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

MAESTRÍA EN ADMINISTRACIÓN DE EMPRESAS DE BASE TECNOLÓGICA

TRABAJO FINAL DE MAESTRÍA

Ciberseguridad y Conciencia Social del Internet de las Cosas

AUTOR: JEIVER ERNESTO RAMIREZ NARVAEZ

DIRECTOR: MIGUEL ÁNGEL BILELLO

[FEBRERO 2019]

Dedicatoria

A mi familia y maestros que acompañaron este hermoso sueño.

Agradecimientos

A quienes me alentaron en la ruta.

A mi esposa Nataly por su apoyo incondicional.

A mis padres que, desde la lejanía, dieron consejos y sabiduría para no desfallecer.

A los profesores Miguel, María y María Eugenia por el compromiso y la paciencia trabajando en conjunto, por sus observaciones y confianza en este proyecto.

Resumen

Este proyecto propone diseñar una propuesta de ciberseguridad para la Internet de las Cosas (IoT, por su sigla del inglés: Internet of Things), la cual contempla tanto el conocimiento de la población general acerca de los riesgos que puede entrañar el uso de la IoT, así como la gestión estratégica empresarial en materia de ciberseguridad para IoT.

Para lograr este propósito, se empieza por identificar el nivel de conocimiento y conciencia que tiene la población de la Ciudad Autónoma de Buenos Aires (CABA) y Gran Buenos Aires (GBA) sobre el uso y los riesgos que puede suponer ingresar al mundo de la Internet de las Cosas (IoT). Tomando como base la expectativa de que sea una de las tecnologías más disruptivas, que incidirá en el comportamiento humano en el futuro, es altamente probable que la vida cotidiana esté cada vez más unida a un ciberespacio donde habrá posibilidades de acceso a bienes y servicios, como también a desafíos de seguridad.

Considerando el enfoque de ciberseguridad, la conciencia sobre los riesgos y ciberataques en el IoT, será uno de los pilares para que los nuevos líderes gestionen estrategias con el fin de mitigarlos. La materialización de un incidente en este contexto podría ser de un gran temor y poner en riesgo empresas, naciones e incluso la vida de las personas.

Este trabajo contempla realizar un sondeo para conocer el nivel de conocimiento de la población general, a partir de la realización de una encuesta en línea compartida por WhatsApp. A su vez, se propone describir los posibles riesgos que acarrea el uso de la Internet de las Cosas (IoT) y proponer los ejes de trabajo para la seguridad de las personas, que se debieran contemplar dentro del entorno laboral y personal. El estudio se enfoca en los habitantes de CABA y GBA.

Palabras clave: Internet de las Cosas (IoT), Ciberespacio, Ciberseguridad, Riesgos.

Índice

Lista de tablas

Lista de figuras

Lista de gráficos

1. Introducción

La Maestría en Administración de Empresas de Base tecnológica MAE-BT, abre un espectro de conocimiento en relación con el avance de la tecnología. La importancia que tienen los nuevos líderes y cómo la tecnología en sus diferentes aspectos va a ser un diferenciador en la estrategia, operación y en el desarrollo de la conducta de las personas al interior de una empresa o en su vida personal. Es en ese punto que una función de la actividad gerencial debiera orientarse a que el uso de la tecnología brinde confianza y seguridad a sus usuarios. Que no sea vista como una amenaza que pueda causar daño social o personal, sino por el contrario, que su presencia y desarrollo colabore en la búsqueda de una mejor calidad de vida.

La Internet de las Cosas (IoT) identifica la conexión digital entre objetos. Es parte de una tecnología que se augura, cambiará (de hecho, ya la está cambiando) la forma de actuar y relacionarse entre seres humanos y objetos entre sí. Objetos y cosas, más allá de los que comúnmente se conocen en informática, como computadoras, tables, y teléfonos celulares, podrán estar en una interconexión digital Objetos cotidianos, podrán ser administrados y controlados de manera remota a través de la red, agilizando muchas de la tareas y actividades de empresas y personas. Considerando que estas nuevas formas de operar, por ejemplo, electrodomésticos a distancia, pueden constituirse en una práctica habitual en la sociedad, supone también un cambio en la manera de vivir y pensar, ya que es la sociedad la que realmente consumirá en gran medida esta tecnología.

Según Hans Vestberg, CEO de Ericsson: “Si una persona se conecta a la red, le cambia la vida. Pero si todas las cosas y objetos se conectan, es el mundo el que cambia” (Serna, 2016).

El panorama de la Internet de las Cosas es positivo. Por ejemplo, en términos de nuevos negocios, aplicaciones para medicina, ciudades inteligentes (Smartcities) invadidas de grandes datos (Big Data) y poder obtener en tiempo real información acerca del estado del tráfico, los niveles de CO2 en el aire, los datos meteorológicos o la temperatura, y también, tener la capacidad de controlar cosas y objetos de manera remota.

Mencionar el ciberespacio, según Sanchez (2015), es hablar hoy de un nuevo elemento, que se suma al agua, la tierra, el aire y el espacio. La existencia de este quinto elemento, al igual que el éter en la antigüedad, invisible y casi indetectable, ya es una realidad en un mundo virtual. Así como todos estos elementos han sido utilizados por las divisiones militares, en las confrontaciones, cabe el interrogante acerca de ¿qué esperar entonces de las interacciones en el ciberespacio?

El ciberespacio representa una infinidad de posibilidades de acción. Asimismo, y desafortunadamente, algunas están enfocadas a temáticas de espionaje, ya sea personal, económico e industrial entre instituciones y países. Conceptos como cibercrimen, ciberguerra o ciberterrorismo, están resonando en el mundo por eventos como la pornografía infantil, venta y compra de drogas, extorsión, intimidaciones a empresas y personas, entre otros. En el momento actual el uso de Internet alcanza al 85% de los países y alrededor del 55% de la población mundial (Miniwatts Marketing Group, 2018). En muchos lugares, sus habitantes conciben a Internet como una prolongación de su vida social y laboral. Esta amplia penetración de Internet, ante hechos de ciberdelincuencia podría desencadenar conflictos a partir de intereses políticos, financieros y sociales en donde la población general sería sin duda la más afectada. En general, la sociedad solo está relacionada con una parte de la red, una manifiesta y hasta superficial, si se considera que hay otra parte profunda, no accesible al público general y que podría designarse como “un lado oscuro”, donde la ciberdelincuencia suele operar.

La introducción de IoT lleva a reflexionar sobre el hecho que “las cosas” podrían ser los nuevos objetivos de ciberdelincuentes, ya que estas cosas son un todo conectado a un ciberespacio donde el impacto de daños físicos y humanos podría ser mucho más alto de lo imaginado. Como ejemplo podría mencionarse que no es lo mismo que un ciberdelincuente acceda a una computadora para sustraer información, a que acceda a un automóvil y tome control del mando. Por otro lado, los ciberataques parecen estar muy enfocados en afectar la privacidad e intimidad de las personas como a las infraestructuras críticas. Según Dinatale (2018) Argentina no está preparada para prevenir o responder a simples ciberataques, donde un incidente puede impactar muy seriamente en servicios básicos como electricidad, gas, comunicaciones y transporte, afectando a la población.

La gestión y liderazgo como Magister en Administración de Empresas de Base Tecnológica (MAE-BT) puede contribuir a emprender el desafío de promover al interior de las empresas de base tecnológica una cultura de ciberseguridad, que brinde confianza en el uso del IoT y que esta sea desplegada en beneficio de la población general. De esta manera se puede lograr mitigar los riesgos. Empresas de base tecnológica que están desarrollando esta tecnología, como Intel, son conscientes de los desafíos en temas de seguridad, pero más allá de una tecnología técnicamente confiable, la persona resulta ser el eslabón más débil de la cadena y es aquí donde se concentra la importancia y el interés por este tema.

La responsabilidad social de un gerente de empresas de base tecnológica va a ser crucial para que, desde la empresa y la academia, se despliegue la enseñanza cultural a través de un liderazgo ejemplar que logre direccionar el buen uso de la nueva tecnología.

Actualmente grandes empresas de vanguardia están basadas en tecnología, como Google, Facebook, Samsung, Apple y Microsoft, las cuales saben que el futuro se va a centrar en tecnología y, en especial, en las emergentes. La garantía frente a la seguridad de la sociedad por proteger datos personales, por ejemplo, se vuelve cada vez más relevante, y la confianza que brinden las compañías puede constituirse en un atributo diferencial de las marcas, que hará que los usuarios se sientan más cómodos y las elijan. Esto, sumado a políticas públicas que atiendan la educación sobre los riesgos de las IoT, se estima que podrá lograr mitigar mucho los ataques cibernéticos.

Nuevas posiciones gerenciales se han ido implementando al interior de las organizaciones, cargos estratégicos que empujan a las compañías en su desarrollo innovativo y de seguridad, por lo que dentro de las posiciones gerenciales podemos distinguir algunos como CEO, CIO, CISO, CDO, etc. Según el artículo "La era de los Cioto: llegan los nuevos gerentes de la inteligencia artificial", existe un nuevo panorama gerencial denominado CIOTO, Chief Internet Of Things Officer (gerente de Internet de las Cosas); lo interesante aquí no está en si puede ser considerada como una verdad, sino que el avance tecnológico va a generar nuevas oportunidades en las posiciones de alto nivel que integran una compañía (Campanario, 2017).

En este sentido, indagar sobre el conocimiento que la sociedad tiene acerca de ciberseguridad es fundamental para empezar desde ya a generar mayor seguridad. Además,

es indispensable que el sector empresarial y académico trabajen en forma coordinada, con el fin de concebir nuevos productos y servicios agregando conciencia social al uso del IoT. Entonces, este trabajo se basa en la importancia de conceptualizar el Internet, Internet de la Cosas, el ciberespacio y la ciberseguridad para poder abordar una investigación coherentemente y buscar de una manera lógica la conexión entre estos conceptos, integrando las normas y la regulación de Argentina sobre el tema.

2. Planteamiento del problema

La preocupación por el tema de la seguridad en el ciberespacio se basa en la proyección de la importancia que va adquiriendo la participación de Internet en la vida cotidiana.

La población de la Ciudad Autónoma de Buenos Aires y GBA tiene un uso masivo de Internet, según la Cámara Argentina de Internet (CABASE) (2017) entre enero de 2011 a julio de 2017, el tráfico cursado en la Red Nacional de Puntos Regionales de Interconexión de Internet aumentó 142 veces y, como se viene planteando, la IoT tiene grandes chances de proporcionar un cambio en la vida de las personas a través del desarrollo de servicios y aplicaciones inteligentes, que prometen aportar cada vez mayor confort para realizar actividades cotidianas. Hoy en día se pueden observar como actividades cada vez más comunes, realizar compras, hacer trámites o llevar a cabo estudios de manera virtual.

A medida que avanza el desarrollo y el acceso por parte de la población a herramientas digitales conectadas a Internet, como pueden ser los electrodomésticos inteligentes, se hace cada vez más frecuente controlar a distancia, programar y automatizar muchas de las actividades domésticas cotidianas. Por otro lado, estar interconectados supone una conexión abierta donde la privacidad y por consiguiente la seguridad se puede ver amenazada.

El desconocimiento por parte de las personas acerca de cómo protegerse en internet, las expone ante a la amenaza que supone todo un dispositivo constituido como ciberdelincuencia. La debilidad frente a estos ataques, por ejemplo, los basados en ingeniería social, que logran robar información y espiar sin que las personas lo sospechen, se vuelve alta en la medida que, si el todo se conecta, el todo puede ser objeto de ataques si una vulnerabilidad está expuesta.

Al incrementar la conectividad de objetos cotidianos muy probablemente se esté poniendo al descubierto los datos personales, qué hace, dónde trabaja, cuántos automóviles tiene una persona, entre otros datos que puedan ser de interés, debido a que al usar IoT podría estar siendo monitoreado todo el tiempo. Por lo tanto, es fundamental que tanto las empresas

como la población general valoren la necesidad de una sólida educación y conocimiento de los riesgos que la Internet de Cosas conlleva para los hogares, las empresas y la cuidad.

En base al problema planteado surgen las siguientes preguntas de investigación ¿Cuál es el nivel de conocimiento acerca de la Internet de las Cosas en la población general de la Ciudad Autónoma de Buenos Aires y GBA en la actualidad? ¿Se conocen los riesgos potenciales de estar conectados a Internet y de los impactos negativos que esto pueda generar tanto a nivel empresarial como personal? ¿Cuáles son estos riesgos? ¿Qué pueden hacer las empresas para posicionarse confiables en cuanto a la ciberseguridad?

A fin de responder a estas preguntas se plantean a continuación los objetivos que guían el presente estudio.

3. Objetivos

3.1. Objetivo general

Diseñar una propuesta de ciberseguridad y sensibilización para la Internet de las Cosas como política de marca dirigida a la organización interna de la empresa y a la población general, tomando como base el nivel de conocimiento que a 2018 tienen los habitantes de CABA y GBA sobre IoT.

3.2. Objetivos específicos

- Realizar un sondeo que permita identificar el nivel de conocimiento y consciencia acerca de la Internet de las Cosas y sus amenazas entre la población general de la Ciudad Autónoma de Buenos Aires y GBA.
- Describir los riesgos más relevantes a que se expone la población general al utilizar la Internet de las Cosas.
- Explorar la normativa vinculada a ciberseguridad en la Argentina.
- Elaborar un plan de acción a nivel organizacional para la concientización y protección de las personas, fundamentado en una perspectiva de Ciberseguridad.

4. Hipótesis

El presente estudio se desarrolla bajo la hipótesis de que la mayoría de la población de la Ciudad Autónoma de Buenos Aires y GBA no conoce el concepto de Internet de las Cosas, ni el riesgo potencial que la conexión de diferentes dispositivos de IoT a Internet supone para la seguridad personal y empresarial.

5. Marco teórico

Dado que la mirada central de esta investigación se basa en lo que la población de CABA y GBA conoce acerca del Internet de las Cosas y cómo esta tecnología tiene ciertos riesgos asociados, que, de no ser mitigados al interior de la sociedad, se contempla la posibilidad de que ocurran incidentes que perjudiquen o impacten en distintos órdenes, desde la privacidad de datos hasta la posibilidad de ocasionar daños a infraestructuras críticas.

Para poder abordar este proyecto de la mejor manera debemos recurrir a una serie de conceptos que nos ayudan a entender el Internet de las cosas y cómo éste forma parte de lo que se puede considerar una tecnología disruptiva, es decir, como aquella innovación que produce un cambio brusco y determinante. El ciberespacio y la ciberseguridad son escenarios en que se pone en evidencia comportamientos humanos como la competencia y la confrontación, lo cual genera nuevos desafíos y riesgos, ante los cuales se han empezado a elaborar teorías y desde el derecho se han comenzado a ordenar derechos y responsabilidades.

En ese sentido, la importancia de la protección de los datos personales, la privacidad de las personas, la protección de la información y la protección de las infraestructuras críticas, amparadas desde la perspectiva de la ciberseguridad, también son temas de importancia a desarrollar.

5.1. Internet

5.1.1. Origen

Hacia el año 1958 se crea la agencia ARPA (Advanced Research Projects Agency), parte del Departamento de Defensa de los Estados Unidos, la cual está encargada de desarrollar tecnología militar espacial. En su momento el presidente Dwight D. Eisenhower y el Secretario de Defensa, Neil H. McElroy, crearon dicha agencia con el fin de contrarrestar el avance soviético que por aquella época habían lanzado el Sputnik II, el cual incluía un pasajero, una perrita llamada Laika, sorprendiendo al mundo y sobre todo a los EE. UU. (Martínez, 2011).

En este mismo año nace la NASA (National Aeronautics Space Administration), agencia gubernamental encargada de los programas espaciales de los Estados Unidos, la cual

asumió los proyectos espaciales que manejaba ARPA, y que ésta última centrara toda su atención en los proyectos de comunicaciones y redes de computadoras (Martínez, 2011). Para el año 1962, ARPA creó un programa de investigación computacional bajo la dirección de John Licklider, un científico del MIT (Massachusetts Institute of Technology) (Facultat d'Informàtica de Barcelona (Universitat Politècnica de Catalunya), s.f.).

En 1969 ARPA realizaba la primera interconexión entre computadoras, la cual conectaba la Universidad Standford y la UCLA (University of California, Los Ángeles) bajo el nombre ARPANET. Hacia 1971 ARPANET tenía 23 puntos conectados, número que fue aumentando a través de los años.

Entre 1974 y 1982 se crearon otras redes entre las que se destacan:

Telenet (1974): Versión comercial de ARPANET.

Usenet (1979): Sistema abierto centrado en el e-mail y que aun funciona.

Bitnet (1981): Unía las universidades americanas usando sistemas IBM.

Eunet (1982): Unía Reino Unido, Escandinavia y Holanda.

En aquel momento el mundo de las redes era limitado, sin embargo, ARPANET seguía siendo el estándar. En 1982, ARPANET adoptó el protocolo TCP/IP (Protocolo de Control de Transmisión/Protocolo de Internet), protocolo que especifica estándares de comunicaciones entre sistemas (Facultat d'Informàtica de Barcelona (Universitat Politècnica de Catalunya), s.f.).

ARPANET deja de existir en 1990 dando paso a Internet y al programa de desarrollo la NSFNET que era operado por la NSF Fundación Nacional para la Ciencia (en inglés, National Science Foundation).

Tim Berners-Lee, científico británico de la Organización Europea para la Investigación Nuclear CERN, presenta oficialmente el World Wide Web en 1991 y consigue que se libere completamente el código y se comprometa a no cobrar por el uso de la tecnología (Rivero, 2002). El World Wide Web (WWW) es una red informática basada en hipertextos utilizando el HyperText Transfer Protocol (HTTP).

Después de 1993 la red Internet empezó a aumentar de manera exponencial en el número de usuarios. Los dos principales motivos de este rápido crecimiento fueron la apertura de Internet y la introducción del navegador web, (Martínez, 2011) programa que permite visualizar páginas web a través de la computadora o smartphone.

Los 90s fue la década en la que más evolucionó Internet. Yahoo! aparece en 1994, Internet Explorer nace gracias a Microsoft para el sistema operativo Windows 95, las creaciones del término weblog en 1997 y el nacimiento de Google en 1998, el cual provocó el crecimiento de usuarios en la red, cerrando así el siglo XX.

Para comienzos del siglo XXI nace Wikipedia (2001), enciclopedia colectiva de gran relevancia en la actualidad. En el 2003 se crea Skype, software que permite comunicaciones de texto, voz y vídeo sobre Internet, y aparece LinkedIn, la cual hoy en día es la mejor red social orientada a las empresas, a los negocios y al empleo. Al año siguiente, 2004, nace Facebook y Gmail (Galiana, 2017). En 2005 Internet ya había alcanzado los mil millones de usuarios mundiales y nace la plataforma de música y videos YouTube que actualmente es propiedad de Google, el cual en 2008 lanzaría su famoso navegador Chrome (marketingdirecto, 2013).

Durante los años siguientes la red incrementaría el número de usuarios y ya para el 2012, Internet alcanzaría los 2.4 billones de usuarios; además, las compras y los movimientos bancarios empiezan a ser una realidad a través de la www.

Actualmente, el planeta tiene más de 7 billones y medio de personas, de los cuales el 53% tiene acceso a Internet, esto quiere decir que son más de 4 billones de personas (Kemp, 2018).

5.1.2. Acceso a Internet

El aumento exponencial del uso de Internet ha sido consecuencia de la adaptabilidad de dispositivos como tabletas, teléfonos inteligentes, televisores, entre otros, logrando que el acceso a este servicio se realice no solamente a partir de una computadora con un browser instalado.

Más de la mitad de la población global tiene acceso a Internet, se estima que el gran crecimiento en cuanto al acceso a Internet y Redes Sociales está fuertemente vinculado a planes de datos y teléfonos inteligentes cada vez más asequibles (Gonzalez I., 2018). De acuerdo con Kemp (2018) más de 200 millones de personas adquirieron su primer dispositivo móvil en 2017, mientras dos tercios de los 7.6 billones de habitantes del planeta, ahora cuentan con un teléfono móvil.

En la Argentina el porcentaje de acceso a internet se encuentran por encima de la media global, que asciende al 73 por ciento (Kemp, 2018). Argentina es el tercer mercado móvil más grande de América Latina, con más de 62 millones de conexiones móviles (Jaimovich, 2018).

Las redes sociales tienen un valor significativo ya que tres cuartas partes de la población con acceso a internet son usuarios activos de redes sociales, esto es 3.2 billones, que representa 42% de la población mundial, y estas cifras siguen en aumento (Kemp, 2018).

Los nuevos hábitos y tendencias hacen que la cantidad de tiempo que se pasa conectado a Internet también aumente. Las personas están orientadas cada vez más a la hiperconectividad y al multitasking. Redes sociales, streaming de video, mensajería instantánea y juegos online, entre otras actividades, son protagonistas del consumo del usuario en Internet, no sólo a través de la computadora sino también mediante otros dispositivos, por ejemplo, más de 32 millones de argentinos acceden a Internet a través del celular.

5.2. Internet de las cosas

5.2.1. Una tecnología disruptiva

La expresión "Internet de las cosas" (IoT, por sus siglas en inglés), nace en el Instituto de Tecnología de Massachusetts (MIT), en 2009 el profesor Kevin Ashton usa este término (IoT) de manera pública en el RFID journal.

> Si tuviésemos ordenadores que fuesen capaces de saber todo lo que pudiese saberse de cualquier cosa –usando datos recolectados sin intervención humana– seríamos capaces de hacer seguimiento detallado de todo, y poder reducir de forma importante

> los costes y malos usos. Sabríamos cuando las cosas necesitan ser reparadas, cambiadas o recuperadas, incluso si están frescas o pasadas de fecha. El **Internet de las Cosas** tiene el potencial de cambiar el mundo como ya lo hizo Internet. O incluso más (Cendón, 2017).

El Internet de las Cosas va mucho más allá, las cosas que nos rodean, desde máquinas industriales, autos, relojes, entre otros. Ya no serán simplemente productos, sino serán puntos de conexión entre el mundo físico y el digital. Se destacan las nuevas habilidades innovadoras de los objetos, como por ejemplo un reloj por medio del cual se vigila el ritmo cardiaco y se da aviso si hay algún cambio brusco que implique atención, y cómo los datos serán factores cada vez más importantes en las prácticas humanas. Desde este punto de vista la medicina a través de la tecnología wearable, artefactos que se llevan en el cuerpo, bien sobre él o bien dentro de él, y relojes inteligentes, lograrán la mejora del estado y deficiencias físicas de los seres humanos. En un futuro, los algoritmos podrán determinar y tomar acciones sobre alertas a los usuarios, a los familiares e incluso a sus médicos sobre tratamientos y prevención de enfermedades (Vazhnov, 2016).

Una de las aplicaciones clave de IoT es en la lucha contra el cambio climático y sus efectos. Los países en desarrollo pueden usar sensores inteligentes para monitorear las condiciones del suelo y guía de sistemas autónomos de riego. También los sistemas inteligentes pueden sincronizar el tráfico en ciudades, ahorrando así tiempo de viaje y consumo de combustible. Incluso, los países pueden desplegar redes inteligentes que utilizan los sistemas de posicionamiento global (GPS), la información del sensor de las cámaras de monitoreo y otras fuentes para detectar el movimiento de la población y facilitar la congestión, y re enrutar el tráfico, en caso de eventos especiales y emergencias (World Development Report, 2016).

El Internet de las Cosas (IoT) es una sólida red de dispositivos integrados con electrónica, software y sensores que permiten intercambiar y analizar datos. Poco a poco este concepto ha tenido un crecimiento exponencial y se está desplegando en todo el mundo como una tecnología que será la que genere un cambio disruptivo en la sociedad. El aumento de la velocidad y capacidad de la conexión de Internet ha permitido hoy en día que objetos y cosas se puedan conectar a gran escala.

Cisco, empresa dedicada a la industria de las tecnologías de la información y la comunicación, y que ha venido realizando algunas investigaciones referentes a IoT, ha estimado que esta tecnología nació entre el 2008 y el 2009, y que para el 2020, 50 billones de dispositivos estarán conectados a Internet (Evans, 2011).

Esto está siendo posible, en cierta medida, gracias a que actualmente los costos de los dispositivos son más asequibles para las personas y las organizaciones, al mismo tiempo el desarrollo veloz de la electrónica está permitiendo crear componentes más pequeños con muchas más capacidades tanto de almacenamiento como de velocidad. La ley de Moore, desarrollada por el cofundador de Intel, Gordon Moore, plantea que aproximadamente cada dos años se duplica el número de transistores en un microprocesador, en donde su tamaño será clave para que los dispositivos se vuelvan más baratos y más pequeños, usen menos energía y sean más potentes. Lo más interesante de la predicción de Moore para nuestro estudio es una frase que hace parte de su artículo en la revista Electronics, en 1965:

> Las ventajas de la integración brindarán una proliferación de electrónica, insertando esta ciencia en muchas áreas nuevas. Los circuitos integrados nos llevarán a las maravillas como computadores domésticos para los autos y dispositivos de comunicación personal". De esto se puede desprender el presagio del auto autónomo y de los teléfonos inteligentes (Vazhnov, 2016).

Tomando lo anterior, se puede considerar que esta ley también aplica al crecimiento que ha tenido Internet. En enero de 2009 un equipo de investigadores en China estudió los datos de enrutamiento, proceso para determinar la ruta óptima que debe seguir un paquete de datos de Internet, en intervalos de seis meses, de diciembre de 2001 a diciembre de 2006. Sus hallazgos mostraron que Internet duplica su tamaño cada 5.32 años (Evans, 2011).

Desde el 2016 se ha venido desarrollando "The Gartner Hype Cycle for Emerging Technologies", en donde IoT se mueve rápidamente como tecnología emergente para los próximos 10 años (Panetta, 2018).

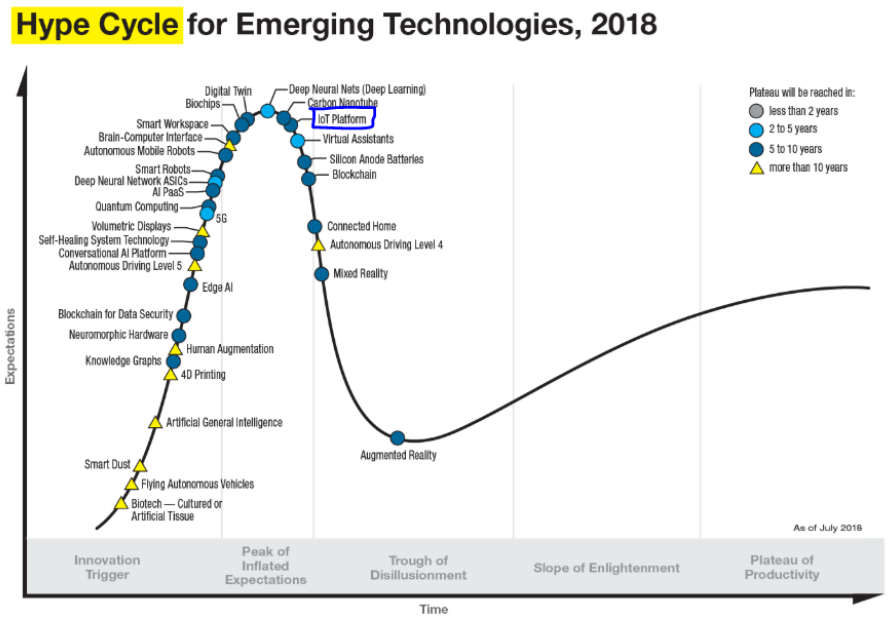

Figura 1. Hype Cycle for Emerging Technologies, 2018. Gartnet (August 2018). Recuperado de https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/

Otro punto clave de esta tecnología disruptiva está en la economía y de cómo las nuevas generaciones van a tener otros focos a nivel financiero, pues ya no será tan importante comprar automóviles o adquirir bienes. La entrada de Google, Uber y Airbnb, agregando la globalización, va a generar que estos servicios se utilicen masivamente alrededor del mundo, luego las plataformas digitales serán claves sobre el impacto de IoT, en donde cualquier dispositivo puede ser una plataforma de productos y servicios (Vazhnov, 2016). Esto nos lleva a conectar con las llamadas ciudades inteligentes, control del tráfico, medio ambiente y energía.

5.2.2. IoT red de redes

Los productos de IoT se pueden clasificar en cinco grandes categorías: Dispositivos wearable, casas inteligentes, ciudades inteligentes, sensores de medio ambiente y aplicaciones de negocios (World Development Report, 2016), en donde se componen de una colección suelta de redes, las cuales son diseñadas específicamente. Por ejemplo, los automóviles tienen múltiples redes para controlar la función del motor, características de seguridad, sistemas de comunicaciones, etc. A medida que IoT siga evolucionando, estas redes, y muchas otras, se conectarán entre sí con capacidades de seguridad, análisis y gestión (Evans, 2011).

Los dispositivos de IoT tienen una estructura inteligente basada en tres aspectos: sensores, procesamiento y conexión, por lo que sobre este punto habría que mencionar cinco tecnologías (Lee & Lee, 2015) esenciales para IoT:

Identificación por radiofrecuencia (RFID). Permite la identificación automática y la captura de datos mediante ondas de radio, una etiqueta y un lector.

Redes de sensores inalámbricos (WSN). Consiste en dispositivos autónomos distribuidos espacialmente y equipados con sensores para monitorear las condiciones físicas o ambientales y pueden cooperar con los sistemas RFID para rastrear mejor el estado de las cosas, como su ubicación, temperatura y movimientos.

Middleware. Es una capa de software interpuesta entre aplicaciones de software para facilitar la comunicación y entrada/salida de los desarrolladores de software.

Computación en la nube (cloud computing). Es un modelo para el acceso a un conjunto compartido de recursos configurables (por ejemplo, computadoras, redes, servidores, almacenamiento, aplicaciones, servicios, software) que se pueden aprovisionar como Infraestructura como un Servicio (IaaS), Plataforma como un servicio (PaaS) o Software como un Servicio (SaaS).

Aplicaciones IoT. IoT facilita el desarrollo de innumerables aplicaciones para esta tecnología, orientadas a la industria y específicas del usuario.

Estas tecnologías serán fundamentales para almacenamiento, procesamiento de datos y acceso a una interfaz para configurar y administrar el producto IoT, porque algunos de estos no cuentan con un disco o pantalla táctil y algunos componentes como una batería y CPU, pueden conllevar a un gasto energético mayor (Vazhnov, 2016).

El término de plataforma Digital cobra un valor muy importante para IoT, siendo esta un lugar de interacción e intercambio de valor entre usuarios de una red (Vazhnov, 2016). Muchas aplicaciones (Apps) se han desarrollado con base en plataformas digitales y de esta manera se ofrecen diferentes clases de servicios transformando una industria en otra. Por ejemplo, Google en la publicidad, Airbnb en alquileres y Uber en el negocio de Taxis. Según Vazhnov (2016) hay tres razones claves y relevantes con la llegada de productos basados en IoT: Superan los límites de espacio y tiempo, generan externalidades de red y ganan ventaja competitiva a través de data y algoritmos.

5.2.3. Tecnología móvil, aplicaciones y APIs

En un comienzo el acceso a una computadora era limitado para el común de las personas por su elevado costo y sus dimensiones, como aquellas grandes computadoras (Mainframes) que ocupaban un gran espacio. Hoy en día el uso de computadoras móviles es mayor que el de las computadoras de escritorio. Internet se vuelve un servicio público fundamental para la sociedad, y las nuevas culturas empresariales se forman con base en el concepto de movilidad y trabajo en casa (Home office). El uso de los teléfonos móviles se vuelve cada vez más relevante ya que el acceso a dispositivos de IoT a partir de aplicaciones para la administración remota, hace que el celular sea vuelva el punto de gestión y control.

El desarrollo de la telefonía móvil data desde la década de los 70s y su evolución se ha dado a través de sus generaciones. La primera generación (1G) consistió en celulares análogos que sería reemplazada por teléfonos digitales para la 2G, comenzando en Finlandia en 1991. La tercera generación 3G de esta tecnología ya proveía un acceso a Internet más rápido y fue lanzada para la copa del mundo FIFA 2002 en Corea. Hacia mediados del 2015 habían alrededor de 2.33 billones de suscriptores para 3G y 757 millones de suscriptores para la 4G, mejorando considerablemente la optimización y uso de datos (World Development Report, 2016).

La generación (5G) es la siguiente generación y sobre esta, muy seguramente, la actividad de IoT estará dada en gran medida. Se estima que esta generación sobrepasará la velocidad de datos de 100 gigabit por segundo (Gbits/s) que brinda 4G. Investigadores del Centro de Innovación 5G de la Universidad de Surrey (5GIC) lograron un terabit por segundo (Tbit / s) durante sus pruebas de velocidad (World Development Report, 2016). Este avance de la Tecnología móvil, aumentando las capacidades año tras año, y su combinación con Internet se vuelve necesario para la gestión de dispositivos de IoT.

Las **APIs** (Application Programming Interfaces) permiten la conectividad entre dispositivos y su control, luego las APIs serán parte fundamental en los nuevos productos inteligentes que, a diferencia de los tradicionales, serán capaces de tomar sus propias decisiones y variar comportamiento en función de las circunstancias. Al usar APIs de distintas empresas se puede construir nuevas propuestas de valor que integren sensores, análisis de datos, procesos en el mundo físico, incluyan diferentes industrias y migren a que los productos se vuelvan servicios. Las APIs de IoT son un punto de contacto entre un

dispositivo y otro o entre el dispositivo y una aplicación en la nube, por lo que el concepto de API se volverá parte del idioma cotidiano (Vazhnov, 2016).

Hoy en día existen millones de aplicaciones en donde Apple y Android tienen gran variedad y cubren distintas necesidades como la aplicación Google maps, que permite en tiempo real conocer tu ubicación y poder compartirla a través de WhatsApp. Desde hace varios años las empresas han estado cambiando sus modelos de negocio, que en lugar de vender productos pasan a vender servicios. Este cambio es una característica general de un mundo digital. Netflix, Spotify y Pandora se venden como servicios de subscripciones continuas y simbólicas entre clientes y vendedores.

La posibilidad de dispositivos conectados a Internet a través de apps va a ser gigante, imaginar, por ejemplo, las miles de aplicaciones para el cuidado de la salud y que mediante un reloj se pueda detectar una caída y comprobar si una persona logró levantarse sola, es solo uno de los tantos beneficios por los que la tecnología wearable se volvería realmente masiva (Vazhnov, 2016).

5.3.Ciberespacio

El ciberespacio se enmarca frente a las disputas y confrontaciones militares que, a lo largo de la historia, han estado presentes en nuestro mundo. El Department of Defense Dictionary of Military and Associated (2016) define el ciberespacio como:

> Un dominio Global dentro del entorno de la información, compuesto por una infraestructura de redes de tecnología de la información interdependientes, que incluye Internet, las redes de telecomunicaciones, los sistemas de Información y los controladores y procesadores integrados junto a sus usuarios y operadores.

Luchas por territorios, por poder o por comida se han realizado desde diferentes ambientes. En la cumbre de la OTAN en Varsovia 2016, el ciberespacio se reconoce como un nuevo dominio legítimo de las operaciones, al lado de los de tierra, mar y aire (Gonzalez J.M., 2016). En términos geopolíticos, un ataque cibernético (Ciberataque) es ahora tan accionable como un ataque naval. En entornos industriales y comerciales, los delincuentes cibernéticos se consideran con frecuencia como una amenaza principal y probablemente una

amenaza permanente (Zulick, 2018). Incluso, se consideraría un ciberataque a una nación miembro como si afectara a los aliados de la organización.

Como lo describe el editor de la revista Wired, Ben Hammersley, el ciberespacio se está convirtiendo en "la plataforma dominante para la vida en el siglo 21" (Singer & Friedman, 2013).

5.3.1. Un quinto domino (elemento)

El primer dominio es la **tierra,** donde aquel que dominara el territorio, imponía su ley. Más tarde, con el desarrollo de los primeros barcos, el **agua** formó parte también de estas luchas. Muchos años después y con la invención de los aviones, el **aire** entraría a ser el tercer elemento que se utilizaría en los campos de batalla. Durante el siglo pasado las guerras mundiales se desarrollaron en estos dominios y las grandes naciones aún invierten millones de dólares con el fin de tener el mejor armamento tanto en tierra, agua y aire (Sanchez, 2015).

El desarrollo de la tecnología por conquistar el **espacio** toma relevancia también como un cuarto dominio, si bien hoy en día se considera insignificante la conquista de naciones por ese entorno, toma importancia en el ámbito de fuerzas militares y de comunicaciones.

La tecnología y su rápido crecimiento desde la invención de la Internet, ha logrado que se desarrolle **"El ciberespacio"**, convirtiéndose este en el quinto dominio. Dicho dominio es de gran importancia y se debe considerar que, a través de un mundo virtual, también es vulnerable.

5.3.2. Estructura del Ciberespacio

Según Libicki (2009) la estructura del ciberespacio está divida en tres capas y cada una de estas tiene sus propias vulnerabilidades y amenazas externas e internas ante objetos de ataque:

- ***La capa semántica.*** Tiene la información que contiene la máquina.

- ***La capa Sintáctica.*** Contiene las instrucciones que los diseñadores y usuarios dan a la máquina y los protocolos a través de los cuales las máquinas interactúan entre sí.
- ***La capa física.*** Todos los sistemas de información descansan en una capa física que consiste en máquinas y cables.

5.3.3. ¿Qué tan seguro es el ciberespacio? – Espionaje

Las estrategias de supervivencia, la posesión de la tierra, la formación de grupos, la necesidad de expandirse y en ese sentido, conquistar nuevos territorios, ha sido un ejercicio permanente de conquista y también se proyecta en el ciberespacio.

Si en el ciberespacio puede estar potencialmente disponible información sensible de la población, las empresas y los gobiernos, la conquista del ciberespacio se revela como de alta importancia y supone un gran atractivo para intereses diversos.

La importancia de la información como uno de los activos intangibles más significativos y estratégicos para personas y empresas, en donde la fuga y perdida los puede afectar de manera relevante, nos orienta a tomar la información como un tipo de poder, el que French y Raven, plantearon como poder informativo. Este tipo de poder se basa en la capacidad del que lo ejerce de obtener y administrar información que puede resultar de utilidad (Psicología en el Bolsillo, 2015).

Volviendo al ciberespacio, han existido tres acontecimientos claves que han marcado pautas para confirmar que quien domina la información y la sociedad interconectada, controla el mundo. En primer lugar, el acontecimiento de los papeles del pentágono (70s), en donde información clasificada del Gobierno de los Estados Unidos fue revelada en torno a la guerra de Vietnam; el caso de WikiLeaks (2010) en que se publicó información de la guerra de Irak, y el caso Snowden (2013), que consistió en que la NSA y la CIA, a través de un proyecto denominado Prism, accedió e interceptó datos personales de millones de usuarios, incluyendo personalidades. Estos acontecimientos se justificaron, al igual que Echelon (programa de espionaje Global ideado por USA), por la lucha antiterrorista, aunque para algunos críticos, el verdadero objetivo es la inteligencia política, diplomática, comercial y económica contra cualquier país (Sánchez, 2015).

Por lo anteriormente expuesto, el espionaje es la actividad más frecuente dentro del ciberespacio, ya sea económico, industrial y tecnológico. El espionaje resulta ser una constante en el intento por conocer información de gobierno, de empresas y de personas que den ventajas de unos sobre los otros. Pocas organizaciones han sido conscientes del valor de la seguridad y no han creado una cultura preventiva que contrarreste algún tipo de riesgo. Existen empresas de espionaje y software de vigilancia, incluso las multinacionales de tecnología, que han ayudado, en cierta medida, ya sea por patriotismo o por otro motivo, en las tareas de espionaje cibernético. Sin duda, estos acontecimientos han supuesto un cambio disruptivo en la manera de entender la seguridad tecnológica y digital.

5.3.4. Ciberataque

Como se ha venido mencionando, IoT interconecta el mundo físico con el mundo virtual, incrementando riesgos en su uso, pues no sería lo mismo hackear una computadora o un sitio web, que a un automóvil o incluso a un marcapasos en el cuerpo de una persona.

En 2015 la agencia de seguridad vial llamó y ordenó a la automotriz Fiat Chrysler, fabricante del carro Jeep, el retiro de 1.4 millones de vehículos que eran afectados por una vulnerabilidad. Esta vulnerabilidad fue demostrada por medio de la revista Wired en su nota “Hackers Remotely Kill a Jeep on the Highway—With Me in It” (Greenberg, 2015) donde los expertos informáticos Charlie Miller y Chris Valasek, logran explotar (Hackear) a través de una conexión inalámbrica (Wireless) el vehículo, conectándose a más de 10 kilómetros, prácticamente toman el control remoto de casi todo el Jeep, el aire acondicionado, limpia parabrisas e incluso apagan el motor. Expertos en Seguridad Informática dieron su opinión para que los vehículos del futuro tengan que incorporar interruptores de emergencia que les asegure ante una eventualidad.

Esa misma revista menciona en otro artículo (Newman, 2018) que las vulnerabilidades en IoT estarán más disponibles para los hackers, ya que los fabricantes de estos productos tienden a parchear las vulnerabilidades lentamente, lo que incrementa el riesgo de ser atacados de manera eficaz.

Un ciberataque es diferente de un ataque tradicional, este incluye daños físicos y lógicos utilizando herramientas digitales como computadoras y smartphones, y crece paralela y exponencialmente a Internet e IoT, recordando la ley de Moore tratada previamente. Según Singer y Friedman (2013) en el ciberespacio un ataque puede, literalmente, moverse a la velocidad de la luz y no se detiene ante fronteras políticas o físicas. En lugar de causar daño físico directamente, un ciberataque siempre comienza con un objetivo informático, que se puede reproducir después en un daño físico.

Dentro de los ciberataques encontramos diferentes tipos y estos vienen dados de acuerdo con los principios que trataremos en el capítulo de Ciberseguridad de este documento, siendo estos: ataques a la disponibilidad, confidencialidad e integridad. Un elemento diferenciador es que un ciberataque es mucho más difícil de identificar, muchas veces se cree que viene de un país, se detecta mediante sistemas de detección de Intrusos (IPS), pero es muy complicado asegurar un responsable, de la misma manera que predecir su efecto (Sanchez, 2015).

5.3.5. Red profunda (Deepweb)

Dentro del ciberespacio se pueden desarrollar tres efectos adversos, que en economía se podrían clasificar como externalidades negativas, desarrollándose en el mercado que ofrece IoT. Siendo estos el “Cibercrimen” enfocado en utilizar herramientas digitales para cometer alguna actividad ilegal, el “Ciberterrorismo” potencial amenaza de destrucción contra Infraestructuras críticas mediante el uso de la tecnología y la “Ciberguerra” que se desarrolla dentro del quinto elemento (Sanchez, 2015).

Muchos de los grupos criminales que operan dentro del ciberespacio son los considerados hackivistas (acrónimo de Hacker y Activista), los cuales actúan sobre la capa oscura del Internet que se denomina “Darknet”. Este lado oscuro está escondido para los usuarios, es decir, la población general que no es experta en tecnología digital y que solo puede ver una pequeña parte del gran océano de Internet. Es como percibir solamente la punta de un iceberg, en donde el 96% se encuentra por debajo de ese océano: comunicaciones cifradas P2P y acceso a información a la que no se puede llegar a través de los motores de búsqueda (Google o Bing).

Darknet fue presentado por cuatro ingenieros de Microsoft en 2002 durante una conferencia de seguridad en Washington, en donde se hablada de la administración del derecho digital y que a medida que la tecnología se hace más sofisticada, resulta más fácil compartir contenidos en Internet (Sanchez, 2015). De hecho, el Darknet se usa muchas veces para delitos como la pornografía infantil, venta y compra de drogas, extorsión, lavado de activos, intimidaciones a empresas y personas, entre otros.

Figura 2. Los niveles de la red profunda. El Heraldo (2013). Recuperado de https://www.elheraldo.co/infografias/los-niveles-de-la-internet-profunda-134361

Facebook, la red social más grande del Internet ha tenido varios acontecimientos que han revelado que cuando existen fallas de seguridad y vulnerabilidades, se compromete de manera directa la privacidad. En Septiembre de 2018 Facebook fue hackeado por ciberdelincuentes, como consecuencia se expusieron datos personales de más de 50 millones

de usuarios y hubo venta de inicios de sesión (usuarios y contraseñas) a bajo costo en la Darknet, lo cual posiblemente está vinculado con el hackeo anterior (Pepper, 2018). También está el caso de la empresa Cambridge Analytica, dedicada al análisis y minería de datos, la cual utilizó datos que procedían de Facebook para sus actividades comerciales, vulnerando así los términos de uso. Esto fue posible gracias a la falta de control de la API (Gonzalez M., 2018).

Lo anterior lleva a pensar: ¿Qué tan segura es Internet? ¿Cómo será el mundo si todo está conectado? Esta es la otra cara de la moneda que no se debe dejar de lado en el desarrollo de las nuevas tecnologías y sobre la cual las grandes empresas y gobiernos deben empezar a reflexionar.

5.4.Ciberseguridad

A partir del 11 de septiembre de 2001, el giro no solo de los Estados Unidos sino del mundo, cambia las políticas de seguridad. Entre el 2016 y el 2017, los hackeos detectados y procesados en la Argentina aumentaron un 700% (Dinatale, 2018). El 97% de las compañías del Fortune 500, han sido hackeadas, siendo que el 3% de estas probablemente ni se han enterado (Singer & Friedman, 2013). Es fundamental que las empresas y el gobierno creen buenas prácticas con relación al ciberespacio, que los seres humanos logremos entender los riesgos asociados y a dónde podemos acudir en caso de un ciberataque, de esta manera podemos establecer la prevención y la reacción como conceptos de gran valor para la defensa y el sostenimiento del ciberespacio útil y confiable.

El desafío de ciberseguridad consiste en tener en cuenta que cualquier tecnología y en especial la del objeto de estudio, IoT, implica un conjunto de beneficios y perjuicios, y es importante mantener una perspectiva equilibrada que tenga en cuenta ambos aspectos (Vazhnov, 2016). Sin duda la hiperconectividad hace la vida más fácil; sin embargo, en cuanto más dependiente de la tecnología se sea, al mismo tiempo se incrementan riesgos. Según Sanchez (2015) al aumentar los niveles de información y la conectividad de los objetos, se está colocando o exponiendo información muy valiosa de cada individuo: “Todo lo que hacemos en nuestras casas, trabajos, coches, escuelas, comunidades y tiempo libre será susceptible de ser monitoreado por la tecnología” (p. 20).

5.4.1. Objetivos de la Ciberseguridad

Ciberseguridad hace parte del campo de la Seguridad de la Información y está más allá de la seguridad de Internet, redes y aplicaciones. Es definida como la protección de los activos de información, al abordar las amenazas a la información procesada, almacenada y transportada por sistemas de información interconectados (ISACA, 2017), teniendo en cuenta su relación con aquellas amenazas que están direccionadas al ciberespacio.

Los ciberataques buscan afectar a lo que en Seguridad de la Información se denomina los pilares o triada de seguridad.

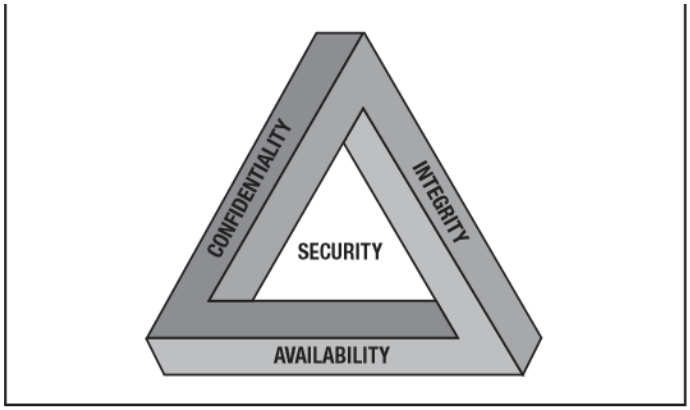

Figura 3. Principios o TRIADA de Seguridad de la Información. ISACA (2017).

***Disponibilidad*.** Está basada en asegurar el acceso y uso oportuno y confiable de la información y los sistemas. Los ataques a la disponibilidad tratan de impedir el acceso a una red y a su información, ya sea hackeándola o sobrecargándola muchas veces por ataques de negación de servicio (**DDoS** por sus siglas en inglés). En 2017 la disponibilidad de dispositivos de IoT ha sido afectada considerablemente, se ha interrumpido su servicio, comprometiendo gran cantidad de dispositivos como routers domésticos, cámaras web y receptores de televisión digital. Los ataques DDoS hacia dispositivos IoT son muy difíciles de contrarrestar porque, esencialmente, los fabricantes prestan poca atención a la seguridad de tales dispositivos y los usuarios no suelen cambiar las contraseñas predeterminadas.

La pérdida de disponibilidad puede tener consecuencias como la pérdida de funcionalidad y efectividad operativa, la pérdida de tiempo productivo, multas de los reguladores o una demanda, interferencia con los objetivos de la empresa y pérdida de cumplimiento (ISACA, 2017) (Sanchez, 2015).

***Confidencialidad*.** Es la protección de la información contra el acceso o la divulgación no autorizada. Los ataques a la confidencialidad buscan penetrar ciertas redes de IoT para extraer información privada, como pueden ser los datos personales. Un ataque muy común es el de phishing, que se ha utilizado mucho en fraude financiero, en donde los delincuentes obtienen su información de autenticación (usuario y contraseña), engañando a la víctima haciéndose pasar por una entidad financiera.

La pérdida de confidencialidad puede tener como consecuencias la divulgación de información protegida por las leyes de privacidad, la pérdida de confianza, la pérdida de ventaja competitiva, acciones legales contra la empresa, interferencia con la seguridad nacional y pérdida de cumplimiento (ISACA, 2017) (Sanchez, 2015).

Integridad. Es la protección de la información de modificaciones no autorizadas. Los ataques contra la integridad buscan modificar la información dejándola inexacta. Cualquier violación de la integridad es significativa porque puede ser el primer paso para un ataque exitoso contra la disponibilidad o la confidencialidad. Muchas veces este tipo de ataque que afecta la integridad corresponde a actos de protesta, vandalismo o sabotaje.

La pérdida de integridad puede tener consecuencias como inexactitud, decisiones erróneas, fraude, fallo del sistema y pérdida de cumplimiento.

Según Sanchez (2015) Internet hará posible el control remoto de cualquier objeto sobre la tierra. Expertos calculan que la Internet de las Cosas tendrá un impacto sobre la vida de las personas entre cinco y diez veces mayor que el de la propia Internet. Cuando IoT se desarrolle plenamente, la distinción del mundo virtual y mundo físico se habrá evaporado, los dos mundos serán uno en forma indisoluble.

El avance tecnológico y la globalización generan un escenario muy competitivo. En el Silicon Valley, sede de muchas compañías emergentes y globales de tecnología, jóvenes sueñan con sacar adelante sus proyectos innovadores y alcanzar el éxito que ha tenido Apple, Facebook y Google (Sanchez, 2015). Por otro lado, junto al desarrollo de la Internet de las cosas y las tendencias de movilidad y conectividad, se presentan una serie de retos, así como nuevos ataques en continuo crecimiento a través de bandas delincuenciales. Los gerentes deben estar informados y ser flexibles para identificar y

gestionar nuevas amenazas potenciales, como los nuevos métodos de cibercrimen y las amenazas persistentes avanzadas (APT del inglés Advanced Persistent Threat), de manera efectiva.

Las APTs requieren de la experiencia, el tiempo, la paciencia y los recursos significativos que le permiten al atacante crear oportunidades para lograr sus objetivos, utilizando múltiples vectores de ataque. Según el Instituto Nacional de Normas y Tecnología de los EE.UU (NIST, 2012) la definición de APT es:

> La amenaza persistente avanzada es un **ataque dirigido con niveles sofisticados** de pericia y recursos que le permiten a los atacantes por medio del uso de **múltiples vectores de ataque** (malware, vulnerabilidades, Ingeniería Social, entre otras), generar oportunidades para alcanzar sus objetivos, que habitualmente son establecer y extender su **posicionamiento** dentro de la infraestructura de tecnología de la información de organizaciones con el objetivo de **filtrar información** hacia el exterior continuamente o minar o impedir aspectos importantes de una misión, un programa o una organización, o ubicarse en una posición que le permita hacerlo en el futuro. Además, la amenaza persistente avanzada **persigue sus objetivos repetidamente** durante un lapso extenso de tiempo, adaptándose a las medidas de defensa del atacado, y con la determinación de mantener el nivel de interacción necesario para ejecutar sus objetivos (Lopes, 2014).

Cada empresa tiene su propia cultura, lo que significa que las condiciones varían ampliamente de una a otra y en este sentido la importancia de las personas y cómo estas pueden ser víctimas de esta clase de ataques, es lo que alarma y motiva el presente estudio. Según el informe “Ciberamenazas y tendencias. Edición 2018” del Centro Criptológico Nacional (2018) de España, los dispositivos de Internet de las cosas, por lo general, tienen una seguridad moderada o baja. Contraseñas predeterminadas o débiles, ausencia de cifrado y las escasas o inexistentes actualizaciones de software para parchear vulnerabilidades y errores básicos de diseño, han dejado puertas abiertas para que estos dispositivos sean víctimas de ataques.

Las posibilidades que ofrece Internet e IoT son interminables y sin duda se ha alcanzado un nivel de dependencia digital que hace vulnerables a las personas. Si todo está

conectado: centrales eléctricas, el tráfico aéreo y terrestre, los ascensores y los electrodomésticos, todo está dependiendo de la tecnología y de su hiperconectividad, la cual implica riesgos potenciales para los más vulnerables. Internet ya te conoce y conoce tus hábitos, por ejemplo, las neveras sabrán qué productos se consumen más y mostrará publicidad ajustada a los hábitos de consumo. También hemos comentado acerca de la tecnología wearable, la que sin duda será muy utilizada: en 2014 se vendieron más de cien millones de artefactos y se espera que para 2018 ascienda a los 485 millones. El problema de esta tecnología es que es muy sencilla de hackear, como el caso de las Google Glass, que se comprobó que las imágenes y los sonidos son retransmitidos en tiempo real, incluyendo la información de usuario (usuario y la contraseña), sin que el propietario sea consciente de nada. Esto se debe a ciertas características de los dispositivos de IoT, las cuales trataremos en el siguiente título de esta sección.

5.4.2. Efectos de las nuevas características de IoT en la ciberseguridad y la privacidad

Uno de los puntos importantes es que algunos de los dispositivos y cosas conectadas a la red tienen menos capacidad de recursos de almacenamiento y suministro de energía por sí solos, lo que los conlleva a tener nuevas y diferentes características. Esto genera la necesidad de apoyarse e interconectarse con otras tecnologías, como la computación de la nube para el almacenamiento de datos.

Los fabricantes a falta de demanda muchas veces suelen concentrarse en implementar las funciones principales de los productos mientras ignoran la seguridad, no envían actualizaciones ni parches a sus dispositivos, a menos que las actualizaciones de firmware sean iniciadas por el usuario.

Zhou, Zhang y Liu (2018) introducen el concepto de “IoT features” que está basado en ocho características que se describen a continuación:

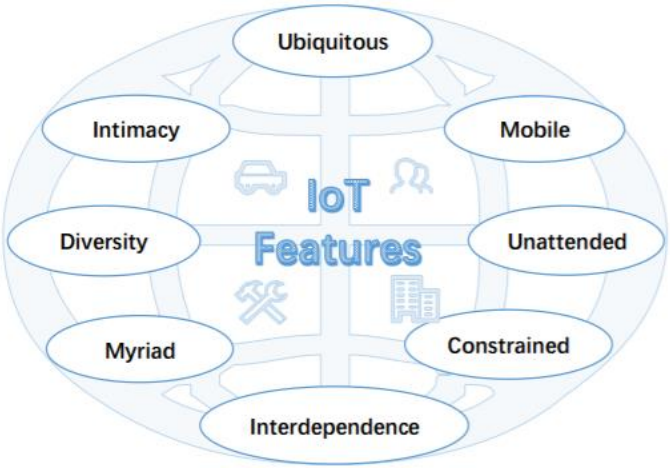

Figura 4. IoT Features. Zhou, Zhang & Liu (2018). Recuperado de https://arxiv.org/ftp/arxiv/papers/1802/1802.03110.pdf.

***Interdependencia*.** El número de dispositivos IoT incrementa la interacción entre sí, volviéndola más compleja y haciendo que el ser humano no tenga esa interacción directa que tiene con un smarphone o una computadora, luego hay una relación implícita con los dispositivos IoT. Esta interdependencia podría ser una amenaza si se usa maliciosamente para reducir la dificultad de ataque y poder eludir defensas estáticas. El reto es poder controlar los niveles de acceso a los dispositivos de IoT y más los privilegiados.

***Diversidad*.** IoT está o va a generar un uso masivo de aplicaciones de todo tipo y que están diseñadas para tareas específicas e interactúan fuertemente con el entorno físico. Esta diversidad se vuelve una amenaza ya que se pueden generar muchos protocolos inseguros de comunicación y vulnerabilidades en el firmware, que es el que establece la lógica de más bajo nivel y que controla los circuitos electrónicos de un dispositivo. El desafio es generar estándares ya que debido a que cada protocolo tiene diferencias con otros, los problemas de seguridad de redes subirán, al mismo tiempo será importante tratar urgentemente las vulnerabilidades que se vayan encontrando.

***Restringido*.** Muchos dispositivos de IoT como sensores industriales y dispositivos médicos implantables han sido diseñados para ser ligeros y de tamaño pequeño, reduciendo la capacidad de cómputo y de almacenamiento. Por otro lado, los dispositivos militares, industriales y agrícolas tienen que funcionar durante mucho tiempo en entornos donde la carga no está disponible, por lo que también tienen requisitos estrictos para el consumo de energía. La amenaza principal de esta característica son los sistemas inseguros, ya que no

despliegan defensas necesarias. El reto es generar defensas ligeras y protocolos con menos recursos de software y hardware.

***Myriad*.** La rápida proliferación de dispositivos de IoT y la cantidad de datos que estos dispositivos generan, transmiten y usan, son muy grandes. Las amenazas sobre esta característica están dadas por los ataques, DDoS e IoT botnet donde este último fue realizado en dispositivos IoT no asegurados en lugar que computadoras. El reto es implementar sistemas de detección y prevención de intrusos adaptados a estos dispositivos, conociendo sus deficiencias en cuanto a su diversidad y a sus restricciones.

Desatención. Esta característica es muy particular en IoT ya que medidores inteligentes, dispositivos médicos implantables, y muchos sensores industriales, agrícolas y militares en el entorno físico especial tienen que realizar funciones y operar durante un largo período de tiempo sin ninguna intervención ni acceso físico. Los accesos remotos se presentan como la gran amenaza en la desatención, ya que no es sencillo colocar interfaces externas para verificar el estado de estos dispositivos, de esta forma es difícil detectar cuando pueden haber sido atacados. El reto será lograr implementar controles que aseguren que operaciones críticas de seguridad se ejecuten correctamente y se considere como una tarea importante la verificación del estado interno de un pequeño dispositivo IoT remoto desatendido.

***Intimidad*.** Hoy en día hay una enorme variedad de dispositivos que usa el común de la gente como dispositivos wearables, por ejemplo, los relojes inteligentes. Estos dispositivos no solamente recopilan mucha información biológica, sino que también monitorean y registran la información que nos rodea y las actividades diarias. Las relaciones íntimas entre los usuarios y los dispositivos de IoT sin duda generarán problemas de privacidad más serios e inadvertidos. Una de las amenazas son los delincuentes que puedan acceder a la información íntima y sacar provecho de esto. El reto está en ofrecer una compensación atractiva entre la utilidad de información sensible y la privacidad.

***Movilidad*.** Muchos dispositivos IoT como dispositivos wereables y autos inteligentes se utilizan en el entorno móvil. Estos dispositivos móviles a menudo necesitan saltar de una red a otra y deben comunicarse con muchos dispositivos nuevos desconocidos**.**

Un hacker puede propagar software malicioso (Malware), luego este es una amenaza latente. El reto está en lograr una confianza entre dominios y en la identificación de cada uno.

***Ubicuo*.** Esta característica está enfocada a uno de los puntos más importantes de este estudio ya que como se ha mencionado, los dispositivos IoT están y van a penetrar en todos los aspectos del ser humano. No solo se usarán, sino que también se dependerá incluso más que del smartphone. Como se ha mencionado, en pocos años existirán millones de dispositivos IoT conectados, que podrían generar algunos inconvenientes:

- La mayoría de las personas todavía carecen de la conciencia de gestión y la protección de la privacidad
- Los fabricantes de dispositivos IoT tampoco asignan suficiente importancia a la seguridad de los productos
- Los dispositivos IoT son ampliamente utilizados en la industria, la agricultura e incluso en los campos militares, y también es necesario aumentar la conciencia de seguridad de los trabajadores.
- Como los dispositivos de IoT se aplican a más escenarios, habrá más tipos y funciones de dispositivos con diferentes recursos y arquitecturas, como mencionamos anteriormente. Los investigadores ya no deberían centrarse solo en el estudio de la teoría, se necesita más cooperación con las empresas y el gobierno.

La seguridad y el ser humano siempre han estado relacionados, y con la IoT lo estará mucho más, especialmente si tomamos la estrecha vinculación de la protección con el hogar. Un nuevo estudio de Juniper Research descubrió que el gasto en soluciones de ciberseguridad de IoT alcanzará más de $ 6 mil millones a nivel mundial para 2023. El rápido crecimiento y el gasto por parte de proveedores de productos y servicios, así como clientes finales, aumentará casi un 300% durante el período de 2018 y 2023 (García, 2018).

6. Metodología

En la siguiente tabla se propone describir la metodología en función de cada objetivo específico:

Tabla 1.

Metodología según objetivos específicos.

Objetivo específico	**Fuente primaria de datos/ Instrumento de recolección**	**Población /muestra**	**Técnicas de procesamiento**
Realizar un sondeo que permita identificar el nivel de conocimiento y consciencia acerca de la Internet de las Cosas y sus amenazas entre la población general de la Ciudad de Buenos Aires y GBA.	Encuesta autoadministrada en soporte digital a través de Internet.	Población general que viven en la Ciudad Autónoma de Buenos Aires y GBA.	Análisis uni y – bivariado.
Describir los riesgos más relevantes a que se expone la población general al utilizar la Internet de las Cosas.	Riesgo en base a fuentes documentales y bibliográficas.		Revisión bibliográfica y sistematización de la información.
Explorar la normativa vinculada a Ciberseguridad en la Argentina.	Regulación actual de Internet, ciberseguridad y protección de datos en Argentina existentes.	Argentina.	Revisión bibliográfica y sistematización de la información.
Elaborar un plan de acción a nivel organizacional para la concientización y protección de las personas fundamentado en una perspectiva de ciberseguridad.	Elaboración propia en base a fuentes documentales y bibliográficas.	Integrantes de la organización empresarial. Población general que vive en la Ciudad Autónoma de Buenos Aires y GBA[1]	

Fuente: Elaboración propia.

[1] Si bien el plan de acción se enfocó en la población de Capital Federal y GBA, es aplicable al resto del país y otros países de América Latina

El presente estudio combina la recolección de datos primarios y la revisión documental sobre el tema.

El sondeo en la población general se realizó mediante una encuesta autoadministrada en soporte digital a través de Internet. Se utilizó Google Work Request para construir el instrumento de medición. A continuación, se presenta la ficha técnica de la encuesta:

Tipo de estudio: cuantitativo.
Método: encuesta autoadministrada.
Soporte: digital.
Aplicación: on-line vía Smartphone.
Plataforma de distribución: whatsApp y correo electrónico.
Muestreo: no probabilístico.
Selección de la muestra: por referencias (bola de nieve).
Tamaño de la muestra: se espera una muestra resultante mayor a 200 casos.

La forma de abordaje se realizó con base en un listado inicial de 50 números de teléfonos celulares. El cuestionario incluyó una presentación en la cual se indicó:

- El motivo de la encuesta
- La solicitud de reenvío al menos a 5 contactos.
- Correo electrónico del investigador para consultas.
- Preguntas sobre el tema de investigación.

Se estimó un tiempo de recopilación de información a través de la encuesta de un mes, pudiéndose extender en función de la tasa de respuesta que se obtuvo.

Si bien la encuesta está propuesta para habitantes de la Capital Autónoma de Buenos Aires y GBA, dado que se trata de una encuesta online por referencias (bola de nieve) a través de WhatsApp, no se pudo controlar esta inclusión durante el trabajo de campo. Una vez cerrada la aplicación, se analizó el perfil y lugar en que habitan quienes finalmente respondieron la encuesta.

A continuación, se exponen las dimensiones, variables e indicadores tenidos en cuenta para este análisis.

Tabla 2.

Matriz de indicadores a medir en la encuesta.

Dimensión	**Variable**	**Indicador**
Clasificación del respondiente.	Datos demográficos.	Edad. Género.
	Datos educativos y laborales.	Nivel educativo. Condición laboral. Empresa en la que trabaja.
	Localidad.	Lugar donde vive.
Perfil de usuario de Internet.	Conocimiento de internet.	Conocimiento de Internet.
	Nivel de uso de Internet.	Uso de Internet. Horas conectado a Internet. Reacción ante la falta de Internet.
Relación con la Internet de las Cosas (IoT).	Conocimiento de IoT.	Conocimiento de IoT. Concepto de IoT.
	Efectos de cambio de IoT.	Percepción al cambio.
	Conectividad de dispositivos a la internet.	Tenencia de electrodomésticos conectados. Predisposición a conectar dispositivos a Internet.
	Gestión de los dispositivos conectados a internet.	Interés en el manejo de dispositivos desde su celular.
Ciberseguridad.	Contraseñas.	Utilización de contraseñas. Frecuencia de cambio.
	Privacidad /vulnerabilidad.	Preocupación por la seguridad. Percepción de vulnerabilidad /ser espiado. Aceptación de actualizaciones.
Perfil uso del celular.	Accesibilidad a Internet.	Medios de acceso.
Regulación de ciberseguridad.	Políticas organizacionales y de gobierno.	Conocimiento de políticas organizacionales y de gobierno. Conocimiento de ciberseguridad en la empresa que trabaja.
	Reporte de incidentes de Ciberseguridad.	Conocimiento del lugar donde reportar incidentes de Ciberseguridad.
Perspectiva de futuro.	Aceptación de cambio basada en la tecnología.	Aceptación para viajar en coche sin conductor.

Fuente: Elaboración propia.

7. Hallazgos y resultados

7.1. Análisis del sondeo

El análisis del sondeo se realizó con base en los indicadores descriptos en la metodología y cuyo formulario de encuesta se incluye en el Anexo.

7.1.1. Descripción del respondiente

El resultado total del sondeo fue de 231 casos, incluyendo población de Capital Federal, GBA y otras localidades y países de acuerdo con el siguiente gráfico

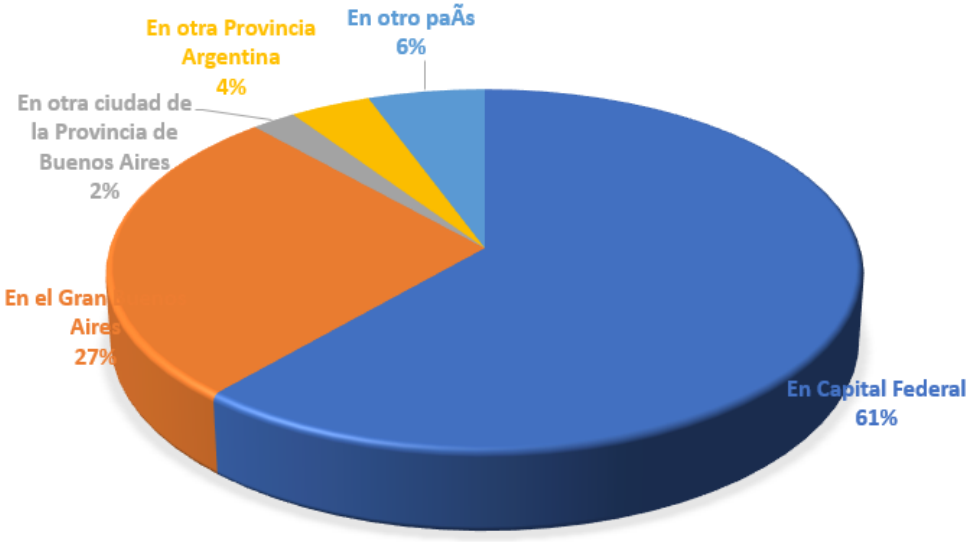

Gráfico N° 1. Lugar de residencia de la población respondiente (en %). Encuesta on-line sobre uso de tecnología 2018. Elaboración propia.

Teniendo en cuenta que el presente estudio se basa en la población general de la Ciudad Autónoma de Buenos Aires y GBA, se toman 204 casos para el análisis, los cuales cubren esta población. De las 204 personas encuestadas, el 70% corresponde a habitantes de CABA y el 30% a habitantes de GBA.

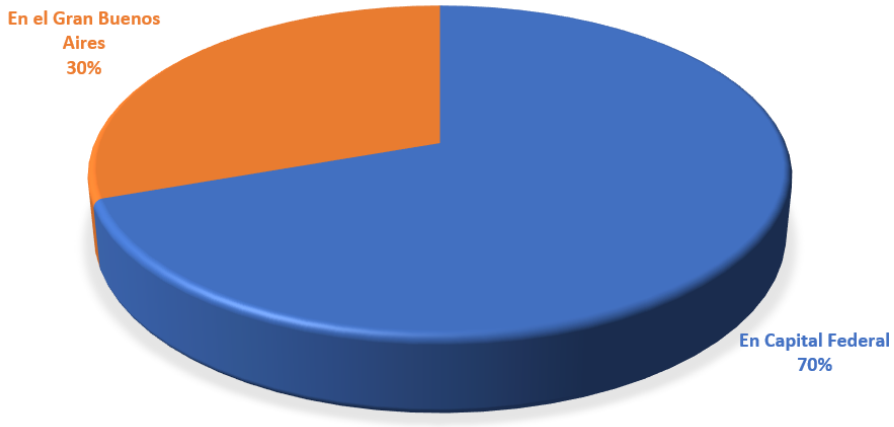

Gráfico N° 2. Distribución de residentes de Capital y GBA (en %). Encuesta on-line sobre uso de tecnología 2018. Elaboración propia.

El porcentaje que corresponde a la característica de género dio como resultado que la muestra resultante se reparte prácticamente en partes iguales, con un 48% femenino y un 52% masculino, muy similar a como se reparte la población general.

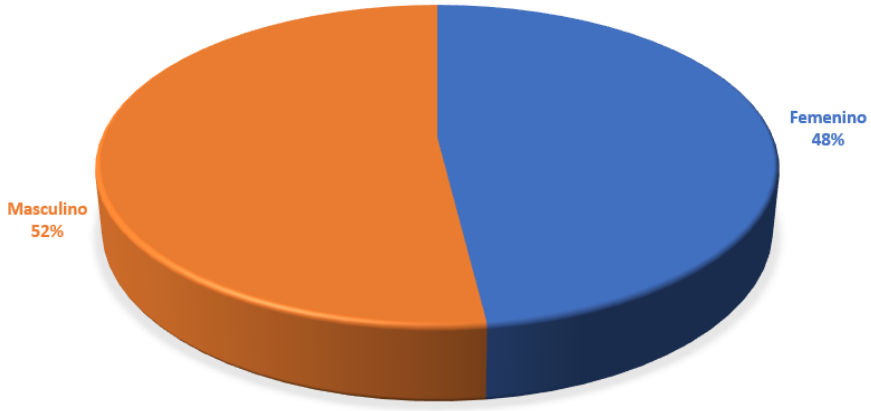

Gráfico N° 3. Distribución de respondientes según género (en %). Encuesta on-line sobre uso de tecnología 2018. Elaboración propia.

Al tratarse de una muestra no probabilística, si bien el nivel de estudios resultó variado, el sondeo alcanzó a una población en su mayoría con estudios universitarios y de posgrado; con una alta participación de respondientes con niveles terciarios y secundarios.

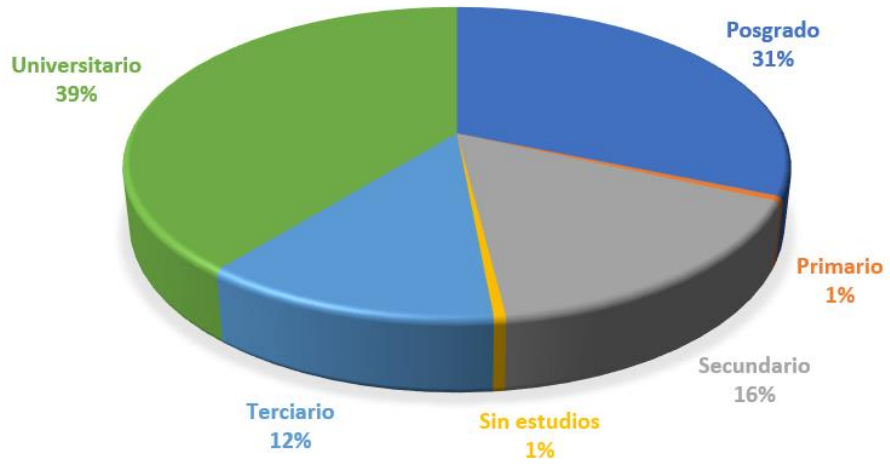

Gráfico N° 4. Distribución de respondientes según nivel educativo (en %). Encuesta on-line sobre uso de tecnología 2018. Elaboración propia.

La mayor parte de quienes respondieron la encuesta dicen trabajar actualmente (80%), y entre quienes trabajan, la mayoría trabaja en la empresa privada (76,6%) mientras que una cuarta parte (23,5%) trabajan en una organización pública. Esto es importante ya que se pudo conseguir datos que evidencian el estado de conocimiento en materia de ciberseguridad que opera en las empresas y organizaciones donde trabajan.

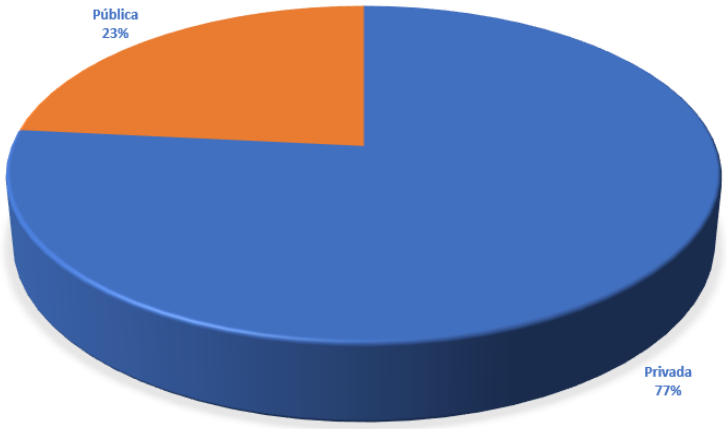

Gráfico N° 5. Tipo de empresa en la que trabajan (en %). Encuesta on-line sobre uso de tecnología 2018. Elaboración propia.

El rango de edades de la población encuestada fue variado, concentrándose en edades laborales y con más baja participación en población de 60 y más años. La diversidad de edades en este estudio resulta importante ya que la IoT es una tecnología que alcanza a todas las personas.

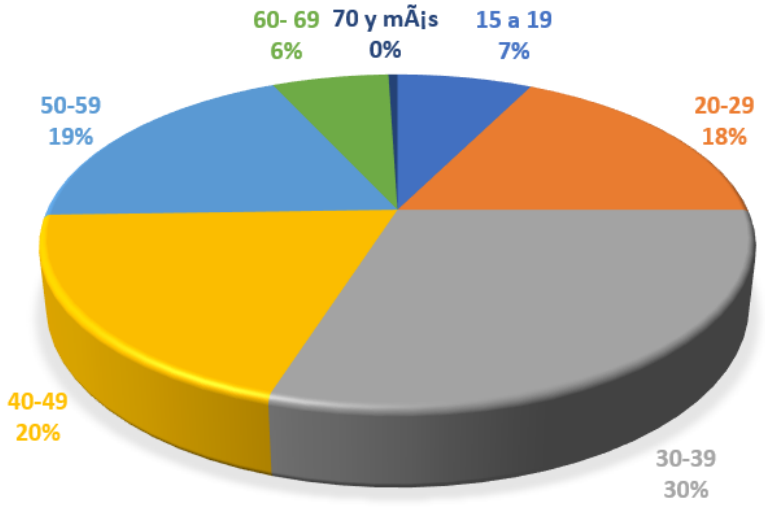

Gráfico N° 6. Distribución según edad (en %). Encuesta on-line sobre uso de tecnología 2018. Elaboración propia.

La transformación digital al interior de las empresas no solo va a ser importante para que los profesionales entiendan de IoT, y todos los roles que participan en la empresa , por ejemplo, aquellas personas que hacen el aseo, vigilantes o recepcionistas también se capaciten, siendo deber de las compañías tenerlos en cuentan, ya que los objetos a conectar a Internet estarán integrados por muchos de los productos de uso común.

7.1.2. Perfil de usuario de Internet

Como se ha venido mencionando, Internet hoy en día es parte fundamental en la cotidianidad de la sociedad por lo que es necesario conocer su uso. Como se comentó en el apartado 5.1.2, Argentina cuenta con un acceso a Internet por encima de la media global, sin embargo, aún no toda la población tiene este acceso, sin embargo, en la encuesta realizada, el 100% de los encuestados usan Internet, independientemente del tiempo que destinan para la realización de tareas y actividades conectados a la web.

Aunque las horas por día de conexión a Internet son divididas y variadas, el tiempo conectado a la red por los respondientes es alta, más de la mitad indican estar conectados 7 horas o más, cuatro de cada 10 (36%) del de la población encuestada dedica entre 7 y 12 horas al uso de internet y dos de cada 10 (20%) utiliza Internet más de 12 horas diarias.

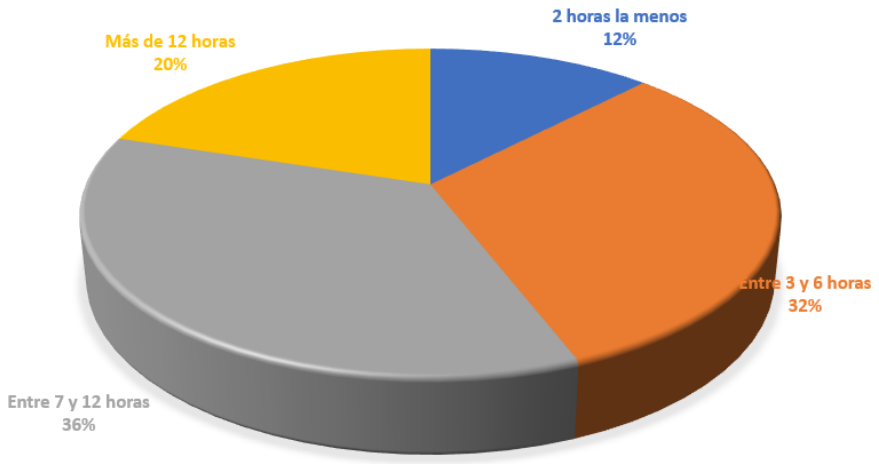

Gráfico N° 7. Tiempo de uso de Internet (en %). Encuesta on-line sobre uso de tecnología 2018. Elaboración propia.

Quienes más horas están conectados a Internet son los universitarios, seguido de los de estudiantes de posgrados. Finalmente, quienes menos usan esta herramienta son los de estudios primarios. Sin embargo, hay que tener en cuenta en este punto, que Internet es de tipo atendido, es decir, es una herramienta de permanente interacción, a diferencia de IoT que como lo mencionamos dos de las características de esta tecnología es la desatención y lo ubicuo, siendo esta última en donde los dispositivos IoT están y van a penetrar en todos los aspectos del ser humano.

La necesidad de acceso a Internet resulta importante entre los encuestados, ya que la falta de este servicio impacta a la gran mayoría. El 77% de la población encuestada se ve afectada ante la no disponibilidad de Internet. La preocupación por la falta de Internet parece aumentar con los estudios. El sector al que más le afectaría es a los universitarios. Podría esperarse que entre ellos se encuentre un mayor interés en utilizar el IoT.

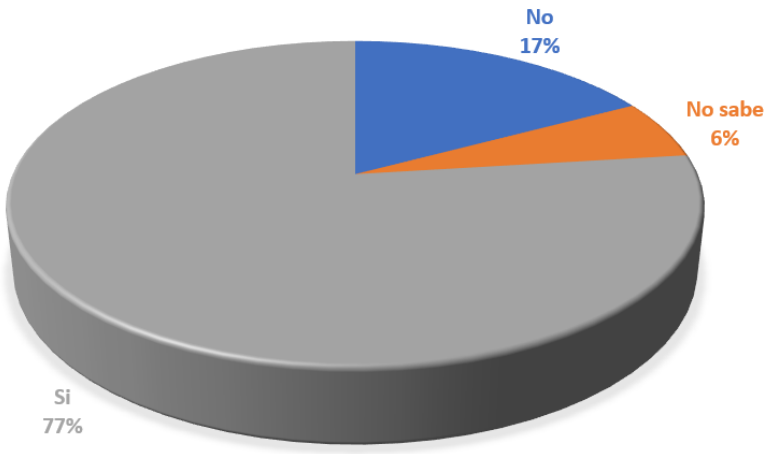

Gráfico N° 8. Preocupación por la falta de Internet (en %). Encuesta on-line sobre uso de tecnología 2018. Elaboración propia.

7.1.3. Relación con la Internet de las Cosas IoT

A fin de realizar un análisis más preciso del conocimiento de IoT por la población encuestada se efectuó la ponderación de los datos en base a las características de la población de Capital y GBA según datos del Censo 2010, donde se refleja el peso que tiene la distribución por edades y por nivel educativo ya que la muestra resultante tiene una presencia mayor de universitarios y posgrado que la población general. Considerando la base ponderada, la población de Capital y GBA, en su mayoría (65.2%) dicen no conocer el IoT, mientras que algo más de tres de cada 10 personas sí lo conocen.

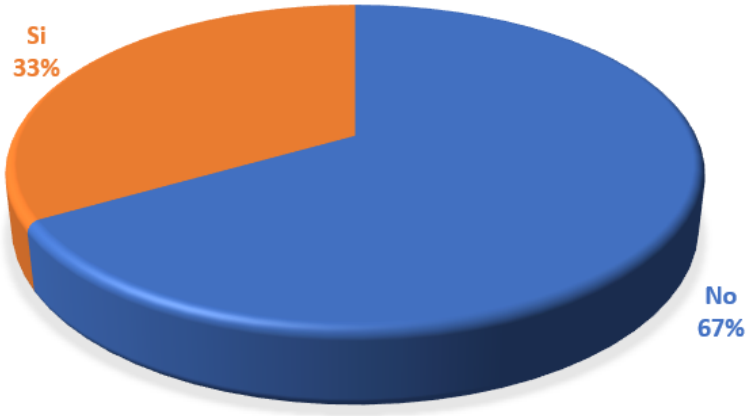

Gráfico N° 9. Conocimiento de IoT (en %). Encuesta on-line sobre uso de tecnología 2018. Base ponderada. Elaboración propia.

El conocimiento de IoT tiende a ser mayor entre los adultos jóvenes de 30 a 39 años y a medida que aumenta el nivel educativo.

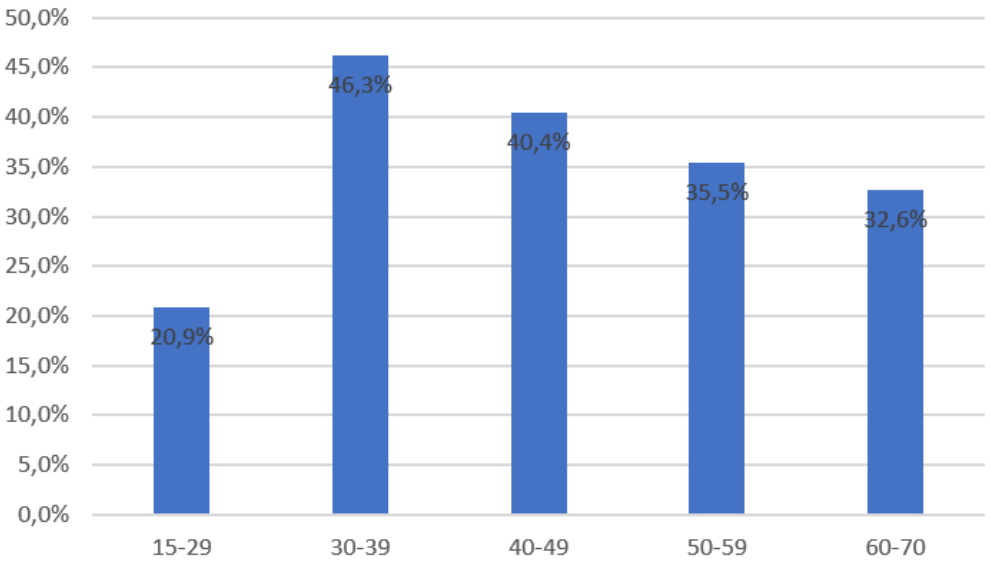

Gráfico N° 10. Conocimiento de IoT según Edad (en%). Encuesta on-line sobre uso de tecnología 2018. Base ponderada. Elaboración propia.

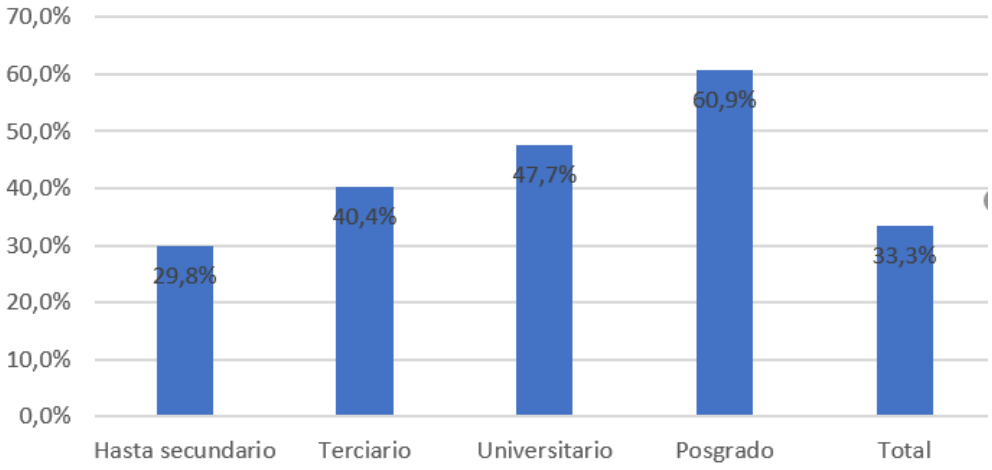

Gráfico N° 11. Conocimiento de IoT según Nivel educativo (en%). Encuesta on-line sobre uso de tecnología 2018. Base ponderada. Elaboración propia.

Entre quienes dijeron conocer el concepto de IoT, prácticamente la totalidad (98%) asoció IoT al concepto que se había establecido como “Cualquier cosa a Internet”. Aunque como se mencionó anteriormente, la IoT es aún una tecnología desconocida al interior de la población.

Con base en la hipótesis que se planteó, se puede comprobar que gran parte de la población no conoce sobre IoT y en ese sentido puede considerarse que su despliegue en la Ciudad Autónoma de Buenos Aires y GBA ha sido insuficiente para su conocimiento. Sin embargo, se debe tener presente que la Internet hoy en día es un servicio masivo en comparación al momento histórico en que comenzó; además, se debe recordar el ciclo de tecnologías emergentes de Gartner Hype Cycle 2018, según la cual se plantea que la IoT será una de las tecnologías emergentes más sobresaliente e invasivas para la población mundial a corto plazo.

En cuanto a los efectos del cambio de IoT, existe una percepción positiva ya que un 61% ve bien a IoT como tecnología. Tanto en las mujeres, como en los hombres, la percepción es similar, aunque un poco más elevada en los hombres.

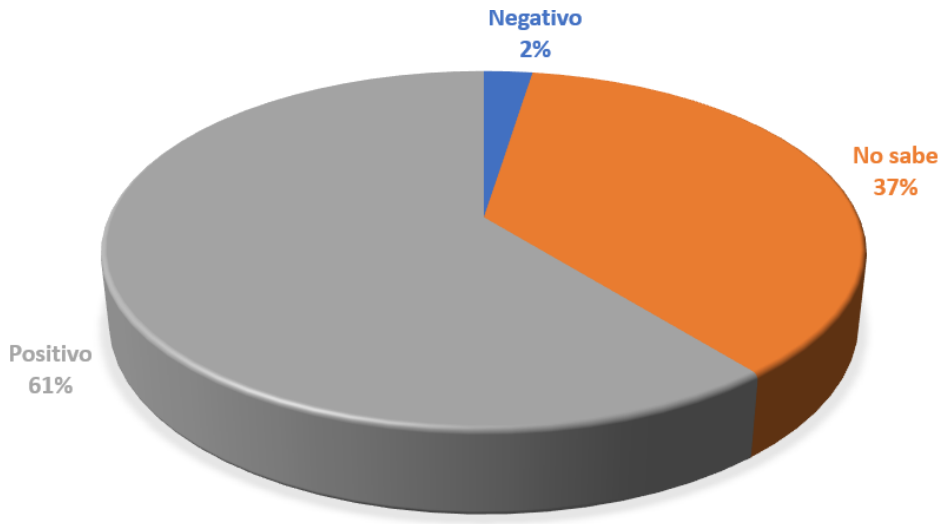

Gráfico N° 12. Valoración positiva o negativa frente a IoT (en %). Encuesta on-line sobre uso de tecnología 2018. Elaboración propia.

Como se ha venido mencionando a lo largo de este trabajo, la Internet de las Cosas está basada precisamente en la interconexión de las cosas a Internet y en ese sentido se indagó acerca de si la población tiene algún dispositivo como televisor o consola de videojuegos conectado a Internet. El 80% lo tiene.

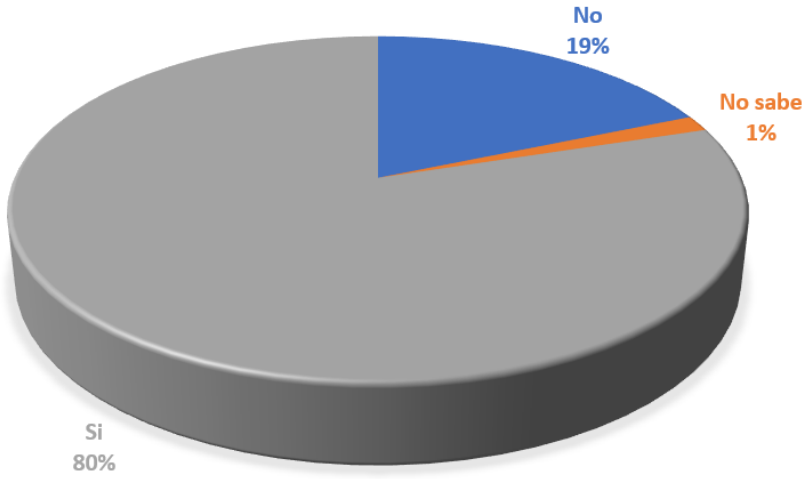

Gráfico N° 13. Dispositivos conectados a Internet (en %). Encuesta on-line sobre uso de tecnología 2018. Elaboración propia.

La tendencia de conectividad de objetos como heladera, climatización, cámaras, etc., pareciera estar dividida, pues un 39% lo haría y un 35% no lo haría.

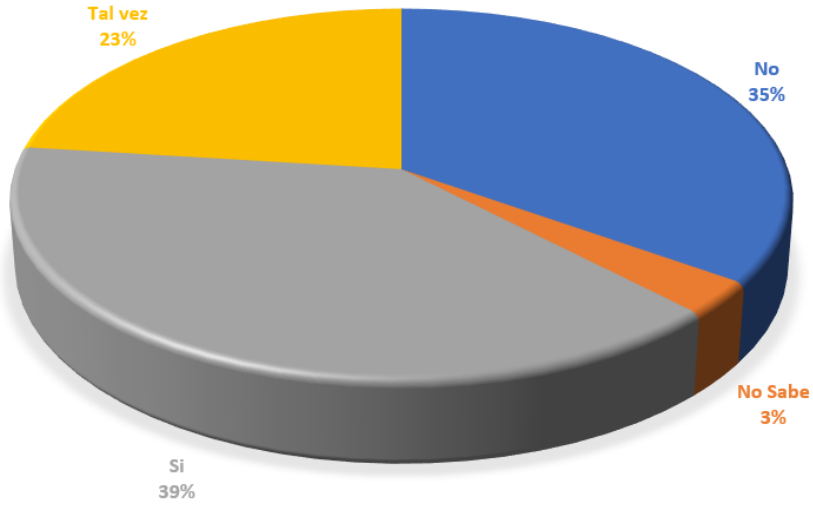

Gráfico N° 14. Predisposición de tener dispositivos conectados a Internet (en %). Encuesta on-line sobre uso de tecnología 2018. Elaboración propia.

Frente a esto, aunque no es muy alto, la conectividad de objetos a Internet llama la atención. La población entre 30 y 39 años es a la que más le interesa poder tener este tipo de acceso. Esta población es en su mayoría universitaria y con posgrado, con un 12% y 13%, respectivamente.

Como se sabe, la tecnología móvil con su amplio catálogo de aplicaciones y APIs, será el control remoto de los dispositivos IoT. La percepción frente a que el smartphone se utilice como herramienta para gestionar estos dispositivos es 50% positiva, sobre todo para aquellos que la utilizan y que actualmente les sirve para conectar dispositivos a Internet.

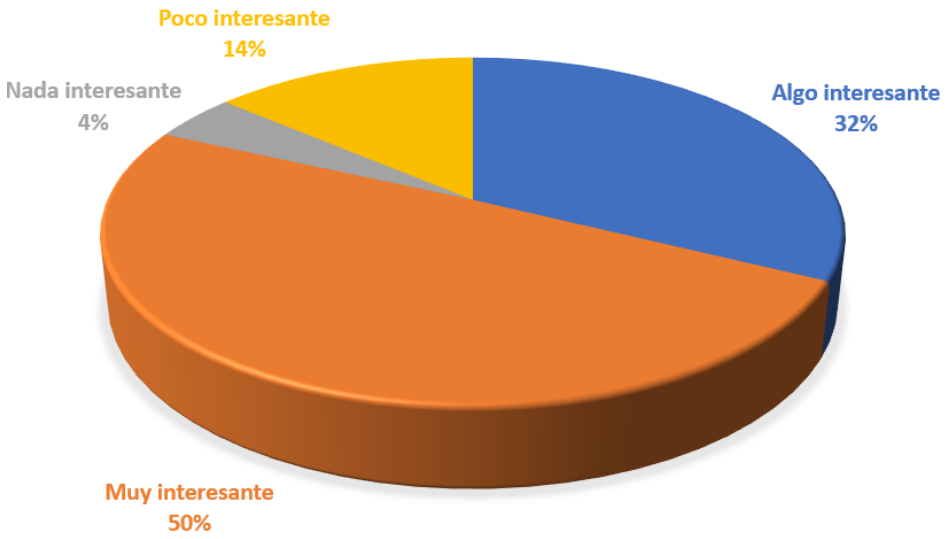

Gráfico N° 15. Predisposición de tener dispositivos conectados a Internet (en %). Encuesta on-line sobre uso de tecnología 2018. Elaboración propia.

7.1.4. Ciberseguridad

Hasta este punto se ha podido corroborar que existe desconocimiento de lo que es la tecnología IoT por parte de la población de la Cuidad Autónoma de Buenos Aires y GBA, más, sin embargo, hay una buena percepción sobre esta tecnología y sabiendo que Internet es base para su funcionamiento, es de esperar que poco a poco las personas se irán adaptando a nuevos hábitos, utilizando esta tecnología.

Ahora bien, este desconocimiento puede traer consecuencias frente a la seguridad de empresas y personas, por lo que es fundamental prevenir sobre hábitos actuales.

Hay un mensaje positivo y es que un 87% de los encuestados sí utilizan contraseñas u otros mecanismos de acceso a su celular.

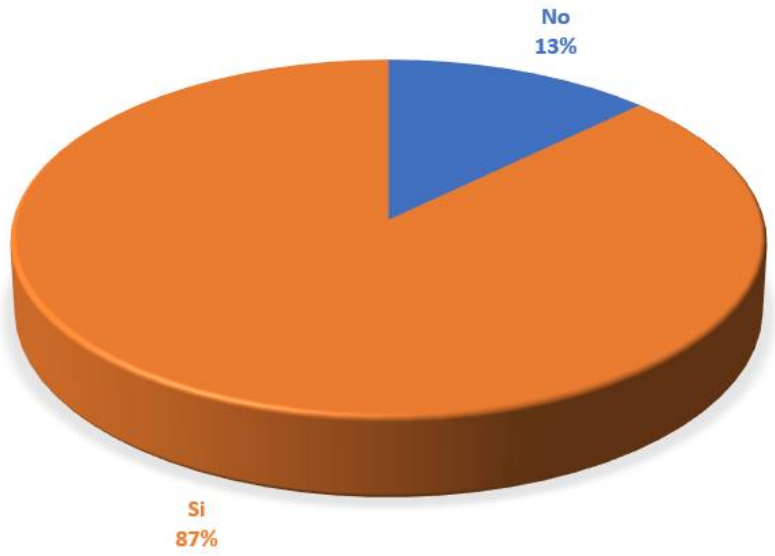

Gráfico N° 16. Utilización de contraseñas (en %). Encuesta on-line sobre uso de tecnología 2018. Elaboración propia.

De ese 13% que no cambia la contraseña se encuentra diversificado entre diferentes edades, estudios y géneros.

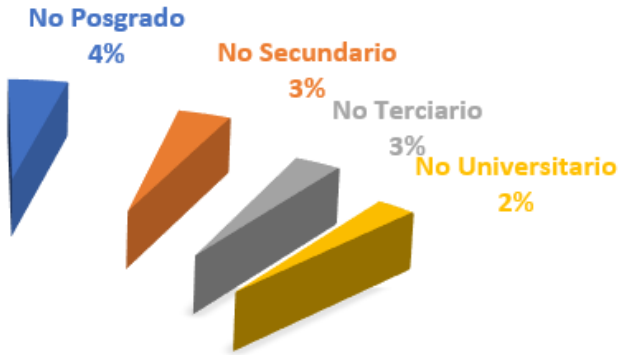

Gráfico N° 17. Población que no cambia las contraseñas (en %). Encuesta on-line sobre uso de tecnología 2018. Elaboración propia.

Por lo general, los dispositivos y en especial los teléfonos móviles no piden cambiar la contraseña. Para nuestro estudio y con el fin de poder conocer cuál es la mejor manera en que las personas podrían cambiar las contraseñas, se preguntó basado en las mejores prácticas de seguridad de contraseñas.

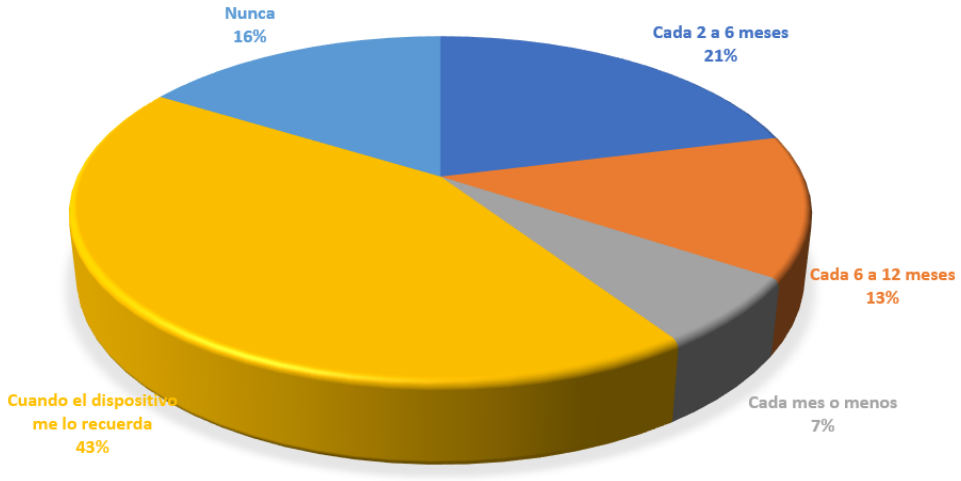

Gráfico N° 18. Frecuencia del cambio de contraseñas (en %). Encuesta on-line sobre uso de tecnología 2018. Elaboración propia.

Un 43% dice que cambia su contraseña cuando el dispositivo se lo recuerda y prácticamente 2 de cada 10 respondientes dicen no hacer este cambio nunca. Puede observarse que más de la mitad de quienes respondieron la encuesta no cambian la contraseña nunca o lo hacen sólo si el dispositivo envía un aviso. Sin embargo, este es un buen punto de partida, como oportunidad de mejora, para que todo dispositivo por configuración predeterminada pida cambiar la contraseña frecuentemente. Recordemos que una de las debilidades de los dispositivos IoT es que los fabricantes prestan poca atención a la seguridad y los usuarios no cambian las contraseñas predeterminadas o débiles, en dispositivos asociados a la IoT.

La accesibilidad a IoT desde cualquier parte del mundo es su beneficio diferencial, así como el continuo traspaso de información de un dispositivo a otro.

La preocupación por parte de la población frente a la seguridad, protección de su intimidad y privacidad de sus datos personales en Internet es significativa. Al 88% le preocupa la seguridad, en este sentido, resulta importante que en esta tecnología se proporcione el control y la seguridad absoluta.

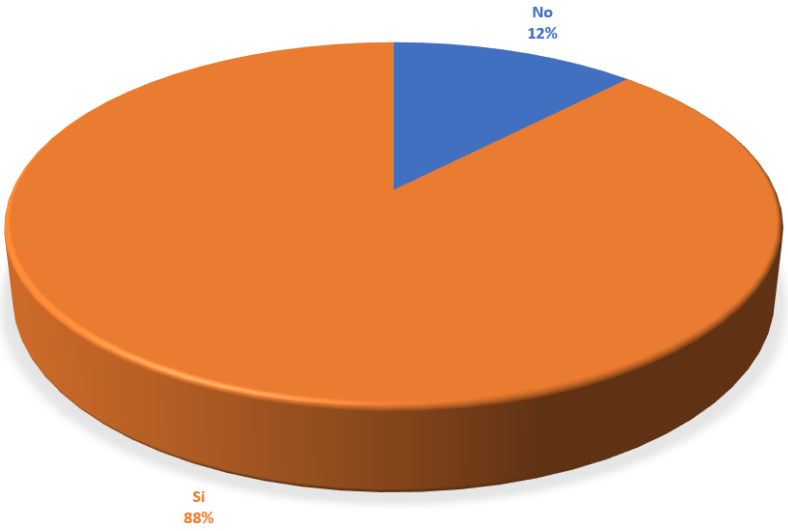

*Gráfico N° 19. P*reocupación por la seguridad (en %). Encuesta on-line sobre uso de tecnología 2018. Elaboración propia.

La ciberseguridad es y será un elemento de confianza fundamental para el uso de IoT. Esta tecnología tiene que demostrar que va a proporcionar una verdadera seguridad y protección a los usuarios, si de verdad quiere establecerse y expandirse.

Tal como se comentó anteriormente sobre el ciberespacio y su parte oculta se debe tener presente que el espionaje es una de las actividades más frecuente dentro del ciberespacio. Sobre este punto se consultó en la encuesta, indagando acerca de la percepción de sentirse espiado. La percepción de haber sido espiado es menor (35%) que quienes no han tenido esta experiencia (35%) y esta percepción aumenta a medida que es mayor el nivel educativo, como se puede observar en el Gráfico Nº21.

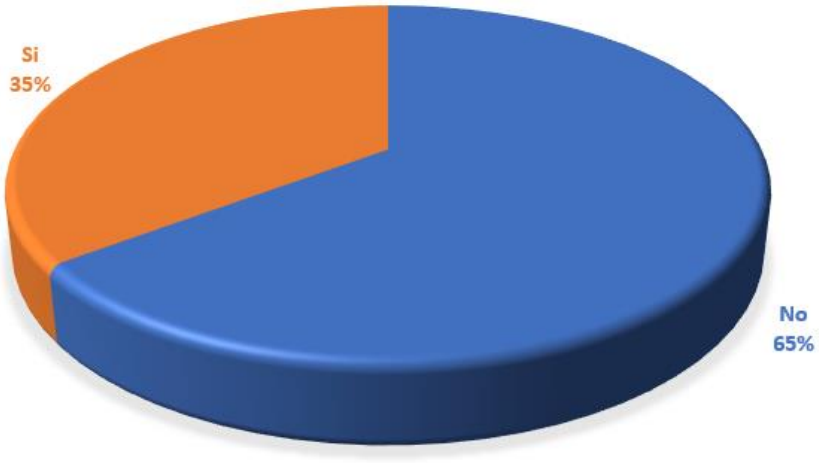

Gráfico N° 20. Percepción de haber sido espiado a través de un dispositivo digital (en %). Encuesta on-line sobre uso de tecnología 2018. Base ponderada. Elaboración propia.

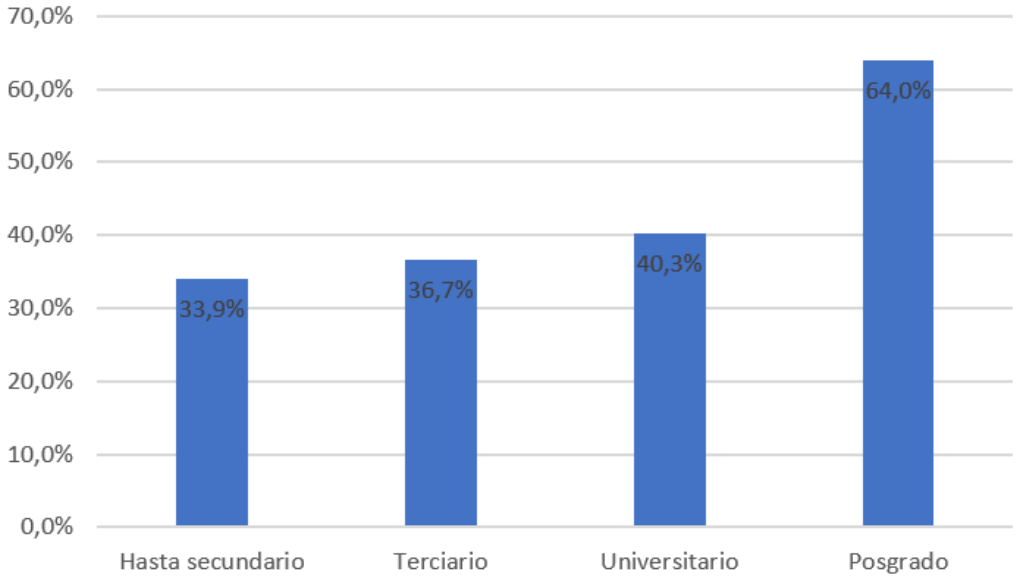

Gráfico N° 21. Percepción de haber sido espiado a través de un dispositivo digital según nivel educativo (en%). Encuesta on-line sobre uso de tecnología 2018. Base ponderada. Elaboración propia.

Más allá de estas percepciones, se trasluce la importancia de conocer qué tan protegidos se puede navegar en internet y cómo las grandes compañías aseguran la información, los datos personales y colaboran a preservar la intimidad de los usuarios.

Otro de los puntos clave para los dispositivos IoT, es la manera en cómo se llevan a cabo las actualizaciones por medio de las cuales se mejoran potencialmente las funcionalidades y la seguridad de los dispositivos. Anteriormente se describió que las actualizaciones de software sirven para corregir deficiencias, vulnerabilidades y errores básicos de diseño que dejan puertas abiertas para que estos dispositivos puedan ser vulnerables a posibles ciberataques.

Un parte de confianza es que el 88% de los encuestados respondieron que, si aceptan realizar actualizaciones a sus aplicaciones, luego es importante que los fabricantes actúen y desplieguen de forma rápida estas, ya que puede existir una cultura sobre este tipo de prácticas en la mayoría de las personas.

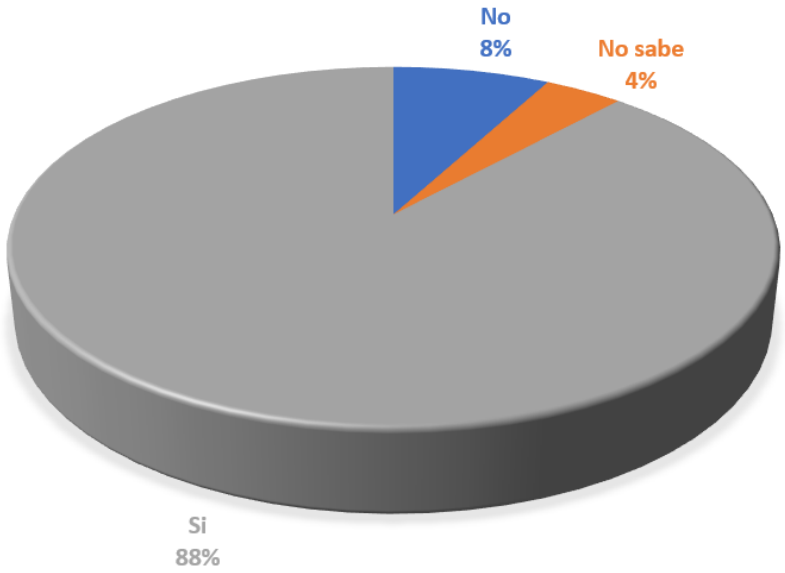

Gráfico N° 22. Aceptación de actualizaciones (en%). Encuesta on-line sobre uso de tecnología 2018. Elaboración propia.

7.1.5. Perfil sobre el uso del celular

En el apartado 5.2.3. Tecnología móvil, aplicaciones y APIs, se detalla la evolución de la telefonía celular y su importancia en el IoT, las velocidades serán claves para que IoT se pueda gestionar y las aplicaciones, junto a las APIs, serán la entrada. Según el sondeo el 80% de los encuestados usa más las aplicaciones en el celular que los navegadores convencionales. Esto es una muestra la evolución de Internet y su innovación. Ya no es necesario escribir un www para acceder a Internet, sino que las aplicaciones conectan a la red con solo descargar y abrir una aplicación.

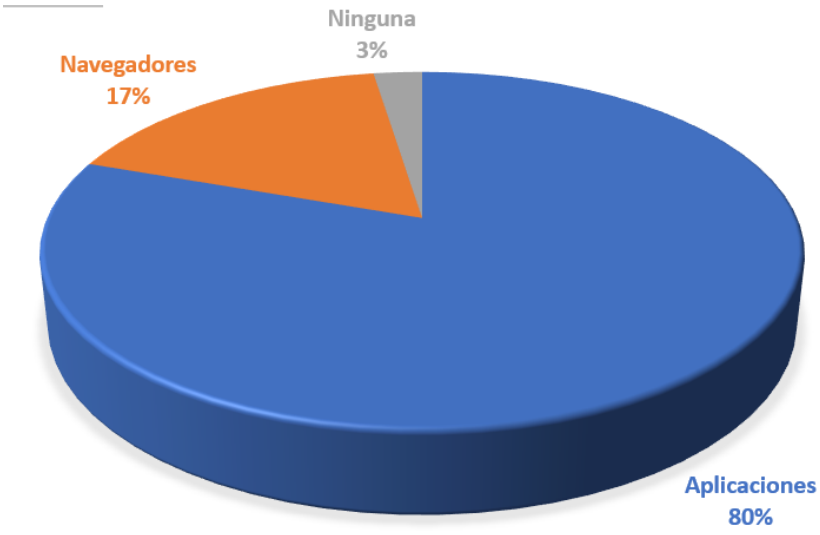

Gráfico N° 23. Accesibilidad a Internet (en%). Encuesta on-line sobre uso de tecnología 2018. Elaboración propia.

7.1.6. Regulación en ciberseguridad en la Argentina

La idea de que la IoT sea una tecnología a disposición de dispositivos cotidianos y donde se involucran datos personales e información privada, el conocimiento no solo de los alcances de esta tecnología, sino estar preparado para saber cómo protegerse y también para saber qué hacer ante un ataque o incidente, resulta de alta importancia para que esta tecnología pueda ser usada con confianza y represente una mejora en la vida humana en lugar de una amenaza.

Tan solo el 46% de las personas encuestadas conoce de políticas de ciberseguridad en sus compañías, siendo, como se ha venido viendo en estos resultados, que aumenta este conocimiento con el nivel educativo, siendo los universitarios y con posgrados los que se muestran más informados al respecto.

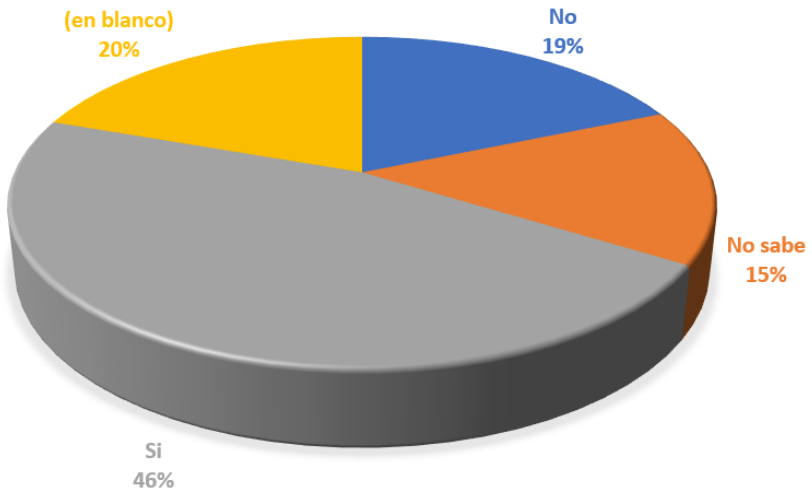

Gráfico N° 24. Conocimiento de Políticas de Ciberseguridad a nivel empresarial (en%). Encuesta on-line sobre uso de tecnología 2018. Elaboración propia.

A nivel Ciudad Autónoma de Buenos Aires y GBA, existe una debilidad muy notoria y es que las personas no conocen de políticas de ciberseguridad y mucho menos de cómo reportar un incidente si está siendo afectado por un ataque o amenaza.

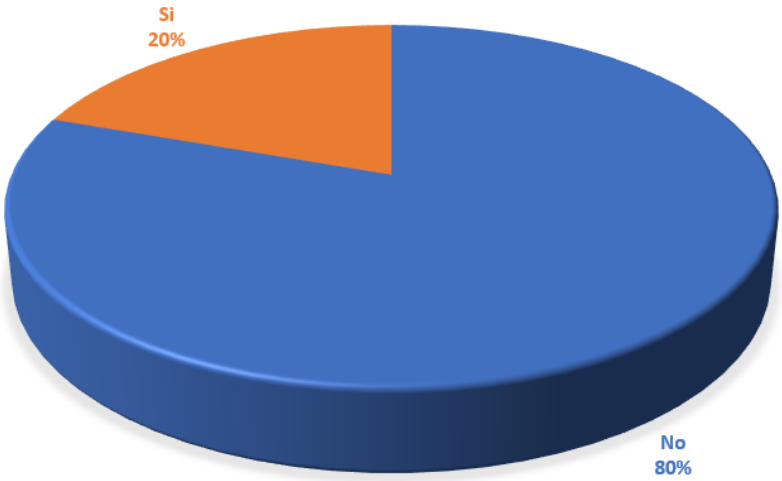

Gráfico N° 25. Conocimiento de políticas de Ciberseguridad a nivel de gobierno (en%). Encuesta on-line sobre uso de tecnología 2018. Elaboración propia.

Solo el 20% de la población encuestada dice conocer de políticas de ciberseguridad y tan solo el 18% sabe reportar un incidente.

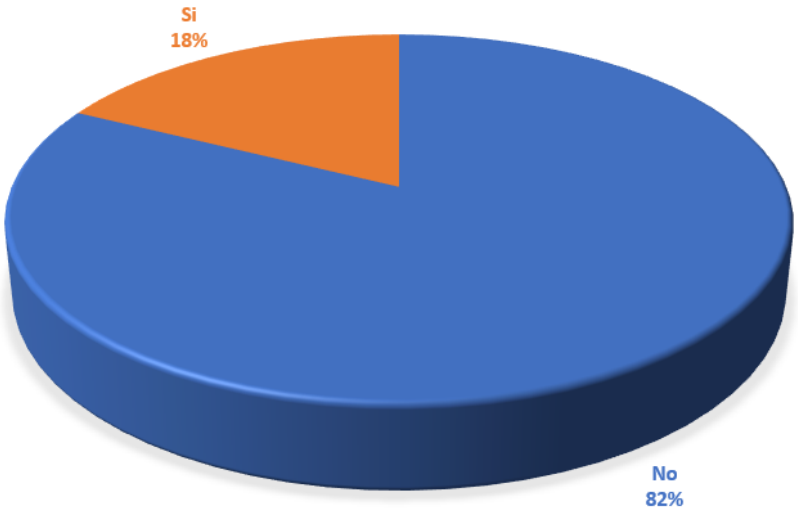

Gráfico N° 26. Conocimiento de cómo reportar incidentes de Ciberseguridad a nivel de gobierno. (en%). Encuesta on-line sobre uso de tecnología 2018. Elaboración propia.

Por otro lado, la posibilidad de poder reportar un incidente debe ser un procedimiento previsto y habilitado en todas las compañías y para todos los integrantes sin importar el cargo o posición de quien reporte, para que de esta manera se pueda actuar proactivamente frente a amenazas. Aproximadamente la mitad (55%) dicen saber dónde reportar un incidente al interior de sus empresas. Según esto se puede observar que el entrenamiento no se está realizando a todas las personas o no existe procedimientos al respecto, o bien no se tiene el hábito de ciberseguridad de reportar.

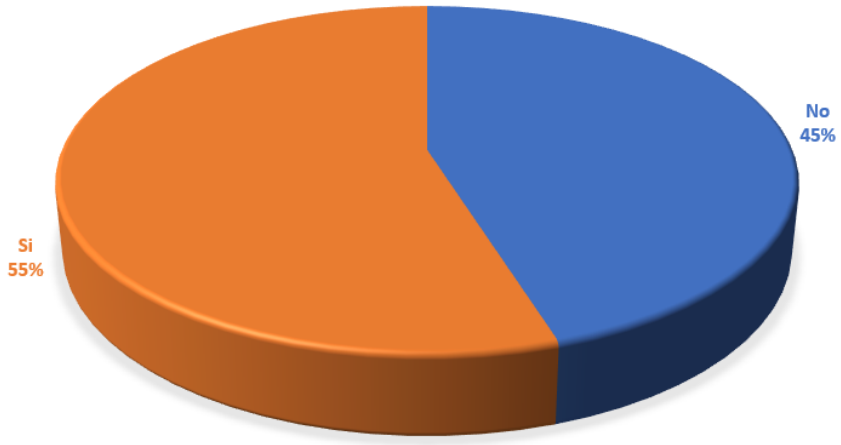

Gráfico N° 27. Conocimiento de cómo reportar incidentes de Ciberseguridad a nivel empresarial (en%). Encuesta on-line sobre uso de tecnología 2018. Elaboración propia.

Se debe tener presente que el reporte y la gestión de incidentes es un tema fundamental para los gobiernos porque permite tener protocolos que permitan actuar ante un incidente de forma rápida. Muchos vectores de ataques dentro de las APTs que se describen en el apartado 5.4.1. Objetivos de Ciberseguridad, están surgiendo y las personas deben poder informar y de esta manera contribuir a conformar un sistema con equipos que puedan dar respuestas y garantizar la seguridad en el entorno virtual.

7.1.7. Perspectiva de futuro

Uno de los sectores que más ha desarrollado el IoT es el de los automóviles. Frente a esto es importante conocer, pensando en un futuro no lejano, la posibilidad de viajar en un coche automático sin conductor, como indicador de confianza hacia una tecnología disruptiva con relación a lo conocido hasta el momento y que requiere ceder el control justamente a la tecnología. El sentimiento está dividido en la población, registrando ciertas dudas al respecto.

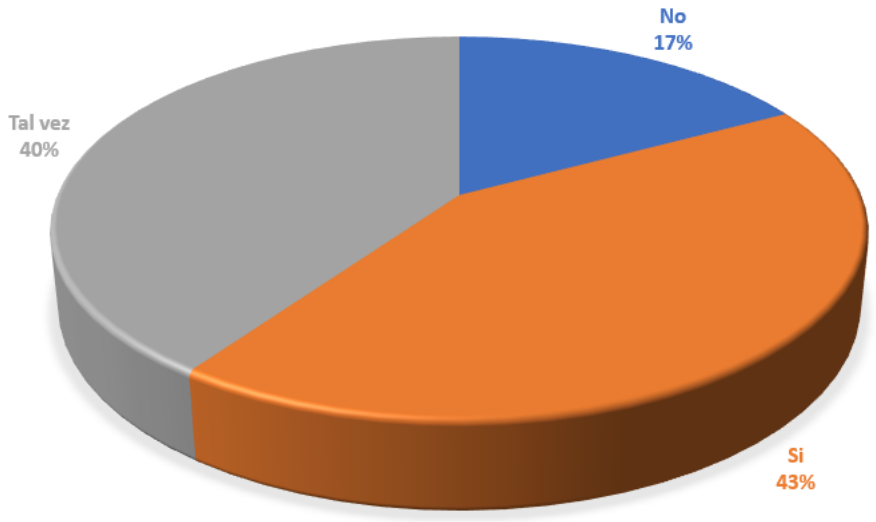

Gráfico N° 28. Aceptación para viajar en un coche automático sin conductor (en%). Encuesta on-line sobre uso de tecnología 2018. Elaboración propia.

Algo menos de la mitad (46%) indican que les gustaría viajar en un coche automático sin conductor, mientras que casi 2 de cada 10 rechazan la idea. Por otro lado, el 40%, aunque se mantiene en la duda, mencionó que tal vez lo haría. La seguridad con la que se pueda respaldar la venta este tipo de tecnología en los automóviles será vital para que pueda incorporarse al mercado. Basta recordar la experiencia comentada en el punto 5.3.4 acerca de cómo los expertos informáticos Charlie Miller y Chris Valasek, logran hackear y tomar el control remoto de casi todas las funciones de un vehículo Jeep, colocándolo en riesgo.

8. Descripción de los riesgos más relevantes de IoT

En esta sección se pretende mostrar los riesgos más relevantes que a través de nuestro análisis se han identificado y a los que se exponen las empresas y la población general al utilizar la Internet de las Cosas.

El desconocimiento y el poco entrenamiento sobre la seguridad de la IoT demuestran que hace falta un esfuerzo muy importante por parte de las empresas y en especial del gobierno sobre este tema. La innovación en materia de seguridad debe ser consecuente con el mismo avance de IoT, teniendo en cuenta que la ciberseguridad se ha convertido en un elemento central, tanto para compañías como para personas, y que son las últimas las más vulnerables.

En la siguiente tabla se pueden apreciar los diferentes riesgos, sus causas, vulnerabilidades y las posibles consecuencias a las que se está expuesto:

Tabla 3

Riesgos más relevantes de IoT.

Riesgos	Vulnerabilidad/Causa	Consecuencias
Violación a la privacidad e intimidad de la población en donde la información pueda tener un fin ilícito. Espionaje, fraude y acceso no autorizado colocando los derechos de las empresas y ciudadanos en cuanto al acceso y uso de sus datos debido a que no siempre se usan de forma autorizada y consentida Robo, perdida, divulgación o fuga de información empresarial y personal.	Poca o nula capacitación empresarial y de gobierno para la población sobre IoT que hacen exponer datos. Manuales de uso de los dispositivos IoT con poco o nulas recomendaciones de seguridad. Claves que el fabricante impone por defecto y que no se cambian y que los delincuentes conocen. Bajo nivel de autenticación a los dispositivos IoT que hacen que un delincuente pueda fácilmente obtener las credenciales de autenticación. Poco control con el manejo de datos personales que los expone en el ciberespacio. Suplantación de identidad que logran superar pruebas de	Perdidas económicas. Pérdida de credibilidad, de confianza y de imagen.

Riesgos	Vulnerabilidad/Causa	Consecuencias
	validación de los dispositivos IoT.	
	Poca estandarización y certificación de IoT que generan poca interoperabilidad en todos los sistemas a los que se conectan los dispositivos IoT.	Sanciones.
Daño a la Infraestructura Crítica (electricidad, agua y gas).		Perdida de bienes.
Uso abusivo de dispositivos IoT que sirvan para activar ciberataques, APTs y botnets.		Daño físico.
	Inexistencia de estándares de fabricación segura que permiten probar muchas variantes de ataques.	Detrimento del patrimonio.
Ataque de denegación de servicio distribuido (DDOS) que dejen por fuera servicios informáticos.		
	Poco o nulo monitoreo de dispositivos IoT con característica desatendida.	
Incremento de fallos al interconectar dispositivos con tecnologías incompatibles y en consecuencia incremento de costes para las organizaciones.		
	La Ciberseguridad no se contempla como una exigencia imprescindible para la innovación y el diseño de dispositivos IoT.	
Inexistencia de estándares de fabricación segura haciendo que los dispositivos IoT sean más vulnerables.		
	Vulnerabilidades no corregidas en un tiempo prudente por parte de fabricantes de IoT podrían permitir a un atacante tomar control de ciertos dispositivos de manera remota.	
	Las aplicaciones móviles que controlan los dispositivos IoT usados en casa no cifran o protegen los datos enviados a la nube.	
	Lanzar al mercado nuevos e innovadores productos en cortos lapsos de tiempo sin verificaciones de seguridad.	
	Inyección de código malicioso.	

Fuente: Elaboración propia.

9. Normatividad vinculada a la ciberseguridad en la Argentina

Según el National Cyber Security Index (NCSI) (2018), organismo que mide la preparación de los países para prevenir las amenazas cibernéticas y gestionar los incidentes cibernéticos, la Argentina, según este índice, se ubica en el puesto 66 con un puntaje de 36.36, entre 126 países y cuyo primer lugar es para Lithuania con 89.61 de puntaje.

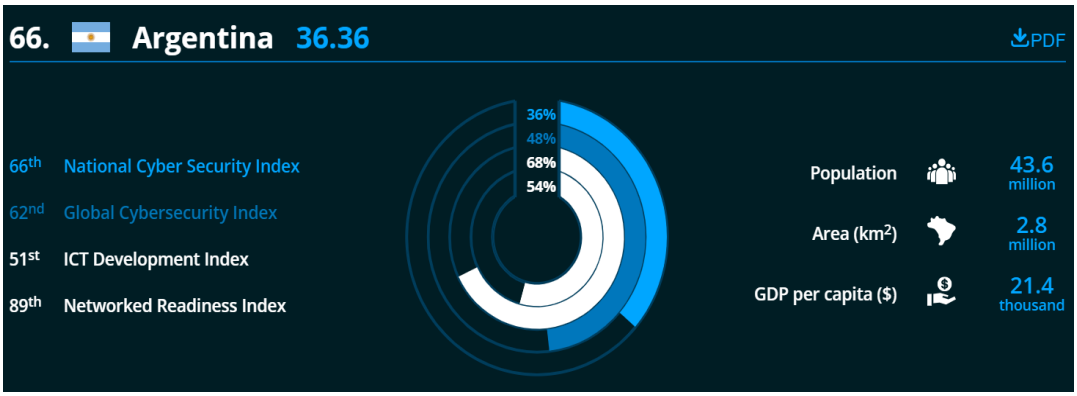

Figura 5. Estado de la Argentina a nivel de ciberseguridad según la NCSI. NCSI (2018). Tomado de https://ncsi.ega.ee/country/ar/

Sobre este punto y en lo que concierna al presente estudio, el país está muy por debajo, mostrándose con un 0% en nivel de desarrollo de políticas, 44% en educación profesional y 50% en respuesta ante incidentes. Sin embargo, ha avanzado mucho frente a la protección de datos personales que le colocan un 100%.

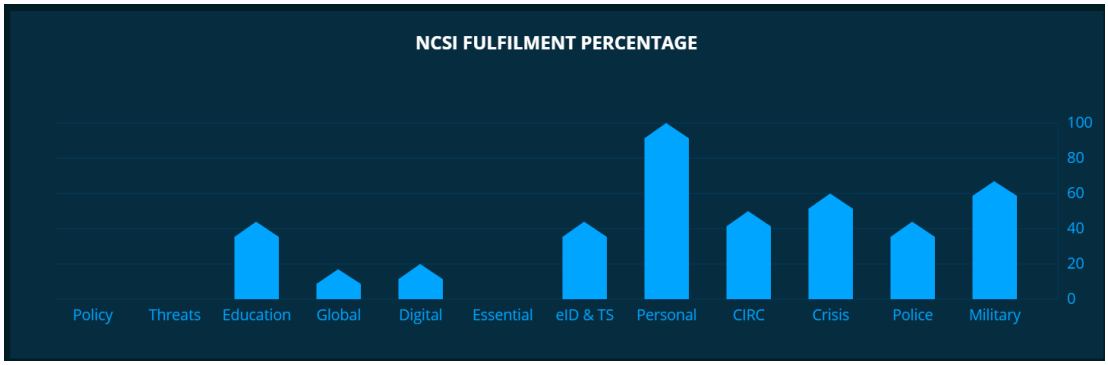

Figura 6. Porcentaje de cumplimiento de Argentina en materia de ciberseguridad, según la NCSI. NCSI (2018). Tomado de https://ncsi.ega.ee/country/ar/

La legislación argentina a nivel de ciberseguridad se muestra muy amplia, pero es lenta en su difusión dentro del territorio y su población. Destacamos las siguientes normas:

El Código Penal Argentino (Informatica legal, 2017) que, a través de su articulado, reúne y describe los principales delitos y conductas ilícitas que se refieren al tema de ciberseguridad de la siguiente forma:

- *Menores y pornografía infantil.* art. 128 (producción, distribución y tenencia de pornografía infantil), art. 131 (contacto a menores por medios electrónicos con una finalidad sexual -grooming-), art. 125 (corrupción de menores por medios digitales) y arts. 145 bis y 145 ter (trata de personas menores de edad).
- *Hostigamientos, discriminación y daños al honor.* art. 109 (calumnias o imputaciones falsas de un delito) y art. 110 (injurias).
- *Amenazas, extorsiones y chantajes.* art. 149 bis (delito de amenazas), art. 168 (delito de extoriones), art. 169 (delito de chantaje o amenaza de imputaciones contra el honor o violación de secretos).
- *Apología del crimen.* art. 213 (hacer pública la apología de un delito o de un condenado por delito).
- *Acceso ilegítimo a datos o sistemas (hacking) y daños informáticos (cracking).* art. 153 bis (acceso ilegítimo a un sistema o dato informático de acceso restringido), arts. 183 y 184 (daño, alteración o destrucción de datos, programas o sistemas).
- *Violación de comunicaciones electrónicas.* art. 153 (violación de comunicaciones electrónicas ajenas), art. 155 (violación de la privacidad de las comunicaciones electrónicas) y art. 197 (interrupción de comunicaciones electrónicas).
- *Estafas y defraudaciones informáticas.* art. 172 y 173, inc. 3, 8 y 16 (defraudación mutilando y ocultando expedientes o documentos digitales o manipulando el normal funcionamiento de un sistema informático o la transmisión de datos).

Decreto 577/2017 (Informatica legal, 2017)**.** Mediante este decreto se crea el comité de Ciberseguridad integrado por representantes de los ministerios de Modernización, Defensa y Seguridad y tendrá el objetivo de desarrollar una estrategia nacional de seguridad informática. De acuerdo con el texto oficial el Comité de Ciberseguridad cumplirá las siguientes tareas:

a) Desarrollar la Estrategia Nacional de Ciberseguridad, en coordinación con las áreas competentes de la Administración Pública Nacional.
b) Elaborar el plan de acción necesario para la implementación de la Estrategia Nacional de Ciberseguridad.
c) Convocar a otros organismos para que participen en la implementación de medidas en el marco del plan de acción elaborado conforme lo establecido en el punto b) precedente.
d) Impulsar el dictado de un marco normativo en materia de Ciberseguridad.
e) Fijar los lineamientos y criterios para la definición, identificación y protección de las infraestructuras críticas nacionales.
f) Participar en el desarrollo de acciones inherentes a la Ciberseguridad nacional que se le encomienden.

Ley 26.388/2008 de Delito informático (Informatica legal, 2017)**.** Esta ley contiene o incorpora al Código Penal (CP) delitos cometidos por medios informáticos, tales como delitos contra la integridad sexual, pornografía infantil, violación de secretos y de la privacidad, acceso a sistema informático, acceso a banco de datos, publicación de una comunicación electrónica, fraude informático y daño informático.

Ley 25.326/2000 de Protección de los Datos Personales (Informatica legal, 2017)**.** Tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean estos públicos o privados, o destinados a dar informes, para de esta forma garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional. Hay cuatro puntos importantes para tener en cuenta de esta ley:

1. Consentimiento de uso de datos personales.
2. Derecho de acceso, modificación y rectificación a los datos personales.
3. Transferencia internacional de los datos personales.
4. Seguridad, confidencialidad y cesión de los datos.

Ley 27.411/2017 Aprueba el convenio sobre ciberdelito del consejo de Europa *(Informatica legal, 2017).* Es el único acuerdo internacional que cubre todas las áreas

relevantes de la legislación sobre ciberdelincuencia (derecho penal, derecho procesal y cooperación internacional) y trata con carácter prioritario una política penal contra la ciberdelincuencia**.**

Ley 26.904 del Grooming (Informatica legal, 2017)**.** Establece el tratamiento de delitos contra menores y pornografía infantil a través de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos.

Ley 863 de la Legislatura de la Ciudad Autónoma de Buenos Aires (Informatica legal, 2017)**.** Establece que los establecimientos comerciales que brinden acceso a Internet deben instalar y activar filtros de contenido sobre páginas pornográficas.

Ley 2.257 del Gobierno de la Ciudad de Buenos Aires (Informatica legal, 2017). Aprueba el Convenio N° 14/04, "Convenio de Transferencia Progresiva de Competencias Penales de la Justicia Nacional al Poder Judicial de la Ciudad Autónoma de Buenos Aires".

Resolución 501/FG/12 de la Fiscalía General de la Ciudad Autónoma de Buenos Aires (Informatica legal, 2017), aprueba en calidad de prueba piloto la implementación del Equipo Fiscal "A" de la Unidad Fiscal, ente especializado en delitos y contravenciones informáticas, que actuará con competencia especial única en toda la Ciudad Autónoma de Buenos Aires.

Resolución PGN N° 3743/15. Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) (Ministerio Publico Fiscal, 2015). Fue creada por la Procuradora General de la Nación para enfrentar el fenómeno del cibercrimen de manera articulada con el resto de las áreas del organismo que se dedican a la investigación del crimen organizado.

Resolución 234/2016 del Ministerio de Seguridad (Informatica legal, 2017). Crea el Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la Investigación y Proceso de Recolección de Pruebas en Ciberdelitos.

Disposición 2/2013 de la Oficina Nacional de Tecnologías de Información (ONTI) (Informatica legal, 2017). Crea el grupo de trabajo "ICIC – CERT" (Computer Emergency

Response Team) en el marco del “Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad”.

Resolución 1046/2015 de la Jefatura de Gabinete de Ministros (Informatica legal, 2017). Establece la estructura organizativa de la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad.

Resolución PGN N° 2035/14 (Informatica legal, 2017) Procuración General de la Nación. Designa al “punto focal” de la Procuración General de la Nación en materia de ciberdelincuencia.

10. Propuesta y Plan de Acción

10.1. Propuesta

El desarrollo de una propuesta y plan de acción dirigidas a la población en materia de ciberseguridad con el uso de dispositivos de IoT, obedece a la creación de **buenos hábitos**. Esto se pudo notar cuando se evaluó el uso de contraseñas, en donde el 87% de la población encuestada afirmó utilizarlas y el 83.5% las cambia con frecuencia, lo que nos da un buen punto de partida.

Según Ortega (2014) la omisión es una de las mayores causales de los incidentes de seguridad y algunos de estas son de sentido común, consisten en algunos actos prudentes que la mayoría de las personas no tienen en cuenta y que dejan expuestas vulnerabilidades que se convierten en blancos fáciles para los delincuentes. Generar buenos hábitos requiere de paciencia y de seguir un buen plan. Un estudio británico llevado a cabo en el University College de Londres demostró que hacen falta 66 días para que se cree un hábito y pueda mantenerse durante años; sin embargo, se puede considerar que los hábitos a nivel de seguridad tecnológica pueden ser algo más complejos para aprenderlos bien. Slotnisky (2016) afirma que los hábitos se están digitalizando a un ritmo desenfrenado. Para Aristóteles, filósofo, lógico y científico de la Antigua Grecia, la excelencia no dependía de los actos de las personas sino de los hábitos, y vale recordar la frase de Charles C. Noble: “Primero hacemos nuestros hábitos, después nuestros hábitos nos hacen a nosotros.”

Para Duhigg (2015) hay tres elementos que forman el ciclo de un hábito: la señal, la rutina y la recompensa, que con el tiempo se vuelven cada vez más automático, y logran influir en individuos, organizaciones o sociedades.

La señal, es el detonante que informa a nuestro cerebro que puede poner el piloto automático y el hábito que ha de usar.

La rutina, que puede ser física, mental o emocional y establece que se desea modificar o generar.

La recompensa, que ayuda al cerebro a decidir si vale la pena recordar en el futuro este bucle en particular.

Por otro lado, la ciberseguridad se muestra como un desafío empresarial, de gobierno y social. Los nuevos gerentes deben mostrar su fuerte compromiso en las discusiones y actividades de ciberseguridad, sabiendo que hoy en día la transformación digital hace que las empresas tengan un fuerte desafío en Internet y más sobre IoT. “La transformación digital es de las personas no de la tecnología” (Slotnisky, 2016). Las decisiones de ciberseguridad tomadas por los equipos de seguridad pueden tener un impacto directo en las oportunidades y procesos de negocios.

Tomando en cuenta la matriz FODA, se establece la Fortaleza, la Oportunidad, la Debilidad y la Amenaza más relevantes de la Internet de las Cosas, a partir de los resultados de este trabajo, en donde la ciberseguridad es la principal debilidad de la tecnología IoT.

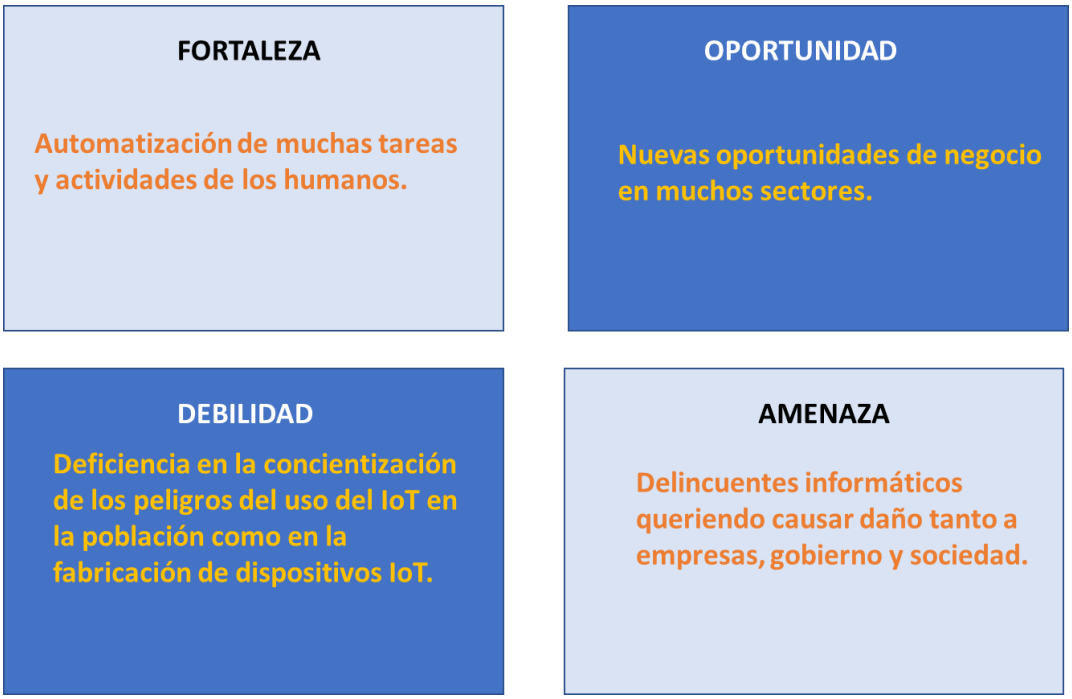

Figura 7. FODA según lo más relevante de IoT. Elaboración propia.

Otro punto para tener en cuenta en el plan de acción es que no solamente el Staff de una compañía debe estar incluido en materia de ciberseguridad, ahora todos deben ser parte, considerando que el **ser humano es la primera línea de defensa**. Recordemos que IoT es un todo conectado y esto implica que muy seguramente aquellos puestos de trabajo de apoyo como por ejemplo los del personal de limpieza, también necesiten de un entrenamiento sobre el manejo seguro de IoT, ya que en cierta medida las cosas que ellos manejan como bienes

de aseo puedan conectarse a Internet haciéndose riesgosos si no se manejan las precauciones necesarias.

Si bien es cierto que hay una amplia normativa de ciberseguridad en Argentina, existe poco despliegue entre la sociedad, así como el desconocimiento de la existencia de los centros de respuesta a incidentes de seguridad.

La propuesta en materia de ciberseguridad de IoT está basada principalmente sobre cuatro actores que deben participar para alcanzar un fin común: **la protección de las personas y del negocio a través del uso de la IoT**. Estos actores son gobierno, academia, empresa y sociedad.

En definitiva, más allá de las políticas, normas y leyes, la conciencia social debe enfocarse en programas de sensibilización que ayuden a generar hábitos y buenas prácticas desde la empresa, llevándola al hogar y por consiguiente a la comunidad.

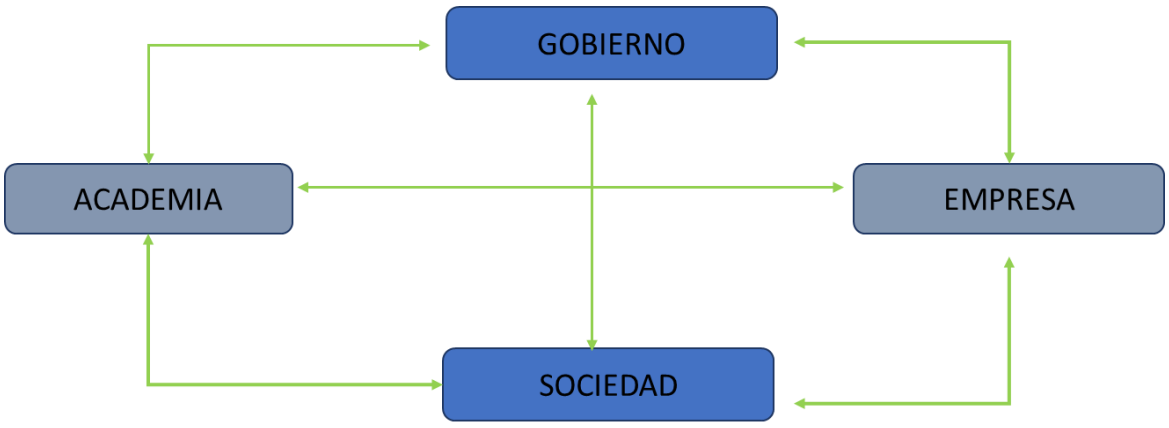

Figura 8. Estructura de Ciberseguridad de IoT enfocada a la generación de buenos hábitos y conciencia del uso de IoT. Elaboración propia.

Tareas que debe desempeñar el Gobierno:

- Definir las funciones y las responsabilidades de los distintos actores.
- La seguridad cibernética debe agregarse a la lista de prioridades.
- Crear un marco para el diálogo entre los distintos actores y la coordinación de diversas actividades emprendidas de la estrategia.
- Crear guías y campañas de concientización de IoT para establecer programas que lleguen a la sociedad, incluyendo la privacidad y protección de datos personales.

- Fomentar el uso de dispositivos de IoT que cumplan con estándares de seguridad adecuados.
- Fomentar el uso del Centro de Respuesta a Incidentes para aumentar la capacidad a nivel nacional.

***Tareas que deben desempeñar las Empresas*:**

- Compromiso de la Dirección con la Ciberseguridad y uso del IoT.
- Gerente estratégico de Ciberseguridad.
- Protocolo de Gestión de Riesgos.
- Programa de concienciación sobre IoT para todos los colaboradores para construir una cultura y hábitos sólidos de seguridad cibernética en la organización.
- Garantizar una configuración segura de dispositivos IoT (control de acceso).
- Gestión de incidentes.
- Monitoreo de sistemas y redes.

***Tareas que debe desempeñar la Academia*:**

- Formar nuevos líderes capaces de desempeñar roles gerenciales con proyectos innovadores en materia de IoT y ciberseguridad.
- Cooperar entre el sector público, el sector privado y la sociedad en la formulación de Cultura, Educación y Capacitación del buen uso de IoT.
- Impulsar la I+D+i para la investigación en seguridad cibernética.
- Educar a la sociedad civil para que pueda participar activamente en el desarrollo de las campañas de concientización.

***Tareas que debe desempeñar la Sociedad*:**

- Responsabilidad social compartida con los otros tres actores acerca del uso del IoT.
- Los programas de sensibilización deben adaptarse a los diferentes públicos dentro de la sociedad y deben incluir mensajes a todos los ciudadanos, incluidos los ciudadanos marginados.
- Tener una buena comprensión de los riesgos y amenazas, pero también de las oportunidades y beneficios del IoT para maximizar su uso.

- Campañas en diferentes idiomas, incluyendo la población indígena.

10.2. Plan de acción

Básicamente y de cara a lo que la población necesita, el plan de acción está basado sobre dos puntos fundamentales: Cultura, Educación y Capacitación de IoT, y la Capacidad de Respuesta a Incidentes Cibernéticos.

Cultura, Educación y Capacitación. Se deben desarrollar campañas que lleven mensajes de diferentes temáticas de IoT y Ciberseguridad para diversos grupos de la población de la Cuidad Autónoma de Buenos aires y GBA, desplegándose a través de los diferentes medios de comunicación (TV, Radio, diarios, etc.), con relativa **frecuencia** y buscando encontrar la formación cultural, mejores prácticas y **buenos hábitos** en materia de uso y seguridad de IoT. También será importante incluir avisos en las aplicaciones de IoT que informe riesgos y amenazas, como espionaje, privación a la intimidad y datos personales.

Se debe aprovechar y mantenerse actualizado el programa de capacitación como "Con Vos en la Web"[2], agregando temáticas sobre seguridad en IoT.

Todos los prestadores de servicios de Internet (ISP), en ingles Internet Service Provider, deben ser partícipes en la implementación de mensajes con buenas prácticas de ciberseguridad cuando se requiera acceso desde redes públicas, recordemos que el teléfono móvil será el control remoto de dispositivos IoT y que este intercambio de información entre este y el dispositivo debe ser consciente y seguro.

Capacidad de Respuesta ante Incidentes Cibernéticos. Si bien es cierto que actualmente la Ciudad Autónoma de Buenos Aires y el Gobierno cuentan con centros de respuesta ante incidentes cibernéticos, la falta de comunicación entre la población hace que su desconocimiento sea evidente y por ende no sabe a dónde acudir para denunciar un incidente en un momento dado.

[2] Para más información, visitar: https://www.argentina.gob.ar/justicia/convosenlaweb

Hay que fortalecer su despliegue y capacitación para mejorar los recursos técnicos y su infraestructura tecnológica para actuar más preventivamente frente a actos delictivos, teniendo en cuenta que el recurso humano es lo más importante. Luego es elemental que las empresas mantengan estos contactos a la mano y existan protocolos formales coordinados contra ciberataques de IoT para conducir a respuestas más oportunas y eficaces.

11. Conclusiones y reflexiones finales

La Internet de las Cosas es una realidad. La innovación y la transformación digital hacen que el uso de Internet sea diferente a como lo conocemos hoy en día. El avance tecnológico de Internet ha logrado que sus capacidades de velocidad y acceso aumenten rápidamente en poco tiempo y se extiendan a objetos, incluso de uso cotidiano, desde electrodomésticos hasta medios de transporte. IoT será parte de cambios disruptivos en la sociedad. Los nuevos hábitos o ciber hábitos, en lo digital, y las tendencias, hacen que la cantidad de tiempo que se pasa conectado a Internet también aumente, siendo el teléfono inteligente (Smartphone) el dispositivo estrella; además, será el control remoto desde donde se gestionen en gran medida los dispositivos IoT.

El Ciberespacio considerado el quinto elemento junto con la tierra, el agua, el aire y el espacio, elementos utilizados en disputas y confrontaciones, contiene una parte profunda (Deepweb) y es por allí por donde los delincuentes suelen operan. La innovación de IoT debe ir de la mano con la Ciberseguridad y el objetivo es encontrar el punto de equilibrio para que su uso sea confiable y seguro, tanto para las empresas, como para las personas.

La IoT contiene características que en cierta manera la hace mucho más vulnerable, por ejemplo, los objetos desatendidos, la movilidad, la interdependencia y lo ubicuo, pueden comprometer de alguna manera a la empresa y la sociedad, pues permite realizar ciberataques desde diferentes vectores, afectando desde la infraestructura crítica, la intimidad, la confidencialidad de información y los datos personales, generando riesgos.

El Darknet actuando en lo profundo de Internet está escondido para los usuarios, es decir, la población general que no es experta en tecnología digital, y que solo puede ver una pequeña parte.

El estudio arrojó que hay que trabajar en una estrategia orientada a la población. Tomando en cuenta esta premisa y considerando a las personas como la primera línea de defensa en el ciberespacio y la más vulnerable, la mejor estrategia frente al uso de IoT seguro, es la de generar buenos hábitos en materia de ciberseguridad (ciber-hábitos), con el objetivo de salvaguardar la vida y proteger la confidencialidad, la integridad y la disponibilidad de las cosas. A la población, en un gran porcentaje, le gusta la tecnología,

pero se deben considerar los riesgos de un mal uso de esta tecnología, por eso es necesario reflexionar y tomar medidas para evitar su materialización.

Dispositivos wearables, casas inteligentes, ciudades inteligentes, sensores de medio ambiente y aplicaciones de negocios estarán a la mano de las empresas y las personas. Hay que tener en cuenta que la IoT necesita un conjunto de componentes para operar, entre ellos la computación en la nube y las aplicaciones, para facilitar la interacción con las cosas que **s**erán fundamentales para almacenamiento, procesamiento de datos y acceso a una interfaz para configurar y administrar el producto IoT. Los fabricantes a falta de demanda muchas veces suelen concentrarse en implementar las funciones principales de los productos mientras ignoran la seguridad, no envían actualizaciones y parches a sus dispositivos a menos que las actualizaciones de firmware sean iniciadas por el usuario, y aquí la importancia de los ciber-hábitos.

Existe la necesidad de que los Centros de Respuesta a Incidentes y la regulación que ya opera en Argentina, y que de hecho es extensa, sea mejor desplegada a la población, de una manera más didáctica y amena, se busca, como se ha mencionado, generar una cultura de buenas prácticas y hábitos de fácil absorción, comprensión y entendimiento. La seguridad y el ser humano siempre han estado relacionada, y con la IoT lo estarán mucho más, especialmente si tomamos la estrecha vinculación de protección con el hogar y la empresa.

Es importante que los nuevos líderes puedan generar una interconexión entre Empresa, Academia, Gobierno y Sociedad. La Maestría de Administración de Empresas de Base Tecnológica nos da un panorama fuerte, enfocándonos a cumplir con este objetivo. Estos cuatro actores no pueden trabajar por separado y cada uno tiene funciones y responsabilidades para la IoT y la ciberseguridad.

La transformación real se basa en cambios de actitud, de confianza y de innovar con seguridad. El plan de acción debe considerar dos puntos fundamentales que se deben introducir como parte de la vida de las personas, independientemente de su relación social y estado laboral: Cultura, Educación y Capacitación, y la Capacidad de Respuesta ante Incidentes Cibernéticos.

12. Referencias bibliográficas

Cámara Argentina de Internet (CABASE). (2017). *Estado de Internet en Argentina.* Recuperado de https://www.cabase.org.ar/wp-content/uploads/2017/09/CABASE-Internet-Index-II-Semestre-2017.pdf

Campanario, S. (16 de septiembre de 2017). La era de los "Cioto": llegan los nuevos gerentes de la inteligencia artificial. La Nación. Recuperado de https://www.lanacion.com.ar/2063399-la-era-de-los-cioto-llegan-los-nuevos-gerentes-de-la-inteligencia-artificial

Cendón, B. (16 de enero de 2017). *El Origen Del IoT* [Mensaje en un blog]. Bruno Cendón. Pensamiento y tecnología. Recuperado de http://www.bcendon.com/el-origen-del-iot/

Centro Criptológico Nacional (2018). *Ciberamenazas y Tendencias. Edición 2018.* Recuperado de https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2835-ccn-cert-ia-09-18-ciberamenzas-y-tendencias-edicion-2018-1/file.html

Department of the Army United States of America. (2016). *Joint publication 1-02. Department of Defense Dictionary of Military and Associated.* Recuperado de https://fas.org/irp/doddir/dod/jp1_02.pdf

Dinatale, M. (11 de febrero de 2018). Los hackeos aumentaron un 700% en Argentina y el gobierno aceleró el comando de ciberseguridad. Infobae. Recuperado de https://www.infobae.com/politica/2018/02/11/los-hackeos-aumentaron-un-700-en-argentina-y-el-gobierno-acelero-el-comando-de-ciberseguridad/

Duhigg, C. (2015). *El poder de los habitos.* Barcelona, España: Urano.

El Heraldo (2013). Los niveles de la red profunda [Figura]. Recuperado de https://www.elheraldo.co/infografias/los-niveles-de- la-internet-profunda-134361

Evans, D. (2011). *The Internet of Things. How the Next Evolution of the Internet is Changing Everything* . Recuperado de https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Facultat d'Informàtica de Barcelona (Universitat Politècnica de Catalunya). (s.f.). *Historia de Internet*. Barcelona, España: Retro informática. Recuperado de https://www.fib.upc.edu/retro-informatica/historia/internet.html

Galiana, P. (2017). *Conoce la historia de Internet desde su primera conexión hasta hoy*. Madrid, España: IEBSCHOOL. Recuperado de https://www.iebschool.com/blog/historia-de-internet-innovacion/

García, B. (17 de octubre de 2018). *La histórica relación entre la tecnológica y la seguridad del hogar* [Mensaje en un blog]. Blogthinkbig.com. Recuperado de https://blogthinkbig.com/iot-protegerte-ciberataques

Gartner (2018). Hype Cycle for Emerging Technologies, 2018 [Figura]. Recuperado de https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/

Gonzalez, I. (9 de febrero de 2018). *Usuarios de internet y redes sociales en el mundo en 2018*.Guatemala, Guatemala: Ilifebelt. Recuperado de https://ilifebelt.com/usuarios-internet-redes-sociales-mundo-2018/2018/02/

Gonzalez, J. M. (2016). *La cumbre de OTAN en Varsovia.* Recuperado de http://www.ieee.es/en/Galerias/fichero/docs_opinion/2016/DIEEEO79bis-2016_CumbreOTAN_Varsovia_Moliner.pdf

Gonzalez, M. (11 de abril del 2018). Qué ha pasado con Facebook: del caso Cambridge Analytica al resto de polémicas más recientes. Xataca. Recuperado de https://www.xataka.com/legislacion-y-derechos/que-ha-pasado-con-facebook-del-caso-cambridge-analytica-al-resto-de-polemicas-mas-recientes

Greenberg, A. (21 de julio de 2015). Hackers Remotely Kill a Jeep on the Highway—With Me in It. Wired. Recuperado de https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Informatica legal. (2017). *Observatorio Argentino de Legislación Informática (OALI)*. Ciudad Autónoma de Buenos Aires, Argentina: Informática legal. Recuperado de http://www.informaticalegal.com.ar/legislacion-informatica/

Lee, I. & Lee, K. (julio-agosto 2015). *The Internet of Things (IoT): Applications, investments, and challenges for enterprises*. Business Horizons. Volumen (58), 431-440. Recuperado de https://www.sciencedirect.com/science/article/pii/S0007681315000373#!

ISACA. (2017). *Cyber, security Fundamentals Study Guide, 2nd Edition*.

ISACA (2017) *Cybersecurity Fundamentals Study Guide, 2nd Edition. Principios o TRIADA de Seguridad de la Información* [Figura].

Jaimovich, D. (12 de marzo de 2018). El 30% de los argentinos no tiene acceso a internet y muchos de los que tienen no saben cómo usarla. Infobae. Recuperado de https://www.infobae.com/tecno/2018/03/12/el-30-de-los-argentinos-no-tiene-acceso-a-internet-y-muchos-de-los-que-tienen-no-saben-como-usarla/

Kemp, S. (30 de enero de 2018). Digital in 2018: world's internet users pass the 4 billion mark. We are social. Recuperado de https://wearesocial.com/blog/2018/01/global-digital-report-2018

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. Recuperado de https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

Lopes, I. (29 de agosto de 2014). *Guía definitiva para entender y protegerte de las APT*. Bratislava, República Eslovaca: We live security. Recuperado de https://www.welivesecurity.com/la-es/2014/08/29/guia-definitiva-entender-protegerte-apt/

marketingdirecto. (2013). *La gran evolución de internet desde su creación en 1969*. Madrid, España: Marketing directo. Recuperado de https://www.marketingdirecto.com/actualidad/infografias/la-gran-evolucion-de-internet-desde-su-creacion-en-1969

Martínez, E. M. (28 de febrero de 2011). *El origen de Internet*. Ciudad de Ensenada, México: Eveliux. Recuperado de http://www.eveliux.com/mx/El-origen-de-Internet.html

Ministerio Público Fiscal. (2015). *Unidad Fiscal Especializada en Ciberdelincuencia*. Ciudad Autónoma de Buenos Aires, Argentina: Ministerio Público Fiscal. Recuperado de https://www.mpf.gob.ar/ufeci/

Miniwatts Marketing Group. (2018). *Internet World Stats*. Recuperado de https://www.internetworldstats.com/stats.htm

Newman, L. H. (16 de abril del 2018). An Elaborate Hack Shows How Much Damage IoT Bugs Can Do. Wired. Recuperado de https://www.wired.com/story/elaborate-hack-shows-damage-iot-bugs-can-do/

NCSI (2018). Estado de la Argentina a nivel de ciberseguridad según la NCSI [Figura]. Recuperado de https://ncsi.ega.ee/country/ar/

NCSI (2018). Porcentaje de cumplimiento de Argentina según la NCSI [Figura]. Recuperado de https://ncsi.ega.ee/country/ar/

NIST. (2012). *Managing Information Security Risk* . Recuperado de https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf

Ortega, J. A. (2 de mayo del 2014). Prevención y seguridad: Cómo desarrollar buenos hábitos en seguridad. La Tribuna. Recuperado de http://www.latribuna.hn/2014/05/02/prevencion-y-seguridad-como-desarrollar-buenos-habitos-en-seguridad/

Panetta, K. (16 de agosto de 2018). *5 Trends Emerge in the Gartner Hype Cycle for Emerging Technologies, 2018*. Gartner. Recuperado de https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/

Pepper, C. (22 de octubre de 2018). Facebook Logins Sold for Cheap on the Dark Web. Dark Web News. Recuperado de https://darkwebnews.com/cyber-security/cheap-fb-login-sold-at-darknet/

Psicología en el Bolsillo. (2015). *Tipos de poder: 6 formas de influir en otros* [Mensaje en un blog]. Psicología en el Bolsillo. Recuperado de http://psicologiaenelbolsillo.com/tipos-de-poder-6-formas-de-influir-en-otros/

Rivero, R. (2002). Evolución de ARPANET/Internet. El Mundo Es. Recuperado de http://www.elmundo.es/imasd/docs/cursos/masterperiodismo/2002/rivero-master01-usa.html

Sanchez, A. S. (2015). *El Quinto Elemento: Espionaje, ciberguerra y terrorismo. Una amenaza real e inminente.* Barcelona, España: Deusto S.A.

Serna, C., (17 de marzo de 2016). El Internet de las cosas: invasión inminente. The objective. Recuperado de http://theobjective.com/investigations/el-internet-de-las-cosas-invasion-inminente/

Singer, P., & Friedman, A. (2013). *Cybersecurity and CyberWar - What everyone needs to know.* New York, EE. UU.: Oxford University Press.

Slotnisky, D. J. (2016). *Transformación Digital: cómo las personas y las empresas deben adaptarse a esta revolución.* Ciudad Autónoma de Buenos Aires, Argentina: Digital House.

Vazhnov, A., (2016). *La Red de Todo: Internet de las Cosas y el Futuro de la economía Conectada (Spanish Edition)* .

World Development Report. (2016). *Enabling digital development - Six digital technologies to watch.* Recuperado de http://documents.worldbank.org/curated/en/896971468194972881/310436360_201602630200216/additional/102725-PUB-Replacement-PUBLIC.pdf

Zhou, W., Zhang, Y., & Liu, P. (2018). *The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved.* IEEE Internet of Things Journal. 1-11. Recuperado de https://arxiv.org/ftp/arxiv/papers/1802/1802.03110.pdf

Zhou, Zhang & Liu (2018). IoT Features [Figura]. Recuperado de https://arxiv.org/ftp/arxiv/papers/1802/1802.03110.pdf.

Zulick, J. (16 de octubre de 2018). Heating industry turns up the temperature on PLC cybersecurity. Multibriefs: Exclusive. Recuperado de http://exclusive.multibriefs.com/content/heating-industry-turns-up-the-temperature-on-plc-cybersecurity/manufacturing

13. Anexos

Preguntas del sondeo realizado a la población utilizando Google Work Request

Genero *

- Masculino
- Femenino
- Otro

Edad *

- 15 a 19
- 20-29
- 30-39
- 40-49
- 50-59
- 60- 69
- 70 y más

Nivel de Estudios *

- ○ Sin estudios
- ○ Primario
- ○ Secundario
- ○ Terciario
- ○ Universitario
- ○ Posgrado

¿Usa Internet? *

- ○ Si
- ○ No
- ○ No tiene internet

¿Cuántas horas suele estar conectado a Internet en un día? *

- ○ 2 horas la menos
- ○ Entre 3 y 6 horas
- ○ Entre 7 y 12 horas
- ○ Más de 12 horas

¿Si NO tiene acceso Internet le afecta? *

- ○ Si
- ○ No
- ○ No sabe

¿Sabe qué es Internet de las cosas, cuya sigla es IoT *

- ○ Sí
- ○ No

Indique cuál de los siguientes conceptos sería el más adecuado para definir Internet de las cosas (IoT) *

- Una plataforma de servicios
- Conexión de cualquier cosa a Internet
- Un objeto de investigación
- Artículos para vender por Internet
- Definitivamente NO sabe

¿Qué tipo de cambio cree que va a traer Internet de las Cosas? *

- Positivo
- Negativo
- No sabe

¿Tiene algún dispositivo como Televisor, consola de videojuegos conectado a Internet? *

- Sí
- No
- No sabe

¿Conectaría o tiene conectado a Internet objetos como heladera, climatización, cámaras, etc. para poder manejarlos a distancia? *

- Si
- No
- Tal vez
- No Sabe

¿Le parece interesante poder manejar desde su celular los electrodomésticos o dispositivos de su hogar? *

- Muy interesante
- Algo interesante
- Poco interesante
- Nada interesante

Utiliza contraseñas u otros mecanismos de acceso a su celular? *

- Sí
- No

¿Con qué frecuencia cambia sus contraseñas en general? *

- Cada mes o menos
- Cada 2 a 6 meses
- Cada 6 a 12 meses
- Cuando el dispositivo me lo recuerda
- Nunca

¿Le preocupa la seguridad y privacidad de sus datos en Internet? *

- Sí
- No

¿Se ha sentido espiado o vigilado a través de su celular u otro dispositivo? *

- Sí
- No

¿Cuándo utiliza el celular, que usa más? *

- Aplicaciones
- Navegadores
- Ninguna

¿Acepta realizar actualizaciones a sus aplicaciones? *

- Sí
- No
- No sabe

¿Conoce alguna política de Gobierno respecto a Ciberseguridad? *

- Sí
- No

¿Sabe donde reportar algún incidente de Ciberseguridad? *

- Sí
- No

Pensando en el futuro ¿Aceptaría viajar en un coche automático sin conductor? *

- Sí
- No
- Tal vez

¿Actualmente esta trabajando? *

- Sí
- No

Section 2 of 4

Section title (optional)

Description (optional)

¿Qué tipo de empresa es? *

- Pública
- Privada
- No sabe

¿Su empresa tiene políticas de Ciberseguridad? *

- Sí
- No
- No sabe

¿Sabe donde reportar algún incidente de Ciberseguridad en su empresa? *

- Sí
- No

Section 3 of 4

Para terminar

Description (optional)

¿Señale el lugar donde vive? *

- En Capital Federal
- En el Gran Buenos Aires
- En otra ciudad de la Provincia de Buenos Aires
- En otra Provincia Argentina
- En otro país

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

Solicitud de constitución de Jurado para Defensa del TRABAJO FINAL DE MAESTRÍA	Código de la Maestría
Nombre y apellido del alumno JEIVER ERNESTO RAMIREZ NARVAEZ	Tipo y N° de documento de identidad DNI - 95.731.284
Año de ingreso a la Maestría – Ciclo 2017	Fecha de aprobación de la última asignatura rendida

Título del Trabajo Final

Ciberseguridad y Conciencia Social del Internet de las Cosas

Solicitud del Director de Trabajo Final

Comunico a la Dirección de la Maestría que el Trabajo Final bajo mi dirección se encuentra satisfactoriamente concluido. Por lo tanto, solicito se proceda constituir el correspondiente Jurado para su evaluación y calificación final.

Firma del Director de Trabajo Final ……

Aclaración……

Lugar y fecha……

Datos de contacto del Director

Correo electrónico	Teléfonos
mbilelloarg@yahoo.com.ar	+5491153385049

Se adjunta a este formulario:

- Trabajo Final de Maestría impreso (2 copias)
- CD con archivo del Trabajo Final en formato digital (versión Word y PDF)
- Certificado analítico

Fecha	Firma del alumno

Form. TFM v0

PRESENTAR EN LA RECEPCIÓN DE LA ESCUELA DE ESTUDIOS DE POSGRADO