


UNIVERSIDAD CENFOTEC

MAESTRÍA EN CIBERSEGURIDAD

DOCUMENTO FINAL DE PROYECTO DE INVESTIGACIÓN APLICADA 2

# EVALUACIÓN DE LA EFECTIVA APLICACIÓN DE LA LEGISLACIÓN COSTARRICENSE EN EL DESARROLLO DE PROYECTOS IOT PARA DIMENSIONAR SUS REPERCUSIONES EN LA CIBERSEGURIDAD Y PRIVACIDAD DE LOS DATOS.

LEITÓN ÁLVAREZ YULIANA

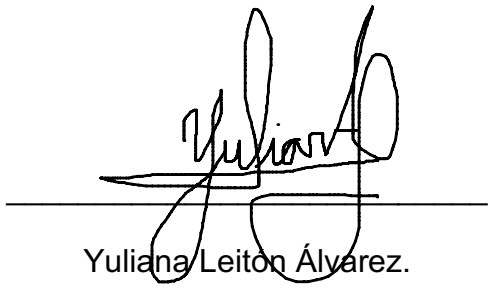
ABRIL, 2018



## Declaratoria

La suscrita; Yuliana Leitón Álvarez, soltero, con cédula de identidad N.1-1492-0953, en este acto debidamente apercibido y consiente de las penas y consecuencias que se castiga el delito de perjurio, declaro que la tesis **"Evaluación de la efectiva aplicación de la legislación costarricense en el desarrollo de proyectos IoT para dimensionar sus repercusiones en la ciberseguridad y privacidad de los datos"**, es una obra original que ha respetado lo preceptuado por las leyes penales, así como la ley de derecho del autor y derechos conexos y sus reformas. Así mismo, autorizo a la Universidad Cenfotec la consulta y uso con fines exclusivamente académicos.

En fe de lo anterior firmo en San José, a los xx días del mes de marzo de dos mil diesciocho.



Yuliana Leitón Álvarez.

Cédula Nº 1-1492-0953



## Agradecimiento

En primera instancia le doy infinitas gracias a Dios por permitirme cumplir esta meta y dirigirme el camino en todo momento para lograr finalizar con éxito este proyecto personal, además de todas esas bendiciones que acompañaron este proceso como lo fue la beca otorgada por la OEA para especializarme en ciberseguridad.

Agradezco a cada uno de los profesores de la Universidad Cenfotec, quienes se esforzaron en sus lecciones para trasmitirnos el conocimiento profesional y sus experiencias laborales. Al igual que a todo el personal de la universidad, les agradezco por velar por el bienestar estudiantil y el apoyo durante todos estos años.

Le doy las gracias a mi tutor don Claudio porque sus lecciones siempre fueron de gran aprecio para mi carrera profesional, además por brindarme su apoyo en este proceso tan importante en mi vida.

Por otra parte le doy gracias a mis compañeros Juan Diego y Bernal porque en ellos encontré un gran equipo de trabajo durante estos dos años. Al igual que a mis compañeros de Intel porque siempre encontré en ellos un apoyo en cuanto conocimiento y tiempo.

Por último les doy las gracias a mi familia porque su apoyo siempre ha sido incondicional y se que sin sus palabras de aliento, ánimo y amor el camino no hubiese sido tan fácil. Ustedes (mami, papi, Fran y Tony) son mi pilar mas fuerte para ser una mejor persona, una mejor profesional y una mejor mujer.



## Dedicatoria

Le dedico esta tesis a todas aquellas mujeres que se esfuerzan día con día para poder encajar de forma profesional en el área de las ingenierías, especialmente en el mundo informático, las insto a que nunca se rindan en el camino, a que cumplan sus sueños, a marcar la diferencia, a brillar en todo momento y a que nunca dejen de soñar, así como lo hizo Ada Lovelace madre de la programación informática y nominada como la primera programadora, Frances E Allen pionera en la automatización de tareas paralelas, Grace Murray H desarrolladora del primer compilador para un lenguaje de programación, Lynn Conway pionera en el campo de diseño de chips microelectrónicos, Evelyn Berezin desarrolladora del primer sistema de reserva de vuelos, Jude Milhon creadora del ciberpunk, programadora y defensora de los ciberderechos y Heydy Lamarr inventora de la tecnología precursora del GPS, Wifi y Bluetooth.

Por otra parte le dedico esta tesis a mi familia, a mi mamá porque es una mujer excepcional, brillante y que siempre me insta a cumplir cada uno de mis sueños, a mi papá, un hombre creativo, lleno de talento y de amor por las personas me anima a seguir adelante y ser mejor persona cada día, a mi hermana porque aunque es más joven me enseña a que la dedicación siempre es fundamental para cumplir los sueños y por último a mi novio Tony porque es un hombre brillante lleno de grandes talentos y amor, siempre me anima a seguir adelante, a luchar por mis sueños y jamás rendirme. Los amo infinitamente y siempre serán mi mayor regalo.

# Tabla de Contenidos


Capítulo I ..... 12
Introducción ..... 12
1.1 Generalidades ..... 13
1.2 Antecedentes del problema ..... 13
1.3 Definición y descripción del problema ..... 16
1.4 Justificación ..... 18
1.5 Viabilidad ..... 21
1.5.1 Punto de vista técnico ..... 22
1.5.2 Punto de vista operativo ..... 22
1.5.3 Punto de vista económico. ..... 22
1.6 Objetivos ..... 23
1.6.1 Objetivo general ..... 23
1.6.2 Objetivos específicos ..... 23
1.7 Alcances del estudio ..... 23
1.7.1 Alcances ..... 23
1.7.2 Limitaciones ..... 24
Capítulo II ..... 26
Marco Teórico ..... 26
2.1 Evolución de la seguridad ..... 27
2.2 Seguridad ..... 30
2.2.1 Seguridad de la información ..... 30
2.2.2 Vulnerabilidad (Vulnerability) ..... 32
2.2.3 Amenaza (Threat) ..... 33
2.2.4 Riesgo ..... 34
2.3 Internet de las Cosas (Internet of Things) ..... 35
2.3.1 Antecedentes de IoT ..... 35
2.3.2 IoT en la actualidad ..... 40
2.3.2.1 ¿Tiene Costa Rica edificios inteligentes? ..... 45
2.3.2.2 Edificios inteligentes internacionales ..... 48
2.4 Aspectos legales ..... 55

2.4.1 Procedencia de la protección de datos personales ..... 56
2.4.2 Recorrido por la legislación internacional ..... 58
A. Europa ..... 58
B. Canadá: ..... 66
C. Estados Unidos ..... 74
2.4.3 Comparación del proceso de protección de datos personales en Europa, Estados Unidos y Canadá ..... 95
2.4.4 Protección de datos en América Latina ..... 100
2.4.5 Principio de la Organización de las Naciones Unidas (ONU) ..... 102
2.4.6 Principio de la Organización de Estados Americanos (OEA) ..... 105
2.4.7 Tratamiento de datos personales en Costa Rica ..... 106
2.4.8 Habeas data en Costa Rica ..... 107
2.4.8.1 Regulación normativa antes de la Ley No.8968 ..... 107
2.4.8.2 Regulación de los delitos informáticos en Costa Rica ..... 111
2.4.9 Creación de la Agencia para la Protección de los Datos Personales (Prodhab) 116
2.4.9.1 Naturaleza jurídica ..... 116
2.4.9.2 Funciones y alcance ..... 117
2.4.10 ¿Hacia dónde se dirige? ..... 121
2.4.10.1 Impacto de IoT ..... 121
2.4.10.2 Impacto de IoT en las personas ..... 124
2.4.10.3 Modelos de negocio ..... 125
2.4.10.4 Impacto en la consumición de recursos ..... 127
2.4.10.5 Factores que decidirán el futuro de IoT ..... 128
2.4.10.6 Obstáculos de IoT ..... 129
2.4.10.7 ¿Quién y dónde se dará el primer paso? ..... 132
2.4.10.8 Aplicaciones de IoT con análisis en la seguridad ..... 136
2.4.10.9 Tecnologías con las que trabaja IoT ..... 143
2.4.11 Amenazas que enfrenta IoT ..... 146
2.4.11.1 Seguridad ..... 146
2.4.11.2 Pilares de seguridad para IoT ..... 148

2.4.11.3 Seguridad en la transmisión de datos....149
*2.4.11.4* Seguridad en el *software*....151
2.4.11.5 Seguridad en la configuración y funcionalidad....152
*2.4.11.6* Seguridad en el *hardware*....153
2.4.11.7 Seguridad en los usuarios....155
Capítulo III....157
Referencias Bibliográficas....157
3.1 Estado de la cuestión....158
Capítulo IV....163
Marco Metodológico....163
4.1 Tipo de Investigación....164
4.2 Alcance investigativo....164
4.3 Enfoque....165
4.4 Diseño....166
4.5 Población y muestreo....166
4.6 Instrumentos de recolección de datos....167
4.7 Técnicas de análisis de información....167
4.8 Variables....167
4.8.1 La efectiva aplicación de la legislación costarricense en el desarrollo de proyectos IoT....168
4.8.2 Repercusiones en la seguridad y privacidad de los datos....169
4.8.3 Los riesgos que implican la incorporación de IoT y las acciones que afectan la privacidad de los datos....170
4.8.4 Las leyes y reglamentos en Costa Rica protegen la seguridad y privacidad de la información....170
4.8.5 Los agujeros de seguridad en los dispositivos que conformarán la gran red de IoT....171
4.8.6 El manejo de la información por parte de los usuarios y en las empresas....172
Capítulo V....173
Análisis de Información....173
5.1 Análisis e interpretación de resultados....174

3.2 Análisis de las Variables en Estudio....174
5.1.1 Análisis de la Variable #1....175
Gráfico #1....175
Gráfico #2....176
Gráfico #3....177
Gráfico #4....177
Gráfico #5....178
Gráfico #6....179
Gráfico #7....180
Gráfico #8....182
Gráfico #9....182
Gráfico #10....183
Gráfico #11....183
Gráfico #12....184
Gráfico #13....185
5.1.2 Análisis de la Variable #2....186
Gráfico #14....186
Gráfico #15....187
Gráfico #16....187
Gráfico #17....188
Gráfico #18....188
Gráfico #19....189
Gráfico #20....190
Gráfico #21....190
Gráfico #22....191
Gráfico #23....192
Gráfico #24....192
Gráfico #25....193
Gráfico #26....193
Gráfico #27....194
5.1.3 Análisis de la Variable #3....195

Gráfico #28 ..... 195
Tabla #1 ..... 196
Gráfico #29 ..... 197
Gráfico #30 ..... 197
Gráfico #31 ..... 198
Tabla #2 ..... 199
Gráfico #32 ..... 200
Gráfico #33 ..... 201
Gráfico #34 ..... 201
Gráfico #35 ..... 202
Gráfico #36 ..... 202
Gráfico #37 ..... 203
Gráfico #38 ..... 203
Gráfico #39 ..... 204
5.1.4 Análisis de la Variable #4 ..... 204
Gráfico #40 ..... 205
Gráfico #41 ..... 206
Gráfico #42 ..... 206
Gráfico #43 ..... 207
Gráfico #44 ..... 208
Gráfico #45 ..... 209
Gráfico #46 ..... 210
Gráfico #47 ..... 211
Gráfico #48 ..... 212
5.1.5 Análisis de la Variable #5 ..... 213
Gráfico #49 ..... 213
Gráfico #50 ..... 214
Gráfico #51 ..... 214
Gráfico #52 ..... 215
Gráfico #53 ..... 216
Gráfico #54 ..... 216

Gráfico #55 ..... 217
5.1.6 Análisis de la Variable #6 ..... 218
Gráfico #56 ..... 218
Gráfico #57 ..... 219
Gráfico #58 ..... 219
Gráfico #59 ..... 220
Gráfico #60 ..... 220
Gráfico #61 ..... 221
Gráfico #62 ..... 221
Gráfico #63 ..... 222
Gráfico #64 ..... 222
Gráfico #65 ..... 223
Gráfico #66 ..... 224
Gráfico #67 ..... 224
Gráfico #68 ..... 225
Gráfico #69 ..... 226
Capítulo VI ..... 227
Conclusiones y Recomendaciones ..... 227
6.1 Conclusiones y recomendaciones ..... 228
6.1.2 Conclusiones ..... 228
6.1.2 Recomendaciones ..... 254
Capítulo VII ..... 260
Referencias Bibliográficas ..... 260
7.1 Bibliografía ..... 261
Capítulo VIII ..... 270
Anexos ..... 270

# Lista de Figuras

Ilustración 1. Tríada (Confidencialidad-Integridad-Disponibilidad). INFOSEGUR .....31
Ilustración 2. Amenazas. (Prandini & Pallero, 2013) .....34
Ilustración 3. Internet en 2017. Pronóstico de Cisco Virtual Networking Index.....42
Ilustración 4. Internet en 2017. Pronóstico de Cisco Virtual Networking Index.....43
Ilustración 5. Unidades de internet de las cosas por categoría (Millones). Gartner (noviembre 2014) .....123
Ilustración 6. Usuarios activos mensuales en las redes sociales. Statista.....133
Ilustración 7. Distribución por países del impacto en los sectores de IoT. Fundación de innovación Bankinter .....134
Ilustración 8. Ataques a la tecnología de IoT. J.D. King .....135
Ilustración 11. seguridad + privacidad + IoT. Propia.....158
Ilustración 12. seguridad + privacidad + ataques +IoT. Propia.....159
Ilustración 13. seguridad + privacidad + ataques +IoT + Costa Rica. Propia .....160
Ilustración 14. seguridad + privacidad + ataques +IoT + leyes en Costa Rica. Propia 161
Ilustración 15. seguridad + privacidad + ataques +IoT + legislación costarricense. Propia .....162

# Capítulo I

# Introducción

## 1.1 Generalidades

Para comprender de forma clara la investigación, es importante tomar en cuenta las siguientes abreviaturas:

**IoT:** Internet de las cosas (Internet of Things)

**PRODHAD:** Agencia de Protección de Datos de los Habitantes

**CIA:** Confidencialidad, integridad y disponibilidad

**TI:** Tecnologías de información

**TFG:** Trabajo Final de Graduación

**CSC:** Centro de Ciberseguridad

## 1.2 Antecedentes del problema

Desde la consolidación de Internet como medio de interconexión global, los incidentes de seguridad relacionados con sistemas informáticos vienen incrementándose de manera alarmante. Este hecho, unido a la progresiva dependencia de la mayoría de organizaciones hacia sus sistemas de información, viene provocando una creciente necesidad de implantar mecanismos de protección que reduzcan al mínimo los riesgos asociados a los incidentes de seguridad.

El cambio constante y rápido es considerado una clave esencial en la informática y la tecnología por lo que consecuentemente es indispensable la adaptación continua, pero ¿se encuentra la sociedad lista para la incorporación de nuevas tecnologías? ¿Se cuenta con sistemas y leyes de protección atinentes?

Al incorporar el tema del Internet de las Cosas o IoT, se forma un nuevo paradigma de investigación que pone en actualización una serie de temas y aspectos

importantes para la sociedad. El tema central de incertidumbre es la seguridad, un punto esencial y con gran trascendencia en el tema de riesgos, pero al mismo tiempo abre una gran posibilidad a la incorporación de leyes y reglamentos que Costa Rica tiene pero que los usuarios desconocen, es por ello que este trabajo de investigación pretende aclarar la posibilidad de implementar nuevas soluciones e integración de la tecnología con las normativas del país.

Vargas 2016, citando a la Consultaría Internacional Gartner, señala que para el 2020 existan 25.000 millones de dispositivos conectados a Internet.

De acuerdo con la revista Costa Rica 2050:

“En el año 2007 el Parlamento Europeo votó por unanimidad enrumbarse hacia la Cuarta Revolución Industrial sobre el lomo de Internet de las Cosas, IoT, el nuevo tsunami tecnológico que revolucionará al mundo. Estados Unidos y China también se montaron en esta locomotora de cambio y de innovación. Sin embargo, en la mayoría de los países en vías de desarrollo, incluyendo Costa Rica, el tema apenas comienza a mostrar su gigantesco potencial.” (Madrigal, 2016)

Con base en la misma revista se aseguró que “el Consorcio de IoT, es el primer ladrillo de lo que debería ser una “estrategia país” orientada a conformar un Ecosistema de Innovación que le permita a Costa Rica insertarse con éxito en la Cuarta Revolución Industrial que emerge de la mano de Internet de las Cosas.” (Madrigal, 2016)

Para describir sobre las políticas y normativas relacionadas con seguridad, se hace un llamado a la norma ISO 27001 la cual se relaciona con la política de seguridad informática.

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada con base en la norma británica BS 7799-2.

Por lo tanto, la Norma ISO 27001 establece lo siguiente:

1. La política tiene que adaptarse a la empresa, esto significa que no puede simplemente copiar la política de una gran organización y utilizarlo en una pequeña organización de TI.
2. Es necesario definir un marco para establecer todos los objetivos de seguridad de la información, la política debe definir cómo se proponen los objetivos, la forma en la que se encuentran aprobados y la manera en la que se revisan.
3. La política tiene que mostrar el compromiso de la alta dirección para cumplir con los requisitos de todas las partes interesadas y mejorar de forma continua el Sistema de Gestión de Seguridad de la Información, eso se hace normalmente mediante un tipo de declaración dentro de la política.
4. La política se debe comunicar dentro de la organización y a todas las partes interesadas, la mejor práctica es definir quién es el responsable de tal comunicación, y entonces esa persona se encarga de hacerlo de forma continua.

5. La política debe ser revisada de forma continua por parte del propietario de una política que debe ser definida. Dicha persona será la responsable de mantenerla hasta la fecha.

Las políticas anteriores, ayudarán a enfocar el trabajo de investigación para que pueda cumplir con lo que solicita la norma y sea parte del cumplimiento de gestionar la seguridad de la información.

Es importante dar a conocer qué leyes y reglamentos tiene Costa Rica para velar por la protección de los datos, como lo es la Agencia de Protección de Datos de los Habitantes (PRODHAB), la cual es una institución de desconcentración máxima adscrita al Ministerio de Justicia y Paz, con independencia de criterio y personalidad jurídica instrumental propia en el desempeño de las funciones y en la administración de sus recursos y presupuesto, así como para suscribir los contratos y convenios que requiera para el cumplimiento de sus funciones.

## 1.3 Definición y descripción del problema

Los delitos informáticos se producen sin duda en un momento en que el mundo vive, más que nunca, dramáticos cambios en materia de tecnología que impactan drásticamente todos los aspectos de las relaciones humanas. Esto proyecta una sociedad de enormes oportunidades, pero también de grandes retos.

El problema de esta investigación radica en la falta de mecanismos de protección para la incorporación y uso del IoT, generando peligros para los usuarios y empresas en Costa Rica. Es por ello, por lo que es fundamental concientizar y dar a

conocer cómo la legislación costarricense puede asegurar la confidencialidad de los datos desde un ámbito legal junto con el de ciberseguridad.

Existen leyes y normativas que permiten las regulaciones sólidas en las cuales se promueve la compresión de la ciberseguridad y crean métodos de defensa y protección contra las constantes amenazas, sin embargo, los usuarios y empresas desconocen de estos reglamentos, aun cuando no es posible alegar ignorancia ante la ley.

El IoT sin duda alguna ha creado métodos y oportunidades de innovación, pero hasta este momento no se ha enfatizado en el aspecto más importante: la seguridad; misma que no solo se trata de la privacidad de los datos, se trata de la identidad digital puesto que los próximos años la tecnología va a formar parte del día a día, controlando e interactuando la red con nosotros en busca de la información.

El uso indebido de las bases de datos que almacenan una gran cantidad de información personal destaca un gran riesgo a nivel de ciberdelitos y para enfrentar este tipo de problemas se deben de desarrollar herramientas legales que se enfoquen en regular el uso que se le da a Internet de esta forma se crea una cultura digital más robusta y precisa.

Como cita el abogado Juan Ignacio Zamora en la revista Pensis- TEC Costa Rica (2017):

“Los datos, tanto personales como empresariales, se convirtieron en oro”, qué afirmación tan cierta, proteger los datos actualmente representa uno de los retos más importantes.

De igual forma afirma: “Regular Internet es tratar de regular un monstruo de mil cabezas; es muy difícil, entre otras cosas, porque existen grandes problemas que abordar, como la jurisdicción bajo la cual se debe enfrentar este tipo de problemas y que la tecnología siempre va por delante de la ley. Por eso es mejor prevenir y usar Internet responsablemente”. (Zamora, 2017)

Desafortunadamente, en ocasiones se ve a la seguridad informática como algo que dificulta la consecución de los propios objetivos de la organización, imponiendo normas y procedimientos rígidos a los usuarios, desarrolladores, a los sistemas y a los gestores. Sin embargo, debe verse la seguridad informática, no como un objetivo en sí mismo, sino como un medio de apoyo a la consecución de la protección de la información.

## 1.4 Justificación

La nueva era tecnológica muestra un mundo virtual absolutamente interdependiente con el mundo real, del cual se depende cada vez más. El ciberespacio es real y reales son también los riesgos que vienen con él. Dependemos de la Internet cada vez más para hacer las transacciones bancarias, pagar recibos, hacer compras, trabajar y gozar de ratos de ocio y eso es aprovechado por algunos para sacar ventajas ilegítimas.

La protección de los sistemas y de la información no suele eliminar completamente la posibilidad de que estos bienes sufran daños. En consecuencia, los gestores deben implantar aquellas medidas de seguridad que lleven los riesgos hasta niveles aceptables, contando para ello con el coste de las medidas por implantar, con el

valor de los bienes por proteger y con la cuantificación de las pérdidas que podrían derivarse de la aparición de determinado incidente de seguridad.

De acuerdo con la constante evolución y actualización de tecnología, uno de los factores de preocupación que surge, es la seguridad informática que marca una pauta en el Internet de las Cosas, debido a que es una tendencia donde los dispositivos no solo se van a conectar a la red, sino que se comunican entre ellos mismos y con las personas.

Con base en un estudio realizado en el 2015 por Hewlett-Packard, se evaluaron 10 dispositivos IoT como televisores, cámaras web, tomas corrientes, termostatos, controladores de riesgo, alarmas, cerraduras de puertas, entre otros. Esta investigación indicó que el 90% de los dispositivos recolectaban datos de las personas, 70% se conectaban a servicios de la red no encriptados y el 80% mostraba problemas de seguridad. Estos resultados son alarmantes porque se está indicando que solo el 20% de los datos no mostró problemas de seguridad, esto es preocupante debido a que perfectamente podrían ser presa fácil de los cibercriminales y ¿quién se va a hacer responsable de estos delitos?, la respuesta actualmente es: “el usuario es responsable de proteger su propia información”, sin embargo, tanta responsabilidad tiene el usuario como los desarrolladores de tecnologías IoT.

Es importante e indispensable que el usuario se asegure de que los aparatos codifiquen y disfracen la información para que estén delimitados por una contraseña.

Por otra parte, entidades como la PRODHAB pretenden actualizar la normativa costarricense sobre Protección de Datos Personales a la corriente de tendencias internacionales en la materia, a través de la aclaración de aspectos que en su momento

suscitaron inquietudes respecto a la Ley y su aplicación, así como coadyuvar a las instituciones públicas y privadas a cumplir con las garantías, derechos otorgados y la simplificación de los trámites que corresponden, garantizando mayor fluidez en la transferencia y comercialización de datos, mejor control y competencia en la protección de datos personales. Esto surge debido a que los creadores de aplicaciones y dispositivos IoT, no velan por la protección de la seguridad desde el primer momento.

Denise Giusto, investigadora de ESET Latinoamérica, afirmó que:

"A veces, se liberan las tecnologías antes de saber si son seguras, entonces, ¿qué sucede? Se deja la puerta abierta a un montón de amenazas que podrían terminar afectando a los usuarios y más si en esas tecnologías se ven incluidas tarjetas de pago o transacciones electrónicas". (2016)

Los efectos de las diversas amenazas puedes ser muy variados. Unos pueden comprometer la integridad de la información o de los sistemas, otros pueden degradar la disponibilidad de los servicios y otros pueden estar relacionados con la confidencialidad de la información. En cualquier caso, una correcta gestión de los riesgos debe implicar un profundo conocimiento de las vulnerabilidades de los sistemas y de las amenazas que los pueden explotar, además de una correcta gestión de las leyes y reglamentos.

Las propias características de las organizaciones deben influir en las medidas de seguridad que resulten más adecuadas y más eficientes en términos de costes, para contrarrestar las amenazas o incluso para tolerarlas conociendo en todo caso sus implicaciones, así como sus deberes en el momento de implementación.

Esta investigación encuentra la justificación principal en analizar que los avances tecnológicos y sobre todo el IoT, base de este trabajo, brinde a las empresas los beneficios para los cuales fueron creados y se minimice por medio de la legislación costarricense los riesgos potenciales que se puedan dar en el ciberespacio con la utilización de normas de seguridad apropiadas y legales.

Además, se pretende analizar si es basta la cobertura y los alcances del derecho positivo en materia de ciberseguridad y lograr establecer si se encuentran vacíos de legalidad que puedan eventualmente subsanarse por medio de fallos de los jueces o haciendo uso de leyes anexas.

No se pretende con la investigación la creación de normas, pero si la construcción de recomendaciones que minimicen el impacto de riesgo en el desarrollo del uso del Internet de las Cosas.

## 1.5 Viabilidad

El TFG se hará con apoyo de personal experto en el área de IoT y abogacía de Componentes Intel Costa Rica, lugar en donde trabaja la investigadora. El departamento de Ciberseguridad (CSC), permitirá hacer uso de las herramientas de este para poder llevar a cabo toda la investigación y de esta forma hacer uso adecuado de las mismas, así como el departamento de innovación digital con él que cuenta la compañía.

Al involucrar un tema de índole riesgoso ante la empresa, la investigación es completamente viable para poder evaluar los riesgos y vulnerabilidades con las que se cuentan actualmente y crear ajustes en el manejo de los dispositivos IoT a nivel nacional.

### 1.5.1 Punto de vista técnico

Al ser parte del equipo del Cyber Security Center la investigadora cuenta con la experiencia necesaria como analista de seguridad para poder realizar dicha investigación, además, al estar involucrada en el crecimiento empresarial, es líder del área de ingeniería social e innovación, así como de implementación de Facial Recognition para el CSC.

### 1.5.2 Punto de vista operativo

Actualmente el CSC está incorporando nueva tecnología IoT para poder controlar el ingreso al CSC, es por ello por lo que decidieron resguardar la seguridad por medio de este dispositivo biométrico, por lo tanto, se cuenta con el apoyo de especialistas en seguridad Informática.

Por otra parte, el funcionamiento del CSC no se verá afectado puesto que se cuenta con un laboratorio de innovación (Innovation Center) para poder realizar pruebas, usar redes externas, *host* especializados y herramientas útiles para la investigación.

### 1.5.3 Punto de vista económico.

La investigación se puede realizar con éxito, puesto que desde el punto de vista de *software* y *hardware* se cuenta con el adecuado, por otra parte, al realizarse en Intel, de acuerdo con las políticas internas, se tomará en cuenta como un proyecto de desarrollo e innovación para el CSC, por lo tanto, no existe costo de hora consultor ya que es parte del proceso anual de la compañía.

Además, cabe destacar que existen presupuestos ya establecidos por parte del departamento para fines investigativos y aplicativos.

Por otra parte, se cuenta con el apoyo de abogados especialista en el área de tecnologías de la información, así como de delitos informáticos.

## 1.6 Objetivos

### 1.6.1 Objetivo general

Evaluar la efectiva aplicación de la legislación costarricense en el desarrollo de proyectos IoT para dimensionar sus repercusiones en la seguridad y privacidad de los datos.

### 1.6.2 Objetivos específicos

1. Establecer los riesgos que implican la incorporación de IoT y las acciones que afectan la privacidad de los datos.
2. Determinar cuáles leyes y reglamentos en Costa Rica protegen la seguridad y privacidad de la información.
3. Evaluar los agujeros de seguridad en los dispositivos que conformarán la gran red de IoT.
4. Recomendar soluciones para mejorar el manejo de la información por parte de los usuarios y en las empresas.

## 1.7 Alcances del estudio

### 1.7.1 Alcances

Es menester de este estudio asentar precedentes en la efectiva y correcta aplicación de la legislación costarricense para incorporar nuevos proyectos de IoT, con el fin de que guie al profesional informático en la correcta inducción de este tipo de proyectos.

Por último, apoyando la investigación en un estudio documental permite facilitar el análisis doctrinal, legal, jurisprudencial y casuístico sobre la legislación costarricense en materia de protección de datos.

Se tomará en cuenta población relacionada con la investigación como lo son abogados especialistas en el área de tecnologías de la información e ingenieros informáticos con énfasis en delitos informáticos.

### 1.7.2 Limitaciones

Conforme a lo expuesto por Ávila (2010) una limitación consiste en que se deja de estudiar un aspecto del problema por alguna razón. Con esto se quiere decir que toda limitación debe estar justificada por una buena razón. (p.87).

Siendo un trabajo final de graduación, existen varias limitaciones en su realización, ya que no se puede prever si con la actual incorporación de IoT se van a subsanar los vacíos existentes hasta el momento, por ser muy reciente.

El tema en estudio presenta una limitante referida relacionada con la formación académica, el campo metodológico es totalmente nuevo, en relación con el conocimiento que se posee por trabajos realizados.

La veracidad de los datos obtenidos queda contemplada en la información suministrada por los sujetos que integran la muestra, misma que se confronta con la doctrina, la jurisprudencia y el área de ciberseguridad.

La falta de fuentes o libros referentes al tema de la legislación costarricense en el área de protección de datos es una restricción, puesto que es un tema innovador. Es por ello, que otra limitación que afecta el proceso de investigación es la falta de

información disponible sobre el tema, debido a que la mayoría de esta se encuentra en revistas y artículos de periódico.

En tal sentido, el tema que nos ocupa conlleva un estudio muy concreto sobre la legislación mencionada y sus implicaciones. Por tal motivo, el tema en análisis nos circunscribe al tratamiento de aspectos de orden casuístico, doctrinal, legal y jurisprudencial, como forma de realizar un estudio integral del objeto mismo de esta investigación.

# Capítulo II

# Marco Teórico

## 2.1 Evolución de la seguridad

"Ser lo que soy, no es nada sin la seguridad". Sin duda W. Shakespeare (1564–1616) tenía un concepto más evolucionado de la seguridad que sus contemporáneos del siglo XV.

El amplio desarrollo de las nuevas tecnologías informáticas está ofreciendo un nuevo campo de acción a conductas antisociales y delictivas manifestadas en formas antes imposibles de imaginar, ofreciendo la posibilidad de cometer delitos tradicionales en formas no tradicionales.

La mayoría del mundo informático desconoce la magnitud del problema con el que se enfrenta y, generalmente no se invierte ni el capital humano ni económico necesario para prevenir, principalmente el daño y/o pérdida de la información que, en última instancia es el conocimiento con que se cuenta.

La seguridad es una necesidad básica. Estando interesada en la prevención de la vida y las posesiones, es tan antigua como ella.

Los primeros conceptos de seguridad se evidencian en los inicios de la escritura con los sumerios (3000 AC) o el Hammurabi (2000 AC). También la Biblia, Homero, Cicerón, César han sido autores de obras en donde aparecen ciertos rasgos de la seguridad en la guerra y el gobierno.

Los descubrimientos arqueológicos marcan, sin duda, las más importantes pruebas de seguridad de los antiguos: las pirámides egipcias, el palacio de Sargon, el templo Karnak en el valle del Nilo; el dios egipcio Anubi representado con una llave en su mano, entre otros.

Se sabe que los primitivos, para evitar amenazas, reaccionaban con los mismos métodos defensivos de los animales: luchando o huyendo (fight or flight), para eliminar o evitar la causa. Así la pugna por la vida se convertía en una parte esencial y los conceptos de alertar, evitar, detectar, alarmar y reaccionar ya era manejado por ellos.

Como todo concepto, la seguridad se ha desarrollado y ha seguido una evolución dentro de las organizaciones sociales. La sociedad se conformó en familias, y esto se convirtió en un elemento limitante para huir. Se tuvieron que concebir nuevas estrategias de intimidación y disuasión para convencer al atacante que las pérdidas eran inaceptables contra las posibles ganancias.

La primera evidencia de una cultura y organización en seguridad “madura” aparece en los documentos de la Res Publica (estado) de Roma Imperial y Republicana.

El próximo paso de la seguridad fue la especialización. Así nace la seguridad externa (aquella que se preocupa por la amenaza de entes externos hacia la organización); y la seguridad interna (aquella preocupada por las amenazas de nuestra organización con la organización misma). De estas dos se pueden desprender la seguridad privada y pública al aparecer el estado y depositar su confianza en unidades armadas.

Desde el siglo XVIII, los descubrimientos científicos y el conocimiento resultante de la imprenta han contribuido a la cultura de la seguridad. Los principios de probabilidad, predicción y reducción de fallos y pérdidas han traído nueva luz a los sistemas de seguridad.

La seguridad moderna se originó con la Revolución Industrial para combatir los delitos y movimientos laborales, tan comunes en aquella época. Finalmente, un teórico y pionero del Management, Henry Fayol en 1919 identifica la seguridad como una de las funciones empresariales, luego de la técnica, comercial, financiera, contable y directiva.

Al definir el objetivo de la seguridad Fayol dice: "…salvaguardar propiedades y personas contra el robo, fuego, inundación contrarrestar huelgas y felonías, y de forma amplia todos los disturbios sociales que puedan poner en peligro el progreso e incluso la vida del negocio. Son, en general, todas las medidas para conferir la requerida paz y tranquilidad (Peace of Mind) al personal".

Las medidas de seguridad a las que se refiere Fayol, sólo se restringían a los exclusivamente físicos de la instalación, ya que el mayor activo era justamente ese: los equipos, ni siquiera el empleado. Con la aparición de los "cerebros electrónicos", esta mentalidad se mantuvo, porque ¿quién sería capaz de entender estos complicados aparatos como para poner en peligro la integridad de los datos por ellos utilizados?

Hoy, la seguridad desde el punto de vista legislativo, está en manos de los políticos, a quienes les toca decidir sobre su importancia, los delitos en que se pueden incurrir, y el respectivo castigo, si correspondiera. Este proceso ha conseguido importantes logros en las áreas de prevención del crimen, terrorismo y riesgo más que en el pensamiento general sobre seguridad.

En cambio, desde el punto de vista técnico, la seguridad está en manos de la dirección de las organizaciones y, en última instancia, en cada uno de ustedes y en su

grado de concientización respecto a la importancia de la información y el conocimiento en este nuevo milenio.

Es en este proceso en donde se aprecia que no se ha añadido ningún nuevo concepto a los ya conocidos en la antigüedad; los actuales sólo son perfeccionamientos de aquellos: llaves, cerraduras, cajas fuertes, puertas blindadas, trampas, vigilancia, etc.

En definitiva, los expertos en seguridad y los expertos en informática deben interactuar interdisciplinariamente para que exista seguridad informática.

## 2.2 Seguridad

### 2.2.1 Seguridad de la información

Según María Jaquelina López y Cintia Quezada en su libro Fundamentos de Seguridad Informática:

“El término seguridad de la información se refiere a la prevención y a la protección a través de ciertos mecanismos, para evitar que ocurra de manera accidental o intencional la transferencia, modificación, fusión o destrucción no autorizada de la información”.

La seguridad de la información engloba todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad (conocida como la tríada CIA, del inglés: “Confidentiality, Integrity, Availability”) de la misma.




**Ilustración 1. Tríada (Confidencialidad-Integridad-Disponibilidad). INFOSEGUR**

A continuación, se explican brevemente los principios básicos de la seguridad de la información.

1. **Confidencialidad**. - Condición que garantiza que la información es accedida solo por las personas autorizadas según la naturaleza de su cargo o función dentro de la organización. La confidencialidad está relacionada con la privacidad de la información.

2. **Integridad**. - Condición que garantiza que la información es consistente o coherente. Está relacionada con la veracidad de la Información.

3. **Disponibilidad**. - Condición que garantiza que la información puede ser accedida en el momento en que es requerida.

Si uno de estos tres pilares se ve comprometido, ya sea por un riesgo, una amenaza o vulnerabilidad, la seguridad de los datos se verá afectada.

Es necesario entender las diferencias entre estos tres conceptos:

### 2.2.2 Vulnerabilidad (Vulnerability)

Según (Prandini & Pallero, 2013).

Una vulnerabilidad es una debilidad de un bien o de un control, que puede ser aprovechada por una amenaza. Se trata de una característica negativa del bien, también conocido como activo o recurso de información, o de un control que se implementó sobre él, que lo hace vulnerable. En efecto, esa vulnerabilidad es susceptible de ser aprovechada y varía de acuerdo con los cambios en las condiciones que dieron origen a su existencia o a las acciones que se tomen con el fin de evitar su explotación o aprovechamiento.” En el mismo documento se indica: “En el campo de la seguridad de la información, el problema de las vulnerabilidades ha dado lugar a un nuevo escenario. Ya no resultan suficientes las soluciones simples o aisladas, sino que se hace necesario implementar “seguridad en profundidad”, que proteja todos los activos de acuerdo con su criticidad, y también contemple la capacitación y la concientización a los empleados sobre las nuevas amenazas.

En el manual de CISM (2013, p. 163) entre algunas de las vulnerabilidades que se pueden mencionar están:

1. Configuración del equipo incorrecta
2. Ejecución de cumplimientos inadecuada
3. Pobre diseño de red.
4. Procesos incorrectos o incontrolables.
5. Gestión inadecuada.
6. No hay suficiente *staff.*

7. Falta de conocimiento para brindar soporte a los usuarios o a los procesos que se encuentran activos.
8. Falta de un mantenimiento adecuado.
9. Pobre gestión de las comunicaciones.

### 2.2.3 Amenaza (Threat)

Según (Magazcitum, 2013).

En contraposición al de vulnerabilidad requiere pensar los posibles problemas que nos pueden afectar en un futuro cercano, por lo que plantea un posicionamiento anterior a un hecho, que representa algún grado de probabilidad de materializarse. A manera de ejemplos de amenazas reales pueden citarse los virus, los delincuentes informáticos o las intrusiones. Otra definición es aquella que la caracteriza como cualquier acción o acontecimiento no deseado e inesperado con la capacidad de ocasionar consecuencias adversas.

Existen amenazas relacionadas con fallas humanas, catástrofes naturales o ataques deliberados. Las fallas humanas pueden ser con intención o sin ella, debido a negligencia, impericia o mal uso. También se clasifican como internas o externas dependiendo de su origen: desde dentro de la propia organización o desde un punto remoto. Dentro de las amenazas naturales son ejemplos los terremotos o las inundaciones.

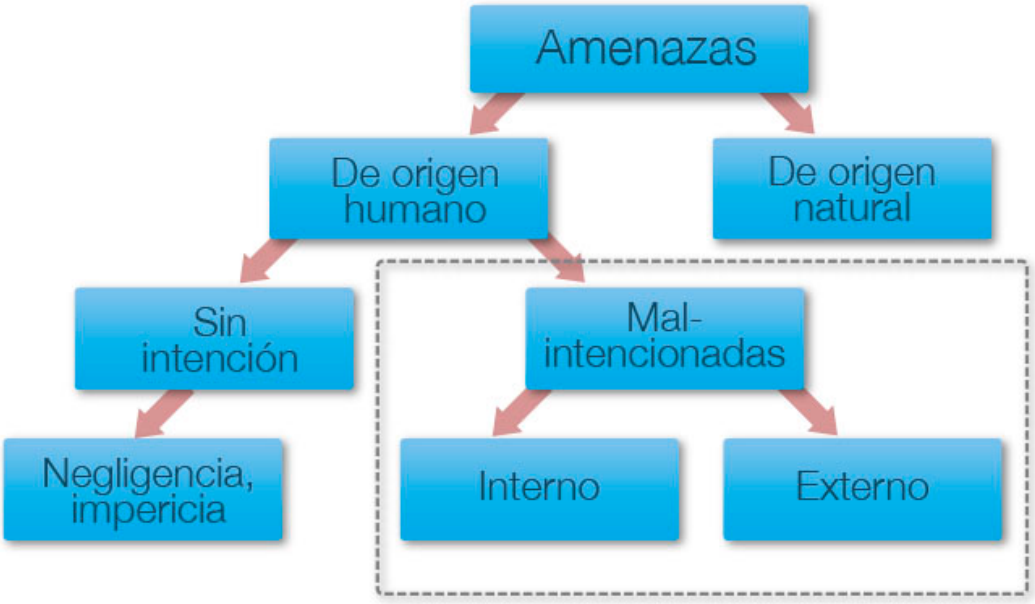



**Ilustración 2. Amenazas. (Prandini & Pallero, 2013)**

Las amenazas varían en el tiempo. Los factores que contribuyen a un panorama de amenazas siempre cambiante son el constante crecimiento de la cantidad y el tamaño de las redes y del número de usuarios interconectados, la profusión de las bases de datos en línea, la inmadurez de las nuevas tecnologías que se lanzan al mercado sin haber sido probadas en forma exhaustiva, la alta disponibilidad de herramientas automatizadas de ataque y las técnicas de ingeniería social. Los distintos escenarios que plantean las amenazas deben contemplarse dentro de planes de continuidad del negocio y siempre deben identificarse y estimarse debidamente al gestionar los riesgos.

### 2.2.4 Riesgo

Según (Prandini & Pallero, 2013).

La materialización de una amenaza que aprovecha una vulnerabilidad expone a las organizaciones y sus sistemas informáticos a lo que se conoce como riesgo. El

riesgo puede ser definido como la posibilidad de que algo que ocurra impacte negativamente sobre la información o sobre los recursos para gestionarla. La norma ISO/IEC-27002 lo define como la combinación de la probabilidad de ocurrencia de un determinado hecho y sus consecuencias. La probabilidad de ocurrencia es el producto del análisis sobre datos históricos respecto a cuántas veces sucedió un hecho similar en un período de tiempo que se tomará como unidad. Se entiende por consecuencias, el impacto, es decir, los hechos o acontecimientos que resultan de uno o varios eventos evaluados para esa organización. La determinación de la probabilidad de ocurrencia y la valoración del impacto tienen lugar en el proceso de gestión del riesgo, que dará como producto la decisión de distribuir o aplicar los controles, sobre la base de una ecuación de costo/beneficio, lo que da como resultado la determinación del nivel de riesgo aceptable y la identificación del riesgo por mitigar.

Los riesgos en las organizaciones pueden ser de todo tipo: ambientales, de mercado, financieros, estratégicos, operacionales, de cumplimiento, etcétera. Los riesgos vinculados al uso de tecnologías de información son transversales a todos.

## 2.3 Internet de las Cosas (Internet of Things)

### 2.3.1 Antecedentes de IoT

IoT no es un tema nuevo ni tampoco novedoso como todos piensan, si retrocedemos el tiempo al año 1927 cuando Nikola Tesla desarrolló una base de comunicaciones inalámbricas y de radio se puede interpretar como las primeras fases de IoT, sin embargo, al adelantar los antecedentes históricos al año 1969 con la incorporación de la red ARPANET, la cual, fue creada para el departamento de Defensa de Estado Unidos como el primer nodo de lo que ahora la gran red del

Internet. Al partir desde ese nodo descentralizado se ha creado una red que ha crecido y ha interconectado computadoras al igual que ha fortalecido el comienzo de nuevas redes.

En aquel momento las redes no trabajaban por si solas, necesitaban del factor humano para pasar la información de un lado otro, sin embargo, diez años después se implantó el protocolo TCP/IP y ya para 1990 Tim Berners-Lee implementó la primera comunicación entre un cliente HTTP y un servidor en Internet.

Un año más tarde se crearía la primera página web y a partir de ahí la evolución de la informática y las comunicaciones ha sufrido un avance exponencial que llega hasta nuestros días y realmente nadie sabe dónde estará el límite.

Como lo indicó Mark Weiser:

“Los ordenadores personales serían reemplazados por “ordenadores invisibles” introducidos en objetos de uso cotidiano” “(1990)

Aunque Mark Weiser dio las primeras pinceladas en el 90 de lo que a la larga se convertiría en IOT, no fue hasta el 1999, cuando se utilizó por primera vez el término IOT. Kevin Ashton impartió una conferencia en Procter and Gamble (1999) donde dijo “Necesitamos un Internet de las cosas, una forma estandarizada para equipos para entender el mundo real.”

En ese mismo año, Neil Gershelfeld (1999) utilizó ese mismo término en su libro Cuando las cosas empiezan a pensar donde escribió: "En retrospectiva parece que el rápido crecimiento de la World Wide Web puede haber sido sólo la acusación de la desencadenada explosión real que ahora está provocando que las cosas comiencen a utilizar la red."

Si se toman en cuenta esas frases, se puede mencionar que los últimos dos autores pensaban en la interconexión de elementos que no fueran computadoras y precisamente esa es la idea de **IOT**: Hacer que podamos concentrar toda nuestra atención en las actividades de la vida cotidiana y laboral sin preocuparnos de suministrar información a los aparatos electrónicos que nos rodean, estando esta tarea en manos de *ellos* mismos.

**Evolución de IoT**

- En 1926 el genio Nikola Tesla realizó patentes y trabajos teóricos los cuales fueron la base de las comunicaciones inalámbricas y de radio. (J & P, 2018)
- En el año 1949 se inventa el código de barras (que posteriormente evolucionaría para su uso en supermercados). (Bliznakoff del Valle, 2014)
- El 29 de octubre de 1969 se envió el primer mensaje a través de ARPANET, (el precursor de internet). (Cuesta, 2009)
- En el año 1973 se otorga la primera patente para un lector/escritor RFID pasivo. (Bliznakoff del Valle, 2014)
- En 1978 TCP se convierte en TCP/IP gracias al esfuerzo de Danny Cohen, David Reed y John Schoch para generar un sistema que soportara tráfico en tiempo real y permitir la creación del User Datagram Protocol (UDP) sobre IP.
- En el año 1980 miembros del departamento de Ciencias de Computación de Carnegie Mellon consiguen instalar micro-switches en una máquina de venta de refrescos y conectarla al ordenador del departamento para poder comprobar desde la terminal el número de botellas que quedan y si están frías o no. (Bliznakoff del Valle, 2014)

- En 1990 Berners-Lee implementó la primera comunicación exitosa entre un cliente Hypertext Transfer Protocol (HTTP) y un servidor a través de Internet, había inventado la World Wide Web. Él mismo, un año más tarde, creó la primera página web. A partir de ese momento el desarrollo tecnológico es vertiginoso, comienza la revolución de Internet. (J, R, & S, 2015)
- En el año 1993 un proyecto de la Universidad de Columbia denominado KARMA diseña un head-up de realidad aumentada con capacidad de sobreponer los planos y las instrucciones de mantenimiento a los objetos.
- En el año 1994 Steve Mann inventó la primera webcam que permitía ver el nivel de café en una cafetera, sin tener que levantarse.
- En 1995 Siemens establece un departamento dedicado dentro de su negocio de teléfonos móviles para desarrollar y lanzar un módulo GSM para aplicaciones máquina a máquina (machine-to-machine M2M). (Bliznakoff del Valle, 2014)
- En 1997 Tiene lugar en Cambridge (USA) el primer simposio internacional del IEEE sobre “wearable computers” (Bliznakoff del Valle, 2014)
- El 22 de julio de 1999 Kevin Ashton, impartió una conferencia en Procter & Gamble donde habló por primera vez del concepto de Internet de las Cosas. That ‘Internet of Things’ Thing. (Defazio & Foglia, 2016)
- En el año 2000 LG anuncia su primera nevera conectada a Internet. [2] (Bliznakoff del Valle, 2014)
- Durante los años 2003-2004 El término IoT es ampliamente usado en publicaciones de primer orden. (Bliznakoff del Valle, 2014)

- La tecnología RFID surgió en el campo militar, durante la II Guerra Mundial, esta utiliza ondas electromagnéticas o electrostáticas para la trasmisión de señal que contiene la información. (Huidobro, 2004)
- En 2005 la Unión Internacional de Telecomunicaciones (UIT) publica el primer estudio sobre el tema. A partir de ese momento Internet de las Cosas adquiere otro nivel. (UIT, 2005)
- En 2006 se comercializa el Nabaztag que fue creado por Rafi Haladjian y Olivier Mével, y lo fabrica la sociedad francesa Violet. Se trata de un pequeño conejo que se conecta a Internet por ondas Wi-Fi 802.11b. Se comunica con su usuario emitiendo mensajes vocales, luminosos o moviendo sus orejas. Difunde informaciones como la meteorología, la Bolsa, la calidad del aire, el estado de la circulación, llegada de los correos electrónicos, entre otros. (Bliznakoff del Valle, 2014)
- En el 2008 fue fundada IPSO Alliance, como una organización sin fines de lucro con miembros especialistas en tecnología, comunicaciones y las empresas de energía, con el objetivo de promover el uso del protocolo de Internet en redes de objetos inteligentes y hacer posible IoT. Actualmente en IPSO participan 59 empresas de todo el mundo como Bosch, Cisco, Ericsson, Motorola, Google, Toshiba o Fujitsu. (IPSO, 2008)
- En 2008 se creó Pachube ahora llamado Xively, se define como una “Plataforma de Servicio” (PaaS) para la Internet de las Cosas. Básicamente Xively es una nube especializada en recibir y desplegar información de los distintos sensores que necesitemos conectar. (Bliznakoff del Valle, 2014)
- Según investigaciones realizadas por Cisco IBSG se estima que IdC “nació” entre 2008 y 2009 en el momento en que las cosas conectadas a internet superaron a las

personas. (CIS; Evans, 2011) Ilustración 2. Internet de las cosas "nació" entre los años 2008 y 2009. Fuente: Cisco IBSG, abril de 2011

- En año 2010 dijo Li Yizhong, ministro de la Industria y Tecnología de la Información, en su discurso de apertura al foro sobre Tecnología de la Información, Comunicación y Desarrollo Urbano, sostenido en la localidad oriental costera china de Ningbo, que se debía acelerar el desarrollo de la industria de la IOT en China para crear una nueva plataforma que sustente el desarrollo económico.
- El 6 de junio de 2012 ha sido seleccionado por la Internet Society (ISOC) y otras organizaciones como el Lanzamiento Mundial de IPv6. Samsung, Google, Nokia y otros fabricantes anuncian sus proyectos NFC. Se crea la iniciativa IoT-GSI Global Standards para promover la adopción de estándares para IoT a escala global. China continúa invirtiendo e impulsando el desarrollo y la investigación en Internet de las Cosas con instituciones como Shanghai Institute o la Chinese Academy of Sciences. (Pisanty, 2012)
- En el 2013 Intel lanza soluciones en grupo para la implementación de IoT

### 2.3.2 IoT en la actualidad

Durante las últimas dos décadas IoT ha dimensionado sus alcances, transformándose en un tema para científicos e investigadores con el fin de incorporar la innovación como una nueva era tecnológica.

Al definir el internet de las cosas: se indica que es una personificación de objetos que solo era parte de la imaginación, no obstante, esa imaginación es real, ya que es en este punto donde los objetos cotidianos cobran vida a través de las interconexiones

digitales con el Internet, creando comunicación con ellos mismos o con personas, algo realmente magnifico y de gran utilidad.

Si enfocamos la educación de los niños con la que se cuenta actualmente en muchas escuelas de Costa Rica, se puede indicar que es un tipo de aprendizaje común, antiguo e incluso para muchos es aburrido. Con la incorporación de IoT estos aspectos pueden cambiar de forma impresionante brindando a los niños una cultura tecnológica efectiva.

Imagine por un instante el siguiente escenario:

Los escolares llegan a sus clases, se desactivan automáticamente los teléfonos, sus cuadernos virtuales se conectan al planeamiento que tiene el profesor en su tableta, quien previamente ha definido la lección y las actividades, al instante cada uno de los estudiantes puede tener toda la información a un solo clic.

El profesor da las notas de las actividades realizadas en clase y automáticamente se envía a los estudiantes y a sus padres.

Al finalizar las clases, se actualiza el registro de asistencia, de trabajo cotidiano y se guardan los cambios para la siguiente clase. De la misma forma le genera al profesor un informe de debilidades que se deben reforzar con el estudiante con las menores calificaciones.

Este escenario parece imposible de lograr a corto plazo, sin embargo, con la incorporación de IoT esto es posible en los próximos años.

De acuerdo con la empresa EMC encargada del desarrollo de *software* y sistemas para la administración y almacenamiento de información, ha indicado que para el 2020 esperan que existan 30.000 millones de dispositivos IoT, aunque eso

suena muy lejano, hay estadísticas anuales de más de 6.400 millones de dispositivos IoT, impactando de forma global el mundo debido a la velocidad en la que avanza.

Se puede tomar en cuenta la siguiente imagen en la cual se observa el avance del Internet para el 2017:

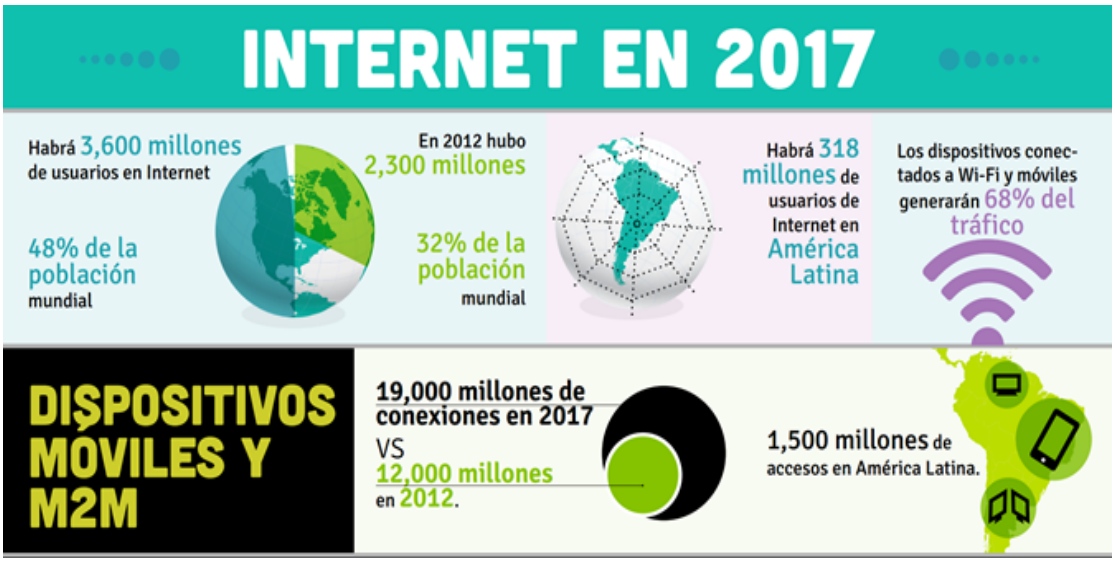



**Ilustración 3. Internet en 2017. Pronóstico de Cisco Virtual Networking Index**

Se espera que para este 2017 haya 3,6 billones de usuarios conectados lo cual manifiesta de que un 68% del tráfico proviene de depósitos conectados a Wifi, entre ellos móviles y dispositivos IoT.

Si se hace una comparación de uso del Internet, en el 2012 había 12.000 millones de conexiones mientras que en el 2017 hay 19.000 millones, esto indica un aumento bastante alto, conectando a 1.500 millones de usuarios en América Latina.

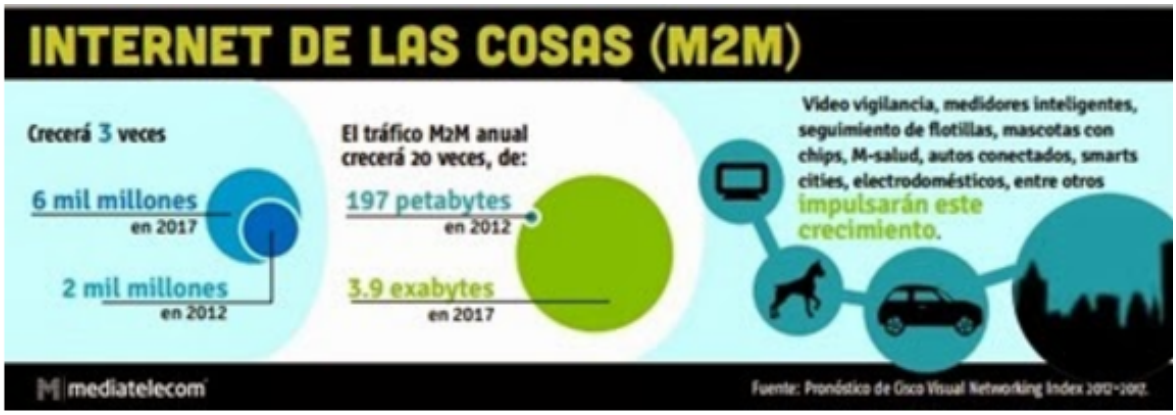



**Ilustración 4. Internet en 2017. Pronóstico de Cisco Virtual Networking Index**

El Internet de las cosas crecerá 3 veces más este 2017, evidenciando que en el 2016 había 2 mil millones de dispositivos y actualmente se cuenta con 6 mil millones. Esto debido a que existen muchas aplicaciones y dispositivos que hacen la vida mucho más sencilla para los usuarios.

Steve Prentice (2014), vicepresidente de Gartner subraya: “El número de dispositivos inteligentes conectados a Internet seguirá creciendo de manera exponencial, otorgando a las cosas inteligentes la capacidad de sentir, interpretar, comunicar y negociar, y efectivamente tener una voz digital”.

IoT contempla una tecnología integrada bastante compleja, sin embargo, ya se encuentra en su primera fase, abarcando de forma segura distintos escenarios y descubriendo métodos para hacer interconexiones adecuadas y satisfacer muchas necesidades.

Sin lugar a duda lo poco que IoT ha impactado, los usuarios lo han adquirido, ya se han empezado a ver cambios en las industrias, en la parte de salud y en el sector ambiental, temas que serán tratados más adelante. Sin embargo, lo que sí es claro es que la protección de IoT no va de la mano con la rapidez con la que evoluciona.

De acuerdo con Telefónica: "Todo el mundo se centra en las oportunidades de innovación que ofrece el IoT, pero hasta este momento se ha hablado relativamente poco de su lado más siniestro", indica John (2016), esta afirmación se realizó en el informe titulado "Alcance, escala y riesgos sin precedentes: asegurar el Internet de las cosas", en donde hace énfasis del déficit que tiene la ciberseguridad con respecto al avance de IoT, esto demuestra preocupación y falta de protección para evitar posibles ataques.

Debido a la deficiencia de seguridad que tiene este desarrollo tecnológico, es fundamental centrar la investigación en el análisis a nivel legislativo y de derechos legales a nivel nacional, por lo que se van a tratar problemas derivados a vacíos legales que existen actualmente en este tipo de tecnologías, además se aportarán datos para conocer el estado actual de la legislación y si verdaderamente los usuarios están protegidos ante la llegada de IoT.

La cantidad de preguntas que se obtienen al pensar en las posibilidades que ofrece la implantación de IoT es abrumadora. ¿Pueden los fabricantes introducir sensores en sus productos para ofrecer un mejor servicio posventa? ¿Pueden fabricantes compartir sus datos personales para ofrecer un mejor servicio? ¿Qué información es segura de almacenar en un dispositivo inteligente? ¿De quién son los datos almacenados en una pulsera inteligente que mide su actividad física? ¿El fabricante puede vender estos datos? ¿Cuándo se sube una foto a Facebook con su localización, Facebook puede vender estos datos? Para resolver todas estas preguntas es necesario antes hacer un recorrido por las leyes de protección de datos.

#### 2.3.2.1 ¿Tiene Costa Rica edificios inteligentes?

La implementación de edificios inteligentes en el país tuvo inicialmente un proceso de crecimiento relativamente lento en comparación con países del Norte, más industrializados.

Modelos sostenibles y eficientes, así son los edificios inteligentes, mejorando la calidad de vida de los usuarios. En Costa Rica la implementación de este tipo de estructuras ha ido en aumento, ya que no solo las personas están haciendo uso de ellos, sino también empresas nacionales.

Para introducir más el tema, la revista Construir conversó con la Ing. Ana Quirós, presidenta de Green Building Council Costa Rica (GBC-CR) la cual se tomará en cuenta como parte fundamental del trabajo de investigación.

**¿Cuál es el panorama actual que tiene el país en cuanto a edificios inteligentes?**

La evidencia muestra que hoy en día, con el repunte de la construcción sostenible, los desarrolladores, propietarios y potenciales usuarios son más conscientes de la importancia de integrar los sistemas, servicios, estructura y administración de un edificio en aras de mejorar su desempeño y el confort de sus usuarios. Por ejemplo, a finales del año 2016, se llevó a cabo en el país el primer congreso de “Facility Management (FM)”, con el apoyo del GBC-CR.

A partir de este evento, se procedió a conformar la Asociación de FM de Costa Rica, mostrando así, el interés por parte de las empresas y de los profesionales a cargo del manejo y administración de las edificaciones e instalaciones para impulsar la gestión responsable y eficiente.

Esta asociación busca, entre otros, impulsar los mejores y más novedosos lineamientos existentes a nivel mundial en cuanto a FM. El país registra varios edificios y proyectos, que han recibido certificaciones de sostenibilidad (como EDGE o LEED) que incorporan, a diferentes niveles, criterios de edificio inteligente, que a su vez inciden en la sostenibilidad.

**¿A qué ritmo avanza nuestra nación en este tipo de construcciones?**

La implementación de edificios inteligentes en el país tuvo inicialmente un proceso de crecimiento relativamente lento en comparación con países del Norte, más industrializados. En primera instancia, este crecimiento se observa relacionado a proyectos y capital internacional, es decir, a proyectos impulsados por casas matriz ubicadas fuera del territorio nacional. Hoy en día, en Costa Rica, se observa un crecimiento cada vez más acelerado y acogido también por empresas de corte netamente nacional.

**¿Con qué aspectos debe contar un edificio para considerarse "inteligente"?**

El concepto de domótica se refiere a la automatización e integración de los diferentes sistemas que componen un edificio, de manera que sean más eficientes. Así, la inteligencia de un edificio viene a ser la capacidad de que todos los sistemas incorporados (telecomunicaciones, iluminación, climatización, accesos, anti incendios, entre otros), por medio de elementos como sensores (de temperatura, de presencia de ocupantes, etc.) se comuniquen con un sistema central que los monitoree, procese la información generada por ellos y ofrezca respuesta (soluciones a fallas, orientación para mejoras, recomendaciones para prevención y mantenimiento) respecto de ellos.

**¿Cuál es el principal factor que influye en el retraso de la región en cuanto a la construcción de proyectos inteligentes?**

Algunos de los factores que han incidido en que se estos proyectos no se hayan difundido tan ampliamente como se desearía, corresponden a la falta de experiencia que se tuvo en un inicio para el desarrollo diseño y gestión de este tipo de proyectos, la inicialmente limitada oferta de productos y servicios orientados a este sector en el país y por carencia de expertos locales, por falla en disponibilidad amplia y oportuna de suministros.

**Ejemplo de edificios inteligentes en Costa Rica**

El Centro de Servicios y Distribución de la farmacéutica Roche para Centroamérica y el Caribe es un ejemplo de edificio que opera de manera inteligente en el país, situado en la zona franca Ultrapark, en La Aurora de Heredia y que tiene 5.000 metros cuadrados.

La estructura dispone de un sistema que integra el manejo completo de las instalaciones. En este se emplean sensores que regulan el uso de la luz artificial, hay luminarias Led y los equipos electrónicos nuevos tienen el sello "Energy Star", que da fe de su eficiencia energética.

Asimismo, los espacios de trabajo tienen un diseño abierto y hay áreas verdes y sitios para laborar de pie, cuando el trabajador lo estime conveniente.

Anteriormente la empresa estaba en otro edificio en la misma zona franca y decidió pasarse a otro más amplio, lo cual requirió la remodelación de este y la edificación de nuevas áreas. El centro se inauguró el 12 de agosto del año pasado.

A finales de octubre del 2015 obtuvo la certificación sostenible Leed Gold, categoría Remodelaciones Interiores (la versión 2009 de la norma).

"La infraestructura del nuevo inmueble nos permite ahorrar más de un 40%, tanto en consumo de agua como de energía", expresó Krishnan Castillo, director financiero de Roche Centroamérica y Caribe.

#### 2.3.2.2 Edificios inteligentes internacionales

**The Edge el edificio más inteligente y ecológico del mundo - Holanda Ámsterdam**

El edificio almacena en una base de datos la información de sus empleados como lo es la dirección de su residencia, el tipo de coche que conduce, la bebida de su preferencia, la agenda diaria, entre otros esta es recibida de los 28.000 sensores instalados en toda la compañía.

Diariamente por medio de una app en el Smartphone a cada trabajador le es asignado un lugar de trabajo dependiendo de su jornada, es el llamado *hot desking*. Esto permite que alrededor de 2.500 trabajadores de Deloitte compartan 1.000 escritorios. El concepto se llama escritorio rápido, y aumenta al máximo el uso de espacios disponibles. Este edificio aprueba el ajuste de la luz y la temperatura según las preferencias de sus ocupantes y sugiere un menú que proporcione todos los ingredientes sugeridos según la dieta.

The Edge es considerado un edificio sostenible. Los paneles solares instalados en el tejado proporcionan mayor cantidad de energía de que necesitan para abastecerse y el agua lluvia es recogida y reutilizada en los baños, la calefacción y los jardines.

Su sistema de localización permite ahorrar energía apagando luces cuando no hay gente o bajando el sistema de climatización. (España, 2016)

**Tecnología usada**

Utilizan paneles LED que requieren poca electricidad por tal motivo el suministro de potencia es por medio de los cables que transportan datos a Internet. Además, cuentan con sensores de movimiento, luz, temperatura, humedad y rayos infrarrojos, creando un “techo digital” que conecta el edificio.

El atrio es el centro de gravedad del sistema solar del Edge. Paneles de malla entre cada piso permiten que el aire circule constantemente creando un bucle de ventilación natural. Incluso en días de tormenta, el edificio mantiene su iluminación con luz natural y ángulos de vidrio. El atrio y su icónico techo inclinado, llena los espacios de trabajo con luz del día y proporciona un amortiguador del sonido que viene del edificio y la carretera adyacentes. Cada espacio de trabajo está a 7 metros de una ventana.

Una cuarta parte de este edificio no se asigna a espacios de escritorio, sino que es un lugar de encuentro.

Algunas habitaciones pequeñas en el Edge cuentan con solo un sillón y una lámpara (sin mesa) perfecto para realizar una llamada telefónica. También hay salas de juego que permiten sincronizar grandes pantallas planas en cada esquina de forma inalámbrica con cualquier teléfono o laptop.

Dado que los trabajadores en el Edge no tienen escritorios asignados, los lockers son usados como base de operaciones para el día. Pueden hacer uso de estos

pasando la tarjeta de identificación cuando la luz verde está encendida, el propósito es alejar a los empleados de lugares fijos y formas rígidas de pensamiento.

Al llegar al Edge, la entrada del garaje está automatizada. Una cámara toma una foto de su placa de matrícula, la compara con su registro de empleo, y eleva la puerta. Incluso el garaje utiliza luces LED equipadas con sensores, que se iluminan según se aproxima y se atenúan al salir, el parqueadero está separado para bicicletas y autos en estos hay cargadores para carros eléctricos. (Deloitte, 2015)

**Oficina inteligente en Kutxabank – España**

El 18 de febrero del 2016 Kutxabank abre su oficina "insignia", en San Sebastián una "moderna y avanzada" sucursal de más de mil metros cuadrados de superficie, donde se prestará un servicio "personalizado" y "multicanal" a las 200.000 personas que podrían utilizarla anualmente.

Esta futurista sucursal, que contará con una veintena de empleados, está dotada de seis cajeros automáticos, dispensadores de entradas, siete terminales de banca a través de Internet y de banca móvil con pantallas de 19 pulgadas con teclado, ratón e impresora.

El director de Kutxabank en Gipuzkoa, Ander Aizpurua, ha explicado que el 85% de los usuarios emplearán herramientas de "autoservicio". La sucursal tiene mil metros cuadrados en dos plantas una de las principales novedades es que la oficina carece de un servicio de caja o ventanilla, de tal forma que el cliente se encontrará en la entrada con un pilar o tótem informático que realizará un registro virtual e identificará al usuario con solo acercar alguna de sus tarjetas bancarias o el DNI electrónico.

Acto seguido, pasará a la zona de espera, donde dispondrá de Wi-fi gratuito y tabletas, y podrá consultar las últimas novedades de la entidad bancaria a través de una pantalla gigante. Un gestor comercial le recibirá y trasladará al espacio que se adecue mejor a sus necesidades de forma "personal y cercana".

García Lurueña ha destacado que la nueva sede busca "adaptarse a los nuevos hábitos de la sociedad", con clientes cada vez más "independientes, autónomos y diestros en el uso de las nuevas tecnologías", pero que también buscan "el mejor asesoramiento especializado y confidencial".

La segunda planta de la sucursal estará dedicada a la atención de autónomos, microempresas y clientes con cartera de valores cuyas gestiones financieras resultan habitualmente más complejas. (García Laureña, 2016)

**Bilbao Kirolak. El polideportivo más sostenible de Europa. Leed Platinium. – España**

El polideportivo del barrio de San Ignacio, en Bilbao, es el primer edificio de España y el primer polideportivo de Europa en conseguir el prestigioso premio "LEED Platino". Fue construido en los años 50 y ha sido remodelado por una Empresa de Servicios Energéticos (ESE), adjudicataria del contrato de suministro y gestión energética y mantenimiento de todos los Centros Deportivos de Ayuntamiento de Bilbao.

Entre las tecnologías empleadas en su rehabilitación se encuentran: paneles solares térmicos y fotovoltaicos, motores de cogeneración, sistemas de iluminación inteligentes y sistemas de recuperación del calor del agua. (Ferrovial, 2012)

Soto del Real: primer municipio español con 100% alumbrado LED – España

Recientemente ha sido adjudicado el contrato de gestión energética del alumbrado público del municipio de Soto del Real, en la Comunidad de Madrid. Este contrato de servicios energéticos, en la modalidad de canon fijo, tiene una duración de 20 años y convertirá a Soto del Real en el primer municipio de España con la totalidad de luminarias con tecnología LED. Se instalarán más de 3.000 luminarias tele gestionadas en todo el municipio, lo cual repercutirá en un ahorro de consumos superior al 80% y una reducción de emisiones por encima de 1.000 toneladas de CO2.

Beneficios sociales y ambientales. Las soluciones de IdC relacionadas con el medio ambiente son numerosas; están generando un impacto social muy auténtico a nivel mundial. Las soluciones de iluminación inteligente abarcan varios micro mercados, incluidas las bombillas inteligentes, los switches y la energía de vidrio (LIFX, Luxera, Kinestral, Enlighted) e inteligente (Sunrun, Ecofactor, Keen Home). En Copenhague, el uso de sensores preparados para IP y de iluminación LED en farolas generó ahorros de costos y menor consumo de energía, ya que las luces se encienden o atenúan según la actividad del entorno. Además, los tiempos de respuesta del personal de la ciudad son mucho más rápidos a la hora de abordar problemas. (Ferrovial, 2012)

**Salón de Ciudadanos – China**

Es la sede de la Oficina de Administración de Servicios de Revisión y Ratificación de Yinchuan. Inició sus operaciones en noviembre de 2014 y hasta ahora ha concentrado 153 asuntos gestionados anteriormente por 100 oficinas en sólo 7 oficinas actuales, con lo cual, el personal encargado de manejar estos asuntos disminuyó un 90%, en tanto que la eficiencia aumento un 75%.

Cuando el Primer Ministro de China, Li Keqiang, realizó una visita al lugar, declaró que el “salón” ha logrado simplificar la administración y descentralizar los poderes.

Esta oficina tiene un mostrador de vidrio, en donde se pueden ver los sellos oficiales descontinuados, gracias al nuevo mecanismo de ratificación que con un solo sello ha desechado a los viejos sellos, que, junto con los complejos procedimientos del pasado, ahora son parte de la historia.

Para los funcionarios que trabajan aquí, el mayor cambio es la actitud de su servicio. La simplificación de los trámites ha elevado mucho el espíritu emprendedor e innovador.

A continuación, se presentan algunos de los procesos que se han mejorado gracias a la implementación de nuevas tecnologías.

- Tras la entrega de los documentos se almacena la información en una base de datos, y automáticamente se genera el certificado de una empresa en menos de una hora, anteriormente duraba semanas la expedición de este.
- Para entrar a la comunidad no se necesita llave, ya que el sistema puede identificar el rostro.
- Para solicitar un pasaporte utilizan una máquina. En donde con tan solo poner la cédula el sistema valida completamente la información y si cumple los requisitos inmediatamente imprime.
- Antes, Yinchuan era conocida por su cultura e historia, y gracias a las medidas para convertirla en una ciudad inteligente, ahora es considerada como una urbe moderna, avanzada y brillante. (Hongyun, 2016)

**Sede de Microsoft - Estados Unidos**

En la sede de Microsoft, en Redmond, Washington, una solución de *software* orientada a los datos ha reducido de manera drástica el costo de operar el campus de la compañía, el cual incorpora más de 125 edificios, a través de una estrategia similar que se enfoca en utilizar Azure y el IoT para centralizar las operaciones de administración de sus edificios, lo que ha servido para inspirar a otros. La estrategia “El Internet de las Cosas junto con el Big Data” ha sido tan exitosa que los servicios de Microsoft y sus socios —como Iconics— ahora están ayudando a otros administradores a implementar la misma solución.

Y no es sólo en el extranjero donde estos tipos de sistemas pueden reducir el consumo de energía. Los datos de la Administración de Información Energética (EIA, por sus siglas en inglés) muestran que el sector industrial es el mayor consumidor de energía en Estados Unidos. En el 2012, representó el 32% de todo el gasto energético en el país, del cual el 74% se les atribuyó a los fabricantes —el 24% de toda la energía que se consume en Estados Unidos. (Chansanchai, 2016)

**Parque inglés- edificio inteligente bicentenario - Chile**

Primer edifico inteligente y sustentable en Chile. Cuenta con acceso controlado por biometría (mediante el uso de huellas dactilares), cámaras de seguridad con registro de 30 días, tele vigilancia y monitoreo las 24 horas por Internet y detectores de movimiento ultrasónico. Además, los ocupantes podrán controlar sus artefactos eléctricos vía remota, a través de una computadora o un teléfono fijo o móvil. El edificio sustentable sigue los siguientes parámetros, que lo transforman en un emprendimiento 40% más rentable que cualquier edificación tradicional: eficiencia en el uso de

energéticos y consumibles renovables. Adaptabilidad a un bajo costo, a los continuos cambios tecnológicos requeridos. Capacidad de proveer un entorno ecológico interior y exterior habitable y sustentable, altamente seguro y que maximiza la eficiencia a los niveles óptimos de confort. (Rony Ricardo Ramírez Vega, 2010)

**Oficinas principales Schattdecor, Thansau. – Alemania**

El edificio cilíndrico de 6 pisos es el centro de la nueva sede de Schattdecor. Su tecnología inteligente fue diseñada para ser tanto emblemática como funcional. Todas las paredes del edificio son de cristal y hacen que toda el área de trabajo esté llena de luz, además de esto cuenta con:

- Iluminación On/Off, atenuación.
- Calefacción / A.A. / Ventilación On/Off, continuo (válvulas, calentadores, ventiladores).
- Persianas eléctricas Arriba/abajo, posición (persianas venecianas enrollables).
- Medición / Meteorología.
- Compuertas a otros protocolos.
- Señales de transmisión a otros sistemas.

## 2.4 Aspectos legales

Debido a los fuertes cambios tecnológicos, se ha evidenciado un mercado agresivo, capaz de recopilar información sensitiva que involucra muchos datos personales e incluso confidenciales, es por esta razón que todos los ciudadanos deben conocer e involucrarse con la legislación costarricense para velar por el cumplimiento de la ley, además de estar involucrado con la agencia que vela por el análisis de la ley en Costa Rica.

El tema legal costarricense alcanza un enfoque en el tratamiento de los datos personales y sobre quien recae sus efectos, indicando que se debe tener conocimiento de los derechos que se pretenden, además de los derechos fundamentales comprendidos en la Constitución Política.

La Asamblea Legislativa de Costa Rica decretó con justificación en el expediente 16:679 la Ley de Protección de la persona frente a sus datos personales, la cual fue actualizada por última vez el 13 de octubre del 2010, apegándose a los artículos del Reglamento de la Asamblea Legislativa.

El 05 de setiembre de 2011 entra en vigor la Ley N º 8968: Ley de Protección de la persona frente a sus datos personales, publicada oficialmente en el diario oficial La Gaceta.

Costa Rica un país con es un Estado de derecho e independiente, al contar autonomía, tiene la capacidad jurídica para crear sus propias leyes; sin embargo, es importante conocer el trasfondo de la situación para que la ley en estudio de esta investigación se lograra institucionalizar, es por ello que se hará un énfasis en los criterios y las bases jurídicas de las grandes organizaciones internacionales amantes de la paz y la armonía entre los países, que sirvieron de inspiración y ejemplo en su creación.

### 2.4.1 Procedencia de la protección de datos personales

Es importante conocer las bases jurídicas y los criterios que son base de este tipo de temas relacionados a la protección de datos, es por ello por lo que se tomará en cuenta la administración legal que se da en Europa, Canadá y Estados Unidos con base en el manejo de los datos.

Desde el punto de vista mundial, tomando en cuenta los gobiernos de E.E.U.U., Canadá y la Unión Europea, se ha identificado el desarrollo de políticas para la protección de la privacidad en materia de Internet, en el cual, se pueden identificar algunos principios considerados básicos en donde se pueden desarrollar los lineamientos de la regulación jurídica emergente sobre esta materia. Para los efectos de hacerlos exigibles, deberán desarrollarse mecanismos que permitan defender ya sea por la vía de la protección brindada por la autoridad, con la consecuente acción para el caso de contravención, o mediante políticas de privacidad o programas de autorregulación sustentados por las propias empresas e informados en las páginas web respectivas.

Existen elementos que sin importar el país o la legislación son universales para todos, esto corresponde a los principios que protegen la privacidad en Internet, los cuales son los siguientes:

- **La información**: es fundamental notificar al usuario en forma previa, clara y detallada, que la entidad o empresa recopilará información personal, el uso que se le dará, el medio en que esta se acopiará, y si los consumidores deberán ser requeridos para hacer uso de ella.
- **El principio de opción;** el cual permite al usuario decidir si la información recolectada de sí mismo será utilizada para propósitos distintos del que le fue señalado y aceptado originalmente.
- **El concepto de acceso;** se refiere a la facultad individual del consumidor para acceder a la información de sí mismo recolectada por el servidor, de manera tal de

poder constatar su existencia, corregirla o complementarla y/o eliminarla, si así lo desea.

- **El principio de seguridad;** se refiere a la obligación de quien acopia la información personal de protegerla ante un acceso, uso y exhibición no autorizados, como asimismo respecto de su pérdida o destrucción.
- **La exigibilidad;** para el cumplimiento sustantivo de los principios antes mencionados, está dada por la regulación jurídica y el régimen sancionador que la autoridad pública debe aplicar en esta materia.

### 2.4.2 Recorrido por la legislación internacional

Como bien se mencionó anteriormente, es fundamental conocer el origen de la protección de datos para ser tomada como base para la evaluación del marco legislativo costarricense.

#### A. Europa

Alemania es categorizada como unos de los países líderes en el tema de la detección de todos aquellos datos que los ciudadanos quieren resguardar con el fin de proteger la intimidad. La entidad encargada de los mecanismos de defensa jurídica en Alemania ha enfocado el objetivo en el análisis de todos aquellos datos personales en Europa, es por ello por lo que desde 1970 este tema se ha hecho presente para ser desarrollado con el apoyo del Parlamento de Estado alemán de Hesse, con el éxito de la promulgación de la primera normativa de protección de datos llamada “Datenshutz”.

En 1977 el Parlamento Federal aprobó un Comisario Federal, cuyo fin era fiscalizar todos aquellos casos en donde existió un percance en perjuicio de todos los derechos relacionados con la intimidad de sus habitantes. Este tipo de acciones les

permitió a los demás países la incorporación a sus sistemas jurídicos de la regulación sobre el uso de los datos personales.

En 1995 la Unión Europea (UE), a través de uno de sus órganos, el Consejo Europeo, redactó un instrumento jurídico que fue adoptado por todos los países miembros de la UE y permitiendo que países de otros continentes pudieran comercializarlo siempre y cuando cumplieran con lo estipulado en él, dicho documento entró en vigor el 13 de diciembre de 1995, recibiendo el nombre de, Directiva 95/46 CE, y se constituyó como un texto jurídico de referencia a escala europea en materia de protección de datos personales.

La finalidad de la creación consistía en que, si algún país no miembro de la UE quería negociar algún tratado internacional, este debía regirse a partir de los principios básicos dispuestos en el texto. Cabe mencionar algunos de los principios básicos: la calidad de datos, la legitimación del tratamiento, las categorías especiales de tratamiento, información a los afectados por dicho tratamiento, el derecho de acceso del interesado, y el derecho del interesado por oponerse. Los anteriores principios se aplican a todas aquellas actividades que contengan procesos automatizados (base de datos informática de clientes, por ejemplo), así como a los datos contenidos en un fichero no automatizado o que vayan a figurar en él.

La consolidación del tratamiento de los datos personales por parte de la institucionalización de la legislación en Europa permitió implementar una iniciativa de crear un día dedicado al tratamiento de datos personales denominado, “ Día Internacional de la Protección de Datos”, el cual, se celebra el 28 de enero de cada año, con motivo de la celebración de la firma del Convenio de la Protección de los

Individuos con respecto del procesamiento automático de datos personales, conocido como el Convenio 108, el cual, permite, reconocer la necesidad de conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos. Esto incluye fortalecer los lazos comerciales entre los estados miembros de la Unión Europea, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados (Agencia Española de Protección de Datos, 2010).

El Reglamento General de Protección de Datos Personales (RGPD) entró en vigor el 25 de mayo de 2016, el cual es catalogado como una normativa europea de obligado cumplimiento y que implica una mayor concienciación sobre la privacidad de las personas y de las empresas. Será directamente aplicable a todos los Estados Miembros a partir del 25 de mayo de 2018.

Algunos puntos de este nuevo reglamento que son interesantes para la presente investigación, enfocando varios puntos en la seguridad y privacidad de IoT, entre ellos:

1. En este nuevo Reglamento de Protección de Datos, aparte de recoger los derechos de acceso, rectificación, cancelación y oposición, se regulan dos nuevos derechos, como son el llamado “Derecho al olvido”, el cual es el derecho del ciudadano de exigir que los datos personales sean suprimidos cuando, entre otros casos, ya no sean útiles para la finalidad en los que fueron obtenidos y recogidos. El segundo derecho añadido es el de la portabilidad de los datos.
2. La necesidad del consentimiento claro y afirmativo de la persona concernida al tratamiento de sus datos personales.

3. El derecho a ser informado si sus datos personales han sido pirateados.
4. Las aplicaciones, redes sociales y demás servicios tendrán que presentar determinados niveles por diseño o por defecto para proteger los datos personales de los usuarios.
5. Otro aspecto positivo que se ha mejorado en este nuevo reglamento es la obligación para las empresas de designar para ciertos casos un delegado de protección de datos “DPO. Data Protection Officer”, para garantizar el cumplimiento de la normativa. También las cuantías de las sanciones se elevan considerablemente, hasta el punto de alcanzar hasta 20.000.000 de euros, o el 4% del volumen de negocio total anual global del ejercicio financiero anterior.
6. La creación de una Unidad de Evaluación de las últimas novedades tecnológicas, pre- vista para la gestión de IoT.
7. Medidas de seguridad y un mantenimiento de un registro de tratamientos.
8. Realización de evaluaciones de impacto sobre la protección de datos.

La Agencia Española de Protección de Datos, indica que es absolutamente necesario que entre los desarrolladores, ingenieros y expertos en privacidad y seguridad exista un diálogo acerca del mejor tratamiento de los datos “teniendo siempre presente que el derecho a decidir sobre la propia información personal es un derecho fundamental y, como tal, es irrenunciable. En este terreno, no todo lo tecnológicamente posible resulta aceptable”, en palabras del director de la agencia, José Luis Rodríguez Álvarez.

**La legislación europea y la tecnología:**

La tecnología cambia radicalmente muchos procesos, es por ello por lo que la ley siempre es más lenta que los delitos cibernéticos, poniendo en desventaja todas aquellas situaciones que se pueden debatir y aprobar una Ley.

Al implementar nuevas tecnologías y no contar con el conocimiento suficiente para utilizarla, pone al usuario como un ciberdelincuente pasivo, puesto que hay acciones que a simple vista parecen no ser nocivas como por ejemplo descargar la serie favorita o incluso hacer una copia de los grandes éxitos musicales, sin embargo, muchas de estas acciones se titulan como delitos.

Actualmente, no se tiene un perfil específico de los ciberdelincuentes, pero sin lugar a duda, las actividades del día a día que se consideran cotidianas pueden estar involucrando acciones delictivas de las cuales no se tiene conocimiento.

Según la revista española La Vanguardia, cataloga a las generaciones de tres tipos:

- Las que han nacido con las nuevas tecnologías “bajo el brazo”.
- Las que se han tenido que adaptar al cambio, familiarizándose poco a poco.
- Por último, aquella generación que no ha querido inmiscuirse en la tecnología y no la utilizan.

Como bien se mencionó anteriormente, la tecnología cambia a grandes velocidades y es por ese motivo que España ha creado La Ley de la Ciencia, la

Tecnología y la Innovación, la cual entró en vigor el 3 de diciembre de 2011. Esta ley sustituye a la Ley de la Ciencia de 1986 y adapta la legislación al gran progreso experimentado por el sistema científico español en los últimos años, al mismo tiempo que facilita el cambio de modelo productivo.

Esta ley fue creada a partir de cinco situaciones que distinguen el actual contexto del sistema español de ciencia, tecnología e innovación del que existía en el momento de aprobación de la ley de 1986:

- El desarrollo de las competencias autonómicas en investigación e innovación requiere nuevos mecanismos de gobernanza basados en la cooperación.
- La creciente dimensión europea de España hace necesario un nuevo marco legal que regule los mecanismos de coordinación y de colaboración entre las administraciones públicas y facilite el protagonismo español en la construcción del espacio europeo de investigación y del espacio europeo de conocimiento.
- El salto cuantitativo y cualitativo en los recursos públicos exige una transformación del actual modelo de gestión de la Administración General del Estado hacia un nuevo esquema: la Agencia Estatal de Investigación.
- La consolidación de una comunidad científica y técnica profesionalizada, competitiva y abierta al mundo necesita un marco legal que apoye una carrera científica y técnica predecible, basada en méritos y socialmente reconocida.

- La transición hacia una economía basada en el conocimiento y en la innovación.

Es importante tomar en cuenta las medidas que España utiliza, porque sin lugar a duda son un ejemplo para Costa Rica en cuanto a la implementación de leyes basadas en el progreso tecnológico. Al igual que existen normativas y legislación para tratar y evitar fraudes, también tienen legislación para la innovación tecnología, ya que el objetivo primordial de esta Ley es promover la innovación y la transferencia de conocimiento al sector empresarial y a la sociedad. Aportando el marco de actuación de los agentes del sistema de ciencia, tecnología e innovación para el diseño e implementación de una gobernanza, en la que:

- Se reconoce a todos y cada uno de los agentes, y su papel en el sistema de ciencia, tecnología e innovación.
- Se define e implementa el papel propio de las administraciones públicas, de cada una y del conjunto de estas.
- Se define e implementa una gestión colaborativa del sistema público.
- Se establecen unas reglas de juego operativas, eficaces, eficientes y equitativas, basadas en la igualdad de oportunidades, para el conjunto y para cada uno de los agentes.

Cabe destacar que parte de la gobernanza en donde el sistema español de ciencia, tecnología e innovación está integrado por el conjunto de agentes, públicos y privados, que desarrollan funciones de financiación, de ejecución, o de coordinación en el mismo. En lo que al ámbito público se refiere, el sistema incluye las políticas públicas

desarrolladas por la Administración General del Estado y las desarrolladas por las comunidades autónomas.

La Administración General del Estado tiene la competencia de coordinación general de las actuaciones de investigación científica y técnica. La coordinación se asienta sobre:

- La Estrategia Española de Ciencia y Tecnología y la Estrategia Española de Innovación, de nueva creación, que constituyen el marco de referencia plurianual para alcanzar los objetivos compartidos por todas las administraciones territoriales.
- El Consejo de Política Científica, Tecnológica y de Innovación, formado por representantes de máximo nivel de la Administración General del Estado y de las comunidades autónomas.
- El Consejo Asesor de Ciencia, Tecnología e Innovación, que asesora al anterior y en el que están representados los agentes económicos y sociales.
- El Comité Español de Ética de la Investigación, que es el órgano consultivo encargado de velar por la ética de la investigación.
- El sistema de información sobre ciencia, tecnología e innovación.

En la Administración General del Estado, el órgano de coordinación previsto es la Comisión Delegada del Gobierno para Política Científica, Tecnológica e Innovación. Además, la ley crea dos instrumentos de planificación plurianual: el Plan Estatal de Investigación Científica y Técnica, y el Plan Estatal de Innovación.

### B. Canadá:

A menudo se comenta que el planteamiento canadiense en lo que se refiere a la protección de la vida privada o de los datos personales se sitúa a medio camino entre lo que se practica en Europa y lo que se hace en EE. UU, sin embargo, son dos temas distintos, debido a que Canadá eligió un marco hibrido.

En Canadá, en muchos sentidos, la cultura jurídica es fruto de la mezcla de tradiciones británicas y francesas que han marcado su historia. Empero, el modelo canadiense de protección de la vida privada también se debe en gran parte a la influencia contemporánea de la Unión Europea y de los EE. UU.

Los gobiernos de todo Canadá están comprometidos con la privacidad y la protección de la información personal utilizada en el curso de la prestación de programas y servicios al público. El gobierno federal está sujeto a la Ley de Privacidad. La mayoría de los gobiernos provinciales y territoriales están sujetos a leyes y políticas de privacidad similares que regulan la recopilación, uso y divulgación de información personal. Además, la Ley de Protección de Datos Personales y Documentos Electrónicos y la legislación provincial equivalente extienden la protección de la privacidad para regular la manera en que la información personal es administrada por el sector privado.

Los departamentos y agencias gubernamentales están implementando la prestación de servicios electrónicos para mejorar los servicios que proporcionan a los canadienses. Las implicaciones de privacidad y los riesgos pueden surgir debido al flujo intrainstitucional, interinstitucional o de jurisdicción de la información personal. La prestación electrónica de servicios también puede implicar al sector privado. Los

riesgos de privacidad inherentes a estas actividades necesitan ser identificados, evaluados y resueltos para asegurar que todas las mejoras del programa y del sistema respeten y fortalezcan la privacidad.

Las encuestas de opinión pública consistentemente demuestran que a los canadienses les preocupa la privacidad cuando su información personal se utiliza en el contexto de la prestación de servicios electrónicos. A menudo son reacios a enviar información personal a través de Internet para realizar transacciones electrónicas. Hay una serie de riesgos de privacidad asociados con los avances en la tecnología. Incluyen monitoreo de transacciones, minería de datos, servicios de directorio común, coincidencia de datos, el uso de identificadores personales comunes y los riesgos de robo de identidad y revelaciones no deseadas de información personal. El reto final es ayudar a los canadienses a entender cómo el gobierno maneja su información personal y confiar en que lo haga de manera responsable, independientemente del canal de servicio que elijan usar.

La Política de evaluación del impacto de la privacidad es una de varias herramientas diseñadas para enfrentar este desafío. Se basa en principios de privacidad comunes a todos los regímenes de protección de datos. Estos principios se enumeran en el "Código de Prácticas de Información Justa" en la Ley Federal de Privacidad, así como en los diez principios de privacidad adjuntos a la Ley de Protección de Información Personal y Documentos Electrónicos. Hay diferencias entre los códigos federales, provinciales y del sector privado que deben ser tenidos en cuenta al colaborar en iniciativas intercomunitarias. Sin embargo, se basan en el concepto fundamental de que las personas tienen derecho, sujeto a las disposiciones

explícitas de otra legislación, a controlar la recopilación, el uso y la divulgación de su información personal.

Las evaluaciones de Impacto de la Privacidad proporcionan un marco para asegurar que la privacidad se considere en todo el diseño o rediseño de programas o servicios. Las evaluaciones determinarán hasta qué punto las propuestas cumplen con todos los estatutos apropiados. Las evaluaciones ayudan a los gerentes y tomadores de decisiones a evitar o mitigar los riesgos de privacidad y promover decisiones de diseño de políticas, programas y sistemas completamente informadas.

La realización de evaluaciones de impacto de la privacidad es una responsabilidad de gestión compartida. Son esfuerzos cooperativos que requieren una variedad de habilidades, incluyendo las de los gerentes de programas, los especialistas técnicos y los asesores legales y de privacidad. El jefe adjunto de una institución federal, departamento u organismo es responsable de determinar si se requiere una EIP.

Es importante señalar que el proceso de evaluación no está destinado al desarrollo de nueva legislación. Se pretende que se adapte a los requisitos institucionales y de servicio particulares. Las directrices para la evaluación del impacto de la privacidad: Un marco para manejar los riesgos de privacidad se adjunta a la política para ayudar a las instituciones en la realización de evaluaciones. Son herramientas que las instituciones pueden adaptar para ayudarlas a evaluar los problemas de privacidad. El proceso también está destinado a ser un iterativo que se mantiene a lo largo del ciclo de vida de los programas o servicios a medida que se alteran o rediseñan.

El resultado final de la evaluación de impacto de la privacidad es la garantía de que todos los problemas de privacidad han sido identificados y resueltos o mitigados. La documentación asociada constituye la base para solicitar el asesoramiento y notificar al Comisionado de privacidad, así como para asegurar al público que las cuestiones de privacidad han sido abordadas.

Con el fin de proporcionar orientación a las instituciones gubernamentales sobre cómo evaluar los impactos sobre la privacidad de programas o actividades nuevos o sustancialmente modificados que involucren la creación, recolección y manejo de información personal, el 01 de abril del 2010 entra en vigor la “Directiva sobre la evaluación del impacto en la privacidad”, la cual sustituye la Política de Evaluación del impacto de la privacidad, emitida el 02 de mayo de 2002 también los Componentes de datos de la política de privacidad y Protección de datos emitida en 1993.

El Gobierno del Canadá se ha comprometido a garantizar que la protección de la privacidad es una consideración fundamental en la elaboración inicial y posterior administración de programas y actividades que incluyen información personal. En los últimos años, los canadienses y los parlamentarios se han preocupado por las complejas y sensibles cuestiones de privacidad que se derivan de las medidas antiterroristas proactivas, el uso de la vigilancia y la tecnología intrusiva a la privacidad, el intercambio de información personal a través de las fronteras y las amenazas a la privacidad. Los canadienses quieren ser informados de cómo su información personal es manejada y asegurada de su protección.

**La Ley sobre datos personales y documentos electrónicos:**

Se hará un recorrido por aspectos importantes de la Ley sobre datos personales y documentos electrónicos en donde se trata la información desde varios ámbitos de aplicación:

**Ámbito de aplicación de la Ley**

**Organismos cubiertos:** la Ley se aplica a cualquier organismo y, en su primera etapa, a los organismos que operen como «empresas federales». Un organismo puede ser una asociación, sociedad, persona o sindicato. La ley incluye una lista no exhaustiva de empresas federales sujetas a la ley. Aunque la mayoría de los organismos federales entran en esta definición, no todos los tipos de organismos son empresas federales.

**Actividad comercial:** la ley se aplica a los datos recogidos, utilizados o divulgados en el curso de actividades comerciales, lo que incluye toda transacción o actividad regular de carácter comercial, incluida la venta, el intercambio o el alquiler de listas de donantes, miembros y demás proveedores de fondos.

Así, las organizaciones no lucrativas o caritativas no están sujetas a la ley, salvo si se dedican a una actividad comercial.

La Ley tampoco se aplica cuando un organismo utiliza datos personales únicamente con fines periodísticos, artísticos y literarios, o bien personales y domésticos. Tampoco se aplica a los organismos cubiertos por la Privacy Act federal.

**Datos sobre salud:** la legislación excluye los «datos personales sanitarios» del ámbito de aplicación de la Ley durante el primer año tras su entrada en vigor (2.1), es decir, hasta el 1 de enero de 2002. Los datos personales sanitarios, referidos a una persona concreta, viva o difunta, son los siguientes:

- los datos sobre la salud física o mental de la persona;
- los datos sobre cualquier servicio sanitario prestado a la persona;
- los datos sobre la donación por parte de la persona de cualquier parte del cuerpo
    - de su sustancia corporal, o datos derivados de controles o exámenes de una parte
    - de su cuerpo o sustancia corporal;
- los datos recogidos al prestar servicios sanitarios a la persona, o
- los datos recogidos accidentalmente al prestar servicios sanitarios a la persona.

**Caso de WhatsApp:**

Noticia tomada de: http://www.elperiodico.com/es/tecnologia/20130129/whatsapp-viola-leyes-privacidad-canada-holanda-acceso-contactos-agenda-2305251

**"WhatsApp**, una de las aplicaciones más populares de mensajería instantánea a nivel mundial, viola las **leyes de privacidad** internacionales. Así lo han dictaminado las autoridades de **protección de datos** en **Canadá** y **Holand**a, que han determinado

que la aplicación no debería obligar a los usuarios a proporcionar el acceso a toda su agenda de contactos.

El servicio de mensajería, uno de los más usados en España, triunfa entre jóvenes y adultos, se ha popularizado como alternativa a los **SMS** y se coloca entre los **más vendidos** desde hace más de un año. De hecho, durante la pasada Nochevieja el servicio procesó 18.000 millones de mensajes (11.000 millones de salida y 7.000 de entrada), récord del servicio.

La Oficina del Alto Comisionado de Privacidad de Canadá (OPC) y la oficina holandesa de Protección de Datos, en un informe conjunto, han dictaminado que la aplicación **viola las leyes de privacidad** ya que los usuarios tienen que facilitar el acceso a todos los números de teléfono de su libreta de direcciones, incluyendo tanto a los usuarios como los no usuarios de la aplicación.

"Esta falta de elección contraviene las leyes de privacidad (canadiense y holandesa). Tanto los usuarios como los no usuarios deben tener el control sobre sus datos personales y los usuarios deben ser capaces de decidir libremente qué datos de contacto desean compartir con WhatsApp", ha dicho el presidente de la Autoridad de Protección de Datos holandés, Jacob Kohnstamm.

En septiembre del pasado año, **WhatsApp** introdujo el cifrado de los mensajes para mejorar su privacidad y se comprometió a realizar más mejoras en el futuro.”

Con respecto a la resolución de este tema que se dio en la oficina de Comisaria de Protección de la Vida Privada de Canadá, se analizó lo siguiente:

Se tenía tres preocupaciones con WhatsApp:

1. los mensajes no están cifrados, lo cual los hace vulnerables a las intrusiones,
2. WhatsApp recopila las agendas de direcciones de los usuarios y no diferencia entre las direcciones de los usuarios y de los no usuarios;
3. los parámetros de confidencialidad no son transparentes, principalmente con respecto a la ubicación que se muestra (p. ej., “oficina”, “gimnasio”, “café”, etc.).

La ventaja de Canadá en este caso es que, al disponer de un régimen de protección de los datos personales independiente – y, por la tanto, reconocido como “adecuado” en Europa –, se ha podido colaborar en esta investigación con el organismo responsable de la protección de los datos personales de los Países Bajos.

En los Países Bajos tenían las mismas preocupaciones con respecto a WhatsApp. Por ello, se decidió compartir los recursos para coordinar las investigaciones. En pocas palabras, los Países Bajos se encargaron del análisis tecnológico, mientras que la Comisaria se ocupó de la negociación con la empresa.

En menos de un año, se logró lo siguiente de la empresa:

1. la mejora de los parámetros de seguridad para cifrar los mensajes;
2. la presentación de una advertencia en el momento oportuno en la que se indica al usuario que está a punto de comunicar su ubicación, ofreciéndole la posibilidad de hacerlo o no;

3. la destrucción de los datos personales de los no usuarios cuando se comunica a la empresa la agenda de direcciones de un usuario con el fin de guardar tan sólo las direcciones de los otros usuarios.

### C. Estados Unidos

Este anexo del documento busca presentar una breve explicación de las leyes en Estados Unidos en lo que respecta a cada uno de los Principios Internacionales de Vigilancia y Derechos humanos. Aunque las leyes en Estados Unidos se desarrollan tanto a nivel federal como estatal, este anexo se focaliza en la Ley Federal. Dando énfasis en las leyes en torno a las investigaciones nacionales, relacionándola con tareas de inteligencia exterior y asuntos de seguridad nacional.

El objetivo de los Principios de Vigilancia y Derechos Humanos ("Principios") es brindar un marco de referencia a través del cual se puedan evaluar leyes, proyectos o prácticas actuales de vigilancia para asegurarse que sean consistentes con los derechos humanos. La elaboración de estos principios es una oportunidad única para analizar la experiencia de los Estados Unidos en temas clave como la regulación de la vigilancia estatal y el acceso a los datos electrónicos.

#### A. Principio de legalidad

En los Estados Unidos, la ley de vigilancia electrónica está contemplada en dos fuentes legales: (1) constitución federal o estatal; y (2) leyes federales o estatales.

La Cuarta Enmienda de la Constitución de los Estados Unidos se aplica al gobierno federal y a todos los estados, y prohíbe que el gobierno incurra en allanamientos y decomisos arbitrarios. Los organismos policiales deben obtener una "orden de allanamiento" antes de registrar un lugar, y eso incluye los dispositivos

electrónicos y otras formas de almacenamiento de datos digitales. La Constitución define “allanamiento” como (1) el traspaso de la propiedad privada por el gobierno con el fin de obtener información, o (2) una intromisión del gobierno en un lugar donde una persona ha manifestado una expectativa subjetiva de intimidad que la sociedad acepta como razonable.

**Electronic Communications Privacy Act, ECPA**

**Fondo.** La Ley de Privacidad de Comunicaciones Electrónicas y la Ley de Comunicaciones Electrónicas de Cables Almacenados se conocen comúnmente como la Ley de Privacidad de Comunicaciones Electrónicas (ECPA) de 1986. La ECPA actualizó la Ley federal de comunicaciones telefónicas de 1968, que abordó la interceptación de conversaciones utilizando líneas telefónicas "duras" pero no se aplica a la interceptación de computadoras y otras comunicaciones digitales y electrónicas. Varios actos legislativos posteriores, incluida la Ley USA PATRIOT, aclaran y actualizan la ECPA para mantener el ritmo de la evolución de las nuevas tecnologías y métodos de comunicación, incluida la reducción de las restricciones al acceso de las fuerzas del orden a las comunicaciones almacenadas en algunos casos.

**Provisiones generales.** La ECPA, según enmendada, protege las comunicaciones por cable, orales y electrónicas mientras se realizan dichas comunicaciones, están en tránsito y cuando están almacenadas en computadoras. La Ley se aplica al correo electrónico, las conversaciones telefónicas y los datos almacenados electrónicamente.

**Derechos Civiles y Libertades Civiles.** "La estructura de la Ley de Comunicaciones Almacenadas (SCA) refleja una serie de clasificaciones que indican

los juicios de los redactores sobre qué tipos de información implican mayores o menores intereses de privacidad. Por ejemplo, los redactores vieron mayor interés de privacidad en el contenido de los correos electrónicos almacenados que en la información de la cuenta del suscriptor. Del mismo modo, los redactores creían que los servicios informáticos disponibles "para el público" requerían una regulación más estricta que los servicios no disponibles para el público... Para proteger la gama de intereses de privacidad identificados por sus redactores, la [Ley] ofrece diversos grados de legalidad, la protección depende de la importancia percibida del interés de privacidad involucrado. Parte de la información se puede obtener de proveedores con una citación, otra información requiere una orden judicial especial y otra información requiere una orden de registro. Además, algunos tipos de procesos legales requieren notificación para el suscriptor, mientras que otros tipos no.

Bajo las leyes federales, la Ley de Privacidad de las Comunicaciones Electrónicas (Electronic Communications Privacy Act, ECPA) regula el acceso policial a diferentes formatos de datos electrónicos. La ECPA se ocupa de distintos formatos específicos de datos; El Título I es la *Ley de Escuchas* (Wiretap Act), que regula la forma en que el gobierno puede escuchar o interceptar el contenido de comunicaciones privadas, incluyendo conversaciones telefónicas. El Título II de la Ley ECPA es la *Ley de Almacenamiento de las Comunicaciones* (Stored Communications Act, SCA), que regula cómo el gobierno puede acceder al contenido de las comunicaciones electrónicas (como correos electrónicos, tweets, mensajes de texto, etc.), además de a otra información no vinculada con el contenido (como por ejemplo los registros de la ubicación de la torre de celular) desde un proveedor de comunicaciones electrónicas o

de almacenamiento en la nube. Por último, las leyes de *Pen Register/Trap and Trace Device (Pen/Trap)* regulan cómo el gobierno puede obtener información de enrutamiento y transmisión de llamadas telefónicas y otras formas de contenido electrónico, como las direcciones IP o los encabezados de los correos electrónicos.

La mayoría de los estados han adoptado (en su totalidad o en parte) estas disposiciones de la ley federal. En general, los estados son libres de adoptar una mayor protección legal de la que existe en la legislación federal, pero no pueden proporcionar una menor protección de la privacidad. Algunos pocos estados han implementado algunas medidas para mejorar sus leyes de privacidad electrónica, y por lo general se han movido mucho más rápido que el gobierno federal, que no ha podido actualizar la Ley ECPA de forma adecuada desde que fue promulgada en 1986.

### B. Principio de necesidad

Bajo la Cuarta Enmienda, las órdenes de allanamiento deben limitarse tanto como sea posible para evitar revolver las pertenencias de una persona como medida general, algo que comprende sus datos electrónicos. Esto también incluye exigir que la Policía le entregue al juez un inventario de todo lo que ha incautado, para que el tribunal pueda supervisarlo. Cuando se trata de datos electrónicos, un tribunal ha advertido (PDF) que los jueces deben ejercer una "mayor vigilancia" para asegurar que el gobierno no esté recolectando más datos de los necesarios.

Sin embargo, a la hora de limitar el acceso policial las leyes de privacidad electrónica en los Estados Unidos han tenido resultados dispares. La Ley de Escuchas contempla una fuerte protección a la privacidad, y requiere que la policía minimice las conversaciones telefónicas que intercepta para asegurarse de que sólo se están

capturando las conversaciones que conciernen a una actividad criminal. Sin embargo, las leyes de SCA y Pen/Trap no incluyen requisitos similares de minimización de los contenidos de las comunicaciones electrónicas o de la información de enrutamiento de Internet. Esto debe ser modificado, en particular en el caso de la Ley SCA, que potencialmente podría otorgarle a la policía un amplio acceso a los correos electrónicos y a otras formas de contenido electrónico.

### C. Principio de idoneidad

Cómo se explica más arriba, y como ha demostrado el escándalo Petraeus, los agentes del orden en los EE. UU no se han restringido a la hora de registrar y de incautar datos electrónicos.

Por si fuera poco, ha existido una gran presión de los organismos policiales en el Congreso para implementar políticas de retención de datos para una amplia gama de datos almacenados por los proveedores de comunicación, como mensajes de texto y la información de la dirección IP. Estas políticas exigirían que los proveedores guarden la información únicamente para el uso de las autoridades en un momento posterior, a menudo en contra de los deseos y los intereses comerciales de los mismos proveedores.

Es por esta razón que hay que luchar contra este tipo de políticas, que sirven sólo para el propósito gubernamental de vigilancia, y como se describe con más detalle a continuación, presentan riesgos para la seguridad.

### D. Principio de proporcionalidad

La Cuarta Enmienda de la Constitución de los EE. UU. Requiere que la policía obtenga una “orden de allanamiento” para llevar a cabo un “registro” o para incautar

datos electrónicos o físicos. Para obtener una “orden de allanamiento”, la policía debe demostrar ante un juez que existe una “causa probable”-- que es más probable que improbable -- de que las pruebas de un delito se encuentran en el lugar que desea registrar. Si el juez cree que la policía ha demostrado esta causa probable, puede emitir la orden de allanamiento, aunque el magistrado debe especificar en qué lugares específicos la policía puede buscar y determinar cuáles son los elementos que puede incautar.

Sin embargo, este estándar de causa probable se aplica sólo si el gobierno está realizando un “allanamiento”. Y hay muchas (de hecho, demasiadas) excepciones al requisito de una orden de allanamiento. Por otra parte, si bien es evidente que la Cuarta Enmienda se aplica a los datos almacenados en los dispositivos físicos de una persona, como su teléfono celular, no está tan claro si también se aplica a los datos almacenados por terceros y en la nube.

Algunos tribunales han interpretado la Cuarta Enmienda en el sentido de que una persona no tiene una expectativa razonable de privacidad en la información que entrega a otra, como un proveedor de Internet o una red social. Esto implica que la policía no tendría la obligación constitucional de obtener una orden de allanamiento para conseguir información del cliente y datos de compañías como Facebook, Twitter o Google. Por ejemplo, un tribunal de Nueva York dictaminó que los fiscales no necesitaban tener una orden de allanamiento para obtener datos de Twitter acerca de Malcolm Harris, un manifestante de Occupy Wall Street, y que en su lugar podía obtener información como sus *tweets*, o dirección IP de inicio de sesión con una citación, ya que los datos pertenecían a Twitter, y no a Harris. Lo mismo ocurrió con los

registros de Twitter de Birgitta Jonsdottir, diputada del Parlamento de Islandia, que el gobierno federal quería ver en relación con la investigación en curso sobre WikiLeaks. Otros tribunales han estado en desacuerdo, entendiendo que aún si se les entrega a terceros información como el correo electrónico, esto sigue estando protegido por la Constitución y las fuerzas del orden deben obtener una orden de registro.

Para empeorar las cosas, las leyes federales tampoco utilizan este estándar de causa probable para todas las formas de almacenamiento de la información. En su lugar, en Estados Unidos se aplican diferentes estándares de protección de la privacidad a las diferentes formas de información electrónica y digital.

La protección más importante de la privacidad se encuentra en la Ley de Escuchas, que no sólo requiere que la policía tenga una causa probable para creer que interceptando las llamadas telefónicas podrá probar un delito específico, sino que también requiere que las fuerzas del orden demuestren: (1) una causa probable de que mediante las escuchas se obtendrá información relacionada con un crimen, (2) que los procedimientos normales de investigación que se han intentado han fracasado o que razonablemente hubiera sido poco probable que tengan éxito si se hubieran intentado, o que son demasiado peligrosos, y (3) una causa probable para creer que el número de teléfono u otra “infraestructura” electrónica en que ocurra la comunicación a ser interceptada tienen una conexión con el delito o con la persona a ser interceptada.

Pero las otras partes de la Ley ECPA no tienen las mismas fuertes protecciones a la privacidad contenidas en la Ley de Escuchas. La SCA sólo exige que la Policía obtenga una orden de allanamiento para acceder al contenido de las comunicaciones electrónicas almacenadas electrónicamente por menos de 180 días. Sin embargo, en el

marco de la SCA se puede conseguir sin una orden de allanamiento acceder a las comunicaciones electrónicas más antiguas, así como otras formas de almacenamiento de datos electrónicos.

Si el gobierno puede demostrar ante un juez que existen “hechos específicos y objetivos” de que los datos son “relevantes y pertinentes para una investigación penal en curso”-- un estándar inferior a la causa probable para una orden de allanamiento -- la SCA le permite al gobierno obtener (1) el contenido de las comunicaciones electrónicas en almacenamiento electrónico de más de 180 días (por ejemplo, un correo electrónico antiguo en la bandeja de entrada); (2) el contenido de las comunicaciones electrónicas almacenadas en un proveedor de almacenamiento en la nube sin necesidad de previo aviso al abonado (como un PDF en Dropbox o en Google Drive); y (3) otros registros de clientes sin incluir el contenido (como información sobre la dirección IP o los registros de la ubicación de la torre de celular).

Y sólo con una citación –que no cuenta con ninguna supervisión judicial y que puede ser emitida por un abogado siempre que sea “relevante”–, el gobierno puede acceder a (1) el contenido de las comunicaciones electrónicas alojadas en un proveedor de almacenamiento en la nube, con previo aviso al cliente; y (2) otra “información sobre los abonados”, incluyendo el nombre del cliente, dirección, registros telefónicos locales o de larga distancia, o los registros de tiempo de sesión y la duración, el tipo y la duración del servicio (incluyendo la fecha de inicio), número de teléfono u otra número o identidad del abonado, incluyendo cualquier dirección de red asignada temporalmente, y medios y fuente de pago por el servicio.

Por último, las leyes de Pen/Trap permiten que el gobierno obtenga información de enrutamiento si puede probar ante un juez que los datos que busca son “relevantes para una investigación criminal en curso”.

Los diferentes estándares de estas leyes confunden a cualquiera. Los consumidores no están seguros de cuán protegida está su privacidad. Las agencias del orden, cómo se ha demostrado, son inconsistentes y poco claras al utilizar la ley en forma correcta para obtener los datos. Y, en este mundo moderno, los tribunales tienen dificultades para aplicar jurisprudencia de casos resueltos mucho antes de la llegada de tecnologías como los teléfonos celulares y las redes sociales.

Es necesario contar con un estándar uniforme que se aplique a todos los formatos de datos electrónicos y que contenga fuertes garantías de privacidad, como el que se recomienda en los principios, para beneficiar por igual a los consumidores y a las agencias del orden.

### E. Debido proceso

Como ya se explicó anteriormente, no todas las solicitudes de la policía para acceder a los datos electrónicos requieren autorización judicial previa. Y aun cuando la aprobación judicial es necesaria, los estándares para revelar información varían en función de los datos que se solicitan. Pero lo más problemático desde la perspectiva del “debido proceso” es la dificultad de probar violaciones de la ley, tanto en contextos penales como civiles.

Un acusado en un caso penal puede accionar legalmente contra un allanamiento del gobierno y las incautaciones de datos electrónicos que se producen sin una orden de allanamiento (o con una orden de allanamiento deficiente). Lo más frecuente es que

esto suceda después de que una persona ha sido acusada de un delito y presenta una moción para suprimir alguna evidencia. Pero la única evidencia que se puede suprimir es aquella que el gobierno tiene la intención de utilizar en contra del acusado en un juicio. Todo lo que una acción legal exitosa puede lograr es eliminar la capacidad del gobierno de utilizar ciertas formas de evidencia para condenar a la persona. Pero esa persona todavía puede ser procesada y encarcelada, en muchos casos, incluso sin el uso gubernamental de las pruebas. Y aunque los tribunales pueden "eliminar" la evidencia que se recolectó violando la Cuarta Enmienda, hay muchas excepciones al recurso de la supresión que disminuyen su eficacia. Por ejemplo, si la evidencia fue descubierta por agentes que actuaron de buena fe --en la creencia razonable, pero equivocada, de que estaban autorizados a confiscar el elemento--, esta no se eliminará. Además, los tribunales son reacios a dudar de la policía o sus colegas en la justicia a la hora de rever el proceso de allanamiento y de incautación. En consecuencia, la supresión de evidencia no es algo muy común.

La situación es aún menos prometedora cuando se trata de demostrar violaciones a las restricciones legales sobre el acceso del gobierno a los datos electrónicos. Ni la Ley de Escuchas, ni la SCA o Pen/Trap contienen un remedio de supresión legal para la incautación ilegal de los contenidos de las comunicaciones electrónicas o de la información de enrutamiento, y esto debe plantearse en el marco de la Cuarta Enmienda y no de las leyes en sí mismas.

Para las personas que han sido vigiladas ilegalmente sin ser acusadas de un delito, tanto la Ley de escuchas como la SCA permiten que un privado pueda iniciar acciones legales por intercepciones de audio e incautaciones de contenidos

electrónicos inadecuadas. Pero, aunque sea difícil superar los muchos obstáculos procesales para presentar una demanda civil contra el gobierno, es algo posible. Por ejemplo, generalmente se necesitará demostrar que la violación fue intencional, algo que puede ser difícil de probar. En los casos de incautaciones ilegales, la EFF ha recurrido en algunas oportunidades a la Ley de Protección de la Privacidad (Privacy Protection Act) --que limita la capacidad del gobierno para buscar o apoderarse de los elementos relacionados con la publicación de un periódico, revistas u otras publicaciones, para demandar al gobierno.

A veces, los asuntos de seguridad nacional pueden presentar una barrera difícil. La EFF ha demandado tanto a la Agencia de Seguridad Nacional (NSA, por su sigla en inglés) y a AT&T por el programa del gobierno federal de escuchas telefónicas sin orden judicial que comenzó durante la presidencia de George W. Bush y que tuvo variados niveles de éxito. El caso en contra de la NSA se ha movido lentamente, con el gobierno tratando de conseguir que se desestime porque el litigio obligaría a revelar "secretos de Estado". Y el Congreso aprobó una ley que le otorga inmunidad judicial a AT&T, poniendo efectivamente un punto final a cualquier acción legal que discuta su papel en el programa de escuchas telefónicas sin órdenes judiciales.

### F. Notificación al usuario

La ley federal permite que las agencias del orden exijan que los proveedores mantengan en silencio las solicitudes de los datos de clientes. Por ejemplo, como parte del Acta PATRIÓTICA post 9/11, el FBI puede eludir a los tribunales y emitir cartas administrativas bajo su propia órbita, llamadas Cartas de Seguridad Nacional (PDF) (NSLs, por su sigla en inglés), y enviarlas a las empresas de telecomunicaciones. Las

NSLs no sólo exigen que las empresas revelen información acerca de un cliente, sino que también requieren que las compañías no informen al cliente de ese pedido, manteniendo en secreto incluso la recepción de una de estas cartas. Sólo ha habido un pequeño número de acciones legales contra esta práctica. Incluso fuera del contexto de Seguridad Nacional, la SCA permite al gobierno retrasar el aviso a un usuario sobre una solicitud del gobierno de acceder a los contenidos de las comunicaciones electrónicas por un máximo de 90 días. Además, existe la posibilidad de solicitar una prórroga adicional de 90 días.

En ausencia de cualquier limitación legal de la capacidad de un proveedor de servicios de notificar a sus usuarios de estas solicitudes de datos, las empresas tienen un historial dispar a la hora de informar a sus clientes. Twitter, por ejemplo, tiene la política de comunicar a sus usuarios sobre todas las solicitudes de información antes de divulgar los datos, a menos que esté prohibido por orden judicial. La política de Facebook es más imprecisa, dando a entender que la policía debe obtener una orden judicial para evitar la notificación, pero también permitiendo no revelar la información si esto “diera lugar a un riesgo de daños”.

No se debe subestimar la importancia de las notificaciones a los usuarios, quienes deben saber acerca de las solicitudes sin demora para salvaguardar sus datos y solicitar asistencia jurídica y orientación. Cualquier solicitud gubernamental para demorar la notificación debe limitarse a circunstancias de emergencia, y este plazo debe ser lo más corto posible. Debe rechazarse el mecanismo secreto de las NSLs, de acceso vedado a los datos de un usuario. También debe rechazarse el enfoque de la SCA de largos períodos de notificación tardía. Al instaurar este tipo de normas para las

agencias del orden, se alentará a que las empresas informen a sus usuarios de las solicitudes de aplicación de las autoridades con mayor frecuencia que la actual.

### G. Transparencia en la vigilancia del gobierno

La ley de EE. UU. está totalmente ausente cuando se trata de la transparencia. Con la excepción de las órdenes de interceptación bajo la Ley de Escuchas, para lo cual el gobierno debe publicar un informe anual sobre el uso de las escuchas telefónicas, existe muy poca transparencia sobre la frecuencia con la que el gobierno trata de acceder a las pruebas electrónicas (e incluso el Departamento de Justicia ha estado bajo la lupa por no entregar al Congreso registros y estadísticas completos de la Ley de Escuchas, como lo requiere la ley). Pero más allá de las órdenes de escuchas, hay poca transparencia por parte del gobierno o de los proveedores de la cantidad de información que el gobierno está recolectando, y con qué fines.

En consecuencia, la información sobre el uso gubernamental de los diversos formatos de datos electrónicos sólo ha salido a la luz a través de una demanda del Congreso para obtener información sobre las solicitudes a las compañías de telefonía celular o de una solicitud de acceso a la información presentada por la Unión Americana de Libertades Civiles (ACLU, por su sigla en inglés) a la policía que exigía información sobre la utilización de los datos de los registros de la ubicación de la torre de celular. También existe más información gracias a los informes elaborados por empresas como Google y Twitter sobre el número de solicitudes nacionales e internacionales del gobierno sobre datos del usuario. Lamentablemente, estos informes son la excepción, y no la regla. La mayoría de las empresas de tecnología no revelan

voluntariamente estos datos, y los intentos a nivel estatal para exigir que así lo hagan se han encontrado con una fuerte oposición de las empresas.

En definitiva, lo que demuestran estas peticiones informales es que las solicitudes del gobierno para acceder a datos de los usuarios están en aumento. Por lo tanto, es necesaria una mayor transparencia para permitir que los usuarios vigilen a estas crecientes demandas y para prevenir los abusos.

### H. Supervisión

En los Estados Unidos, la supervisión presumiblemente proviene de distintas ramas del gobierno. Los organismos policiales dentro de la rama ejecutiva cuentan con inspectores generales que revisan las prácticas internas, mientras que las agencias de seguridad nacional reportan al Director de Inteligencia Nacional. En el poder legislativo, los comités de supervisión del Congreso reciben los informes de los diferentes organismos policiales. Y la rama judicial recibe las acciones legales contra la vigilancia del gobierno.

Pero ninguno de estos comités de vigilancia es verdaderamente independiente. Incluso los comités supuestamente “independientes” no lo son en sentido literal. Por ejemplo, la Junta de Supervisión de Inteligencia (IOB, por su sigla en inglés) es una junta independiente de supervisión civil, cuyos miembros son designados por el presidente, que tiene la misión de asegurar que el gobierno cumple con la ley durante las investigaciones de inteligencia exterior. Sin embargo, sus acciones, e incluso por un tiempo sus miembros, están bajo un manto de secreto. A nivel de inteligencia nacional, se creó la Junta de Vigilancia de Derechos Civiles y Privados (PCLOB, por su sigla en inglés) con la intención de actuar como una institución de control independiente de las

prácticas de vigilancia domésticas. Pero esta junta ha sido en gran medida ineficaz, abandonada tanto por los presidentes Bush como por Obama, y, a pesar de su relativamente corta existencia, ya fue reorganizada (PDF). Tanto la IOB como la PCLOB existen dentro (y responden) a la oficina del presidente, con lo que su verdadera "independencia" plantea serias dudas.

Así, además de los esfuerzos de varias organizaciones de libertades civiles como la EFF, ACLU, Center for Democracy and Technology (CDT) y el Electronic Privacy Information Center (EPIC), entre otros, que buscan dar cuenta de las prácticas de vigilancia del gobierno a nivel nacional, no existe ningún comité efectivo, público y de supervisión independiente encargado de examinar las prácticas nacionales. Y, por supuesto, a pesar de sus mejores esfuerzos, estas organizaciones están limitadas en cuanto a la información a la que pueden acceder. La mayor parte de los datos se obtienen gracias a procesos judiciales y solicitudes de acceso a la información, y estas organizaciones no están ciertamente en condiciones de examinar, en la mayoría de los casos, información secreta o clasificada.

Para evitar abusos de las libertades civiles y arrojar una mayor transparencia sobre las prácticas de gobierno es necesario que exista un comité de supervisión más formal y verdaderamente independiente, que se encargue de revisar tanto las prácticas de vigilancia a nivel nacional como internacional y las tareas de inteligencia.

## I. Integridad de las comunicaciones y los sistemas

Para contar con un mundo digital seguro es fundamental la integridad de la arquitectura de la red. Sin embargo, el gobierno de EE. UU. ha librado una larga batalla en aparente contradicción con este objetivo. A pesar de los evidentes riesgos para la

seguridad y la privacidad, ha instado al Congreso a implementar largos períodos obligatorios de retención de datos, empujados por la prohibición del cifrado-- una herramienta crucial para proteger las comunicaciones electrónicas --y todo mientras hacía lobby para garantizar el acceso, asegurándose la existencia de su propia puerta trasera en los sistemas de comunicación.

La propuesta de una puerta trasera en las comunicaciones por Internet proviene de un esfuerzo para actualizar el Programa de Asistencia para el Cumplimiento de la Ley de Comunicaciones (Communications Assistance for Law Enforcement Act, CALEA). En 1994, el Congreso aprobó CALEA, obligando a las compañías telefónicas a rediseñar sus arquitecturas de red para facilitar las escuchas telefónicas. Pero esto excluía específicamente los datos que viajan a través de Internet. A medida que se expandió el uso de la web, las agencias del orden han aplicado una creciente presión sobre el Congreso para actualizar CALEA y exigir a los proveedores que aseguren que sus redes de comunicación tienen una puerta trasera que también permita al gobierno interceptar las comunicaciones por Internet. Esta actualización propuesta a CALEA (más que nada como una demanda policial de retención de datos) tiene evidentes consecuencias negativas de largo alcance para la privacidad, la seguridad y la innovación.

Por otra parte, hubo momentos en que el gobierno aplicó mano dura a individuos que dejaron en evidencia vulnerabilidades de seguridad y fallas. Un investigador fue recientemente condenado por un delito federal que prohíbe el acceso ilegal a una computadora, cuando reveló un error en la página web de AT&T. Este error le permitió obtener las direcciones de correo electrónico de los usuarios de iPad de AT&T con sólo

visitar un sitio web sin restricciones, y sin pasar por las barreras tecnológicas para acceder a esos datos. En otro caso, la Autoridad de Transporte de Massachusetts intentó silenciar a un grupo de investigadores que tenían previsto presentar en una conferencia un trabajo acerca de las vulnerabilidades que descubrieron en el sistema de pago de tarifas de tránsito.

Básicamente, el gobierno debería alentar a las empresas de tecnología para que mantengan los datos de sus clientes de forma segura. Sin embargo, al minimizar el riesgo de divulgación también se debe prohibir que el gobierno acceda a esta información por una puerta trasera y se debe limitar la retención de datos. Al mismo tiempo, los investigadores de seguridad que no acceden a la información electrónica de forma ilegal no deberían ser tratados como criminales simplemente por informar al público sobre sus hallazgos.

### J. Garantías para la cooperación internacional

Lamentablemente, muchos países han tratado de exportar algunas de las peores prácticas de vigilancia de los Estados Unidos. Y, desafortunadamente, estos países han utilizado la cooperación internacional como un medio para vigilar a los ciudadanos, violando sus respectivas leyes internas. Por ejemplo, en la investigación penal de los EE. UU. de la página web de Megaupload y su fundador Kim Dotcom por infracción de derechos de autor, se descubrió que las autoridades de Nueva Zelanda no sólo obtuvieron órdenes de allanamiento incorrectas para la casa de Doctom pero que también lo habían espiado ilegalmente mediante el control de todo el tráfico de Internet que entraba y salía de su casa.

Es por ello por lo que es importante asegurarse de que cualquier ley o tratado que legitima la vigilancia masiva deba ser cuestionado. Y todo tratado de asistencia legal mutua (MLAT, por su sigla en inglés) debe asegurar que frente a leyes en conflicto se aplicará aquella norma que ofrezca mayores garantías.

### K. Prevenir el acceso ilegítimo

Como se ha explicado anteriormente, en contextos de carácter no penal, las personas que han sido víctimas de vigilancia ilegal disponen de recursos tanto bajo la Ley de Escuchas y la SCA para iniciar acciones legales. Pero los tribunales y las legislaturas deberían asegurarse de que no existen barreras excesivamente onerosas para demandar.

### L. Costos de vigilancia

Poco se sabe sobre el costo de la vigilancia que ejerce el gobierno en los EE. UU., aun cuando los proveedores de servicios han insistido reiteradamente en que no están obteniendo ganancias de los organismos policiales y que sólo están recuperando los costos. Un completo pedido de acceso a la información de la ACLU en 2012 reveló en detalle los precios que las empresas cobran para que los organismos policiales accedan a las escuchas telefónicas y los registros de la ubicación celular, revelando que las sumas que cobran los proveedores varían, y que muchos no le cobran nada a los organismos en respuestas a situaciones de emergencia.

Asegurarse que los organismos policiales son responsables de los costos de la vigilancia puede en muchos casos servir como un estandarte contra el abuso del gobierno: cuanto más oneroso sea obtener los registros electrónicos y contenidos, más cuidadoso será el gobierno en sus búsquedas.

**Privacy Shield**

Este nuevo acuerdo viene a sustituir al de Safe Harbour que fue anulado por el Tribunal de Justicia de Unión Europea en octubre de 2015 por no garantizar el suficiente nivel de protección establecido.

Desde la anulación del Safe Harbour se han suscitado muchas dudas y temores en cuanto a la responsabilidad por el uso de aplicaciones y herramientas que almacenan y tratan datos de usuarios europeos en Estados Unidos (Mailchimp, Dropbox, Drive, Facebook, etc.) y las consecuencias sancionadoras por el incumplimiento de la normativa europea de protección de datos personales.

Este nuevo acuerdo se fundamenta en establecer un sistema de auto-certificación mediante el cual las empresas de EE. UU. se comprometen a cumplir un conjunto de principios de privacidad, así como en su revisión conjunta entre la Comisión Europea y el Departamento de Comercio de EE. UU., en colaboración con las entidades de control y protección de datos de los estados miembros de la Unión Europea.

Privacy Shield recoge las obligaciones que deben cumplir las empresas norteamericanas para conseguir la certificación del Departamento de Comercio de EE. UU., así como las garantías ofrecidas por las autoridades de EE. UU. para evitar el tratamiento masivo e indiscriminado de datos de personas físicas europeas.

Esto quiere decir que las empresas europeas que transfieran datos de usuarios europeos a empresas en Estados Unidos no tendrán que solicitar autorización previa a

la Agencia de Protección de Datos sino verificar que la empresa a la que transfieren datos se haya en adherida al acuerdo y comunicar la transferencia.

Dado que las empresas norteamericanas que realicen esta importación de datos personales de usuarios europeos tendrán que renovar anualmente su certificación de adhesión al acuerdo, verificando que sus políticas cumplen los principios establecidos en el acuerdo, será conveniente revisar la Lista Shield con regularidad para verificar que se continúa dentro de los parámetros de cumplimiento.

Las empresas de Estados Unidos deberán poder probar que cumplen los **principios** establecidos en el acuerdo Privacy Shield, entre los cuales destacamos:

1. **Principio de notificación y opción**: Proporcionar **información** a los usuarios **en sus políticas de privacidad sobre el tratamiento de los datos** personales (tipo de datos recopilados, finalidad del tratamiento, el derecho de acceso y de oposición, las condiciones para las transferencias posteriores, el régimen de responsabilidad, etc.).

Deberán además facilitar en sus políticas el enlace a la web del Departamento de Comercio en la que se tenga publicada la Lista Shield, así como la web de un proveedor adecuado para la solución de alternativa de controversias que puedan suscitarse en relación con el tratamiento de datos transferidos.

Deberá además darse la opción a los interesados de elegir si su información personal se transfiere a una tercera parte o si su información se utiliza para un fin distinto al que se recabaron los datos inicialmente.

2. **Limitar el almacenamiento y tratamiento de datos a lo estrictamente relevante y compatible con la finalidad para la que fueron recabados** conforme al consentimiento prestado por el titular de los datos.

3. **Garantizar la obtención del consentimiento expreso y explícito en sentido afirmativo a la finalidad concreta** por parte del titular de los datos y, más concretamente en caso de tratamiento de datos sensibles (opt in), así como el principio de oposición (opt out) a los usuarios en el caso de que la finalidad con la que se recabaran los datos haya sido modificada.

4. **Conservar los datos sólo durante el tiempo que sirve a la finalidad para la que fueron inicialmente recogidos** o autorizados. El tratamiento de datos personales extralimitado a dicho plazo sólo se permite en la medida que el tratamiento sirva para fines de archivo en interés público, periodismo, literatura y arte, ciencia e investigación histórica y análisis estadístico.

5. **Tomar las medidas de seguridad técnicas y organizativas "razonables y adecuadas" a la recogida de datos, su almacenamiento y tratamiento**, teniendo en cuenta los riesgos involucrados en el tratamiento y la naturaleza de los datos.

Entre estas medidas no debe olvidarse la **necesaria firma de contrato con el encargado de tratamiento de datos** en el caso de cesión de estos con dicha finalidad, obteniendo así el mismo nivel de compromiso a la protección y medidas de seguridad que garanticen el cumplimiento del acuerdo.

6. **Garantizar el derecho de acceso** al titular de los datos, así como a la c**orrección, modificación y eliminación de información personal inexacta o tratada en incumplimiento de los principios** establecidos en el acuerdo.

7. Proporcionar mecanismos robustos para asegurar el cumplimiento de los principios y establecer las vías necesarias de recurso y reparaciones efectivas para los interesados de la Unión Europea, cuyos datos personales sean tratados de forma contraria al acuerdo.

### 2.4.3 Comparación del proceso de protección de datos personales en Europa, Estados Unidos y Canadá

El Consejo de Europa reconoce el derecho a la privacidad como un "derecho humano fundamental".[1] Además, la Declaración Universal de Derechos Humanos y el Pacto Internacional de las Naciones Unidas sobre los Derechos Civiles y Políticos definen a la privacidad como un derecho ("Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.")[2] Los dos tratados explican luego: "Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".[3]

En consecuencia, la visión europea del derecho a la privacidad cubre todos los aspectos de la vida del individuo. Con base en esta perspectiva expansiva del derecho a la privacidad, la legislación europea correspondiente cubre el procesamiento de datos personales con organizaciones gubernamentales y privadas.[4] El Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal ("el Convenio") define en términos generales los datos

personales como “toda información relacionada con una persona identificada o identificable” y describe los principios de la protección de datos, que han servicio de base para la legislación en este campo en todo el mundo. [5] Más tarde, en la Directiva sobre protección de datos de la Unión Europea (“la Directiva”) se afirmó que los principios sobre protección de datos consagrados en los consiguientes principios del Convenio fijaban el nivel estándar de la protección de datos para los miembros de la Unión Europea y, aún más importante, reconoció el derecho de los particulares a la privacidad.[6] A raíz de esta preocupación expansiva por el derecho a la privacidad del individuo, la Directiva pasa a admitir la transferencia de datos personales a países de fuera de la Unión Europea sólo cuando el país afectado “garantice un nivel de protección adecuado [de los datos]” o si demuestra que los datos quedarán debidamente protegidos una vez que hayan sido transferidos.[7] De esta manera, la Directiva amplía a los países fuera de sus fronteras el alcance de la protección otorgada a los datos personales originados en la Unión Europea.

El alcance de la Directiva se ha extendido más allá de las fronteras europeas, y ha incidido en la regulación de la protección de datos en todo el mundo, al obligar a otros países con empresas interesadas en transferir datos personales a examinar su propia legislación sobre protección de datos y, de ser necesario, modificarla para satisfacer los estándares de la Unión Europea.[8] Cabe destacar, sin embargo, que la Comisión Europea emprendió una revisión de la Directiva en 2010 debido, en parte, a que “es preciso mejorar, en general, los mecanismos existentes de transferencia internacional de datos personales”. El vicepresidente de la Comisión Europea responsable de la Agenda Digital ha explicado también que el marco regulatorio relativo

a la protección de datos de la Unión Europea debe ser actualizado conforme a la era digital a fin de proteger los derechos fundamentales y, al mismo tiempo, “tener la mejor economía y mejores condiciones de vida que permiten las tecnologías digitales”. Se anticipa que hacia finales de año se presente una propuesta para una nueva ley que reemplace a la Directiva.

En Estados Unidos, los orígenes del derecho a la privacidad pueden encontrarse en su Constitución y en el derecho consuetudinario.[9] En uno de los artículos más influyentes de ese país sobre el derecho a la privacidad, los autores argumentaban que el de la privacidad era el “derecho a que a uno lo dejen tranquilo.”[10] Desde entonces, la Suprema Corte de Estados Unidos se ha pronunciado en favor de los intereses privados derivando el derecho a la privacidad de la Constitución.[11] En sus decisiones, la Suprema Corte ha declarado que la Constitución protege el interés de las personas de evitar la divulgación de sus asuntos personales y el interés en la independencia para tomar cierto tipo de decisiones importantes.[12] Sin embargo, la Suprema Corte también ha sostenido que el derecho a la privacidad no era absoluto y que el interés de una persona por su privacidad debe ponderarse frente a la competencia del interés público.[13]

En Estados Unidos, el derecho a la privacidad, a diferencia del enfoque europeo, protege sólo contra la intrusión del gobierno federal en los asuntos privados de las personas. Por ende, la legislación específica sobre la cuestión de la protección de los datos personales se limita a los datos tratados o custodiados por el gobierno federal.[14] Fuera de unas pocas leyes que tratan de la información personal financiera y médica, Estados Unidos no cuenta con una legislación que rija el procesamiento de datos

personales por entidades privadas.[15] Por el contrario, el sistema de ese país prevé la auto regulación por parte de los sectores económicos en materia de datos personales manejados por entidades privadas. En tal sentido, los sectores de la actividad privada de Estados Unidos están básicamente autorregulados, incluida la mayoría de las empresas privadas, las actividades de búsqueda de datos, los depósitos de datos personales y los sitios de redes sociales de Internet, entre otros. Sin embargo, debe tenerse en mente que también existen muchas leyes en materia de privacidad de aplicación estatal. Durante el último año, la Comisión Federal de Comercio y el Departamento de Comercio de Estados Unidos han publicado proyectos de informes y recomendaciones para lograr que la privacidad sea protegida de manera más amplia y en todo el país. En tales proyectos han dejado en claro que el objetivo de asegurar que el creciente y cambiante mercado de la información tenga sus bases en la promoción de la privacidad, la transparencia, la innovación empresarial y las opciones para el consumidor.[16] Asimismo, el Congreso de ese país ha tomado en consideración varias propuestas relativas a la privacidad.

En los casos en que quieran cumplir con directrices predeterminadas sobre el manejo de datos personales, los particulares pueden ampararse en una disposición de la Comisión Federal de Comercio de Estados Unidos por la que certifica que la entidad en cuestión establece un nivel adecuado de protección de los datos personales.[17] Aunque esta disposición tiene carácter voluntario en el contexto interno, las empresas que reciben datos personales de miembros de la Unión Europea deben emplear estas pautas para el manejo de información transfronteriza. Además, el hecho de que la legislación estadounidense se centre exclusivamente en la protección de la información

de las personas que procesa el gobierno federal, no queda claro cuál es el nivel de protección asignado a los datos personales procesados por entidades privadas en Estados Unidos y, luego transferidos a otro país.[18] En Canadá, la privacidad es protegida gracias a un régimen legislativo de varios niveles. Las actividades de las instituciones gubernamentales en relación con los datos personales están sujetos a la Carta de Derechos y Libertades de Canadá, que forma parte de la Constitución. A este respecto, el Tribunal Supremo de Canadá ha reconocido que el derecho a oponerse a un registro e incautación, mencionado en la sección 8 de la Carta, protege contra toda injerencia injustificada por parte del Gobierno en la privacidad que razonablemente espera tener un individuo. Aunque esta disposición no es una prohibición absoluta a la injerencia del Estado en la privacidad de una persona, sí permite asegurar que cualquier actividad del Gobierno en este sentido sólo represente una interferencia razonable. El Gobierno federal y todas las provincias y territorios también tienen leyes que rigen la recolección, uso, divulgación y eliminación de la información personal en manos de entidades gubernamentales. Con respecto a la protección de datos en el sector privado, Canadá se adhirió a las Directrices de la OCDE en 1984 y promovió la autorregulación, como ocurrió en Estados Unidos. En el año 2000, el Parlamento de Canadá aprobó una ley de aplicación general en toda la nación para la protección de información personal. En dicha ley se estableció un conjunto de normas que han de aplicarse uniformemente en el mercado canadiense, de modo que existan garantías tanto para los consumidores como para las empresas y se fomente la confianza en el comercio electrónico. Esta ley se ajusta a las leyes sobre la privacidad en el sector privado, en el ámbito subnacional en cuanto que son "sustancialmente similares" a la

ley federal. Algunas provincias han promulgado leyes que son también aplicables a las actividades no comerciales del sector privado.

### 2.4.4 Protección de datos en América Latina

**Habeas data**

Literalmente, habeas data significa “debes tener los datos”.[19] Aunque sus orígenes pueden encontrarse en Europa, el habeas data en América Latina es una acción que se entabla ante la justicia para permitir la protección de la imagen, la privacidad, el honor, la determinación por sí misma de la información y la libertad de información de una persona. El habeas data es un mecanismo que otorga a la persona la facultad de detener el abuso de sus datos personales En general, permite a la persona el acceso a la información personal en las bases de datos públicas o privadas, la capacidad de corregir y actualizar los mismos y la posibilidad de asegurarse de que los datos delicados mantengan su confidencialidad, y permite el retiro de los datos personales delicados que pueden atentar contra el derecho a la privacidad. A diferencia de las leyes de protección de datos de Europa y Estados Unidos, el habeas data no exige que las entidades públicas y privadas protejan por su iniciativa los datos personales que procesan, sino que sólo requiere que la persona agraviada, tras presentar una denuncia ante la justicia, obtenga acceso y la capacidad de rectificar todo dato personal que pueda atentar contra su derecho a la privacidad. Además, el habeas data se reserva como recurso legal sólo para personas a las que se compromete su privacidad. Por otra parte, este mecanismo puede no otorgar un recurso legal a una persona agraviada si sus datos personales han sido transferidos fuera del país. En consecuencia, la protección del habeas data es más limitada que la

del modelo europeo. Algunos países como Argentina, por ejemplo, han aprobado leyes de protección de los datos personales que complementan la legislación ya vigente de habeas data.

**Legislación reciente**

México aprobó una nueva Ley federal sobre la protección de los datos personales, en julio de 2010. A diferencia del criterio de Estados Unidos, que principalmente regula el procesamiento de datos por entidades del Estado, la nueva ley mexicana regula el tratamiento de datos personales exclusivamente por el sector privado. Además, el Instituto Federal de Acceso a la Información, que antes de la aprobación de la nueva Ley sobre Datos Personales ejercía la supervisión exclusiva del acceso a información en custodia de organismos estatales, ahora posee facultades ampliadas para incluir la supervisión del sector privado en lo que hace a los datos personales, aunque la nueva ley, paradójicamente, no se aplica a los datos personales procesados por organismos estatales. Existen interrogantes en relación con el funcionamiento de la nueva ley mexicana, marca una evolución importante en la legislación sobre protección de la privacidad y de los datos en las Américas y, junto con los regímenes de la Unión Europea, Estados Unidos y del habeas data, ofrece una serie de principios y normas que ayudan a regular esta importante esfera dentro de los estados miembros de la OEA.

Colombia aprobó en 2010 una nueva ley general de protección de datos, la cual incorpora los principales lineamientos internacionales sobre la materia al igual que elementos innovadores como el de la autorregulación. La nueva ley se encuentra actualmente en revisión por parte de la Corte Constitucional y se espera que el fallo

correspondiente se emita en junio de 2011. La ley aprobada por el Congreso regula de manera integral el derecho que tienen todos los titulares a conocer, actualizar y rectificar la información que sobre ellos repose en bases de datos o archivos. Las disposiciones contenidas en esta ley son aplicables para bases de datos tanto de naturaleza pública como privada, estableciendo así, bajo una sola normativa las obligaciones de responsable y encargados, tanto del sector público como privado.

### 2.4.5 Principio de la Organización de las Naciones Unidas (ONU)

La Organización de la Naciones Unidas (ONU) está conformada por la participación de 193 países miembros, siendo parte de este estudio debido a que la investigación toma en cuenta un tema de discusión mundial que tienen dichos miembros frente al esfuerzo que hacen para regular adecuadamente el uso de los datos personales de sus habitantes.

Desde 1945, Costa Rica forma parte de la organización y a pesar de que no ha tratado el tema de los datos personales frente a la ONU, sí ha tomado en cuenta algunos criterios que se han emitido por parte de los estados miembros.

La ONU emitió el 14 de diciembre de 1990 una directriz titulada “Principios rectores para la reglamentación de los ficheros computarizados de datos personales”, con la finalidad de servir de base legal para que los Estados miembros lo adoptaran y de esa forma proveer seguridad jurídica sobre la forma como las personas, ya sean físicas o jurídicas de los países, manipulan la información personal de sus habitantes. Esta directriz está conformada por una serie de principios esenciales para apoyar las normas legales internas de las diferentes legislaciones internaciones.

Costa Rica, tomó como base de estudio y guía la directriz emitida por la ONU y adoptó para la elaboración de la ley que hoy rige, algunos de los principios, no lo hizo desde el mismo concepto implícito en la directriz, pero sí buscó la forma de acoplarlo a las necesidades de los costarricenses de ver protegidos sus derechos de la personalidad y resguardo de la intimidad. Algunos de los principios que guardan similitud en ambos instrumentos jurídicos por conceptualizarlo de alguna manera, desde una misma interpretación, son los que describe la Ley en la sección I, artículos 4 al 8. Al analizar los principios rectores para la reglamentación de los ficheros computarizados, se observa que el primer principio de la licitud y lealtad, invocado en la directriz de la ONU, se refiere a la prohibición de recopilar los datos personales a través de procedimientos desleales. Al compararlo con lo estipulado en la normativa costarricense relacionado al tratamiento de los datos personales, se encuentra la adopción de este principio internacional de licitud y lealtad, en el artículo 6, inciso 4, donde se refiere al principio de la calidad de la información, con respecto a la adecuación, el cual dispone que "los datos de carácter personal serán recopilados con fines determinados, explícitos y legítimos (…)". El segundo principio sugerido en la directriz es el principio de exactitud, el cual obliga a las personas creadoras de las bases de datos, por verificar que la información custodiada sea exacta; este principio está ligado también al artículo 6, inciso 3, bajo el mismo nombre, sobre la calidad de la información, y exactitud, "… los datos de carácter personal deberán ser exactos (…)". El tercer principio corresponde a principio de finalidad, el cual establece que la creación y utilización de un fichero debe ser especificado y justificado, y se encuentra ligado al capítulo II, artículo 6 inciso 4, sobre adecuación: "… las bases de datos no pueden

tener finalidades contrarias a la ley (…)". Otro principio se refiere al principio de acceso de la persona interesada, ya que toda persona tiene derecho a conocer la información que sobre ella administren los ficheros; en Costa Rica lo regula expresamente el artículo 7, sobre los derechos que le asisten a la persona, donde se señala que "se garantiza el derecho a toda persona al acceso de sus datos personales. El principio sobre seguridad señala que se deben adoptar medidas apropiadas para proteger los ficheros, lo tutela la ley costarricense en la sección III, artículo 10, sobre seguridad de los datos: "El responsable de los bases de datos deberá de adoptar las medidas necesarias para garantizar la seguridad de los datos".

De acuerdo el principio de la ONU relacionado al control y sanciones, cada legislación debería designar a la autoridad, de conformidad con su sistema jurídico, para controlar y fiscalizar el respeto de los principios anteriormente enunciados. En la ley costarricense se ubica en el capítulo V, sección II, artículo 28, el cual describe tres tipos de categorías: faltas leves, faltas graves y faltas gravísimas para diferentes circunstancias. El otro principio de la directriz se refiere al campo de aplicación, y sugiere que se aplique a todos los ficheros automatizados, tanto públicos como privados. Al igual que en la legislación costarricense, lo describe en el capítulo I, artículo 2, sobre el ámbito de aplicación: "Esta ley será de aplicación sobre organismos públicos o privados". Por último, es importante analizar el principio de flujo de datos a través de las fronteras, cuando no haya garantías comparables de protección de vida no se podrán imponer limitaciones injustificadas a la circulación de información fuera de las fronteras de un país. Si se compara con la ley costarricense existe este vacío para regular el flujo de datos a través de las fronteras. Como se observa en el comparativo

anterior, de los principios rectores recomendados por la ONU de aplicación para los estados miembros, Costa Rica introdujo la mayoría en la normativa que rige la tutela del tratamiento de datos personales, lo cual es evidencia de que sirvió de inspiración para la redacción del marco jurídico que nos rige.

### 2.4.6 Principio de la Organización de Estados Americanos (OEA)

Con base en el tema de investigación, es importante analizar desde el punto de vista de protección de datos, el papel que tiene la OEA con la aprobación jurídica la cual lo hizo mediante su representante, el Comité Jurídico Interamericano a solicitud de la Organización. Es un proyecto denominado "Proyecto de Convención Americana sobre Autodeterminación Informativa", el objetivo es fortalecer la regulación normativa referente al tratamiento de datos personales de los Estados miembros, de la cual Costa Rica forma parte. Este proyecto empezó en 1997 y se consolidó el 19 de noviembre de 2010, cuando fue expuesto ante la OEA y aprobado por este mismo órgano. En el 2011, se promulgó dicho documento a los países interesados bajo el código CP/CAJP-2921/10 rev.1 (Organización de los Estados Americanos, 2011). El proyecto propone una regulación para la protección y movimiento internacional de datos, el cual también aborda temas importantes como el derecho a la información en la recolección de datos, el consentimiento del afectado, la calidad, categorías, seguridad y cesión de datos, los derechos y las garantías de las personas, el habeas data, las sanciones, los recursos, las agencias de protección de datos y el registro de datos.

Este tipo de proyecto tuvo un proceso de análisis, correpondiente a un estudio exhaustivo, en el cual se realizó un método comparativo de los marcos jurídicos de los países de América Latina, así como la utilización de los antecedentes de Europa y

Estados Unidos. El proyecto hace mención detallada de los conceptos que envuelven esta regulación y figura como una guía para la creación y perfeccionamiento del instituto de habeas data y tratamiento de datos personales para todas las legislaciones.

### 2.4.7 Tratamiento de datos personales en Costa Rica

Con base en el tema del tratamiento de los datos personales, éste surge como un proyecto de ley el 25 de junio de 2007, registrado en el expediente 16.779, promovido por varios diputados, entre ellos miembros de los partidos políticos Liberación Nacional (PLN) y Partido Acción Ciudadana (PAC). Fue en ese momento en el que adquirió mayor relevancia jurídica por cuanto su contenido era más acertado y cercano a lo que Costa Rica requería para la tutela del bien jurídico “datos personales” además del evidente crecimiento tecnológico. Esto permitió realizar la publicación oficialmente en el Diario Oficial La Gaceta el 5 de setiembre de 2011 bajo el nombre de Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales N º 8968. El fin primordial de esta ley es resolver las diferentes controversias generadas por la vulnerabilidad de los derechos de la personalidad y otros derechos fundamentales.

El proceso de creación e institucionalización de una ley no es tan ágil como se esperaría; entre las principales razones que provocaron la tardanza para que la Ley N º 8968 en estudio, sea hoy una realidad, estaba que el texto jurídico no explicaba cabalmente ni los conceptos ni tampoco los efectos que perseguía la normativa. Por otra parte, fue necesario cambiar algunos conceptos implícitos en el proyecto, por ejemplo, como lo mencionó el diputado Mario Quirós Lara en su dictamen afirmativo del 6 de enero del 2009, debía de enfocarse el término de “dato de carácter personal” por

“dato de carácter sensible”, para no crear un desequilibrio entre el derecho a la información y el acceso al dato público. Este tipo de análisis, más las consideraciones de la Defensoría de los Habitantes, aunado también a la agenda legislativa y a la larga lista de proyectos de ley y modificaciones a las vigentes, hicieron que el proyecto tardara varios años, mientras tanto el tratamiento legal que estaba siendo aplicado para dar reparo a quienes experimentaron algún perjuicio en contra de sus datos personales era mediante un recurso de amparo.

### 2.4.8 Habeas data en Costa Rica

#### 2.4.8.1 Regulación normativa antes de la Ley No.8968

Sin embargo, anterior al proyecto que logró consolidarse para crear la ley que se encuentra hoy vigente, Costa Rica hizo varios intentos por regular la manipulación de datos personales. En 1996, el Dr. Constantino Urcuyo, quien en ese momento fungía como diputado del PUSC, presentó un proyecto de ley que pretendía reformar la ley de Jurisdicción Constitucional No 7135 del 19 de octubre de 1989, para tratar de institucionalizar la figura del habeas data, por primea vez. A pesar de que la revisión era nueva, se aprobó en primer debate y una vez que llegó a la Sala Constitucional, esta determinó la existencia de vicios que justificaron que el expediente fuera archivado. Uno de los vicios fue que los derechos que se pretendían tutelar no estaban conceptualizados en el proyecto de ley, otro de ellos fue que la ley no regulaba ningún tipo de infracción a quienes atentaran contra los derechos tutelados. Según algunos criterios de los diputados miembros de la comisión creadora de la Ley 8968, integrada en su mayoría por diputados del PLN, el recurso de habeas data no es más que un instrumento o un mecanismo de garantía procesal a favor de personas que han sufrido

un menoscabo en su ámbito de intimidad producto de usos abusivos de sus datos e informaciones. Se trata, entonces, de un derecho procesal reactivo frente a una lesión ya ocasionada. Esta es una de las justificaciones en la que se sustenta la creación de un instrumento jurídico exclusivo que procure la prevención de delitos contra nuestra intimidad. Cuando se presentó este primer proyecto se consideró que el recurso de amparo era más amplio, por su composición para la tutela de la libertad informática.

En la búsqueda de su consolidación, este instrumento jurídico sufrió algunos atrasos, como lo fue el haber sido archivado en el año 2006 por el vencimiento del plazo cuatrienal. Además, el proyecto de ley que estuvo más cerca y que, además, logró asentarse jurídicamente en nuestra legislación fue el 16.779, redactado por varios diputados miembros representantes de los partidos PLN, ML, PAC y PUSC. Este proyecto pasó a estudio de la Comisión Permanente de Asuntos Jurídicos el 25 de junio de 2007, y en primer debate se discutió acerca de a cuál ministerio debía estar adscrito el órgano descentralizado de Prodhab. Inicialmente, la primera redacción de ese proyecto le asignaba la obligación de ejercer la tutela y velar por el cumplimiento de la ley a la Defensoría de los Habitantes.

Es importante recordar e identificar la función que ejerce la Defensoría de los Habitantes en representación de quienes residen en Costa Rica; este es un órgano auxiliar de la Asamblea Legislativa en la labor que ejerce este poder público con plena independencia funcional, administrativa y de criterio. Está encargada de recibir, investigar y emitir informes sobre la arbitrariedad o legalidad de una acción, cuyo ámbito de aplicación sea el sector público. Desde este criterio es lógico determinar que no puede fungir como juez al resolver los conflictos en nombre de la Agencia y,

además, ser parte defensora de los intereses de los costarricenses.

Antes de la entrada en vigencia de la ley 8968, publicada el 5 de setiembre 2011, Costa Rica regulaba el tema de la protección de datos no enfocada con el grado de importancia que merecía, pero al menos la contemplaba en normas contenidas en el Código Penal Costarricense, Código Civil, Constitución Política y en otras normas, tales como Ley General de Aduanas, la Ley de Administración Financiera de la República y Presupuestos Públicos, el Código de Normas y Procedimientos Tributarios, y la Ley General de Telecomunicaciones, entre otras.

El artículo 196 bis de nuestro Código Penal contiene una pena de cárcel de uno a tres años para quienes vulneren la intimidad de otra persona, es decir, que sin su consentimiento se apodere, acceda, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino mensajes, datos e imágenes contenidas en medios electrónicos, informáticos, magnéticos y telemáticos. No han sido lo suficientemente efectivas como para enfrentar, por ejemplo, a las empresas privadas que utilizan la información personal, si bien es cierto en la mayoría de los casos para fines comerciales o bien el mismo sector público quienes utilizan la información personal en sano principio para fines estrictamente públicos ; esta norma penal es eminentemente con efecto reactivo, cuando lo que necesitan de carácter urgente los ciudadanos son medidas preventivas para el aumento de este mercado.

Otra ley que resguarda la violación a la intimidad a través del ofrecimiento insistente de productos, antes de la iniciativa de crear una ley exclusiva en materia de datos personales, es la Ley General de Telecomunicaciones No 8642 del 4 de junio de

2008, que regula el uso de correos, mensajes de texto y las llamadas para vender productos. Superficialmente, vino a regular el tratamiento de datos personales en un único artículo, literalmente artículo 42 dice:

"Privacidad de las comunicaciones y protección de datos personales Los operadores de redes públicas y proveedores de servicios de telecomunicaciones disponibles al público deberán garantizar el secreto de las comunicaciones, el derecho a la intimidad y la protección de los datos de carácter personal de los abonados y usuarios finales, mediante la implementación de los sistemas y las medidas técnicas y administrativas necesarias. Estas medidas de protección serán fijadas reglamentariamente por el Poder Ejecutivo (Salas, 2012, p.16).

Por otra parte, la Carta Magna garantiza en su artículo 24 la privacidad y el derecho a la intimidad, que debe ser respetada frente a las relaciones comerciales. También, encuentra fundamento legal en la Convención Americana de Derechos Humanos (Pacto de San José de Costa Rica), del 22 de noviembre de 1969, la cual señala en su artículo 11, inciso 2, lo siguiente: "Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación." Sin embargo, en la práctica, la anterior normativa no abarca de pleno la regulación del tratamiento de los datos personales cuyo alcance es muy general, lo cual es prueba fáctica de la insuficiencia que se enfrenta en Costa Rica, en relación con la protección de nuestros datos personales

#### 2.4.8.2 Regulación de los delitos informáticos en Costa Rica

En la misma línea, existe la legislación de los delitos informáticos, la cual se encuentra estrechamente vinculada con la regulación de datos personales, porque la esfera informática envuelve una ilimitada cantidad de información personal, que, según los expertos en la rama, no está siendo protegida de forma segura y la regulación actual no es suficiente para proteger los derechos fundamentales de los habitantes. Para entender el alcance de la legislación del delito informático, debe comprenderse con claridad el concepto; puede entenderse como delitos informáticos, aquella acción típica, antijurídica y culpable realizada a través de medios electrónicos o de la Internet, que tienen por objetivo destruir o dañar dispositivos electrónicos y las redes de esta.

Este tipo de delitos engloba otros delitos ya tipificados en el Código Penal Costarricense como lo son el fraude, robo, chantaje y malversación de caudales públicos, los cuales se convierten en delitos informáticos cuando su consumación se lleva a cabo mediante instrumentos informáticos. Por tal razón, en este momento se encuentra en la Asamblea Legislativa el proyecto de ley N ° 17613, que procura reformar el artículo 229 BIS del Código Penal y adicionar un nuevo capítulo denominado “Delitos Informáticos”, de forma que este apartado incluya más tipos penales, adaptables a la realidad criminal actual.

Este proyecto pasó a estudio e informe de la Comisión Especial de Seguridad Ciudadana el 15 de febrero de 2009; esta Comisión la integran miembros de diferentes partidos como el ML y el PLN, se espera que para este año 2012 ya se apruebe en segundo debate del plenario. Las causas que han atrasado su decreto oficial han sido por atender varias de las recomendaciones elevadas por la Comisión designada para la

revisión y aprobación de este proyecto, entre ellas porque en la consulta legislativa se confirmó que el proyecto era inconstitucional en cuanto al procedimiento por haberse infringido el principio de conexidad, el cual se refiere a que no hubo relación entre el primer proyecto presentado y el que fue aprobado en primer debate. Así mismo, diputados del Frente Amplio y del PAC rechazaron la aprobación por considerar que se violentaba el derecho a la privacidad, porque existían artículos que le permitía a las autoridades intervenir cualquier comunicación por la comisión de cualquier delito (Sala Constitucional, 20119). Entre las principales consideraciones que deben tener presentes los usuarios de redes sociales están la cantidad y la calidad de la información que decidan compartir en las redes, esto por cuanto una gran parte de la responsabilidad depende de los mismos usuarios. Esto no quiere decir que tengan que restringirse a formar parte del mundo informático, pero los usuarios sí deben ser cautelosos y recelosos con la información que publiquen.

Costa Rica protege el bien jurídico de la información de forma escueta en los artículos 196 BIS, 217 BIS y 229 BIS del Código Penal, Ley N °4573, e incluye únicamente la violación de comunicaciones electrónicas, el fraude informático y la alteración de datos y sabotaje informático. Sin embargo, este tipo de delitos debe ser tutelados más ampliamente, ya que los efectos por la consumación del delito no solo recaen sobre el ámbito patrimonial de las personas, como lo serían la acción antijurídica sobre los sistemas bancarios, sino también sobre la integridad e imagen de una persona, capaz de causar estragos irremediables si no se llegara a comprobar que se trata de un sabotaje de su imagen.

El proyecto en estudio incluye más tipos penales, como la suplantación de identidad, el cual es muy susceptible de cometerse por las facilidades de la internet; violación de datos personales, clonación de páginas electrónicas, uso de virus y estafa informática, entre otros (La Gaceta, 2010). La inserción de más tipos penales viene a garantizar mayor protección a los datos personales de los usuarios de redes informáticas. No obstante, se requiere crear conciencia en los habitantes para que seleccionen detenidamente el tipo de información que registran en los diferentes sistemas electrónicos, porque, como es sabido, la persecución y la prueba de un delito de esta categoría es bastante complicada, ya que generalmente quienes delinquen contra los usuarios de redes informáticas son profesionales en la materia, es decir, son delincuentes expertos en el uso de sistemas informáticos, los cuales, usan sus conocimientos para producir daños materiales e inmateriales en las personas. La naturaleza misma del bien jurídico que se pretende proteger, el de la información, es ya vulnerable y susceptible de que cualquier persona se adjudique información de terceros fácilmente, porque así lo facilitan los medios electrónicos e inicialmente, depende de los mismos usuarios de cómo manipulan su información personal en las redes sociales.

El tema de la tutela de la información que se manipula en medios electrónicos es delicado y es por eso por lo que se hace estrictamente necesario que se esté actualizando constantemente su legislación, al mismo paso que se actualizan los sistemas informáticos y con ellos las nuevas formas de delinquir.

En esta misma línea, los derechos fundamentales no solo surgen a la vida jurídica como instrumentos para delimitar los poderes del Estado, sino también, para definir la esfera individual de protección, donde se desarrollan las relaciones

interpersonales entre los individuos.

Existe una teoría generacional analizada y expuesta por Castillo, (2002) referente a los derechos fundamentales, la cual nace en respuesta a los cambios en las costumbres, modos de vida y en la evolución de los diferentes sectores de la sociedad, como los son: el sector económico, político y tecnológico.

Es trascendental conocer la existencia de esta tipología, ya que, según Castillo, (2002), sirve de base para definir e identificar las variaciones y calificaciones de los derechos humanos en cada uno de los momentos de la historia. Los llamados derechos de primera generación son: derechos civiles y políticos. Dentro de esta categoría podemos identificar específicamente: igualdad, dignidad, libertad, vida (integridad física, psíquica y moral, la no esclavitud, la justicia, la personalidad jurídica, el derecho a no ser arrestado arbitrariamente (defendido por el recurso de habeas corpus), entre otros.

Los derechos de segunda generación: derechos sociales, económicos y culturales; estos son considerados derechos modernos cuyo ejercicio es individual pero la titularidad no solo debe ser individual sino también colectiva. Estos derechos procuran la exigencia al Estado, de garantizar la protección de los bienes sociales que amparan al individuo. Algunos de los que encajan en esta conceptualización son: el derecho al trabajo, el derecho a la equidad, la dignidad, la seguridad e higiene, entre otros.

Derechos de tercera generación: derechos colectivos de los pueblos. Protegen derechos o bienes comunes de los pueblos. Entre ellos: derecho al medio ambiente, a

la cultura, al ocio, a la paz, a la regulación de la informática.

Hasta este momento, los derechos de la cuarta generación: derechos de la sociedad del conocimiento, son considerados como los nuevos derechos de futuras generaciones, derivados de la revolución tecnológica de finales del siglo XX y principios del siglo XXI. Tal y como lo refleja el concepto de esta categoría, apunta directamente a los cambios tecnológicos y se refiere a la necesidad latente, de ajustar la normativa a las nuevas sociedades de la información, que surgen con la evolución de la capacidad del hombre.

Se resguardan derechos como: el derecho de acceso a la informática, el derecho a acceder al espacio que supone la nueva sociedad de la información en condiciones de igualdad y de no discriminación, el derecho al habeas data, el derecho a la limitación del uso de la informática para garantizar los derechos fundamentales y la seguridad digital.

Los derechos considerados como fundamentales tutelados por la Constitución Política costarricense son los mismos, sin embargo, algunos de ellos como lo es el derecho a la autodeterminación informativa, se derivan del derecho a la intimidad. Por ende, el anterior desprendimiento demuestra que Costa Rica ha procurado crear nuevos derechos de los ya existentes, para acoplar la normativa a los nuevos hechos delictivos y así proteger los derechos de sus habitantes.

Por lo anterior expuesto, también el derecho penal costarricense, es ejemplo de la evolución jurídica que pretende condenar a quienes lesionen los derechos considerados dentro de esta cuarta generación, tales como la intimidad, la

autodeterminación informativa cuando la información personal es manipulada en algún medio tecnológico.

### 2.4.9 Creación de la Agencia para la Protección de los Datos Personales (Prodhab)

#### 2.4.9.1 Naturaleza jurídica

La Agencia de Protección de Datos (Prodhab) es creada mediante la Ley No 8968, capítulo IV, el cual en su sección I contiene disposiciones generales, atribuciones, acerca de la dirección y el personal de la agencia, las prohibiciones, el presupuesto y en su sección II se expone acerca de su estructura interna. La agencia abrió sus puertas el 7 de marzo de 2012, según lo dispuesto en el transitorio II del cuerpo normativo que la creó, bajo la Dirección General de la M.Sc Arlene González Castillo. Actualmente, la agencia cumple con sus funciones en la oficina-despacho del ministro, ubicada en el Registro Nacional, Zapote, San José.

Debido a la reciente publicación de la ley el 5 de setiembre de y en obediencia de los transitorios I, II y III redactados en la ley N o 8968, el proceso de conformación e integración de la Prodhab debía ajustarse a lo dispuesto en los transitorios; en primer orden, el transitorio II dispuso que las instalaciones de la Prodhab debían estar listas seis meses después de la fecha de entrada en vigor de la ley, lo cual fue cumplido cabalmente. Seguidamente, a la luz de lo dispuesto en el transitorio I, quienes en la actualidad sean propietarios o administradores de bases de datos cuentan con el plazo de un año a partir de 5 de marzo de 2012 para ajustar la información de sus bases de datos a lo que señala la citada ley de protección de datos. Por último, el transitorio III dispone que el Poder Ejecutivo deberá emitir la reglamentación de la ley, seis meses

después de la conformación de la Prodhab.

La reglamentación de la ley debe incluir los aspectos técnicos para que la Prodhab emita sus resoluciones conforme con lo que la ley dispone, entre ellos: trámite de denuncias, formalidades, especificar los plazos de resolución, la composición del órgano encargado de resolver, en caso de que su estructura interna así lo contemple. De forma que el interesado o quien ostente un derecho subjetivo entienda a plenitud el proceso al que se está sometiendo, en procura de la defensa de su derecho a la autodeterminación informativa y al respeto de los principios básicos que rigen la protección de los datos personales.

#### 2.4.9.2 Funciones y alcance

En cuanto a sus funciones, la Prodhab debe velar por el cumplimiento de la normativa en materia de protección de datos; rige esta normativa, tanto para personas físicas como jurídicas. Sus funciones incluyen:

1. Llevar un registro de las bases de datos reguladas por esta ley. Este numeral consiste en que la agencia debe de custodiar bajo un estricto control cada una de las bases de datos que manejan las empresas sean públicas o privadas, categorizadas, según la ley, en datos personales, datos sensibles, etc.

2. Imponer las sanciones a quienes infrinjan las normas sobre la protección de datos personales y trasladar al Ministerio Público las que se puedan configurar como delito.

3. Promover y contribuir en la redacción de la normativa tendiente a implementar

las normas que regulan esta materia. Este numeral obliga a la agencia a participar en la reforma de la normativa, de acuerdo con los cambios y necesidades jurídicas que transcurran en el tiempo, de forma que se ajuste a las nuevas situaciones delictivas que se presenten.

4. Fomentar entre los habitantes el conocimiento de los derechos concernientes al acopio, el almacenamiento, la transferencia y el uso de sus datos personales. Lo anterior constituye una obligación de la agencia, pues debe promulgar la información pertinente de forma clara y precisa, para que los habitantes de Costa Rica comprendan cuáles son los derechos que los invisten y no consientan por falta de información, ninguna práctica considerada por la ley como abusiva en el uso de sus datos personales.

En cuanto a su alcance, la Agencia podrá acceder a las bases de datos reguladas por la ley; a fin de hacer cumplir la norma, se aplicará a los casos presentados ante la agencia y, excepcionalmente, cuando se tenga evidencia de un mal manejo de datos personales en sistemas de información.

La agencia tiene la atribución de ordenar de oficio o a petición de parte la supresión, rectificación, adición o restricción en la circulación de las informaciones contenidas en los archivos o bases de datos cuando estas contravengan las normas de la ley. Así mismo, debe resolver los reclamos por las infracciones a las normas sobre protección de los datos personales, dictar las directrices necesarias, que deberán ser publicadas en el Diario Oficial La Gaceta, a efectos de que las instituciones públicas implementen los procedimientos adecuados con respecto del manejo de los datos

personales. La anterior afirmación se encuentra descrita en el artículo 16 literal i) de la Ley 8968. Evidentemente deja por fuera que este artículo sea de alcance a las empresas privadas, las cuales también tienen acceso al uso de bases de datos y es en estas donde mayor énfasis hay que hacer, pues las usan con fines lucrativos a diferencia de la empresa pública.

**Importancia de una sólida institucionalización de la Prodhab**

Los constantes y lamentables delitos en perjuicio de la intimidad de los costarricenses hacen necesaria la urgente institucionalización de la Prodhab, tal es el caso de los recientes pronunciamientos que ha redactado la Sala Constitucional con respecto al acceso, por ejemplo, que tiene el mercado de telefonía, ya no solamente para ofrecer productos o servicios, sino que también involucran a otros miembros de la familia en el cobro de deudas que no le conciernen a la persona.

Este caso se observa fundamentado en la sentencia 04721 del 8 de abril de 2011 donde la recurrente alegaba una lesión en contra del derecho a la intimidad y autodeterminación informativa provocada por una empresa privada, toda vez que la empresa recurrida la llamaba insistentemente a la casa, celular y cualquier número que estuviera a nombre del recurrente y que no era utilizado por este, con el fin de contactar a un familiar para el cobro de una deuda. Lo anterior refleja una práctica de acoso, interrumpir la vida privada de una persona por las deudas de un tercero, donde además se denota la intención de la empresa no solo de insistir en las llamadas, sino también de que se le otorgue información personal de otra persona sin derecho a hacerlo.

Con base en los hechos probados y bajo el criterio de la Sala Constitucional, se declaró con lugar el recurso, con fundamento en el artículo 24 de la Constitución Política que expresamente tutela estas situaciones, al prohibir cualquier práctica abusiva de acoso u hostigamiento para cobro de deudas. Sin embargo, existe una latente necesidad por asegurar información más importante que los números telefónicos y es la información referente a las enfermedades congénitas o transmitidas producto de la interacción humana, que están presentes en las personas y de la cual son generalmente las empresas públicas las encargadas de la custodia de información de la salud de las personas. El avance tecnológico, que, si bien es cierto procura facilitar la vida del hombre, tiende a dejar en descubierto los pormenores o posibles afectaciones negativas en su afán por mejorar el espacio cibernético, sin embargo, en el tema como el uso y custodia de la información de la salud de las personas la tutela debe ser reforzada.

Una fuga de este tipo de información puede significar el aislamiento total de una persona en la sociedad, por verse agotadas las posibilidades de integrarse a un trabajo y de continuar con una vida normal. Ante situaciones de este tipo, se violentan, a su vez, una serie de derechos fundamentales como igualdad y no discriminación, aunque es cierto que el Estado tiene la obligación de proteger la salud y seguridad pública en caso de encontrarse frente a una pandemia, en el tanto la individualización de esos casos no signifique un menoscabo en la vida en sociedad de los habitantes. El secreto profesional está íntimamente ligado a este criterio, para que a través de su aplicación pueda llegar a salvaguardar la información médica de las personas.

Los casos donde deba defenderse la tutela del derecho a la autodeterminación informativa en el ámbito de la salud es una de las áreas en las que en definitiva el Estado debe involucrarse más exhaustivamente, especialmente la gestión que realizan las entidades públicas relacionadas con la salud por los graves perjuicios que se pueden generar si llega a darse un mal uso de esta información.

En el mundo, la información sobre las personas portadoras de la epidemia del VIH-sida continúa siendo la información más vulnerable para quienes padecen la enfermedad por cuanto estas personas han sido objeto de discriminación y estigmatización, y la principal implicación recae sobre su vida laboral y en sociedad, ya que la misma sociedad generalmente les niega las condiciones de igualdad en la prestación de bienes y servicios. Así mismo, estas personas tienen el derecho a vivir una vida plena hasta el último día y si esta información no es manipulada con estrictos protocolos de seguridad provocará agravios irreparables en la vida de quienes la padecen.

### 2.4.10 ¿Hacia dónde se dirige?

#### 2.4.10.1 Impacto de IoT

Es importante plantear ¿cuál es el futuro de IoT?, ya que debido a la parte de innovación que involucra es seguro que va a provocar un gran impacto en todos los sectores de actividad. IoT es una red de gran magnitud en donde incorpora y hace uso de muchos objetos “inteligentes” que se encuentran conectados entre sí. Al incorporar el internet de las cosas, los sectores profesionales podrían desaparecer, otros en cambio, comenzarán gracias a la nueva era de la tecnología. En este escenario, quedarán los que sepan adaptarse más rápido a estos cambios, así como ocurrió con

las tecnologías de la información. Según la firma de analistas Gartner, en todos los sectores tendrá un gran impacto toda la red de dispositivos conectados, desde empresas, autoridades locales, hospitales y consumidores, llegando a unos gastos totales de 260.000 millones en 2020. Estos datos suenan prometedores en cuanto a la economía, pero ¿en qué sector se estima que será el que tenga más objetos conectados? El estudio realizado por Gartner que se presentó en la "Gartner Symposium/ITxpo" del 9 de noviembre de 2014 en Barcelona, estima que las aplicaciones para los consumidores, principalmente en el sector de la automoción, serán las que más difusión en los próximos años. Calculan que aproximadamente 13.000 millones de dispositivos conectados pertenecerán al sector de consumo. Como indican en el estudio: "El número de dispositivos inteligentes conectados seguirá creciendo de manera exponencial, ofreciendo a los objetos inteligentes la capacidad de sentir, interpretar, comunicar y negociar, y efectivamente tener una 'voz' digital", según Steve Prentice, vicepresidente de la consultora. "Los CEO deben buscar oportunidades para crear nuevos servicios, escenarios de uso y modelos de negocio basados en este crecimiento". Seguido del sector consumo, afectará también en gran medida al sector industrial: los servicios públicos, la fabricación y el transporte serán los mercados clave de esta tecnología. Las empresas estarán obligadas a buscar un equilibrio entre los datos recogidos y almacenados en la red por los dispositivos y sensores conectados, y el análisis de toda esa cantidad de información con el riesgo de su pérdida o mal uso.

Todos los retos que plantea el IoT y que incluso actualmente forman parte de muchos objetos involucra un reto mayor para la seguridad de toda la información que almacena, es por ello por lo que pondrá a las empresas en la obligación de invertir en

seguridad tecnológica a unos niveles que nunca se habían pensado. Terminando con el análisis de beneficios, International Data Corporation (2015) los especialistas en información tecnológica calculan que el mercado mundial de IoT crecerá hasta llegar a 3.040 millones de dólares hasta el año 2020, el cual es representado en el siguiente cuadro:

| Category | 2013 | 2014 | 2015 | 2020 |
|---|---|---|---|---|
| Automotive | 96 | 189 | 372 | 3.511 |
| Consumer | 1.842 | 2.440 | 2.874 | 13.172 |
| Generic Business | 395 | 479 | 623 | 5.158 |
| Vertical Business | 698 | 836 | 1.009 | 3.164 |
| **Grand Total** | **3.032** | **3.750** | **4.880** | **25.006** |

**Ilustración 5. Unidades de internet de las cosas por categoría (Millones). Gartner (noviembre 2014)**

Como se comentó al inicio de la investigación, desde que apareció Internet en la vida de todas las personas se ha convertido en un factor imprescindible en la economía mundial. En todos los sectores de la sociedad es algo fundamental y se utiliza día a día por todo el mundo. Cuando apareció la tecnología inalámbrica, hizo que aumentaran las posibilidades de la red, pudiendo ser alcanzable desde cualquier parte del mundo y esto facilitó las velocidades de conexión, además de la disponibilidad del servicio de Internet. De esta forma las nuevas tecnologías que aparecen y derivan de esta tecnología tienen un enfoque innovador y están basados en la ubicuidad como se hizo mención en anteriores capítulos. Internet de las cosas, sin duda tiene un potencial enorme y desde ya está marcando un impacto muy significativo en la sociedad, como

hizo Internet desde el momento que fue lanzado al mercado.

Para esta investigación es importante analizar el impacto a través de tres puntos de vista: en las personas, modelos de negocio y el impacto a la hora de consumir recursos.

#### 2.4.10.2 Impacto de IoT en las personas

En la comunicación de IoT en donde involucra a las personas se puede denotar la interconexión de personas con personas, de personas con cosas y de cosas con otras cosas. En la misma definición de la tecnología ya se puede observar el impacto que tiene y tendrá en la sociedad IoT. Todo estará interconectado con las personas, tomando como principal objeto el celular, el cual es identificado como el punto central con la que las personas se conectan con el resto del mundo. Y es que todas las aplicaciones que se están desarrollando actualmente ya dan por hecho que el usuario tiene una conexión a Internet y se podrá conectar a una red sin problema. Los desarrolladores de aplicaciones y *hardware* solo tienen que reinventar lo que ya existe, dotándolo de conexión. Más adelante se analizarán todos los peligros que esto conlleva, porque todo proceso de innovación conlleva a muchos agujeros que generan riesgos en todo el proceso de desarrollo-comercialización-usuario. La conexión en todo momento en una red, sin importar dónde ni cuándo, permaneciendo intercambiando datos con todos los destinos muestra de por sí el peligro que puede ocasionar. De la resolución de esos problemas dependerá que el impacto hacia las personas sea bueno y útil, o sea,  un verdadero problema y una violación de todos los derechos de la sociedad.

#### 2.4.10.3 Modelos de negocio

Seguidamente, se toma el tema del impacto de IoT en los negocios. El hecho de que todo esté interconectado y las personas con ello, hace que las empresas sean capaces de adaptarse rápidamente a la nueva tecnología, sin que ello conlleve un cambio en su función principal a la que se dedique, ya que IoT cambiará seguro la forma de trabajar y de prestar servicios a la sociedad. La arquitectura orientada a servicios, o SOA, en el argot de una empresa es la arquitectura que se encarga de aislar las funciones principales del negocio independientes que no cambian de los que sí. Con la era del 2.0 y las redes sociales, todas las empresas tuvieron que adaptarse a esta nueva forma de prestar servicios y descubrir nuevas líneas de negocio, creando nuevos puestos de trabajo orientados a nuevos expertos en la nueva tecnología. De igual forma va a ocurrir con IoT, se abrirán nuevas vías de negocio orientadas a la interconexión y aparecerán nuevas áreas de conocimiento y de trabajo.

Incluso, muchas de las empresas han optado por eliminar los sistemas de publicidad antiguos que se hacían con panfletos y los adaptaron a las redes sociales, desde la empresa más grande con potencial de atraer cliente con solo el nombre por ejemplo, con de la misma forma lo hizo la empresa pequeña, aquella que se dedica a dar servicios de belleza, vender productos de limpieza e incluso hasta las panaderías.

De la misma forma en que se adaptaron a la incorporación de las redes sociales se hará con IoT, haciendo uso de la tecnología para garantizar el servicio de forma continua.

**Escenario 1:**

En Coronado, San Antonio existe un restaurante llamado Sentosa, el inicio de este fue duro al igual que cualquier pequeña empresa.

En su inicio, las instalaciones involucraban la modificación y adaptación de una casa esquinera, ubicada en una urbanización que incluso no tenía visibilidad ya que era poco transitada.

En poco tiempo el restaurante empezó a realizar publicidad en Facebook y de esta forma muchas personas empezaron a visitar el lugar por primera vez, con un solo clic agregaban cinco estrellas en los comentarios y de esta forma la fama de este fue aumentando.

Actualmente, se tuvo que extender en infraestructura porque las visitas eran tantas que ya las personas no cabían así que decidieron incluso comprar las casas de los lados y hacer parqueo, salón de fiestas entre otras cosas.

Sin embargo, el éxito del restaurante no solo está en los buenos sabores de la comida, sino que también están involucrados con la tecnología, además de usar las redes sociales también han incorporado en las mesas un dispositivo en el cual se puede llamar al mesero, solicitar la cuenta, cancelar un pedido o realizar la orden, de esta forma los meseros reciben una alerta en un reloj y rápidamente están dando el servicio solicitado.

Esto ya es posible en muchos restaurantes de Costa Rica, que simplemente le han dicho “Sí” al cambio y sin lugar a duda han tenido un gran éxito.

#### 2.4.10.4 Impacto en la consumición de recursos

La preocupación que existe hoy en día por el estado de salud de la tierra, las energías renovables, y el consumo de recursos con la frecuencia y magnitud que se está haciendo, además del cambio climático y el aumento masivo de la población, ha hecho que los avances tecnológicos se centren en ayudar a frenar el proceso lo máximo posible. La tecnología de Internet de las Cosas parece estar diseñada especialmente para esta tarea y es uno de los campos más prometedores. Al incorporar esta tecnología junto con herramientas como los sensores puede controlar las diferentes variables necesarias para el mantenimiento de estos recursos. En uno de los siguientes apartados se tratará en más profundidad las diferentes aplicaciones derivadas del IoT en el ámbito de las energías renovables.

**Escenario 2:**

Una fuente en una plaza de una ciudad importante se atasca. La fuente tendrá un sensor que informará a los técnicos del ayuntamiento qué circuitos se han estropeado y cuál es la manera más rápida de solucionarlo, así como las herramientas que deberán llevar para su reparación. Si no se hiciera de esta forma, los técnicos tendrían que haber parado el funcionamiento total de la fuente hasta que pudieran revisar todos los circuitos y ver cuál es el que se ha estropeado y una vez hecho esto, pedir los repuestos y esperar a que llegasen. La diferencia de eficacia y eficiencia que se aprecia en este escenario es considerable. En este escenario se pasa de una situación cotidiana a una situación en el ámbito empresarial en la que se pone de manifiesto la gran importancia y peso que cobrará en la industria la introducción de los dispositivos IoT. Según el informe Connected Life: The next five years in Asia (2013) de

GSMA, organización de operadores móviles que se dedica al apoyo de la normalización, implementación y promoción de telefonía móvil GSM, que ha estudiado el impacto de IoT, prevé que Asia será la región más interconectada y la que más beneficios obtendrá de una economía más productiva; China conseguirá llegar a 22.000 millones de dólares de ganancias al reducir la congestión del tráfico; India podrá llevar la electricidad a 10 millones de hogares en 2017 y evitar que el 24% de la electricidad que cada año genera se pierda; Japón ahorrará más de 10.000 millones de dólares en coses sanitarios y Corea del Sur reducirá el coste educativo por estudiante hasta 12.000 dólares.

#### 2.4.10.5 Factores que decidirán el futuro de IoT

La población actual del mundo se encuentra en casi siete millones y medio de personas. Todas ellas con necesidades de comunicación de cualquier índole. Teniendo en cuenta esta estadística resulta muy atractivo el hecho de que las máquinas sean capaces de conectarse entre sí y con la población mundial. Estas cifras crecen día a día de manera exponencial. Imagine por un segundo un mundo perfecto donde IoT se ha integrado perfectamente. Un mundo donde cualquier incidencia es resuelta en cuestión de segundos. Suponga que ocurre un accidente de tráfico entre dos coches. Los sensores que tienen estos coches detectarán el accidente que hará que automáticamente se active el servicio médico. Por otra parte, el sistema de los semáforos y señalización recibirá un aviso y regulará el tráfico conforme al accidente para evitar posibles atascos. Finalmente, el accidente es avisado a la compañía de seguros para gestionar el accidente. Es fácil ver que en ese mundo perfecto interconectado todo será muy eficiente, rápido y sobre todo seguro. En este capítulo va

a hablar sobre los factores que van a hacer que IoT pueda adaptarse al mundo, analizando los que pueden impulsarlo como los que pueden ralentizarlo.

#### 2.4.10.6 Obstáculos de IoT

Los problemas a los que se va a enfrentar IoT, como se mencionó en los primeros capítulos no van a ser sino similares a los que se enfrentan otros desarrollos tecnológicos que pueden afectar a la vida de las personas. Y profundizando en los que tienen mayor relación con esta investigación, son: asegurar la privacidad y seguridad de los usuarios y las personas, y conseguir que se creen estándares aceptados globalmente. Otros de los obstáculos pueden ser las limitaciones actuales de infraestructuras, la gran necesidad de inversión en los actuales equipos, y las barreras de entrada psicológicas en las personas. Hay que ser conscientes de que todavía nos cuesta dejar el mando a aparatos y procesos automáticos, ya sea por inseguridad o porque se es consciente de que una máquina no va a poder realizar mejor el trabajo. Para que una máquina pueda considerarse inteligente, debe de pasar el llamado “test de Turing”. Consiste en una prueba en la que la inteligencia artificial debe de convencer a un jurado de que están hablando con una persona real que está en otra habitación. Hasta el año 2014 ninguna máquina había superado esta prueba. Se trata de chatbot, un robot programado para mantener una conversación online, él pudo convencer al 33% de los jueces de que estaban hablando con un niño de 13 años.

Es por eso por lo que nos es tan difícil confiar la vida y la seguridad a una máquina actualmente. Ya se han tratado en este proyecto todas las posibilidades que tiene IoT, y es por esto por lo que la preocupación por la seguridad de los usuarios por sus datos es muy alta. Hay gente que está totalmente en contra de esta tecnología ya

que piensa que va a suponer una total violación de su persona y su información. Otro de los problemas va a ser la capacidad de creación de estándares. Cada sensor que está en las ciudades, automóviles, campos agrícolas, funcionan de manera independiente e incompatible. Esto dificulta que entre dos sensores diferentes puedan comunicarse entre sí y operar en conjunto. Por ejemplo sobre los sensores adaptados en un campo agrícola, midiendo las variables del cultivo y obteniendo información de este. Al lado hay un sistema de control del clima que obtiene datos en tiempo real del clima. En el momento que empiece a llover el sistema medioambiental debe de poder cooperar con el sistema de control del cultivo. Al estar tan dividido el mercado de fabricantes, actualmente no existe ningún estándar que pueda que todos los dispositivos funcionen correctamente en conjunto. Todo apunta a que existirá un sistema operativo que podrá gestionar todos los mecanismos y sensores. Como hemos estado hablando en anteriores puntos, recordamos que los sensores son dispositivos que se conectan con objetos cotidianos para medir variables como la temperatura, movimiento, etc., y enviar esa información a través de internet. Es cierto que actualmente los sensores son cada vez más baratos, pero muchos de los dispositivos y herramientas necesarias que son complementarios a los sensores como las estructuras de red o plataformas de análisis de datos son muy costosas, y que realmente no son rentables a nivel personal o particular. El motivo del elevado precio de estos dispositivos es el no haber una normativa clara y el actual estado de esta tecnología. Este hecho provoca que los fabricantes tengan miedo a un cambio de normativa.

En este punto, se trata otro de los factores importantes que debe de superar IoT. Y no es más que el cuello de botella al que está destinado debido a las direcciones IP.

Recordemos que actualmente se está trabajando con el protocolo IPv4 e incluso no se ha hecho la migración completa a IPv6, sin embargo, en IPv4 solo hay cabida para unos 4300 millones de direcciones. Actualmente el tercio de la población mundial ya está conectada, unos 2000 aproximadamente de personas, por tanto, no queda mucho margen para seguir conectando todas las “things” de esta tecnología. Con el cambio de protocolo a la versión IPv6 se permitiría conectar unos 340 billones de billones de billones de direcciones IP. Prácticamente cualquier dispositivo podrá conectarse a internet con una IP única.

De igual modo, aunque se consiga solventar los problemas de conectividad, se irá creando una red cada vez más compleja de objetos interconectados que puede suponer un gran problema. El llamado efecto dominó puede producir que la caída del sistema pueda crear grandes problemas en los dispositivos conectados. ¿Qué pasaría si un dispositivo médico interrumpiera y comience a ir de un modo erróneo produciendo daños a alguna persona? O que ocurra algún desastre natural que estropeara los servicios, o un ataque cibernético que pusiera en jaque a los aparatos conectados. Los daños que pueden ocasionar son incalculables. Otro de los problemas será el de la gran cantidad de datos que van a generar estos sensores. ¿Es realmente necesaria toda esa información?, ¿cómo podremos saber la información que necesitamos y la que no? Realmente será complicado manejar la cantidad ingente de datos que habrá en las plataformas de datos la cual estará a disposición de todo el mundo. Es por ello por lo que se está creando un nuevo modelo de negocio que consiste en la estructuración de datos y contenidos en Internet. Finalmente, IoT con el tiempo deberá responder la siguiente pregunta: ¿Realmente es necesaria la solución que puede

aportar a los problemas cotidianos?

Piense un momento en los siguientes dispositivos que pueden aparecer: Un dispositivo que avise cuándo echar de comer a los peces, un paraguas que cambie de color según la previsión del tiempo, o un dispositivo que avise cuándo cambiar la cerradura de la puerta. Sin duda son avances importantes, pero todos estos problemas tienen soluciones más sencillas y seguramente más económicas sin poner en riesgo nuestros datos y nuestra privacidad. Sin duda otros campos se beneficiarán de esta tecnología en mayor medida como veremos en el siguiente apartado donde analizaremos los 10 sectores en los que IoT tendrá mayor impacto. Pero aún es una incógnita saber si la población mundial aceptará que todos estos dispositivos ingresen en la vida de las personas haciéndole la vida más fácil, o, todo lo contrario.

#### 2.4.10.7 ¿Quién y dónde se dará el primer paso?

Es importante trabajar en esta sección: tres preguntas que faltan por responder acerca del futuro de IoT. Primero, aún queda por saber quién será el que guiará en el camino del cambio hacia esta nueva tecnología: ¿los gobiernos?, ¿las grandes empresas?, ¿los consumidores o los fabricantes? En segundo lugar, se analizará en qué zonas es posible que se desarrolle con más fuerza esta tecnología. ¿Serán Estados Unidos y Europa, o los países asiáticos? En último lugar, se abordará el debate sobre si Internet de las cosas debe tener una mentalidad colaborativa u “Open Source”, o será una mentalidad privativa.

Para poder abarcar la respuesta a la primera pregunta se tiene que hablar primero del poder de los usuarios de Internet actualmente. Los usuarios de las redes

sociales tienen un gran peso y pueden definir el rumbo que puede seguir cualquier tecnología.

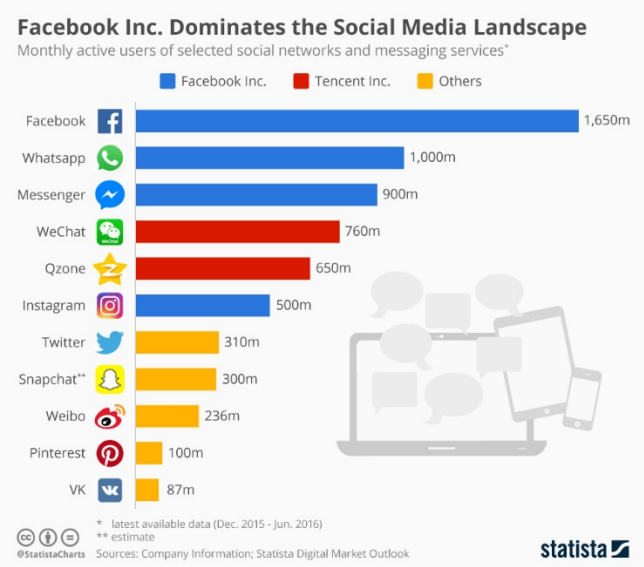



**Ilustración 6. Usuarios activos mensuales en las redes sociales. Statista**

Pero, aunque el escenario donde los usuarios puedan decidir todo lo relacionado con IoT, no es muy lógico pensar que el grupo que sea el que dé comienzo y lleve la voz cantante sean los usuarios de internet. Si pensamos en los gobiernos, no tardamos mucho en darnos cuenta de que la rapidez en la que los gobiernos cambian y los largos plazos que existen en la burocracia, parece complicado la creación de estándares que rijan IoT.

Por supuesto, los gobiernos serán piezas clave en la innovación, pero se podría tratar más de un papel de liderazgo. Creación de estándares y leyes y derechos individuales de los usuarios son sus principales funciones en el comienzo y desarrollo de IoT. Es importante que las empresas y los emprendedores emergentes que se dediquen a fabricar dispositivos de IoT sean los que, entre ellos, consigan marcar el

rumbo que va a seguir esta tecnología, y gracias a la ayuda de los usuarios y los gobiernos puedan formar y comenzar a dar un sentido y una forma más homogénea para que en todos los lugares del mundo se usen los mismos protocolos, y pueda ser más fácil y seguro el poder hacer uso de todos los dispositivos.

La segunda respuesta parece a apuntar a los países como Estados Unidos, China y Europa. Aunque es China el país que está posicionado en cabeza al ser el mayor fabricante de dispositivos IoT actualmente, y uno de los países más consumistas del mundo. También es el país más avanzado tecnológicamente y con una cultura respecto a las nuevas tecnologías que viene promovida por su gobierno.

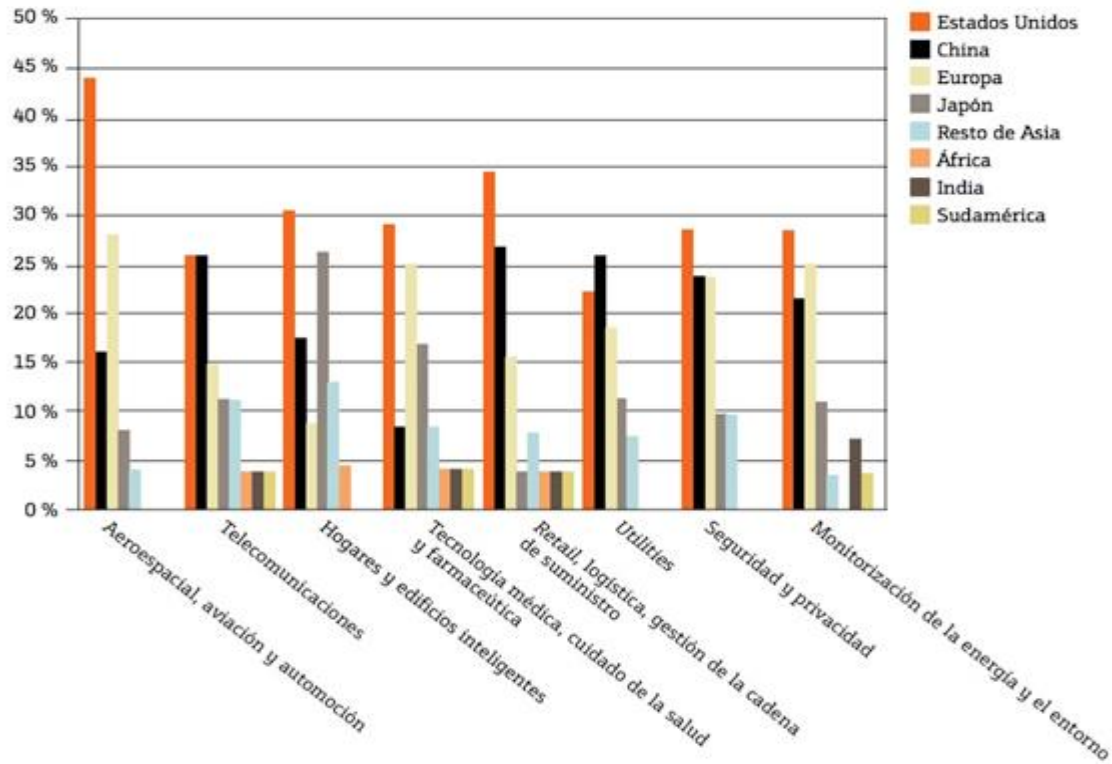



**Ilustración 7. Distribución por países del impacto en los sectores de IoT. Fundación de innovación Bankinter**

Por último, todo indica que la mentalidad de desarrollo “Open Source” va a predominar estos desarrollos, pero con matices. En los sectores donde es necesaria

una gran inversión de dinero y con procesos costosos y complejos, como en los sectores de medicina, aeronáutica y automoción, serán las grandes industrias y empresas las que dirijan estos desarrollos.

El reto para fabricantes y gobiernos de todo el mundo será el de crear dispositivos y sensores que sean eficientes energéticamente, robustos y que aguanten el paso del tiempo en ambientes de todo tipo. Pero, sobre todo, deberán crear dispositivos seguros. Y sobre este aspecto se centra la investigación. ¿Con qué amenazas se van a encontrar y cómo se pueden proteger los usuarios?

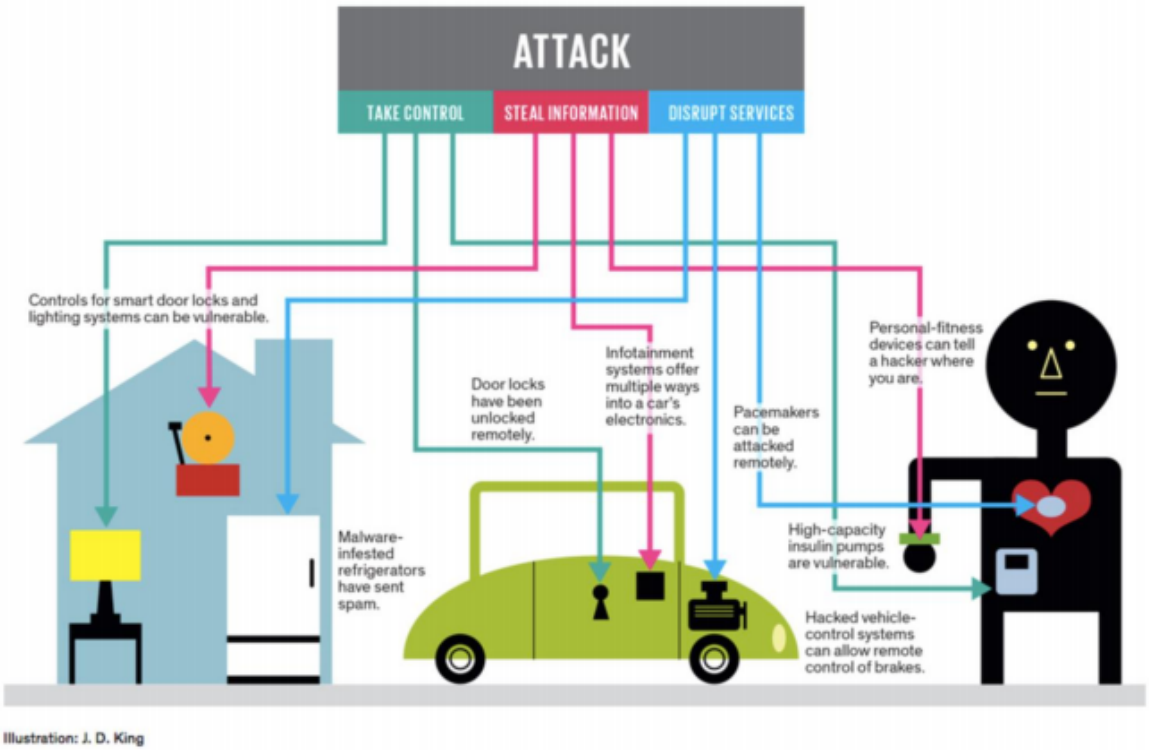



**Ilustración 8. Ataques a la tecnología de IoT. J.D. King**

**Escenario 3:**

Un sistema inteligente con multitud de sensores conectados en la totalidad de

una ciudad como puede ser Jaén, podría ser capaz de analizar los datos atmosféricos, climáticos, y otros datos relacionados con el estado actual del clima para predecir con antelación, cómo varía la contaminación en la ciudad debido a las fábricas, transporte, etc.… y ayudar a tomar medidas preventivas contra las subidas del nivel de polución, como parar temporalmente las fábricas, o reducir la velocidad máxima en las vías.

Esto ya es una realidad, y el proyecto Green Horizont de IBM, se está centrando en el desarrollo de una tecnología para controlar la contaminación y proteger el medio ambiente. Aplicada a Pekín, esta tecnología ya es capaz de prever la evolución en el aire en la ciudad con 72 horas de antelación.

#### 2.4.10.8 Aplicaciones de IoT con análisis en la seguridad

En este apartado se van a desglosar de una manera más amplia y diferenciada cada uno de los campos en los que IoT aportará aplicaciones y ayudará en el desarrollo de las actividades de estos. Este recorrido por los diferentes ámbitos se va a realizar desde el punto de vista de la seguridad sobre los usuarios.

##### A. Aviación

En este sector, como es el de la aviación los efectos que podría tener la inclusión de IoT son variadas, como reducir los tiempos de viaje, aumentar la seguridad y comodidad de los pasajeros, reducir costes a las compañías y aeropuertos, hacer más eficiente el viaje y abaratar costes.

Rutas optimizadas: aviones interconectados entre sí y con el centro de control. De esta manera las rutas podrían calcularse exactamente al momento, pudiendo salir

de las rutas establecidas y poder evitar accidentes, aterrizajes de emergencia, etc. De esta forma se ahorraría combustible al tener cada avión su ruta exacta.

Aeropuertos inteligentes: los aeropuertos serán capaces de gestionar todo el proceso de embarque, salida, entrada, controles de todo tipo de forma automática y segura, haciendo todo más fácil para el usuario y más eficaz y eficiente. Actualmente el aeropuerto de Dubai se encuentra en proceso de cambio para integrar tecnología IoT incluyendo servicio de limpieza inteligente, portamaletas automáticos, escáner facial para controles, etc. Dr. Ian Bache, director de preventa técnica, ARINC aeropuertos de información de gestión de servicios, Rockwell Collins, dijo: “los aeropuertos están siempre en busca de automatizar el procesamiento de pasajeros, manteniendo los más altos niveles de seguridad ofrecemos soluciones a medida que se pueden configurar con el aeropuerto. Las soluciones de gestión de identidad. Muchos aeropuertos en esta región están mostrando interés en estas tecnologías “. Pero aún queda mucho por hacer en este sector ya que siendo un transporte tan importante y usado en el mundo debe de asegurarse al máximo nivel que la seguridad de usar esta tecnología, como vuelos automáticos y customizables, aeropuertos sin personal de control, etc.…

### B. Automoción

Al igual que en el sector de la aviación, este sector también va a ser uno de los que más se beneficiarán de las nuevas tecnologías, y con él, los millones de usuarios que utilizan el coche, transporte público, etc. Las empresas más importantes del mundo de la automoción como General Motors van a invertir una gran suma de dinero para desarrollar taxis inteligentes. Ford y Google siguen trabajando en coches automáticos

sin conductor. En este sector vuelve a ser el protagonista la seguridad del usuario al viajar, por ejemplo, en un coche sin conductor, y con ello, las leyes que se deben de aplicar en caso de que se produzca alguna incidencia. Todo para que el usuario esté protegido y sienta la necesidad y seguridad de utilizar esta tecnología en su día a día.

### C. Telecomunicaciones

La capacidad más importante de IoT está precisamente en su definición: Interconexión y comunicación. En el sector de la comunicación, vemos que las empresas operadores de telecomunicaciones van a tener un gran protagonismo respecto al uso de IoT, ya que en su poder están todas las infraestructuras actuales que recogen los datos y tienen las capacidades comunicativas que comentábamos anteriormente El servicio más básico que deberán cumplir todas las operadoras será el de proporcionar la conectividad necesaria para que los dispositivos puedan conectarse a Internet. Pero conforme avanza la tecnología, se espera que estas compañías generen nuevas líneas de negocio y servicios añadan los posibles como nuevos sistemas de facturación y tramitación inteligente o diseño de nuevos tipos de redes que se adapten a los nuevos sistemas inteligentes interconectados, etc.

### D. Edificios inteligentes

El sector de edificios inteligentes es el que más rápido ha crecido con respecto a esta tecnología y es sin duda una realidad presente. Las casas se convertirán en un sistema inteligente capaz de adaptarse al usuario y a su forma de vida, de modo que el usuario pueda dejar de prestar atención a las tareas domésticas, hacer la comida o apagar las luces cuando vaya a dormir. Sin duda la seguridad también tendrá un factor

importante ya que la casa puede funcionar como no debiera y producir algún accidente doméstico.

### E. Salud

IoT tendrá muchas aplicaciones en el sector de la salud. La posibilidad de poder usar el teléfono móvil con sensores para medir las variables corporales y estar conectado con nuestro médico en todo momento. Poder realizar un diagnóstico rápido de un paciente, prevención de enfermedades o monitorear accidentes son las funciones principales que se esperan en este sector.

### F. Agricultura y alimentación

Anteriormente se ha explicado acerca de la explotación de recursos y cómo IoT puede ayudar a esta tarea que se antoja muy complicada. Según la FAO (Organización de las Naciones Unidas para la alimentación y la agricultura) predice que el sector agrícola deberá enfrentarse al reto de tener que alimentar a 9,6 millones de personas que predicen para el año 2050. La producción del alimento deberá aumentar en 70% a pesar de los muchos de inconvenientes que debe superar como la escasez de tierras de cultivo, el impacto del cambio climático en la agricultura, etc. Aquí entra en juego la investigación de diferentes aplicaciones de IoT para este sector.

Es necesario aumentar la calidad y cantidad de producción agrícola, y los sensores y la interconexión de estos producirán una agricultura inteligente. Está ocurriendo ya, aunque en menor medida. Instituciones y corporaciones ya están reconectando grandes cantidades de información sobre cultivos, suelos, fertilizantes,

información climática, maquinaria, etc. Por ejemplo, en el sector de la ganadería, ya se están utilizando sensores para monitorear y detectar las posibles enfermedades y trastornos en la salud de los animales, la temperatura corporal y hasta el pulso, incluso la posición mediante GPS. Varias empresas privadas también están comenzando a moverse y ser activas en este sector, algunas como Anemon (Suiza), eCow (Reino Unido), Connected Cow (Alemania). Incluso la pesca inteligente está también en sus etapas iniciales con algunos proyectos en Europa, Corea del sur, Norteamérica, y Japón. “La agricultura de precisión no es nueva. Los fabricantes de vehículos agrícolas (John Deere, CNH Global, Class y otros) han estado involucrados en este segmento durante un tiempo. Inicialmente, comenzaron principalmente con tecnologías de posición (GNSS)”, señala Saverio Romeo (2015, citado por Federico Guerrini), analista principal de Beecham Research.

Romeo es el coautor de un informe llamado “Hacia la agricultura inteligente – La adopción de la agricultura de la visión IoT” (2015) publicada en enero por Beecham, centrado en explorar cómo las operaciones agrícolas están cambiando a través del IoT. “Me gustaría destacar el hecho”, dice Romeo, “de que el objetivo no debería ser el ‘industrializar’ la agricultura, sino hacer la agricultura más eficiente, sostenible y de alta calidad. No debemos buscar revoluciones. Debemos buscar una reinterpretación de las prácticas agrícolas por medio del uso de tecnologías de manejo de información. Y esta reinterpretación debería tomar lugar junto con una nueva visión de las áreas rurales”. Esto significa que el sector de la agricultura deberá estar interconectado a su vez con la industria inteligente, turismo inteligente, y demás actividades que giran en torno a la agricultura, El problema en este sector, es el mismo que en los demás, el alto costo de

implementación y puesta en marcha de esta tecnología. Pero es no significa que no pueda empezar a implementarse en menor escala. En viñas, por ejemplo, “hay sensores instalados en varias ubicaciones en el campo, para recolectar datos sobre el suelo y las plantas, para luego ser usados en la prevención de enfermedades como la peronospera”, señala Romeo. Sin duda uno de los sectores más importantes y que hay que tener en cuenta cómo se irá desarrollando, ya que su impacto en el resto de los sectores y en el mundo es muy elevado.

### G. Farmacéutica

Este sector va de la mano con el sector de la salud y por lo tanto también se va a ver afectado por esta tecnología. Aunque en la industria farmacéutica la tecnología de IoT está todavía llegando, el potencial que se puede prever es enorme, sobre todo en la transmisión de datos de pacientes y seguimiento de medicamentos. Esta tecnología va a cambiar la manera de recoger los datos clínicos durante todo el proceso. Algunos ejemplos de lo que se está empezando a desarrollar son el proyecto llevado a cabo por Novartis, que con la ayuda de la compañía Qualcomm están desarrollando un inhalador conectado a internet para enviar información de su uso y datos que los sensores puedan proporcionar. Así podrán monitorear cada inhalación y pueden hacer un seguimiento a sus pacientes. En el futuro veremos muchos más acuerdos de este tipo entre farmacéuticas y tecnológicas. La llegada del IoT a la industria farmacéutica junto con otra tecnología importante como es Big Data, supondrá una revolución, tanto a la hora de realizar los ensayos clínicos como la comercialización de medicamentos, hacer seguimiento a los pacientes, etc.

### H. Vida independiente

En la vida de las personas mayores y su independencia también se prevé un impacto gracias a las nuevas tecnologías. De nuevo entran en juego multitud de sensores que podrían hacer un seguimiento completo de la persona, para monitorear a la persona. Las aplicaciones y las “things” pueden aprender rutinas de la persona a la que están conectadas, generar alertas, mandar notificaciones, etc.

### I. Transporte de personas y mercancías

IoT puede ofrecer soluciones para sistemas de peaje y tarificación, control de pasajeros, control de cargas y mercancías, y así poder satisfacer la demanda de seguridad necesaria para este tipo de actividad. También se podrá monitorear el tráfico al instante, que junto a sistemas de transporte inteligentes harán los transportes de personas y mercancías más eficientes. Las empresas de transporte se convertirán en más eficientes con contenedores de embalaje que puedan pesarse y escanearse por sí solos y optimizando los flujos de transporte.

### J. Medio ambiente

Como hemos hablado anteriormente, uno de los mayores impactos y más importantes que se prevé es en el sector medioambiental, donde se estima que será el sector que más crezca en la utilización de dispositivos inalámbricos. La integración de estos sensores y dispositivos abrirá las puertas a nuevas aplicaciones con impactos positivos sobre la sociedad como pueden ser el estado actual de los bosques, el nivel de contaminación, mediciones sobre el reciclaje, consumos de energía, etc.

#### 2.4.10.9 Tecnologías con las que trabaja IoT

La arquitectura de IoT se basa en la comunicación entre dispositivos conectados unos con otros, produciéndose la comunicación máquina a máquina (M2M), que, aunque es un concepto general se aplica a la arquitectura de IoT. En este apartado final, se explicará más a fondo la tecnología con la que trabaja IoT que se ha dividido en cuatro grupos.

**A. Tecnologías de recolección de datos**

En todos los puntos anteriores se ha explicado la importancia de los sensores en la tecnología de IoT. En este apartado se recopilará y describirán algunos de los sensores más usuales y sus características. Los sensores recogen por lo general variables físicas del entorno. Un sensor puede estar conectado a una calle, a una persona o a un automóvil, y se encargará de recoger datos característicos de lo que están conectados. Según la RAE, un sensor es: "Dispositivo que detecta una determinada acción externa, temperatura, precisión, etc.…, y la transmite adecuadamente". Con base a esta definición, un sensor es un dispositivo eléctrico. Un sensor también podría ser un componente M2M, como un lector RFID (Radio Frecuency IDentification), o un medidor de SCADA (Supervisory Control And Data Adquisition). A parte de estos sensores, tenemos otros dispositivos que actúan como sensores ya sean porque tienen sensores incrustados, como por ejemplo los teléfonos móviles, dispositivos del hogar, vehículos etc.… Debido a las grandes diferencias existentes entre los sensores que recogen datos, debe de existir una plataforma que gestione las diferencias de datos. Como se comentó, los actuales Smartphones, recolectan infinidad de datos precisos en tiempo real, lo que se convierten en el

dispositivo número uno en la integración de IoT. Los fabricantes de dispositivos móviles deberán de comenzar a crear sensores más sofisticados para aumentar aún más la potencia y capacidad de recolección de datos. Los lectores RFID, NFIC, lectores NFIC, e incluso los códigos QR pueden ser leídos por los Smartphones.

### B. Tecnologías de comunicación de datos

Igual de importante que los sensores es la infraestructura de comunicación. Las redes inalámbricas son las que van a permitir la conexión entre todos las “things” y las personas. Las redes inalámbricas permiten crear y desarrollar aplicaciones basados en la ubicuidad y la innovación. Actualmente cualquier usuario asume que en cualquier lugar a dónde va, va a disponer de una conexión a internet y va a poder utilizar todos los servicios disponibles.

El cambio necesario que se va a producir en el cambio de IPV4 a IPV6 va a permitir que todos los objetos del planeta conectados tengan una IP propia. Las redes inalámbricas para la IoT se pueden clasificar en redes de corto alcance como son PAN, LAN, MAN, RFID, WIFI, WiMax y redes de largo alcance como WAN, GSM, CDMA, WCDMA y otras redes como vía satélite.

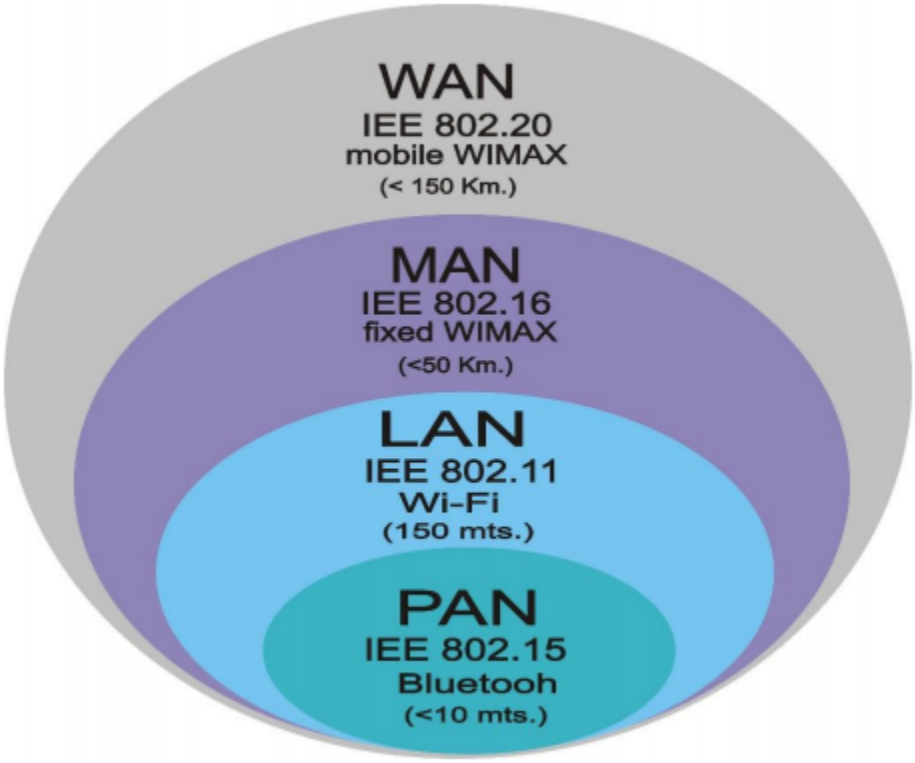



**Ilustración 9. Cobertura geográfica de las redes. Amelicia Castillo**

Por último, existe otra tecnología de comunicación como son los satélites COMSAT. Son satélites de comunicaciones en una localización determinada que recibe ondas procedentes de una posición y las transmite a otra. Estos satélites funcionan actualmente trabajando para las comunicaciones de buques, aviones, telefonía, televisión, radio o GPS. Estos satélites se pueden utilizar para la tecnología M2M, produciendo una mejor cobertura en zonas remotas.

### C. Tecnologías de almacenamiento y análisis

Por último, para completar el trío de tecnologías necesarias para el desarrollo de IoT, se tiene que hablar de plataformas donde se almacena la gran cantidad de datos que provienen de todos los sensores y transportadas por las redes inalámbricas. Estas

plataformas deben de permitir la gestión y el análisis de los datos en tiempo real y poder relacionar tecnologías como Big data, data mining o fusión de datos.

### 2.4.11 Amenazas que enfrenta IoT

#### 2.4.11.1 Seguridad

En este momento que se encuentra el TFG, es donde se tienen que identificar los agujeros de seguridad en los dispositivos que conformarán la gran red de IoT, se tiene que tener en cuenta las diferentes vías de ataque de estos dispositivos, así como los ordenadores personales. Hay que tener claro entonces las diferencias de estos dispositivos con respecto a los demás. Estos dispositivos empotrados son menos complejos que un ordenador personal ya que están diseñados para ejecutar una tarea o funcionalidad en específico y no algo general. Esto hace que estos sistemas sean muy variables ya que cada fabricante lo realice de una forma diferente a los demás, siguiendo su propio diseño. Esto dificulta que se pueda seguir un operativo común como ocurre con los ordenadores personales o smarthphones. Así, los ordenadores personales utilizan un sistema operativo común (Windows, Linux, …), y los Smartphones (Android, iOS,). De este modo se pueden mantener actualizaciones de seguridad comunes a cada sistema operativo porque es el fabricante de software quien las crea y despliega en los diferentes dispositivos. En el caso de los dispositivos de IoT, es el fabricante del propio hardware quien se encarga de la creación y mantenimiento del software. De esta forma, puede que no se tenga la experiencia ni recursos para poder generar un buen sistema de seguridad y protegerse ante posibles amenazas. A esto hay que añadirle que estos sistemas no se fabricaron ni se diseñaron para estar conectados a la red, lo que conlleva que sean todavía más vulnerables y tengan un

riesgo más alto. Existe un concepto que se denomina “Security by Default”, que no es más que el establecimiento de una configuración por defecto que sea segura en el momento de la fabricación y distribución de un dispositivo. Con este concepto se pretende solucionar el problema que tienen estos dispositivos, que no vienen dados por las capacidades o calidad de estos, sino por la ausencia de interfaces amigables que permitan administrarlos como en el caso de los PC o Smartphones. Lamentablemente el problema es que estas configuraciones no se tienen demasiado en cuenta, y los dispositivos salen al mercado y se comercializan con un nivel de seguridad medio o bajo. Finalmente, otro de los puntos débiles de los dispositivos de IoT es su ubicación física, ya que pueden ser desde frigoríficos, sensores en semáforos, casas inteligentes, actuadores medioambientales, etc., haciendo más difíciles de proteger por el hecho de que son accesibles a todo el mundo. Tal vez este sea uno de los problemas más graves. Todo esto, añadido a los problemas de seguridad por defecto sobre la confidencialidad, integridad y disponibilidad, y que estos dispositivos tienen la capacidad de hacer cambios y actuar sobre el mundo real, puede ser un verdadero problema si no se consigue crear un sistema de seguridad fuerte y robusto que los proteja de todas las amenazas.

Existen varias formas en que un atacante puede acceder a distintas características o a distintos datos de un dispositivo conectado. Los tres puntos principales que suelen ser objeto de los hackers son: el dispositivo, la red y la infraestructura de la nube.

**Dispositivos:** Un gran número de proveedores de silicio han realizado recientemente adquisiciones estratégicas para acreditar sus credenciales de seguridad

y permitir a desarrolladores de software que establezcan altos niveles de seguridad en sus aplicaciones de IoT. En muchos casos, los fabricantes de chips empiezan a reconocer la seguridad no como una competencia básica, sino como un conductor fundamental de valor dentro del ecosistema IoT. (WillisTowersWatson, 2016)

**Redes:** A medida que el IoT ha ido más allá de los móviles, se han ido introduciendo una serie de nuevas tecnologías inalámbricas, cada una con su propio listado de riesgos. Por ejemplo, la incorporación del Wi-Fi y el Bluetooth en los coches, ha creado miles de puntos que podrían ser hackeados. (WillisTowersWatson, 2016)

**La nube:** Como parte de la magia del IoT está la habilidad para almacenar mega volúmenes de datos en la nube. Circunstancia que aumenta las expectativas para operaciones de seguridad de tránsito de datos desde los aparatos hasta la nube. (WillsTowersWatson, 2016)

Hay tres pilares fundamentales para proteger un dispositivo vinculado a IoT y así garantizar que tanto la información en reposo como la información en movimiento se mantengan a salvo. (WillisTowersWatson, 2016)

#### 2.4.11.2 Pilares de seguridad para IoT

**Primer pilar - La seguridad del dispositivo**

Miles de millones de dispositivos conectados aumentan el uso de las aplicaciones de software y de los datos que se encuentran en los recursos de las empresas y en los dispositivos de consumo, lo que implica nuevos puntos de ataque para los hackers maliciosos. (Gemalto, 2016)

**Segundo pilar - La seguridad de la nube**

Las amenazas más urgentes vienen del entorno de la empresa o del entorno de la nube al que estos dispositivos inteligentes están conectados. (Gemalto, 2016)

**Tercer pilar – La gestión del ciclo de vida de la seguridad**

Si bien a menudo se pasa por alto, la gestión del ciclo de vida de los componentes de seguridad del dispositivo y del espectro de la nube, es un elemento fundamental para una estrategia de seguridad digital robusta y de largo plazo. La seguridad no es una actividad de una sola vez, sino una parte en evolución del ecosistema de IoT. El agregado de nuevos dispositivos, el desmantelamiento del dispositivo al final de su vida útil, la integración del dispositivo en un nuevo ecosistema de la nube o viceversa, la gestión de la descarga de firmware/software seguro son actividades que necesitan una gestión completa de las identidades, las claves y los tokens. (Gemalto, 2016)

#### 2.4.11.3 Seguridad en la transmisión de datos

Se procederá entonces a analizar detalladamente los posibles agujeros (o canales) de los que se puede sacar información en la vida útil de los dispositivos de IoT. Se empezará con la que parece la vía más obvia en cuanto a posibles ataques se refiere. La transmisión de datos entre los dispositivos conectados a IoT, puesto que estos dispositivos están enfocados a estar continuamente transmitiendo información entre ellos o hacia la nube.

Es fácil reconocer que es en este aspecto donde se debe centrar la defensa

respecto a posibles ataques ya que los sistemas distribuidos emplean numerosos canales de distribución, ya sea inalámbricos, por cable u otros. Todas estas vías de información, sobre todo las que son inalámbricas y públicas, son susceptibles de sufrir ataques.

Es por eso por lo que estos dispositivos necesitan garantizar un nivel de seguridad mínimo en cuanto a la integridad, protección y encriptación de sus comunicaciones, ya que si no se proporcionan estos niveles de seguridad, no será complicado que un atacante pueda acceder a esa información intercambiada.

La información puede contener tanto datos privados como datos personales, incluso información acerca de los dispositivos que puedan permitir el control de este. Es necesario por tanto, un buen sistema de cifrado de datos para evitar los ataques de tipo *Man in The Middle*, en el que el atacante se encuentra en el medio de los dos extremos de la comunicación y simplemente interfiere todos los mensajes de esta sin que los comunicadores se den cuenta de que están siendo interceptados y posiblemente alterados. Esto último es altamente peligroso debido a que, si la información que se modifica actúa directamente sobre el dispositivo y su actividad, puede causar un gran problema, siendo incluso peligroso para la vida de las personas.

Vamos a poner un escenario en el que se va a poder apreciar las consecuencias de un posible ataque en la comunicación entre un dispositivo y su conexión con los datos a la nube.

Supongamos que hemos comprado una moto de último modelo, que incorpora entre otras cosas un sistema inteligente conectado a la red que ofrece servicios

ofrecidos por el fabricante, facilitándonos información como la velocidad, posición, tiempo medio, estado general de la moto, etc. Supongamos también que la comunicación entre nuestro vehículo e Internet es poco segura y tiene un nivel bajo de encriptación. Un atacante podría acceder a la comunicación y obtener valores como la posición del vehículo, sabiendo en todo momento la ruta que seguimos, dónde vivimos, donde trabajamos etc. También podría conocer el estado del motor, nivel de líquidos.

El otro factor importante, es que, si este atacante puede modificar la información en la comunicación y pudiera dar las mismas órdenes que damos nosotros, podría hacer que se encendieran las luces, cambiar de marcha, acelerar, frenar, dependiendo de las funcionalidades que permita hacer el dispositivo de IoT.

#### *2.4.11.4* Seguridad en el *software*

Se pasará ahora a otro de los canales sobre los que se pueden realizar más ataques. Es el aprovechamiento de las debilidades en el *software* en los dispositivos IoT. Cuando se crea un dispositivo y se le añade un sistema operativo, normalmente se utilizan versiones simplificadas de los sistemas operativos de uso común como pueden ser *Windows, Linux*, etc. De esta forma los costes de fabricación de estos dispositivos se reducen considerablemente. Esta práctica, evidentemente supone un riesgo a la seguridad,  ya que cuando se detecta una vulnerabilidad en estos sistemas operativos se explotan en todos los dispositivos que lo tengan instalado.

Otra característica que se obtiene al desarrollar el dispositivo abaratando costes en su desarrollo, es la interfaz web. Estos, al ser de pequeño tamaño, y no disponer la mayoría de una pantalla, tienen que ser controlados a través de Internet. Si estas

interfaces para acceder a los dispositivos y configurarlos, manipularlos, etc., no se protegen debidamente, cuando se produzca algún ataque y accedan intrusos, podrán acceder a todos los dispositivos que usen esa interfaz.

Una última característica que tienen en común la mayoría de los dispositivos de IoT es su acceso a los servicios en la nube. Si en estas plataformas de servicio no se llevan a cabo tareas de mantenimiento, actualización y protección, puede ser una vía muy peligrosa acceder a toda la información y poder tomar el control de los dispositivos.

Algunos dispositivos como Smartphones o televisiones inteligentes pueden acceder a repositorios de aplicaciones para añadir nuevas funcionalidades. Ésta puede ser la puerta de entrada a aplicaciones maliciosas que puedan tomar el control de los dispositivos, explotar vulnerabilidades, obtener información confidencial, o incluso descargando más aplicaciones maliciosas sin nuestro consentimiento. Por tanto, de igual manera, los responsables de estos servicios en la nube y repositorios tienen la misma responsabilidad de mantener correctamente sus servicios para permitir que los dispositivos accedan a ellos sin ningún problema para su seguridad.

#### 2.4.11.5 Seguridad en la configuración y funcionalidad

Muchas veces, el principal problema en cuanto a seguridad se refiere, radica principalmente en la configuración (por defecto, y posibles opciones configurables) y la funcionalidad del propio dispositivo. Muchos fabricantes, a la hora de establecer la configuración por defecto del dispositivo, eligen unas opciones que posiblemente el usuario no va a utilizar nunca, o bien, que por estar activadas y permitir el uso de esa

funcionalidad avanzada, el usuario no tenga suficientes conocimientos y la emplee mal, produciendo una brecha de seguridad y posible acceso para intrusos.

De nuevo, entra en juego el papel de fabricantes, que son los responsables directos de esta posible vía de acceso de intrusos. Los distribuidores deben ser conscientes, y adoptar una política de configuración segura, permitiendo además a los usuarios poder configurar el dispositivo acorde a sus necesidades, sin ser un sistema rígido, marcado con las opciones de fábrica.

Se pondrá un ejemplo para poder entender mejor este problema.

Cuando adquirimos un Smartphone, este viene con unas configuraciones por defecto generales del dispositivo, y además viene con un apartado de configuración para redes. Esta configuración por defecto puede ser peligrosa. Si viene activado para que el dispositivo esté conectado permanentemente a Internet, y un usuario inexperto no es consciente de esto, puede ser un problema, ya que el dispositivo estará continuamente conectado a Internet, descargando y transfiriendo datos, a lo mejor sin el conocimiento del usuario.

#### *2.4.11.6* Seguridad en el *hardware*

Para este caso, esta posible brecha de seguridad ya existe antes de IoT. Los problemas debidos a la mala política de seguridad para el *hardware* son las menos frecuentes, pero lamentablemente son las que producen problemas más difíciles de solucionar.

Obviamente, los problemas de seguridad en el *hardware* se producen sin la

necesidad de estar conectados a Internet, pero puesto que los dispositivos de IoT también cuentan con este problema, se ha incluido en esta lista de posibles brechas de seguridad.

Los ataques contra el *hardware s*e producen, sobre todo, cuando el dispositivo tiene una gran seguridad a nivel de *software*, cuando se encuentran en puntos aislados de la red, o cuando están bien protegidas para un acceso a través de Internet.

Es entonces cuando se producen estos ataques, que suelen estar dirigidos a los componentes conectados a la red eléctrica.

La diferencia de estos ataques es que para realizarlos es necesario un equipamiento especializado para producirlos. Según el equipo del que se disponga se podrán realizar diferentes tipos de ataques, desde ingeniería inversa a monitorización de interfaces.

Los ataques más habituales son los accesos a la información, tanto volátil y no volátil como memoria RAM y discos duros. Si podemos acceder a la memoria no volátil, es posible acceder a claves, información de acceso, etc. Si podemos acceder a la memoria no volátil, se puede acceder a toda la información guardada.

Hay dos posibles protecciones para este tipo de ataques:

El primero de ellos es garantizar que, si el dispositivo es manipulado, automáticamente se destruya la información que contenta. La segunda es un buen sistema de cifrado de información, de modo que, si finalmente acceden a los datos, les sea imposible descifrarlos.

Un punto para tener en cuenta en este apartado es el borrado de información.

Cuando un dato se borra de un dispositivo no volátil, se modifican las tablas de asignación de archivos en el sistema de ficheros, haciendo que el espacio que ocupaba el dato está disponible para otro nuevo dato, pero sin realizar un borrado efectivo.

Existen herramientas que, sin un mínimo de procesos de formateo, es posible recuperar la información que se encontraba en el disco.

#### 2.4.11.7 Seguridad en los usuarios

Se va a terminar con una vía de acceso que no está relacionada directamente con los dispositivos IoT, sino con los usuarios. En muchos casos, si todos los puntos anteriores como el *software, hardware*, comunicaciones y configuraciones están perfectamente protegidos y construidos, un mal uso del usuario puede poner en serio peligro toda la información del dispositivo. Es probablemente el principal motivo por el que se producen ataques sobre los dispositivos, ya que, como parte de la cadena, los usuarios somos el eslabón más débil y podemos cometer errores.

El principal ataque se basa en la llamada ingeniería social. Básicamente se centra en aprovechar los errores humanos para comprometer la seguridad de los dispositivos mediante la confusión y el engaño.

Debido a que la mayoría de los accesos a las plataformas privadas en Internet son a través de unas credenciales, la ingeniería social intenta acceder a ellas mediante estafas a través de correos electrónicos, sitios web falsos, o suplantación de identidad.

Estos ataques están dirigidos a grandes empresas y clientes potenciales para

poder obtener un mayor beneficio.

Es necesario crear una cultura de seguridad para los usuarios y concienciarlos sobre los problemas que pueden producir si no ponen atención a sus actividades mientras utilizan los dispositivos, ya que como hemos comentado anteriormente, no sirve de nada que un dispositivo esté perfectamente protegido, si nuestra clave de seguridad la apuntamos en nuestra red social preferida.

# Capítulo III

# Referencias Bibliográficas

## 3.1 Estado de la cuestión

Se ha decidido realizar una investigación relacionada a la seguridad y privacidad de la información en la incorporación de IoT, debido a que se ha incrementado una cantidad importante de dispositivos de este tipo al igual que los ciberdelitos.

El siguiente estado de la cuestión recorre una selección de diferentes autores expertos en seguridad de la información, los cuales han publicado sus artículos referentes a este tema y de los cuales su calificación se ha verificado en la fuente scholar.google.com

Inicialmente, para realizar el sondeo del estado de la cuestión de este tema se utilizó Google Académico (scholar.google.com) en donde se aplicaron los siguientes criterios de búsqueda.

**seguridad + privacidad + IoT**

Se obtuvieron 594 resultados:

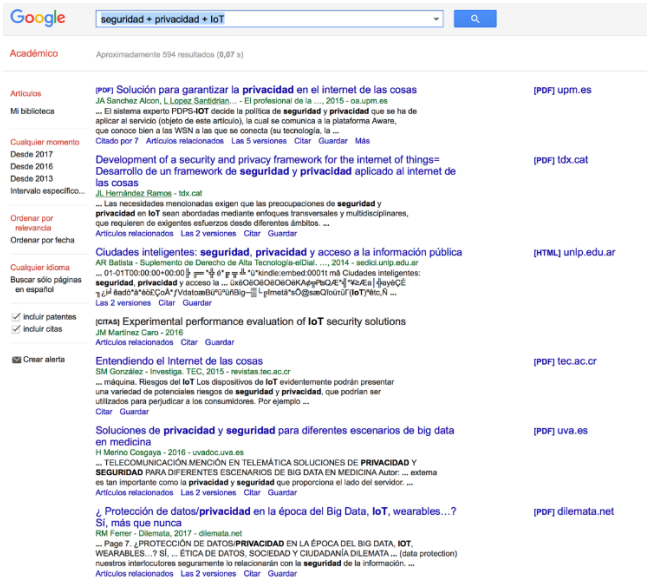



**Ilustración 9. seguridad + privacidad + IoT. Propia**

Al modificar la búsqueda con el siguiente criterio:

**seguridad + privacidad + ataques +IoT**

Se obtuvieron 242 resultados:

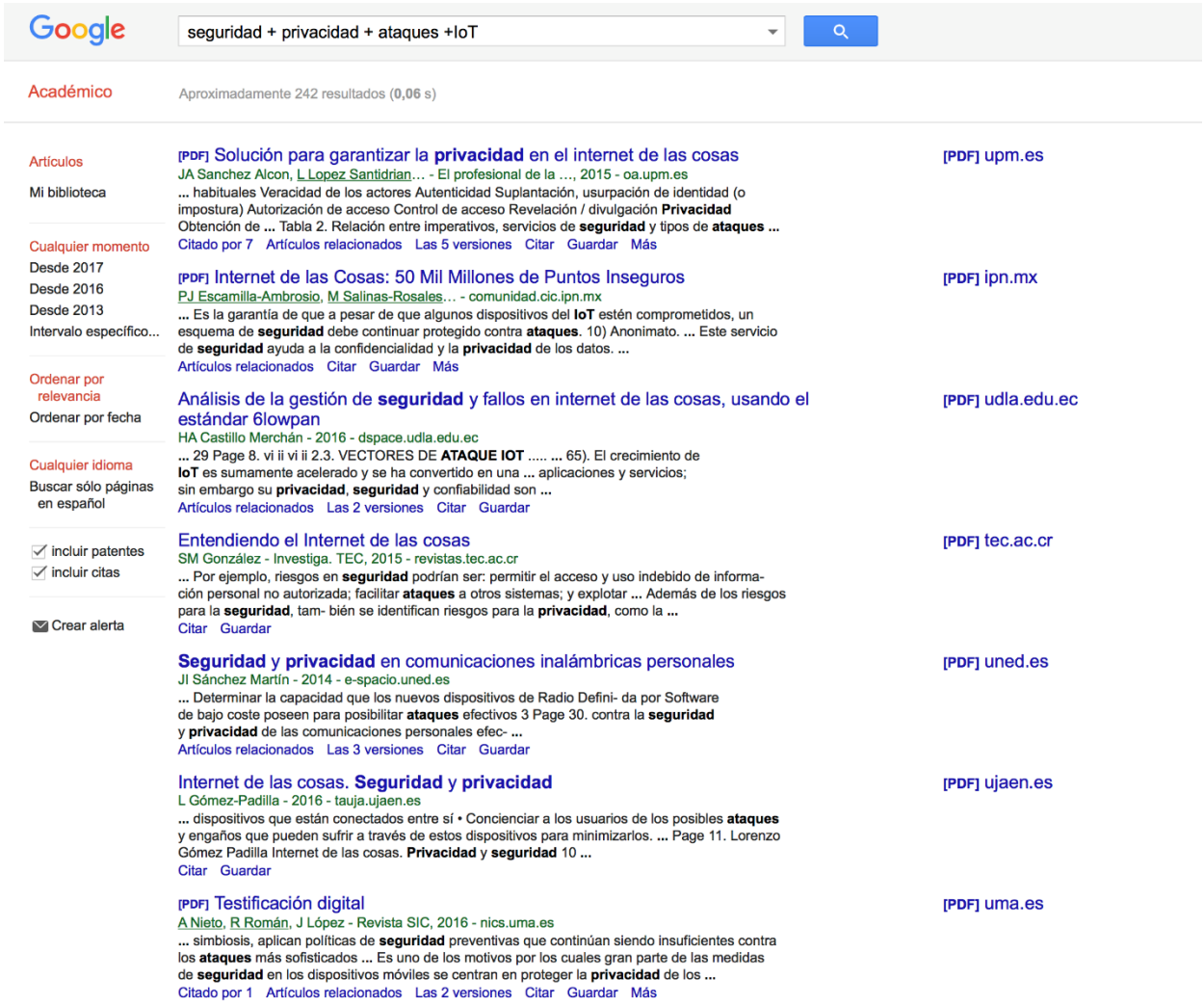



**Ilustración 10. seguridad + privacidad + ataques +IoT. Propia**

Se procede a especificar el país Costa Rica.

**seguridad + privacidad + ataques +IoT + Costa Rica**

Se obtuvieron 23 resultados:

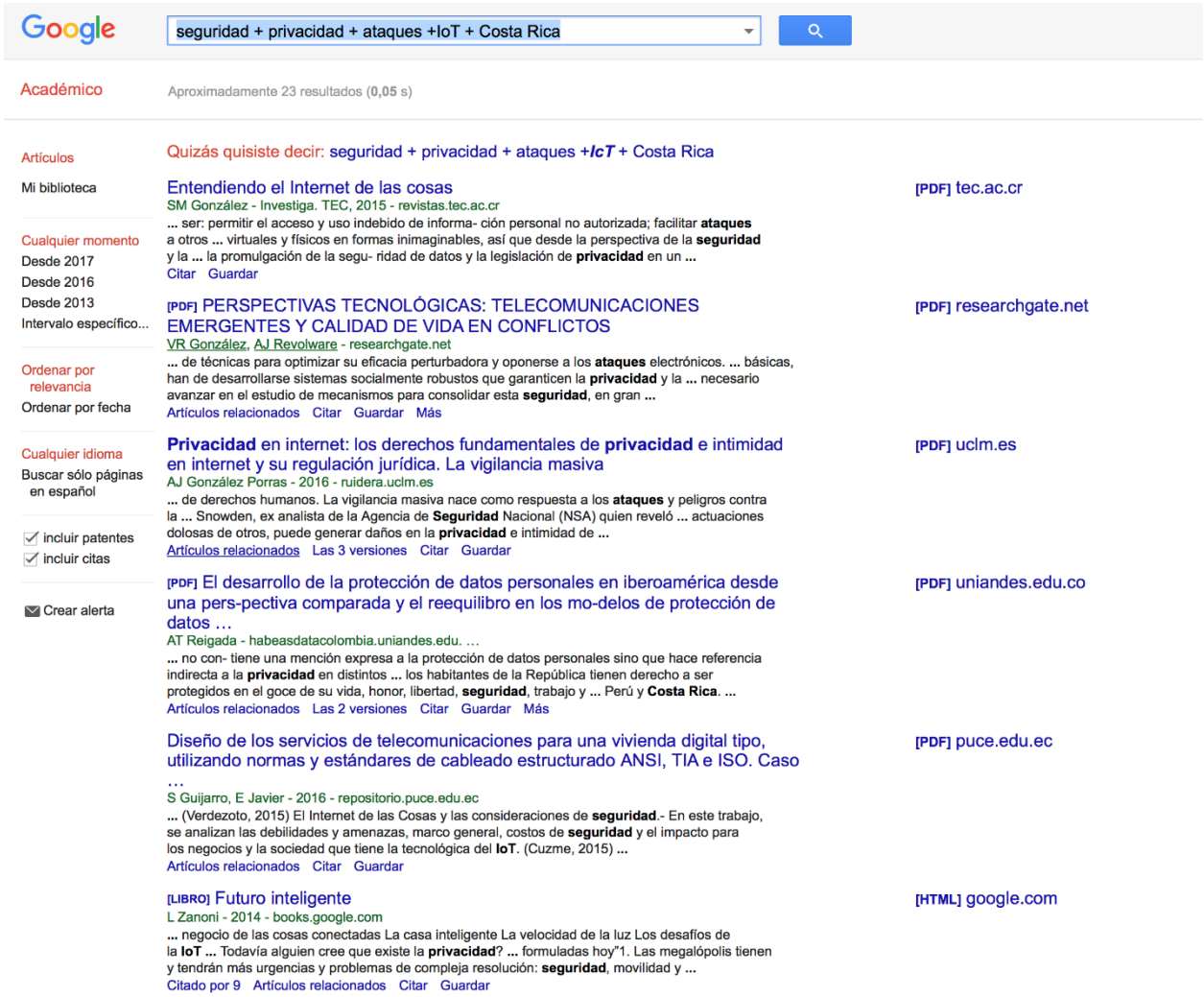



**Ilustración 11. seguridad + privacidad + ataques +IoT + Costa Rica. Propia**

Se procede a especificar el país y específicamente las leyes de Costa Rica para obtener datos más específicos:

**seguridad + privacidad + ataques +IoT + leyes en Costa Rica**

Se obtuvieron 23 resultados:

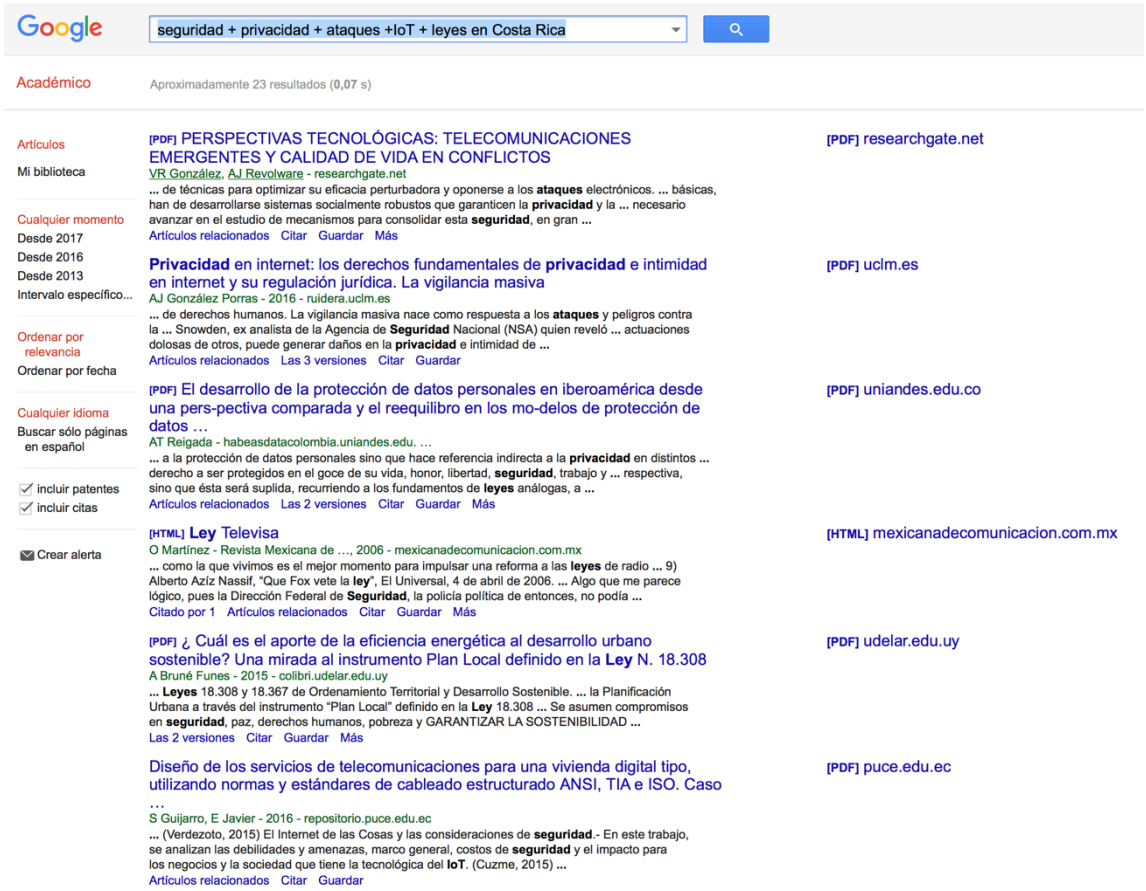



**Ilustración 12. seguridad + privacidad + ataques +IoT + leyes en Costa Rica. Propia**

El especificar las palabras “legislación costarricense” se delimitan los resultados únicamente a 3 resultados denotando solamente un único caso en el 2017, el cual hace énfasis a un caso en Ecuador, por lo tanto, no hay especificaciones exactas de este año con esos atributos:

**seguridad + privacidad + ataques +IoT + legislación costarricense**

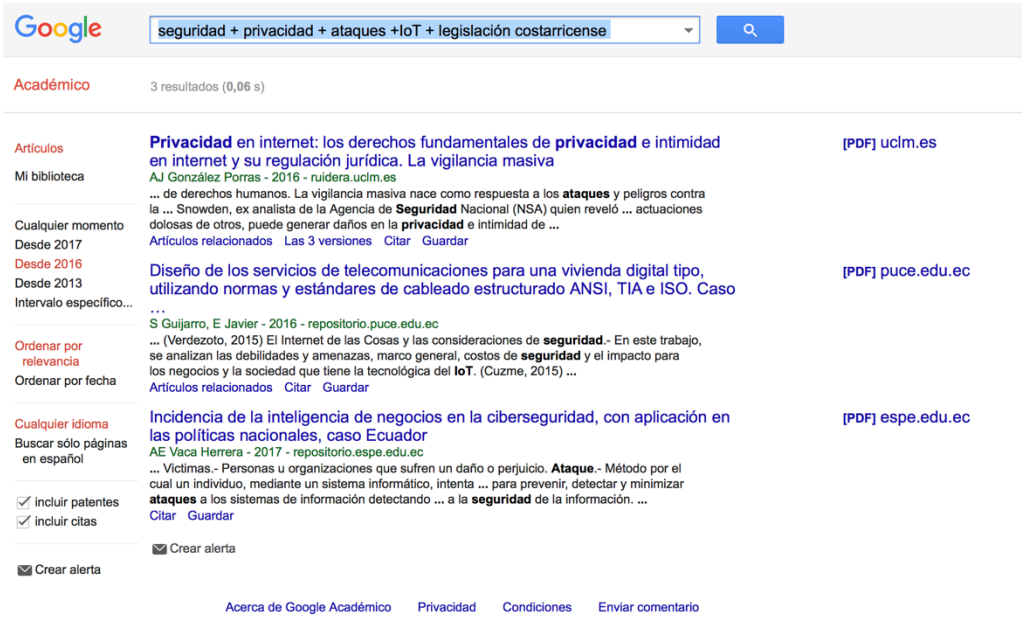



**Ilustración 13. seguridad + privacidad + ataques +IoT + legislación costarricense. Propia**

Con los resultados obtenidos de la búsqueda anterior, la investigadora estudia la selección de publicaciones con el fin de evaluar la revolución tecnológica conocida como seguridad y privacidad de IoT en Costa Rica, los riesgos que conlleva y las mejores prácticas de cómo asegurarla con la legislación costarricense.

Esta investigación se centra, entonces, en el análisis de uno de los mayores cambios que han incrementado en los últimos dos años, sin lugar a duda, IoT se ha convertido en una era de innovación que también involucra consecuencias a nivel de seguridad de la información.

Ahora bien, basado en la lectura de los artículos investigados anteriormente, los cuales guiarán esta investigación, se procede al desarrollo del TFG con el fin de poder mitigar el problema actual presentado en la sección 1.3 Definición y Descripción del Problema del capítulo introductorio.

# Capítulo IV

# Marco Metodológico

## 4.1 Tipo de Investigación

Este estudio define la investigación como evaluativa, ya que el objetivo principal es evaluar lo que ya existe y comparar la legislación costarricense con marcos jurídicos de Europa, Canadá, Estados Unidos y otros, con el fin de emitir criterios a la luz de los hallazgos y de aquellos agujeros jurídicos encontrados, los cuales se harán por medio de recomendaciones.

## 4.2 Alcance investigativo

Este estudio por su naturaleza y por las características que presenta se considera de tipo exploratorio, explicativo y descriptivo.

De acuerdo con la literatura estudiada hasta el momento, el tema seleccionado ha sido poco investigado. Por lo tanto y citando a Hernández y otros (2003, pág.113) **"los estudios exploratorios son aquellos que se efectúan cuando el objeto es examinar un tema o un problema de investigación poco estudiado o que no ha sido abordado antes".**

Según el mismo autor, los estudios exploratorios sirven **"para familiarizarse con fenómenos relativamente desconocidos, obtener información sobre la posibilidad de llevar a cabo una investigación más completa sobre un contexto particular, investigar problemas del comportamiento humano"**

(2003, pág. 116).

Tal es la situación que se desea investigar, pues el fenómeno existe, pero no se ha indagado desde todos los ángulos posibles, lo cual resta perspectiva para una futura visión del conjunto, como es el caso de evaluar la efectiva aplicación de la legislación

costarricense en el desarrollo de proyectos IoT para dimensionar sus repercusiones en la seguridad y privacidad de los datos.

Por otra parte, se dice que es explicativo, pues de acuerdo con Hernández y otros (2003, pág. 126) **"Los estudios explicativos van más allá de la descripción de conceptos o fenómenos. Como su nombre lo indica, su interés se centra en explicar por qué ocurre un fenómeno y en qué condiciones se da éste".**

Por último, este estudio se define como descriptivo pues "**busca especificar las propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno que sea sometido análisis"** Hernández y otros. (2003, pág.117).

Esta investigación busca evaluar la legislación actual de Costa Rica en el tema del Internet de las cosas estableciendo la situación actual en la que se está viendo vulnerable la incorporación y el uso de esta nueva tecnología, recomendando soluciones para mejorar el manejo de la información por parte de los usuarios y empresas.

## 4.3 Enfoque

Este estudio es de enfoque cuantitativo y como indica Gómez, de acuerdo con este tipo de enfoque, **"la recolección de datos es equivalente a medir"** Gómez (2006:121)

Por otra parte, Galeano indica que **"los estudios de corte cuantitativo pretenden la explicación de una realidad social vista desde una perspectiva externa y objetiva. Su intención es buscar la exactitud de mediciones o indicadores sociales con el fin de generalizar sus resultados a poblaciones o situaciones amplias. Trabajan fundamentalmente con el número, el dato**

**cuantificable**” (Galeano, 2004:24).

## 4.4 Diseño

Para lograr dar cuerpo a la investigación y establecer las características de los temas en estudio es necesario **“seleccionar una serie de cuestionarios, recolectar y tabular la información recopilada en cada uno de ellos, para así describir lo que se investiga”** Hernández y otros. (2003, pág.118)

Esta investigación busca evaluar la efectiva aplicación de la legislación costarricense en el desarrollo de proyectos IoT para dimensionar sus repercusiones en la seguridad y privacidad de los datos y qué mejor forma de poder realizar dicha evaluación por medio de la recolección de datos.

Este estudio busca evaluar el tema entre las personas fenómenos que serán sometidos a análisis mediante la recopilación de información, la cual se llevará a cabo a través de encuestas, cuestionarios y observación de grupos.

## 4.5 Población y muestreo

Para el estudio se considera la participación de la siguiente población: son cinco abogados, dos ingenieros informáticos con énfasis en delitos informáticos, cinco empleados del departamento de TI del sector público y cinco empleados del departamento de TI del sector privado, un investigador del OIJ, dos investigadores de empresas privadas, cinco especialistas de seguridad informática, diez civiles.

Para llevar a cabo el trabajo se someterán a las treinta y cinco personas de las diferentes áreas, cuya información se recopilará mediante los cuestionarios, que se aplicarán al 100% de la población.

## 4.6 Instrumentos de recolección de datos

Los instrumentos de recolección de datos que se utilizan en la investigación son cuestionarios, ya que la encuesta permite evaluar la información de la muestra de sujetos representativa de un colectivo más amplio, utilizando procedimientos estandarizados de interrogación con el fin de obtener mediciones cuantitativas de una gran variedad de características objetivas y subjetivas de la población.

## 4.7 Técnicas de análisis de información

Las técnicas de análisis de información que se utilizarán en el capítulo IV de análisis de datos corresponden a la tabulación de la información y a la representación gráfica de los resultados obtenidos, los cuales se desarrollarán por medio de variables.

## 4.8 Variables

Variables son las condiciones o características que manipula, controla u observa el investigador. Son importantes debido a que miden y se relacionan para determinar las causas y efectos, además las posibles relaciones entre sí. Estas deben ser observadas y medidas.

Para efectos de este estudio, se tomarán en cuenta las siguientes variables:

1. La efectiva aplicación de la legislación costarricense en el desarrollo de proyectos IoT.
2. Repercusiones en la seguridad y privacidad de los datos.
3. Los riesgos que implican la incorporación de IoT y las acciones que afectan la privacidad de los datos.

4. Las leyes y reglamentos en Costa Rica protegen la seguridad y privacidad de la información.
5. Los agujeros de seguridad en los dispositivos que conformarán la gran red de IoT.
6. El manejo de la información por parte de los usuarios y empresas.

### 4.8.1 La efectiva aplicación de la legislación costarricense en el desarrollo de proyectos IoT.

**Definición conceptual**

Se entenderá como legislación, por una parte, a todo el conjunto de leyes que existen en un Estado y que regulan los comportamientos de los individuos pertenecientes al territorio de un país. En este sentido, consiste en todo el ordenamiento jurídico, todo el sistema o conjunto de normas que pueden encontrarse en un país, y que responden a un sistema jurídico específico.

**Instrumentalización**

La información correspondiente a esta variable se obtendrá mediante la aplicación de los cuestionarios correspondientes a toda la muestra en estudio.

**Operacionalización**

En el caso de la información recopilada mediante los cuestionarios y el análisis de resultados de una serie de preguntas las cuales constan en el cuestionario adjunto en los anexos. Los resultados serán positivos si al menos el 70% a 100% de la población encuestada contestan en forma satisfactoria los cuestionamientos.

### 4.8.2 Repercusiones en la seguridad y privacidad de los datos.

**Definición conceptual**

Se entenderá como seguridad (del latín securitas), a la ausencia de riesgo o a la confianza en algo o en alguien. Sin embargo, el término puede tomar diversos sentidos según el área o campo a la que haga referencia en la seguridad. En términos generales, la seguridad se define como "el estado de bienestar que percibe y disfruta el ser humano".

Por otra parte, se entiende como privacidad, el ámbito de la vida personal de un individuo, quien se desarrolla en un espacio reservado, el cual debe mantenerse confidencial. También se aplica a la cualidad de privado.

**Instrumentalización**

La información correspondiente a esta variable se obtendrá mediante la aplicación los cuestionarios correspondientes a toda la muestra en estudio.

**Operacionalización**

En el caso de la información recopilada mediante los cuestionarios y el análisis de resultados de una serie de preguntas las cuales constan en el cuestionario adjunto en los anexos. Los resultados serán positivos si al menos el 70% a 100% de la población encuestada contestan en forma satisfactoria los cuestionamientos.

### 4.8.3 Los riesgos que implican la incorporación de IoT y las acciones que afectan la privacidad de los datos.

**Definición conceptual**

Se entenderá como IoT, a la Internet de las cosas (IoT, por sus siglas en inglés) es un sistema de dispositivos de computación interrelacionados, máquinas mecánicas y digitales, objetos, animales o personas que tienen identificadores únicos y la capacidad de transferir datos a través de una red, sin requerir de interacciones humano a humano o humano a computadora.

**Instrumentalización**

La información correspondiente a esta variable se obtendrá mediante la aplicación los cuestionarios correspondientes a toda la muestra en estudio.

**Operacionalización**

En el caso de la información recopilada mediante los cuestionarios y el análisis de resultados de una serie de preguntas las cuales constan en el cuestionario adjunto en los anexos. Los resultados serán positivos si al menos el 70% a 100% de la población encuestada contestan en forma satisfactoria los cuestionamientos.

### 4.8.4 Las leyes y reglamentos en Costa Rica protegen la seguridad y privacidad de la información.

**Definición conceptual**

Se entenderá como ley (en latín, lex, legis), a la norma jurídica dictada por el legislador, es decir, un precepto establecido por la autoridad competente, en que se manda o prohíbe algo en consonancia con la justicia cuyo incumplimiento conlleva a una sanción. Por otra parte, se entiende como reglamento un documento que

especifica una norma jurídica para regular todas las actividades de los miembros de una comunidad. Establecen bases para la convivencia y prevenir los conflictos que se puedan generar entre los individuos.

**Instrumentalización**

La información correspondiente a esta variable se obtendrá mediante la aplicación de los cuestionarios aplicados a los empleados de TI de empresas públicas y privadas, además de los especialistas en ciberseguridad informática y por último a los ingenieros informáticos con énfasis en delitos informáticos.

**Operacionalización**

En el caso de la información recopilada mediante los cuestionarios y el análisis de resultados de una serie de preguntas las cuales constan en el cuestionario adjunto en los anexos. Los resultados serán positivos si al menos el 70% a 100% de la población encuestada contestan en forma satisfactoria los cuestionamientos.

### 4.8.5 Los agujeros de seguridad en los dispositivos que conformarán la gran red de IoT.

**Definición conceptual**

Se entenderá como agujeros de seguridad, al fallo de un programa que permite mediante su explotación violar la seguridad informática de un sistema.

**Instrumentalización**

La información correspondiente a esta variable se obtendrá mediante la aplicación, los cuestionarios aplicados a los empleados de TI de empresas públicas y privadas, además de los especialistas en ciberseguridad informática y por último a los ingenieros informáticos con énfasis en delitos informáticos.

**Operacionalización**

En el caso de la información recopilada mediante los cuestionarios y el análisis de resultados de una serie de preguntas, las cuales constan en el cuestionario adjunto en los anexos. Los resultados serán positivos si al menos el 70% a 100% de la población encuestada contestan en forma satisfactoria los cuestionamientos.

### 4.8.6 El manejo de la información por parte de los usuarios y en las empresas.

**Definición conceptual**

Se entenderá como información, al conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

**Instrumentalización**

La información correspondiente a esta variable se obtendrá mediante la aplicación los cuestionarios aplicados a los civiles y a los ingenieros informáticos de empresas privadas y públicas.

**Operacionalización**

En el caso de la información recopilada mediante los cuestionarios y el análisis de resultados de una serie de preguntas las cuales constan en el cuestionario adjunto en los anexos. Los resultados serán positivos si al menos el 70% a 100% de la población encuestada contestan en forma satisfactoria los cuestionamientos.

# Capítulo V
# Análisis de Información

## 5.1 Análisis e interpretación de resultados

El procedimiento que se aplicará permitirá por lo descriptivo y explicativo en cada una de las etapas, el inferir según las necesidades de análisis de las variables si realmente se tomaron los datos de forma independiente y destacar posteriormente los resultados más relevantes, para dar respuesta al problema de investigación y lograr los objetivos propuestos. En este proceso se utilizará el diseño estadístico simple, que favorecerá la utilización de cifras porcentuales, que logren con ello, una interpretación más exacta a pesar de que hay preguntas de complemento.

## 3.2 Análisis de las Variables en Estudio

Este trabajo se aplicó a 35 personas en donde se destacan cinco abogados, dos ingenieros informáticos con énfasis en delitos informáticos, cinco empleados del departamento de TI del sector público y cinco empleados del departamento de TI del sector privado, un investigador del OIJ, dos investigadores de empresas privadas, cinco especialistas de seguridad informática, diez civiles. Sin lugar a duda son base para poder comprobar los grandes vacíos legales que se tienen actualmente.

Se realizaron entrevistas con cada una de las personas por medio de la página de *online* encuestas, en la cual se obtuvo el 100% de las respuestas a la población total.

Los resultados se presentan en su orden según las variables de estudio y cuya información se da en términos relativos o porcentuales para hacer análisis comparativos.  Dichos datos se presentarán de forma visual mediante una herramienta gráfica tanto de Excel como Word.

Una vez representada la información obtenida de las diversas fuentes a través de gráficos, se procede a realizar un análisis general de toda la información, la cual se tomará como referencia para proceder con las conclusiones y recomendaciones.

### 5.1.1 Análisis de la Variable #1

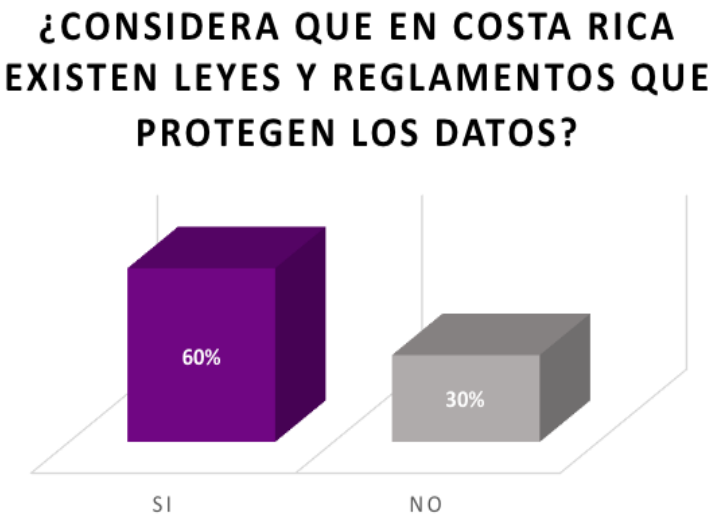
**La efectiva aplicación de la legislación costarricense en el desarrollo de proyectos IoT.**

Corresponde a la aplicación de la legislación con base en los delitos reportados o incumplimientos en el desarrollo de proyectos IoT.

**Objetivo analizado:**

Evaluar la efectiva aplicación de la legislación costarricense en el desarrollo de proyectos IoT para dimensionar sus repercusiones en la seguridad y privacidad de los datos.

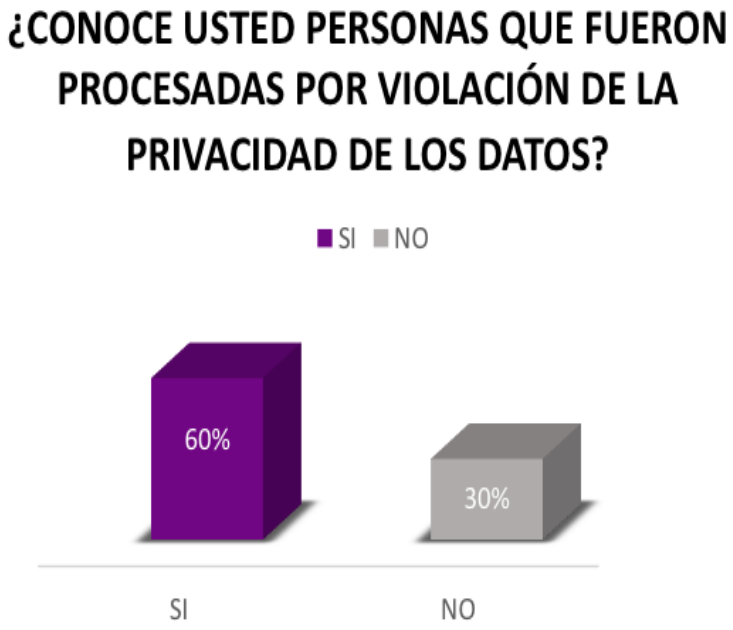
**Gráfico #1**




**Fuente: Anexo 1-Cuestionario para abogados**

El gráfico anterior fue aplicado a los cinco abogados en donde se puede observar que consideran que las leyes y reglamentos efectivamente protegen los datos de Costa Rica, dando como resultado un 60%. Por otra parte, un 30% de la población indicó que no se cuenta con las leyes y reglamentos adecuados o necesarios para proteger los datos del país.

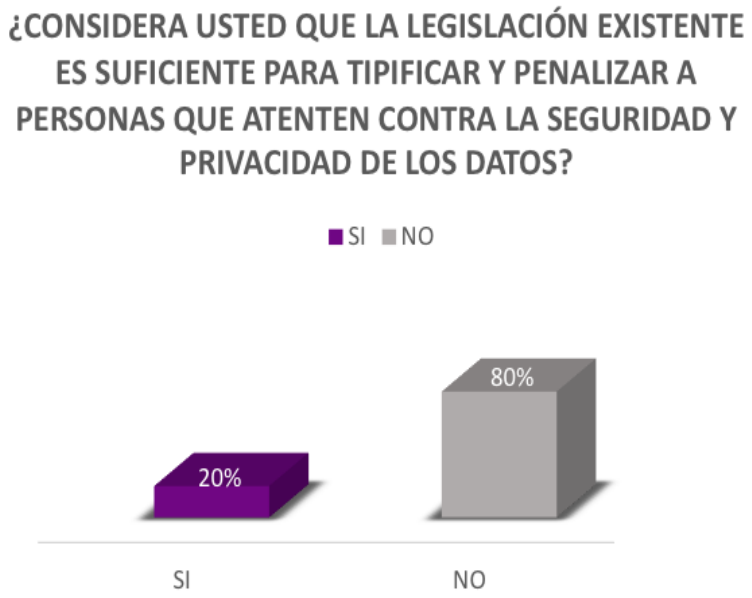
**Gráfico #2**




**Fuente: Anexo 1-Cuestionario para abogados**

El gráfico anterior, fue aplicado a los abogados, el 60% de los mismos han tratado casos relacionados a la violación de la privacidad de los datos, mientras que el 30% indicó que no conocen personas que fueran procesadas por esta situación.

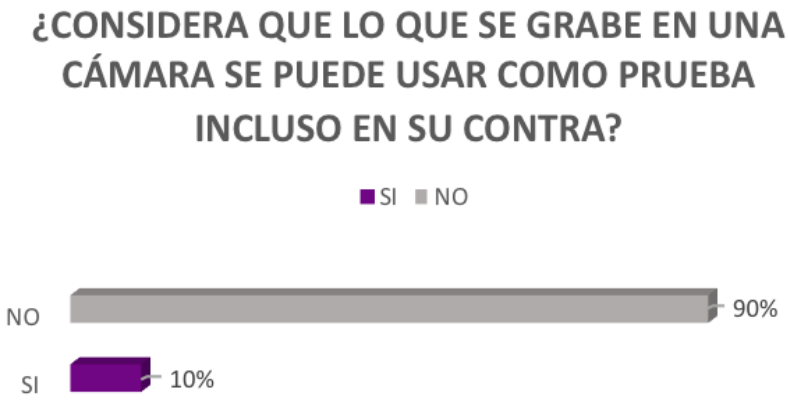
**Gráfico #3**




**Fuente: Anexo 1-Cuestionario para abogados**

Con base en la información anterior, se puede observar que el 80% de los abogados indicaron que la legislación existente no es suficiente para tipificar y penalizar a personas que atenten contra la seguridad y privacidad de los datos, por lo tanto, únicamente el 20% de ellos indicó lo contrario.

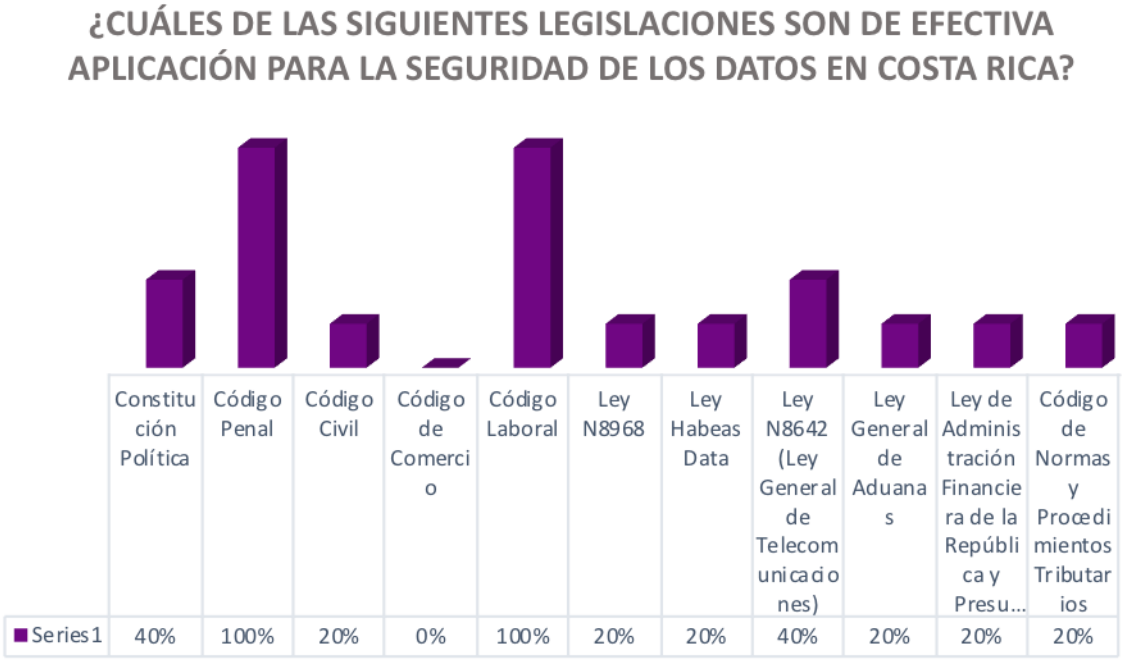
**Gráfico #4**




**Fuente: Anexo 2-Cuestionario para usuarios**

La información obtenida del gráfico anterior señala que el 90% de la población correspondiente a 9 personas, indicaron que desconocen que lo que se grabe en cualquier cámara puede usarse incluso en su contra ante cualquier situación, por lo tanto, únicamente un 10% indicó que sí conoce este tipo de pruebas.

**Gráfico #5**

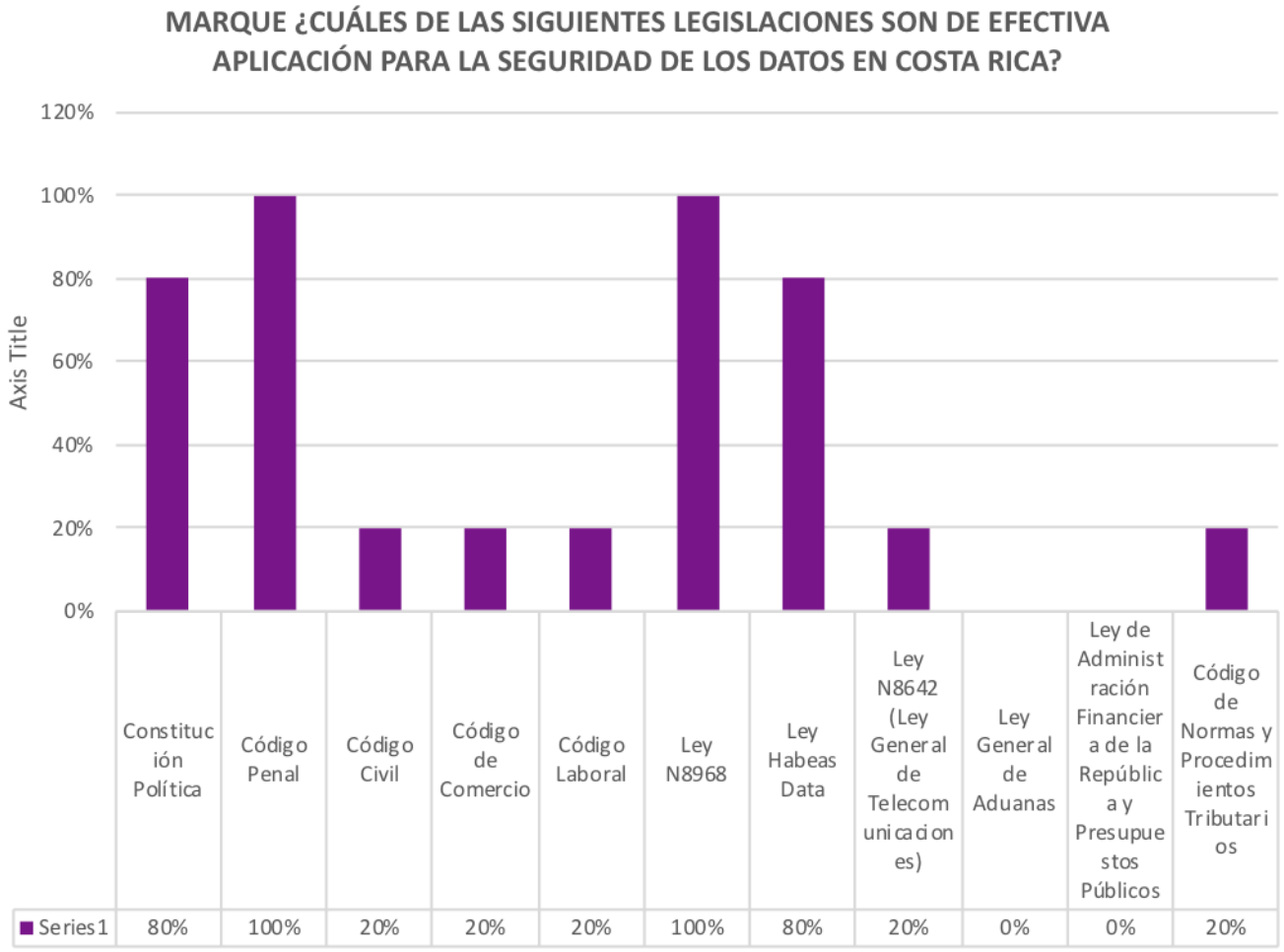



**Fuente: Anexo 3- Cuestionario para Ingenieros especialistas en ciberseguridad**

Se realizó un estudio con base en las legislaciones que se aplica para el manejo seguro de los datos en Costa Rica, por lo tanto, se aplicó dicho cuestionario a los especialistas en ciberseguridad y se obtuvo lo siguiente: toda la muestra indicó en un 100% que conocen el código Penal y el Código Laboral como legislaciones de seguridad de datos, únicamente un 20% indicó conoce la Ley No.8968 nombrada como la ley de protección de la persona frente al tratamiento de sus datos personales, por otra parte 20% conoce la Ley Habeas Data y un 40% indicó saber sobre la Ley General

de Telecomunicaciones, en igual porcentaje se tiene conocimiento de la Constitución Política y en un menor rango de 20% indicaron conocer sobre la Ley General de Aduanas, Ley de Administración Financiera de la República y Presupuestos Públicos y el Código de Normas y Procedimientos Tributarios.

**Gráfico #6**




**Fuente: Anexo 1-Cuestionario para abogados**

En el gráfico anterior se les preguntó a los abogados sobre las leyes que son de efectiva aplicación para la seguridad de los datos en Costa Rica y el 100% indicó El Código Penal y la Ley No.8968, además un 80% indicó la Constitución Política y la Ley

Habeas Data, involucrando en un 20% el código Civil, el Código de Comercio, Laboral, la Ley No.8642 y el Código de Normas y Procedimientos Tributarios.

**Gráfico #7**




**Fuente: Anexo 5- Cuestionario para ingenieros informáticos con énfasis en delitos informáticos**

El gráfico anterior fue aplicado a dos especialistas en delitos informáticos, en donde se observa que al consultarles sobre si la legislación costarricense está preparada para afrontar la incorporación de IoT, se tiene un 50% que indica que no y un 50% que indica que si, por lo tanto, se les consultó el porqué de tales respuestas para fundamentar ambas posiciones.

Las respuestas se analizarán en la siguiente tabla:

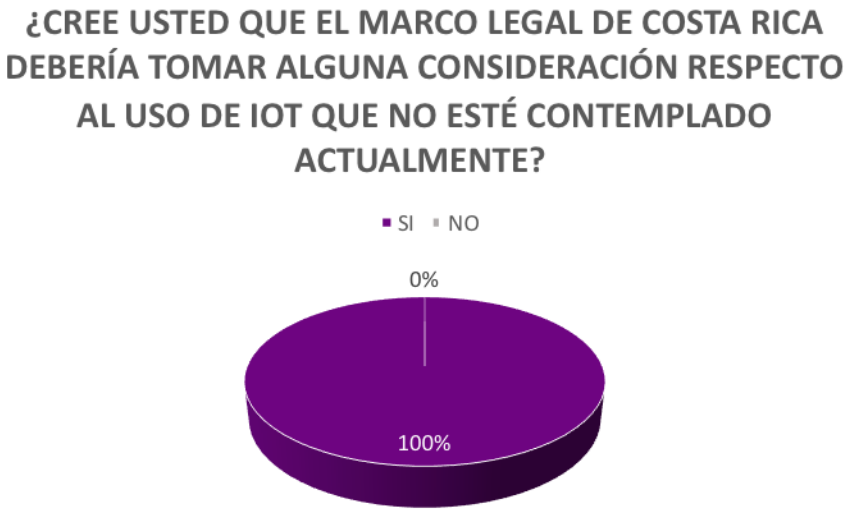
***Respuesta abierta en el cuestionario aplicado a los ingenieros informáticos con énfasis en delitos informáticos***

***Respuesta #1:*** *Algunos artículos hacen referencia específica a ciertos tipos de crímenes en plataformas específicas. Sin embargo, puede ser fácil de subsanar para quitar definiciones como computador o red para indicar tecnología que sirva para procesar, almacenar o distribuir información.*

***Respuesta #2:*** *Actualmente sí, aunque debe seguirse actualizando, el marco normativo se actualizó a lo interno (nuestro código penal) y a nivel de colaboración internacional al aprobarse la Convención de Ciberdelincuencia terminó de reforzar el marco legal para poder perseguir de manera más efectiva estos delitos, máxime que trascienden fronteras, dicha afirmación se refuerza con los informes internacionales del estado de la ciberseguridad en el país que indican que nuestro punto fuerte está en la legislación sobre delitos informáticos.*

**Fuente: Anexo 5- Cuestionario para ingenieros informáticos con énfasis en delitos informáticos**

**Gráfico #8**




**Fuente: Anexo 5- Cuestionario para ingenieros informáticos con énfasis en delitos informáticos**

Con base en la información anterior se evaluó una posible restructuración del marco legal actual con el fin de contemplar el uso de IoT que aún no esté siendo tomado en cuenta y la población consideró al 100% estar en completo acuerdo.

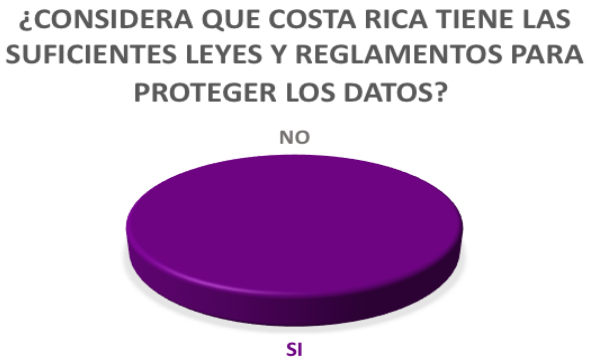
**Gráfico #9**




**Fuente: Anexo 5- Cuestionario para ingenieros informáticos con énfasis en delitos informáticos**

Con base en la pregunta anterior se puede observar que el 50% de la población indica que, sí se tienen los mecanismos para velar por cumplimiento de las leyes referente a delitos informáticos, mientras que el 50% indica que no.

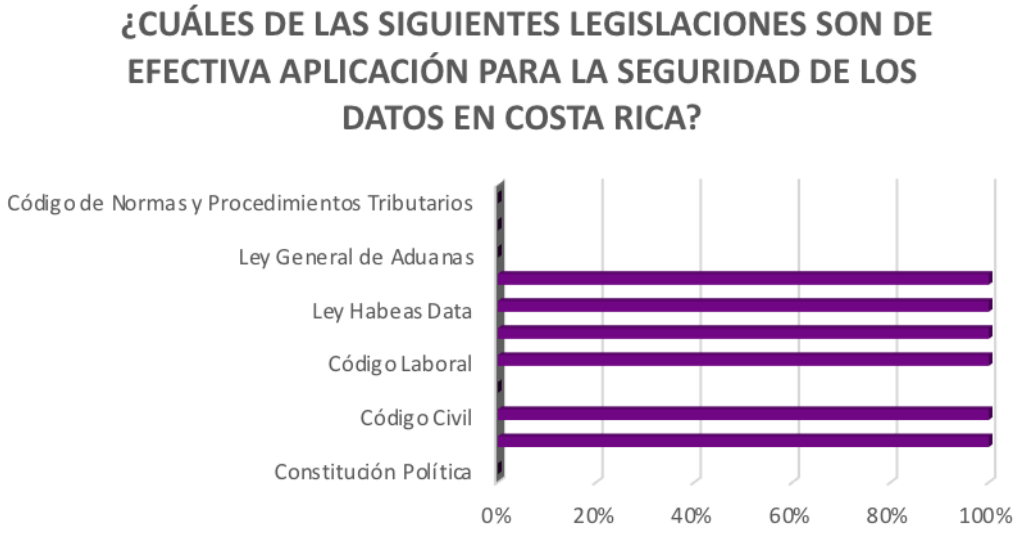
**Gráfico #10**




**Fuente: Anexo 6-Cuestionario para investigador del OIJ**

De acuerdo con la información anterior, se observa que la población sí está de acuerdo con el 100% de que Costa Rica tiene las suficientes leyes y reglamentos para proteger los datos.

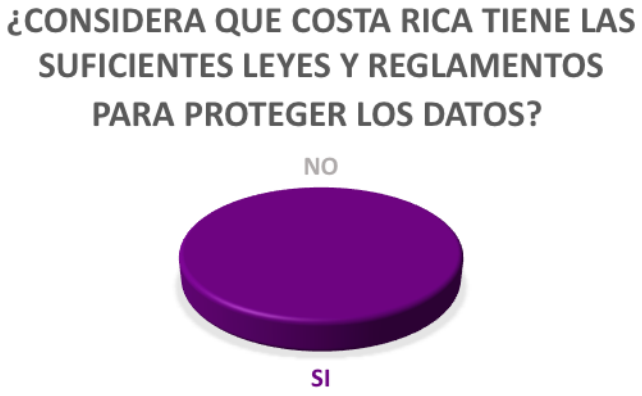
**Gráfico #11**




**Fuente: Anexo 6-Cuestionario para investigador del OIJ**

Al consultarle a un investigador del OIJ sobre las legislaciones de efectiva aplicación para la seguridad de los datos en Costa Rica, indicó conocer la Ley No.8642, la Ley Habeas Data, Ley No.8968, el Código Laboral, Civil y Penal.

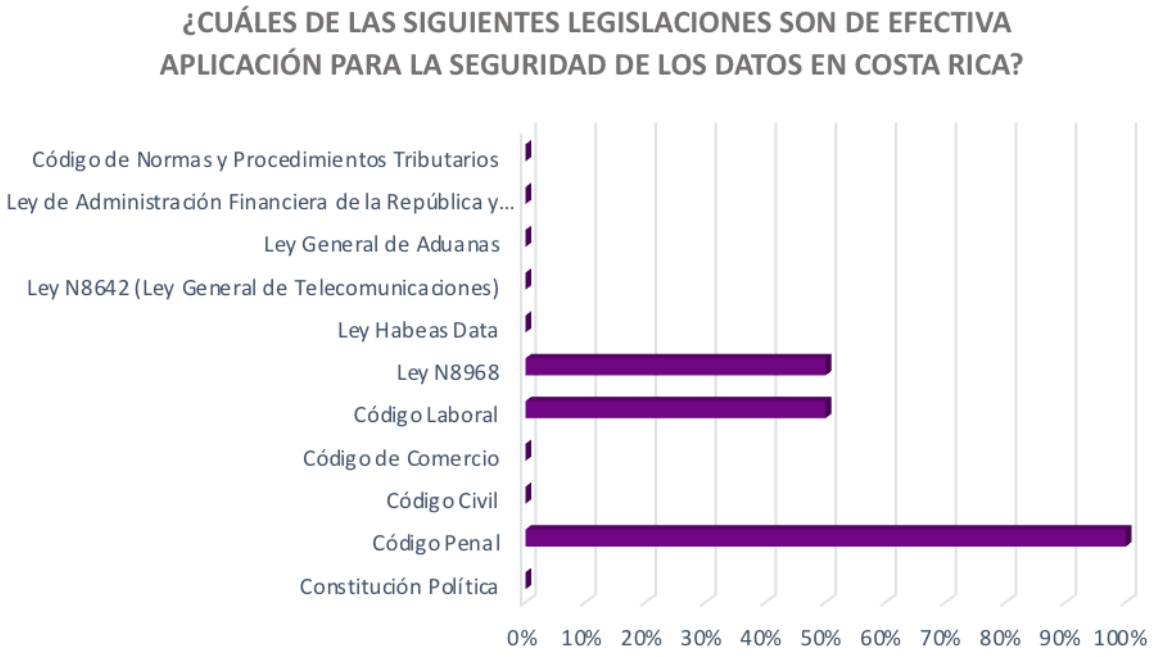
**Gráfico #12**




**Fuente: Anexo 7- Cuestionario para investigadores privados**

Al consultarle sobre si considera que Costa Rica tiene las suficientes leyes y reglamentos para poder proteger los datos, se observa que el 100% de los sujetos indicó que sí.

**Gráfico #13**




**Fuente: Anexo 7- Cuestionario para investigadores privados**

Al igual que muestras anteriores, se les consultó cuáles legislaciones son de efectiva aplicación para la seguridad de los datos, por lo tanto, se obtiene que un 50% indica conocer la Ley No.8968 y el Código Laboral, por otra parte, el 100% indicó que el Código Penal es efectivo para la seguridad de los datos.

### 5.1.2 Análisis de la Variable #2

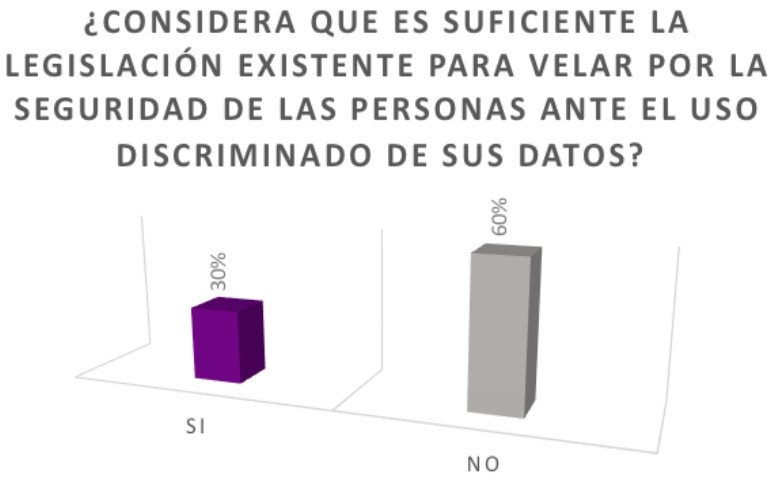
**Repercusiones en la seguridad y privacidad de los datos.**

Hace referencia a la dimensión que tienen todas aquellas repercusiones en la seguridad y la privacidad de los datos, impactando a las personas y a las empresas.

**Objetivo analizado:**

Evaluar la efectiva aplicación de la legislación costarricense en el desarrollo de proyectos IoT para dimensionar sus repercusiones en la seguridad y privacidad de los datos.

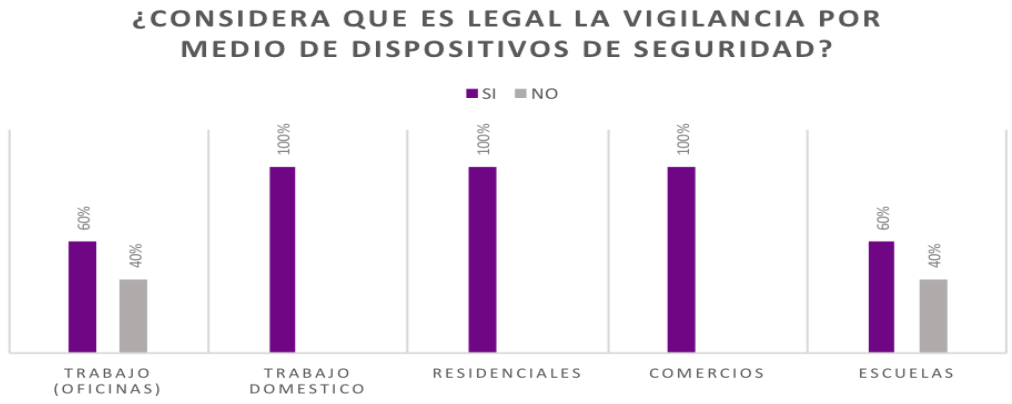
**Gráfico #14**




**Fuente: Anexo 1-Cuestionario para abogados**

El gráfico anterior evalúa si la legislación actual es suficiente para velar por la seguridad de las personas ante el uso discriminado de los datos, dicho cuestionario fue aplicado a los abogados, el 60% indican que esta no es suficiente y solamente un 30% indicó lo contrario.

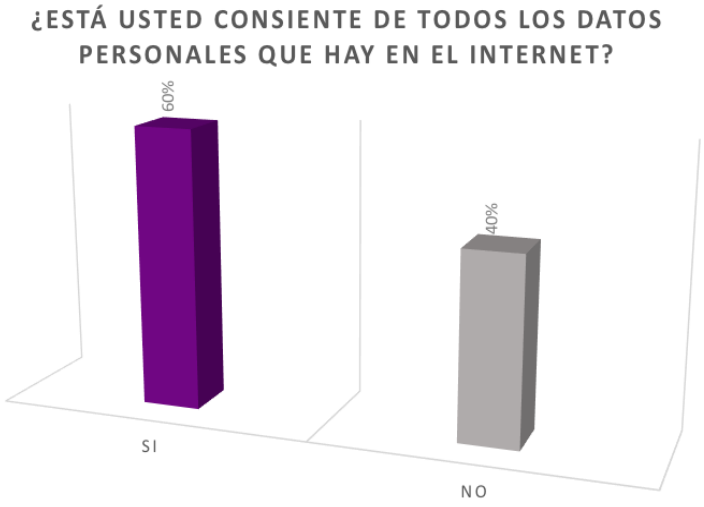
**Gráfico #15**




**Fuente: Anexo 1-Cuestionario para abogados**

De acuerdo con la información obtenida en el gráfico anterior, es importante destacar que el 100% de los abogados opinan que sí es legal la vigilancia por medio de dispositivos de seguridad en los trabajos domésticos, residenciales y comercios, sin embargo, solamente un 60% de los mismos están de acuerdo con que suceda lo mismo en los trabajos de oficina y en las escuelas.

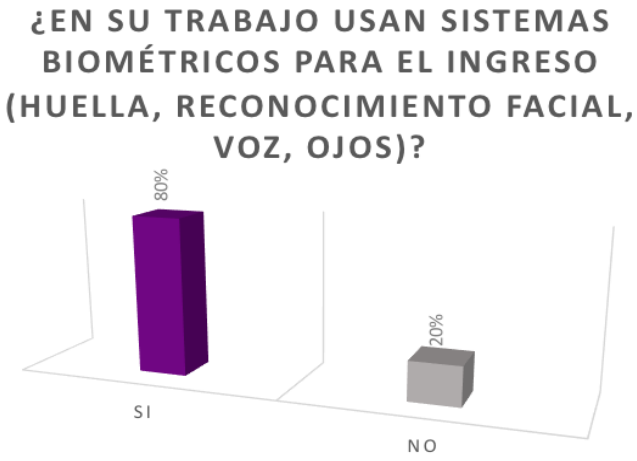
**Gráfico #16**




**Fuente: Anexo 2-Cuestionario para usuarios**

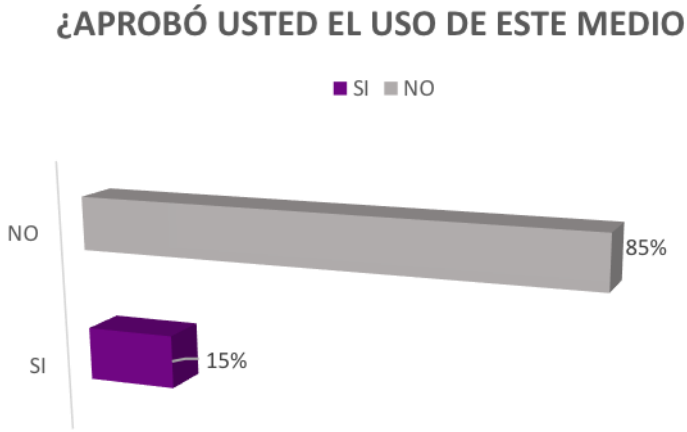
El gráfico anterior demuestra que solamente el 60% de los civiles se encuentran conscientes de los datos personales que hay en el Internet y un 60% indicó desconocer sobre los datos expuestos.

**Gráfico #17**




**Fuente: Anexo 2-Cuestionario para usuarios**

**Gráfico #18**




**Fuente: Anexo 2-Cuestionario para usuarios**

De acuerdo con los gráficos anteriores, se puede observar que las empresas están implementando tecnología para ingresar, por lo tanto, un 80% de la muestra indicó que usan sistemas biométricos en las empresas. Sin embargo, en el Gráfico #16 solamente un 15% aprobó este medio, demostrando que un 85% depende de lo que la empresa quiera incorporar.

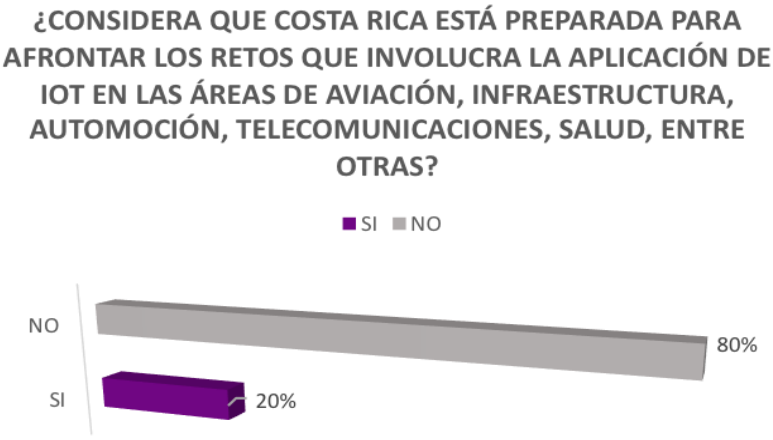
**Gráfico #19**




**Fuente: Anexo 3- Cuestionario para ingenieros especialistas en ciberseguridad**

El gráfico anterior evalúa qué tan protegida está la ciudadanía costarricense a nivel legal en casos de acoso, robos o violación de la privacidad y el resultado demuestra que un 80% de los especialistas en ciberseguridad no consideran que no está protegida.

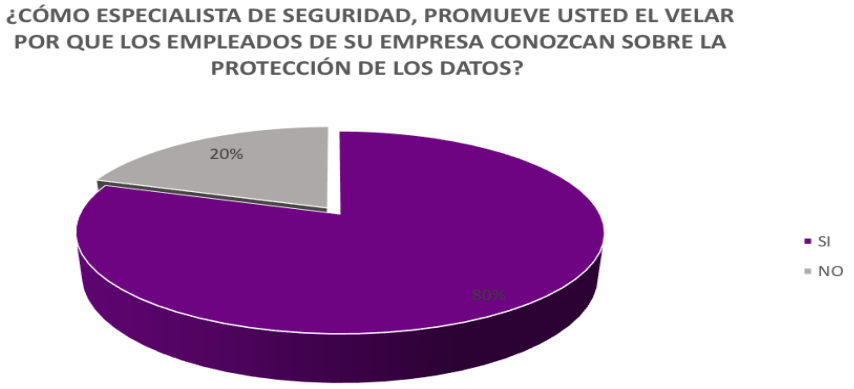
**Gráfico #20**




**Fuente: Anexo 3- Cuestionario para ingenieros especialistas en ciberseguridad**

En el gráfico anterior se les consultó a los especialistas de seguridad si consideran que Costa Rica está preparada para afrontar el reto de IoT en diferente áreas y el 80% de la población indicó que no, mientras que solamente un 20% consideró que sí.

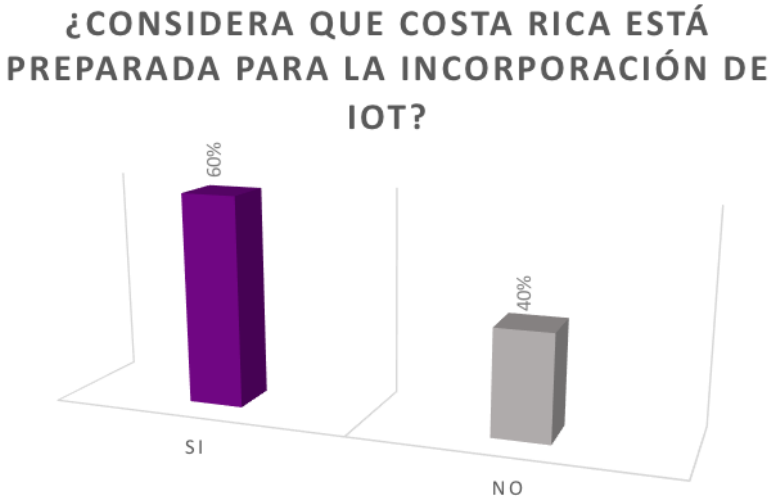
**Gráfico #21**




**Fuente: Anexo 3- Cuestionario para ingenieros especialistas en ciberseguridad**

En el gráfico anterior se les consultó a los especialistas de seguridad si promueven el conocimiento sobre la protección de los datos personales y un 80% de la población indicó que si lo hace mientras que un 20% indicó que no.

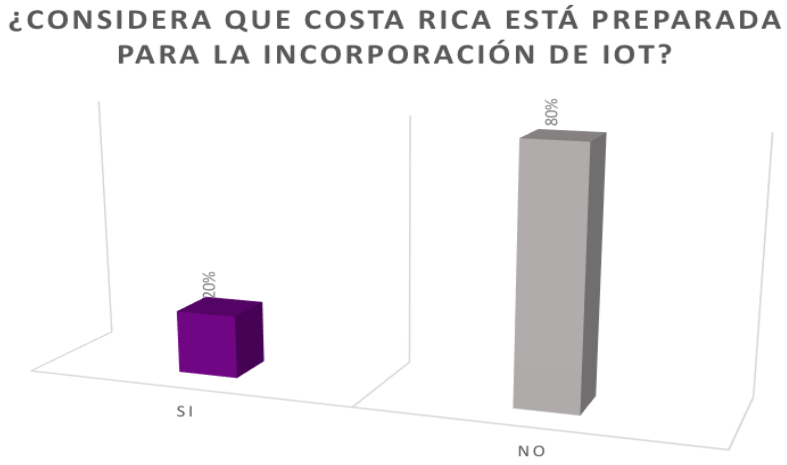
**Gráfico #22**




**Anexo 4 – Cuestionario para IT/Privado**

Con base en la información antes suministrada, un 60% de los ingenieros de IT en empresas privadas indicó que Costa Rica sí está preparada para la incorporación de IoT mientras que un 30% opinó lo contrario.

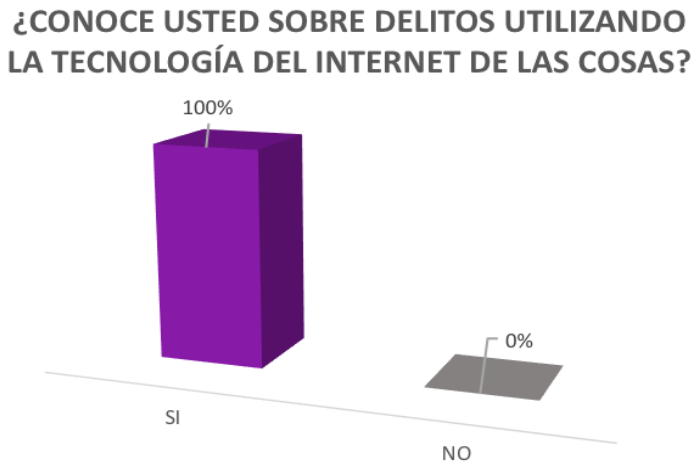
**Gráfico #23**




**Anexo 4 – Cuestionario para IT/Publica**

El gráfico anterior evalúa la respuesta de ingenieros de IT en empresas públicas con base en la incorporación de IoT en Costa Rica y un 80% de los mismos indicó que el país no está preparado para este proyecto mientras que un 20% indicó lo contrario.

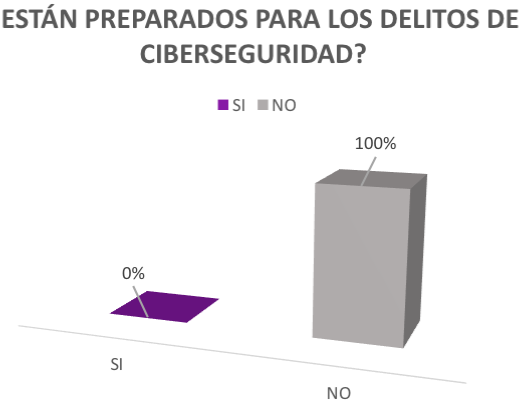
**Gráfico #24**




**Fuente: Anexo 6-Cuestionario para investigador del OIJ**

En el gráfico anterior se le consultó a un investigador del OIJ sobre si conocía delitos utilizando la tecnología del IoT y el mismo indicó que Sí.

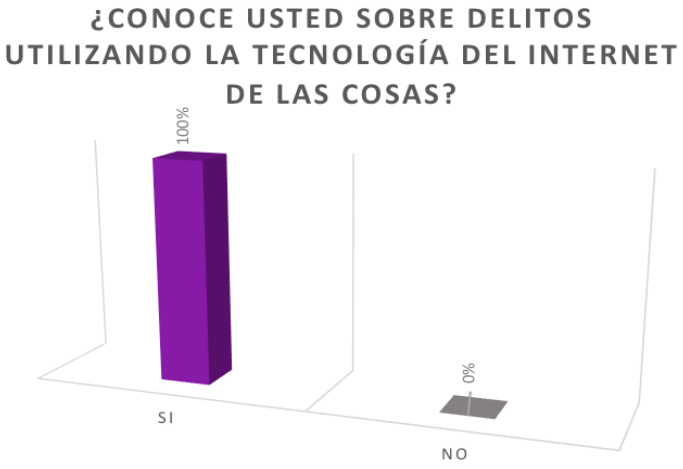
**Gráfico #25**




**Fuente: Anexo 6-Cuestionario para investigador del OIJ**

Al consultarle al investigador del OIJ sobre si están preparados para los delitos de ciberseguridad se puede observar que el resultado equivale a un 100% en la respuesta de No.

**Gráfico #26**




**Fuente: Anexo 7- Cuestionario para investigadores privados**

El gráfico anterior evalúa los investigadores privados, por lo tanto, al consultarles sobre si conocen delitos utilizando la tecnología de IoT, estos, indican que sí en un 100% de la población.

**Gráfico #27**




**Fuente: Anexo 7- Cuestionario para investigadores privados**

Al observar el gráfico anterior con base en si están preparados para afrontar los delitos de ciberseguridad, los investigadores privados indicaron en un 100% que no lo están.

### 5.1.3 Análisis de la Variable #3

**Los riesgos que implican la incorporación de IoT y las acciones que afectan la privacidad de los datos.**

Con base en esta variable, se establecen todos aquellos riesgos que implican la incorporación de IoT y las acciones que afectan la privacidad de los datos.

**Objetivo analizado:**

Establecer los riesgos que implican la incorporación de IoT y las acciones que afectan la privacidad de los datos.

**Gráfico #28**




**Fuente: Anexo 1-Cuestionario para abogados**

El gráfico anterior evaluó a los abogados con base en todas aquellas propiedades que se violentan cuando se hacen mal uso de la información, es por ello por lo que se puede observar que un 100% de la población indicó que se violenta la

propiedad intelectual y financiera, le sigue en un 80% el honor y acoso y en un 0% la estafa.

**Tabla #1**

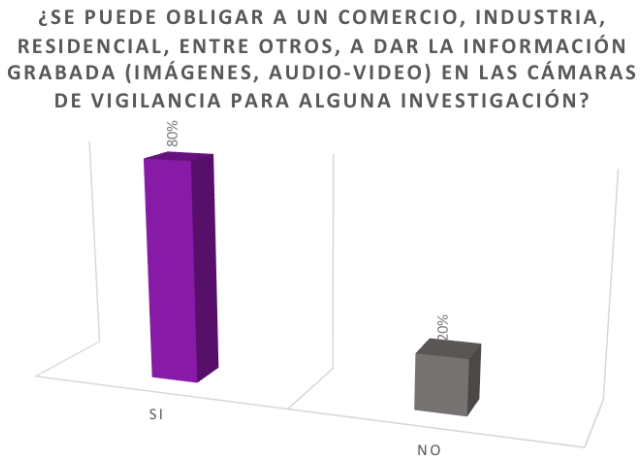
*¿Conoce usted casos en que la misma seguridad se convierte en una potencial amenaza ante: delincuencia, denuncias, pedofilia, violencia sexual, violencia doméstica, entre otros? Coméntelo a continuación de lo contrario ponga NO y continúe a la siguiente pregunta*

| *Sujeto* | Respuesta |
|---|---|
| *1* | No |
| *2* | Sí. Respecto a un centro comercial donde se transgredió el sistema de seguridad informático para cometer un robo en horas de la madrugada. |
| *3* | Sí. Una clienta realizo la demanda hacia su esposo debido a que el vehículo se encontraba completamente monitoreado con micrófonos, cámara y GPS. |
| *4* | No |
| *5* | No |

**Fuente: Anexo 1-Cuestionario para abogados**

Con base en la tabla anterior, se les preguntó a los abogados si conocían sobre casos en donde la seguridad se convierte en una amenaza, por lo tanto, solo dos de los abogados contestaron conocer y ambos se relacionan con dispositivos IoT.

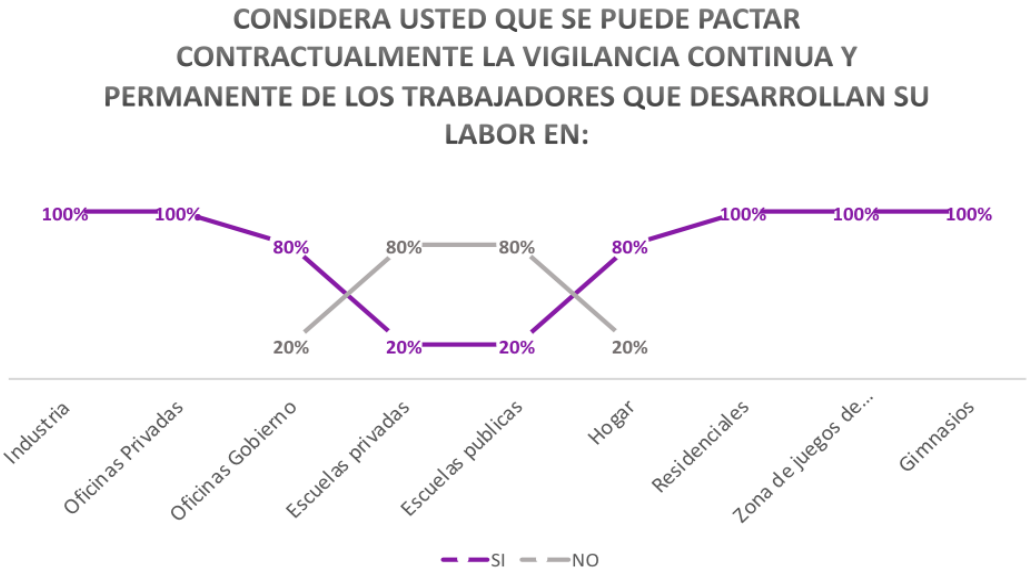
**Gráfico #29**




**Fuente: Anexo 1-Cuestionario para abogados**

De acuerdo con la pregunta ante evaluada el 80% de los abogados indica que sí se puede obligar a un comercio, industria, residencial, entre otros, a dar la información grabada, mientras que un 20% indicó que no se puede obligar.

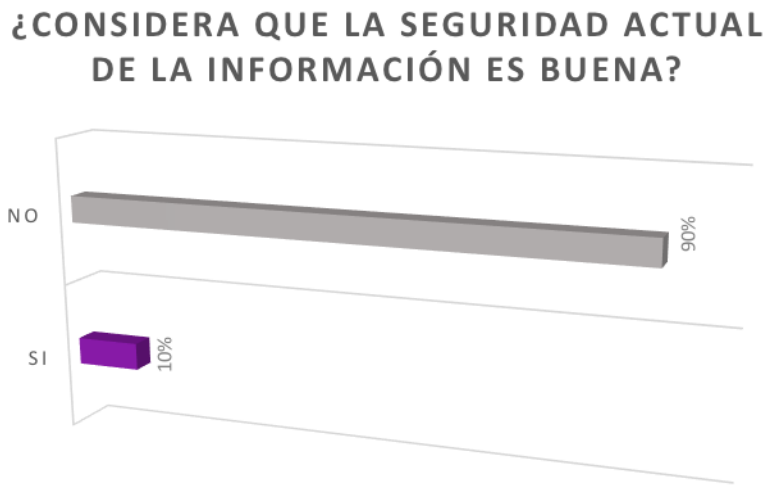
**Gráfico #30**




**Fuente: Anexo 1-Cuestionario para abogados**

Al evaluar la información antes observada los abogados opinan en un 100% que se puede pactar tener vigilancia continua en la industria, oficinas privadas, residenciales, zonas de juego y gimnasios, mientras que solo un 80% indica estar de acuerdo con que se vigilen las escuelas, hogar y oficinas de gobierno.

**Gráfico #31**




**Fuente: Anexo 2-Cuestionario para usuarios**

El gráfico anterior y la tabla #2 evalúan si la seguridad actual es buena, la cual fue aplicada en el cuestionario de los usuarios y un 90% de la población indicó que No la consideran buena, en la Tabla#2 se evalúa por qué no la considera buena y la mayoría indicó que la exposición de los datos personales es el mayor problema.

**Tabla #2**

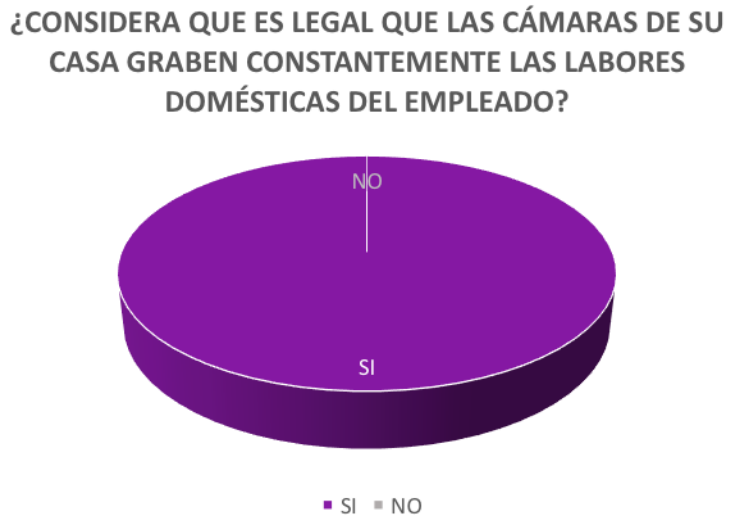
Respuestas abiertas:

| *Sujeto* | *¿Por qué considera que No es buena la seguridad de la información?* |
|---|---|
| *1* | Ahora con tantas páginas de internet nuestra información está expuesta ya sea por pagos por internet, claves, información personal. |
| *2* | Porque mientras se esté conectado a una red hay vulnerabilidad o riesgo en cuanto a información, fraudes y demás. Aunque haya muchos métodos de seguridad no me siento confiada. |
| *3* | Se filtra mucha información personal por ejemplo las cuentas bancarias y núm. de teléfono |
| *4* | En apariencia es bastante vulnerable o tiene muchos bugs |
| *5* | Para ser una herramienta de uso continuo y exhaustivo no se leen noticias de forma continua que mencionen problemas de seguridad. Personalmente desde el 2000 uso internet y sólo un par de veces he tenido problemas con el fishing. |
| *6* | No hay una certeza del control total de la misma información en cada uno de los rincones de las áreas informáticas. Por ello los delitos cibernéticos son tan frecuentes. |
| *7* | Por el hecho de que el Internet de las cosas es un arma de doble filo ya que puede brindar facilidades y seguridad en la vida cotidiana, pero a la vez puede dar acceso a delincuentes y hacker si no se custodian con cuidado las claves de acceso. |

| | |
|---|---|
| *8* | El Internet está en constante evolución y los delincuentes cibernéticos no descansan y pasan estudiando las vulnerabilidades de los sistemas para atacarlos, robar información e implantar virus, entre otras cosas. |
| *9* | Porque me he dado cuenta de amigos a los cuales les han robado dinero de cuentas en Bancos Nacionales muy importante a través de Internet y luego de la investigación por parte de la justicia estas personas delincuentes están internas en centros penales. |

**Fuente: Anexo 2-Cuestionario para usuarios**

**Gráfico #32**




**Fuente: Anexo 2-Cuestionario para usuarios**

En el gráfico anterior se puede observar que el 100% indicó que sí consideran legal que las cámaras que se encuentran en la casa graben constantemente las labores domésticas del empleado.

**Gráfico #33**




**Fuente: Anexo 2-Cuestionario para usuarios**

De acuerdo con el gráfico anterior un 90% indicó que, sí les usarían un *smartwatch* a los hijos/as con localización, mientras que un 10% indicó que No.

**Gráfico #34**




**Fuente: Anexo 3- Cuestionario para ingenieros especialistas en ciberseguridad**

Cabe destacar que el gráfico anterior demuestra la opinión de los ingenieros especialistas en ciberseguridad en donde el 100% está de acuerdo en que la incorporación de IoT involucra un reto mayor para el monitoreo constante ante amenazas.

**Gráfico #35**

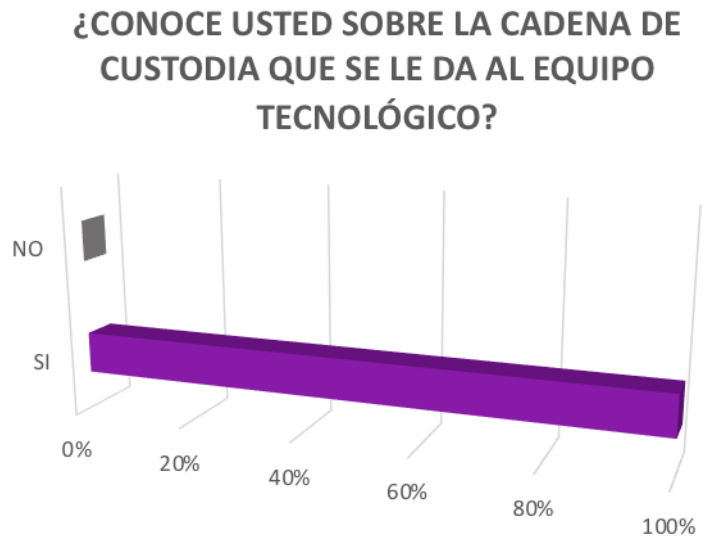
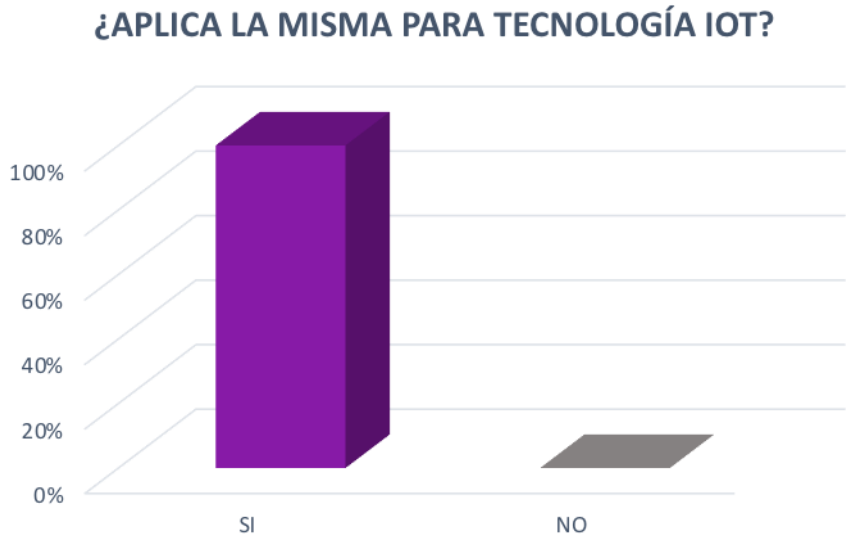



**Gráfico #36**




**Fuente: Anexo 6-Cuestionario para investigador del OIJ**

Los dos gráficos anteriores aplicados al investigador del OIJ demuestran que sí se conoce sobre la cadena de custodia de los equipos tecnológicos y que además indica en un 100% que es el mismo procedimiento en caso de dispositivos de IoT.

**Gráfico #37**

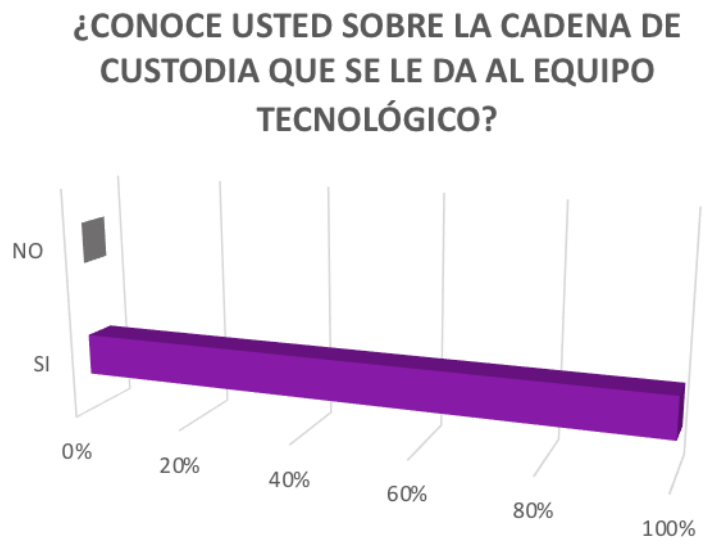
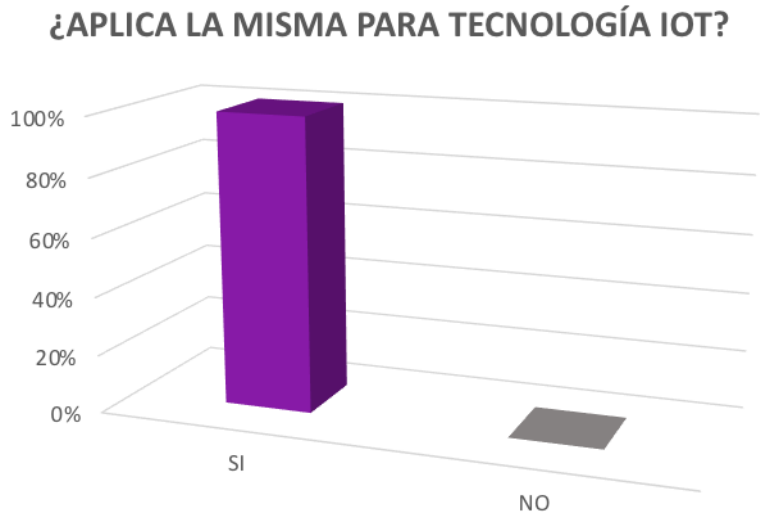


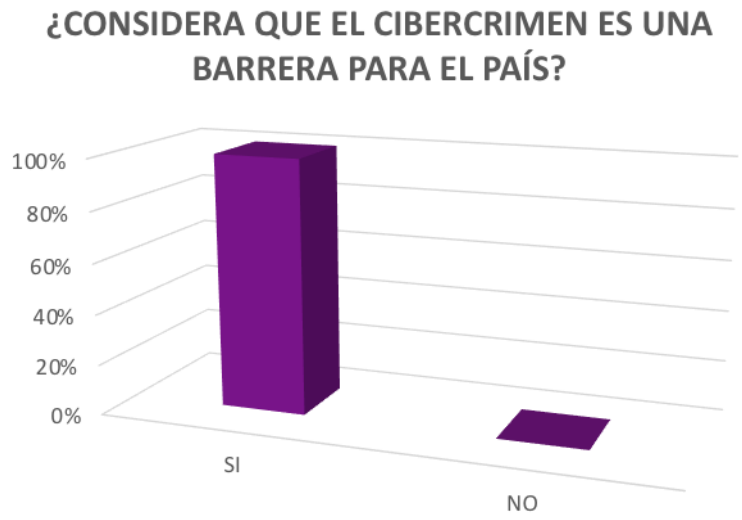

**Gráfico #38**




**Fuente: Anexo 7- Cuestionario para investigadores privados**

Ambos gráficos evalúan las respuestas de los investigadores privados y el 100% indica que si conocen de la cadena de custodia y además el 100% de igual forma indicó que se aplica la misma para dispositivos IoT.

**Gráfico #39**




**Fuente: Anexo 6-Cuestionario para investigador del OIJ**

Al analizar el gráfico anterior cuya pregunta fue aplicada al investigador del OIJ, indica en un 100% que el cibercrimen sí es una barrera para el país.

### 5.1.4 Análisis de la Variable #4

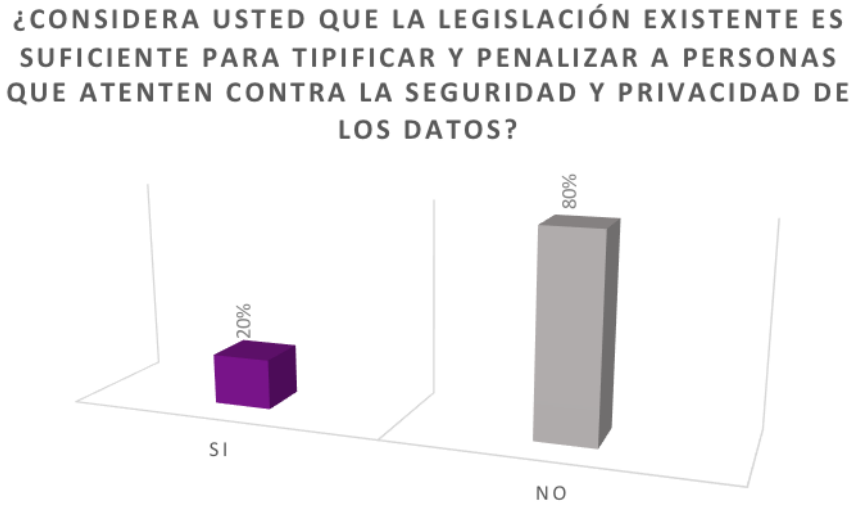
**Las leyes y reglamentos en Costa Rica protegen la seguridad y privacidad de la información.**

Esta variable se encarga de determinar cuáles leyes y reglamentos en Costa Rica protegen la seguridad y privacidad de la información.

**Objetivo analizado:**

Determinar cuáles leyes y reglamentos en Costa Rica protege la seguridad y privacidad de la información.

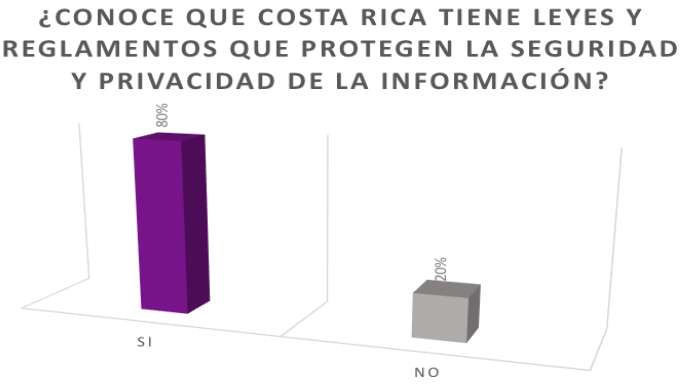
**Gráfico #40**




**Fuente: Anexo 1-Cuestionario para abogados**

En el gráfico se puede observar que el 80% de los abogados indicó que la legislación existente no es suficiente para tipificar y penalizar personas que atentan contra la seguridad y privacidad de los datos, mientras que solo un 20% indicó lo contrario.

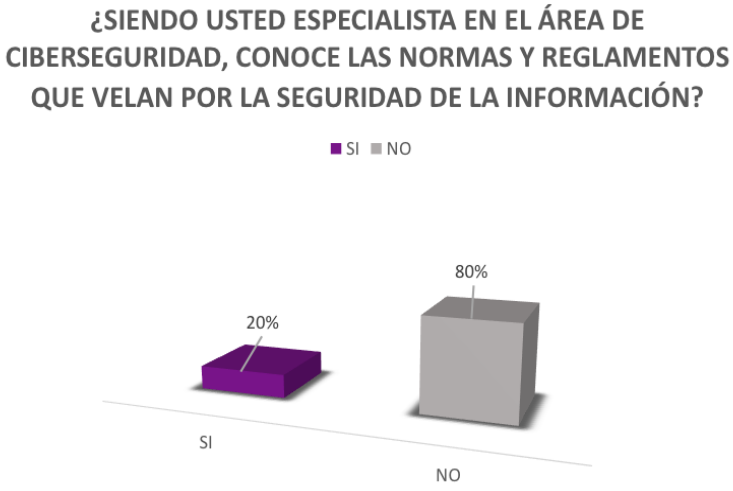
**Gráfico #41**




**Fuente: Anexo 2-Cuestionario para usuarios**

En el gráfico anterior un 80% de los usuarios dicen que sí conocen que Costa Rica tiene leyes y reglamentos que protegen la seguridad y privacidad de la información, sin embargo, hay un 20% que desconoce del tema.

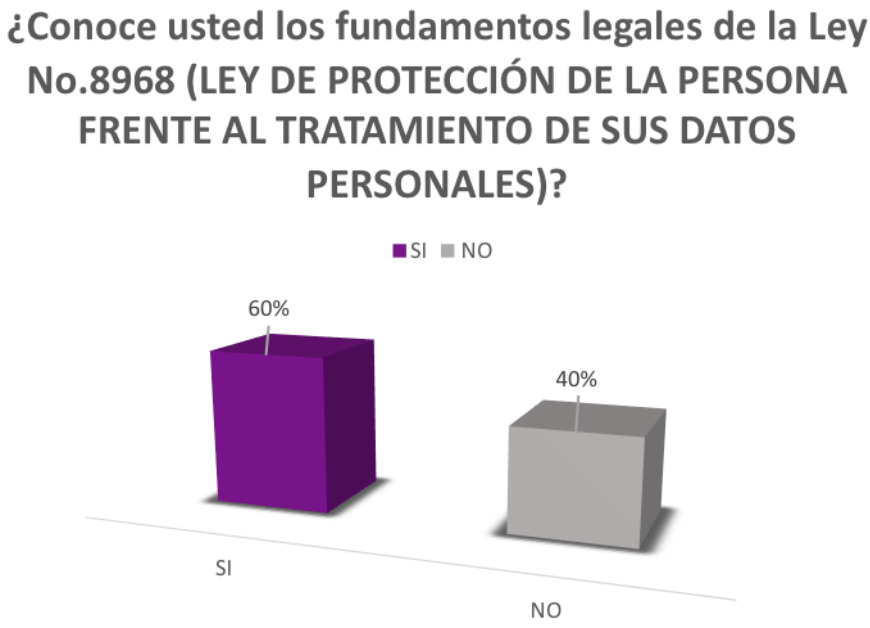
**Gráfico #42**




**Fuente: Anexo 3- Cuestionario para ingenieros especialistas en ciberseguridad**

Se puede observar que existe un 80% de los especialistas en Ciberseguridad que dicen no conocer las normas y reglamentos que velan por la seguridad de la información, mientras que solo un 20% sí conoce de las mismas.

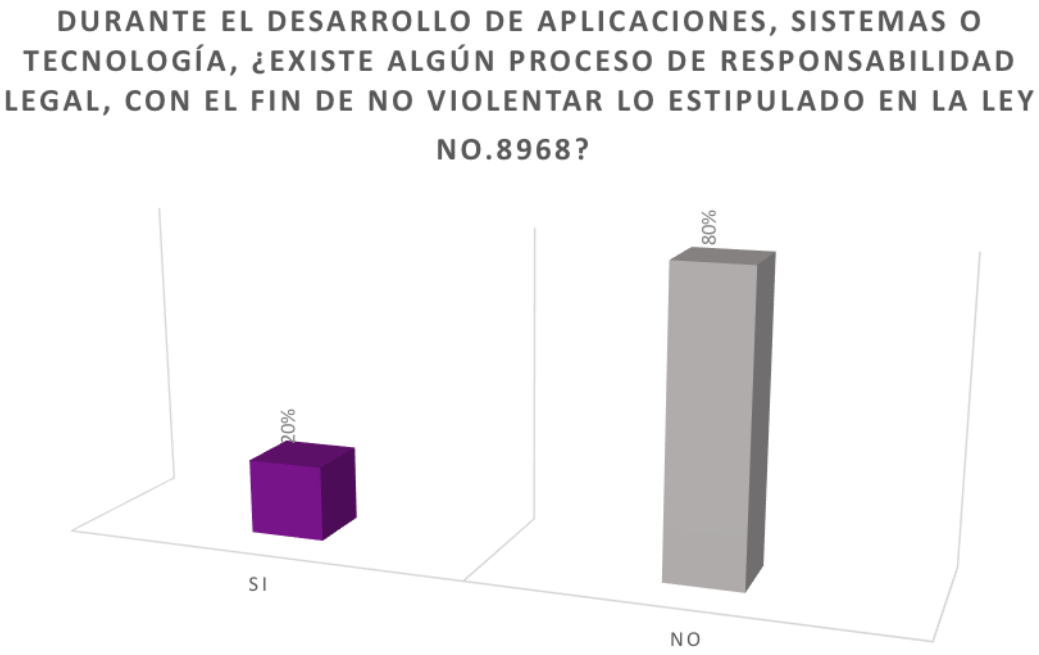
**Gráfico #43**




**Fuente: Anexo 3- Cuestionario para ingenieros especialistas en ciberseguridad**

Al consultar sobre el conocimiento de la ley No.8968, un 60% de los especialistas conoce sobre los fundamentos de esta mientras que un 40% indicó no conocerlos.

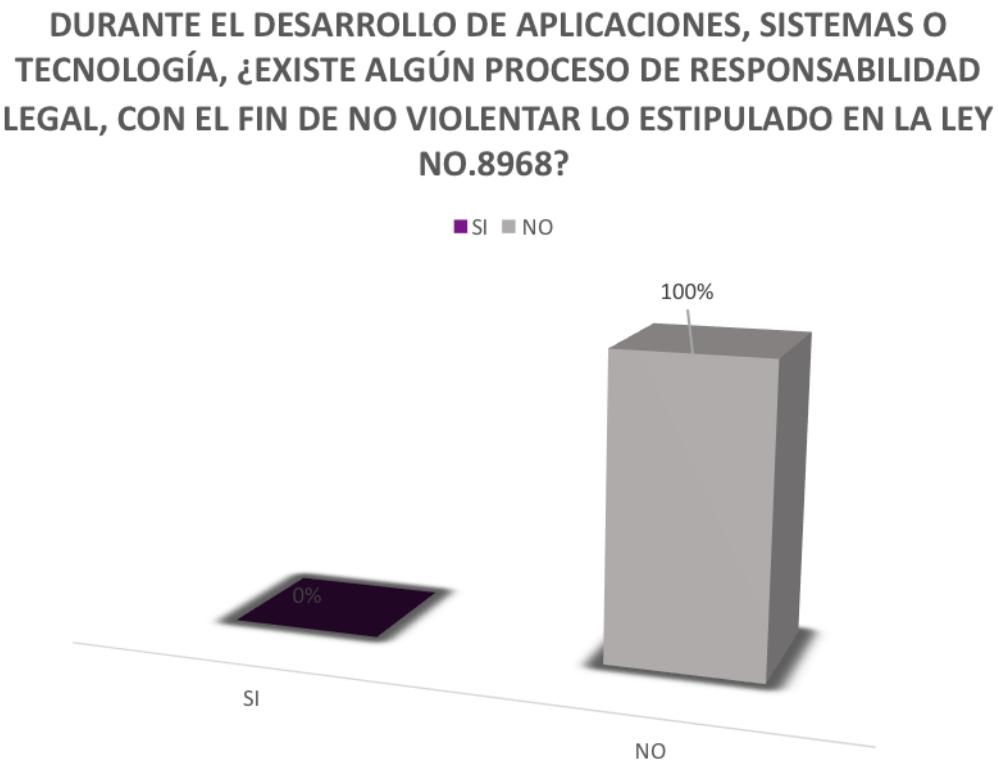
**Gráfico #44**




**Anexo 4 – Cuestionario para IT/Privado**

En el gráfico anterior se puede observar que el 80% de los ingenieros de IT en empresa privada no tienen ningún proceso de responsabilidad legal con el fin de no violentar lo estipulado en la ley No.8968, únicamente un 20% indicó tener un proceso relacionado con esto.

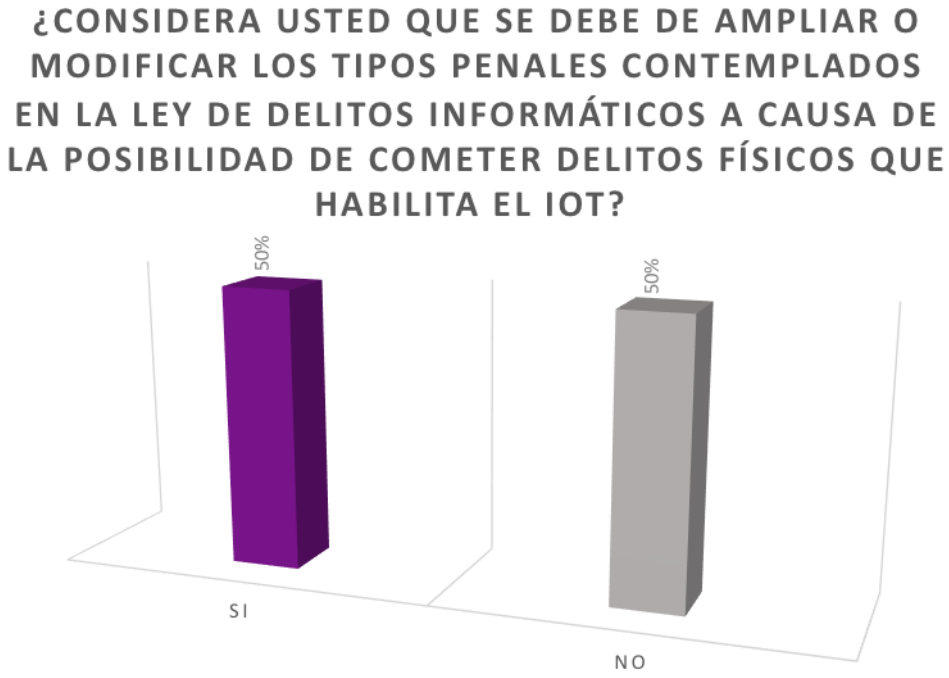
**Gráfico #45**




**Anexo 4 – Cuestionario para IT/Publica**

En el gráfico antes mencionado se puede observar que el 100% de los ingenieros de IT de empresas públicas no realizan ningún proceso de responsabilidad legal alineado con la Ley 8968.

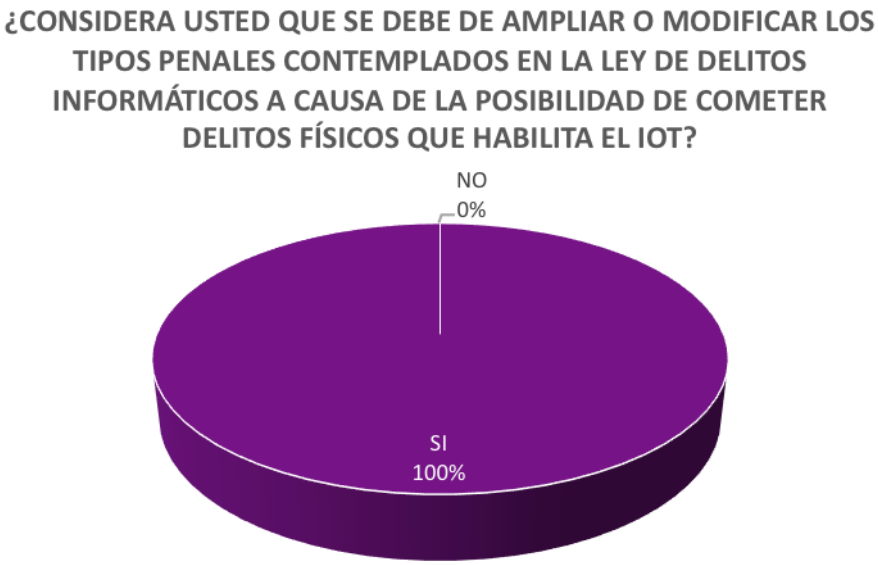
**Gráfico #46**




**Fuente: Anexo 5- Cuestionario para ingenieros informáticos con énfasis en delitos informáticos**

El gráfico anterior demuestra las respuestas de 2 expertos en informática con énfasis en delitos informáticos, sin embargo, al consultarles sobre si se debe ampliar o modificar los tipos penales contemplados en la ley de delitos informáticos a causa de la posibilidad de cometer delitos físicos que habilita el IoT, se obtuvo una respuesta 50/50.

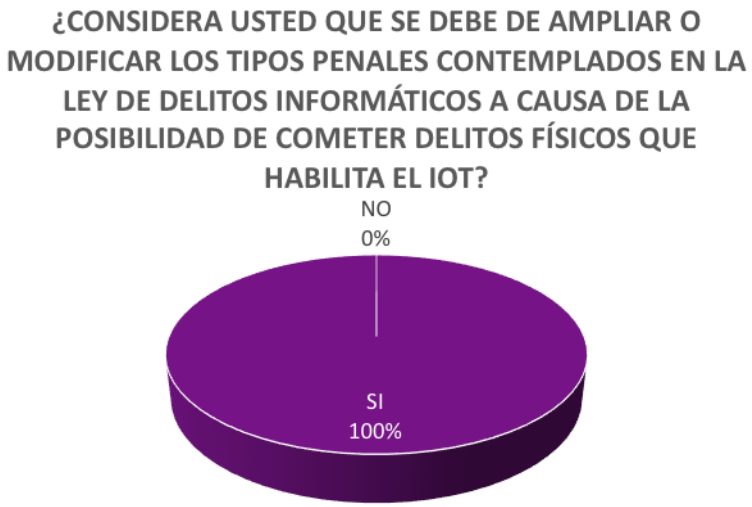
**Gráfico #47**




**Fuente: Anexo 6-Cuestionario para investigador del OIJ**

En el gráfico anterior el investigador del OIJ indicó en un 100% que sí se debe de ampliar o modificar los tipos penales contemplados en la Ley de Delitos Informáticos a causa de posibilidad de cometer delitos físicos producto de la tecnología IoT.

**Gráfico #48**




**Fuente: Anexo 7- Cuestionario para investigadores privados**

En el gráfico antes en mención, se puede observar un 100% de los investigadores privados indicaron que sí se debe de ampliar o modificar los tipos penales contemplados en la Ley de Delitos Informáticos a causa de posibilidad de cometer delitos físicos producto de la tecnología IoT.

### 5.1.5 Análisis de la Variable #5

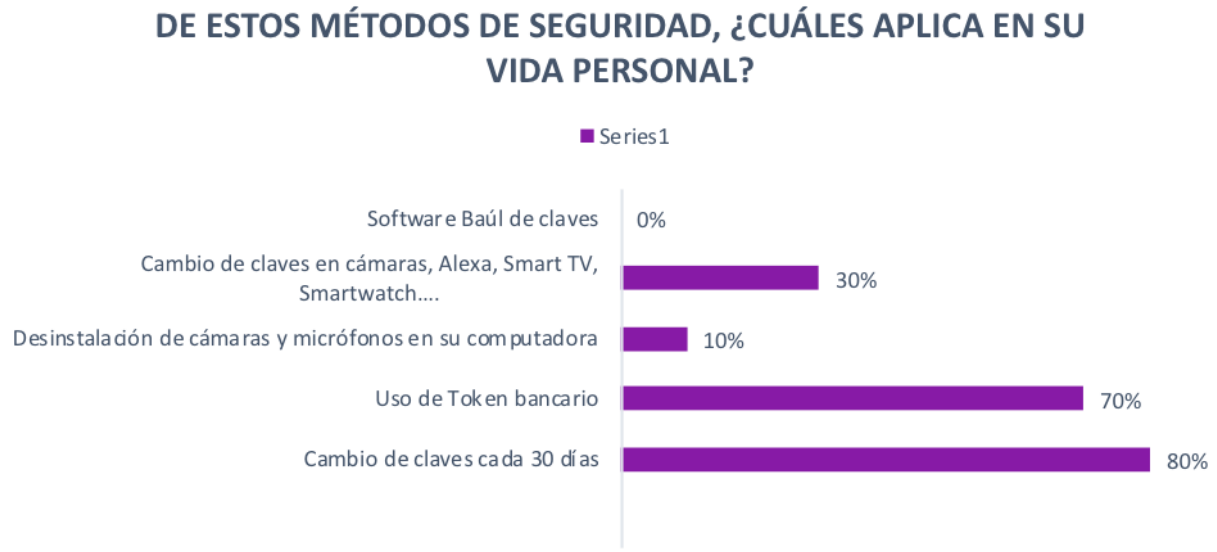
**Los agujeros de seguridad en los dispositivos que conformarán la gran red de IoT.**

Esta variable evalúa todos aquellos agujeros de seguridad que son parte de la incorporación de IoT en Costa Rica.

**Objetivo analizado:**

Evaluar los agujeros de seguridad en los dispositivos que conformarán la gran red de IoT.

**Gráfico #49**

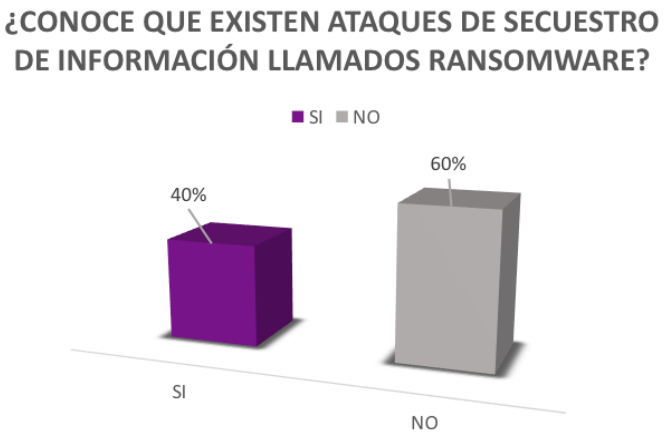



**Fuente: Anexo 2-Cuestionario para usuarios**

En el gráfico anterior se puede observar la opinión de los usuarios con base en los métodos de seguridad, por lo tanto, se obtiene que el 80% de la población cambia las claves cada 30 días, un 70% utilizan Token bancario, un 30% cambia las claves de

dispositivos como cámaras, Alexa, Smart TV, smartwatch, un 10% desinstala cámaras y micrófonos de las computadoras y un 0% de la población utiliza baúles de claves.

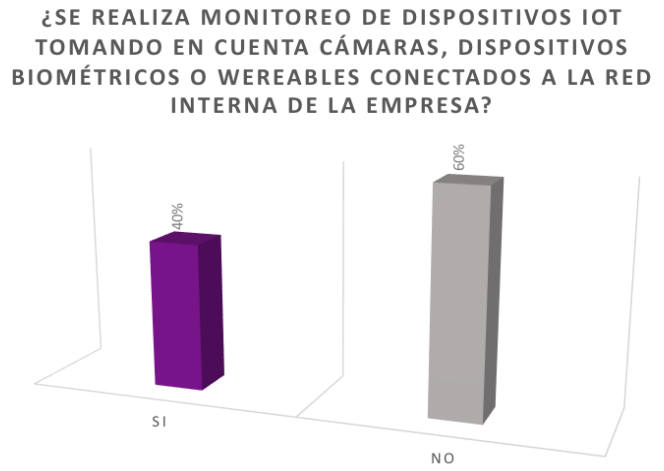
**Gráfico #50**




**Fuente: Anexo 2-Cuestionario para usuarios**

En el gráfico anterior se puede observar que solo un 40% de los usuarios conocen sobre los *ransomware* o ataques de secuestro de información, mientras que el 60% restante indicó no conocerlos.

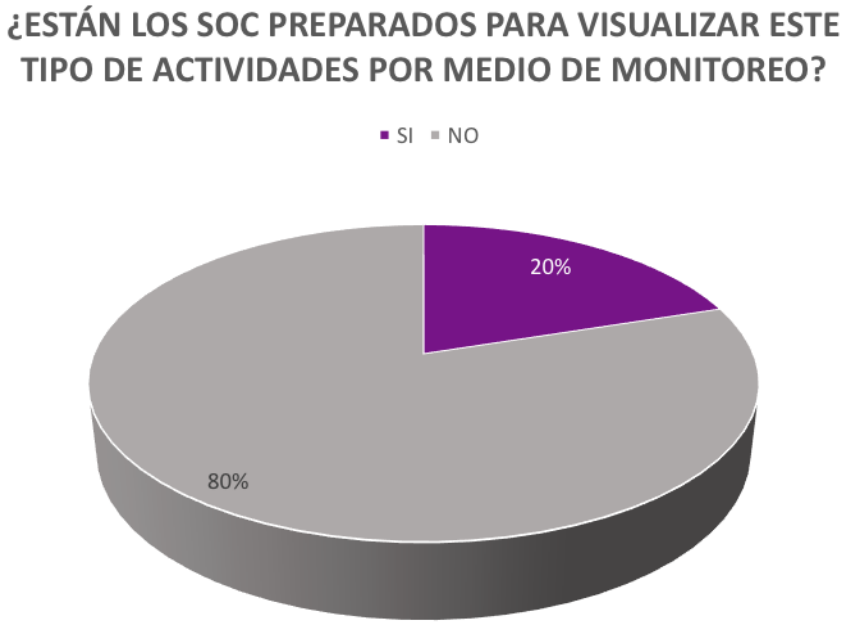
**Gráfico #51**




**Fuente: Anexo 3- Cuestionario para ingenieros especialistas en ciberseguridad**

La información antes evaluada proviene de los especialistas en ciberseguridad, en donde un 60% de los mismos indico que no se realizan monitoreo constantes de dispositivos IoT que utilizan la red interna de la empresa, mientras un 40% indicó que sí lo realizan.

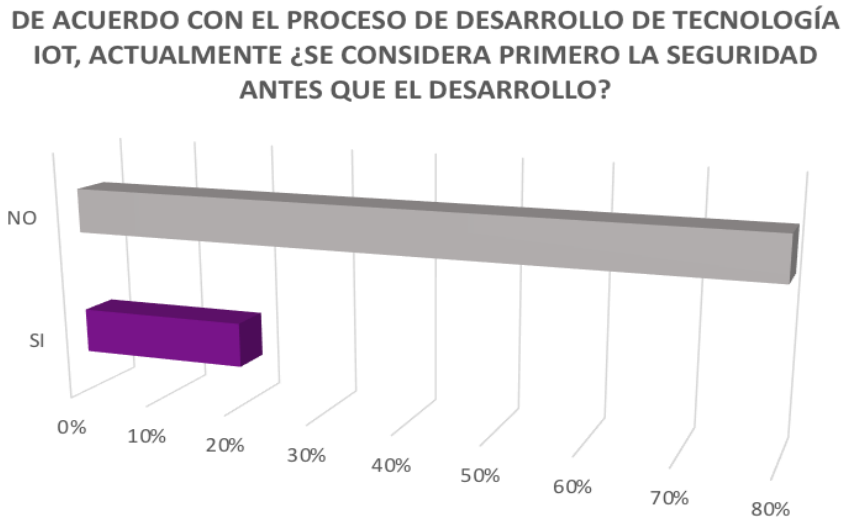
**Gráfico #52**




**Fuente: Anexo 3- Cuestionario para ingenieros especialistas en ciberseguridad**

En el gráfico anterior indica que un 80% de los especialistas en ciberseguridad indican que los SOC no están preparados para visualizar actividad proveniente de IoT mientras que solo un 20% indicó lo contrario.

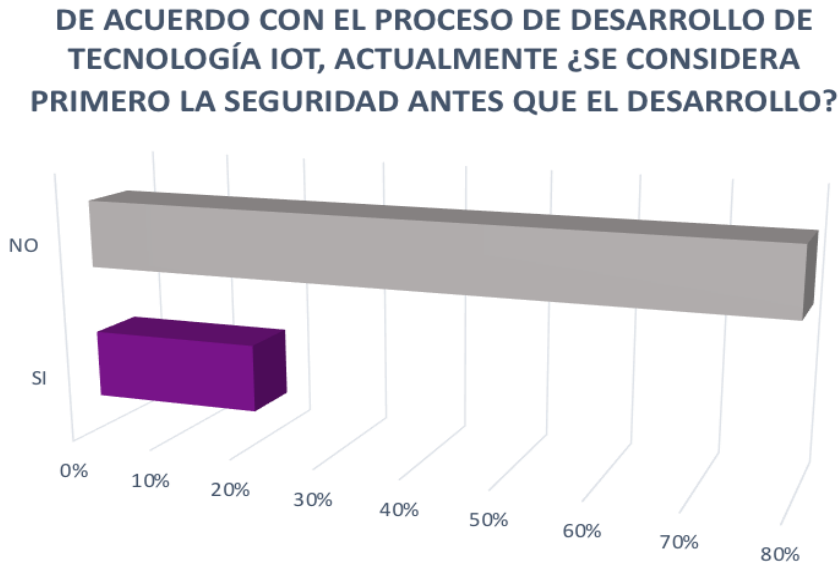
**Gráfico #53**




**Anexo 4 – Cuestionario para IT/Privado**

En el gráfico anterior se puede observar que el 80% de los ingenieros informáticos de empresa privada indicaron que no se considera primero la seguridad antes que el desarrollo y solo un 20% indicó que sí toma en cuenta de primero.

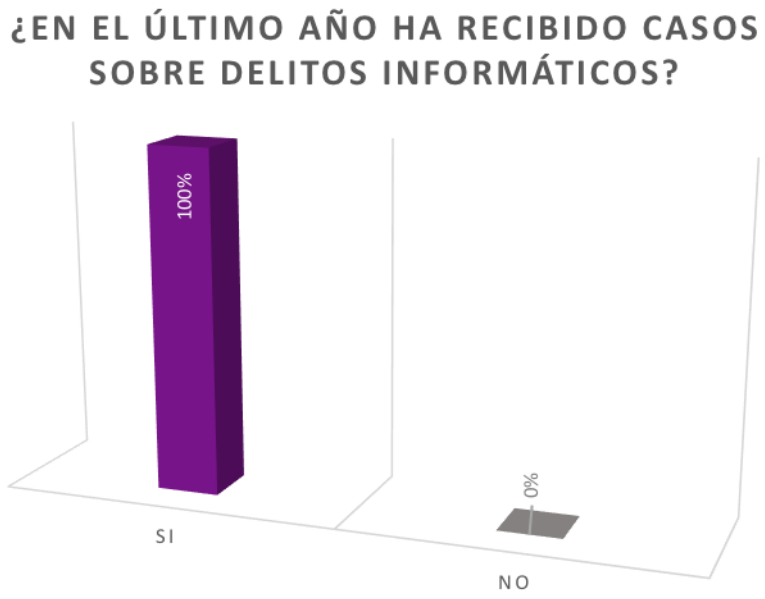
**Gráfico #54**




**Anexo 4 – Cuestionario para IT/Publicas**

En el gráfico anterior se puede observar que el 80% de los ingenieros informáticos de empresa pública indicaron que no se considera primero la seguridad antes que el desarrollo y solo un 20% indicó que sí toma en cuenta de primero.

**Gráfico #55**




**Fuente: Anexo 7- Cuestionario para investigadores privados**

El 100% de la población indicó que efectivamente durante el último año han recibido casos sobre delitos informáticos.

### 5.1.6 Análisis de la Variable #6

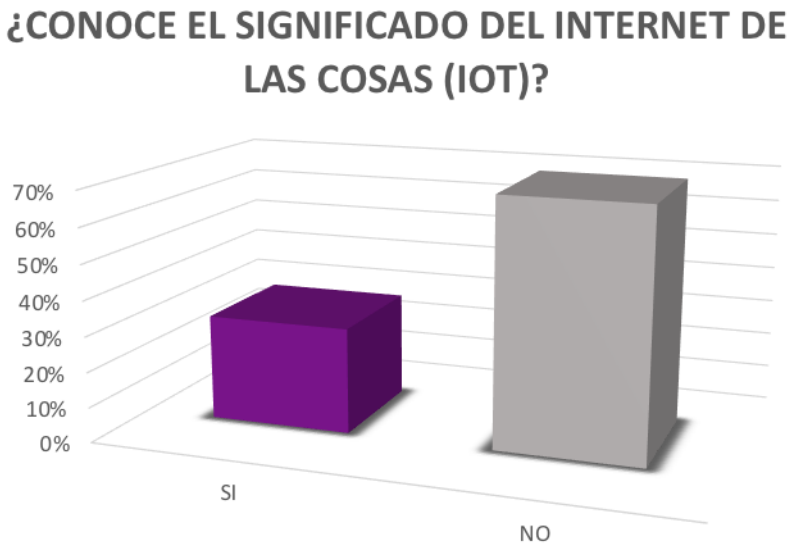
**El manejo de la información por parte de los usuarios y empresas.**

Esta variable se encarga de analizar el manejo actual de la información por parte de los usuarios y empresas.

**Objetivo analizado:**

Recomendar soluciones para mejorar el manejo de la información por parte de los usuarios y en las empresas.

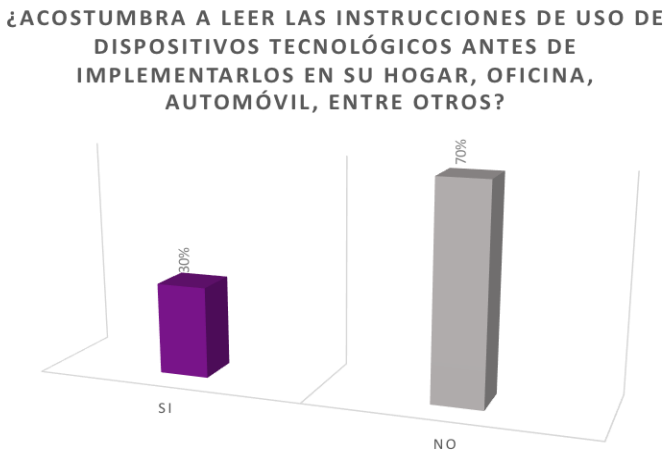
**Gráfico #56**




**Fuente: Anexo 2-Cuestionario para usuarios**

En el gráfico anterior aplicado a los usuarios, se puede observar que el 80% de la población indicó desconocer sobre el significado de IoT, muestran que un 20% indicó saber el significado.

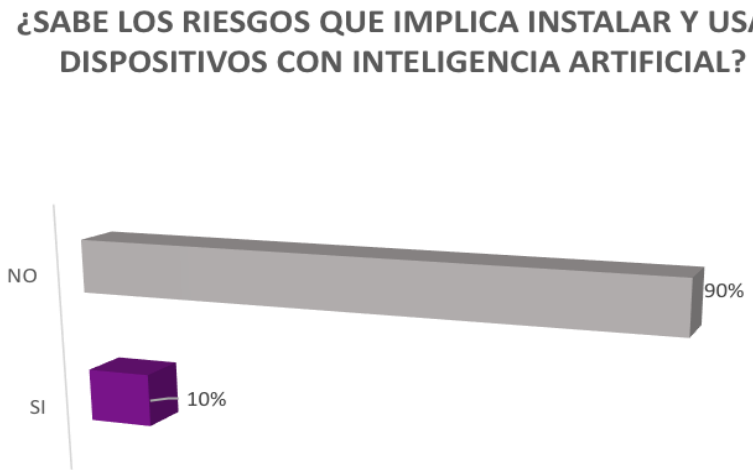
**Gráfico #57**




**Fuente: Anexo 2-Cuestionario para usuarios**

Se puede observar que un 70% de los usuarios no acostumbra a leer las instrucciones de uso de dispositivos tecnológicos antes de implementarlos, mientras que solo un 30% de la población lo realiza.

**Gráfico #58**




**Fuente: Anexo 2-Cuestionario para usuarios**

Se observa que un 90% de los usuarios desconoce sobre los riesgos que implica instalar y usar dispositivos con inteligencia artificial, mientras que solo un 10% sabe los riesgos.

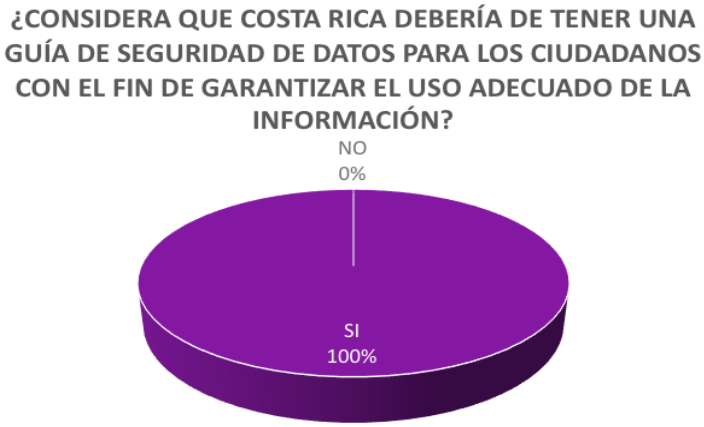
**Gráfico #59**




**Fuente: Anexo 2-Cuestionario para usuarios**

En el gráfico anterior el 100% de los usuarios considera que es importante que Costa Rica implemente una guía de seguridad de datos para los ciudadanos en donde se garantice el uso adecuado de la información.

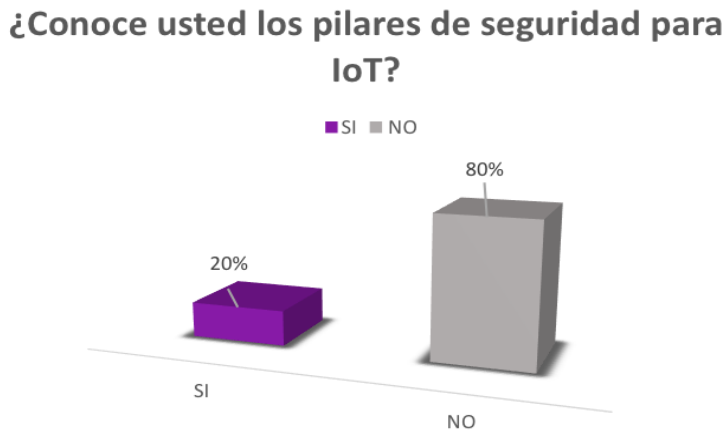
**Gráfico #60**




**Fuente: Anexo 3- Cuestionario para ingenieros especialistas en ciberseguridad**

En el gráfico anterior el 100% de los especialistas en ciberseguridad considera que es importante que Costa Rica implemente una guía de seguridad de datos para los ciudadanos en donde se garantice el uso adecuado de la información.

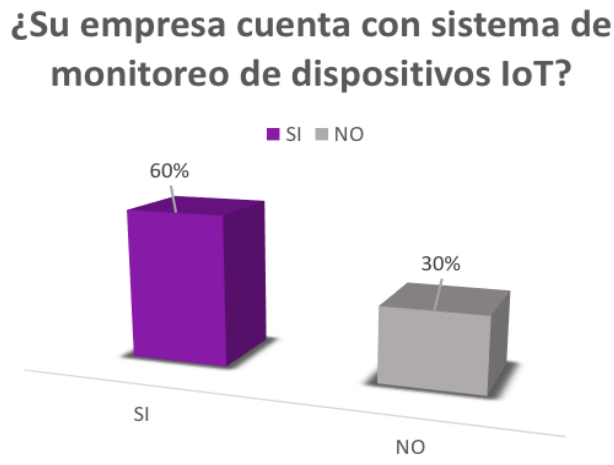
**Gráfico #61**




**Fuente: Anexo 3- Cuestionario para ingenieros especialistas en ciberseguridad**

Se puede observar que un 80% de los especialistas en ciberseguridad desconocen sobre los pilares de IoT, mientras que solo un 20% conoce de los mismos.

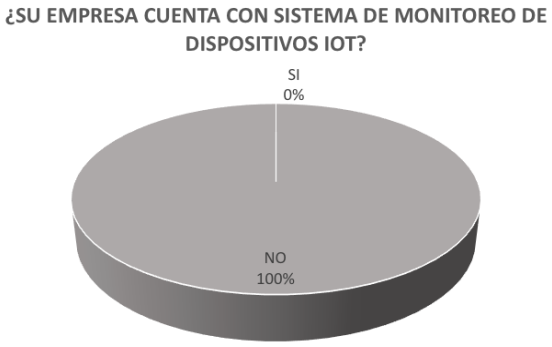
**Gráfico #62**




**Anexo 4 – Cuestionario para IT/Privada**

Con base en el gráfico anterior solo un 60% de las empresas privadas cuentan con monitoreo de dispositivos IoT, muestras que un 30% de las mismas no tiene.

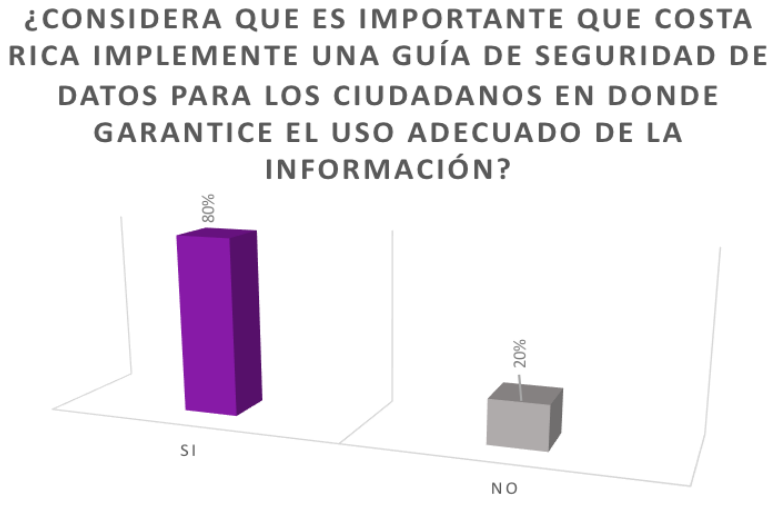
**Gráfico #63**




**Anexo 4 – Cuestionario para IT/Publica**

De acuerdo con el gráfico anterior, se puede observar que el 100% de las empresas públicas no cuentan con monitoreo de dispositivos IoT.

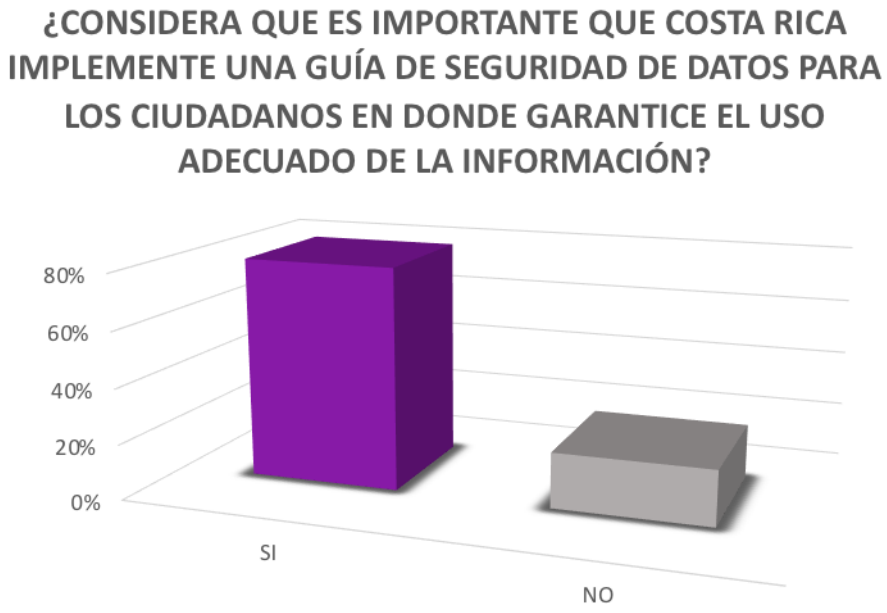
**Gráfico #64**




**Anexo 4 – Cuestionario para IT/Publica**

En el gráfico anterior se puede observar que el 80% de los ingenieros de empresas públicas indicó que si consideran que sea importante que Costa Rica implemente una guía de seguridad de datos para los ciudadanos en donde se garantice el uso adecuado de la información, muestras que un 20% indicó que no lo consideran importante.

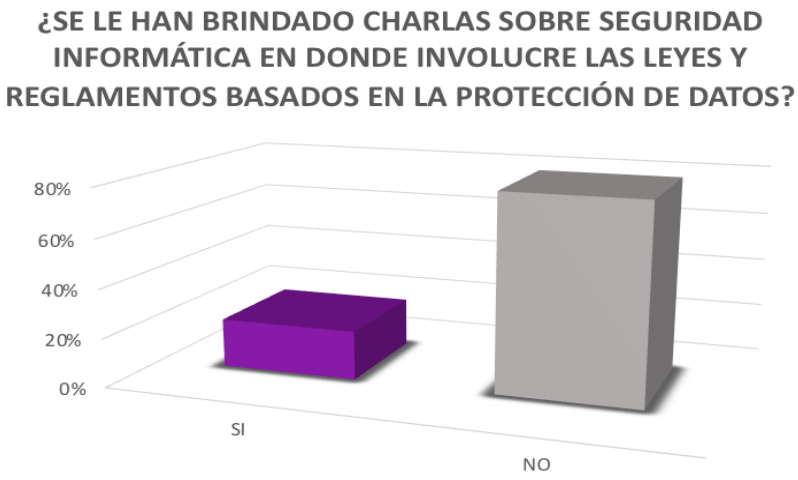
**Gráfico #65**




**Anexo 4 – Cuestionario para IT/Privada**

En el gráfico anterior se puede observar que el 80% de los ingenieros de empresas privadas indicó que sí consideran que sea importante que Costa Rica implemente una guía de seguridad de datos para los ciudadanos en donde se garantice el uso adecuado de la información, muestras que un 20% indica que no lo consideran importante.

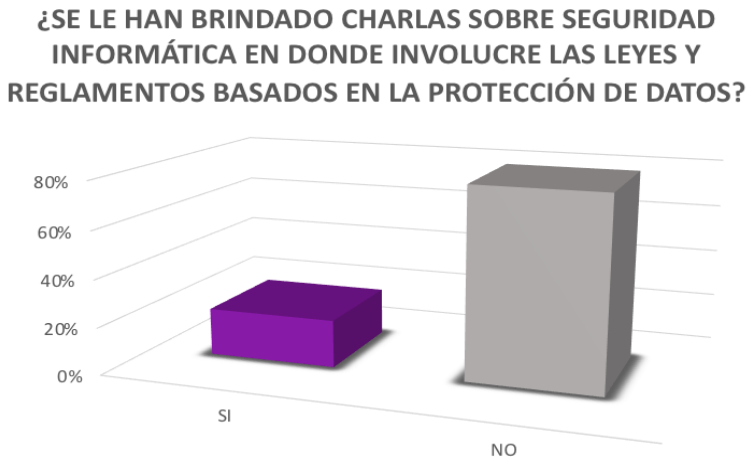
**Gráfico #66**




**Anexo 4 – Cuestionario para IT/Privada**

Se observa que un 80% de los ingenieros de empresas privadas indican que no se les han brindado charlas sobre seguridad informática en donde se involucren las leyes y reglamentos basados en la protección de datos, muestras que un 20% indicó lo contrario.

**Gráfico #67**




**Anexo 4 – Cuestionario para IT/Publica**

Se observa que un 80% de los ingenieros de empresas públicas indican que no se les han brindado charlas sobre seguridad informática en donde se involucren las leyes y reglamentos basados en la protección de datos, muestras que un 20% indicó lo contrario.

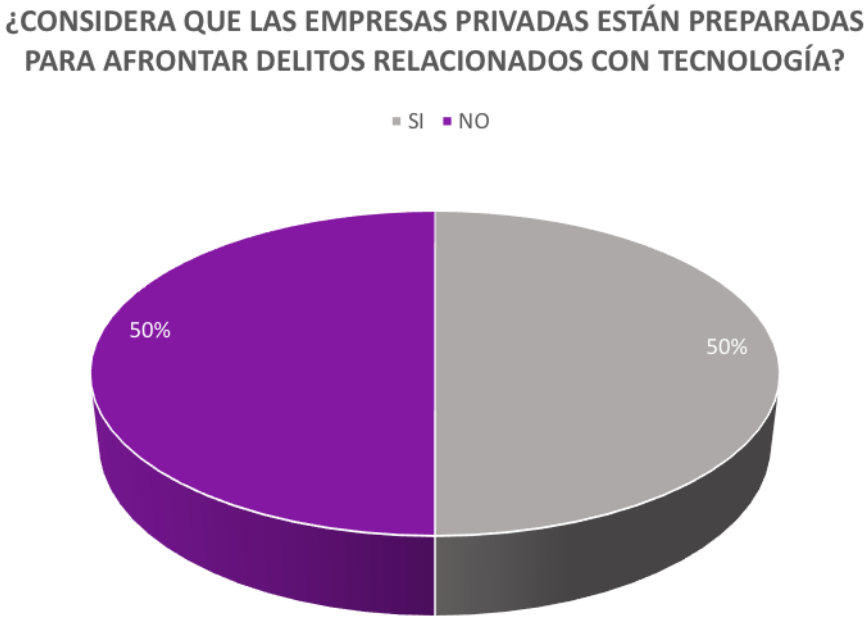
**Gráfico #68**




**Fuente: Anexo 6-Cuestionario para investigador del OIJ**

En el gráfico anterior se puede observar que el 100% indicó que el OIJ no se encuentra preparado para afrontar delitos relacionados con tecnología.

**Gráfico #69**




**Fuente: Anexo 7- Cuestionario para investigadores privados**

En el gráfico anterior se puede observar que los investigadores privados consideran 50/50 que las empresas privadas están preparadas para afrontar los delitos relacionados con tecnología.

# Capítulo VI

# Conclusiones y Recomendaciones

## 6.1 Conclusiones y recomendaciones

### 6.1.2 Conclusiones

Al finalizar la etapa de los resultados es fundamental el planteamiento de conclusiones y recomendaciones que se obtuvo en la presente investigación.

Dichas conclusiones se desprenden de los objetivos y las variables que se presentaron en el inicio del trabajo como ejes fundamentales del estudio.

De acuerdo con los resultados, se realizan en forma general una síntesis considerando cada una de las variables planteadas en el capítulo quinto con la finalidad de brindar las recomendaciones requeridas de acuerdo con los resultados obtenidos.

Mediante el desarrollo de la investigación, se pretende dar a conocer de manera sincrónica y diacrónica estado del arte de “el Internet de las cosas” o IoT, mismo que forma parte de la cotidianidad en la vida de cada individuo. Esta manera de pensar no es nueva y se viene dando desde las primeras interconexiones en donde intervienen las computadoras, pero que cada vez se han ido añadiendo a esta red más y más dispositivos que hasta ahora era impensable que pudieran estar conectados con otros, intercambiando información.

Esta investigación se centró en la importancia de que a la par de esta evolución, debe tenerse en cuenta una evolución en la seguridad involucrando tres factores primordiales: producción – legislación – usuario.

La seguridad y privacidad de los datos e información es uno de los aspectos que más preocupan a la población, así como la integridad física.

En términos generales, la seguridad debe de estar centrada tanto en los dispositivos (configuración, acceso, información cifrada, localización) y seguridad de la red.

A nivel empresarial, esta evolución de la tecnología también supone un importante reto debido a que el nivel de aportación en los distintos ámbitos de trabajo es incalculable, pero también, el reto consiste en controlar todas amenazas a la seguridad que conlleva.

Como conclusiones primordiales de esta investigación se destacan las siguientes, las mismas se brindarán de acuerdo con el orden de las variables.

Con respecto a la **variable #1** en la cual se evaluó la efectiva aplicación de la legislación costarricense en el desarrollo de proyectos IoT, se puede concluir con base en los datos obtenidos, que efectivamente Costa Rica tiene legislación vigente y atinente, misma que se manifiesta en las leyes y reglamentos que protegen los datos, información que fue proporcionada por el 60% de los abogados, los mismos que han trabajado en casos de personas que han sido procesadas por violación de la privacidad de los datos. Sin embargo, a pesar de que existen leyes y reglamentos, estos no son considerados suficientes,  ya que sus alcances no dimensionan de manera positiva los procesos necesarios para proteger correctamente los datos y tipificar los delitos.

Por otra parte, la población costarricense en un 90% desconoce que, así como muchos datos pueden ser útiles en una investigación, también pueden usarse en su contra sin que medie su consentimiento, por lo tanto, queda en evidencia falta de conocimiento y aplicación correcta de leyes y procesos adecuados con base en la información que se tienen en dispositivos tecnológicos.

Las mejoras que ha tenido Costa Rica en cuanto a los delitos informáticos y el Derecho Penal se considera significativo desde el año 2001, debido a que el Código Penal de 1971 no contempló durante muchos años los ilícitos informáticos, fue hasta el

año 2001 cuando se hizo la promulgación de la Ley No.8184 en donde se establecieron tres disposiciones legales para poder combatir el crimen informático, es por ello por lo que la Asamblea Legislativa indicó en el 2001:

"*se pretende regular y sancionar una serie de conductas que, sorprendentemente, no tienen aún mención alguna en nuestra legislación penal. Se trata de una serie de tipos penales que buscan prevenir y solucionar problemas evidentes y manifiestos en nuestro entorno,*

*(…). En razón de lo anterior, se han elaborado los siguientes tipos penales que se espera, sean lo suficientemente precisos para abarcar las diferentes conductas que hemos detectado como no reguladas"*

Los delitos que se agregaron al código penal fueron:

1. Violación de comunicaciones Electrónicas (artículo 196 bis del Código Penal)
2. Fraude Informático (artículo 217 bis del Código Penal)
3. Alteración de Datos y Sabotaje Informático (artículo 229 bis del Código Penal)

Al evaluar las legislaciones actuales que velan por la seguridad de los datos en Costa Rica hubo una deficiencia en respuestas, tanto de los especialistas en ciberseguridad como de los abogados, ya que 100% de los abogados conocen sobre la Ley de Delitos informáticos No.8968, sin embargo de los especialistas solo el 20% conoce de la misma, al igual que el reglamento de Habeas Data. Existe también una deficiencia de conocimiento con base en la Ley No.8642 relacionada con Telecomunicaciones.

De acuerdo con los resultados obtenidos y los datos demostrados, se puede indicar que los profesionales de Costa Rica no están preparados para asumir el reto de

la incorporación de IoT con todos sus alcances, además el marco legal costarricense debe de tomar consideraciones respecto al uso que se la da a la tecnología y que actualmente se evidencia la no contemplación porque aun cuando un 20% de los sujetos consultados considere que las leyes actuales son bastas para proteger los datos, hay un 80% de los sujetos que considera que las leyes actuales no cuentan con el suficiente alcance de especialización para proteger los datos y brindar de esta manera la seguridad requerida, por lo tanto persiste una deficiencia con base en el cumplimiento de las mismas producto del desconocimiento especializado de profesionales en derecho que carecen del área informática y de profesionales informáticos que carecen del conocimiento legal.

En referencia con la **variable #2**, misma que evalúa todas aquellas repercusiones en la seguridad y privacidad de los datos se logra determinar que el 60% de los abogados indican que la legislación actual no vela por la seguridad de las personas ante el uso indiscriminado de sus datos, a nivel legal se pueden hacer vigilancias por medio de dispositivos de seguridad, sin embargo, el uso de las mismas no puede violentar la privacidad de las personas en recintos determinados de trabajo, no así, en espacios abiertos donde la finalidad es la vigilancia general de activos y de elementos como la eficiencia y la eficacia del recurso humano.

Arroja la investigación que los usuarios no están conscientes de los datos personales que hay en el Internet y que evidentemente estos dispositivos almacenan, e incluso ya están en muchas de las empresas, los cuales son de uso diario para ingresar, cuyos sistemas biométricos son utilizados por el 80% de la población encuestada, sin embargo únicamente el 15% de los mismos aprobó dicho uso, por lo

tanto, hay un desconocimiento del manejo de esos datos personales, de sus repercusiones y de su almacenamiento.

Los especialistas en ciberseguridad indicaron sentirse desprotegidos a nivel legal en caso de acoso, robo o violación de la privacidad por lo que no consideran que Costa Rica esté preparado para la incorporación de IoT en áreas de aviación, infraestructura, automoción, telecomunicaciones, salud, entre otras. Sin embargo, la delincuencia no piensa lo mismo, ya que esta gran vulnerabilidad la han aprovechado para convertirse en ciberdelincuentes, por tal razón, el Organismo de Investigación Judicial ha recibido más de 500 reportes al año causados por delitos informáticos y en el gráfico #12 se confirmó que dicha institución no está preparada para afrontar delitos relacionados con tecnología.

Las amenazas de los delitos informáticos se consideran una realidad en el mundo y Costa Rica no escapa a este fenómeno de la nueva delincuencia.

Es claro que jurídicamente en el campo penal se cuenta con una deficiencia de desarrollo amplio en el tema y muy desactualizado.

Lo más preocupante en el caso de las repercusiones del ingreso de proyectos tecnológicos es que ya Costa Rica ha sido impactado económicamente cuando en el 2007 se hizo un traslado de $8.000.000 de cuentas corrientes de bancos costarricenses a bancos de Etiopía y Rumania en apenas tres meses. Esta fue una pequeña muestra de un impacto económico, pero se tiene que tener claro que se está en una cibersociedad y aldea global que en estos casos de ciberdelincuencia no hay barreras territoriales perjudicando no solo económicamente, sino que también de forma física cuyos casos no se han contemplado. Bajo este panorama, Costa Rica enfrenta

penalmente los delitos informáticos modernos con tan solo tres artículos, es claro que no se está listo y más preocupante aún, tampoco se está mitigando el problema o haciendo acciones para solucionarlo.

De acuerdo a la **variable #3**, la cual establece todos aquellos riesgos que implican la incorporación de IoT y las acciones que afectan la privacidad de los datos, se puede concluir que al realizar un mal uso de la información con fines delictivos se ven afectados factores de propiedad intelectual financiera, tanto personal como a nivel nacional, así como el honor cuyos alcances de afectación son invaluables, ya que afectan la imagen, la integridad y el posicionamiento social. Otra afectación de repercusiones mayores es riesgo laboral producto del mal manejo de los datos.

Por otra parte, los profesionales en el área legal establecieron en menor valor la estafa y la extorsión, dato interesante debido a que la mayoría de los delitos informáticos se basan en estos dos factores y cuya especialidad en *ransomware* y *Phishing* ha aumentado considerablemente en el último año.

El fraude de los delitos informáticos en los cuales los procesos judiciales que se han llevado a cabo para recuperar el perjuicio económico causado a los clientes, solamente se abarca procesos contra banco estatales, en ningún momento se ha direccionado en procesos contra banco privados, estos últimos cuidan la imagen que este tipo de situaciones acarrea, además, se logra determinar que el poco desarrollo de figuras penales sobre delitos informáticos en el país, no están tipificados dentro de un tipo penal determinado, situación que mediante derecho comparado se logra investigar que en otros países sí se encuentran contenidos en los códigos penales, lo que facilita que se pueda realizar la denuncia correspondiente cuando se dé una acción delictiva.

En Costa Rica, bajo el principio de legitimación debe de contenerse el hecho punible ante una acción antijurídica para poder determinar el tipo de delito en el que encaja, las penas que se establecen y las acciones que se deben de tomar en cada caso, es por ello que hay impunidad en Costa Rica ante algunos delitos informáticos.

Otro aspecto que afecta la privacidad de los datos es el desconocimiento que tiene la población sobre el tema, se conoce sobre los delitos informáticos de una forma escasa y básica, ya que sobre delitos mucho más avanzados son pocas las personas que cuentan con información tecnológica reciente.

Lo más preocupante del desconocimiento es que tampoco los profesionales en el área conocen del tema y se sienten de cierta forma desprotegidos, ya que los especialistas en ciberseguridad indicaron que la incorporación de IoT involucra un reto mayor para los SOC actuales y estos aún no cuentan con el monitoreo de ese tipo de amenazas.

Por otra parte, los usuarios están haciendo uso de esta tecnología sin estar informados, desconfiados y sin tomar medidas para proteger los datos.

Sin lugar a duda el cibercrimen actualmente es una barrera para el país y esto debido a la falta de información, capacitación y alcance legal.

Con respecto a la **variable #4** en la cual se determinan todas aquellas leyes y reglamentos que protegen la seguridad y privacidad de la información en Costa Rica se realizó una investigación exhaustiva con el fin de poder definir a continuación toda aquella jurisprudencia que es de efectiva aplicación en la actualidad.

La Ley No.8968 correspondiente a la Ley de protección de la persona frente al tratamiento de sus datos personales, la cual se explicó en profundidad en el capítulo II

del presente trabajo, sin embargo, durante todo el proceso de investigación se pueden concluir varios vacíos legales presentes en esta la Ley, los cuales se definen a continuación:

Se detectan ausentes aspectos reguladores necesarios para un eficiente y eficaz desempeño en el cumplimiento del objetivo constituido legalmente como por ejemplo, que la agencia no tiene injerencia sobre los posibles casos en donde sean personas jurídicas a las que se les violentan los derechos de la información relativa a la empresa, ya que las empresas también están expuestas a ser investigadas y la regulación no se pronuncia expresamente al respecto. Las personas jurídicas cuentan con una estructura propia y única como lo es su cédula jurídica, su información financiera, la información sobre sus actividades, información que tiende a ser susceptible de ser comercializada. Por lo tanto, la ley debería adicionar un capítulo exclusivo para el tratamiento de información de las personas jurídicas.

Otro aspecto ausente en el texto de la ley es de qué forma se tutelarán los derechos, en el caso de que sea traficada la información personal a nivel internacional, pues no menciona de ninguna forma la gestión que debe ejecutar la Prodhab para defender estos casos. Esto es evidencia de que debe reforzarse más la ley en cuanto al uso de la información e identificar los posibles portillos que existan para trasladar datos personales de frontera a frontera.

No se persigue identificar a Costa Rica como un país incapaz de emerger en la globalización con respecto al manejo de información de las personas o bases de datos, se trata de que exista acceso a los datos, pero no que estos sean datos sensibles, es

decir, que se construya a partir de datos como calidades personales y generales un grupo difuso de personas que coincidan en algún perfil.

Es lógico que, en las diferentes poblaciones, con el transcurso del tiempo y las nuevas tendencias, surjan cambios en el modo de vida y se hace no solo necesario, sino obligatorio que el derecho sea novedoso y se ajuste a los cambios de la sociedad. Por eso es por lo que ante los avances tecnológicos que generalmente facilitan la vida de algunos, se espera que todas las personas estén investidas de protección legal para salvaguardar sus intereses, principalmente porque la circulación de información de las personas es fundamental para el funcionamiento del mercado y economía de un país, pero esa información debe ser información veraz, exacta y autorizada por las personas.

La tutela del tratamiento de datos personales debe adquirir mayor relevancia jurídica y social para que la Ley 8968 no sea una ley más. La misma ley prevé la obligación de la Prodhab, en el artículo 22 de la divulgación, es decir, de promocionar la ley y de educar a la población sobre la importancia de conocer las funciones de la Prodhab. A la fecha, después de la publicación de la Ley 8968, los costarricenses, según el resultado de la muestra tomada para emitir estas afirmaciones a través de las encuestas electrónicas y evaluadas en el capítulo anterior, no tienen conocimiento sobre el objetivo de esta ley y sobre quién surte efectos.

El Código Penal tiene un papel fundamental en los delitos informáticos que velan en Costa Rica por la seguridad y privacidad de la información, por lo que después de investigar se concluyen los siguientes artículos como base fundamental de este trabajo:

***Artículo 196 bis.-Violación de datos personales.*** *Será sancionado con pena de prisión de uno a tres años quien en beneficio propio o de un tercero, con peligro o*

*daño para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, desvíe para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónicos, ópticos o magnéticos.*

*La pena será de dos a cuatro años de prisión cuando las conductas descritas en esta norma:*

***a)** Sean realizadas por personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.*

***b)** La información vulnerada corresponda a un menor de edad o incapaz.*

***c)** Las conductas afecten datos que revelen la ideología, la religión, las creencias, la salud, el origen racial, la preferencia o la vida sexual de una persona.*

*No constituye delito la publicación, difusión o transmisión de información de interés público, documentos públicos, datos contenidos en registros públicos o bases de datos públicos de acceso irrestricto cuando se haya tenido acceso de conformidad con los procedimientos y limitaciones de ley.*

***Artículo 209.- Hurto agravado***

*Se aplicará prisión de un año a tres años, si el valor de lo sustraído no excede de cinco veces el salario base (*), y de uno a diez años, si fuere superior a esa suma, en los siguientes casos:*

***1)** Cuando el hurto fuere sobre cabezas de ganado mayor o menor, aves de corral, productos o elementos que se encuentren en uso para explotación agropecuaria.*

***2)** Si fuere cometido aprovechando las facilidades provenientes de un estrago, de una conmoción pública o de un infortunio particular del damnificado.*

***3)** Si se hiciere uso de ganzúa, llave falsa u otro instrumento semejante, o de la llave verdadera que hubiere sido sustraída, hallada o retenida.*

***4)** Si fuere de equipaje de viajeros, en cualquier clase de vehículos o en los estacionamientos o terminales de las empresas de transportes.*

***5)** Si fuere de vehículos dejados en la vía pública o en lugares de acceso público.*

***6)** Si fuere de cosas de valor científico, artístico, cultural, de seguridad o religioso, cuando, por el lugar en que se encuentren estén destinadas al servicio, a la utilidad o a la reverencia de un número indeterminado de personas, o librados a la confianza pública.*

***7)** Si fuere cometido por dos o más personas.*

*(Así reformado por el artículo 19 de la Ley de Protección a Víctimas, Testigos y demás intervinientes en el Proceso Penal N° 8720 de 4 de marzo de 2009.)*

***Artículo 217 bis.- Estafa informática***

*Se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro.*

*La pena será de cinco a diez años de prisión, si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.*

*(Así adicionado por Ley "Adición de los artículos 196 BIS, 217 BIS y 229 BIS al Código Penal, Ley N° 4573 para reprimir y sancionar los delitos informáticos"; ley N° 8148 de 24 de octubre del 2001. Posteriormente reformado en la forma indicada por el artículo 1° de la ley "Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal"; ley N° 9048 del 10 de julio de 2012,)*

***Artículo 229 bis.- Daño informático.***

*Se impondrá pena de prisión de uno a tres años al que sin autorización del titular o excediendo la que se le hubiera concedido y en perjuicio de un tercero, suprima,*

*modifique o destruya la información contenida en un sistema o red informática o telemática, o en contenedores electrónicos, ópticos o magnéticos.*

*La pena será de tres a seis años de prisión, si la información suprimida, modificada, destruida es insustituible o irrecuperable.*

*(Así adicionado por el artículo único de la Ley "Adición de los artículos 196 BIS, 217 BIS y 229 BIS al Código Penal, Ley N° 4573 para reprimir y sancionar los delitos informáticos"; N° 8148 de 24 de octubre del 2001. Posteriormente reformado en la forma indicada por el artículo 1° de la ley "Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal"; N° 9048 del 10 de julio de 2012,)*

***Artículo 229 ter.- Sabotaje informático***

*Se impondrá pena de prisión de tres a seis años al que, en provecho propio o de un tercero, destruya, altere, entorpezca o inutilice la información contenida en una base de datos, o bien, impida, altere, obstaculice o modifique sin autorización el funcionamiento de un sistema de tratamiento de información, sus partes o componentes físicos o lógicos, o un sistema informático.*

*La pena será de cuatro a ocho años de prisión cuando:*

***a)** Como consecuencia de la conducta del autor sobrevenga peligro colectivo o daño social.*

***b)** La conducta se realice por parte de un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.*

***c)*** *El sistema informático sea de carácter público o la información esté contenida en bases de datos públicas.*

***d)*** *Sin estar facultado, emplee medios tecnológicos que impidan a personas autorizadas el acceso lícito de los sistemas o redes de telecomunicaciones.*

*(Así adicionado por el artículo 2° de la Ley N° 9048 del 10 de julio de 2012, "Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal")*

*Tampoco constituye delito la recopilación, copia y uso por parte de las entidades financieras supervisadas por la Sugef de la información y datos contenidos en bases de datos de origen legítimo de conformidad con los procedimientos y limitaciones de ley."*

*(Así adicionado por Ley N° 8148 de 24 de octubre del 2001 y posteriormente reformado en la forma indicada por el artículo 1° de la ley N° 9135 del 24 de abril de 2013)*

***Delitos informáticos y conexos***

*(Así adicionada la Sección VIII "Delitos informáticos y conexos", anterior por el artículo 3° de la Ley N° 9048 del 10 de julio de 2012, "Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal")*

***Artículo 230.- Suplantación de identidad.*** *Será sancionado con pena de prisión de uno a tres años quien suplante la identidad de una persona física, jurídica o de una marca comercial en cualquiera red social, sitio de Internet, medio electrónico o tecnológico de información.*

*(Así adicionado por el artículo 3° de la Ley N° 9048 del 10 de julio de 2012, "Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal")*

*(Así reformado por el artículo 1° de la ley N° 9135 del 24 de abril de 2013)*

***Artículo 231.- Espionaje informático***

*Se impondrá prisión de tres a seis años al que, sin autorización del titular o responsable, valiéndose de cualquier manipulación informática o tecnológica, se apodere, transmita, copie, modifique, destruya, utilice, bloquee o recicle información de valor para el tráfico económico de la industria y el comercio.*

*(Así adicionado por el artículo 3° de la Ley N° 9048 del 10 de julio de 2012, "Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal")*

***Artículo 232.- Instalación o propagación de programas informáticos maliciosos***

*Será sancionado con prisión de uno a seis años quien sin autorización, y por cualquier medio, instale programas informáticos maliciosos en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos.*

*La misma pena se impondrá en los siguientes casos:*

***a)** A quien induzca a error a una persona para que instale un programa informático malicioso en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos, sin la debida autorización.*

***b)** A quien, sin autorización, instale programas o aplicaciones informáticas dañinas en sitios de Internet legítimos, con el fin de convertirlos en medios*

*idóneos para propagar programas informáticos maliciosos, conocidos como sitios de Internet atacantes.*

***c)*** *A quien, para propagar programas informáticos maliciosos, invite a otras personas a descargar archivos o a visitar sitios de Internet que permitan la instalación de programas informáticos maliciosos.*

***d)*** *A quien distribuya programas informáticos diseñados para la creación de programas informáticos maliciosos.*

***e)*** *A quien ofrezca, contrate o brinde servicios de denegación de servicios, envío de comunicaciones masivas no solicitadas, o propagación de programas informáticos maliciosos.*

*La pena será de tres a nueve años de prisión cuando el programa informático malicioso:*

***i)*** *Afecte a una entidad bancaria, financiera, cooperativa de ahorro y crédito, asociación solidarista o ente estatal.*

***ii)*** *Afecte el funcionamiento de servicios públicos.*

***iii)*** *Obtenga el control a distancia de un sistema o de una red informática para formar parte de una red de ordenadores zombi.*

***iv)*** *Esté diseñado para realizar acciones dirigidas a procurar un beneficio patrimonial para sí o para un tercero.*

***v)*** *Afecte sistemas informáticos de la salud y la afectación de estos pueda poner en peligro la salud o vida de las personas.*

***vi)*** *Tenga la capacidad de reproducirse sin la necesidad de intervención adicional por parte del usuario legítimo del sistema informático.*

*(Así adicionado por el artículo 3° de la Ley N° 9048 del 10 de julio de 2012, "Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal")*

***Artículo 233.- Suplantación de páginas electrónicas***

*Se impondrá pena de prisión de uno a tres años a quien, en perjuicio de un tercero, suplante sitios legítimos de la red de Internet.*

*La pena será de tres a seis años de prisión cuando, como consecuencia de la suplantación del sitio legítimo de Internet y mediante engaño o haciendo incurrir en error, capture información confidencial de una persona física o jurídica para beneficio propio o de un tercero.*

*(Así adicionado por el artículo 3° de la Ley N° 9048 del 10 de julio de 2012,"Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal")*

***Artículo 234.- Facilitación del delito informático***

*Se impondrá pena de prisión de uno a cuatro años a quien facilite los medios para la consecución de un delito efectuado mediante un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos.*

*(Así adicionado por el artículo 3° de la Ley N° 9048 del 10 de julio de 2012,"Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal")*

***Artículo 235.- Narcotráfico y crimen organizado***

*La pena se duplicará cuando cualquiera de los delitos cometidos por medio de un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos afecte la lucha contra el narcotráfico o el crimen organizado.*

*(Así adicionado por el artículo 3° de la Ley N° 9048 del 10 de julio de 2012, "Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal")*

***Artículo 236.- Difusión de información falsa***

*Será sancionado con pena de tres a seis años de prisión quien, a través de medios electrónicos, informáticos, o mediante un sistema de telecomunicaciones, propague o difunda noticias o hechos falsos capaces de distorsionar o causar perjuicio a la seguridad y estabilidad del sistema financiero o de sus usuarios.*

*(Así adicionado por el artículo 3° de la Ley N° 9048 del 10 de julio de 2012, "Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal")*

Con respecto a la **variable #5**, la cual evalúa todos aquellos agujeros de seguridad que son parte de la incorporación de IoT en Costa Rica, se puede concluir que a pesar de que los usuarios no tienen un alto conocimiento en el manejo de la tecnología, se preocupan por tomar medidas en cuanto al cambio de claves y uso de Token bancario, sin embargo, más del 50% de la población en estudio desconoce sobre los ataques de secuestro de información llamados *ransomware*.

Los riesgos y problemas que surgen en la seguridad relacionados con el uso y expansión

de IoT no son nuevos, sino que existen desde las primeras interconexiones con computadoras. Lo que cambia es la escala en la que estos problemas y amenazas ocurren es por ello por lo que, el hecho de que la interconexión de dispositivos aumente exponencialmente a medida que la tecnología se afianza en el uso cotidiano supondrá un gran tráfico de internet que afectará en gran medida a las infraestructuras que existen actualmente. Será un reto conseguir que esta tecnología se pueda afianzar en todo el mundo, incluso en países en los que aún las estructuras de acceso a internet son precarias y poco avanzadas.

La sociedad interconectada hasta el último extremo de la palabra no solo supondrá un cambio a nivel tecnológico sino a nivel personal de individuo, donde la mentalidad y forma de vida cambiará totalmente para adaptarse a la nueva forma de pensar, trabajar, y realizar tareas cotidianas.

Al contar con sociedades interconectadas es necesario que la seguridad informática vaya de la mano con el crecimiento de esta, de lo contrario, los agujeros de seguridad serán mucho más profundos, dicha afirmación se da debido a que el 60% de los especialistas en ciberseguridad indicaron no estar preparados actualmente para el monitoreo constante de diferentes dispositivos IoT conectados a las redes empresariales.

Por otra, parte se logró comprobar que las empresas privadas y públicas que se dedican a realizar desarrollo de aplicación no velan en su mayoría por implementar seguridad en el código antes de sacar a producción cualquier dispositivo, esto demuestra la gran cantidad de agujeros de seguridad que presentan estos dispositivos que sin lugar a duda son vulnerables, provocando un sin número de delitos los cuales

se han reportado tanto al Organismo de Investigación Judicial así como a empresas de investigadores privadas.

El principal agujero de seguridad detectado en los sistemas IoT es que el propio fabricante de *hardware* es el que se encarga del mantenimiento de su *software*, y en muchos casos no disponen de la experiencia y recursos para poder dar una respuesta aceptable ante posibles brechas de seguridad.

Como se ha comentado, en muchos casos se emplean sistemas empotrados y en la mayoría de los casos estos dispositivos no se diseñaron inicialmente para estar conectados a la red, lo cual provoca que potencialmente sean más vulnerables. Algo similar está sucediendo con los sistemas de control industrial (SCADA), que originalmente se diseñaron para situarse en redes aisladas y actualmente se empiezan a conectar a Internet. Su exposición sin las medidas adecuadas supone un elevado riesgo.

En muchos casos, el problema no está en las capacidades del dispositivo, sino en las decisiones tomadas en las configuraciones por defecto de estos. En general, los dispositivos IoT no disponen de una entrada o salida de datos amigables como las de un PC, y tienen que facilitar acceso a sus interfaces de administración mediante otros medios más opacos y menos amigables para el usuario medio. Alrededor de este problema surge el concepto de Security by Default (en adelante SbD), que se traduce en la necesidad de establecer una configuración por defecto lo más segura posible para un dispositivo en su fabricación.

Por desgracia, en la mayoría de los casos esto no es así. Los fabricantes suelen establecer una solución intermedia o baja, que no requiera elevados conocimientos del

usuario ni la configuración del dispositivo para su funcionamiento. Con esto, se busca mejorar la experiencia del usuario y posiblemente dar una “buena” imagen de marca y producto. Este hecho es un arma de doble filo, ya que no es frecuente que los usuarios tengan conocimiento de las posibilidades de configuración de seguridad de su dispositivo, así que los dispositivos posiblemente mantengan una configuración potencialmente insegura.

Otra de las principales debilidades de estos dispositivos es su ubicación física, ya que pueden ser desde televisores, dispositivos tecnológicos vestibles, sensores en redes de detección de incendios, sistemas demóticos, actuadores luminosos de tráfico, etc. Este hecho hace que sean más difíciles de proteger, ya que esta situación puede permitir un sencillo acceso físico a ellos, lo que entraña uno de los riesgos más graves de cara a su seguridad. Los dispositivos IoT, adicionalmente a los riesgos de seguridad habituales sobre la disponibilidad, integridad y confidencialidad de la información, abarcan actuadores o componentes que pueden realizar cambios en el “mundo real” y como es lógico, este tipo de acciones pueden afectar a la seguridad y la salud de las personas.

En el transcurso de la investigación se logró comprobar una serie de deficiencias en dispositivos IoT que son importantes de mencionar como parte de los agujeros de seguridad que se tienen en la actualidad:

**Deficiencias de la seguridad en la transmisión de datos**

En la mayoría de los casos, los sistemas distribuidos que forman requieren un elevado uso de canales de comunicación, bien sea empleando redes cableadas, inalámbricas o cualquier otro medio de transmisión. Sea como sea, todas estas

comunicaciones, especialmente las que se propagan por medios inalámbricos o por redes públicas son sensibles de sufrir ataques a la confidencialidad en las comunicaciones.

Cuando los dispositivos o implementaciones no garanticen un nivel aceptable de seguridad en la identificación, privacidad, e integridad en las comunicaciones realizadas, es muy probable que estas deficiencias puedan ser aprovechadas por un atacante remoto para comprometer la información intercambiada. Esta información puede incluir datos privados o de carácter personal, o bien puede tratarse de datos técnicos que se puedan emplear para realizar otro tipo de ataques que, por ejemplo, faciliten el control del dispositivo.

Si no se protege adecuadamente el canal de comunicación mediante el cifrado de datos, puede ser sencillo para un intruso realizar ataques de tipo *Man In The Middle*. Este tipo de ataques se basan en que el atacante puede capturar el tráfico del cliente, rectificarlo para aparentar ser él el originador del mismo y remitirlo al servidor legítimo, de modo que actúa como un punto intermedio en las comunicaciones, invisible tanto para el origen como para el destino del tráfico. Así puede obtener toda la información que desee, incluso modificarla para alterar el comportamiento o funcionamiento de cualquiera de los dos extremos.

**Deficiencias en la seguridad de la plataforma software**

Uno de los vectores de ataque más frecuentes tanto en este ámbito como en general, es el aprovechamiento de vulnerabilidades de *software.*

El primero de los vectores de ataque por considerar es el propio sistema operativo. En cierto tipo de dispositivos se utilizan versiones ajustadas de sistemas operativos de uso común (Windows XP, Android, Linux, etc.) de forma que se abaratan los costes de fabricación. Este hecho, evidentemente supone un riesgo de seguridad, ya que cuando se detectan vulnerabilidades sobre dichas plataformas son explotables sobre todos los dispositivos que las instalan, facilitando a los potenciales atacantes una puerta de entrada para infinidad de dispositivos.

Otro vector de ataque incluso más habitual que el anterior son las interfaces web, de uso muy frecuente en dispositivos IoT, ya que éstos normalmente son de tamaño reducido y no disponen de monitor, teclado o dispositivos apuntadores, permitiendo su administración desde otro dispositivo habilitado. Adicionalmente, es importante destacar que es común que estas interfaces web se publiquen directamente a Internet para facilitar la administración del dispositivo desde la red. Del mismo modo que con los sistemas operativos, es habitual que se empleen plataformas web comunes, de modo que cuando se identifican vulnerabilidades de seguridad afectarán a todos los dispositivos que las implementen.

Otra característica común a una gran cantidad de dispositivos es el uso de servicios en la nube. En este caso dichas aplicaciones suponen otro vector de ataque, ya que si existen deficiencias en la gestión o actualización de este tipo de plataformas se podrá acceder a la información que puedan almacenar; así como dependiendo del servicio que se preste, incluso tomar el control del dispositivo IoT.

En algunos dispositivos como las Smart TV se pueden descargar e instalar aplicaciones de terceros sobre el propio dispositivo que amplían su funcionalidad, al igual que sucede con los Smartphones, las cuales normalmente se obtienen de repositorios de aplicaciones o tiendas que mantienen los propios fabricantes. En estos casos se pueden emplear estas aplicaciones como puerta de entrada para tomar el control del dispositivo, así como para obtener información. Este tipo de ataque se puede perpetrar de dos formas posibles; la primera sería explotando vulnerabilidades identificadas en el *software*, y la segunda podría ser descargando aplicaciones maliciosas, bien sea desde una fuente oficial que no analice suficientemente la seguridad de las aplicaciones que incorpora, o bien desde un canal no oficial de aplicaciones.

Por último, se popularice el uso de aplicaciones móviles que se instalan en los Smartphone para cualquier tipo de gestión, bien sea obtener datos o controlar el dispositivo. Debido a ello, las aplicaciones móviles también pueden ser objetivo de ataques, ya sea aprovechando vulnerabilidades o deficiencias en su implementación, o mediante el desarrollo de aplicaciones maliciosas que emulen el comportamiento y aspecto de las legítimas para obtener acceso a los dispositivos IoT.

**Deficiencias en la seguridad de la funcionalidad y configuración**

Otro punto fundamental en la seguridad de cualquier sistema es su propia funcionalidad. En muchas ocasiones, bien los desarrolladores (configuración por defecto) o los propios usuarios no mantienen un criterio alineado con la seguridad en la implementación o configuración de la funcionalidad de un servicio. En este aspecto, el

panorama en el mundo de IoT es semejante, ya que la mayoría de los dispositivos no siguen una política adecuada de SbD.

Como consecuencia de este hecho, la mayoría de los dispositivos habilitan muchas de sus funcionalidades en sus configuraciones por defecto, normalmente muchas más de las que emplea el usuario. Hay que ser conscientes de que cada uno de estos servicios habilitados puede suponer una brecha de seguridad en la actualidad o en un futuro si no se actualizan o gestionan adecuadamente.

Con base a la **variable #6**, la cual se encarga de analizar el manejo actual de la información por parte de los usuarios y empresas, se concluye que a pesar de que los usuarios aplican algunas medidas de seguridad para proteger la información, no conocen sobre las nuevas tecnologías, ya que el 80% de la muestra indicó desconocer que es IoT o el Internet de las cosas, además, no leen sobre el uso de tecnología simplemente adquieren un nuevo producto y lo ponen a funcionar sin percatarse del verdadero uso y dejando todos los ajustes por defecto. La falta de conocimiento que tienen los usuarios con la tecnología sobrepasa el beneficio que tienen del mismo, por lo que se logró demostrar que el 90% de los encuestados no saben de los riesgos que involucra instalar y usar dispositivos con inteligencia artificial.

Desgraciadamente en muchas ocasiones, a pesar de que los sistemas estén bien configurados una negligencia de un usuario podría comprometer el servicio.

El principal ataque que se puede llevar a cabo es la denominada Ingeniería Social (Social Engineering). Se basa en una manipulación psicológica de los usuarios, empleándolos como vía de acceso a los sistemas mediante acciones de engaño o

estafa. Empleándola, los atacantes se aprovechan del desconocimiento o la ignorancia para obtener la información necesaria para alcanzar su fin.

Dado que la mayoría de los sistemas y servicios en la red se protegen mediante el uso de nombres de usuario y contraseñas, el objetivo habitual es intentar obtener este tipo de credenciales mediante estafas por cualquier vía, habitualmente correo electrónico. La mayoría conocemos casos de *phishing,* que normalmente se envían de forma masiva y poco personalizada, centrados en la obtención de credenciales de acceso a servicios de correo electrónico o acceso a banca *online.* Sin embargo, cuando se trata de un ataque algo más elaborado es habitual realizar una investigación previa de la víctima en Internet consultando fuentes públicas, realizando actividades de recolección de información. Cuanto más descuidada o incauta sea la víctima al publicar o facilitar su información en la red, más fácil le resultará al atacante perpetrar un ataque más preciso, y en consecuencia con una mayor probabilidad de éxito.

Como se ha comentado con anterioridad, los ataques de ingeniería social se pueden realizar desde una forma sencilla hasta ataques sumamente elaborados y dirigidos. Evidentemente, el esfuerzo que dedique el atacante dependerá del beneficio que pueda obtener o sus intereses. Los ataques más elaborados estarán dirigidos a objetivos de mayor provecho, generalmente las empresas o administraciones públicas.

Cabe destacar que estos factores antes mencionados afectan a la población costarricense con la cantidad de ciberdelitos que se han desatado en los últimos dos

años, en donde se confirmó que tanto las empresas de seguridad privada como el OIJ se sienten poco preparados para afrontar delitos relacionados con tecnología.

### 6.1.2 Recomendaciones

Por la forma en que se plantearon los objetivos de esta investigación y la relación que se da entre las variables, las recomendaciones se harán de manera general abarcando sugerencias para cada una de las deficiencias encontradas.

Es necesario que la promoción de la Ley No.8968 llegue a todos los extremos geográficos de Costa Rica y para ello deben utilizarse todos los medios masivos e idóneos, electrónicos y escritos, entre otros, para que, sin importar la zona, todos los costarricenses tengan el conocimiento de la existencia de la ley creada para garantizar la protección de los derechos de su vida privada.

Por otra parte, se hace necesaria la participación, tanto del costarricense como de la **Agencia Protectora del Tratamiento de Datos Personales,** para que las medidas de protección que contiene la normativa sean lo suficientemente eficaces. Para ello, ambas partes, tanto sobre quienes recaen los efectos de la ley, como la entidad encargada para velar por su cumplimento, deben interactuar para comprender el alcance normativo. Uno de los resultados obtenidos en la aplicación de la encuesta electrónica despertó el interés del 100% de los encuestados, con respecto a crear una guía de seguridad de datos para los ciudadanos en donde garantice el uso adecuado de la información**.** Es una posible herramienta para establecer los parámetros del uso de información al que pueden tener acceso las empresas y el manejo adecuado de los datos.

Es estrictamente necesario que la **Prodhab** actúe de oficio y no solo a petición de parte sobre las diferentes empresas que comercialicen productos o información personal, de forma que la Prodhab pueda realmente ser un ente fiscalizador de la gestión que realizan las empresas para vender sus productos; y aprobar los lineamientos que se refieren a la contratación de las personas, para confirmar que la manipulación de la información de datos que custodian para sus fines no sean contrarios a la ley y los derechos de la privacidad de las personas. Esto implica que la entidad tenga poder de realizar auditorías externas sobre los diferentes sectores, tanto público como privado, ajenas a las auditorías de calidad, auditorías internas o auditorías para certificaciones ISO que realizan las empresas internamente para poder procesar correctamente los delitos, es por ello, que es necesario hacer una mejora en los mismos con el objetivo de tipificar y penalizar adecuadamente a las personas que atenten contra la seguridad y privacidad de los datos.

Por otra parte, para minimizar el impacto en caso de sufrir una posible estafa, se recomienda mantener credenciales de acceso diferentes para cada uno de los servicios de los que seamos usuarios (correo, banca online, redes sociales, etc.). Ya que en caso de que se faciliten es fácil extrapolar las mismas a otros servicios, y de ese modo el atacante obtendría fácilmente más información.

Otra buena solución será, siempre que el servicio lo permita, optar por habilitar autenticación por dos factores, de modo que, aunque se comprometieran las credenciales de acceso al servicio, no se vería comprometido al requerirse un segundo factor de autenticación, como por ejemplo un mensaje SMS al móvil.

Además de la precaución, la formación y la concienciación son la principal salvaguarda en estos casos, ya que otorgan al usuario la capacidad de identificar las estafas y reaccionar adecuadamente contra ellas. Por desgracia, la ingeniería social es una de las técnicas más empleadas en la actualidad y cada vez se diseñan técnicas más elaboradas y complejas que resultan mucho más difíciles de identificar para cualquiera. Dada dicha circunstancia, se le recomienda a la **Agencia de Protección de Datos de los Habitantes** realizar campañas de concienciación y cursos para facilitar cultura de seguridad de los usuarios.

Se les recomienda a los usuarios las siguientes buenas prácticas para tener la información de forma segura:

**1. Contraseñas de acceso seguras:**

Una de las mejores prevenciones para mantener una correcta seguridad en la experiencia como usuario en internet es tener un completo control de las contraseñas manteniéndolas seguras en aplicaciones de almacenaje como por ejemplo 1Password en dispositivos IOS y Keeper en Android, estas aplicaciones son bastante robustas y confiables.

**2. Realizar copias de seguridad:**

En el caso de que por algún motivo reciba un ataque a su dispositivo, sería un problema muy grave que pudiera haber borrado todos los datos que el dispositivo ha ido guardando a lo largo del tiempo. Aunque el perjuicio se ha producido, una buena práctica para poder reducir el daño es realizar copias de seguridad periódicas de los

datos que le gustaría conservar en el caso de que se perdieran. Estas copias de seguridad deberán guardarse en otro dispositivo o en la nube.

**3. Proteger físicamente los dispositivos:**

Si dispone de un dispositivo que realiza un escáner diario mediante sensores, sería crucial que por algún motivo (sea un atacante o causa natural), los dispositivos se bloqueen o se apaguen. Para prevenir este tipo de incidentes, es necesario proteger los dispositivos con herramientas como SAI (sistema de alienación ininterrumpida), y otros aparatos que ayuden a relanzar el dispositivo en caso de que deje de funcionar.

**4. Redes sencillas: Si el dispositivo no necesita una compleja red para poder funcionar:**

Es recomendable que la red que se usa no sea mayor que la que necesita, ya que una red pequeña, es más administrable y, por tanto, es más segura.

**5. Redes complejas:**

En el caso en el que el dispositivo necesite de una red más amplia para funcionar, se deben de establecer políticas de acceso de usuarios para gestionar totalmente quién puede acceder a la red.

**6. Antivirus y antiespías:**

Desde cualquier sitio en el que se controle el dispositivo de IoT es necesario que disponga de algún *software* diseñado exclusivamente para poder proteger el sistema

operativo de posibles *malware* y espías que puedan acceder al equipo y con ello poder suplantar la identidad y acceder a el control total del dispositivo.

**7. Actualizar sistemas operativos y aplicaciones:**

Se deben de implementar la actualización de aplicaciones que le permitan controlar los dispositivos inteligentes. Estas actualizaciones de las aplicaciones también corrigen problemas de seguridad.

**8. Usar con precaución el correo electrónico y mensajería:**

Es necesario concienciar a los usuarios para el correcto uso del correo electrónico y servicios de mensajería, ya que es la principal vía de ataques de ingeniería social. Lo más seguro es no transmitir datos confidenciales ni sensibles si no se tienen elementos de autenticación y no aceptar programas o datos que provengan de fuentes desconocidas. Por tanto, hay que confirmar la fuente previamente.

**9. Precaución en el uso de Internet:**

No acceder a sitios web que tengan direcciones extrañas, ni que estén contenidos en correos electrónicos mencionados en el punto anterior. Tampoco es recomendable introducir ningún dato confidencial que no tenga los elementos de seguridad adecuados.

Por otra parte es fundamental sugerir a las siguientes entidades una serie de recomendaciones las cuales son fundamentales para poder mitigar y empezar a trabajar en las deficiencias encontradas durante el proceso de la investigación:

**Al Organismo de Investigación Judicial de Costa Rica**, se le recomienda capacitación en ámbitos de la ciberseguridad, puesto que muchos de los temas actuales los desconocen, por lo cual es fundamental que miembros del OIJ participen en los cursos de actualización sobre el cibercrimen que realiza la OEA junto con entidades robustas como Incibe, el Gobierno Español, Europol e Interpol. Costa Rica necesita tener profesionales en ciberseguridad que a su vez conozcan las leyes del país para crear procesos penales fundamentados en la evidencia.

**A las empresas** se les recomienda brindar charlas sobre protección de datos, manejo de correos electrónicos personales y empresariales, realizar campañas de detección de *phishing* y recomendar el uso adecuado de todos aquellos dispositivos electrónicos que son parte del día a día de las personas. Además, es fundamental que las empresas que se dedican al desarrollo de aplicaciones y mejoramiento de *software* implementen medidas de seguridad previamente al desarrollo del código de estas.

**A las universidades**, se les recomienda inculcar cursos de protección de datos enfatizando en cada una de las carreras, puesto que los ataques informáticos se empiezan a mitigar fomentando conocimiento en la población para crear bases de protección de la información.

# Capítulo VII

# Referencias Bibliográficas

## 7.1 Bibliografía


Agencia Española de Protección de Datos. (2010). Convenio 108 Consejo de Europa. Recuperado de: https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf . Recuperado el 11 Octubre de 2017.

Asamblea Legislativa. (2011). Expediente 16.679: Ley de Protección de la Persona Frente a sus Datos Personales. Recuperado de http://www.infocom.cr/downloads/docs/Documentos%20para%20consulta/Le y%20protecci%C3%B3n%20persona%20frente%20tratamiento%20datos%20personales%20Exp%2016,679%2011-10.pdf

Castillo, A, (2002). R.E.D.I. Los derechos fundamentales en Internet, Costa Rica. Recuperado el 20 Octubre de 2017 de: http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=167326 Código Penal de Costa Rica. (2002). San José, Costa Rica: Investigaciones Jurídicas S. A.

Álvarez, M., Castro, F.A. y Chavarría, H. (2007). La tutela de los derechos fundamentales en Costa Rica por medio del recurso de amparo. San José, Costa Rica: Investigaciones Jurídicas S. A

Agencia Española de Protección de Datos. (2010). Convenio 108 Consejo de Europa. Recuperado de:

https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf . Recuperado el 23 noviembre 2017.

Asamblea Legislativa. (2011). Expediente 16.679: Ley de Protección de la Persona Frente a sus Datos Personales. Recuperado de: http://www.infocom.cr/downloads/docs/Documentos%20para%20consulta/Le y%20protecci%C3%B3n%20persona%20frente%20tratamiento%20datos%20personales%20Exp%2016,679%2011-10.pdf

Castillo, A, (2002). R.E.D.I. Los derechos fundamentales en Internet, Costa Rica. Recuperado el 15 de diciembre 2017 de: http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=167326 Código Penal de Costa Rica. (2002). San José, Costa Rica: Investigaciones Jurídicas S. A.

Álvarez, M., Castro, F.A. y Chavarría, H. (2007). La tutela de los derechos fundamentales en Costa Rica por medio del recurso de amparo. San José, Costa Rica: Investigaciones Jurídicas S.A http://www.juridicas.unam.mx/inst/evacad/Eventos/2011/0310/doctos/Res2661Sp.pdf Sáenz, H. (2009). El derecho a la determinación Informativa y el Recurso de Hábeas Data. (Tesis de licenciatura inédita). Universidad de Costa Rica, San José, Costa Rica.

Sala Constitucional. (2011). La Sala en la Prensa. Delitos Informáticos. Recuperado de http://www.poderjudicial.go.cr/salaconstitucional/documento/salaenprensa/salaenprensa2011.pdf

Salas, J. F., (2012). Simposio de Redes Sociales y Derecho, la desprotección de los datos personales en las redes sociales. Recuperado de: http://www.jurisisabogados.com/pdf/12_JoseFranciscoSalas.pdf

Lemaître,(2011). Manualsobre Delitos Informaticos para la ciber-sociedad costarricense. San José, Costa Rica: Investigaciones Jurídicas S.A

Lemaître, (2010). La impunidad de los delitos informáticos en la ciber-sociedad costarricense en el ámbito del derecho penal. Recuperado de http://iij.ucr.ac.cr/wp-content/uploads/bsk-pdf-manager/2017/06/La-Impunidad-de-los-Delitos-Informáticos-en-la-Ciber-sociedad-Costarricense.pdf

SCIJ. Codigo Penal. Recuperado de: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=5027&nValor3=96389&strTipM=TC

Internet of Things :https://club.globallogic.com.ar/la-internet-de-las-cosas-parte-1/

ARPANET : https://es.wikipedia.org/wiki/ARPANET

D. Martínez, F. Blanes, J. Simo, and A. Crespo, “Redes de sensores y actuadores inalámbricas: Una caracterización y caso de estudio para aplicaciones médicas

en espacios cerrados," Pendiente de publicación: XXIX Jornadas de Automática. Universidad Rovira i Virgili de Tar- ragona, España, 2008.

History of Internet of things: http://www.sorayapaniagua.com/2012/04/15/un-poco-de-his- toria-sobre-internet-de-las-cosas/

IOT: "Desde la Internet de los equipos hacia la Internet de las cosas" Friedemann Mattern y Christian Floerkemeier

"Making your home 'smart', the Indian way". The *Times of India. Retrieved26 June 2015.* [7] EMC Corporation: https://es.wikipedia.org/wiki/EMC_Corporation [8] Mark Weiser: https://es.wikipedia.org/wiki/Mark_Weiser

Jiniper Research: "El Internet de las Cosas: Consumo, Industria y Servicios Públicos" http://www.juniperresearch.com/researchstore/key-vertical-markets/internet-of-things/consu- mer-industrial-public-services.

Dispositivos conectados: http://hipertextual.com/2015/11/internet-de-las-cosas-dispo-sitivos

Moss, Jamie. "The internet of things: unlocking the marketing potential".theguardian.com. The Guardian. Retrieved 31 March 2015.

Estadísticas IOT: http://www.marketingdirecto.com/actualidad/digital/2020-sera-ano-del-internet-las-cosas-numero-dispositivos-conectados-superara-los-38-millones/

Estudio de previsión: http://www.ticbeat.com/tecnologias/previsiones-de-futuro-domi-nado-por-el-internet-de-las-cosas/

"Internet of Things: The "Basket of Remotes" Problem". Monday Note. Retrieved 26 June 2015.

"IoT Security Foundation – Executive Steering Board". IoT Security Foundation.

Estudio previsión Gartner Symposium/ITxpo 2014 :http://www.gartner.com/news-room/id/2905717

Vargas, Monserrath (2016). “Segurida: el principal reto para Internet de las Cosas”. https://www.nacion.com/tecnologia/informatica/seguridad-el-principal-reto-para-internet-de-las-cosas/S4KUHLUCOFHXDJPOWEW4OLSAA4/story/

Madrigal, Ana (2016). “El internet de las cosas tiene gran relevancia en el Consejo de Innovación”. http://costarica2050.cr/el-internet-de-las-cosas-tiene-gran-relevancia-en-el-consejo-de-innovacion.html

Estudio previsión beneficio Asia: http://www.gsma.com/connectedliving/wp-content/uploads/2013/06/GSMA_PwC_Connected-life_260613.pdf

Seguridad por defecto https://en.wikipedia.org/wiki/Secure_by_default [20] Man in the middle: https://es.wikipedia.org/wiki/Ataque_Man-in-the-middle

Ingeniería Social http://hipertextual.com/archivo/2012/04/que-es-la-ingenieria-social- y-como-estar-prevenidos/

Recomendaciones G29 sobre IoT http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

INTECO recomendaciones contraseñas, recuperado de:
http://www.egov.ufsc.br/portal/sites/default/files/recomendaciones_creacion_y_uso_con- trasenas.pdf

VPN, recuperado de: https://es.wikipedia.org/wiki/Red_privada_virtual [25] Firewall
https://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica)

Sistema de Detección de intrusos (IDS), recuperado de:
https://es.wikipedia.org/wiki/Sistema_de_de- tecci%C3%B3n_de_intrusos

Cloud Services, recuperado de:
https://es.wikipedia.org/wiki/Computaci%C3%B3n_en_la_nube [28] Wize Mirror :
http://www.semeoticons.eu/

Green Horizont, recuperado de: https://robotsia.com/2015/08/31/inteligencia-artificial-contaminacion- polucion-green-horizon/

Alcance, escala y riesgo sin precedentes: Asegurar el Internet de las cosas, recuperado de:
https://www.telefonica.com/documents/23283/5538439/Telef%C3%B3nica_Secu- rity_IoT_Spanish.pdf/5137cc8e-e572-44c8-aecd-2f29f3f236be

Triangulación por antenas, recuperado de:
https://www.google.es/search?q=triangulaci%C3%B3n+te-lef%C3%B3nica&oq=triangulaci%C3%B3n+te-lef%C3%B3nica&aqs=chrome..69i57.4925j0j7&sourceid=chrome&ie=UTF-8

Coche Tesla, recuperado de: http://www.xataka.com/automovil/asi-sera-el-tesla-para-el-gran-publico-el- model-e

Moral Utilitaria, recuperado de: https://es.wikipedia.org/wiki/Utilitarismo

Política de privacidad de Facebook, recuperado de: https://www.facebook.com/privacy/explanation Richard Prince https://es.wikipedia.org/wiki/Richard_Prince

Eprivacidad, recuperado de: http://www.eprivacidad.es/

Arquitectura orientada a servicios, recuperado de: https://es.wikipedia.org/wiki/Arquitectura_orien- tada_a_servicios

Aeropuertos inteligentes, recuperado de: http://tecniciencia.net/tecnologia-inteligente-revolucionara-ae- ropuerto-de-dubai/

Satélites COMSAT, recuperado de: http://www.astromia.com/glosario/comsat.htm

Prueba de Turing, recuperado de: http://www.elmundo.es/cien-cia/2014/06/09/539589ee268e3e096c8b4584.html

Adrian McEween (2013). Designing the internet of Things.

Ian G Smith, The Internet of Things 2012 New Horizons, IERC - Internet of Things Euro-pean Research Cluster, 2012.

Internet Protocol, Version 6 (IPv6) Specification, https://www.ietf.org/rfc/rfc2460.txt, ob-tenido 2014.

M. Karpiriski, A. Senart, V. Cahill (2006), Sensor networks for smart roads, PerCom Workshops.

Changki Mo, J. Davidson (2013), Energy harvesting technologies for structural health monitoring applications IEEE Conference on Technologies for Sustainability (SusTech)

S. Dey, A. Chakraborty (2012), S. Naskar, P. Misra, Smart city surveillance: Leveraging benefits of cloud data stores IEEE 37th Conference on Local Computer Networks Workshops

J. Lee ; J.E. Kim ; D. Kim ; P.K. Chong ; J. Kim ; P. Jang (,2008) RFMS: Real-time Flood Monitoring System with wireless sensor networks, MASS

Amazon Web Services, http://aws.amazon.com,

Dave Evans (April 2011). "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything" (PDF). Cisco.

Wood, Alex. "The internet of things is revolutionizing our lives, but standards are a must". theguardian.com. The Guardian.

Swan, Melanie (8 November 2012). "Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0". Sensor and Actuator Net- works. 1 (3): 217–253.

Porup, J.M. ""Internet of Things" security is hilariously broken and getting worse". Ars Technica. Condé Nast.

Vongsingthong, S.; Smanchat, S. (2014). "Internet of Things: A review of applications & technologies" (PDF). Suranaree Journal of Science and Technology.

E. Polycarpou, L. Lambrinos, E. Protopapadakis (2013.), Smart parking solutions for urban areas, WoWMoM.

# Capítulo VIII

# Anexos

## ANEXO 1

San José, 20 de noviembre, 2017.

Sres. – as

Estimado Señor (as):
Les saludo respetuosamente y les solicito su colaboración para contestar un cuestionario con diferentes preguntas relacionadas a la seguridad informática, con el fin de evaluar la seguridad de la información.

Como estudiante de la Universidad Cenfotec a nivel de Maestría en Ciberseguridad, agradecería que me dieran respuesta al siguiente cuestionario para efectos de trabajo de grado.

Manifestándoles que la información que ustedes me puedan brindar será totalmente confidencial, anónima; la cual no será de tratamiento individual sino de carácter colectivo.

Agradeciendo su atención y apoyo.
Respetuosamente,

Yuliana Leitón Álvarez
Céd: 114920953
Estudiante

**ANEXO 2**
**Cuestionario para abogados**

1. ¿Considera que en Costa Rica existen leyes y reglamentos que protegen los datos?

   ( ) Si
   ( ) No

¿Por qué?

| |
|---|
| |

2. Marque con una X ¿Cuáles de las siguientes legislaciones son de efectiva aplicación para la seguridad de los datos en Costa Rica?

| | |
|---|---|
| | Constitución Política |
| | Código Penal |
| | Código Civil |
| | Código de Comercio |
| | Código Laboral |
| | Ley N8968 |
| | Ley Habeas Data |
| | Ley N8642 (Ley General de Telecomunicaciones) |
| | Ley General de Aduanas |
| | Ley de Administración Financiera de la República y Presupuestos Públicos |
| | Código de Normas y Procedimientos Tributarios |

3. ¿Se puede procesar legalmente a una persona física o jurídica que haga mal uso de los datos de sus clientes?

| |
|---|
| |

4. ¿Conoce usted personas que fueron procesadas por violación de la privacidad de los datos?

   ( ) Si
   ( ) No

Comente el caso

| |
|---|
| |

5. ¿Considera usted que la legislación existente es suficiente para tipificar y penalizar a personas que atenten contra la seguridad y privacidad de los datos?

   ( ) Si
   ( ) No

¿Por qué?

| |
|---|
| |

6. ¿Considera que es suficiente la legislación existente para velar por la seguridad de las personas ante el uso discriminado de sus datos?

| |
|---|
| |

7. ¿Qué propiedades se violenta cuando se hace un mal uso de la información (puede marcar varias)

| | |
|---|---|
| | Propiedad intelectual |
| | Propiedad financiera |
| | Propiedad patrimonial |
| | Honor |
| | Riesgo laboral |
| | Redes sociales |
| | Acoso |
| | Estafa |
| | Extorsión |
| | Seguridad residencial |
| | Acoso financiero |

8. ¿Considera que es legal la vigilancia por medio de dispositivos de seguridad? Marque con una X Si o No:

| | SI | NO |
|---|---|---|
| Trabajo (oficinas) | | |
| Trabajo doméstico | | |
| Residenciales | | |
| Comercios | | |
| Escuelas | | |

9. Considera usted que se puede pactar contractualmente la vigilancia continua y permanente de los trabajadores que desarrollan su labor en:

| | SI | NO |
|---|---|---|
| Industria | | |
| Oficinas privadas | | |
| Oficinas Gobierno | | |
| Escuelas privadas | | |
| Escuelas públicas | | |
| Hogar | | |
| Residenciales | | |
| Zona de juegos de niños | | |
| Gimnasios | | |

10. ¿Conoce usted casos en que la misma seguridad se convierte en una potencial amenaza ante: delincuencia, denuncias, pedofilia, violencia sexual, violencia doméstica, entre otros?

| |
|---|
| |

11. ¿Se puede obligar a un comercio, industria, residencial, entre otros, a dar la información grabada (imágenes, audio-video) en las cámaras de vigilancia para alguna investigación?

( ) Si
( ) No

¿Por qué?

| |
|---|
| |

12. **Escenario #1:** Comente el siguiente escenario.

Hay una familia que tiene vigilancia 24x7 en el hogar en la cual continuamente se monitorean muchas zonas de la casa.
La pareja constantemente tiene discusiones y en varias ocasiones la esposa se ha visto expuesta a las agresiones por parte del esposo en donde involucra violencia doméstica y psicológica.
La esposa recuerda que en su casa hay cámaras y decide presentar una denuncia de violencia domestica contra su esposo presentando dichos videos.
¿Puede tomar estos datos como evidencia? Si o no, ¿Por qué?

| |
|---|
| |

¿Se ve violentada la privacidad del esposo?

| |
|---|
| |

**ANEXO 3**
**Cuestionario para usuarios**

1. ¿Conoce el significado del Internet de las Cosas (IoT)?

( ) Sí
( ) No

2. ¿Considera que la seguridad actual es buena?

( ) Sí
( ) No

¿Por qué?

| |
|---|
| |

3. ¿Considera que lo que se grabe en una cámara se puede usar como prueba incluso en su contra?

( ) Sí
( ) No

¿Por qué?

| |
|---|
| |

4. ¿Está usted consciente de todos los datos personales que hay en el Internet sobre su persona?

( ) Si
( ) No

5. De estos métodos de seguridad, ¿cuáles aplica en su vida personal?

| | |
|---|---|
| | Cambio de claves cada 30 días |
| | Uso de Token bancario |
| | Desinstalación de cámaras y micrófonos en su computadora |
| | Cambio de claves en cámaras, Alexa, Smart TV, Smartwatch…. |
| | Software Baúl de claves |

6. ¿Conoce que Costa Rica tiene leyes y reglamentos que protegen la seguridad y privacidad de la información?

( ) Si
( ) No

¿Cuales?

| |
|---|
| |

7. ¿Conoce que existen ataques de secuestro de información llamados ransomware?

( ) Si
( ) No

8. ¿Considera que es legal que las cámaras de su casa graben constantemente las labores domésticas del empleado?

( ) Si
( ) No

9. ¿Le usaría a su hijo/hija un *smartwatch* con localización?

( ) Si
( ) No

¿Por qué?

| |
|---|
| |

10. ¿Acostumbra a leer las instrucciones de uso de dispositivos tecnológicos antes de implementarlos en su hogar, oficina, automóvil, entre otros?

( ) Si
( ) No

11. ¿Sabe los riesgos que implica instalar y usar dispositivos con inteligencia artificial?

( ) Si
( ) No

12. ¿Considera que es importante que Costa Rica implemente una guía de seguridad de datos para los ciudadanos en donde garantice el uso adecuado de la información?

( ) Si
( ) No

13. ¿En su trabajo usan sistemas biométricos para el ingreso (huella, reconocimiento facial, voz, ojos)?

( ) Si Aprobó usted el uso de este medio ( ) Si ( ) No
( ) No

## ANEXO 4
## Cuestionario para Ingenieros Especialistas en Ciberseguridad

1. ¿Considera que la incorporación de tecnología IoT involucra un reto mayor para el monitoreo constante ante amenazas?
   ( ) Si
   ( ) No

2. ¿Siendo usted especialista en el área de ciberseguridad, conoce las normas y reglamentos que velan por la seguridad de la información?
   ( ) Si
   ( ) No

¿Cuales?

| |
|---|
| |

3. ¿Considera que la ciudadanía costarricense está protegida a nivel legal en caso de acoso, robo o violación de la privacidad?
   ( ) Si
   ( ) No

4. ¿Se realiza monitoreo de dispositivos IoT tomando en cuenta cámaras, dispositivos biométricos o wereables conectados a la red interna de la empresa?
   ( ) Si
   ( ) No

5. ¿Considera que Costa Rica debería de tener una guía de seguridad de datos para los ciudadanos con el fin de garantizar el uso adecuado de la información?
   ( ) Si
   ( ) No

¿Por que?

| |
|---|
| |

6. ¿Conoce usted los pilares de seguridad para IoT?
   ( ) Si
   ( ) No

¿Cuáles son?

7. ¿Considera que Costa Rica está preparada para afrontar los retos que involucra la aplicación de IoT en las áreas de aviación, infraestructura, automoción, telecomunicaciones, salud, entre otras?
   ( ) Si
   ( ) No

7.1 ¿Están los SOC preparados para visualizar este tipo de actividades por medio de monitoreo?
   ( ) Si
   ( ) No

8. ¿Conoce usted los fundamentos legales de la Ley No.8968 (LEY DE PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES)?
   ( ) Si
   ( ) No

9. ¿Cómo especialista de seguridad, promueve usted el velar por que los empleados de su empresa conozcan sobre la protección de los datos?
   ( ) Si
   ( ) No

10. Marque con una X ¿Cuáles de las siguientes legislaciones son de efectiva aplicación para la seguridad de los datos en Costa Rica?

| | |
|---|---|
| | Constitución Política |
| | Código Penal |
| | Código Civil |
| | Código de Comercio |
| | Código Laboral |
| | Ley N8968 |
| | Ley Habeas Data |
| | Ley N8642 (Ley General de Telecomunicaciones) |
| | Ley General de Aduanas |

| | |
|---|---|
| | Ley de Administración Financiera de la República y Presupuestos Públicos |
| | Código de Normas y Procedimientos Tributarios |

## ANEXO 5
## Cuestionario para IT/Privado-Publico

1. ¿Su empresa cuenta con sistema de monitoreo de dispositivos IoT?
   ( ) Si
   ( ) No

2. ¿Se le han brindado charlas sobre seguridad informática en donde involucre las leyes y reglamentos basados en la protección de datos?
   ( ) Si
   ( ) No

3. ¿Considera que Costa Rica está preparada para la incorporación de IoT?
   ( ) Si
   ( ) No

4. De acuerdo con el proceso de desarrollo de tecnología IoT, actualmente ¿Se considera primero la seguridad antes que el desarrollo?
   ( ) Si
   ( ) No

5. ¿Considera que es importante que Costa Rica implemente una guía de seguridad de datos para los ciudadanos en donde garantice el uso adecuado de la información?
   ( ) Si
   ( ) No

6. Durante el desarrollo de aplicaciones, sistemas o tecnología, ¿existe algún proceso de responsabilidad legal, con el fin de no violentar lo estipulado en la Ley No.8968?
   ( ) Si
   ( ) No

## ANEXO 6
## Cuestionario para ingenieros informáticos con énfasis en delitos informáticos

1. ¿Considera usted que la legislación costarricense está preparada para afrontar la incorporación de IoT?

( ) Si
( ) No

¿Por qué?

2. ¿Cree usted que el marco legal de Costa Rica debería tomar alguna consideración respecto al uso de IoT que no esté contemplado actualmente?

( ) Si
( ) No

¿Cuál?

3. ¿Considera usted que se debe de ampliar o modificar los tipos penales contemplados en la Ley de delitos informáticos a causa de la posibilidad de cometer delitos físicos que habilita el IoT?

( ) Si
( ) No

¿Por qué?

4. ¿Tiene Costa Rica los mecanismos para velar por el cumplimiento de las leyes referentes a delitos informáticos?

( ) Si
( ) No

En caso de que No, ¿qué mejoras son necesarias?

**ANEXO 7**

**Cuestionario para investigador del OIJ**

1. ¿Considera que Costa Rica tiene las suficientes leyes y reglamentos para proteger los datos?

( ) Si

( ) No

2. Marque con una X ¿Cuáles de las siguientes legislaciones son de efectiva aplicación para la seguridad de los datos en Costa Rica?

| | |
|---|---|
| | Constitución Política |
| | Código Penal |
| | Código Civil |
| | Código de Comercio |
| | Código Laboral |
| | Ley N8968 |
| | Ley Habeas Data |
| | Ley N8642 (Ley General de Telecomunicaciones) |
| | Ley General de Aduanas |
| | Ley de Administración Financiera de la República y Presupuestos Públicos |
| | Código de Normas y Procedimientos Tributarios |

3. ¿Conoce usted sobre delitos utilizando la tecnología del Internet de las cosas?

( ) Si

( ) No

4. ¿El Organismo de Investigación Judicial está preparado para afrontar delitos relacionados con tecnología?

( ) Si

( ) No

5. ¿Conoce usted sobre la cadena de custodia que se le da al equipo tecnológico?

( ) Si

( ) No

Si es SI:
¿Aplica la misma para tecnología IoT?
( ) Si
( ) No

6. ¿Están preparados para los delitos de ciberseguridad?
( ) Si
( ) No

7. ¿Considera que el cibercrimen es una barrera para el país?
( ) Si
( ) No

8. ¿Considera usted que se debe de ampliar o modificar los tipos penales contemplados en la Ley de delitos informáticos a causa de la posibilidad de cometer delitos físicos que habilita el IoT?
( ) Si
( ) No

**ANEXO 8**
**Cuestionario para investigadores privados**

1. ¿Considera que Costa Rica tiene las suficientes leyes y reglamentos para proteger los datos?

( ) Si
( ) No

2. Marque con una X ¿Cuáles de las siguientes legislaciones son de efectiva aplicación para la seguridad de los datos en Costa Rica?

| | |
|---|---|
| | Constitución Política |
| | Código Penal |
| | Código Civil |
| | Código de Comercio |
| | Código Laboral |
| | Ley N8968 |
| | Ley Habeas Data |
| | Ley N8642 (Ley General de Telecomunicaciones) |
| | Ley General de Aduanas |
| | Ley de Administración Financiera de la República y Presupuestos Públicos |
| | Código de Normas y Procedimientos Tributarios |

3. ¿Conoce usted sobre delitos utilizando la tecnología del Internet de las cosas?

( ) Si
( ) No

4. ¿Considera que las empresas privadas están preparadas para afrontar delitos relacionados con tecnología?

( ) Si
( ) No

5. ¿Conoce usted sobre la cadena de custodia que se le da al equipo tecnológico?

( ) Si
( ) No

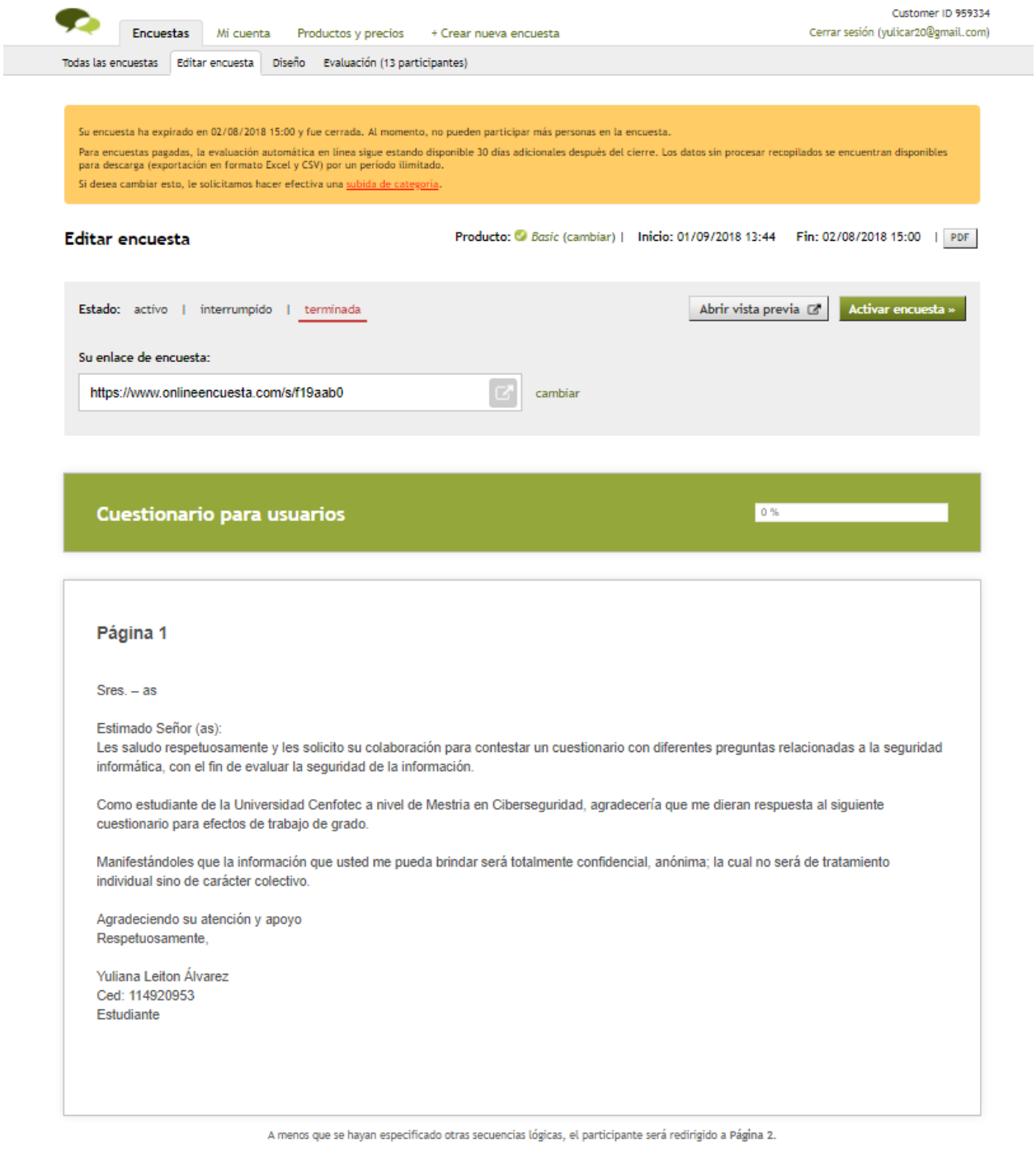
Si es SI:
¿Aplica la misma para tecnología IoT?
( ) Si
( ) No

6. ¿Están preparados para los delitos de ciberseguridad?
( ) Si
( ) No

7. ¿En el último año ha recibido casos sobre delitos informáticos?
( ) Si
( ) No

8. ¿Considera que el cibercrimen es una barrera para el país?
( ) Si
( ) No

9. ¿Considera usted que se debe de ampliar o modificar los tipos penales contemplados en la Ley de delitos informáticos a causa de la posibilidad de cometer delitos físicos que habilita el IoT?
( ) Si
( ) No


Customer ID 959334
Encuestas
Mi cuenta
Productos y precios
+ Crear nueva encuesta
Cerrar sesión (yulicar20@gmail.com)
Todas las encuestas
Editar encuesta
Diseño
Evaluación (13 participantes)
Su encuesta ha expirado en 02/08/2018 15:00 y fue cerrada. Al momento, no pueden participar más personas en la encuesta.
Para encuestas pagadas, la evaluación automática en línea sigue estando disponible 30 días adicionales después del cierre. Los datos sin procesar recopilados se encuentran disponibles para descarga (exportación en formato Excel y CSV) por un período ilimitado.
Si desea cambiar esto, le solicitamos hacer efectiva una subida de categoría.
Editar encuesta
Producto: Basic (cambiar) | Inicio: 01/09/2018 13:44 Fin: 02/08/2018 15:00 | PDF
Estado: activo | interrumpido | terminada
Abrir vista previa
Activar encuesta »
Su enlace de encuesta:
https://www.onlineencuesta.com/s/f19aab0
cambiar
Cuestionario para usuarios
0 %
Página 1
Sres. – as
Estimado Señor (as):
Les saludo respetuosamente y les solicito su colaboración para contestar un cuestionario con diferentes preguntas relacionadas a la seguridad informática, con el fin de evaluar la seguridad de la información.
Como estudiante de la Universidad Cenfotec a nivel de Mestria en Ciberseguridad, agradecería que me dieran respuesta al siguiente cuestionario para efectos de trabajo de grado.
Manifestándoles que la información que usted me pueda brindar será totalmente confidencial, anónima; la cual no será de tratamiento individual sino de carácter colectivo.
Agradeciendo su atención y apoyo
Respetuosamente,
Yuliana Leiton Álvarez
Ced: 114920953
Estudiante
A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a Página 2.

## Página 2

1. ¿Conoce el significado del Internet de las Cosas (IoT)? *

- ( ) sí
- ( ) no

2. ¿Considera que la seguridad actual de la información es buena? *

- ( ) sí
- ( ) no

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a Página 3.

## Página 3

¿Por qué? *

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a Página 4.

## Página 4

3. ¿Considera que lo que se grabe en una cámara se puede usar como prueba incluso en su contra? *

- ( ) sí
- ( ) no » continuar con Página 6

## Página 5

¿Por qué? *

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 6.**

## Página 6

4. ¿Está usted consiente de todos los datos personales que hay en el Internet sobre su persona? *

- ○ sí
- ○ no

5. De estos métodos de seguridad, ¿cuáles aplica en su vida personal? *

- ☐ Cambio de claves cada 30 días
- ☐ Uso de Token bancario
- ☐ Desinstalación de cámaras y micrófonos en su computadora
- ☐ Cambio de claves en cámaras, Alexa, Smart TV, Smartwatch....
- ☐ Software Baúl de claves
- ☐ Otro

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 7.**

## Página 7

6. ¿Conoce que Costa Rica tiene leyes y reglamentos que protegen la seguridad y privacidad de la información? *

- ○ sí
- ○ no » continuar con Página 9

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 8.**

## Página 8

¿Cuales? *

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 9**.

## Página 9

7. ¿Conoce que existen ataques de secuestro de información llamados ransomware? *

- sí
- no

8. ¿Considera que es legal que las cámaras de su casa graven constantemente las labores domésticas del empleado? *

- sí
- no

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 10**.

## Página 10

9. ¿Le usaría a su hijo/hija un smartwatch con localización? *

- sí
- no

10. ¿Acostumbra a leer las instrucciones de uso de dispositivos tecnológicos antes de implementarlos en su hogar, oficina, automóvil, entre otros? *

- sí
- no

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 11**.

## Página 11

**11. ¿Sabe los riesgos que implica instalar y usar dispositivos con inteligencia artificial? ***

- ◯ sí
- ◯ no

**12. ¿Considera que es importante que Costa Rica implemente una guía de seguridad de datos para los ciudadanos en donde garantice el uso adecuado de la información? ***

- ◯ sí
- ◯ no

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 12**.

## Página 12

**13. ¿En su trabajo usan sistemas biométricos para el ingreso (huella, reconocimiento facial, voz, ojos)? ***

- ◯ sí
- ◯ no » continuar con terminar la encuesta

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 13**.

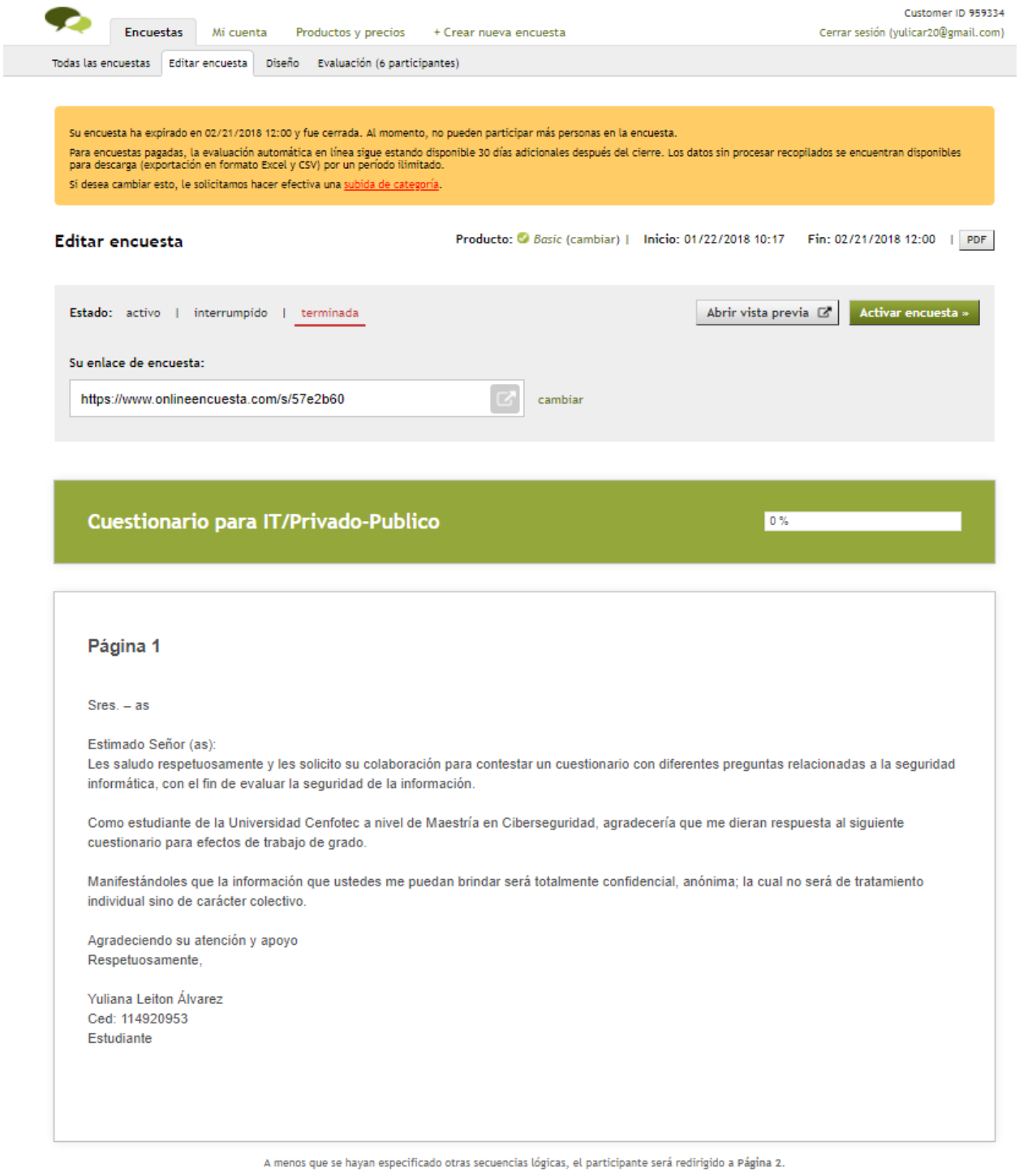
## Página 13

**Aprobó usted el uso de este medio ***

- ◯ sí
- ◯ no

A menos que se hayan especificado otras secuencias lógicas, la encuesta **finalizará** después de esta página.

» Redirection to final page of Online Encuesta


Customer ID 959334
Encuestas
Mi cuenta
Productos y precios
+ Crear nueva encuesta
Cerrar sesión (yulicar20@gmail.com)
Todas las encuestas
Editar encuesta
Diseño
Evaluación (6 participantes)
Su encuesta ha expirado en 02/21/2018 12:00 y fue cerrada. Al momento, no pueden participar más personas en la encuesta.
Para encuestas pagadas, la evaluación automática en línea sigue estando disponible 30 días adicionales después del cierre. Los datos sin procesar recopilados se encuentran disponibles para descarga (exportación en formato Excel y CSV) por un período ilimitado.
Si desea cambiar esto, le solicitamos hacer efectiva una subida de categoría.
Editar encuesta
Producto: Basic (cambiar) | Inicio: 01/22/2018 10:17 Fin: 02/21/2018 12:00 | PDF
Estado: activo | interrumpido | terminada
Abrir vista previa
Activar encuesta »
Su enlace de encuesta:
https://www.onlineencuesta.com/s/57e2b60
cambiar
Cuestionario para IT/Privado-Publico
0 %
Página 1
Sres. – as
Estimado Señor (as):
Les saludo respetuosamente y les solicito su colaboración para contestar un cuestionario con diferentes preguntas relacionadas a la seguridad informática, con el fin de evaluar la seguridad de la información.
Como estudiante de la Universidad Cenfotec a nivel de Maestría en Ciberseguridad, agradecería que me dieran respuesta al siguiente cuestionario para efectos de trabajo de grado.
Manifestándoles que la información que ustedes me puedan brindar será totalmente confidencial, anónima; la cual no será de tratamiento individual sino de carácter colectivo.
Agradeciendo su atención y apoyo
Respetuosamente,
Yuliana Leiton Álvarez
Ced: 114920953
Estudiante
A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a Página 2.

## Página 2

Indique el tipo de empresa para el que labora: *

- Privada
- Pública

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 3**.

## Página 3

¿Su empresa cuenta con sistema de monitoreo de dispositivos IoT? *

- sí
- no

¿Se le han brindado charlas sobre seguridad informática en donde involucre las leyes y reglamentos basados en la protección de datos? *

- sí
- no

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 4**.

## Página 4

¿Considera que Costa Rica está preparada para la incorporación de IoT? *

- sí
- no

De acuerdo con el proceso de desarrollo de tecnología IoT, actualmente ¿Se considera primero la seguridad antes que el desarrollo? *

- sí
- no

## Página 5

¿Considera que es importante que Costa Rica implemente una guía de seguridad de datos para los ciudadanos en donde garantice el uso adecuado de la información? *

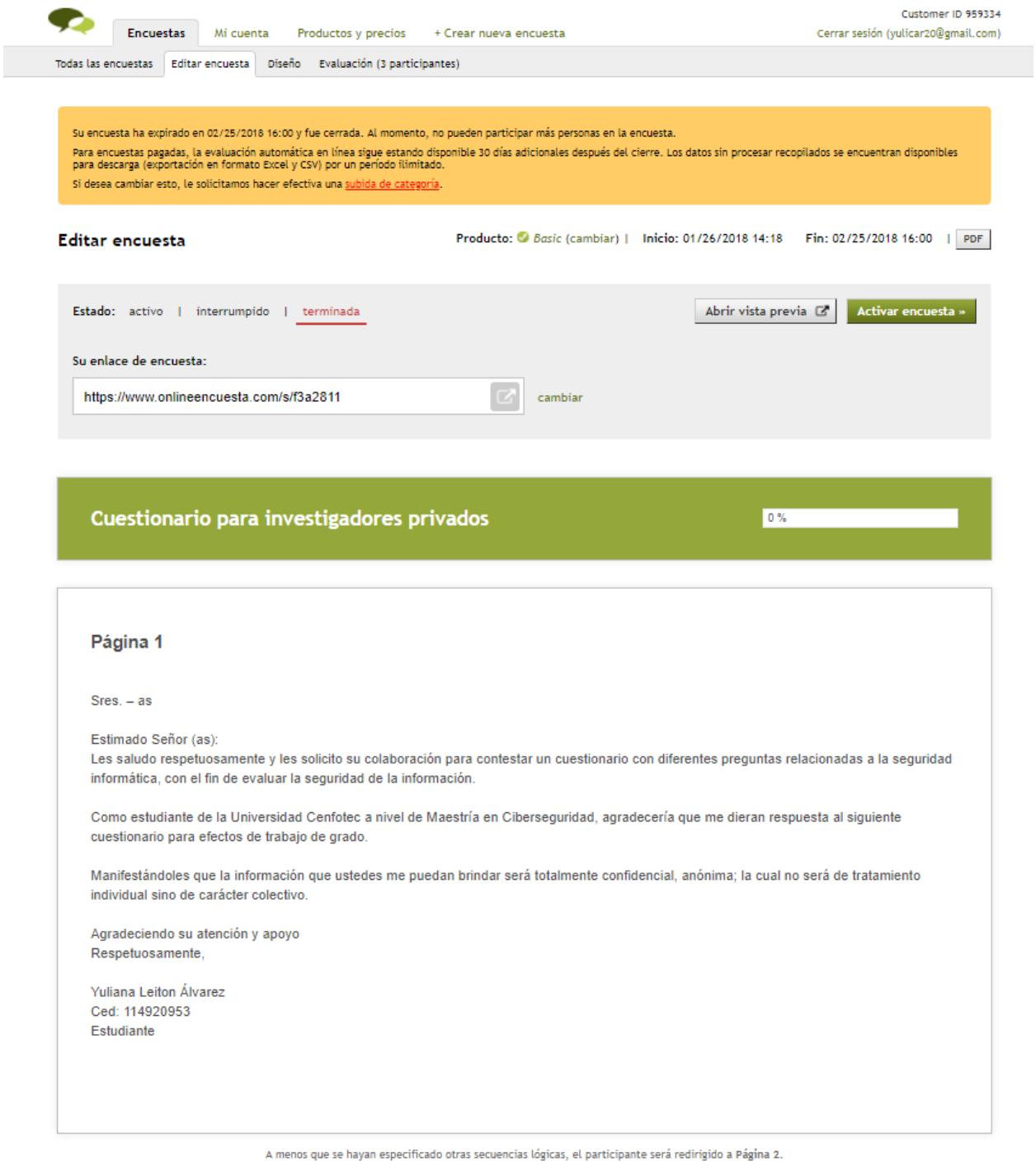
- sí
- no

Durante el desarrollo de aplicaciones, sistemas o tecnología, ¿existe algún proceso de responsabilidad legal, con el fin de no violentar lo estipulado en la Ley No.8968? *

- sí
- no

A menos que se hayan especificado otras secuencias lógicas, la encuesta finalizará después de esta página.

» Redirection to final page of Online Encuesta


Customer ID 959334
Encuestas
Mi cuenta
Productos y precios
+ Crear nueva encuesta
Cerrar sesión (yulicar20@gmail.com)
Todas las encuestas
Editar encuesta
Diseño
Evaluación (3 participantes)
Su encuesta ha expirado en 02/25/2018 16:00 y fue cerrada. Al momento, no pueden participar más personas en la encuesta.
Para encuestas pagadas, la evaluación automática en línea sigue estando disponible 30 días adicionales después del cierre. Los datos sin procesar recopilados se encuentran disponibles para descarga (exportación en formato Excel y CSV) por un período ilimitado.
Si desea cambiar esto, le solicitamos hacer efectiva una subida de categoría.
Editar encuesta
Producto: Basic (cambiar) | Inicio: 01/26/2018 14:18 Fin: 02/25/2018 16:00 | PDF
Estado: activo | interrumpido | terminada
Abrir vista previa
Activar encuesta »
Su enlace de encuesta:
https://www.onlineencuesta.com/s/f3a2811
cambiar
Cuestionario para investigadores privados
0 %
Página 1
Sres. – as
Estimado Señor (as):
Les saludo respetuosamente y les solicito su colaboración para contestar un cuestionario con diferentes preguntas relacionadas a la seguridad informática, con el fin de evaluar la seguridad de la información.
Como estudiante de la Universidad Cenfotec a nivel de Maestría en Ciberseguridad, agradecería que me dieran respuesta al siguiente cuestionario para efectos de trabajo de grado.
Manifestándoles que la información que ustedes me puedan brindar será totalmente confidencial, anónima; la cual no será de tratamiento individual sino de carácter colectivo.
Agradeciendo su atención y apoyo
Respetuosamente,
Yuliana Leiton Álvarez
Ced: 114920953
Estudiante
A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a Página 2.

## Página 2

**¿Considera que Costa Rica tiene las suficientes leyes y reglamentos para proteger los datos? ***

- ◯ sí
- ◯ no

**Marque con una X ¿Cuáles de las siguientes legislaciones son de efectiva aplicación para la seguridad de los datos en Costa Rica? ***

- ☐ Constitución Política
- ☐ Código Penal
- ☐ Código Civil
- ☐ Código de Comercio
- ☐ Código Laboral
- ☐ Ley N8968
- ☐ Ley Habeas Data
- ☐ Ley N8642 (Ley General de Telecomunicaciones)
- ☐ Ley General de Aduanas
- ☐ Ley de Administración Financiera de la República y Presupuestos Públicos
- ☐ Código de Normas y Procedimientos Tributarios

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 3**.

## Página 3

**¿Conoce usted sobre delitos utilizando la tecnología del Internet de las cosas? ***

- ◯ sí
- ◯ no

**¿Considera que las empresas privadas están preparadas para afrontar delitos relacionados con tecnología? ***

- ◯ sí
- ◯ no

## Página 4

**¿Conoce usted sobre la cadena de custodia que se le da al equipo tecnológico? ***

- ◯ sí
- ◯ no » continuar con Página 6

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 5**.

## Página 5

**¿Aplica la misma para tecnología IoT? ***

- ◯ sí
- ◯ no

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 6**.

## Página 6

**¿Están preparados para los delitos de ciberseguridad? ***

- ◯ sí
- ◯ no

**¿En el último año ha recibido casos sobre delitos informáticos? ***

- ◯ sí
- ◯ no

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 7**.

## Página 7

**¿Considera que el cibercrimen es una barrera para el país? ***

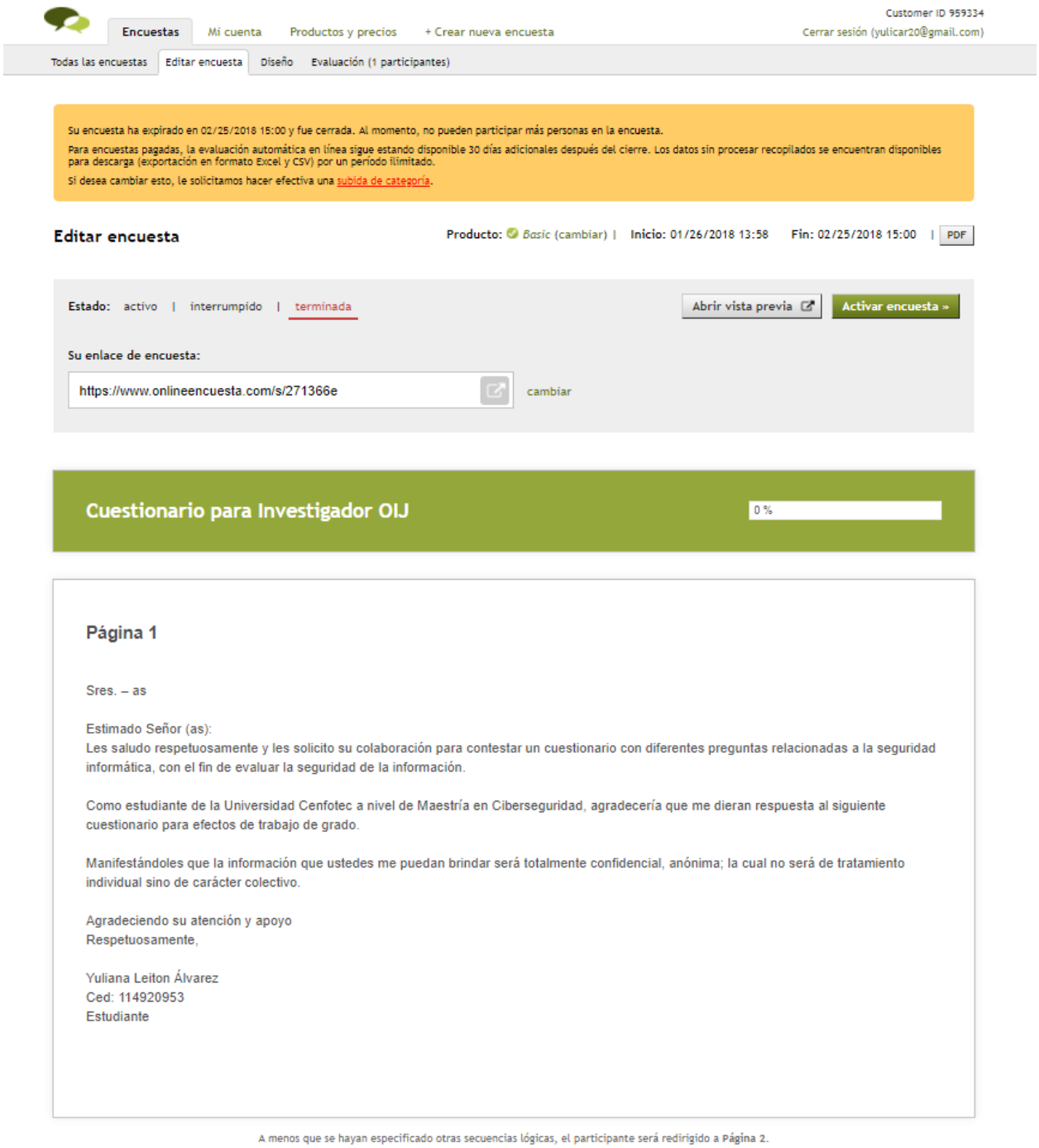
- ◯ sí
- ◯ no

**¿Considera usted que se debe de ampliar o modificar los tipos penales contemplados en la Ley de delitos informáticos a causa de la posibilidad de cometer delitos físicos que habilita el IoT? ***

- ◯ sí
- ◯ no

A menos que se hayan especificado otras secuencias lógicas, la encuesta **finalizará** después de esta página.

» Redirection to final page of Online Encuesta


Customer ID 959334
Encuestas
Mi cuenta
Productos y precios
+ Crear nueva encuesta
Cerrar sesión (yulicar20@gmail.com)
Todas las encuestas
Editar encuesta
Diseño
Evaluación (1 participantes)
Su encuesta ha expirado en 02/25/2018 15:00 y fue cerrada. Al momento, no pueden participar más personas en la encuesta.
Para encuestas pagadas, la evaluación automática en línea sigue estando disponible 30 días adicionales después del cierre. Los datos sin procesar recopilados se encuentran disponibles para descarga (exportación en formato Excel y CSV) por un periodo ilimitado.
Si desea cambiar esto, le solicitamos hacer efectiva una subida de categoría.
Editar encuesta
Producto: Basic (cambiar) | Inicio: 01/26/2018 13:58 Fin: 02/25/2018 15:00 | PDF
Estado: activo | interrumpido | terminada
Abrir vista previa
Activar encuesta »
Su enlace de encuesta:
https://www.onlineencuesta.com/s/271366e
cambiar
Cuestionario para Investigador OIJ
0 %
Página 1
Sres. – as
Estimado Señor (as):
Les saludo respetuosamente y les solicito su colaboración para contestar un cuestionario con diferentes preguntas relacionadas a la seguridad informática, con el fin de evaluar la seguridad de la información.
Como estudiante de la Universidad Cenfotec a nivel de Maestría en Ciberseguridad, agradecería que me dieran respuesta al siguiente cuestionario para efectos de trabajo de grado.
Manifestándoles que la información que ustedes me puedan brindar será totalmente confidencial, anónima; la cual no será de tratamiento individual sino de carácter colectivo.
Agradeciendo su atención y apoyo
Respetuosamente,
Yuliana Leiton Álvarez
Ced: 114920953
Estudiante
A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a Página 2.

## Página 2

**¿Considera que Costa Rica tiene las suficientes leyes y reglamentos para proteger los datos? ***

- ○ sí
- ○ no

**Marque ¿Cuáles de las siguientes legislaciones son de efectiva aplicación para la seguridad de los datos en Costa Rica? ***

- ☐ Constitución Política
- ☐ Código Penal
- ☐ Código Civil
- ☐ Código de Comercio
- ☐ Código Laboral
- ☐ Ley N8968
- ☐ Ley Habeas Data
- ☐ Ley N8642 (Ley General de Telecomunicaciones)
- ☐ Ley General de Aduanas
- ☐ Ley de Administración Financiera de la República y Presupuestos Públicos
- ☐ Código de Normas y Procedimientos Tributarios

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 3**.

## Página 3

**¿Conoce usted sobre delitos utilizando la tecnología del Internet de las cosas? ***

- ○ sí
- ○ no

**¿El Organismo de Investigación Judicial está preparado para afrontar delitos relacionados con tecnología? ***

- ○ sí
- ○ no

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 4**.

## Página 4

**¿Conoce usted sobre la cadena de custodia que se le da al equipo tecnológico?** *

- ◯ sí
- ◯ no » continuar con Página 6

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 5**.

## Página 5

**¿Aplica la misma para tecnología IoT?** *

- ◯ sí
- ◯ no

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 6**.

## Página 6

**¿Están preparados para los delitos de ciberseguridad?** *

- ◯ sí
- ◯ no

**¿Considera que el cibercrimen es una barrera para el país?** *

- ◯ sí
- ◯ no

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 7**.

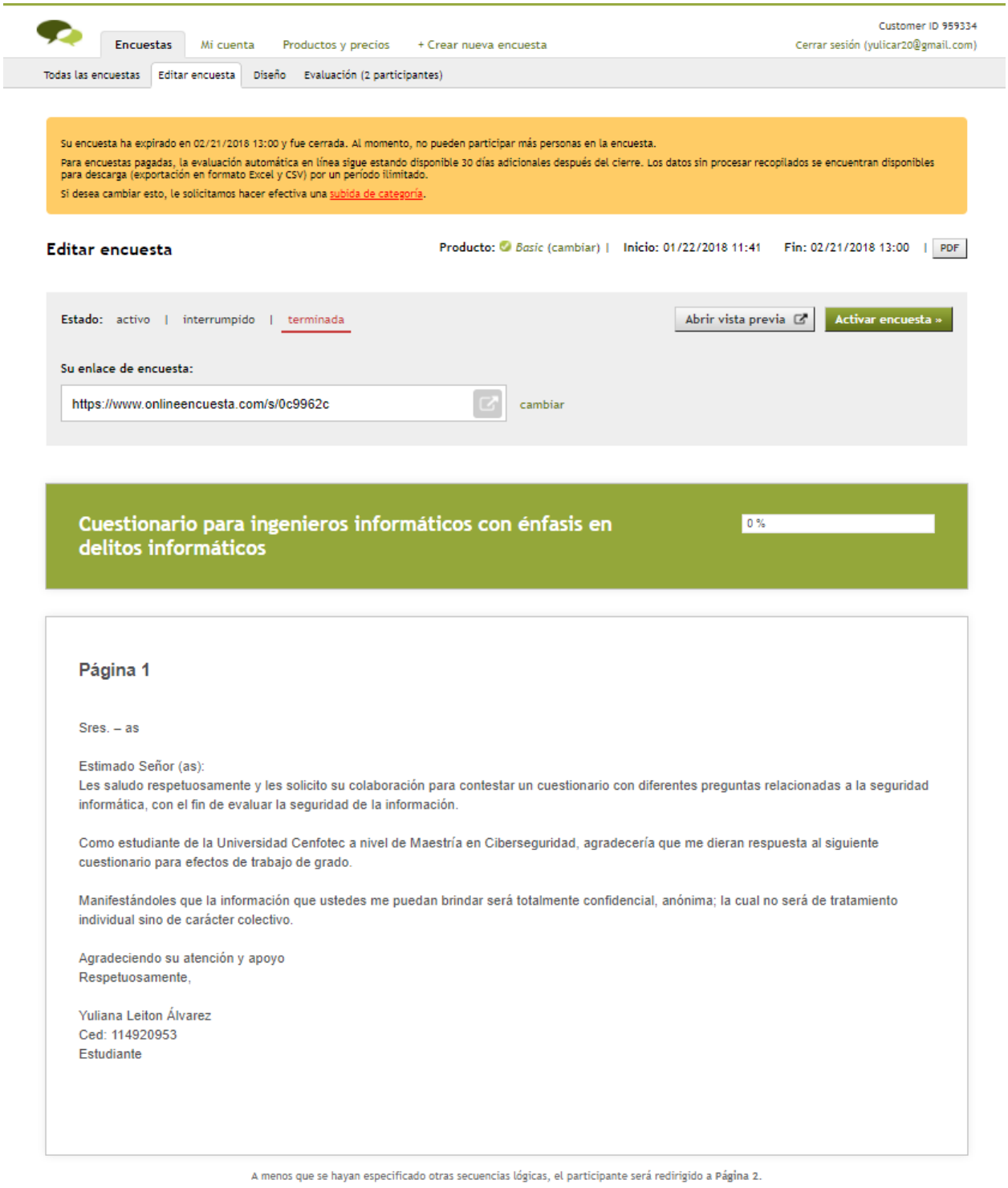
## Página 7

**¿Considera usted que se debe de ampliar o modificar los tipos penales contemplados en la Ley de delitos informáticos a causa de la posibilidad de cometer delitos físicos que habilita el IoT?** *

- ◯ sí
- ◯ no

A menos que se hayan especificado otras secuencias lógicas, la encuesta **finalizará** después de esta página.

» Redirection to final page of Online Encuesta


Encuestas
Mi cuenta
Productos y precios
+ Crear nueva encuesta
Customer ID 959334
Cerrar sesión (yulicar20@gmail.com)
Todas las encuestas
Editar encuesta
Diseño
Evaluación (2 participantes)
Su encuesta ha expirado en 02/21/2018 13:00 y fue cerrada. Al momento, no pueden participar más personas en la encuesta.
Para encuestas pagadas, la evaluación automática en línea sigue estando disponible 30 días adicionales después del cierre. Los datos sin procesar recopilados se encuentran disponibles para descarga (exportación en formato Excel y CSV) por un período ilimitado.
Si desea cambiar esto, le solicitamos hacer efectiva una subida de categoría.
Editar encuesta
Producto: Basic (cambiar) | Inicio: 01/22/2018 11:41 Fin: 02/21/2018 13:00 | PDF
Estado: activo | interrumpido | terminada
Abrir vista previa
Activar encuesta »
Su enlace de encuesta:
https://www.onlineencuesta.com/s/0c9962c
cambiar
Cuestionario para ingenieros informáticos con énfasis en delitos informáticos
0 %
Página 1
Sres. – as
Estimado Señor (as):
Les saludo respetuosamente y les solicito su colaboración para contestar un cuestionario con diferentes preguntas relacionadas a la seguridad informática, con el fin de evaluar la seguridad de la información.
Como estudiante de la Universidad Cenfotec a nivel de Maestría en Ciberseguridad, agradecería que me dieran respuesta al siguiente cuestionario para efectos de trabajo de grado.
Manifestándoles que la información que ustedes me puedan brindar será totalmente confidencial, anónima; la cual no será de tratamiento individual sino de carácter colectivo.
Agradeciendo su atención y apoyo
Respetuosamente,
Yuliana Leiton Álvarez
Ced: 114920953
Estudiante
A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a Página 2.

## Página 2

**¿Considera usted que la legislación costarricense está preparada para afrontar la incorporación de IoT? ***

- ◯ sí
- ◯ no

**¿Porque? ***

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 3**.

## Página 3

**¿Cree usted que el marco legal de Costa Rica debería tomar alguna consideración respecto al uso de IoT que no esté contemplado actualmente? ***

- ◯ sí
- ◯ no » continuar con Página 5

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 4**.

## Página 4

**¿Cual? ***

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 5**.

## Página 5

**¿Considera usted que se debe de ampliar o modificar los tipos penales contemplados en la Ley de delitos informáticos a causa de la posibilidad de cometer delitos físicos que habilita el IoT?** *

- ◯ sí
- ◯ no

**¿Porque?** *

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 6**.

## Página 6

**¿Tiene Costa Rica los mecanismos para velar por el cumplimiento de las leyes referentes a delitos informáticos?** *

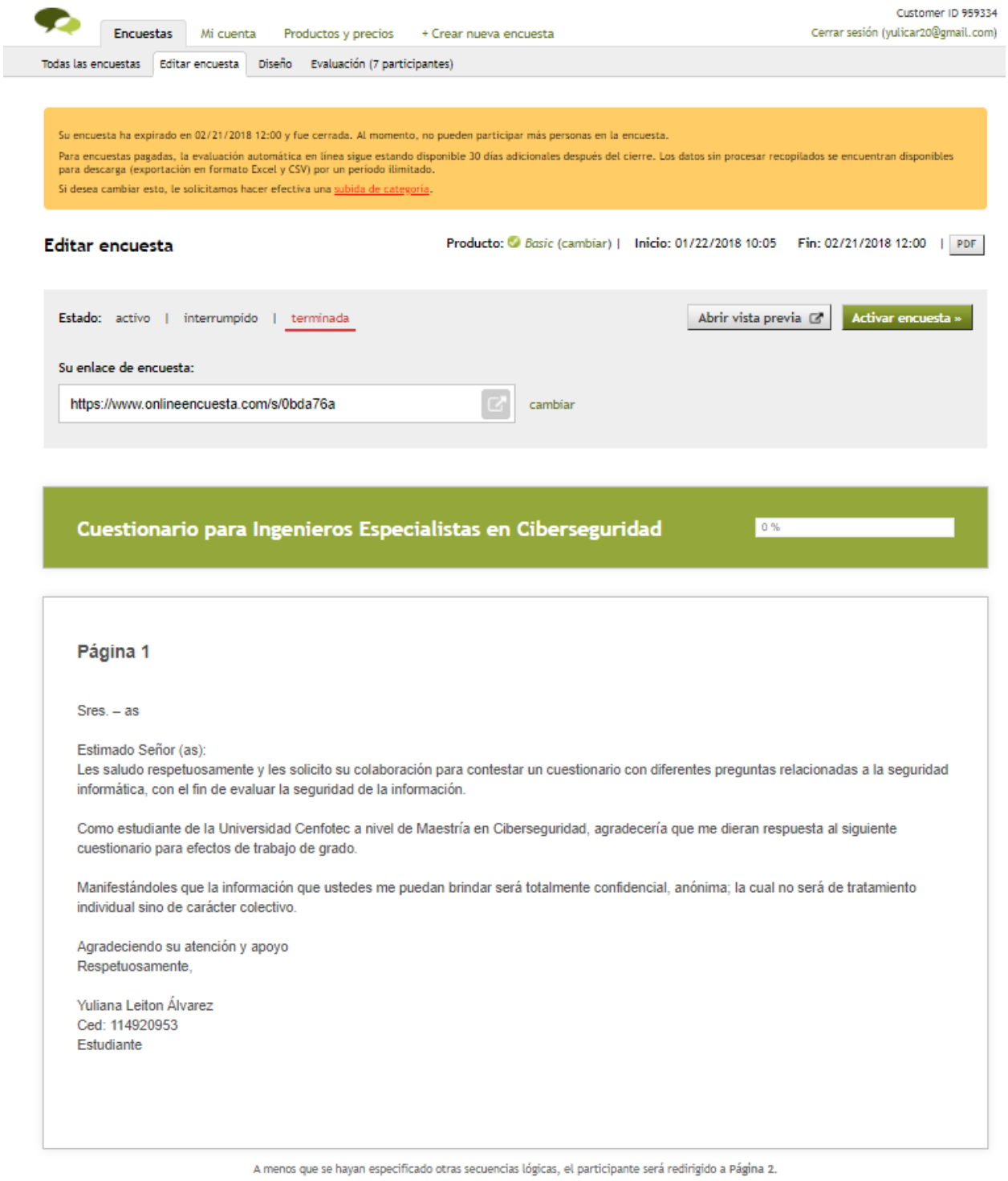
- ◯ sí » continuar con terminar la encuesta
- ◯ no

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 7**.

## Página 7

**En caso de que No, ¿qué mejoras son necesarias?** *

A menos que se hayan especificado otras secuencias lógicas, la encuesta **finalizará** después de esta página.


Customer ID 959334
Encuestas
Mi cuenta
Productos y precios
+ Crear nueva encuesta
Cerrar sesión (yulicar20@gmail.com)
Todas las encuestas
Editar encuesta
Diseño
Evaluación (7 participantes)
Su encuesta ha expirado en 02/21/2018 12:00 y fue cerrada. Al momento, no pueden participar más personas en la encuesta.
Para encuestas pagadas, la evaluación automática en línea sigue estando disponible 30 días adicionales después del cierre. Los datos sin procesar recopilados se encuentran disponibles para descarga (exportación en formato Excel y CSV) por un periodo ilimitado.
Si desea cambiar esto, le solicitamos hacer efectiva una subida de categoría.
Editar encuesta
Producto: basic (cambiar) | Inicio: 01/22/2018 10:05 Fin: 02/21/2018 12:00 | PDF
Estado: activo | interrumpido | terminada
Abrir vista previa
Activar encuesta »
Su enlace de encuesta:
https://www.onlineencuesta.com/s/0bda76a
cambiar
Cuestionario para Ingenieros Especialistas en Ciberseguridad
0 %
Página 1
Sres. – as
Estimado Señor (as):
Les saludo respetuosamente y les solicito su colaboración para contestar un cuestionario con diferentes preguntas relacionadas a la seguridad informática, con el fin de evaluar la seguridad de la información.
Como estudiante de la Universidad Cenfotec a nivel de Maestría en Ciberseguridad, agradecería que me dieran respuesta al siguiente cuestionario para efectos de trabajo de grado.
Manifestándoles que la información que ustedes me puedan brindar será totalmente confidencial, anónima; la cual no será de tratamiento individual sino de carácter colectivo.
Agradeciendo su atención y apoyo
Respetuosamente,
Yuliana Leiton Álvarez
Ced: 114920953
Estudiante
A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a Página 2.

## Página 2

**¿Considera que la incorporación de tecnología IoT involucra un reto mayor para el monitoreo constante ante amenazas? ***

- ◯ sí
- ◯ no

**¿Siendo usted especialista en el área de ciberseguridad, conoce las normas y reglamentos que velan por la seguridad de la información? ***

- ◯ sí
- ◯ no » continuar con Página 4

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 3**.

## Página 3

**¿Cuales? ***

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 4**.

## Página 4

**¿Considera que la ciudadanía costarricense está protegida a nivel legal en caso de acoso, robo o violación de la privacidad? ***

- ◯ sí
- ◯ no

**¿Se realiza monitoreo de dispositivos IoT tomando en cuenta cámaras, dispositivos biométricos o wereables conectados a la red interna de la empresa? ***

- ◯ sí
- ◯ no

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 5**.

## Página 5

**¿Considera que Costa Rica debería de tener una guía de seguridad de datos para los ciudadanos con el fin de garantizar el uso adecuado de la información? ***

- ◯ sí
- ◯ no

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 6**.

## Página 6

**¿Porque? ***

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 7**.

## Página 7

**¿Conoce usted los pilares de seguridad para IoT? ***

- ◯ sí
- ◯ no » continuar con Página 9

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 8.**

## Página 8

**¿Cuáles son? ***

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 9.**

## Página 9

**¿Considera que Costa Rica está preparada para afrontar los retos que involucra la aplicación de IoT en las áreas de aviación, infraestructura, automoción, telecomunicaciones, salud, entre otras? ***

- ◯ sí
- ◯ no

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 10.**

## Página 10

**¿Están los SOC preparados para visualizar este tipo de actividades por medio de monitoreo? ***

- ◯ sí
- ◯ no

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 11.**

## Página 11

**¿Conoce usted los fundamentos legales de la Ley No.8968 (LEY DE PROTECCIÓN DE LA PERSONA FRENTE AL. TRATAMIENTO DE SUS DATOS PERSONALES)? ***

- ◯ sí
- ◯ no

**¿Cómo especialista de seguridad, promueve usted el velar por que los empleados de su empresa conozcan sobre la protección de los datos? ***

- ◯ sí
- ◯ no

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 12.**

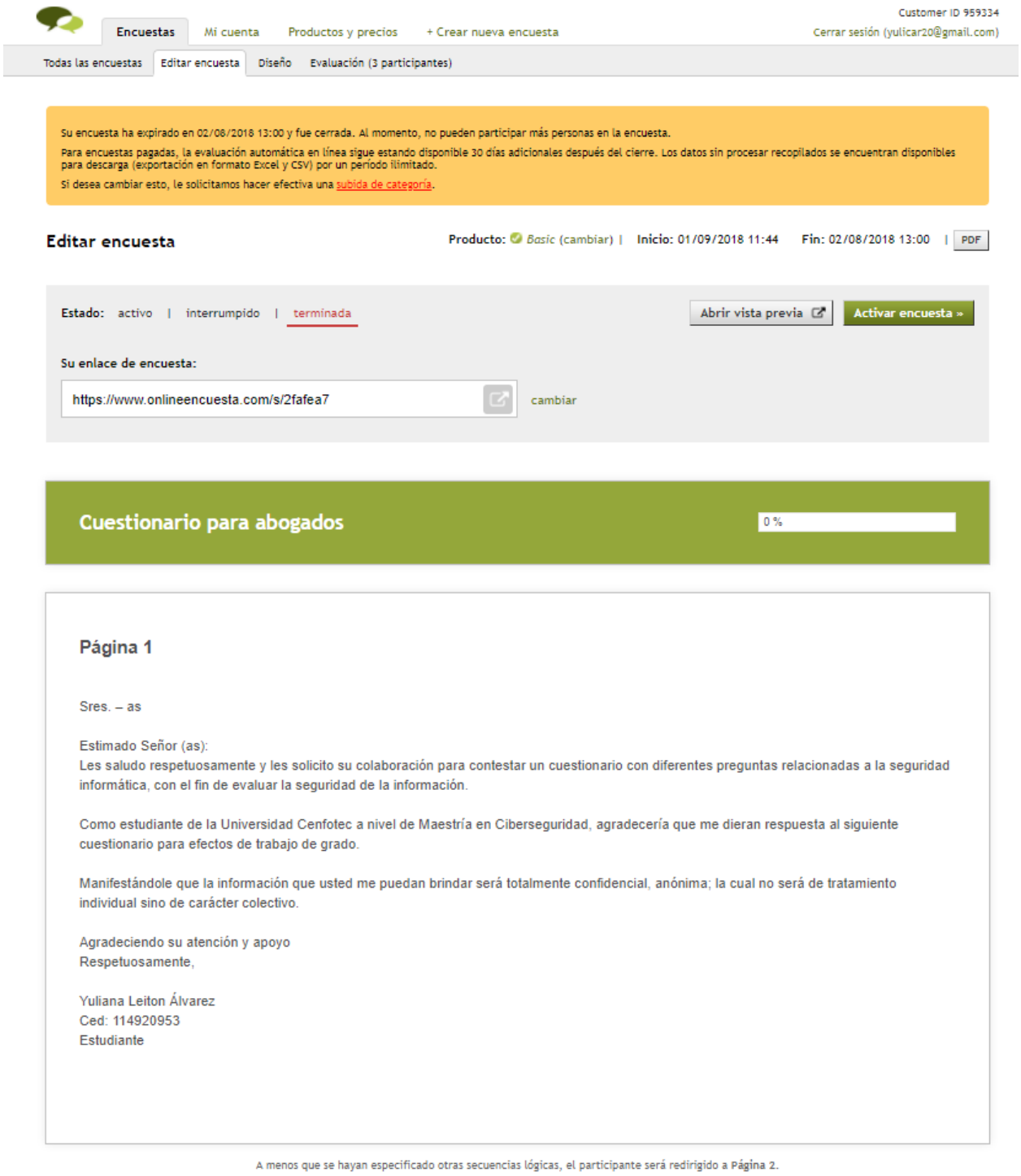
## Página 12

**Marque ¿Cuáles de las siguientes legislaciones son de efectiva aplicación para la seguridad de los datos en Costa Rica?** *

- [ ] Constitución Política
- [ ] Código Penal
- [ ] Código Civil
- [ ] Código de Comercio
- [ ] Código Laboral
- [ ] Ley N8968
- [ ] Ley Habeas Data
- [ ] Ley N8642 (Ley General de Telecomunicaciones)
- [ ] Ley General de Aduanas
- [ ] Ley de Administración Financiera de la República y Presupuestos Públicos
- [ ] Código de Normas y Procedimientos Tributarios

A menos que se hayan especificado otras secuencias lógicas, la encuesta **finalizará** después de esta página.

» Redirection to final page of Online Encuesta


Customer ID 959334
Encuestas
Mi cuenta
Productos y precios
+ Crear nueva encuesta
Cerrar sesión (yulicar20@gmail.com)
Todas las encuestas
Editar encuesta
Diseño
Evaluación (3 participantes)
Su encuesta ha expirado en 02/08/2018 13:00 y fue cerrada. Al momento, no pueden participar más personas en la encuesta.
Para encuestas pagadas, la evaluación automática en línea sigue estando disponible 30 días adicionales después del cierre. Los datos sin procesar recopilados se encuentran disponibles para descarga (exportación en formato Excel y CSV) por un período ilimitado.
Si desea cambiar esto, le solicitamos hacer efectiva una subida de categoría.
Editar encuesta
Producto: Basic (cambiar) | Inicio: 01/09/2018 11:44 Fin: 02/08/2018 13:00 | PDF
Estado: activo | interrumpido | terminada
Abrir vista previa
Activar encuesta »
Su enlace de encuesta:
https://www.onlineencuesta.com/s/2fafea7
cambiar
Cuestionario para abogados
0 %
Página 1
Sres. – as
Estimado Señor (as):
Les saludo respetuosamente y les solicito su colaboración para contestar un cuestionario con diferentes preguntas relacionadas a la seguridad informática, con el fin de evaluar la seguridad de la información.
Como estudiante de la Universidad Cenfotec a nivel de Maestría en Ciberseguridad, agradecería que me dieran respuesta al siguiente cuestionario para efectos de trabajo de grado.
Manifestándole que la información que usted me puedan brindar será totalmente confidencial, anónima; la cual no será de tratamiento individual sino de carácter colectivo.
Agradeciendo su atención y apoyo
Respetuosamente,
Yuliana Leiton Álvarez
Ced: 114920953
Estudiante
A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a Página 2.

## Página 2

¿Considera que en Costa Rica existen leyes y reglamentos que protegen los datos? *

- ◯ sí
- ◯ no » continuar con Página 4

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 3**.

## Página 3

¿Por qué? *

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 4**.

## Página 4

**Marque ¿Cuáles de las siguientes legislaciones son de efectiva aplicación para la seguridad de los datos en Costa Rica?** *

- [ ] Constitución Política
- [ ] Código Penal
- [ ] Código Civil
- [ ] Código de Comercio
- [ ] Código Laboral
- [ ] Ley N8968
- [ ] Ley Habeas Data
- [ ] Ley N8642 (Ley General de Telecomunicaciones)
- [ ] Ley General de Aduanas
- [ ] Ley de Administración Financiera de la República y Presupuestos Públicos
- [ ] Código de Normas y Procedimientos Tributarios
- [ ] Otra

**¿Se puede procesar legalmente a una persona física o jurídica que haga mal uso de los datos de sus clientes?** *

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 5**.

## Página 5

**¿Conoce usted personas que fueron procesadas por violación de la privacidad de los datos?** *

- ( ) sí
- ( ) no » continuar con Página 7

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 6**.

## Página 6

**Comente el caso** *

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 7**.

## Página 7

**¿Considera usted que la legislación existente es suficiente para tipificar y penalizar a personas que atenten contra la seguridad y privacidad de los datos?** *

- ( ) sí
- ( ) no » continuar con Página 9

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 8**.

## Página 8

**¿Por qué?** *

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 9**.

Página 9

**¿Considera que es suficiente la legislación existente para velar por la seguridad de las personas ante el uso discriminado de sus datos?** *

**¿Qué propiedades se violenta cuando se hace un mal uso de la información (puede marcar varias)** *

- [ ] Propiedad Intelectual
- [ ] Propiedad Financiera
- [ ] Propiedad Patrimonial
- [ ] Honor
- [ ] Riesgo Laboral
- [ ] Redes Sociales
- [ ] Acoso
- [ ] Estafa
- [ ] Extorsión
- [ ] Seguridad Residencial
- [ ] Acoso Financiero

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 10**.

## Página 10

**¿Considera que es legal la vigilancia por medio de dispositivos de seguridad? ***

| | SI | NO |
|---|---|---|
| Trabajo (Oficinas) | ☐ | ☐ |
| Trabajo Doméstico | ☐ | ☐ |
| Residenciales | ☐ | ☐ |
| Comercios | ☐ | ☐ |
| Escuelas | ☐ | ☐ |

**Considera usted que se puede pactar contractualmente la vigilancia continua y permanente de los trabajadores que desarrollan su labor en: ***

| | SI | NO |
|---|---|---|
| Industria | ◯ | ◯ |
| Oficinas Privadas | ◯ | ◯ |
| Oficinas Gobierno | ◯ | ◯ |
| Escuelas privadas | ◯ | ◯ |
| Escuelas públicas | ◯ | ◯ |
| Hogar | ◯ | ◯ |
| Residenciales | ◯ | ◯ |
| Zona de juegos de niños | ◯ | ◯ |
| Gimnasios | ◯ | ◯ |

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 11.**

## Página 11

**¿Conoce usted casos en que la misma seguridad se convierte en una potencial amenaza ante: delincuencia, denuncias, pedofilia, violencia sexual, violencia doméstica, entre otros? Comentelo a continuacion de lo contrario ponga NO y continue a la siguiente pregunta** *

**¿Se puede obligar a un comercio, industria, residencial, entre otros, a dar la información grabada (imágenes, audio-video) en las cámaras de vigilancia para alguna investigación?** *

- sí
- no » continuar con Página 13

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 12**.

## Página 12

**¿Por qué?** *

A menos que se hayan especificado otras secuencias lógicas, el participante será redirigido a **Página 13**.

## Página 13

**Escenario #1: Comente el siguiente escenario.**
**Hay una familia que tiene vigilancia 24x7 en el hogar en la cual continuamente se monitorean muchas zonas de la casa. La pareja constantemente tiene discusiones y en varias ocasiones la esposa se ha visto expuesta a las agresiones por parte del esposo en donde involucra violencia doméstica y psicológica.**
**La esposa recuerda que en su casa hay cámaras y decide presentar una denuncia de violencia doméstica contra su esposo presentando dichos videos.** *

¿Puede tomar estos datos como evidencia? Si o no, ¿Por qué?
¿Se ve violentada la privacidad del esposo?

A menos que se hayan especificado otras secuencias lógicas, la encuesta **finalizará** después de esta página.

» Redirection to final page of Online Encuesta