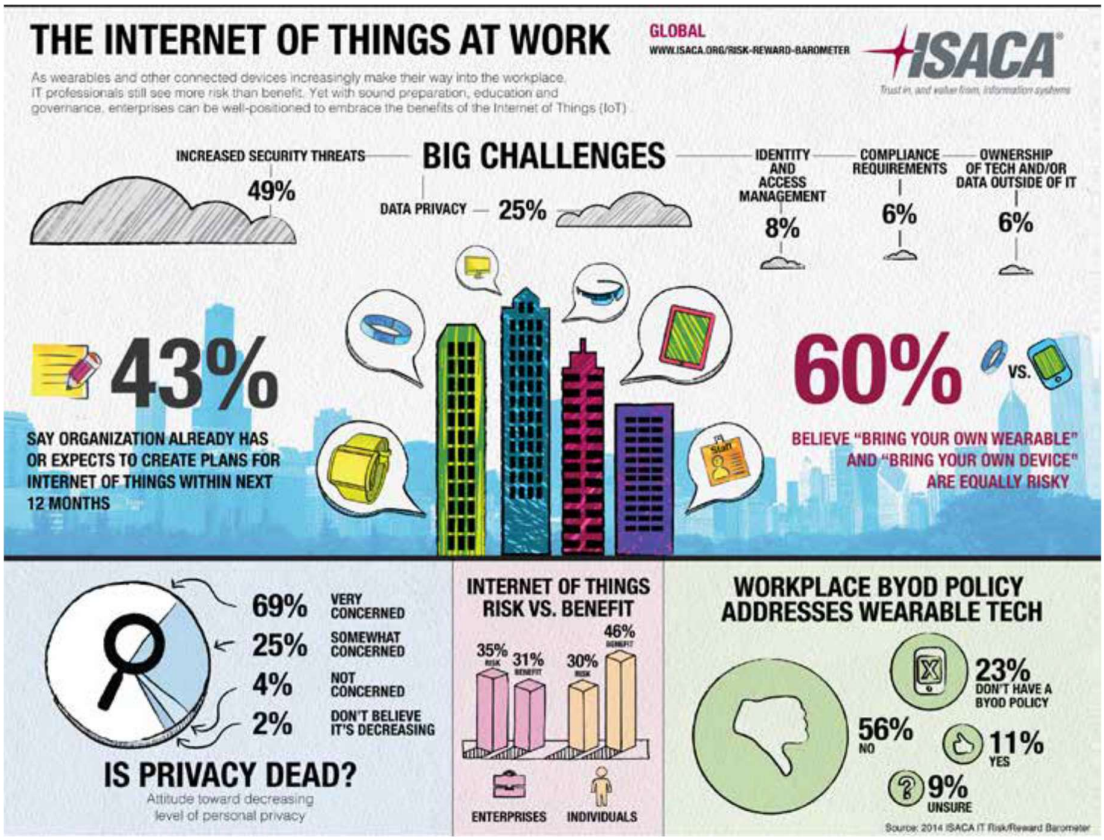
La llegada de la tecnología de Internet de las Cosas junto con otras tecnologías emergentes supone también la llegada de nuevo forma de exponer y tratar los datos en internet, asimismo nuevas formas de ataques de las cuales no existen planes de acción los cuales pueden traer como consecuencia exposición de datos sensibles, extorsiones, daños físicos de los dispositivos y demás consecuencias conocidas, pero haciendo uso de nuevos vectores de ataque.

De acuerdo con *ISACA*[48], la encuesta realizada a miembros globales de esta institución en 110 países, el 43% de las empresas tienen o se encontraban en proceso de inducción de internet de las cosas en su organización, también se demuestra en la encuesta ilustrada en la **Figura 23** que el 60% de las empresas consideran que políticas *BYOD* (*bring your own device*) y *BYOW* (*bring your own wearable*) son igualmente riesgosas. Asimismo, las empresas encuestadas encuentran que el mayor riesgo de la adopción de *IoT* en las empresas es el aumento en los riesgos de seguridad y la privacidad de los datos, en

[48] *Information Systems Audit and Control Association*. Asociación que promueve el desarrollo de certificaciones y metodologías para realizar actividades de auditoría y control en los sistemas de información.

menor medida, destacan los requerimientos de cumplimiento o el uso de tecnología fuera del área de IT. Esto refleja también que en las empresas los riesgos y beneficios de uso de *IoT* es bastante parejo mientras que en los usuarios finales hay una mayor diferencia, 46% de beneficios y 30% riesgos. Estos porcentajes demuestran, entre otras cosas, por qué la lenta y baja adopción de *IoT* en las empresas.

Figura 23. *Encuesta ISACA "2014 ISACA Risk/Reward Barometer"*



Nota. Tomado de *The Internet of Things at Work,* por ISACA, 2014, ISACA (www.isaca.org/pages/2014-risk-reward-barometer.aspx)

Los riesgos de la implementación de *IoT* en las empresas depende principalmente del tipo de industria, no es lo mismo por ejemplo vulnerar un marcapasos inteligente que un detector de humo. A mayor nivel de sensibilidad de los datos y de exposición de los mismos, mayores precauciones se deben tener para la protección de estos ya que en el momento en que se vulneran los datos de una compañía, los datos privados de los usuarios se encuentran expuestos a ser manipulados de diversas formas.

Al momento de implementar la tecnología *IoT* en las empresas es necesario tener en cuenta una serie de situaciones para determinar posibles riesgos, partes interesadas, entre otros. En primer lugar es necesario tener claro el objetivo del dispositivo que se esté incorporando, de acuerdo con esto cuáles serían las posibles amenazas nuevas o existentes

a dar prioridad, también, es necesario conocer las personas o grupos de personas que harán uso este dispositivo y con qué grado de involucramiento, para conocer los accesos permitidos y el tipo de información a procesar, es importante también tener claros los procedimientos y controles para mantener los dispositivos actualizados como forma de prevenir ataques por falta de implementación de parches o nuevas versiones. Se deben también establecer roles sobre la supervisión y monitoreo de los dispositivos implementados y el tipo de información que recopila y cómo esto se encuentra protegido y disponible en todo momento. Finalmente, es importante conocer cómo estos datos trabajan y cómo interactúan con otros dispositivos principalmente porque es primordial los datos que estos dispositivos estén recopilando de forma directa o indirecta.

Una vez implementado el o los dispositivos *IoT* en la empresa, como en cualquier proceso tecnológico/operacional, el mayor riesgo lo representa el factor humano por lo cual la forma primordial para minimizar este riesgo es la concientización de empleados en todas las áreas, lo cual también es una deficiencia, ya que se suele capacitar solamente al área de tecnología cuando una amenaza puede llegar por cualquier área y todo el personal debe estar capacitado para actuar de la mejor forma.

Esta concientización de trabajadores dentro de la compañía ayuda a mejorar en gran medida la ciberseguridad de la compañía, aunque esto debe ir acompañado de una serie de controles que mitiguen riesgos y la comunicación de mejores prácticas para tener en cuenta en el día a día laboral, muchas de estas recomendaciones no son aplicadas solamente a dispositivos *IoT*, de hecho son genéricas para ambientes no solo laborales pero ayudan a mantener un ambiente tecnológico seguro, esto por ejemplo, es el uso de contraseñas robustas, configuración de dispositivos eliminando la configuración por defecto, protección de los datos y en general, tomar conciencia de los riesgos relacionados a la seguridad tecnológica de forma general. Finalmente, además de tomar conciencia sobre los activos tecnológicos y su mejor uso, es necesario también tomar conciencia sobre los datos que se manejan y los riesgos a los que se encuentran expuestos desde diferentes ámbitos los cuales pueden convertirse en vectores de ataque.

5.3EVALUACIÓN (AUDITORÍA O CONSULTORÍA) EN CIBERSEGURIDAD

Una auditoría en ciberseguridad es necesaria en una compañía para asegurar el ambiente tecnológico en los distintos procesos y detectar vulnerabilidades que puedan existir en un ambiente de tecnología y comunicación (TIC) tanto en infraestructuras de tecnología de la información (IT) como tecnología de las operaciones (OT). La auditoría en ciberseguridad, al igual que cualquier tipo de auditoría brinda un panorama completo respecto a la situación de la empresa y por consiguiente las decisiones o acciones a tomar respecto a los resultados de esta para asegurar la confidencialidad, disponibilidad e integridad de información en los distintos sistemas. Dentro de una auditoría, es necesario tener en cuenta aspectos generales de seguridad para mitigar riesgos a través de controles preventivos y detectivos, adicionalmente, se deben tener en cuenta las regulaciones aplicables al territorio, por ejemplo, está el caso más común que es la regulación sobre protección de datos personales, en el caso argentino es la ley 25.326, decreto número 1558/2001 la cual busca proteger los datos personales resguardándolos en distintos medios físicos y digitales para su tratamiento.

Dependiendo el tamaño de la compañía y su involucramiento tecnológico, la auditoría puede abarcar más o menos aspectos, en todo caso, existen aspectos generales a tener en cuenta como análisis de redes, capacitaciones, inventario de *hardware* y *software*, políticas y procedimientos, actualización de sistemas, revisión de vulnerabilidades, entre otros.

Dentro de los distintos tipos de auditoría se encuentran por ejemplo las auditorías web las cuales analizan el rendimiento de un sitio web de acuerdo con su diseño, infraestructura y contenido para evaluar su nivel de seguridad, esto mismo se hace en una auditoría de código que revisa que el código fuente esté acorde a las mejores prácticas y estándares de seguridad, similar a esto se realiza en las auditorías de red analizando tráfico, protocolos y uso de recursos para evaluar el rendimiento de la red. También, están las auditorías de hacking ético la cual intenta vulnerar los sistemas de la compañía, con su consentimiento, para evaluar la seguridad de estos a través de distintas pruebas de ciberseguridad. Finalmente, existen auditorías enfocadas a distintas normativas, dentro de las cuales están las auditorías de certificación SOX para empresas que cotizan en la bolsa de valores de Nueva York, la ISO 27001 sobre seguridad de la información, la ISO 22301 sobre la gestión de continuidad del negocio, entre otros.

Si bien las auditorías suelen realizarse cada cierto periodo de tiempo, los controles deben revisarse de forma más constante con el fin de asegurar buenos resultados en la auditoría.

Para garantizar un buen manejo en la seguridad de las compañías, es importante tener en cuenta los diferentes puntos de ataque e invertir en una arquitectura robusta que soporte los distintos controles definidos para el monitoreo de seguridad dentro de la empresa. En caso de contar con una buena arquitectura tecnológica, es importante mantener el monitoreo y buen mantenimiento sobre los sistemas para garantizar la correcta ejecución de los controles previniendo y detectando ataques informáticos.

Como parte de los controles generales a tener en cuenta, es importante considerar las diferentes normativas aplicables, dentro de estas se encuentran las distintas políticas y procedimientos para la correcta ejecución de los procesos en la cual se debe especificar el paso a paso de las tareas, tiempos y responsables, las mismas deben mantenerse actualizadas y garantizar su cumplimiento.

También, como medida importante, se debe considerar una buena ciberseguridad, esto puede considerarse como una medida para prevenir ataques de ingeniería social y esto incluye capacitaciones y ejercicios de ciberseguridad dirigidos a todo el personal y de carácter mandatorio. Es importante tener en cuenta que el usuario es siempre el eslabón más débil y puede representar la puerta de entrada a distintos tipos de ataques de ciberseguridad.

5.3.1 SITUACIÓN ACTUAL: EVALUACIONES DE CIBERSEGURIDAD EN LAS EMPRESAS

Existen diferentes formas de realizar una auditoría en ciberseguridad en la compañía y esto depende del tamaño de la misma, el enfoque y el propósito. El objetivo es siempre el mismo, conocer y detectar las diferentes vulnerabilidades que se pueden presentar en la compañía y a partir de dónde surgen, para así tomar las medidas correspondientes.

Lo recomendable es comenzar realizando un análisis de la situación actual de la empresa, recopilar toda la información base necesaria para obtener un panorama amplio y actualizado, esto se hace a través de documentos como inventarios de *hardware* y *software*, listado de activos, herramientas utilizadas, entre otros. A partir de esto es posible conocer los puntos débiles de la compañía en cuanto a ciberseguridad dando lugar a la toma de decisiones para reducir las vulnerabilidades detectadas y mitigar los diferentes riesgos. Este tipo de evaluación debe realizarse de forma periódica, para ello, una gran

ayuda es la implementación de controles de seguridad tanto preventivos como detectivos, las capacitaciones y el cumplimiento de las mejores prácticas de seguridad.

Es importante, en primera instancia, definir el objetivo de la auditoría a realizar, ya que como se mencionó al principio de este capítulo, una evaluación en ciberseguridad puede llevarse a cabo de acuerdo con el enfoque definido, el cual puede ser para evaluar una actividad o proceso en particular, o para una revisión global dentro de la compañía.

Una vez definido el o los objetivos de la evaluación en ciberseguridad, se debe realizar un plan de trabajo en donde se detalle el alcance de la revisión y, por consiguiente, los procesos, herramientas y actividades a validar.

De acuerdo con el plan de trabajo, se debe obtener toda la información y documentación necesaria que ayude para el enfoque de la revisión en el alcance definido, esto se hace a través de reportes de los distintos sistemas, revisión de listados e inventarios y también, reuniones con los diferentes referentes de los procesos en alcance para conocer la operatoria de las distintas tareas o actividades.

Toda esta información recopilada, debe ser analizada para encontrar las distintas debilidades que pueden representar algún tipo de vulnerabilidad y así tomar acciones correctivas, también, puede utilizarse para robustecer la operatoria de los distintos procesos y estandarizarlos para mantener un control sobre las actividades que se realizan o incluso para conocer un estado de los sistemas de la compañía y realizar los cambios o implementaciones necesarias.

Finalmente, al conocer a detalle la operatoria de los procesos en alcance, la documentación existente y el estado de los sistemas, se puede emitir un informe detallado de los resultados obtenidos, observaciones realizadas, vulnerabilidades detectadas, recomendaciones y pasos a seguir. Este informe ayuda a brindar un detalle sobre la posición actual de la compañía en términos de seguridad y funciona como base para próximas auditorías y realizar un seguimiento sobre las observaciones detectadas y los pasos a seguir para mejorar la seguridad.

Estos pasos mencionados anteriormente funcionan como base para evaluación en ciberseguridad en cualquier tiempo de empresa ya que actualmente, prácticamente todas las compañías dependen de la interconexión y herramientas informáticas, por lo cual las vulnerabilidades pueden presentarse sin importar la cantidad de recursos o herramientas con las que se cuenten, el riesgo existe siempre. Es importante aclarar esto, ya que muchas veces se tiene la percepción de que si una empresa es pequeña, es inmune o poco probable a ser víctima de un ciberataque, al contrario de empresas grandes y robustas que si

necesitan implementar fuertes medidas de seguridad debido a la gran cantidad de actividades que realizan, como se mencionó anteriormente, una vez se integra la tecnología en un ambiente, ya la exposición a un riesgo de ciberseguridad existe, sea una pequeña, mediana o grande empresa. Para entender esto, es necesario conocer los distintos riesgos y tipos de ataques que se pueden presentar, para ello, la base para una buena evaluación de seguridad siempre será la educación y el control constante a través de actividades para la prevención y detección de vulnerabilidades. Muchas veces no se tiene consciencia sobre las vulnerabilidades a las que se encuentra expuesto, una evaluación o auditoría en ciberseguridad es la manera ideal de conocer los distintos riesgos a los que se está o se podría estar expuesto.

Las compañías suelen contar con un equipo de auditoría interna la cual es realizada por recursos propios de la empresa, y también con equipos de auditoría externa que son empresas contratadas para realizar algún tipo de auditoría solicitado, esto dependiendo del objetivo. Dentro de las distintas auditorías de ciberseguridad se encuentran:

- Auditorías forenses: Son realizadas posterior a un incidente de ciberseguridad, tienen como finalidad recopilar información y pruebas sobre las causas de dicho incidente.
- Auditorías web: Se realizan sobre las distintas aplicaciones y sitios web para conocer las distintas vulnerabilidades que se puedan presentar.
- Auditorías de redes: Es uno de los tipos de auditorías más importantes debido a los riesgos que se pueden encontrar allí. En este tipo de auditoría se realiza un mapeo de redes y dispositivos conectados y a partir de allí se realizan distintas validaciones, como actualizaciones de *software*/*firmware*, antivirus, cortafuegos, *VLANs*, protocolos, usos de *VPNs*, entre otros.
- Auditorías de código: Como su nombre lo indica, se realiza una revisión de los códigos fuentes para identificar vulnerabilidades.
- Análisis de vulnerabilidades: Este tipo de revisión se lleva a cabo para identificar las diferentes brechas de seguridad que se puedan presentar.
- Hacking ético: Se trata de un *test* de intrusión en el cual se hace uso de las diferentes técnicas y tácticas que llevan a cabo los atacantes, pero esta vez con total permiso y conocimiento de la compañía, con el fin de conocer el nivel de seguridad de los sistemas a través de diferentes pruebas.

También, existen tres tipos de auditorías de ciberseguridad que se clasifican de acuerdo con la información proporcionada, estas son:

- Auditorías de caja blanca: En este caso, se le proporciona al auditor todo tipo de información y accesos necesarios para su revisión, este realiza una serie de pruebas en la que intentará encontrar y explotar vulnerabilidades en los sistemas, simulando ser un recurso interno de la compañía.
- Auditorías de caja gris: En este caso, los auditores pueden encontrar limitaciones a la información o el acceso a los sistemas. En este caso, se lleva a cabo un test simulando ser un tercero o un recurso interno con pocos privilegios o un recurso en particular, para intentar encontrar vulnerabilidades en los sistemas.
- Auditorías de caja negra: Para esta auditoría, no se cuenta con ningún tipo de dato o acceso a los sistemas, una vez más, el auditor intenta ingresar a través de distintas pruebas, desde afuera de la compañía, para identificar vulnerabilidades, pero esta vez, sin ningún tipo de información proporcionada. Para ello, el auditor intentará desde afuera recopilar la mayor cantidad de información útil y con ello intentar ingresar a los sistemas con lo cual puede identificar posibles vulnerabilidades.

5.3.2 EVALUACIÓN DE SEGURIDAD ENFOCADA A *IoT*

Actualmente, debido al auge del Internet de las Cosas, múltiples compañías han comenzado a ofrecer sus servicios de auditoría enfocada a esta tecnología, esto se ofrece como un servicio bastante innovador el cual propone securizar los dispositivos inteligentes en las distintas redes y evitar incidentes de seguridad. Esto supone una mejora en las revisiones de seguridad ya que suele dejarse de lado este tema aun cuando su uso es bastante frecuente y un mal control de ello puede suponer grandes consecuencias. Estas revisiones parten de la falta de seguridad y actualizaciones por parte de los fabricantes y asimismo la falta de foco en la seguridad por parte de los usuarios. Para estas revisiones se toman en cuenta metodologías como *OWASP*, vulnerabilidades conocidas y arquitectura de los dispositivos a revisar, ya que aun cuando pertenecen a una misma tecnología, pueden funcionar de distintas maneras haciendo uso de recursos en formas diferentes.

El fin de una evaluación en seguridad enfocada a *IoT*, es garantizar la seguridad de los dispositivos inteligentes, esto a través de un análisis del *firmware*, *hardware*, aplicaciones, redes, conectividad, recursos, datos procesados, entre otras actividades.

Los beneficios de estas revisiones son similares a los de una auditoría en seguridad, los cuales incluyen garantizar la seguridad de los sistemas, redes y aplicaciones, desarrollar actividades para la prevención y detección de vulnerabilidades, generación de normas, políticas y procedimientos para estandarización y buenas prácticas en los procesos, gobernabilidad, entre otros.

Una de las empresas que ofrecen este servicio es la firma *Puffin Security*[49], la cual detalla en su sitio web que las principales estrategias de ataque de los cibercriminales en dispositivos *IoT* son el acceso a datos sensibles, el sabotaje y los *botnet*s. De acuerdo con esto, define una metodología de auditoría *IoT* la cual propone los siguientes pasos:

- Contexto
- Análisis de *hardware*
- Análisis de *firmware*
- *Software* y aplicaciones relacionadas
- Comunicaciones
- Generación de resultados

Para el desarrollo de esta auditoría, se basan en la metodología *OWASP IoT* y el uso de herramientas usadas en auditorías de tecnología como pruebas de penetración y realizar una revisión del *hardware* y *firmware* de cada dispositivo para encontrar vulnerabilidades, siguiendo cada uno de los pasos definidos en su metodología y concluyendo con un informe de resultados el cual detalla las pruebas realizadas y descubrimientos, el cual funciona como base para mitigar riesgos y tomar las decisiones y acciones necesarias.

La compañía *Tarlogic*[50], dentro de sus portafolios de servicios, incluye auditorías de seguridad web, de código fuente, de aplicaciones móviles y otros dentro de los cuales se incluye la auditoría de seguridad *IoT*. *Tarlogic* realiza su análisis partiendo de una revisión de la infraestructura de los dispositivos, esto incluye diferentes puertos de conexión o redes con tecnología comúnmente usadas en *IoT* como *Zigbee* o *bluetooth*. Una vez auditadas las redes, se realiza la búsqueda de vulnerabilidades la cual es similar a la que se realizaría en cualquier otro tipo de dispositivo. Finalmente, se realiza una revisión de puertos expuestos en estos dispositivos para concluir en un informe de resultados.

[49] Consultora enfocada en proveer servicios y soluciones de ciberseguridad.
[50] Proveedor Europeo de servicios de ciberseguridad.

La auditoría *IoT* se encuentra también dentro del catálogo de servicios de *TalSoft*[51], en la cual afirma que realizar un análisis de riesgos podría reducir en un 75% las intrusiones. La metodología de *TalSoft* se resume en cuatro fases:

- Planificación: Reconocimiento del *software*
- Detección y explotación de vulnerabilidades en el *software*
- Informes de alertas de las debilidades de seguridad
- Corrección de las debilidades de seguridad

Como beneficios, *TalSoft* detalla en su sitio web, la detección temprana de vulnerabilidades, detección de vulnerabilidades en el ciclo de desarrollo de *software*, mejora de la confianza del cliente y de la empresa, reducción de incidentes de seguridad y mitigación de problemas legales, imagen y negocio del cliente.

*Sapsi Consultores*52 ofrece un servicio de auditoría a dispositivos *IoT* que comienza desde el diseño del dispositivo y las fases posteriores. Dentro de esta auditoría, *Sapsi* ofrece servicios de revisión de código, sistema operativo, *hardware*, parches de seguridad, gestión de vulnerabilidades, entre otros.

*Nethemba*53 dentro de su amplio portafolio de soluciones y servicios de seguridad, ofrece auditorías y consultorías de seguridad *IoT* para empresas donde realiza un relevamiento desde la fase de diseño y fases posteriores garantizando la seguridad de los dispositivos y el cumplimiento de las regulaciones necesarias, finalmente, este servicio detalla sus resultados en un informe que también incluye niveles de riesgo, vulnerabilidades identificadas y pasos a seguir o recomendaciones.

Dentro de las compañías mencionadas anteriormente, se observa gran similitud en el servicio ofrecido dentro de lo que es la auditoría de seguridad *IoT*, en todos los casos se ofrece un acompañamiento desde la etapa inicial y revela las distintas vulnerabilidades a las cuales se encuentran expuestos y de acuerdo con esto, se ofrecen recomendaciones para mantener la seguridad de los dispositivos y la compañía. Adicional a una auditoría *IoT*, las empresas deben garantizar la seguridad de las redes, nube y demás tecnologías que intervengan de alguna forma con el funcionamiento e incorporación de tecnologías *IoT* en el entorno empresarial.

[51] Consultora especializada en servicios de seguridad informática
[52] Firma consultora que ofrece servicios de evaluación de ciberseguridad en las empresas.
[53] Compañía Eslovaca/Checa enfocada en la seguridad de aplicaciones web y pruebas de penetración.

De acuerdo con el documento *Auditoria básica TI: Auditando el internet de las cosas* escrito por Ian Cooke en 2019, el proceso de auditar *IoT* inicia desde la clara definición de esta tecnología. Una vez definido esto, se pasa a identificar el riesgo, lo cual es la base o el objetivo de cualquier auditoría, mitigar riesgos a través de controles de prevención y detección que abarquen los distintos sistemas y procesos en alcance. Dentro de los riesgos, se identifican vulnerabilidades y se detalla cómo estás pueden afectar la compañía y con qué nivel de impacto. Dentro de los riesgos identificados por Ian Cooke, se incluyen la falta de actualizaciones de *software* y parches en tiempo y forma, los ID y contraseñas de usuario no robustos o estandarizados por política, la falta de dispositivos de seguridad como antivirus o cortafuegos, entre otros.

Una vez definido el objetivo de la auditoría y conociendo el significado de Internet de las Cosas y lo que esto agrupa, se determinan los distintos sistemas y dispositivos en alcance, es decir, aquello que se va a auditar, posteriormente, el siguiente paso es realizar la planificación de la auditoría. En este punto se debe considerar todo el ambiente de *IoT*, cómo interactúan los dispositivos, cómo estos pueden representar vulnerabilidades, cómo trabajan los datos, qué otras tecnologías se incluyen, qué personas están involucradas en el proceso, entre otras cuestiones.

Finalmente, después de establecer el plan de auditoría, se comienza a desarrollar el plan de auditoría a través de la definición de procedimientos y pasos a seguir. Ian Cooke propone como marco de referencia cuatro áreas separadas por controles de línea base, datos relacionados, análisis y aprendizaje y alineación de procesos y negocios.

Estas áreas, como se observa en la **figura 24**, contienen fuentes de aseguramiento a revisar para garantizar el cumplimiento de los controles.

Figura 24. *Fuentes de documentación de aseguramiento.*

Figura 3—Fuentes de documentación de aseguramiento	
Área	**Fuente de Aseguramiento**
Línea base general de controles	• Guía de seguridad de IoT para: Proyecto de seguridad de aplicaciones web abiertas - Open Web Application Security Project (OWASP)[16] • Evaluación de seguridad de IoT para: Sistema global para la asociación de comunicaciones móviles - Global System for Mobile Communications Association (GSMA)[17] • Pruebas de concepto de un mundo conectado Future Proofing the Connected World[18] • Guía de implementación técnica de seguridad del Departamento de Defensa de los Estados Unidos Security Technical Implementation Guide (STIG)[19] • Puntos de referencia (Benchmarks) de CIS[20]
Datos relacionados	• Orientación de seguridad de IoT para OWASP[21] • Evaluacion de seguridad de IoT para GSMA • Pruebas de concepto de un mundo conectado Future Proofing the Connected World[22] • *COBIT® 5: Información habilitadora*[23] • Programa de Auditoría/Aseguramiento para: US Health Insurance Portability and Accountability Act (HIPAA)[24] • *Guía para la Gestión de Programas y Principios de Privacidad de ISACA®*[25] • *Auditoría de la privacidad de los datos*[26] • Preparación, evaluación y cumplimiento de: Reglamento general de protección de datos EE. UU. General Data Protection Regulation (GDPR)[27]
Análisis y aprendizaje	• Orientación de seguridad de IoT para OWASP[28] • Evaluacion de seguridad de IoT para GSMA • Pruebas de concepto de un mundo conectado Future Proofing the Connected World[29] • *Guía para la Gestión de Programas y Principios de Privacidad de ISACA*[30] • *Auditoría de la privacidad de los datos*[31] • Preparación, evaluación y cumplimiento de: Reglamento general de protección de datos GDPR[32] • Pruebas de sesgo para aplicaciones de aprendizaje automático generalizadas[33]
Alineación de procesos y negocios	• COBIT® 5[34]

Nota. Tomado de *Fuentes de documentación de aseguramiento,* por Cooke, Ian, 2019, 03 de octubre, ISACA, 2014. ISACA (https://www.isaca.org/es-es/resources/isaca-journal/issues/2018/volume-5/is-audit-basics-auditing-the-*IoT*)

5.3.3 MARCOS DE REFERENCIA, ESTÁNDARES, CERTIFICACIONES Y REGULACIONES EN AUDITORÍA RELACIONADOS A CIBERSEGURIDAD *IoT*.

Actualmente no se cuenta con un marco de referencia o regulaciones específicamente para *IoT*, existen para las auditorías en general y a su vez segmentadas de acuerdo con el tipo de auditoría, asimismo, las leyes aplicables van de acuerdo con el tipo de negocio.

Para realizar una auditoría *IoT*, se propone integrar los diferentes controles y recomendaciones dentro de una auditoría financiera como parte del proceso de revisión de IT/OT, ya que desde este negocio se puede mantener el entendimiento y compartir ciertos controles genéricos asociados a la seguridad que pueden ser aplicables a los distintos sistemas y dispositivos dentro de una revisión del ambiente *IoT*, además de incorporar

controles preventivos y detectivos apoyados en marcos de referencia y estándares sobre seguridad ampliamente reconocidos como los mencionados a continuación:

- *ASVS* (*Application Security Verification Standard* o Estándar para la Verificación de la Seguridad en Aplicaciones por sus siglas en español): Proyecto *OWASP* que propone establecer un marco de referencia para ayudar a las compañías a crear y mantener aplicaciones seguras.
- *ENISA*: Marco de seguridad de la información de *Microsoft* basado en controles *ISO/IEC* 27001 y la matriz de controles en la nube (*CCM*) de *CSA* (*Cloud Security Alliance*) que contiene principios de seguridad para ayudar a los clientes en la nube a evaluar la seguridad de un *CSP* (Proveedor de servicios en la nube).
- *COBIT*: Marco de referencia reconocido globalmente para la gestión y regulación gubernamental de las tecnologías de la información en las empresas aplicable a ambientes de seguridad de la información, tecnologías de la información y gestión de riesgo. Es gestionada por *ISACA* junto con el Instituto de Gobierno de IT (*ITGITM*[54]). El uso de este marco de referencia se recomienda para funciones de gobierno y cumplimiento.
- *ITIL* (*IT Infrastructure Library*): Marco de referencia para la administración de servicios de tecnología de la información enfocado a la administración de los procesos. Se encuentra gestionado por la Oficina de Comercio Gubernamental de Reino Unido. El uso de este marco de referencia se recomienda para mejorar la toma de decisiones respecto a la correcta gestión de los servicios de *IT*.
- *ISO/IEC* 27000: Marco de referencia publicado por la Organización Internacional de Estandarización (*ISO*) en conjunto con la Comisión Electrotécnica Internacional (*IEC*), el cual contiene una serie de estándares que ayudan a la proteger los Sistemas de Gestión de la Seguridad de la Información *(SGSI)* en las empresas. Mediante una auditoría, las compañías pueden obtener la certificación *ISO* 27001 la cual garantiza que la empresa cuenta con una adecuada gestión de la información. Asimismo, se han popularizado también las certificaciones *ISO* 27017 e *ISO* 27018 las cuales

[54] Organización sin ánimo de lucro que orienta a las empresas en temas de gobierno para los activos en *IT*.

garantizan la seguridad a los servicios en la nube y al ciclo de vida de los datos, respectivamente.

- Para el análisis de riesgos en los *SGSI* es posible aplicar la metodología OCTAVE (*Operational Critical, Threat, Asset and Vulnerability Evaluation)* que se enfoca en garantizar la seguridad de los sistemas informáticos en las empresas.
- *COSO* (*Comité de Organizaciones Patrocinadoras de la Comisión Treadway)*: Marco de referencia utilizado en auditoría para evaluar el control interno de las organizaciones. Es ampliamente utilizado en compañías que deben cumplir con la Ley *SOX*[55].
- *ISA* (Estándares internacionales de Auditoría): Conjunto de estándares que reglas y principios aplicables a las auditorías de información financiera.
- El estándar *ISA/IEC* 62443 es el principal marco de referencia para la ciberseguridad de los sistemas industriales en donde se prioriza la integridad y disponibilidad de la información en la prevención de incidentes.
- *CIS (Critical Security Controls):* Desarrollado por el *Center for Internet Security* y cuenta con un set de controles que contienen las acciones recomendadas para proteger los datos de la organización de ciberataques.
- *NIST CSF (National Institute of Standards and Technology Cybersecurity Framework)*: Este marco de ciberseguridad pretende guiar a las compañías a conocer los riesgos de ciberseguridad para mitigarlos y proteger los datos. Es un marco genérico adaptable a pequeñas, medianas y grandes empresas de cualquier rubro ya que requiere muy mínima personalización para obtener resultados óptimos. *NIST CSF* se enfoca en la protección de la seguridad de las infraestructuras críticas y toma como base estándares ampliamente reconocidos como *NIST, ISO/IEC 27001, COBIT, CIS*, entre otros).

La aplicación de los distintos estándares y marcos de referencia mencionados anteriormente debe ir acompañado de un excelente entendimiento del negocio, la empresa y el ambiente tecnológico.

[55] La *Ley Sarbanes Oaxley* regula los informes financieros y de auditoría aplicable a las compañías que cotizan en la bolsa de Estados Unidos.

Actualmente, diferentes organismos especializados ofrecen gran variedad de certificaciones con varios enfoques. Esto permite preparar profesionales capaces de aprovechar las distintas herramientas, conocimientos e información disponible para el desarrollo de programas de trabajo, toma de decisiones y estrategias dentro de los distintos de los proyectos, en el caso de esta tesis, una auditoría en ciberseguridad enfocada a tecnología *IoT*.

Dentro de las principales certificaciones y con mayor demanda en el ámbito de ciberseguridad se encuentran las ofrecidas por *ISACA*, entre ellas se encuentran:

- *CISM (Certified Information Security Manager):* Certifica experiencia en gobierno de Seguridad de la Información y gestión de riesgos e incidentes.
- *CGEIT (Certified in the Governance of Enterprise IT):* Certifica experiencia en los distintos principios y prácticas relacionados al marco de gobierno empresarial de *IT*.
- *CRISC (Certified in Risk and Information Security Control):* Certifica experiencia en gestión de riesgos empresariales de *IT*. Se enfoca en garantizar el conocimiento vigente sobre las distintas amenazas y cómo abordarlas dentro de un ambiente empresarial a través de la creación de un programa de gestión de riesgos basado en las mejores prácticas.
- *CISA (Certified Information Systems Auditor):* Dentro de las diferentes certificaciones de *ISACA*, esta certificación de seguridad es la más aplicable a lo que se propone en esta tesis ya que está dirigida a profesionales en auditoría y control de los sistemas de información. Es también la certificación más antigua y se encuentra aprobada por el Departamento de Defensa de Estados Unidos. Esta certificación garantiza experiencia en temas como la gestión, desarrollo e implementación de sistemas de información a través de políticas y procedimientos, gobierno de *IT*, protección de activos de información garantizando la protección de la triada *CID*[56], entre otros.

La organización internacional sin ánimo de lucro (ISC)² ofrece también reconocidas certificaciones relacionadas a ciberseguridad, entre ellas se encuentran:

[56] Confidencialidad, Integridad y Disponibilidad de la información.

- *CISSP (Certified Information Systems Security Professional)* es una certificación altamente reconocida e incluso tomada como referencia por la *NSA*[57] o el Departamento de Defensa de Estados Unidos. Esta certificación garantiza experiencia en el área de seguridad de la información.
- *CGRC (Certified in Governance, Risk and Compliance):* Esta certificación garantiza experiencia y habilidades en temas de Gobierno, Riesgo y Cumplimiento (*GRC* por sus siglas en inglés), lo cual al igual que la certificación *CISA* de *ISACA* se encuentra bastante alineada con el propósito de esta tesis. Un profesional con esta certificación es capaz de aplicar de forma óptima los distintos marcos de referencia para a gestión de riesgo de los diferentes sistemas de información aplicando las mejores prácticas, recomendaciones, políticas, normativas y procedimientos.

Si bien, como se mencionó anteriormente, no existe un marco de referencia aplicable únicamente a auditorías *IoT*, tomar como referencia marcos de trabajo, conocer las distintas regulaciones y contar con el personal capacitado, puede garantizar el desarrollo de proyectos de gestión que garanticen la seguridad de los dispositivos y los sistemas en los distintos ambientes y frentes asociados dentro de un ecosistema *IoT* soportado por una auditoría enfocada a ciberseguridad y los distintos procesos de IT/OT e nivel empresarial.

[57] La *NSA* es la Agencia de Seguridad Nacional del departamento de defensa de Estados Unidos.

6) INVESTIGACIÓN, IMPLEMENTACIÓN Y SOLUCIONES.

Teniendo en cuenta los distintos conceptos explicados anteriormente en esta tesis, como resultado del mismo, en este capítulo se ofrecen una serie de herramientas que pretenden ayudar a compañías en un contexto de transformación digital que buscan garantizar la seguridad de sus sistemas priorizando el ecosistema *IoT* entendiendo que es un entorno que actualmente se encuentra en auge y por consiguiente debe tenerse en cuenta dentro de los planes de gestión de riesgos conociendo las distintas vulnerabilidades a las cuales se encuentran expuestos por sí mismos y a las que pueden exponer a gran escala a la compañía.

6.1PLAN DE TRABAJO

Para el desarrollo del plan de trabajo y matriz de controles propuesta en esta tesis, inicialmente se realizó una comparativa sobre algunos marcos de referencia para definir la opción más completa para el propósito de la tesis.

Dentro de los marcos de referencia a comparar, se tomaron NIST 1.1, ISO/IEC 27001:2022 – ISO/IEC 27002:2022, COBIT 2019 e ITIL v4, para los cuales se consolidaron los detalles más relevantes con el fin de seleccionar la mejor opción, esta comparativa se detalla en la **Tabla 2**.

Tabla 2. *Comparativa entre marcos de referencia (Elaboración propia)*

	ALCANCE	**PLAN DE TRABAJO**	**ENFOQUE**	**VERSIÓN**
NIST CSF	Empresas de cualquier tamaño y rubro.	* Funciones: identificación protección, detección, respuesta y recuperación * Categorías (23) * Subcategorías (108) *Referencias informativas (COBIT 5, ISO/IEC 27001:2013, NIST SP 800-53, ISA 62443-2-1:2009, CIS CSC, entre otros).	Ciberseguridad	1.1 (2018)
ISO/IEC	Empresas de cualquier tamaño y rubro.	* 27001:2022: Fases: planificación, implementación, evaluación y mejora continua. * 27002:2022: Contiene 93 controles de seguridad (8 controles para personas, 14 físicos, 34 tecnológicos y 37 organizacionales).	GRC Ciberseguridad	ISO/IEC 27001:2022 ISO/IEC 27002:2022
COBIT	Empresas de cualquier tamaño y rubro.	* Dominios: Planificación y organización, adquisición e implementación, entrega y soporte del servicio, supervisión y evaluación.	GRC	COBIT 2019

ITIL	Empresas de cualquier tamaño y rubro.	* Componentes: Sistema de valor del servicio (SVS) y modelo de cuatro dimensiones. ** SVS (5): Cadena del valor del servicio de ITIL, principios rectores de ITIL, gobernanza, mejora continua, prácticas ITIL. ** Dimensiones (4): Organizaciones y personas, información y tecnología, socios y proveedores, flujos de valor y procesos.	GRC	ITIL V4 (2019)

Como puede observarse en la **Tabla 2**, para cada marco de referencia en estudio, se identificó el alcance o a quién está dirigido cada estándar, en todos los casos, estos *frameworks* pueden ser aplicables a cualquier proceso en pequeñas, medianas y grandes empresas sin importar el rubro. De acuerdo con el enfoque, se determinó que tanto COBIT e ITIL buscan fortalecer principalmente las áreas de gobierno, riesgo y cumplimiento comúnmente conocidas como GRC, mientras que el marco NIST CSF se enfoca en robustecer la ciberseguridad, por otro lado, los estándares ISO/IEC 27001/27002 abarcan ambos frentes ya que son estándares complementarios, en ISO/IEC 27001 se busca realizar una evaluación de riesgos y crear una sistema de gestión de seguridad de la información (SGSI) el cual se apoya en los controles detallados en la norma ISO/IEC 27002, por lo cual es bastante recomendable implementar estos controles sólo después de haber seguido lo detallado en el estándar ISO/IEC 27001.

Teniendo en cuenta las distintas fases, categorías y controles de los marcos de referencia en comparación, se seleccionaron las áreas consideradas fundamentales dentro de la evaluación de seguridad propuesta en esta tesis y buscando que las mismas sean contempladas en los distintos *frameworks* detallados en la **Tabla 3**.

Estas áreas son: gobierno o marco regulatorio, políticas y procedimientos, capacitación y concientización, segregación de funciones y accesos sensitivos (*SOD/AS*), seguridad física, seguridad lógica, continuidad de negocio y actividades de control. Se seleccionaron estas áreas como foco ya que algunas validaciones son básicas de cualquier marco de referencia aplicable a *IT*.

Tabla 3. *Comparativa de áreas de foco entre marcos de referencia. (Elaboración propia)*

	GOBIERNO	POLÍTICAS Y PROCEDIMIENTOS	CONCIENTIZACIÓN Y CAPACITACIÓN	*SOD/AS*	SEG. FISICA	SEG. LÓGICA	CDN	ACT. CONTROL
NIST CSF	✔	✔	✔	✔	✔	✔	✔	✔
ISO/IEC	✔	✔	✔	✔	✔	✔	✔	✔
COBIT	✔	✔	✔	✕	✕	✔	✔	✔
ITIL	✔	✔	✔	✔	✔	✔	✔	✔

De acuerdo con estas comparativas se decidió avanzar el plan de trabajo y la matriz de controles propuestos tomando como referencia tanto NIST CSF como ISO/IEC 27001/27002 ya que, aunque NIST CSF toma como referencia normas ISO/IEC en varias de sus subcategorías, estas dos normas complementarían de la mejor manera lo propuesto por NIST CSF especialmente en las áreas de gobierno, riesgo y cumplimiento.

De acuerdo con la información y controles indicados en los marcos de referencia seleccionados como base, se proponen los siguientes pasos para comenzar con la evaluación de ciberseguridad enfocada en *IoT* en la empresa:

1. Definir riesgos y vulnerabilidades de la compañía y clasificarlos por nivel de criticidad (impacto financiero, legal, reputación, seguridad, entre otros.). Esta definición debe ir alineada con los intereses de la organización y el principal objetivo del desarrollo de la evaluación de ciberseguridad. Una clasificación por nivel riesgos, permite dar un panorama respecto a las prioridades y el foco al momento de definir también los controles a implementar.
2. Identificar los activos (físicos y lógicos) dentro del alcance de la evaluación de ciberseguridad. Realizar este paso permite conocer los sistemas y herramientas de mayor valor dentro de la organización. Este paso es de gran importancia ya que será la base para la definición de controles a implementar y el nivel de riesgo asociado además de otras características.
3. Identificar amenazas técnicas relacionadas a los activos físicos y lógicos previamente establecidos. Este paso lleva a definir los controles de seguridad a aplicar para resguardar la confidencialidad, integridad y disponibilidad de los datos dentro de los activos de la organización.
4. Identificar amenazas de tipo humano. Al igual que el paso anterior, la identificación de errores o amenazas asociadas a actividades humanas es muy importante, ya que los ataques pueden provenir no solamente de brechas de seguridad en activos físicos y lógicos, los ataques de ingeniería social son una realidad por lo cual identificarlos y asociarlos a controles como capacitación y concientización dentro de la evaluación de ciberseguridad es fundamental dentro de cualquier compañía.
5. Implementación y seguimiento de una matriz de controles de seguridad asociadas a cada uno de los pasos anteriores. La matriz de controles a

implementar debe contemplar los alcances en cuanto a activos físicos, lógicos, humanos y las amenazas identificadas asociadas a los riesgos encontrados, de acuerdo con esto se decidirá qué controles incluir en la evaluación de ciberseguridad y asimismo la naturaleza de cada uno de ellos en cuanto a tipo, riesgo asociado, objetivo, frecuencia, evaluación y demás características que se consideren de impacto.

6. Definir roles y responsabilidades para cada control implementado y a su vez, para cada procedimiento formalizado a través de una norma o política. Asociar un puesto de trabajo a una tarea específica ayuda a mantener un control permanente sobre las distintas actividades de la compañía asegurando una supervisión dentro de cada área de evaluación. También, estos roles deben pasar por una evaluación de segregación de funciones, de tal forma que el rol designado a una tarea específica no tenga incompatibilidad de funciones con otras tareas o que exista alguna limitación por descripción del puesto.
7. Diseñar un cronograma para el desarrollo de cada tarea dentro del plan de trabajo para la evaluación de ciberseguridad e *IoT*, para ello, cada paso debe estar debidamente especificado con una fecha de ejecución o entrega definida por parte del o los responsables establecidos en el paso anterior.
8. Análisis de resultados y definición de pasos a seguir. De acuerdo con os resultados obtenidos de acuerdo con la implementación de controles y vulnerabilidades encontradas se deben tomar las acciones necesarias para mitigar posibles riesgos y controlar la ciberseguridad de la compañía.

Gracias al desarrollo e implementación de un plan de trabajo junto a la definición de matriz de controles, es posible obtener un panorama completo del nivel de ciberseguridad de la compañía, fortalezas, debilidades y por consiguiente, las acciones a tomar en cualquier momento ya que esto se trata de un trabajo diario en constante monitoreo en el cual se evalúan distintos aspectos con diferentes niveles de impacto que pueden irse corrigiendo en el momento para la mejora continua de la compañía en materia de ciberseguridad.

6.2MATRIZ DE CONTROLES

Antes de comenzar a definir los controles, se definieron ocho áreas generales, en adelante llamadas dominios, para las cuales es necesario realizar algunas tareas previas que luego serán asociadas a actividades de control. Estos dominios representan grupos de controles que en conjunto buscan mitigar posibles riesgos dentro de la compañía.

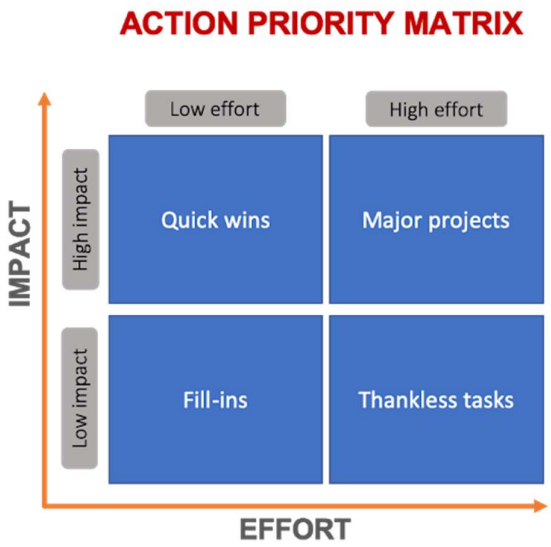
Los dominios establecidos como base para la creación de la matriz de controles en la evaluación en ciberseguridad enfocada a *IoT* propuesta en esta tesis, son:

- Gobierno.
- Políticas y procedimientos.
- Concientización y capacitación.
- Segregación de funciones y accesos sensitivos (*SoD/AS*).
- Seguridad Física.
- Seguridad Lógica.
- Continuidad de negocio.
- Actividades De Control

Dentro de cada uno de estos dominios, las actividades de desarrollo fueron clasificadas de acuerdo con la herramienta *Action Priority Matrix* o matriz de prioridades, como se observa en la **Figura 25**, en donde de acuerdo con el impacto y el esfuerzo requerido, se le asigna a cada tarea un nivel de prioridad que puede ser:

- *Quick wins (QW):* Es de alto impacto y requiere poco esfuerzo.
- *Major projects (MP): Es* de alto impacto y requiere mayor esfuerzo.
- *Fill-ins (FI):* Es de bajo impacto y requiere poco esfuerzo.
- *Thankless tasks (TT): Es* de bajo impacto y requiere mayor esfuerzo.

Figura 25. *Matriz de prioridades*



Nota. Tomado de *Action priority matrix*, por ProductPlan, 2023, ProductPlan (https://www.productplan.com/glossary/action-priority-matrix/)

En la **Tabla 4** se observan los dominios definidos y las actividades previas a realizar en cada dominio por proceso (Ciberseguridad o *IoT*), para implementar de manera efectiva los controles de la matriz de riesgos.

Tabla 4. *Dominios y actividades de control relacionadas. (Elaboración propia).*

DOMINIO	ACTIVIDADES	QW	MP	FI	TT
Gobierno	Identificar las regulaciones aplicables de acuerdo con el negocio.	●			
Políticas y procedimientos	Definición, documentación y publicación de normas, políticas y procedimientos relacionadas con Ciberseguridad.		●		
	Definición, documentación y publicación de normas, políticas y procedimientos relacionadas con *IoT*.		●		
Concientización y capacitación	Creación e implementación de planes de capacitación y ejercicios de ciberseguridad orientados a personal de la compañía.			●	
	Creación e implementación de planes de capacitación en temas de *IoT* orientados a personal de la compañía.			●	
SoD/AS	Definición de un área/referente en Ciberseguridad.	●			
	Definición de un área/referente en *IoT*.	●			
Seguridad física	Realizar un inventario de activos electrónicos de la compañía con su correspondiente asignación.	●			
	Realizar un inventario de dispositivos *IoT* de la compañía con su correspondiente asignación.	●			
	Realizar bloqueo de puertos en los dispositivos de la compañía.	●			
Seguridad lógica	Realizar un reconocimiento de redes y segmentación de la misma.		●		
	Realizar un inventario de activos digitales de la compañía con su correspondiente asignación.	●			
	Realizar un mapeo de dispositivos conectados a las redes de la compañía.	●			
	Realizar un mapeo de dispositivos que hacen uso de la tecnología *IoT*.	●			
	Implementar dispositivos de protección (antivirus, firewall, WAF, VPN, 2FA, etc.)	●			
	Realizar un mapeo y revisión de usuarios en la red.		●		
	Realizar un mapeo y revisión de usuarios con dispositivos *IoT* conectados a la red empresarial.		●		
	Realizar un mapeo de puertos abiertos en la red empresarial.	●			
	Implementar un SOC dedicado al monitoreo y detección de amenazas en la red.				●
Continuidad de negocio	Realizar y mantener actualizado un plan de recuperación de desastres.				●
	Definir la estrategia de *backup* y *restore* o guardado y recuperación de copias de seguridad de la información contenida en los diferentes sistemas.			●	

	Definir la estrategia de *backup* y *restore* de la información contenida en dispositivos *IoT*.			●	
Actividades de control	Realizar un mapeo de verificación de *software* actualizado.	●			
	Realizar un mapeo de verificación de *firmware* actualizado.	●			
	Definir un cronograma de escaneos periódicos sobre los diferentes sistemas.	●			
	Definir un cronograma de escaneos periódicos sobre los dispositivos *IoT*.	●			

Como se observa en la **Tabla 4**, se definieron 26 actividades o tareas asociadas a los ocho dominios generales aplicables tanto a Ciberseguridad como a *IoT* las cuales se recomienda realizar previo a la evaluación e implementación de la matriz de controles para garantizar la efectividad de estos.

Los dominios definidos, se clasificaron de acuerdo con:

- Gobierno: Contiene controles relacionados con regulaciones, propiedad intelectual, información personal, políticas organizacionales, entre otros. Este dominio se enfoca en asegurar la parte normativa de la compañía y el cumplimiento de las regulaciones aplicables al negocio.
- Políticas y procedimientos: Este dominio se enfoca en garantizar el diseño, documentación, aprobación y publicación de las distintas normas, políticas y procedimientos relacionados con tecnología, ciberseguridad e internet de las cosas.
- Concientización y capacitación: Contiene controles enfocados al desarrollo y monitoreo de actividades y ejercicios de capacitación en ciberseguridad e internet de las cosas orientado a todo el personal de la compañía. Abarca distintos enfoques de tal forma que se brinden las herramientas para detectar y prevenir distintos tipos de vulnerabilidades a los sistemas y proteger los datos.
- Segregación de funciones y accesos sensitivos (*SoD/AS*): Contiene controles que validan los roles y responsabilidades asignados a los distintos servicios, sistemas y plataformas para garantizar que se encuentren correctamente segregados y la información sensitiva se encuentre debidamente resguardada.
- Seguridad física: Incluye controles que garantizan el acceso físico a las instalaciones y centro de cómputos de manera segura y que los mismos se encuentren condicionados de acuerdo con las mejores prácticas.

- Seguridad lógica: Abarca la mayor cantidad de controles ya que incluye temas de accesos, cambios a programas, nuevos desarrollos, seguridad de las tecnologías, revisión de usuarios, entre otros, enfocados a la seguridad de los sistemas, plataformas y dispositivos inteligentes.
- Continuidad de negocio: Ante un posible incidente de seguridad, esta actividad incluye controles de recuperación de información y mecanismos de resiliencia para la compañía.
- Actividades de control: Finalmente, esta actividad incluye controles de monitoreo para garantizar la seguridad de los sistemas a través de actividades periódicas de revisión de vigencia de los sistemas y dar soporte a varios de los controles incluidos en las actividades mencionadas anteriormente.

Para cada actividad, se definió un nivel de prioridad asociado de acuerdo con la matriz de prioridades detallada anteriormente, evaluando el impacto y el nivel de esfuerzo de cada actividad.

Una vez desarrolladas las actividades de control, para cada dominio, se detallaron una serie de controles tomando como base los estándares *NIST, ISO/IEC 27001-27002, OWASP IoT Top 10, CIS Controls, Cybersecurity Kill Chain, MITRE ATT&CK* entre otros recursos, además de lo investigado a través del marco teórico de esta tesis.

Estos controles pretenden cubrir los principios de la ciberseguridad (confidencialidad, integridad y disponibilidad de la información) e incluyen:

- ID Dominio: Contiene la abreviatura del dominio al cual hace parte el control (GOB, PYP, CYC, SYA, SGF, SGL, CDN, ACC)
- Dominio: Contiene el nombre del dominio al cual hace parte el control, sin abreviatura.
- ID control: Contiene el código del control, el cual es un valor único de identificación.
- Título de control: Detalla el título del control.
- Desc. Control: Contiene la descripción del objetivo, condiciones o actividades a realizar para la evaluación del control.

- Nivel Riesgo: Se encuentra clasificado en alto (A), medio (M) o bajo (B) de acuerdo con el nivel de riesgo de control.
- Periodicidad: Se encuentra clasificado de acuerdo con la frecuencia en la que se llevará a cabo el control ya sea de forma anual (AN), semestral (SE), trimestral (TR), mensual (ME), semanal (SL), diaria (DI) o por ocurrencia (OC).
- Tipo: Se encuentra clasificado de acuerdo con el propósito del control, es decir, si se trata de un control preventivo (P) o detectivo (D).

A continuación, se detalla la matriz de controles propuesta la cual incluye controles aplicables a una evaluación de ciberseguridad enfocada a dispositivos *IoT*.

ID DOMINIO	DOMINIO	ID CONTROL	TÍTULO DE CONTROL	DESC. CONTROL	NIVEL RIESGO			PERIODICIDAD							TIPO	
					A	M	B	AN	SE	TR	ME	SL	DI	OC	P	D
GOB	Gobierno	GOB-001	Control de Legalidad	La compañía cuenta con el conocimiento y documentación respecto a los requisitos legales, reglamentarios y contractuales a los que se encuentra sujeto la compañía.	●			●							●	
GOB	Gobierno	GOB-002	Certificados	La compañía cuenta con la documentación digital sobre derechos de propiedad intelectual, identidad del propietario y mecanismos de cifrado en la red para proteger dicha información.	●			●								●
GOB	Gobierno	GOB-003	Protección de la información personal	La compañía cuenta con políticas y herramientas enfocadas a la privacidad y protección de la información personal de sus empleados y terceros, asimismo para los datos generados de acuerdo con su clasificación para los cuales se tiene derecho.			●							●	●	
GOB	Gobierno	GOB-004	Políticas organizacionales	La compañía cuenta con la documentación aprobada, vigente y pública de la misión, visión y objetivos de la empresa.			●	●								●
GOB	Gobierno	GOB-005	Acuerdos de confidencialidad	La compañía realiza acuerdos de confidencialidad o no divulgación con terceros, los cuales se encuentran debidamente aprobados y resguardados.	●									●	●	
GOB	Gobierno	GOB-006	Requerimientos legales de ciberseguridad	Los requerimientos legales relacionados a ciberseguridad, privacidad y obligaciones están correctamente establecidos y gestionados.			●							●	●	
GOB	Gobierno	GOB-007	Gobierno y ciberseguridad	Dentro de las actividades y políticas de gobierno y gestión de riesgos de la compañía, se encuentran contemplados los riesgos de ciberseguridad.	●			●							●	

ID DOMINIO	DOMINIO	ID CONTROL	TÍTULO DE CONTROL	DESC. CONTROL	NIVEL RIESGO			PERIODICIDAD							TIPO	
					A	M	B	AN	SE	TR	ME	SL	DI	OC	P	D
PYP	Políticas y procedimientos	PYP-001	Políticas y procedimientos de ciberseguridad	La compañía cuenta con políticas, normas y procedimientos relacionados a ciberseguridad tales como: Seguridad de la información, clasificación de la información, control de accesos, cambios a programas, nuevos desarrollos, segregación de funciones, accesos sensitivos, carpetas sensitivas, acceso a espacios físicos, entre otros.			●							●	●	
PYP	Políticas y procedimientos	PYP-002	Políticas y procedimientos de *IoT*	La compañía cuenta con políticas, normas y procedimientos relacionados a *IoT* tales como: *Backup*, *restore*, configuración de línea base, parcheo, instalación de *software*, etiquetado de información, transferencias bancarias, transferencia de información, contraseñas, BYOD, uso de la información, entre otros.			●							●	●	
PYP	Políticas y procedimientos	PYP-003	Normativa de ciberseguridad	Existen estándares definidos y aprobados en los cuales se especifican los requerimientos de ciberseguridad para cada plataforma.			●							●	●	
CYC	Concientización y capacitación	CYC-001	Programas de concientización y capacitación	La compañía cuenta con programas para la sensibilización y capacitación en temas de ciberseguridad y tecnología orientado a todas las áreas dentro de la compañía, teniendo en cuenta posibles amenazas de tipo técnico o humano ya sea por errores, de carácter malicioso o por ingeniería social. Estas capacitaciones se encuentran definidas y presentadas por diferentes canales dentro de los cuales se incluyen e-learnings, carteleras, correos electrónicos, trivias, videos, encuestas, ejercicios de ciberseguridad, entre otros.	●									●	●	

ID DOMINIO	DOMINIO	ID CONTROL	TÍTULO DE CONTROL	DESC. CONTROL	NIVEL RIESGO			PERIODICIDAD							TIPO	
					A	M	B	AN	SE	TR	ME	SL	DI	OC	P	D
CYC	Concientización y capacitación	CYC-002	Control de capacitación	Para cada usuario dentro de la compañía, se mantiene un monitoreo y registro sobre las capacitaciones realizadas y pendientes referentes a Ciberseguridad e *IoT*.			●							●	●	
CYC	Concientización y capacitación	CYC-003	Ciberseguridad en RRHH	La compañía cuenta con actividades de capacitación en ciberseguridad orientadas al área de Recursos Humanos para promover buenas prácticas en los procesos de reclutamiento y monitoreo de personal. Estas buenas prácticas pueden incluir rutinas de personal screening para validar que la persona es la adecuada para asumir el rola asignado dentro de la compañía.			●							●	●	
SYA	*SoD/AS*	SYA-001	Control de acceso	Los accesos a los diferentes sistemas y plataformas se encuentran restringidos al personal adecuado de acuerdo con el procedimiento vigente. Existen herramientas para la creación, asignación, monitoreo y eliminación de accesos de acuerdo con los roles y responsabilidades asociados al puesto. Estas funciones y accesos autorizados se encuentran definidos de tal forma que se pueda garantizar una correcta segregación de funciones y roles incompatibles.	●									●	●	
SYA	*SoD/AS*	SYA-002	Control de acceso *Cloud*	La compañía cuenta con sistemas de gestión de identidad y acceso a los distintos sistemas alojados en la nube. El acceso debe estar acompañado de herramientas de seguridad como el 2FA de acuerdo con la política vigente.	●									●	●	
SYA	*SoD/AS*	SYA-003	Acceso a información sensible	La información sensible se encuentra identificada y resguardada de acuerdo con el procedimiento vigente. El acceso y modificación a dicha información se encuentra previamente autorizado por los niveles correspondientes.		●								●	●	

ID DOMINIO	DOMINIO	ID CONTROL	TÍTULO DE CONTROL	DESC. CONTROL	NIVEL RIESGO			PERIODICIDAD							TIPO	
					A	M	B	AN	SE	TR	ME	SL	DI	OC	P	D
SYA	*SoD/AS*	SYA-004	Código Fuente	Al momento de realizar un cambio a los programas o implementar un nuevo desarrollo, el área de pruebas valida la integridad del código a implementar y verifica su seguridad para prevenir accesos innecesarios y código malicioso.	●									●	●	
SYA	*SoD/AS*	SYA-005	Roles y Responsabilidades	Los roles y responsabilidades enfocados a ciberseguridad se encuentran correctamente definidos y establecidos para el personal interno de acuerdo con la política vigente.	●									●	●	
SYA	*SoD/AS*	SYA-006	Roles y Responsabilidades con Terceros	Los roles y responsabilidades enfocados a ciberseguridad se encuentran correctamente definidos y establecidos para el personal externo de acuerdo con la política vigente.	●									●	●	
SGF	Seguridad física	SGF-001	Inventario de Activos Informáticos	Existe un inventario actualizado de los activos informáticos de la compañía la cual incluye dispositivos finales de los usuarios tales como equipos de escritorio, portátiles, dispositivos *IoT*, de red, de almacenamiento, servidores y demás que se encuentren conectados de alguna manera a la red corporativa para garantizar un monitoreo y protección de estos.		●								●	●	
SGF	Seguridad física	SGF-002	Seguridad de Activos Informáticos	La compañía cuenta con políticas y herramientas que garantizan la seguridad de activos informáticos a fin de proteger el resguardo y acceso a los mismos por el personal adecuado.	●									●	●	
SGF	Seguridad física	SGF-003	Acceso seguro a espacios físicos	El acceso a los espacios físicos de la compañía se encuentra restringido al personal adecuado y previamente autorizado. Se cuentan con medidas de seguridad para el ingreso tales como tarjetas magnéticas, acceso biométrico o trampas de seguridad.			●							●	●	

ID DOMINIO	DOMINIO	ID CONTROL	TÍTULO DE CONTROL	DESC. CONTROL	NIVEL RIESGO			PERIODICIDAD							TIPO	
					A	M	B	AN	SE	TR	ME	SL	DI	OC	P	D
SGF	Seguridad física	SGF-004	Acceso seguro al Data Center	El acceso al centro de cómputos se encuentra restringido a personal previamente autorizado, el mismo cuenta con ingreso por tarjeta magnética o acceso biométrico haciendo uso de trampas de seguridad si se considera necesario, gestionado a través de un requerimiento de acuerdo con la política.			●							●	●	
SGF	Seguridad física	SGF-005	Monitoreo de actividades	Las actividades del personal se encuentran monitoreadas constantemente con el fin de detectar potenciales eventos de ciberseguridad e identificar vulnerabilidades.		●							●			●
SGL	Seguridad lógica	SGL-001	Inventario de Activos Digitales	Existe un inventario actualizado de los activos digitales de la compañía en la cual se incluyen sistemas operativos, aplicaciones y demás *software* que se encuentre dentro de la red corporativa para garantizar un monitoreo y protección de estos.			●							●	●	
SGL	Seguridad lógica	SGL-002	Seguridad de Activos Digitales	La protección de activos digitales se encuentra asegurada gracias a actividades de defensa contra *software* malicioso las cuales incluyen revisiones de instalación, descargas y ejecución, políticas de protección de activos, especificación de listas blancas y negras, entre otros.	●									●	●	
SGL	Seguridad lógica	SGL-003	Seguridad de la red	La red corporativa se encuentra protegida a través de herramientas como firewall, WAF, honey pots, entre otros. La configuración e incorporación de estas herramientas se realizan de acuerdo con la política establecida.	●									●	●	
SGL	Seguridad lógica	SGL-004	Protección de web y correo	Los sitios web y correos electrónicos se encuentran debidamente protegidos a fin de evitar amenazas y notificarlas al área de tecnología en caso de presentarse.	●									●	●	

ID DOMINIO	DOMINIO	ID CONTROL	TÍTULO DE CONTROL	DESC. CONTROL	NIVEL RIESGO			PERIODICIDAD							TIPO	
					A	M	B	AN	SE	TR	ME	SL	DI	OC	P	D
SGL	Seguridad lógica	SGL-005	Monitoreo a Terceros	Para terceros con acceso a datos sensitivos o responsables de actividades o procesos críticos, los terceros son monitoreados en cuanto a las actividades realizadas de acuerdo con la política vigente para garantizar la protección de las distintas plataformas y datos.			●							●	●	
SGL	Seguridad lógica	SGL-006	Control de Autenticación	El acceso a todos los dispositivos o sistemas debe requerir autenticación para su manejo, cambios y/o acceso a funciones críticas. Los mecanismos de autenticación se deben encontrar alineados a las políticas de acceso, cambios y contraseñas.	●									●	●	
SGL	Seguridad lógica	SGL-007	Control de Autorización	La autorización al uso de los sistemas y dispositivos se encuentra configurada correctamente para prevenir accesos no autorizados al ingreso a dichos sistemas o cambios, la autorización se encuentra alienada a las políticas de accesos y cambios y soportada por herramientas como 2FA, adicionalmente la configuración incluye el bloqueo ante repetidos intentos fallidos de acceso	●									●	●	
SGL	Seguridad lógica	SGL-008	Segmentación de red	La red corporativa se encuentra segmentada a fin de restringir el acceso a funciones críticas del sistema.	●									●	●	
SGL	Seguridad lógica	SGL-009	Listas blancas y negras	La compañía cuenta con una definición de listas blancas y negras para identificar las direcciones de correo electrónico y los sitios web y herramientas aprobadas y consideradas seguras, este inventario se mantiene actualizado de acuerdo con las necesidades de la empresa.	●									●	●	
SGL	Seguridad lógica	SGL-010	Cambios a los programas	Todo cambio en la configuración debe estar correctamente documentado y aprobado de acuerdo con la política vigente.	●									●	●	

ID DOMINIO	DOMINIO	ID CONTROL	TÍTULO DE CONTROL	DESC. CONTROL	NIVEL RIESGO			PERIODICIDAD							TIPO	
					A	M	B	AN	SE	TR	ME	SL	DI	OC	P	D
SGL	Seguridad lógica	SGL-011	Alta y modificación de usuarios	Todas las altas y modificaciones de usuario se encuentran debidamente documentadas, monitoreadas y aprobadas de acuerdo con el procedimiento vigente.	●									●	●	
SGL	Seguridad lógica	SGL-012	Baja de usuarios	Todas las bajas de usuario se encuentran debidamente documentadas, monitoreadas y aprobadas de acuerdo con el procedimiento vigente. Con fines de auditoría, los usuarios dados de baja en los distintos sistemas deben ser bloqueados, no eliminados, para no perder la trazabilidad de este.	●									●	●	
SGL	Seguridad lógica	SGL-013	Transmisión de Datos	La compañía cuenta con herramientas de seguridad y clasificadas para garantizar la transmisión cifrada de la información a través de los canales adecuados.	●									●	●	
SGL	Seguridad lógica	SGL-014	IPS/IDS	La compañía cuenta con un Sistema de Detección de Intrusos (IDS) en la red corporativa con el fin de detectar tráfico no autorizado y descubrir vulnerabilidades. Asimismo, cuenta con un Sistema de Prevención de Intrusos (IPS) para realizar el bloqueo preventivo de tráfico inusual.	●								●		●	
SGL	Seguridad lógica	SGL-015	Separación de ambientes	Los ambientes de desarrollo, prueba y producción se encuentran correctamente separados a nivel lógico, asimismo existe una correcta segregación de funciones entre roles.	●									●	●	
SGL	Seguridad lógica	SGL-016	Desarrollo seguro	La compañía cuenta con herramientas que gestionan y garantizan el ciclo de vida de desarrollo seguro de los programas.			●							●	●	
SGL	Seguridad lógica	SGL-017	Acceso Remoto	El acceso remoto de los usuarios a la red de la compañía se encuentra debidamente monitoreado y securizado a través de herramientas de cifrado, VPNs y procesos de autenticación y autorización robustos de acuerdo con la política vigente.	●									●	●	

ID DOMINIO	DOMINIO	ID CONTROL	TÍTULO DE CONTROL	DESC. CONTROL	NIVEL RIESGO			PERIODICIDAD							TIPO	
					A	M	B	AN	SE	TR	ME	SL	DI	OC	P	D
SGL	Seguridad lógica	SGL-018	Configuración de Línea de Base	La configuración de línea base para las distintas tecnologías, plataformas y sistemas se encuentra debidamente creada y monitoreada de acuerdo con la política vigente y los principios de seguridad tales como el concepto de mínima funcionalidad.			●							●	●	
SGL	Seguridad lógica	SGL-019	Contraseñas Seguras	La compañía realiza un monitoreo y mantiene configuraciones en los sistemas sobre las contraseñas para asegurar que son robustas y difieren de las credenciales por defecto de acuerdo con la política vigente. Adicionalmente, tanto el usuario como la contraseña se encuentran cifrados.	●									●	●	
SGL	Seguridad lógica	SGL-020	Análisis de Tráfico	La compañía realiza un monitoreo de la red con el fin de detectar posibles amenazas hacia la infraestructura de la empresa de acuerdo con la política vigente. La revisión se lleva a cabo a través del análisis de patrones en el tráfico de la red y paquetes sospechosos provenientes de intercambio de datos a través de protocolos exclusivos a dispositivos *IoT* tales como *bluetooth*, NFC, *Zigbee*, entre otros.	●								●			●
SGL	Seguridad lógica	SGL-021	*Software* Seguro	La compañía cuenta con mecanismos de actualización de *software* de acuerdo con la política vigente. Los dispositivos cuentan con alertas para identificar nuevas actualizaciones y actualizaciones automáticas.	●									●	●	
SGL	Seguridad lógica	SGL-022	*Firmware* Seguro	La compañía cuenta con mecanismos de actualización de *firmware* de acuerdo con la política vigente. Los dispositivos cuentan con alertas para identificar nuevas actualizaciones y actualizaciones automáticas.	●									●	●	

ID DOMINIO	DOMINIO	ID CONTROL	TÍTULO DE CONTROL	DESC. CONTROL	NIVEL RIESGO			PERIODICIDAD							TIPO	
					A	M	B	AN	SE	TR	ME	SL	DI	OC	P	D
SGL	Seguridad lógica	SGL-023	Control de Cifrado	Los datos dentro de la red de la compañía se encuentran debidamente protegidos y resguardados a través de mecanismos de cifrado conforme con la política vigente.		●								●	●	
SGL	Seguridad lógica	SGL-024	Control de Versiones	La compañía cuenta con herramientas para conservar el versionado de los documentos. Todas estas versiones se mantienen en resguardo en caso de necesitar volver atrás en algún momento.		●								●	●	
SGL	Seguridad lógica	SGL-025	Usuarios inactivos	Mensualmente, la compañía realiza una revisión de los accesos de los usuarios en los distintos sistemas para identificar aquellos usuarios que no registran actividad por un periodo de 60 días y procede a su inhabilitación. En el caso que la herramienta cuente con la opción, la inhabilitación se realizará automáticamente.		●					●					●
SGL	Seguridad lógica	SGL-026	Usuarios Externos Inactivos	Mensualmente, la compañía realiza una revisión de los accesos de los usuarios externos en los distintos sistemas para identificar aquellos usuarios que no registran actividad por un periodo de 60 días y procede a su inhabilitación. En el caso que la herramienta cuente con la opción, la inhabilitación se realizará automáticamente.		●					●					●
SGL	Seguridad lógica	SGL-027	Nuevos Desarrollos	Para nuevos desarrollos, se deben especificar y documentar las principales características relacionadas a ciberseguridad tales como arquitectura, herramientas, tecnologías, *software*, usuarios, interfaces y realizar una prueba de vulnerabilidades previo a su implementación en producción.		●								●	●	

ID DOMINIO	DOMINIO	ID CONTROL	TÍTULO DE CONTROL	DESC. CONTROL	NIVEL RIESGO			PERIODICIDAD							TIPO	
					A	M	B	AN	SE	TR	ME	SL	DI	OC	P	D
SGL	Seguridad lógica	SGL-028	Control de Código	Dentro del área de pruebas en el departamento de IT, se verifica el cumplimiento del procedimiento y documentación vigente para cambios a los programas y nuevos desarrollos, se controla la integridad del código y se verifican posibles riesgos referentes a datos involucrados y código malicioso.	●									●		●
SGL	Seguridad lógica	SGL-029	Cuentas Bancarias de Proveedores	La compañía cuenta con procesos de verificación en caso de realizar cambios en la información de la cuenta bancaria de proveedores de acuerdo con la política vigente. Estos cambios deben ser monitoreados y aprobados al ser considerados información crítica.	●									●	●	
SGL	Seguridad lógica	SGL-030	Transferencias Electrónicas	La compañía cuenta con sistemas verificados y monitoreados para la liberación de transferencias electrónicas las cuales deben estar debidamente autorizadas y monitoreadas a través de protocolos de autenticación con el fin de verificar las solicitudes de transferencias bancarias de acuerdo con la política vigente.	●									●	●	
CDN	Continuidad de negocio	CDN-001	*Backup & Restore*	La compañía realiza procesos de *backup* y *restore* de acuerdo con la política vigente con los cuales se logra identificar, securizar, clasificar y administrar la información. Dicha política clasifica los sistemas por criticidad y dentro de ellos establece criterios para la ejecución de procesos de *backup* y *restore* en cuanto a frecuencia, esquema y modo de almacenamiento.	●									●	●	

ID DOMINIO	DOMINIO	ID CONTROL	TÍTULO DE CONTROL	DESC. CONTROL	NIVEL RIESGO			PERIODICIDAD							TIPO	
					A	M	B	AN	SE	TR	ME	SL	DI	OC	P	D
CDN	Continuidad de negocio	CDN -002	DRP	La compañía cuenta con un DRP (plan de respuesta a incidentes) establecido a través de políticas, programas, definición de roles, capacitaciones, entre otros, para preparar, detectar y asegurar una pronta respuesta ante un posible ciberataque.			●	●								●
CDN	Continuidad de negocio	CDN -003	Manejo de Incidentes	Ante la presencia de un incidente, el mismo se encuentra debidamente documentado detallando su análisis y proceso para de seguimiento para validar la criticidad y procesos de mitigación o corrección. Estos incidentes son reportados al área correspondiente y registrados para su seguimiento hasta el cierre del caso.	●									●		●
CDN	Continuidad de negocio	CDN -004	Continuidad de Negocio	La compañía cuenta con un plan de continuidad de negocio vigente debidamente definido, aprobado y documentado.		●								●	●	
CDN	Continuidad de negocio	CDN -005	Ciber-resiliencia	La compañía cuenta con una definición e implementación de procesos, mecanismos y herramientas tales como sistemas fail safe, balanceo de cargas o hot swap, entre otras, orientadas a alcanzar la resiliencia ante posibles incidentes de ciberseguridad.		●								●	●	
CDN	Continuidad de negocio	CDN -006	Actividades de Recuperación	Las actividades de recuperación son comunicadas tanto al personal interno como externo y se encuentran debidamente documentadas de acuerdo con la política vigente.			●							●	●	
ACC	Actividades de control	ACC-001	Monitoreo de configuración	Semestralmente, la compañía realiza una revisión de la configuración de seguridad del *software* en los distintos activos de la empresa, todo esto se encuentra alineado con la política vigente. Cualquier anomalía es derivada al área correspondiente para realizar los ajustes correspondientes.	●				●							●

ID DOMINIO	DOMINIO	ID CONTROL	TÍTULO DE CONTROL	DESC. CONTROL	NIVEL RIESGO			PERIODICIDAD							TIPO	
					A	M	B	AN	SE	TR	ME	SL	DI	OC	P	D
ACC	Actividades de control	ACC-002	*Audit log*	La compañía recolecta, alerta, revisa y retiene *audit logs* o registros de auditoría de eventos con el fin de prevenir ataques, detectar vulnerabilidades y fortalecer el proceso de resiliencia en caso de ser necesario. La revisión se lleva a cabo a través de la evaluación de alertas en los sistemas de gestión y a través de la revisión de los logs de forma manual semestralmente. Asimismo, los sistemas de la compañía deben tener habilitado el registro de logs de auditoría siempre que se permita por configuración.			●			●							●
ACC	Actividades de control	ACC-003	Monitoreo de Red	La compañía realiza un monitoreo de la red de forma diaria con el fin de detectar posibles amenazas hacia la infraestructura de la empresa de acuerdo con la política vigente. La revisión se lleva a cabo a través del análisis de patrones en el tráfico de la red y paquetes sospechosos.	●								●			●
ACC	Actividades de control	ACC-004	*PenTesting*	Anualmente, la compañía realiza pruebas de penetración o *pentestings* con el fin de identificar posibles vulnerabilidades y evaluar la efectividad de los sistemas y plataformas de la empresa. En caso de encontrar vulnerabilidades explotables, se deriva al área encargada para su solución.	●			●								●
ACC	Actividades de control	ACC-005	*PenTesting* en la nube	Anualmente, la compañía realiza pruebas de penetración con el fin de identificar posibles vulnerabilidades y evaluar la efectividad de los sistemas y plataformas de la empresa alojados en la nube. En caso de encontrar vulnerabilidades explotables, se deriva al área encargada para su solución.	●			●								●

ID DOMINIO	DOMINIO	ID CONTROL	TÍTULO DE CONTROL	DESC. CONTROL	NIVEL RIESGO			PERIODICIDAD							TIPO	
					A	M	B	AN	SE	TR	ME	SL	DI	OC	P	D
ACC	Actividades de control	ACC-006	Control de Parches	La compañía realiza una revisión sobre la aplicación oportuna de parches de seguridad en los distintos sistemas y plataformas a través de un monitoreo constante sobre novedades para mantener al día los distintos sistemas y plataformas, en caso de comunicarse una vulnerabilidad, realizar el parcheo necesario de forma inmediata acompañándolo con su documentación y resguardo.	●									●		●
ACC	Actividades de control	ACC-007	Control de Vulnerabilidades	Anualmente, se realiza una revisión de vulnerabilidades sobre los activos de la compañía. Las vulnerabilidades identificadas se encuentran documentadas de acuerdo con la política vigente.	●			●								●
ACC	Actividades de control	ACC-008	Inteligencia de Amenazas	La compañía se encuentra al día en cuanto a novedades de ciberseguridad desde diferentes fuentes fiables a fin de garantizar el proceso de inteligencia de ciber amenazas, que puede ser aplicable a la empresa. En caso de encontrar novedades aplicables a algunos de los sistemas, se deriva al área correspondiente para su tratamiento.			●						●		●	
ACC	Actividades de control	ACC-009	Control de Amenazas	Las amenazas detectadas con base en los controles de monitoreo se encuentran documentadas acordes a la política vigente.		●								●		●
ACC	Actividades de control	ACC-010	Control de Alertas sobre Incidentes	La compañía cuenta con herramientas que alertan actividades de modificación de registros en tablas consideradas de criticidad alta en las bases de datos principales de la compañía. Ante una alerta se realiza la revisión del incidente y se deriva al área responsable para su solución.			●						●			●

ID DOMINIO	DOMINIO	ID CONTROL	TÍTULO DE CONTROL	DESC. CONTROL	NIVEL RIESGO			PERIODICIDAD							TIPO	
					A	M	B	AN	SE	TR	ME	SL	DI	OC	P	D
ACC	Actividades de control	ACC-011	Control de Protección	Los activos informáticos de la compañía cuentan con protección contra *software* malicioso a través de herramientas de seguridad como antivirus y antispyware.	●									●	●	
ACC	Actividades de control	ACC-012	Control de *Firmware* Vigente	Trimestralmente, la compañía realiza un monitoreo sobre el *software* para validar la vigencia de este. En caso de encontrar *software* obsoleto, se realiza inmediatamente la actualización correspondiente y se documenta de acuerdo con la política vigente.	●					●						●
ACC	Actividades de control	ACC-013	Control de *Software* Vigente	Trimestralmente, la compañía realiza un monitoreo sobre el *firmware* para validar la vigencia de este. En caso de encontrar *firmware* obsoleto, se realiza inmediatamente la actualización correspondiente y se documenta de acuerdo con la política vigente.	●					●						●
ACC	Actividades de control	ACC-014	Monitoreo de *Backups*	Diariamente, se valida la correcta ejecución de *backups*, ante un error se realiza la re-ejecución de este, en caso de persistir el error, se deriva al área correspondiente.	●								●			●
ACC	Actividades de control	ACC-015	Pruebas de *Restore*	Anualmente, la compañía realiza revisiones sobre la eficiencia de las herramientas de respaldo tales como bases de datos o máquinas virtuales dentro de cada herramienta de *backup*. El resultado de la prueba debe ser documentando de acuerdo con la política vigente, en caso de presentarse errores en la ejecución o la integridad de los datos, se deriva al área correspondiente para su solución.	●			●								●

ID DOMINIO	DOMINIO	ID CONTROL	TÍTULO DE CONTROL	DESC. CONTROL	NIVEL RIESGO			PERIODICIDAD							TIPO	
					A	M	B	AN	SE	TR	ME	SL	DI	OC	P	D
ACC	Actividades de control	ACC-016	Monitoreo de Desarrolladores	Mensualmente, se realiza una revisión sobre los accesos de desarrolladores a ambientes productivos de bases de datos y sistemas operativos para validar que los mismos cuenten con permiso de sólo lectura. En caso de encontrar inconsistencias, se realiza una revisión sobre las actividades realizadas por el usuario y si es necesario dar de baja el permiso.	●						●					●
ACC	Actividades de control	ACC-017	Actualización de Matriz *SoD*	Anualmente la compañía realiza una revisión sobre los roles, funciones y accesos sensitivos a los distintos aplicativos. En caso de identificar accesos que no corresponden, se deriva al área correspondiente para su justificación y dar de baja en caso de ser necesario.	●			●							●	
ACC	Actividades de control	ACC-018	Monitoreo de Inventario de Activos Informáticos	Anualmente, la compañía realiza una revisión sobre el inventario de los activos informáticos de la compañía que se encuentran conectados de alguna manera a la infraestructura empresarial con el fin de garantizar las actividades de monitoreo y protección sobre todos los activos informáticos de la compañía. En caso de detectar anomalías, se revisa el caso, se documenta el incidente y se remedia actualizando el inventario de acuerdo con la política vigente.	●			●								●

ID DOMINIO	DOMINIO	ID CONTROL	TÍTULO DE CONTROL	DESC. CONTROL	NIVEL RIESGO			PERIODICIDAD							TIPO	
					A	M	B	AN	SE	TR	ME	SL	DI	OC	P	D
ACC	Actividades de control	ACC-019	Monitoreo de Inventario de Activos Digitales	Anualmente, la compañía realiza una revisión sobre el inventario de los activos digitales de la compañía que se encuentran conectados de alguna manera a la infraestructura empresarial con el fin de garantizar las actividades de monitoreo y protección sobre todos los activos digitales de la compañía. En caso de detectar anomalías, se revisa el caso, se documenta el incidente y se remedia actualizando el inventario de acuerdo con la política vigente.	●			●								●
ACC	Actividades de control	ACC-020	Vigencia de accesos en los sistemas	Anualmente, la compañía revisa la vigencia de los accesos de los usuarios a los sistemas y carpetas considerados sensitivos y en caso de encontrar anomalías lo deriva al área correspondiente para su justificación o corrección.	●			●								●
ACC	Actividades de control	ACC-021	Seguimiento de incidentes	Mensualmente, la compañía realiza una revisión sobre los incidentes identificados, reportados y documentados en la herramienta correspondiente para su correcto monitoreo y seguimiento. De acuerdo con esto, la compañía registra la cantidad de incidentes y el estado de seguimiento de estos para alimentar métricas que se documentan en un reporte de situación sobre los incidentes.	●						●					●

6.3RECOMENDACIONES

Alineado al plan de trabajo propuesto en el capítulo anterior, existen actualmente una serie de metodologías, herramientas y recomendaciones de grandes compañías reconocidas a nivel global, las cuales se pueden utilizar como base o adicional a lo propuesto en esta tesis.

Dentro de las herramientas recomendadas, se encuentra principalmente el *OWASP IoT* Top 10 el cual detalla las principales vulnerabilidades a las que se enfrentan los dispositivos inteligentes y esto puede servir como base para implementar controles que se enfoquen en garantizar la seguridad de los dispositivos frente a estas vulnerabilidades.

También, la evaluación de seguridad *IoT* de *GSMA* ofrece un marco de referencia adaptable a cada compañía a través de una serie de mejores prácticas y soluciones. Esta evaluación permite darle a conocer a la empresa el nivel de seguridad de sus procesos y dispositivos.

Otra metodología ampliamente reconocida y de gran ayuda es *STIG* o *Guía de implementación técnica de seguridad del Departamento de Defensa de los Estados Unidos* la cual ofrece una referencia para la instalación segura y gestión de *hardware* y *software*.

Existen también herramientas para el prototipado o virtualización de entornos *IoT* como la *Azure Digital Twins* de *Microsoft*.

Dentro de los controles propuestos en esta tesis como parte de la matriz de ciberseguridad e *IoT*, se detalla la importancia de la segregación de funciones y accesos sensitivos en las distintas herramientas y entornos, una herramienta de gran ayuda para la definición de roles y responsabilidades es la *Matriz RACI* la cual es ampliamente utilizada en gestión de proyectos.

Finalmente, las metodologías *Cybersecurity Kill Chain* propuesta por *Lockheed Martin*[58] y *ATT&CK* de *MITRE*[59] abordan la ciberseguridad desde distintos enfoques. La principal diferencia, es que la *Cybersecurity Kill Chain* se basa en los pasos para un ciberataque mientras que *ATT&CK* es una matriz basada en las técnicas y tácticas utilizadas para los ciberataques. Ambas metodologías son ampliamente reconocidas y aceptadas, por lo cual los controles y pasos propuestos pueden ser adaptados de acuerdo con la necesidad de la compañía.

---

[58] Multinacional Estadounidense enfocada en la industria aeroespacial y militar.

[59] Organización no gubernamental sin fines de lucro proveniente del MIT (Instituto de Tecnología de Massachusetts) enfocado en brindar asistencia tecnología a distintas agencias gubernamentales de Estados Unidos.

Finalmente, como complemento de la matriz de controles de ciberseguridad e *IoT* propuestas en esta tesis, se detallan a continuación una serie de recomendaciones o buenas prácticas para el uso correcto y seguro de dispositivos *IoT* en cualquier entorno.

- Cambiar las credenciales por defecto y establecer contraseñas seguras y únicas.
- Establecer doble factor de autenticación a las aplicaciones.
- Cambiar las contraseñas máximo cada 90 días.
- No compartir contraseñas, códigos de verificación o información sensible/privada con nadie ni a través de comentarios o publicaciones en redes sociales. Esta información no es necesaria para ninguna persona o entidad en ningún caso.
- Habilitar únicamente los servicios a utilizar en el momento, asegurarse de mantener desactivados aquellos que no son necesarios. Ejemplo: *bluetooth*, *AirDrop*, *Wifi*, entre otros.
- Realizar una breve indagación sobre el proveedor o dispositivo a adquirir para garantizar que este permita actualizaciones de seguridad, protección de datos y cuente con buena reputación.
- Mantener copias de respaldo de la información.
- Instalar aplicaciones únicamente desde sitios oficiales.
- Mantener las aplicaciones actualizadas.
- Asegurarse de que la comunicación entre aplicaciones sea cifrada.
- Modificar las configuraciones de seguridad de acuerdo con las necesidades del usuario.
- Limitar el acceso a los dispositivos únicamente a lo necesario.
- Mantener firewall activo y actualizado.
- Revisar los términos y condiciones de uso de las diferentes herramientas relacionadas al dispositivo *IoT*.
- Mantener el Sistema Operativo y *Firmware* actualizado.
- Mantener el navegador web actualizado.
- Utilizar antivirus y antispyware.
- No conectarse a redes públicas si es posible, en caso de hacerlo, abstenerse de ingresar a plataformas críticas como bancos o billeteras virtuales.

- Evitar vincular el dispositivo *IoT* a dispositivos desconocidos o a los cuales no sea posible garantizar su nivel de seguridad.
- Garantizar la seguridad física del dispositivo limitando su acceso únicamente a los usuarios habilitados.

Es importante entender que, como se mencionó retiradamente en este documento, la seguridad de los dispositivos *IoT* no se encuentra siempre garantizada desde fábrica por su proveedor, de hecho, esta es una de las principales desventajas de estos dispositivos, por lo cual el usuario debe garantizar por su parte la seguridad de los dispositivos a su cargo y por consiguiente de los datos y la información que estos manejan para de esta forma prevenir posibles incidentes de seguridad.

7) CONCLUSIONES.

A lo largo de esta tesis, se han planteado diferentes situaciones actuales respecto al Internet de las Cosas y su inclusión en diferentes entornos, de acuerdo con esto se obtuvo un conocimiento respecto a esta tecnología, sus ventajas, desventajas, usos, regulaciones, vectores de ataque y demás temas para los cuales se puede concluir que el Internet de las cosas se encuentra en auge y en crecimiento exponencial, es posible determinar que la principal desventaja hoy en día en los dispositivos inteligentes, es la falta o poca seguridad incorporada lo cual es una falencia del lado del proveedor, por lo cual, la seguridad de estos dispositivos recae en gran medida de las buenas prácticas del lado del usuario.

Se concluye también, que si bien esta desventaja es significativa, no se sugiere que se limite el uso de estos dispositivos, al contrario, su inclusión facilita los procesos en entornos empresariales, minimiza costos y en general facilita las tareas diarias de las personas lo cual es un gran beneficio, pero esta inclusión debe hacerse de forma responsable, teniendo en cuenta recomendaciones de seguridad especialmente cuando estos dispositivos son pieza clave dentro de un proceso y por consiguiente pueden llegar a manejar información sensitiva.

En cuanto a la inclusión de la tecnología *IoT* en empresas en proceso de transformación digital, la información proporcionada en esta tesis, junto con el plan de trabajo, recomendaciones y matriz de controles, pretende ofrecer una guía para la correcta incorporación de objetos inteligentes en los procesos de negocio, garantizando su seguridad desde la incorporación, así como mantener un seguimiento y control de los mismos para evitar posibles incidentes de ciberseguridad.

Durante el desarrollo y la investigación para esta tesis, se encontró que la estandarización para *IoT* y las normas o regulaciones asociadas a esta tecnología son mínimas teniendo en cuenta lo presente que se encuentra esta tecnología en diferentes ambientes. Si bien, en países como Estados Unidos o Brasil se ha comenzado recientemente a trabajar en este tema a través de regulaciones para garantizar la ciberseguridad de los dispositivos inteligentes desde su etapa de desarrollo, esto debería replicarse de forma global teniendo en cuenta que existen varios países en donde hay *Smart Cities* como Argentina o Colombia, y también, esta tecnología ha ayudado en la innovación en áreas como la salud, ganadería, transporte, indumentaria, e incluso en infraestructuras críticas, por lo cual, una regulación debería ser el primer paso a tener en cuenta antes de realizar una implementación de gran tamaño e impacto.

Asimismo, las evaluaciones de seguridad actualmente se enfocan en las tecnologías de la información y de la operación, incluso a la ciberseguridad, pero son pocas las que se ofrecen o realizan con un enfoque a Internet de las Cosas, lo cual debería considerarse de manera prioritaria cuando esta tecnología es utilizada dentro de los procesos de la compañía, adicionalmente, teniendo en cuenta que una evaluación enfocada a *IoT* puede de igual forma agrupar otras tecnologías como *Big Data*, *Cloud* o Inteligencia Artificial que son también grandes puertas de entrada para un ciber incidente si estas no se encuentran correctamente configuradas y monitoreadas.

Teniendo en cuenta lo identificado a partir de la investigación realizada, se propone en esta tesis una ayuda para las empresas en proceso de transformación digital con tecnologías *IoT* incluidas en sus procesos, a través de un plan de trabajo, un set de buenas prácticas y una matriz de controles, los cuales se pretende sean utilizados como como complementos entre sí ya que deben ser adaptados al tipo y objetivo del negocio.

Adicionalmente, la información, educación y capacitación sobre Internet de las Cosas debería ser más accesible y no limitarse a personas dentro del rubro de la tecnología, teniendo en cuenta que prácticamente hoy en día, cualquier persona cuenta con al menos un *Smartphone* y hace uso del mismo sin saber que este hace parte de la tecnología *IoT*. Si este tema se tuviera más en el común actualmente, seguramente su adopción y credibilidad sería mayor, teniendo en cuenta que varios de sus casos de uso se encuentran en áreas críticas como la salud en marcapasos o prótesis inteligentes, así como también en *Smart Cities* para prevención de desastres por ejemplo, pero todo lo relacionado a la tecnología *Smart* suele asociarse a objetos menos críticos como relojes inteligentes, luces, candados, cafeteras, monitores, asistentes virtuales, entre otros.

Finalmente, se espera que esta investigación y los recursos propuestos, sean de gran ayuda para la correcta y segura adopción de la tecnología *IoT* en diferentes entornos, especialmente, ambientes empresariales para pequeñas, medianas y grandes empresas que desean conocer y monitorear el estado de la ciberseguridad de su compañía al incluir objetos inteligentes en su negocio como parte de su proceso de transformación digital.

Se espera también, que esta tesis de alguna manera sirva como base para el desarrollo de evaluaciones en ciberseguridad más exigentes y con enfoque a nuevas tecnologías como el Internet de las cosas haciendo uso de las diferentes herramientas existentes o que se puedan desarrollar, sin dejar de lado la capacitación, concientización y monitoreo constante como prioridad al incluir IoT en diferentes procesos o en el día a día.

8) BIBLIOGRAFÍA.

Adeva, Roberto (2020). Tecnologías inalámbricas: diferencias y usos de *Wifi*, *Bluetooth*, *Zigbee* y *Z-wave*. ADSL Zone. Recuperado de: https://www.adslzone.net/reportajes/tecnologia/estandares-conexion-inalambrica/

Álvarez, Martin (2019). Estándares del W3C para *IoT*. Fundación CTIC. Recuperado de: https://www.fundacionctic.org/es/actualidad/estandares-del-w3c-para-*IoT*

Anscombe, Tony (2019). Legislar la seguridad de los dispositivos *IoT*: ¿es realmente la solución? WeLiveSecurity. Recuperado de: https://www.welivesecurity.com/la-es/2019/05/06/legislar-seguridad-dispositivos-*IoT*/

Arechalde Ugarteche, Ibon (2019). Estandarización de protocolos de datos: clave para el éxito de proyectos de *IoT*. Tecnalia. Recuperado de: http://blogs.tecnalia.com/inspiring-blog/2019/03/14/estandarizacion-protocolos-datos-clave-exito-proyectos-*IoT*/

Bhagat, Varun (2019). *IoT* Trends in 2020: 5 Things You Need to Know. *IoT* for all. Recuperado de: https://www.*IoT*forall.com/*IoT*-devices-by-2020

Biurrun Abad, Fernando (2020). La seguridad del Internet de las cosas (*IoT*) va a tener su primera regulación en California. LegalToday. Recuperado de: https://www.legaltoday.com/legaltech/nuevas-tecnologias/la-seguridad-del-internet-de-las-cosas-*IoT*-va-a-tener-su-primera-regulacion-en-california-2020-01-03/

Casadomo (2020). La nueva ley de seguridad de dispositivos *IoT* de Reino Unido se basa en contraseñas, actualizaciones e incidencias. Casadomo. Recuperado de: https://www.casadomo.com/2020/01/29/nueva-ley-seguridad-dispositivos-*IoT*-reino-unido-basa-contrasenas-actualizaciones-incidencias

Casadomo (2020). Reino Unido dispone de 30 verificaciones para garantizar la seguridad y privacidad de los dispositivos *IoT*. Casadomo. Recuperado de:

https://www.casadomo.com/2020/01/14/reino-unido-dispone-30-verificaciones-garantizar-seguridad-privacidad-dispositivos-*IoT*

Computer World (2020). El 'Shadow *IoT*' se convierte en uno de los principales riesgos empresariales. España. Computerworld. Recuperado de: https://cso.computerworld.es/tendencias/el-shadow-*IoT*-se-convierte-en-uno-de-los-principales-riesgos-empresariales

Dark Reading (2020). New Report Links *Cybersecurity* and Sustainability. Dark Reading. Recuperado de: https://www.darkreading.com/risk/new-report-links-*Cybersecurity*-and-sustainability/d/d-id/1339274

e*Smart*City (2018). La Organización Internacional de Normalización publica el primer estándar internacional para Internet de las Cosas. España. e*Smart*City. Recuperado de: https://www.e*Smart*city.es/2018/11/08/organizacion-internacional-normalizacion-publica-primer-estandar-internacional-internet-de-las-cosas

Espinoza Carrión, Cecibel del Rocío. Pérez Espinoza, María José. Peralta Mocha, María Beatriz. (2017). El Internet de las cosas: Antecedentes, conceptualización y riesgos.

Evans, Dave (2011). *Internet of Things*: La próxima evolución de Internet lo está cambiando todo.

Hernández Sampieri, R., Mendoza Torres, C. P. (2018). Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta. México: McGraw-Hill Interamericana.

García Rubio, Gabriel (2018). La estandarización se refuerza en materia de *IoT* a través de la ISO. La innovación necesaria. Recuperado de: https://www.lainnovacionnecesaria.com/la-estandarizacion-se-refuerza-en-materia-de-*IoT*-a-traves-de-la-iso/

Goodin, Dan (2020). When coffee makers are demanding a ransom, you know *IoT* is screwed. Ars Technica. Recuperado de: https://arstechnica.com/information-technology/2020/09/how-a-hacker-turned-a-250-coffee-maker-into-ransom-machine/

Granero, Gustavo (2018). Primera Norma internacional ISO/IEC para Internet de las cosas. España. UNE. Recuperado de: https://www.une.org/salainformaciondocumentos/NP%20Primera%20Norma%20ISO%20de%20*IoT*%20nov-18.pdf

IoT Security Fundation (2020). Recuperado de: https://www.*IoT*securityfoundation.org/

ISO Tools (2018). Norma ISO/IEC 30141 sobre Internet de las Cosas (*IoT*). ISO Tools. Recuperado de: https://www.isotools.org/2018/11/21/norma-iso-iec-30141-internet-cosas-*IoT*/

Johnston, Kevin (2020). *OWASP IoT* Top 10. A gentle introduction and an exploration of root causes. Recuperado de: https://*OWASP*.org/www-chapter-toronto/assets/slides/2019-12-11-*OWASP*-*IoT*-Top-10---Introduction-and-Root-Causes.pdf

Lovells, Hogan (2019). A comparison of *IoT* regulatory uncertainty in the EU, China, and the United States. Recuperado de: https://www.hoganlovells.com/~/media/hogan-lovells/pdf/2019/a_comparison_of_*IoT*_regulatory_uncertainty.pdf?la=en

Martin, James A. (2019). What is shadow *IoT*? How to mitigate the risk. CsoOnline. Recuperado de: https://www.csoonline.com/article/3346082/what-is-shadow-*IoT*-how-to-mitigate-the-risk.html

Menze, Thomas. (2020). The state of industrial *Cybersecurity* in the era of digitalization. Recuperado de: https://ics-cert.*Kaspersky*.com/media/*Kaspersky*_ARC_ICS-2020-Trend-Report.pdf

Ministerio de Modernización. Presidencia de la Nación. Argentina. (2017). “Consulta pública sobre Internet de las Cosas”

Network World (2020). Internet de las cosas en 2020: más vital que nunca. España. NetworkWorld. Recuperado de:

https://www.networkworld.es/telecomunicaciones/internet-de-las-cosas-en-2020-mas-vital-que-nunca

OWASP IoT Security Team. (2018). *OWASP Internet of Things* Top 10. Recuperado de: https://*OWASP*.org/www-project-internet-of-things/

OWASP (2023). Projects. Recuperado de: https://*OWASP*.org/projects/

Paz, Álvaro (2020). Seguridad en dispositivos *IoT*. España. Gurú de la informática. Recuperado de: https://gurudelainformatica.es/seguridad-en-dispositivos-*IoT*.

Prensa CambioDigital Online (2018). La ISO publica su primer estándar para *IoT*. Cambio Digital Online. Recuperado de: https://cambiodigital-ol.com/2018/11/la-iso-publica-su-primer-estandar-para-*IoT*/

RedesTelecom (2020). Shadow *IoT*: la amenaza de la hiperconectividad. España. Computing. Recuperado de: https://www.computing.es/seguridad/noticias/1118123002501/shadow-*IoT*-amenaza-de-hiperconectividad.1.html

Rodriguez, Desiree (2019). ¿Estamos cerca de una regulación *IoT*? GlobbSecurity. Recuperado de: https://globbsecurity.com/estamos-cerca-de-una-regulacion-*IoT*-44868/

Rose, Karen. Eldridge, Scott. Chapin, Lyman. (2015). La Internet de las Cosas – Una breve reseña.

Telefónica (2020). Telefónica presenta su segundo estudio sobre *IoT* en el que se constata un aumento de su uso en un 66% en dos años. Madrid, España. Telefónica. Recuperado de: https://www.telefonica.com/es/web/sala-de-prensa/-/telefonica-presenta-su-segundo-estudio-sobre-*IoT*-en-el-que-se-constata-un-aumento-de-su-uso-en-un-66-en-dos-anos

I-Scoop (2023). Making sense of *IoT* (*Internet of Things*) – the *IoT* business guide. Recuperado de: https://www.i-scoop.eu/internet-of-things-guide/

Rout, Deepak (2015). Developing a Common Understanding of *Cybersecurity*. *ISACA, 6*. Recuperado de: https://www.isaca.org/resources/isaca-journal/issues/2015/volume-6/developing-a-common-understanding-of-*Cybersecurity*

Foomany, Farbod H. Mohammed, Nathanael (2019). Building Security Into *IoT* Devices. *ISACA, 6*. Recuperado de: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-6/building-security-into-*IoT*-devices

Instituto nacional de transparencia, acceso a la información y protección de datos personales (2021). *INAI, 261.* Inai advierte riesgos a la privacidad por conexión de aparatos domésticos al internet. Recuperado de: https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-261-21.pdf

Patel, Hemant (2017) *ISACA, 3*. *IoT* Needs Better Security. Recuperado de: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/*IoT*-needs-better-security

Moor, John (2018). *IoT Security Foundation*. *IoT Cybersecurity*: Regulation Ready.

Berthing, Hans Henrik. Blum, Dan. Boardman, Allan. Hanson, Robert. Herold, Rebecca. Lageschulte, Phil J. Marks, Norman. Tavares Da Silva, Aureo Monteiro. Newell, Dave. Nyamari, Jotham. Singh, Gurvinder (2015). *ISACA. Internet of Things*: risk and value consideration. Recuperado de: https://vbn.aau.dk/ws/portalfiles/portal/208325607/Internet_of_Things_whp_Eng_0115.pdf

Wlosinski, Larry G. (2019). *ISACA, 4.* The *IoT* as a Growing Threat to Organizations. Recuperado de: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-4/the-*IoT*-as-a-growing-threat-to-organizations

Banco Interamericano de Desarrollo; Organización de los Estados Americanos (2020) Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. Recuperado de: https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

Morgan Stanley Research. (2016). The *Internet of Things* and the new industrial revolution. Recuperado de: https://www.morganstanley.com/ideas/industrial-internet-of-things-and-automation-robotics

Industry *IoT* Consortium. (2023). Industry *IoT* Consortium. Recuperado de: https://www.iiconsortium.org/

ABI Research. (2014). The Internet of Robotic Things (IoRT), Greatly Expanding Capabilities and Business Opportunities. Recuperado de: https://www.abiresearch.com/press/the-internet-of-robotic-things-iort-greatly-expand/

Verizon. (2016). State of the Market: *Internet of Things* 2016. Recuperado de: https://www.verizon.com/about/sites/default/files/state-of-the-internet-of-things-market-report-2016.pdf

CABASE. (2020). Impulsada por CABASE, nace la Cámara Argentina de *IoT*. Recuperado de: https://www.cabase.org.ar/impulsada-por-cabase-nace-la-camara-argentina-de-*IoT*/

Telecom. (2020). *IOT*: las perspectivas para 2021. Recuperado de: https://www.telecom.com.ar/blog/nota/*IoT*-las-perspectivas-para-2021

Microsoft. (2020). Señales de *IoT*. Recuperado de: https://azure.*Microsoft*.com/mediahandler/files/resourcefiles/*IoT*-signals/es-es/*IoT*%20Signals_Edition%202_Spanish.pdf

Moura, Philipe. Nicoletti, Stefano. (2018). *GSMA*. Ciudades inteligentes e Internet de las Cosas: cómo fomentar su desarrollo en América Latina. Recuperado de: https://www.*GSMA*.com/latinamerica/wp-content/uploads/2018/11/*IoT*Guide-ESP-NOV-DIG.pdf

CISCO. (2020). *Cisco* Annual Internet Report (2018–2023) White Paper. Recuperado de: https://www.*Cisco*.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

IoT Security Foundation. (2020). Consumer *IoT*: Vulnerability disclosure – Expanding the view into 2021. Recuperado de: https://www.*IoT*securityfoundation.org/wp-content/uploads/2020/11/Vulnerability-Disclosure-2021.pdf

IoT For All. (2023). Recuperado de: https://www.*IoT*forall.com/

Herzberg, Ben. Zeifman, Igal. Bekerman, Dima. (2016). Breaking Down *Mirai*: An *IoT DDOS Botnet* Analysis. Recuperado de: https://www.imperva.com/blog/*malware*-analysis-*Mirai*-*DDOS*-*botnet*/?redirect=Incapsula

Cirani, Simone. Ferrari, Gianluigi. Picone, Marco. Veltri, Luca. (2018). *WILEY*. *Internet of Things*. Architectures, Protocols and Standards. Recuperado de: https://aitskadapa.ac.in/e-books/CSE/*IOT*/Internet%20of%20Things_%20Architectures,%20Protocols%20and%20Standards%20(%20PDFDrive%20).pdf

IBM. (2023). Genere confianza en sus datos de *IoT* con *blockchain*. Recuperado de: https://www.*IBM*.com/es-es/topics/*blockchain*-*IoT*

Cuomo, Jerry. (2020). How *blockchain* adds trust to AI and *IoT*. Recuperado de: https://www.*IBM*.com/blogs/*blockchain*/2020/08/how-*blockchain*-adds-trust-to-ai-and-*IoT*/

Miñano Carmona, Pablo Antonio. (2019). *Universitat Oberta de Catalunya (UOC).* Seguridad en los ecosistemas *IoT*. Recuperado de: http://openaccess.uoc.edu/webapps/o2/handle/10609/96607

Strom, David. (2020). *Avast*. El regreso de la *botnet Mirai*. Recuperado de: https://blog.avast.com/es/return-of-*Mirai*-*botnet*-avast

Centro de respuestas ante incidentes cibernéticos (CERT-PY). (2016). *Botnet Mirai* y otras amenazas a dispositivos conectados a Internet (*IoT*). Recuperado de: https://www.cert.gov.py/application/files/1814/7801/3058/Boletin_20161031_*Botnet_Mirai*.pdf

BBC News Mundo. (2015). El virus que tomó control de mil máquinas y les ordenó autodestruirse. Recuperado de: https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_*Stuxnet*

Abbott. (2023). Recuperado de: https://www.*Abbott*.com/about-*Abbott*.html

INFOBAE. (2017). Por qué las autoridades alemanas ordenaron a los padres destruir "con un martillo" una polémica muñeca. Recuperado de: https://www.infobae.com/america/tecno/2017/04/18/las-autoridades-alemanas-ordenaron-destruir-con-un-martillo-a-mi-amiga-*Cayla*-la-polemica-muneca-acusada-de-espionaje/

La Sexta. (2018). *Cayla*, la muñeca perfecta para espiar y la peor enemiga de la seguridad de los más pequeños. Recuperado de: https://www.lasexta.com/noticias/sociedad/*Cayla*-la-muneca-perfecta-para-espiar-y-la-peor-enemiga-de-la-seguridad-de-los-mas-pequenos_2017030558bc810c0cf2894da4629d55.html

BBC News Mundo. (2015). La polémica Barbie a la que acusan de espiar a los niños. Recuperado de: https://www.bbc.com/mundo/noticias/2015/12/151215_finde_tecnologia_barbie_interactiva_habla_polemica_espia_ninos_lv

BBC News Mundo. (2016). La muñeca *Cayla* y otros juguetes interactivos a los que acusan de espiar a niños. Recuperado de: https://www.bbc.com/mundo/noticias-38268689

BBC News Mundo. (2017). Por qué las autoridades de Alemania pidieron a los padres que destruyan a *Cayla*, la "muñeca espía". Recuperado de: https://www.bbc.com/mundo/noticias-39010133

TLIFE. (2016, 19 de mayo). *Cayla*, la muñeca conectada que conversa con tu hijo [Video]. YouTube. Recuperado de: https://www.youtube.com/watch?v=aYejrCc-_V0

Curiosidades con Mike. (2017, 14 de septiembre). Qué Hay Dentro de *Cayla* la muñeca espía prohibida en ALEMANIA? Y la muñeca poseída de Perú? [Video]. YouTube. Recuperado de: https://www.youtube.com/watch?v=J1nprWXK8qQ

Esposito, Jeffrey. (2017, 21 de febrero). *Kaspersky Daily.* La muñeca conectada *Cayla* pone a los niños en riesgo. Recuperado de: https://www.*Kaspersky*.es/blog/my-friend-*Cayla*-risks/10112/

Borghello, Cristian. (2017, 01 de septiembre). *Segu-Info.* Marcapasos deben ser actualizados por riesgo de hacking. Recuperado de: https://blog.segu-info.com.ar/2017/09/marcapasos-deben-ser-actualizados-por.html

Borghello, Cristian. (2018, 23 de mayo). *Segu-Info.* Actualiza tu marcapasos para evitar fallos. Recuperado de: https://blog.segu-info.com.ar/2018/05/actualiza-tu-marcapasos-para-evitar.html?m=0

La Vanguardia Barcelona. (2022, 14 de enero). Un joven de tan solo 19 años asegura haber hackeado más de 25 coches *Tesla*. Recuperado de: https://www.lavanguardia.com/motor/actualidad/20220114/7987123/joven-19-anos-asegura-haber-hackeado-25-coches-*Tesla*-pmv.html

14CORE. (2023). The *IOT* Protocols The Base of *Internet of Things* Ecosystem. Recuperado de: https://www.14core.com/the-*IoT*-protocols-the-base-of-internet-of-things-ecosystem/

Clarín. (2022, 26 de enero). Tiene 19 años y encontró la forma de hackear autos de *Tesla* en 13 países distintos. Recuperado de: https://www.clarin.com/autos/19-anos-encontro-forma-hackear-autos-*Tesla*-13-paises-distintos_0_zrMKjnARUl.html

ADSL Zone. (2022, 11 de enero). «Tengo el control de 25 coches *Tesla* en 13 países». Recuperado de: https://www.adslzone.net/noticias/seguridad/hackeo-coches-*Tesla*-2022-cuenta-vulnerabilidad/

Semana. (2022, 14 de enero). Descubren una vulnerabilidad en los autos *Tesla* que permite su hackeo. Recuperado de: https://www.semana.com/tecnologia/articulo/descubren-una-vulnerabilidad-en-los-autos-*Tesla*-que-permite-su-hackeo/202235/

Carvajal, Chema. (2021, 22 de octubre). *Computer hoy.* Consiguen hackear un *Tesla* para acceder a los datos del conductor: velocidad máxima, estilo de conducción.... Recuperado de: https://computerhoy.com/noticias/tecnologia/consiguen-hackear-*Tesla*-acceder-datos-conductor-velocidad-maxima-estilo-conduccion-952137

Colombo, David. (2022, 24 de enero). *Medium*. How I got access to 25+ *Tesla*'s around the world. By accident. And curiosity. Recuperado de: https://medium.com/@david_colombo/how-i-got-access-to-25-*Tesla*s-around-the-world-by-accident-and-curiosity-8b9ef040a028

Peris, Javier. (2021, 25 de marzo). *Service Management Institute.* Necesidades de Estandarización en *IoT*. Recuperado de: https://news.itsmf.es/necesidades-de-estandarizacion-en-*IoT*/

GSMA. (2020). The mobile economy Latin America 2020. Recuperado de: https://www.*GSMA*.com/mobileeconomy/wp-content/uploads/2020/12/*GSMA*_MobileEconomy2020_LATAM_Eng.pdf

Innovate UK. Office of the Secretary of State for Scotland. Mundell, David. (2017, 07 de noviembre). Glasgow becomes a world-leading *Smart City*. Recuperado de: https://www.gov.uk/government/news/glasgow-becomes-a-world-leading-*Smart*-city

Borghello, Cristian. (2022, 19 de marzo). *Segu-Info.* Los 11 nuevos controles de la ISO 27002:2022. Recuperado de: https://blog.segu-info.com.ar/2022/03/los-11-nuevos-controles-de-la-iso.html?m=0

Borghello, Cristian. (2021, 12 de junio). *Segu-Info.* Novedades sobre ISO 27002:2013. Recuperado de: https://blog.segu-info.com.ar/2021/06/novedades-sobre-iso-2700232013.html?m=0

ISO/IEC JTC 1/SC 27. (2022). ISO/IEC 27002:2022 Information security, *Cybersecurity* and privacy protection — Information security controls. Recuperado de: https://www.iso.org/standard/75652.html

Borghello, Cristian. (2022, 25 de enero). *Segu-Info.* Cambios en la nueva ISO/IEC 27002:2022. Recuperado de: https://blog.segu-info.com.ar/2022/01/cambios-en-la-nueva-isoiec-270022022.html

Taich, Diego. (2022, 20 de enero). *iProUP*. Privacidad e Internet de las Cosas: momento de replantear las políticas de privacidad. Recuperado de: https://www.iproup.com/innovacion/29037-privacidad-e-*IoT*-hay-que-replantear-politicas-de-privacidad

Gartner. (2018, 31 de enero). 2018 *IoT* Security Survey Report. Recuperado de: https://www.gartner.com/en/documents/3855285

Kaspersky. (2020). Benefits and challenges of *IoT* in business. Recuperado de: https://media.*Kaspersky*daily.com/wp-content/uploads/sites/85/2020/05/21102818/2020_*Kaspersky_IoT*_report.pdf

Stelfox, Sam. (2019, 01 de noviembre). *Minim*. What is Gafgyt *malware*? *Smart* home *Cybersecurity* news. Recuperado de: https://www.minim.com/blog/*Smart*-home-*Cybersecurity*-news-roundup-what-is-gafgyt-*malware*-october-2019-edition

Demeter, Dan, Preuss, Marco, Shmelev, Yaroslav. (2019, 15 de octubre) *Securelist by Kaspersky*. *IoT*: a *malware* story. Recuperado de: https://securelist.com/*IoT*-a-*malware*-story/94451/

Kuzin, Mikhail. Shmelev, Yaroslav. Kuskov, Vladimir. (2018, 18 de septiembre). *Kaspersky* Secure ListNew trends in the world of *IoT* threats. Recuperado de: https://securelist.com/new-trends-in-the-world-of-*IoT*-threats/87991/

Trendmicro. (2019, 30 de mayo). The *IoT* Attack Surface: Threats and Security Solutions. Recuperado de: https://www.trendmicro.com/vinfo/fr/security/news/internet-of-things/the-*IoT*-attack-surface-threats-and-security-solutions

Massimi, Marcelo. (2023). *Murky Robot.* Protocolos: la comunicación para *IoT*. Recuperado de: https://www.murkyrobot.com/review/domotica/protocolos-comunicacion-*IoT*?utm_content=buffer31776&utm_medium=social&utm_source=*Twitter*.com&utm_campaign=buffer

Azure. (2023). Protocolos y tecnologías de *IoT*. Recuperado de: https://azure.*Microsoft*.com/es-es/solutions/*IoT*/*IoT*-technology-protocols/

Sigfox. (2023). *Sigfox* 0g technology by Unabiz. Recuperado de: https://www.*Sigfox*.com/

Sigfox. (2023). Tecnología *Sigfox*: Internet de las cosas. Recuperado de: http://productos-*IoT*.com/*Sigfox*-3/

Aprendiendo Arduino. (2018, 17 de noviembre). Protocolos *IoT* Capa Aplicación. Recuperado de: https://aprendiendoarduino.wordpress.com/2018/11/17/protocolos-*IoT*-capa-aplicacion/

Vidales, Mike. (2017, 16 de mayo). *Medium.* 802.15.4 Wireless for *Internet of Things* Developers. Recuperado de: https://blog.helium.com/802-15-4-wireless-for-internet-of-things-developers-1948fc313b2e

Samaniego, Juan F. (2022, 04 de agosto). *Orange.* ISO/IEC 30141 abrió el camino: así es la nueva familia de estándares para internet de las cosas. Recuperado de: https://blog.orange.es/innovacion/estandar-*IoT*/

NC Tech. (2023). ISO 30141. Recuperado de: https://nctech.com.mx/blog/*IoT*-industrial/iso-30141/

Software Testing Help. (2023, 24 de agosto). TOP 11 Best *Internet of Things* (*IoT*) Companies To Watch In 2023. Recuperado de: https://www.*software*testinghelp.com/top-*IoT*-companies/

Innowise. (2023). *IoT software* development company. Recuperado de: https://innowise-group.com/*IoT*-development-services/

Science Soft. (2023). *Internet of Things* (*IoT*) Solutions. Recuperado de: https://www.scnsoft.com/services/*IoT*/solutions

Vention. (2023). *IoT software* development. Recuperado de: https://www.itechart.com/solutions/*IoT*/

Oxagile. (2023). Portfolio. Recuperado de: https://www.oxagile.com/portfolio/domain/internet-of-things/

SUMATOSOFT. (2023). Projects we successfully developed. Recuperado de: https://sumatosoft.com/portfolio

IoT Global Network. (2023). *IoT* Companies. Recuperado de: https://www.*IoT*globalnetwork.com/companies/single/id/1780/r-style-lab

HQ *Software*. (2023). Partner With an *Internet of Things* Company. Recuperado de: https://hq*software*lab.com/solutions/internet-of-things/

PTC Digital Transforms Physical. (2023). Accelerate Success With ThingWorx *IIoT* Solutions Platform. Recuperado de: https://www.ptc.com/en/products/thingworx

CISCO. (2023). *Cisco* Industrial *IoT* Solutions. Recuperado de: https://www.*Cisco*.com/c/en/us/solutions/internet-of-things/overview.html

Arm Group. (2022, 26 de abril). Arm expands Total Solutions for *IoT* portfolio to continue delivering transformative innovation to ecosystem. Recuperado de:

https://www.arm.com/company/news/2022/04/arm-expands-total-solutions-for-*IoT*-portfolio

Amazon Web Services. (2023). AWS *IoT*. Recuperado de: https://aws.*Amazon*.com/*IoT*/

Azure *Microsoft*. (2023). *Internet of Things* (*IoT*) Develop robust *IoT* solutions—from device to *Cloud*—on an open and scalable platform. Recuperado de: https://azure.*Microsoft*.com/en-us/products/category/*IoT*

Huawei. (2023). Building a Better Connected World. Recuperado de: https://www.huawei.com/apac/huawei-ecoconnect/*IoT*.html

AT&T Business. (2023). *Internet of Things*. Turn big ideas into the next big thing. Recuperado de: https://www.business.att.com/portfolios/internet-of-things.html

Ericsson. (2023). Connect anything. Anywhere.. Recuperado de: https://www.ericsson.com/en/internet-of-things/platform

Telefónica Tech. (2023). Transformamos los datos en valor gracias a *IoT* & *Big Data*. Recuperado de: https://aiofthings.telefonicatech.com/

Vodafone. (2023). Can you intelligently connect your business with *IoT*?. Recuperado de: https://www.vodafone.com/business/*IoT*

Sierra Wireless. (2023). *IoT* Resources. Recuperado de: https://www.sierrawireless.com/resources/

Verizon. (2023). Transformative *IoT* solutions to advance any organization. Recuperado de: https://www.verizon.com/business/products/internet-of-things/

Philips Engineering Solutions. (2023). Connect your product to the digital world. Recuperado de: https://www.engineeringsolutions.philips.com/looking-expertise/electronic-systems-*IoT*/

IBM. (2023). *IoT* solutions. Recuperado de: https://www.*IBM*.com/*Cloud*/internet-of-things

IBM. (2023). *Internet of Things* architecture. Recuperado de: https://www.*IBM*.com/*Cloud*/architecture/architectures/*IoT*Architecture/solutions

Telefónica. (2022, 18 de enero). Telefónica se sitúa entre los tres líderes mundiales del mercado *IoT*, según Transforma Insights. Recuperado de: https://www.telefonica.com/es/sala-comunicacion/telefonica-se-situa-entre-los-tres-lideres-mundiales-del-mercado-*IoT*-segun-transforma-insights/

Chakray. (2023). *IOT*: 4 casos de éxito del internet de las cosas. Recuperado de: https://www.*Chakray*.com/es/*IoT*-4-casos-de-exito-del-internet-de-las-cosas/

CIC Consulting Informático. (2018, 21 de marzo). Industria 4.0: Nuevos retos para la Transformación Digital. Recuperado de: https://www.cic.es/industria-40-transformacion-digital/

European Commission, Directorate-General for Research and Innovation, Breque, M., De Nul, L., Petridis, A. (2021). Industry 5.0 : towards a sustainable, human-centric and resilient European industry, Publications Office. Recuperado de: https://data.europa.eu/doi/10.2777/308407

Frost & Sullivan. (2019). Industry 5.0—Bringing Empowered Humans Back to the Shop Floor. Recuperado de: https://www.frost.com/frost-perspectives/industry-5-0-bringing-empowered-humans-back-to-the-shop-floor/

Wikipedia. (2023). John von Neumann. Recuperado de: https://es.wikipedia.org/wiki/John_von_Neumann

Rolls Royce. (2023). Powering better performance and customer experience with the Internet of Engines. Recuperado de: https://www.rolls-royce.com/country-sites/sea/discover/2019/delivering-better-engine-performance-with-*IoT*.aspx

Kite-Powell, Jennifer (2015, 2 de marzo). *Forbes*. Johnnie Walker *Smart* Bottle Debuts At Mobile World Congress. Recuperado de: https://www.forbes.com/sites/jenniferhicks/2015/03/02/johnnie-walker-*Smart*-bottle-debuts-at-mobile-world-congress/?sh=6f00d4517ca1

The Food Tech (2015, 12 de marzo) Johnny Walker lanza botella inteligente. Recuperado de: https://thefoodtech.com/historico/johnny-walker-lanza-botella-inteligente/)

Saltzman, Ashley. (2017, 22 de enero). *LinkedIn*. Johnnie Walker launches the '*Smart*' bottle. Recuperado de: https://www.linkedin.com/pulse/johnnie-walker-launches-*Smart*-bottle-ashley-saltzman

British Gas. (2023). British Gas and Hive. Build your *Smart* home with Hive. Recuperado de: https://www.britishgas.co.uk/*Smart*-home/hive-partnership.html

Treviño, Myrla. (2023). *Telcel Empresas*. El *IoT* y 5 sectores que han crecido con él. Recuperado de: https://www.telcel.com/empresas/tendencias/notas/sectores-que-crecen-con-*IoT*.html

Diazgranados, Hernan. (2020, 23 de abril). *Kaspersky Daily*. El 61% de las empresas ya usan plataformas *IoT*. Recuperado de: https://latam.*Kaspersky*.com/blog/el-61-de-las-empresas-ya-usan-plataformas-*IoT*/18491/

Techno Apes. (2023). Reduce procesos manuales y aumenta la competitividad optimizando los procesos en tus operaciones. Recuperado de: https://www.technoapes.co/

Férnandez, Marina. (2022, 26 de noviembre). *Meteored.* La pelota del Mundial de Qatar 2022 usa inteligencia artificial. Recuperado de: https://www.meteored.com.ar/noticias/actualidad/la-pelota-del-mundial-de-qatar-2022-usa-inteligencia-artificial-imu-al-rihla-offside-lautaro-martinez-argentina-mexico.html

Filozof, Silvia. Grasso, Néstor. Viglianti, Rosana. Levit, Marcelo. Stanislavsky, Julieta. (2017, julio). *Ministerio de Justicia y Derechos Humanos Informe de auditoría. Unidad de Auditoría Interna (26/2017, 18).* Recuperado de:

https://www.argentina.gob.ar/sites/default/files/2017-26_-_dnrua_proteccion_de_datos_personales_0.pdf

Toledo, Rogelio. (2023). *Cibernos Grupo.* ¿Qué se determina en una auditoría de ciberseguridad? Recuperado de: https://www.grupocibernos.com/blog/que-se-determina-en-una-auditoria-de-ciberseguridad#:~:text=Una%20auditor%C3%ADa%20de%20ciberseguridad%20es%20un%20proceso%20sistem%C3%A1tico%20y%20met%C3%B3dico,(TIC)%20de%20una%20empresa.

Martín, Eliseo. (2023). *Cibernos Grupo.* La importancia de una auditoría de ciberseguridad en las empresas. Recuperado de: https://www.grupocibernos.com/blog/la-importancia-de-una-auditoria-de-ciberseguridad-en-las-empresas#:~:text=%C2%BFQu%C3%A9%20es%20una%20auditor%C3%ADa%20de,y%20de%20sus%20servicios%20inform%C3%A1ticos.

García, David. (2021, 23 de junio). *Bidaidea Cybersecurity & Intelligence.* ¿Qué es una Auditoría de Ciberseguridad? Recuperado de: https://ciberseguridadbidaidea.com/auditoria-de-ciberseguridad/

Academia Pirani. (2023). Auditoría de ciberseguridad: todo lo que necesitas saber. Recuperado de: https://www.piranirisk.com/es/academia/especiales/auditoria-de-ciberseguridad-empresas

Axentio. (2022, 15 de abril). Auditorías de ciberseguridad para empresas. Recuperado de: https://www.axentio.com/auditorias-de-ciberseguridad-para-empresas/

Guash Granell, Alejandro. (2022, 15 de noviembre). *IEBS.* Cómo hacer una auditoría de Ciberseguridad: consejos. Recuperado de: https://www.iebschool.com/blog/consejos-ciberseguridad-empresas-era-digital-business-tech-tecnologia/

Asesorae. (2023, 08 de agosto). La importancia de realizar una auditoría de ciberseguridad. Recuperado de: https://www.asesorae.com/blog/auditoria-ciberseguridad/

CSO Computer World España. (2015, 09 de octubre). ¿Cuáles son las certificaciones de seguridad para empresas más fiables? Recuperado de: https://cso.computerworld.es/ciberseguridad/cuales-son-las-certificaciones-de-seguridad-para-empresas-mas-fiables

Puffin Security. (2023). Auditoria de *Internet of Things* (*IoT*). Recuperado de: https://www.puffinsecurity.com/es/auditorias-de-ciberseguridad/internet-of-things

Tarlogic. (2023). Auditoría de seguridad *IoT*. Recuperado de: https://www.tarlogic.com/es/auditoria-seguridad-*IoT*/

Talsoft. (2023). Auditoría de seguridad en *IoT* (*Internet of Things*). Recuperado de: https://www.talsoft.com.ar/site/es/servicios/seguridad-informatica/auditoria-seguridad-*IoT*/

Sapsi. (2023). Auditoría *IoT*. Recuperado de: https://www.sapsi.org/service/auditorias-*IoT*/

Nethemba. (2023). Las redes y seguridad del sistema. Recuperado de: https://nethemba.com/es/servicios/las-redes-y-seguridad-del-sistema/auditoria-de-seguridad-*IoT*/

Cooke, Ian. (2019, 03 de octubre). *ISACA.* Auditoria basica TI: Auditando el internet de las cosas. Recuperado de: https://www.isaca.org/es-es/resources/isaca-journal/issues/2018/volume-5/is-audit-basics-auditing-the-*IoT*

Espinosa Garrido, Carmen B. Rosales Roldán, Luis. (2022). Marco de referencia de ciberseguridad para dispositivos de *IoT*
usando la tecnología de IDS. Recuperado de: https://www.iiis.org/CDs2022/CD2022Spring/papers/CB199FX.pdf

ISACA. (2023). CISA: Certified Information Systems Auditor. Recuperado de: https://isaca.org.ar/certificar/cisa/

ISC2. (2023). CISSP - Certified Information Systems Security Professional. Recuperado de: https://www.isc2.org/Certifications/CISSP

Editorial Esp. (2020, 02 de diciembre). ITIL vs. COBIT: ¿qué marco es más recomendable? Recuperado de: https://www.freshworks.com/freshservice/es/itil/itil-vs-cobit-que-marco-es-mas-recomendable-blog/

National Institute of Standards and Technology - NIST. (2023). National Institute of Standards and Technology. Recuperado de: https://www.nist.gov/

ISO. (2022). ISO/IEC 27001 Information security management systems. Recuperado de: https://www.iso.org/standard/27001

Mendoza, Miguel Ángel. (2023, 09 de febrero). *We live security - ESET.* ISO 27001:2022: ¿qué cambios introdujo el nuevo estándar de seguridad? Recuperado de: https://www.welivesecurity.com/la-es/2023/02/09/iso-270012022-cambios-nuevo-estandar-seguridad/

National Institute of Standards and Technology - NIST. (2018, 16 de abril). Framework for Improving Critical Infrastructure *Cybersecurity*. Recuperado de: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Mendoza, Miguel Ángel. (2022, 13 de diciembre). *We live security - ESET*. 8 pasos para la evaluación de riesgos de ciberseguridad de una empresa (parte I). Recuperado de: https://www.welivesecurity.com/la-es/2022/12/13/8-pasos-evaluacion-de-riesgos-1/

Mendoza, Miguel Ángel. (2022, 13 de diciembre). *We live security – ESET*. 8 pasos para la evaluación de riesgos de ciberseguridad de una empresa (parte II). Recuperado de: https://www.welivesecurity.com/la-es/2022/12/13/8-pasos-evaluacion-de-riesgos-2/

ProductPlan. (2023). Action Priority Matrix. Recuperado de: https://www.productplan.com/glossary/action-priority-matrix/

Center of Internet Security - CIS. (2023). The 18 CIS Critical Security Controls. Recuperado de: https://www.cisecurity.org/controls/cis-controls-list

GSMA. (2017, 26 de octubre). Lineamientos de Seguridad *IoT* para el Ecosistema de Servicios de *IoT*. Recuperado de: https://www.*GSMA*.com/*IoT*/wp-content/uploads/2018/05/CLP.12-v2.0_Spanish.pdf

GSMA. (2023). *IoT* Security Assessment. Recuperado de: https://www.*GSMA*.com/*IoT*/*IoT*-security-assessment/

Alibaba. (2023). *Smart*. Recuperado de: https://www.alibaba.com/trade/search?tab=all&searchText=*Smart*

Mercado Libre. (2023). *Smart*. Recuperado de: https://listado.mercadolibre.com.ar/*Smart*#D[A:*Smart*]

Ministério da Ciência, Tecnologia e Inovação - Brasil. (2020, 17 de diciembre). Lei da Internet das Coisas é sancionada pelo presidente da República. Recuperado de: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/noticias/2020/12/lei-da-internet-das-coisas-e-sancionada-pelo-presidente-da-republica

Dark Reading. (2020, 08 de diciembre). Trump Signs *IoT* Security Bill into Law. Recuperado de: https://www.darkreading.com/endpoint/trump-signs-*IoT*-security-bill-into-law

Azure *Microsoft*. (2023). Azure Digital Twins. Recuperado de: https://azure.*Microsoft*.com/es-es/products/digital-twins/

Robin, Kelly. (2020, 04 de diciembre). *USA Congress*. H.R.1668 - *IoT Cybersecurity* Improvement Act of 2020. Recuperado de: https://www.congress.gov/bill/116th-congress/house-bill/1668

Red Hat Customer Portal. (2023). 7.5. Guía de implementación de seguridad técnica. Recuperado de: https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/6/html/security_guide/sect-security_guide-federal_standards_and_regulations-security_technical_implementation_guide

The MITRE Corporation. (2023). ATT&CK Matrix for Enterprise. Recuperado de: https://attack.mitre.org/#

CSF Tools. (2023). ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources. Recuperado de: https://csf.tools/reference/nist-*Cybersecurity*-framework/v1-1/id/id-ra/id-ra-2/

Petrov, Michael. (2022, 14 de junio). *Digital Edge.* Mandatory Manual Reviews and Audits – NIST CSF Requirements. Recuperado de: https://knowledge.digitaledge.net/compliance/mandatory-manual-reviews-and-audits-nist-csf-requirements/

Jones, Edward. (2022, 22 de noviembre). *Kinsta.* Una guía completa de *Cloud* Security en 2023 (Riesgos, mejores prácticas, certificaciones). Recuperado de: https://kinsta.com/es/blog/seguridad-nube/

The MITRE Corporation. (2020, 02 de octubre). Gather Victim Host Information: *Firmware*. Recuperado de: https://attack.mitre.org/techniques/T1592/003/