

Universidad Cenfotec.

Maestría en Ciberseguridad.

Documento Final de Proyecto de Investigación Aplicada 2.

Internet de las cosas y los riesgos para la privacidad causados por el rastreo satelital (GPS) por medio de torres telefónicas.

Cambronero Sánchez Carlos Raúl.

Hernández Ugarte Marcela.

Febrero 2018

Declaratoria de derechos de autor.

Prohibida la reproducción total o parcial de este proyecto de investigación sin previo permiso de los autores por un periodo de cinco años (2018-2023), luego de cumplido este periodo se autoriza su uso solamente para fines académicos.

Dedicatoria.

Dedico este proyecto de tesis a Dios por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos. A mis padres por ser el pilar fundamental en todo lo que soy, en toda mi educación, tanto académica, como de la vida, por su incondicional apoyo perfectamente mantenido a través del tiempo. Todo este trabajo ha sido posible gracias a ustedes, los amo.

A mi compañero de tesis, gracias por el apoyo y el trabajo en equipo que hicimos para desarrollar con éxito este proyecto.

A mis profesores y todas aquellas personas que de una u otra forma hicieron posible los resultados y culminación de este proyecto.

Marcela Hernández Ugarte.

Este Proyecto de graduación se lo dedico a mi padre Carlos Luis Cambronero quien ha trabajado muy fuerte para sacar adelante nuestra familia y siempre ha estado presente para darme los mejores consejos en el tiempo correcto.

A mi madre Giselle Sánchez Ulate quien es un ejemplo de superación y lucha y que con su amor se preocupó para que me pudiera superar en el tiempo.

A mi novia Sandra Villamil Beltrán quien ha sido una compañera de vida, me brindó su tiempo, dedicación y consejos; además, me impulsó y apoyó en este y muchos proyectos más.

Muchas gracias a todos.

Carlos Raúl Cambronero Sánchez.

Hoja de Aprobación del Proyecto

Tabla de contenido

1. Introducción 10
1.1 Definición y antecedentes del problema 10
1.2 Justificación del proyecto 10
1.3 Objetivos 12
1.3.1 Objetivo general 12
1.3.2 Objetivos específicos 13
1.4 Alcance del proyecto 13
1.5 Limitaciones 14
1.6 Estado de la cuestión 14
2. Marco teórico 18
2.1. Internet de las cosas 18
2.1.1 Origen del Internet de las Cosas 18
2.1.2 Protocolos del IoT 18
2.1.3 Dificultades del IoT 19
2.1.4 Desventajas del Internet de las cosas 20
2.1.5 Cantidad de dispositivos conectados al internet 21
2.1.6 Ciudades inteligentes 22
2.1.7 Vulnerabilidades y ataques 23
2.2 Privacidad 24
2.2.1 Conceptos 24
2.2.2 Riesgos 25
2.3 Legislación en Costa Rica 25
2.3.1 Ley Nº 8968: Protección de la Persona frente al tratamiento de sus datos personales. 25
2.3.2 Ley General de Telecomunicaciones 27
2.3.3 Reglamento de medidas de protección de la privacidad en telecomunicaciones 28
2.4 Tecnología Móvil 29
2.4.1 Telefonía Móvil 29
2.4.2 Sistema de Posicionamiento Global (GPS) 31
2.5 ISO IEC 27001 35

2.5.1 ¿Qué es ISO? 35
2.5.2 ISO IEC 27001 35
2.5.3 ¿Qué es un SGSI? 36
2.5.4 Modelo Planear-Hacer-Verificar-Actuar 37
3. Marco Metodológico 39
3.1 Contexto del lugar donde se realiza el proyecto 39
3.2 Información general de la institución donde se realiza el proyecto 39
3.2.1 Misión: 39
3.2.2 Visión: 39
3.2.3 Valores: 40
3.3 Procedimiento Metodológico 40
3.3.1 Tipo de investigación 40
3.3.2 Diseño de la investigación 40
3.3.3 Enfoque de la investigación 41
3.4 Técnicas e instrumentos de recolección de datos 41
3.4.1 Entrevista 42
3.4.2 Técnica de observación 42
3.5 Fuentes de información 42
3.6 Procedimientos para la elaboración del proyecto 43
4. Propuesta y Resultados 45
4.1 Resultados 45
4.1.1 Riesgos para la privacidad 45
4.1.2 Implicaciones Legales 56
Propuesta 58
4.2 Pruebas de Penetración 58
4.2.1 Objetivos de una prueba de penetración 61
4.2.2 Requerimientos mínimos para la creación de un laboratorio de Pruebas de Penetración 61
4.2.3 Requisitos de software especializado para evaluación de vulnerabilidades y pruebas de penetración 63
4.2.4 Pasos para efectuar un buen plan de pruebas de penetración 65
4.3 Hallazgos 70
5. Diagnóstico 72

Conclusiones 83
Recomendaciones 86
Glosario de términos 87
Bibliografía 92
Anexos 96

Lista de ilustraciones y cuadros.

Imagen 1-Internet de las cosas……. 21

Imagen 2- Ejemplo de interrelación entre sistemas……. 22

Imagen 3 – Ejemplo archivos CDR……. 31

Imagen 4- Geolocalización……. 33

Imagen 5. Situaciones útiles o inquietantes…….. 48

Imagen 6. Trayectoria proyectada por medio de geolocalización……. 51

Imagen 7: Infraestructura segura……... 63

Imagen 8: Infraestructura segura……. 63

Tabla 1: Diferencia entre escaneo de vulnerabilidades y pruebas de penetración……... 60

¿Cómo se puede mitigar el riesgo a la privacidad en las telecomunicaciones que impliquen dispositivos IoT conectados a redes de datos móviles?

Capítulo I

Introducción

1. Introducción

1.1 Definición y antecedentes del problema

A través de los años la tecnología ha venido evolucionando rápidamente y poco a poco interactúa más con las personas. En la actualidad existen millones de dispositivos conectados a internet, y según varios estudios para el 2020 podrían existir alrededor de 50 mil millones de dispositivos interconectados, creando lo que se conoce como internet de las cosas, o IoT (Internet of Things) por sus siglas en inglés. La mayoría de la población interactúa de alguna u otra manera con uno de estos dispositivos, ya sea mediante un celular, vehículo inteligente, casas inteligentes o Smart TVs, entre muchas otras cosas.

A pesar de la simplicidad y las ventajas que se obtienen del uso de esta tecnología, nos encontramos con puntos críticos que involucra su uso, como lo son la privacidad y la seguridad. Los desarrolladores y productores de este tipo de tecnologías no se preocupan por estos 2 puntos tan importantes, y lamentablemente existen personas mal intencionadas dispuestas a encontrar portillos que les permitan poder ingresar a estos dispositivos y robar información personal, espiar o bien utilizarlos para causar ataques a grandes corporaciones, y logran dañar la integridad e imagen de sus víctimas.

1.2 Justificación del proyecto

Los avances tecnológicos de la actualidad abarcan muchas áreas, sin embargo, se han notado avances muy acelerados en los últimos años en áreas tales como la comunicación y tecnologías de la información. La Internet y los servicios que a través de ella se prestan se han convertido en un elemento imprescindible para nuestras vidas. Además, la explosión de la conectividad ubicua o red 3.0 mediante el uso masivo de dispositivos móviles inteligentes, especialmente los Smartphone,

y redes de datos móviles cada vez más rápidas, hacen que todos estos servicios se puedan consumir en cualquier lugar y a cualquier hora del día.

En buena parte de los casos, los servicios más usados en la red se prestan gracias a la cantidad de información y datos personales que los usuarios aportamos, tanto a las empresas que ofrecen los servicios como a otros usuarios, por lo que debemos ser conscientes de los riesgos que esto puede suponer para nuestra seguridad y privacidad.

La privacidad y seguridad son dos términos que van de la mano, y estos al ser utilizados de la mejor manera nos llevan al camino del buen uso de internet y las nuevas tecnologías. El gran problema hoy en día es que la protección de la privacidad no solo depende de los usuarios, sino también de las compañías que ofrecen servicios, como por ejemplo compañías telefónicas, las cuales recolectan datos acerca de nuestra vida, dónde vamos, con quién estamos, a quién llamamos, dónde dormimos, dónde vivimos. Toda esta información no sabemos si está siendo bien manipulada, no sabemos si estos datos se brindan a ciertas empresas con fines lucrativos, pero la pregunta más importante es si esta información puede ser brindada a cada persona que la solicite.

Conociendo los lugares que una persona visita, la frecuencia con que lo hace, y el tiempo que permanece, se obtiene información que está reservada al ámbito exclusivo de la privacidad y de la intimidad. Siguiendo los movimientos de una persona, una empresa se puede dar cuenta de si pertenece a un grupo religioso, determinados hábitos personales, apoyo a grupos políticos, orientación sexual, etc.

En el ambiente personal, la privacidad es importante debido a que es un derecho que tenemos y es parte de la Declaración Universal de los Derechos Humanos, con esto se busca respetar la intimidad y secretos de las personas. Por su parte, en el ambiente laboral, ayuda a preservar secretos corporativos y permite conservar la competitividad empresarial, todo esto ayuda a que la competencia no obtenga información que eventualmente pueda usar para elaborar estrategias y obtener ventajas en el mercado.

El análisis se llevará a cabo por medio de recolección de información y entrevistas a personas involucradas en el tema de la privacidad en Costa Rica, y así también se solicitará información a una empresa telefónica del país para así poder limitar el alcance del proyecto.

Se requerirá analizar archivos de tipo IPDR y CDR, los cuales son los que almacenan diversos tipos de metadatos como: la ubicación, nombre de persona y número telefónico, entre otro tipo de datos de abonados de un ISP. Estos archivos son almacenados según la oficina y área, generalmente se guardan bajo el formato de ubicación, año, mes, día, hora, minuto y segundo. Por ejemplo, WA20170504174018.dat o ALASUR20170807195500.rec, son de tipo plano, lo que significa que están compuestos de texto sin formato.

Los resultados que se quieren obtener son los siguientes:

- Riesgos del uso de GPS en telefonía móvil.
- Identificar la existencia de un manual de buenas prácticas para la manipulación de datos almacenados por empresas telefónicas.
- Forma en que se resguardan los archivos IPDR y CDR.
- Acceso a la información recopilada por ISPs.
- Riesgos a la privacidad y seguridad de los usuarios.

1.3 Objetivos

1.3.1 Objetivo general

Analizar el impacto a la privacidad que causan los dispositivos móviles (IoT) en las redes de datos de telefonía, por medio del análisis de los datos de geolocalización en los archivos IPDR y CDR recolectados por empresas telefónicas que brindan servicios en Costa Rica, para detectar posibles riesgos a la intimidad en la población.

1.3.2 Objetivos específicos

- Investigar los requisitos y/o pasos necesarios para la ejecución de pruebas de penetración, para poder examinar la infraestructura crítica que resguarda los archivos IPDR y CDR.
- Analizar los riesgos a la privacidad a los que están expuestos los usuarios de aplicaciones móviles que utilizan el servicio de ubicación por medio de dispositivos IoT.
- Crear una propuesta de buenas prácticas con normas y estándares de seguridad de la información para el resguardo de los datos de la infraestructura tecnológica de la organización.
- Evaluar los archivos de IPDR y CDR almacenados por las empresas telefónicas generados por dispositivos de IoT para la determinación de posibles riesgos de la privacidad de la población costarricense.
- Valorar las implicaciones legales a las que se enfrentan las empresas que recolectan estos datos y los almacenan durante cierta cantidad de tiempo sin el conocimiento de los usuarios.

1.4 Alcance del proyecto

Con este proyecto se quiere demostrar si la población costarricense se enfrenta a posibles riesgos en su privacidad por el uso del GPS en dispositivos móviles, debido a que las empresas telefónicas capturan información mediante las redes móviles. El análisis de archivos IPDR y CDR ayudará a identificar qué información sensible podría estar siendo expuesta a personas no autorizadas, lo que permitirá identificar si existen implicaciones legales en nuestro país de que dichas compañías telefónicas capturen estos datos

1.5 Limitaciones

Durante el desarrollo del trabajo de investigación podrían surgir diversas limitaciones que afectan la estructura y el desarrollo del plan de trabajo, con ello generar retrasos en los entregables. A continuación, se presenta una lista de posibles factores externos que podrían provocar demoras durante la gestión del proyecto de graduación:

- Dependencia total de la información suministrada por el ISP.
- Poco compromiso por parte de los encargados del departamento DCTI como un proyecto relevante dentro de la estrategia de la organización.
- Pocas sesiones de seguimiento con los interesados del proyecto para el diseño del documento de buenas prácticas.
- No se contempla la implementación del documento de buenas prácticas en un ambiente de producción, debido al poco tiempo con que se cuenta (4 meses).

1.6 Estado de la cuestión

En el año 2007 el Parlamento Europeo votó por unanimidad apoyar la revolución del Internet de las Cosas (conocido como la cuarta revolución industrial), la cual fue considerada como el nuevo tsunami que revolucionará al mundo. Las otras grandes potencias mundiales como China y Estados Unidos ya habían ingresado en ese mundo y habían estado invirtiendo en esta tecnología por mucho tiempo atrás. Para los países en vías de desarrollo como Costa Rica, este es un tema que apenas inicia y se comienza a entender su potencial y beneficios para la población en general.

Para el año 2016, un medio de comunicación llamado Costa Rica 2050 conversó con el ministro de Ciencia y Tecnología Marcelo Jenkins y con la viceministra Ana Helen Chacón encargada del consejo Presidencial de Innovación y Talento Humano, quienes aseguraron que el país debe hacer esfuerzos mayores para poder impulsar esta tecnología y así promover la apertura de nuevos negocios, sin embargo, se recalcó que en el país este tema está en “pañales”. Según mencionan,

IoT es sumamente importante para el consejo de innovación y talento humano debido a que podría mejorar los sectores de salud, transporte, agropecuario, manufacturero, e inclusive vida personal.

A finales del año 2015, el Instituto Tecnológico de Costa Rica (TEC) anunció la alianza con PTC, la empresa líder mundial en Internet de las Cosas, con el fin de crear el primer centro mundial de excelencia para formar ingenieros en IoT. También esta institución trabaja en la creación de un centro de investigación en sistemas inteligentes, estos 2 centros podrían ser la clave para que el país empiece a crecer en esta tecnología tan importante e impactante a nivel mundial.

Existen firmas locales que se unieron para la creación de un consorcio que permita desarrollar nuevas tecnologías de IoT, esta iniciativa es liderada por las compañías Mecsoft, Controlsoft, Lantern Technologies y Tecnoinso, entre otras. La idea principal es poder crear soluciones en sistemas inteligentes enfocados a carros, edificios, viviendas y ciudades inteligentes. Lamentablemente estas iniciativas no cuentan con el apoyo suficiente, esto porque en Costa Rica se desconocen los beneficios que se derivan de la implementación de estos dispositivos. Al menos en el sector público se sabe que la Caja Costarricense de Seguro Social (CCSS) ha estado sacando provecho de los beneficios que se ofrecen actualmente para poder implementar servicios nuevos, como solicitud de citas médicas en teléfonos celulares y obtención de expedientes en diversos dispositivos móviles.

Para que la población costarricense logre sacar provecho de todo el potencial que ofrece el IoT, debe mejorar la conectividad de internet, esto implica la velocidad y calidad de la transmisión de datos. Además, se deben desarrollar estrategias de seguridad cibernética y regulaciones de privacidad de datos, así como establecer precios de servicios de internet más accesibles.

Si bien es cierto IoT brinda múltiples beneficios para facilitar el diario vivir, también afecta mucho la privacidad. Para nadie es un secreto que las empresas telefónicas de nuestro país recaudan información de nuestra vida, dónde estamos cada minuto, qué lugares visitamos, con quién estamos regularmente y hasta a qué hora dormimos. Entonces nacen varias preguntas, ¿qué sucede con todos esos datos

que recaudan estas empresas?, ¿estarán resguardados?, ¿quién manipula mis datos? ¿Para qué necesitan estas empresas estos datos? Y de todas estas preguntas, nace una más importante, ¿dónde queda la privacidad de cada uno de nosotros?

En nuestro país existe la Agencia de Protección de Datos de los Habitantes (PRODHAB), en donde Mediante Ley N° 8968 de 7 de julio del 2011 y publicada en el Diario Oficial La Gaceta No. 170 del 5 de setiembre del 2011, se promulgó la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales. Su primer Reglamento fue creado mediante Decreto Ejecutivo No. 37554-JP del 30 de octubre del 2012 y publicado en el Alcance No. 45 del Diario Oficial La Gaceta del 5 de marzo del 2013.

El principal objetivo de este organismo es garantizarle a cualquier persona el respeto y derecho a la privacidad, así como la defensa a la libertad. Esto es sumamente importante debido a la gran cantidad de datos que recolectan los dispositivos y sensores de IoT, donde en muchas ocasiones nuestra privacidad se podría ver comprometida.

De igual forma existen algunas leyes y regulaciones que definen la manera en que se deben tratar o manipular estos datos, esta información la definiremos en el siguiente apartado.

Capítulo II

Marco Teórico

2. Marco teórico.

2.1. Internet de las cosas.

2.1.1 Origen del Internet de las Cosas.

El origen de los objetos conectados no es un suceso de hace pocos años, según estudios este tipo de acciones se remonta alrededor del siglo XIX donde se consideran los primeros experimentos en telemetría de la historia. En 1874 científicos franceses instalaron dispositivos de información meteorológica en la cima del Mont Blanc (punto más alto de la unión europea). Por medio de un enlace de radio de onda corta la información se enviaba hasta París donde eventualmente los datos eran analizados y estudiados por los científicos (Cendon, 2017).

Según Cendon (2017), en 2009 fue cuando se usó por primera vez la expresión de Internet of Things, la cual surgió del profesor del MIT Kevin Ashton. Desde ese momento el crecimiento y expectación del término ha crecido exponencialmente.

El año 2014 es el año del Internet de las Cosas según una feria de tecnología, donde se exponía que el mejor escenario eran objetos conectados dando aparición a diversos dispositivos inteligentes. Este tipo de tecnología fue fundada con la idea de que cuando objetos con los que el ser humano está en constante interacción se conectan a internet, cosas interesantes pueden suceder, esto incluye la posibilidad de poner relacionarnos y tener un mejor control sobre estas cosas.

2.1.2 Protocolos del IoT.

Tres de los protocolos más utilizados actualmente por el IoT son XMPP, MQTT y COAP.

XMPP: Protocolo extensible de mensajería y presencia, es un protocolo abierto utilizado para mensajería instantánea el cual ha sido utilizado por compañías como Google y Facebook. Fue desarrollado en 1998 y se le conocía como Jabber, en la

actualidad este protocolo soporta mensajería instantánea, videoconferencia, transferencia de archivos y hasta vista de estados de usuarios, aplicaciones tales como WhatsApp, Facebook y Messenger son algunos de los ejemplos donde podemos encontrar la implementación de XMPP. Su funcionamiento se encuentra bien documentado y trabaja en ambientes descentralizados (González, 2014).

MQTT: Su nombre proviene de MQ Telemetry Transport (Transporte de telemetría de cola de mensajes). Este protocolo se desarrolló para redes de bajo ancho de banda, problemas de latencia o poco confiables. Su fin principal es intentar la confiabilidad y seguridad a las diversas aplicaciones y dispositivos que lo utilizan. Su mayor desventaja es que no trabaja en tiempo real, lo que genera que las aplicaciones que lo utilizan se hagan lentas (Arrow, 2015).

COAP: Es un protocolo lanzado por la IETF en 2013, es un protocolo RESTful (arquitectura cliente/servidor sin estado donde los recursos están identificados por URIs), el cual está alineado con el protocolo HTTP. Utiliza UDP, lo que significa que muchas respuestas se intercambian asincrónicamente. Generalmente es utilizado en ambientes web (Arrow, 2015).

2.1.3 Dificultades del IoT.

Debido a que la industria del IoT crece día con día se da paso a nuevas tecnologías, aplicaciones y servicios generando que nos vayamos encontrando con inconvenientes que eventualmente podría materializarse en serios problemas para sus usuarios.

- Seguridad y privacidad: Muchos de los dispositivos que se fabrican en la actualidad carecen de seguridad en su arquitectura lo que puede dar paso a infecciones o vulnerabilidades en la red donde se utilizan.
- Limitación de recursos: Cada dispositivo debe gestionar su propia energía y capacidad de almacenamiento.

- Heterogeneidad: Considerada una de las principales limitaciones del internet de las cosas, debido a que existen muchos fabricantes y se requiere que todos los objetos interactúen y logren hablar el mismo idioma.
- Plug and play: Una de las características del IoT es que en su mayoría los dispositivos entran en funcionamiento tan pronto se conectan a una red, lograr que todas estas cosas mediante un proceso automático logren interactuar con otros objetos sin la necesidad de intervención humana es un gran desafío.

2.1.4 Desventajas del Internet de las cosas.

- Compatibilidad: No existe un concepto uniforme o estándar como el que tiene USB o Bluetooth.
- Seguridad: El software utilizado por muchos de los dispositivos tiene muchas probabilidades de ser hackeado, lo que genera múltiples riesgos para sus usuarios.
- Privacidad: Es una de las grandes interrogantes del IoT, en su mayoría los datos no se encuentran cifrados.
- Mantenimiento: Muchos de los fabricantes de estos dispositivos se “olvidan” de hacer actualizaciones al software, lo que podría generar que se encuentren diversas vulnerabilidades.

2.1.5 Cantidad de dispositivos conectados al internet.

En la siguiente imagen, se establece que, en el 2003, la población mundial era aproximadamente de 6,3 mil millones de personas y un total de 500 millones de dispositivos conectados a Internet, lo que en porcentaje sería 0.8 dispositivos por persona. Estos índices aumentan luego de que Steve Jobs, presenta el iPhone en el 2007, lo que elevó el uso de los smartphones y tablets. En el 2010, 12,5 mil millones de dispositivos estaban conectados al Internet, donde se observa que el porcentaje varía de 0,8 en el 2003 a 1,84 en solo 7 años. Cisco IBSG prevé que habrá 25 mil millones de dispositivos conectados a Internet para 2015, y 50 mil millones para 2020 (Evans, 2011).

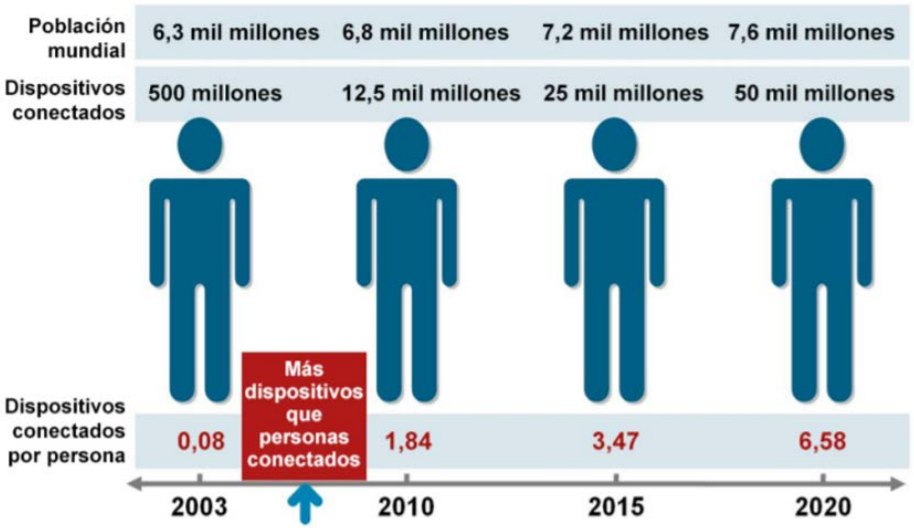


Imagen 1-Internet de las cosas. Fuente: Cisco IBSG, abril 2011.

Olguín (2016) establece que, en el 2020, serán 50 mil millones de dispositivos conectados al internet, lo que equivale a 6 veces la población en el planeta para ese entonces. Esto porque cada persona tiene diversos dispositivos, como celular, computadora, tablet, entre otros, lo que concuerda con lo establecido por Cisco en el 2011. Además, establece que actualmente pueden haber cerca de 22 mil millones de dispositivos digitales conectados a Internet.

2.1.6 Ciudades inteligentes.

Cuando se genera el proceso de urbanización, se debe tener un control político y económico, además es necesario que la ciudad cumpla con las necesidades mínimas de la población, como el transporte, el agua, la energía, las comunicaciones, la prestación de servicios a empresas y ciudadanos. Lo anterior hace necesario que para poder aprovechar las oportunidades y garantizar un crecimiento sostenible, las ciudades tendrán que aprender a ser "inteligentes" (Dirks, n.f). Esto concuerda con Paniagua (2017), quien establece que la base de las ciudades inteligentes es la tecnología de la información y comunicación, ya que hacen que funcionen de forma más eficiente y ordenada.

En la siguiente imagen se establece la interrelación que debe tener una ciudad inteligente, y se observan los diversos componentes esenciales de estos sitios:

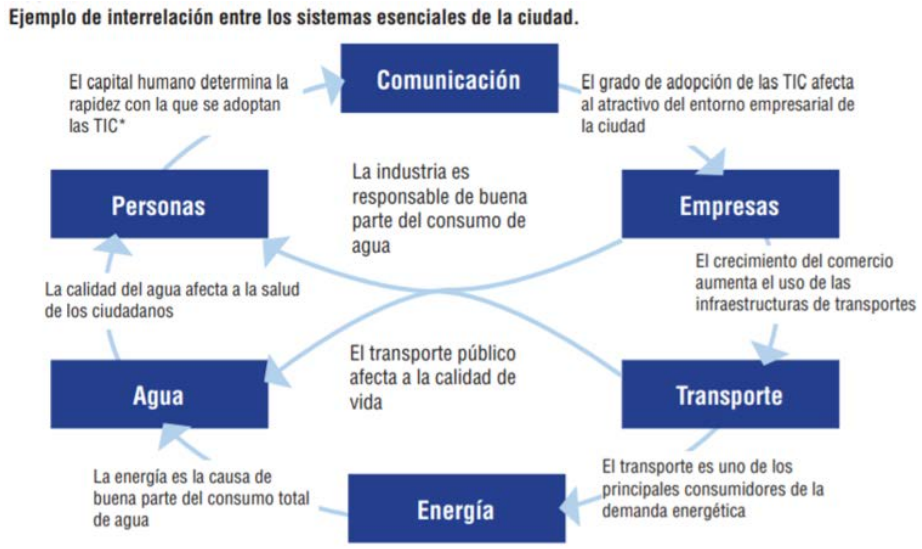


Imagen 2- Ejemplo de interrelación entre sistemas. Fuente: Análisis de IBM Center.

Los dispositivos IoT son fundamentales para el desarrollo y funcionamiento de estas ciudades, se prevé que para el año 2020 el 40% de los datos globales procederán de los sensores de estos equipos (Cisco, 2014).

2.1.7 Vulnerabilidades y ataques.

La reducción del tamaño de los dispositivos electrónicos, y su disminución en el precio ha permitido que las máquinas logren conectarse a internet, desde aires acondicionados, televisores, hasta el funcionamiento de grandes trenes, lo que hace que este tipo de tecnologías como IOT necesite seguridad y privacidad.

Una de las amenazas más probables son los códigos “zero-day”, los cuales tienen la capacidad de aprovechar vulnerabilidades de los dispositivos, un ejemplo son los televisores inteligentes, los cuales son capaces de transmitir conversaciones por medio del mismo micrófono por el que reciben instrucciones. Incluso se puede observar en el campo médico, ya que existen dispositivos que los usuarios deben llevar puestos como tratamiento de una enfermedad y al igual que los televisores pueden ser vulnerados (Vásquez, 2016).

Akamai realizó un estudio sobre la seguridad de los dispositivos IoT, en donde destaca que las cámaras y los routers son canales idóneos por el que los hackers puedan lanzar una serie de ataques vía botnets que impactan la seguridad de las empresas. Los DDoS o ataques de denegación de servicio son los más conocidos y, según Akamai, se incrementaron considerablemente en el último trimestre del año pasado, lo preocupante es que los ataques alcanzaron más de 100Gbps, lo que causa gran preocupación en la industria tecnológica (Manaure, 2017).

Durante el año pasado, los dispositivos IoT no protegidos, se convirtieron en el caldo de cultivo para el nacimiento de una serie de ataques, entre los que destacaron Mirai y Spike, los más peligrosos con más de 300Gbps por Botnet (Manaure, 2017).

El uso de phishing por los ciberdelincuentes es cada vez más frecuente y más sofisticado con el fin de engañar tanto a las empresas como a los usuarios, lo que seguirá siendo una amenaza para todos los que utilicen algún tipo de dispositivo IoT (Partner, 2017).

Toda aquella persona que posea algún tipo de IoT puede llegar a ser vulnerada. Los hackers pueden llegar a utilizar dispositivos como los monitores de bebés para atacar la web de otra persona u otro dispositivo que este dentro de la red

doméstica como las computadoras portátiles que contienen datos personales importantes (Partner, 2017).

Actualmente se encuentran más exploits en el internet basado en PowerShell, uno de los diversos lenguajes existentes de scripting. También se observan ataques que utilizan técnicas de penetración y herramientas administrativas, que ya existen en la red de la víctima, sin necesidad de levantar sospechas (Partner, 2017).

2.2 Privacidad.

2.2.1 Conceptos.

2.2.1.1 Privacidad.

Según la definición de la Real Academia, la privacidad es el ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión.

La protección de datos, también llamada privacidad de información es el aspecto de la tecnología de la información (TI) que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos en un sistema informático pueden ser compartidos con terceros.

2.2.1.2 Intimidad.

La intimidad es la preservación del sujeto y sus actos del resto de seres humanos, pero también se refiere a la característica de un lugar que invita a este estado del ser humano. La intimidad a veces se relaciona con anonimato, a pesar de que por lo general es más preciada por las personas que son más conocidas por el público. La intimidad puede ser entendida como un aspecto de la seguridad, en el cual el balance entre los intereses de dos grupos puede ponerse en evidencia.

2.2.2 Riesgos.

El crecimiento de la cantidad de cosas conectadas genera muchas dudas sobre el derecho a la privacidad e intimidad de las personas, y abre un debate necesario y urgente sobre el tema. La tecnología avanza día con día de manera que facilita la vida de las personas, pero es muy importante que se valore el balance entre los beneficios y los perjuicios de estos avances tecnológicos. Hoy en día los aparatos electrónicos nos rastrean, escuchan nuestras conversaciones, miden nuestro ritmo cardiaco y en general, si lo permitimos, pueden controlar nuestras vidas.

Algunos de los riegos a los que nos exponemos son los siguientes:

- Información personal en manos de terceros.
- Ingeniería Social.
- Mal uso de la tecnología.
- Rastreo de personas.

2.3 Legislación en Costa Rica.

En Costa Rica existen varios documentos legislativos en los cuales apoyaremos nuestra investigación. En ellos se indica el tratamiento que se debe de dar a los datos personales de los ciudadanos y el cuidado que se debe tener a la hora de utilizar los mismos. Mucha de esta información es utilizada para resolver problemas legales relacionados con la privacidad y las tecnologías de información, específicamente tecnología móvil.

2.3.1 Ley Nº 8968: Protección de la Persona frente al tratamiento de sus datos personales.

La ley de Protección de la Persona frente al tratamiento de sus datos personales define en su artículo 3 los datos personales como “cualquier dato relativo a una persona física identificada o identificable”. En sus artículos se define la forma en

que deben ser tratados estos datos, a continuación, mencionaremos algunos de los artículos relacionados con la investigación.

ARTÍCULO 5.- Principio de consentimiento informado

El artículo 5 define la obligación de informar a las personas titulares cuando se soliciten datos de carácter personal, de igual forma se debe indicar los destinatarios de la información, así como de quiénes podrán consultarla. También se debe informar el tratamiento que se dará a los datos recolectados o solicitados.

Quien recopile datos personales deberá obtener el consentimiento expreso de la persona titular de los datos o de su representante. Este consentimiento deberá constar por escrito, ya sea en un documento físico o electrónico, el cual podrá ser revocado de la misma forma, sin efecto retroactivo.

Se prohíbe el acopio de datos sin el consentimiento informado de la persona, o bien, adquiridos por medios fraudulentos, desleales o ilícitos.

ARTÍCULO 7.- Derechos que le asisten a la persona.

El artículo 7 se refiere al derecho que tiene toda persona al acceso de sus datos personales, rectificación o supresión de estos y a consentir la cesión de sus datos.

La persona responsable de la base de datos debe cumplir lo solicitado por la persona, de manera gratuita, y resolver en el sentido que corresponda en el plazo de cinco días hábiles, contado a partir de la recepción de la solicitud.

ARTÍCULO 10.- Seguridad de los datos.

El artículo 10 indica que el responsable de la base de datos deberá adoptar las medidas de índole técnica y de organización necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, dichas medidas deberán incluir, al menos, los mecanismos de seguridad física y lógica más adecuados de acuerdo con el desarrollo tecnológico actual, para garantizar la protección de la información almacenada.

Si las bases de datos que no reúnen las condiciones que garanticen la seguridad e integridad de los datos, no podrán registrar datos personales.

2.3.2 Ley General de Telecomunicaciones.

Por su parte la Ley General de Telecomunicaciones define la forma en que deben protegerse las redes de datos. Esta ley indica lo siguiente referente a la privacidad en su artículo 42:

> *"Los operadores y proveedores deberán adoptar las medidas técnicas y administrativas idóneas para garantizar la seguridad de las redes y sus servicios. En caso de que el operador conozca un riesgo identificable en la seguridad de la red, deberá informar a la Sutel y a los usuarios finales sobre dicho riesgo."*

Por lo tanto, los operadores y proveedores deberán garantizar que las comunicaciones y los datos de tráfico asociados a ellas, no serán escuchadas, gravadas, almacenadas, intervenidas ni vigiladas por terceros sin su consentimiento, salvo cuando se cuente con la autorización judicial correspondiente, de conformidad con la ley.

El artículo 43 menciona que los datos de tráfico y de localización relacionados con los usuarios finales que sean tratados y almacenados bajo la responsabilidad de un operador o proveedor, deberán eliminarse o hacerse anónimos cuando no sean necesarios para efectos de la transmisión de una comunicación o para la prestación de un servicio.

Algo muy importante que se menciona en este artículo y que es de suma importancia para la investigación es que los datos de localización podrán tratarse solamente si se hacen anónimos o previo consentimiento de los abonados o usuarios, en la medida y por el tiempo necesario para la prestación de un servicio.

2.3.3 Reglamento de medidas de protección de la privacidad en telecomunicaciones.

La Superintendencia de Telecomunicaciones creó un reglamento que define las medidas de protección a la privacidad, el cual en su artículo 6 dispone que:

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 instalación y operación de los sistemas y las medidas técnicas y administrativas para cumplir ese propósito.

En cuanto a medidas de seguridad, el artículo 7 dispone que:

Los proveedores y operadores de servicios de telecomunicaciones deberán adoptar las medidas técnicas y administrativas adecuadas para preservar la seguridad de sus servicios, de ser necesario en colaboración con otros operadores o proveedores de telecomunicaciones en materia de la seguridad de la red. Para tales efectos, los operadores o proveedores deberán considerar las técnicas más avanzadas a fin de garantizar un nivel de seguridad adecuado al riesgo existente.

En el artículo 9 se indica que la SUTEL mediante el presente reglamento velará por el cumplimiento del mandato establecido en el artículo 42 de la Ley Nº 8642, en donde se le ordena a los operadores y proveedores de servicios de Telecomunicaciones garantizar la confidencialidad de las comunicaciones realizadas a través de sus redes y de los servicios de telecomunicación que brindan.

2.4 Tecnología Móvil.

2.4.1 Telefonía Móvil.

2.4.1.1 Definición telefonía.

La telefonía móvil es una de las tecnologías de mayor éxito en las telecomunicaciones, su historia se remonta a los años 40 cuando la empresa Motorola, motivada por la Segunda Guerra Mundial, desarrolla un teléfono móvil que utilizaba ondas de radio las cuales no superaban los 60 MHz.

Hasta el día de hoy se han desarrollado 4 generaciones de esta tecnología.

- ✓ Primera generación 1G: Los teléfonos eran muy grandes y pesados y usaban señales de radio con modulación de frecuencia.
- ✓ Segunda generación 2G: Nace a principios de los años 90, en esta generación se abandona el uso de ondas de radio y se inicia con la era digital, en esta época se obtuvieron muchas mejores tales como la calidad de la voz, seguridad y precios más accesibles para el público en general.
- ✓ Tercera generación 3G: Su mayor característica es una mejora notable en el ancho de banda y manejo de datos, a este punto se obtuvo servicios nuevos tales como teleconferencias, televisión y descarga de archivos, entre otros.
- ✓ Cuarta generación 4G: Ofrece un mayor ancho de banda, es 50 veces más rápida que la generación anterior, a este punto se puede recibir y observar señal de televisión en alta definición (Red Gráfica Latinoamérica, 2012).

2.4.1.2 Funcionamiento

Cuando se efectúa o se recibe una llamada mediante un teléfono móvil lo primero que el dispositivo hace es buscar señal de la estación base (ente fundamental para el correcto funcionamiento de estos dispositivos) más cercana de su proveedor de servicios. Las llamadas se pueden recibir o realizar en movimiento sin impactar la

calidad de la voz; al alejarse de la antena la señal celular se ve afectada y la comunicación verse interrumpida.

Cuando la estación base capta una señal de un dispositivo móvil, lo que hace es dirigirla a un conmutador encargado de conectar la llamada basándose en el tipo de llamada que se trata realizar sea teléfonos fijos o móviles.

2.4.1.3 Archivos IPDR y CDR

CDR son las siglas para Call Detail Record, según Bartley (2017), los archivos CDR proveen metadatos (campos de texto que van incrustados en archivos como audio o imágenes, entre muchos otros más) sobre cómo un número telefónico y/o usuario utilizan el sistema de llamadas. Alguna información de metadatos que podemos encontrar en estos archivos es lo siguiente:

- Fecha y hora del momento en que se realizó una llamada.
- Tiempo de duración de la llamada.
- Número de origen y número de destino de la llamada.
- Tipo de llamada (entrante, salida, gratuita)
- Costo de la llamada

IPDR son las siglas para Internet Protocol Detail Record, el contenido de este tipo de archivos se encuentra definido por el proveedor de servicios y en ellos se puede incluir información de red, proveedor y ubicación geográfica, entre otros.

Los archivos IPDR son utilizados para la transmisión avanzada de datos, donde se requiere intercambio de información contable. Cabe destacar que su funcionamiento como protocolo permite obtener informes en tiempo real que funciona con plantillas negociado entre el recopilador y el exportador.

Ejemplo:

Time	Caller ID	From	To	Disposition	Minutes	Cost
2017-02-27T21:01:04+00:00	"Cranford NJ" <19083418126>	19083418126	13157031086	answered	1	$0.0290
2017-02-24T18:49:57+00:00	"Ponte Vedra FL" <19045674141>	19045674141	13157031086	answered	1	$0.0290
2017-02-23T22:56:29+00:00	"Verona IL" <17792044080>	17792044080	13157031086	answered	1	$0.0290
2017-02-23T00:15:14+00:00	"Nacogdoches TX" <19365568051>	19365568051	13157031086	answered	1	$0.0290
2017-02-21T16:15:31+00:00	"FORBES REG HOSP" <14128582000>	14128582000	12157838370	answered	1	$0.0290
2017-02-21T14:42:09+00:00	"Del Norte CO" <17196575010>	17196575010	13157031086	answered	1	$0.0290
2017-02-20T23:50:10+00:00	"Ponte Vedra FL" <19045674141>	19045674141	13157031086	answered	1	$0.0290
2017-02-16T22:25:28+00:00	"Tampa FL" <18136148017>	18136148017	13157031086	answered	1	$0.0290
2017-02-15T20:46:38+00:00	"Gillett TX" <18304773116>	18304773116	13157031086	answered	1	$0.0290
2017-02-14T23:58:07+00:00	"Galveston TX" <14096329079>	14096329079	13157031086	answered	1	$0.0290
2017-02-07T16:23:23+00:00	"PRO NON PRO" <12027485263>	12027485263	13157031086	answered	1	$0.0290
2017-02-06T20:34:51+00:00	"PRO NON PRO" <12027485263>	12027485263	13157031086	answered	1	$0.0290
2017-02-03T00:23:57+00:00	"Little Rock AR" <15014860044>	15014860044	13157031086	answered	1	$0.0290
2017-02-02T18:39:06+00:00	"Los Angeles CA" <13239225767>	13239225767	13157031086	answered	1	$0.0290
2017-02-02T15:18:57+00:00	"West Jordan UT" <13858870689>	13858870689	13157031086	answered	1	$0.0290
2017-02-01T17:53:27+00:00	"La Porte TX" <13462229777>	13462229777	13157031086	answered	1	$0.0290

Imagen 3 – Ejemplo archivos CDR Fuente: Onsip.com

La importancia de estos archivos para los proveedores de servicios es lo siguiente:

- Facilitan la elaboración de facturación y a la vez funcionan de respaldo para determinar cuándo y cómo el dispositivo telefónico fue utilizado.
- Los CDR son utilizados para encontrar interrupciones en el servicio telefónico.
- Los archivos funcionan para resolución de conflictos y disputas legales.
- Sirven para encontrar tendencias de llamadas y obtener información sobre el uso que hacen los empleados, lo cual permite a las empresas elaborar estrategias de negocios.

2.4.2 Sistema de Posicionamiento Global (GPS)

2.4.2.1 Historia

Según Rioacha (2017), el primer sistema de navegación que utilizó satélites para localizar objetos en la superficie terrestre se llamó TRANSIT, desarrollado por la Fuerza Aérea y Marina de los Estados Unidos, este dispositivo fue utilizado por primera vez en 1965. TRANSIT estaba constituido por un total de 6 satélites y trabajaban a una altura de 1074 km, era capaz de cubrir la totalidad de la tierra, sin

embargo tenía problemas de lentitud por lo que no era apto para medios de transporte.

Para el año 1974 se pone en marcha el sistema llamado NAVSTAR Global Positioning System, este proyecto incluía 24 satélites. Su potencial fue demostrado durante la Guerra del Golfo Pérsico, donde se puso a prueba toda su capacidad y su respuesta fue un rotundo éxito (uno de estos ejemplos fue la precisión con que se dirigían los misiles a sus objetivos).

A pesar de su éxito y popularidad en los 90s, seguía existiendo un error de localización de 3 metros para todos los usuarios, mas no para el ejército estadounidense quienes lograron reducir esa diferencia a menos de un centímetro. Esto sucedía debido a que el departamento de defensa introducía un error aleatorio en los relojes atómicos de los satélites, la cual se podía corregir con información adicional proporcionada por equipos militares. Este problema fue solucionado gracias a que en el año 2000 el presidente Bill Clinton ordenó la eliminación de ese error, esto permitió que la población mundial pudiese geolocalizarse sin limitaciones (Palazzesi, 2010).

En la actualidad el GPS sigue funcionando mediante la red de 24 satélites a una altura de 20.200 km.

2.4.2.2 Funcionamiento.

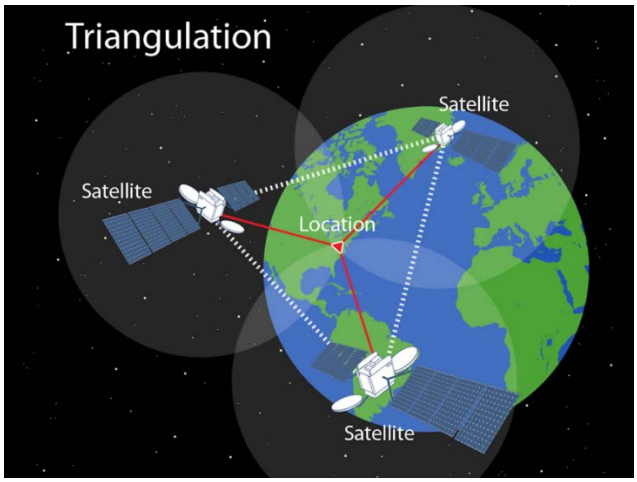


Imagen 4- Geolocalización. Fuente: Iraola, (2016)

Si un usuario desea utilizar este sistema, el receptor localiza automáticamente un total de tres satélites, esta comunicación intercambia información tal como identificación y hora. El tiempo debe estar perfectamente sincronizado entre ambos dispositivos, mediante estos datos es posible hacer el cálculo de tiempo que se tardará para movilizarse de un punto A hacia un punto B. Cabe destacar que los satélites utilizan un reloj atómico de cesio, mientras que los dispositivos receptores uno normal de cuarzo (García, 2015).

Generalmente, para que estos equipos funcionen se debe evitar que existan obstáculos que impidan la visibilidad con los satélites, esto evita problemas para captar las señales y reduce limitantes en el funcionamiento de los sistemas.

2.4.2.3 Ventajas de la geolocalización

La geolocalización es una tecnología que nos ayuda a mejorar la eficiencia en muchos aspectos de nuestra vida cotidiana. Esta tecnología ofrece información en un doble sentido, nosotros como usuarios nos beneficiamos de la información que nos facilita. Muchas tareas sin esta tecnología serían más complicadas de realizar, como obtener la ruta más corta a nuestro destino, o directamente imposibles como

conocer el punto exacto donde está el último paquete que hemos comprado por Internet.

Algunas de las ventajas que podemos mencionar:

- Obtener resultados de una búsqueda basados en la ubicación.
- Publicidad personalizada en función de la ubicación.
- Pedir ayuda en caso de emergencia, como por ejemplo un accidente
- Conocer la posición de una flota de vehículos.
- Dar a conocer en redes sociales la ubicación de una foto o un video.
- Analizar el comportamiento de los usuarios para mejorar la “experiencia de uso”.
- Realizar estudios con los que mejorar una tecnología existente o crear una nueva.

2.4.2.4 Desventajas de la geolocalización

Los dispositivos GPS son muy importantes en la actualidad, sin embargo, como toda tecnología existen vulnerabilidades y amenazas que afectan su buen funcionamiento.

- Una reconocida vulnerabilidad del GPS (conocida como GPS Spoofing) genera señales de GPS falsas haciéndole creer a los dispositivos que se encuentra en otros lugares o en diferentes zonas horarias; esto permite que hackers y/o terroristas la exploten para poder secuestrar aviones comerciales, cruceros y yates. Según el sitio guidewhat.com, por tan solo $3000 se puede elaborar un sistema que permita controlar un yate valorado en $80 millones y de 63 metros de largo. También existen vulnerabilidades en aplicaciones utilizadas para administrar diversos dispositivos, ejemplo de esto son los drones comerciales, muchos de ellos son controlados por medio de aplicaciones. Estos softwares no siempre se diseñan pensando en una buena plataforma de seguridad, por lo que muchas veces se vuelve muy

sencillo para los cibercriminales encontrar formas de vulnerarlos (Paganini, 2012).

2.5 ISO IEC 27001

2.5.1 ¿Qué es ISO?

La Organización Internacional para la Estandarización (ISO) es un ente mundial que está conformado por miembros de 130 países. Se caracteriza por ser una organización no gubernamental, que existe desde 1947. El objetivo de ISO es promover la estandarización mundial para facilitar el intercambio de servicios y bienes para promover los ámbitos científicos, intelectuales, tecnológicos y económicos. Todos los trabajos realizados por la ISO resultan en acuerdos internacionales, los cuales son publicados como Estándares Internacionales (GestioPolis, 2013).

Se entiende por norma a aquellos documentos que proveen los requisitos, especificaciones, directrices o características que pueden ser usados para asegurar que diferentes productos y servicios sean adecuados para sus propósitos. A nivel de Costa Rica, la entidad encargada de publicar dichas normas es el INTECO, una entidad que vela porque los insumos sean seguros y de alta calidad. A nivel empresarial, sirven para reducir costos, desperdicios y, además, incrementar la productividad. Además, con dichas normas se puede acceder a mercados internacionales, ya que se nivela el mercado de los países.

2.5.2 ISO IEC 27001

ISO IEC 27001 surge para gestionar la seguridad de la información disponiendo de controles que permiten asegurar a las organizaciones los diversos activos de información que poseen. La revisión más reciente de esta norma fue en 2013, por lo que su nombre cambio a ISO/IEC 27001:2013.

Este estándar se puede implementar en cualquier tipo de empresa sin importar si es pública o privada, ya que su fin principal objetivo es el manejo y administración de los datos dentro de las compañías. Las instituciones pueden optar por una certificación, sin embargo, deben cumplir varias condiciones, las cuales se encuentran estipuladas en la normativa.

Para una empresa, enfocarse en estándares de calidad que aseguren su información les genera un gran valor agregado, tanto a nivel interno como para sus clientes, y garantiza ventajas comerciales frente a otras instituciones que no se rigen bajo la norma. Cabe destacar que el motivo primordial de tener controles de seguridad es con el fin de evitar incidentes o problemas de seguridad que eviten materializarse en afectación de imagen de la empresa o bien costos económicos significativos.

2.5.3 ¿Qué es un SGSI?

SGSI es la abreviatura para Sistema de Gestión de Seguridad de la Información, este sistema tiene como fin principal proteger y velar por que se cumpla la confidencialidad, integridad y disponibilidad de la información de una organización. Se encuentra conformado por diversas actividades de gestión, las cuales tienen como propósito asegurar que los riesgos relacionados con la información de una compañía sean gestionados, asumidos, tratados y minimizados de forma sistemática, efectiva e integralmente (Iso27000.es, 2012).

El SGSI puede enfocarse tanto a nivel corporativo o bien a un departamento en específico de la empresa, se recomienda que quienes lleven a cabo este proceso sea personal con experiencia y certificados en ISO 27001, todo esto para garantizar un sistema que cumpla con las prácticas éticas y de garantía que ofrece la norma. Las compañías no necesariamente deben certificarse en esta norma, pero poder contar con ella genera un gran valor agregado a nivel de mercado y definitivamente los diferenciará del resto de las empresas.

2.5.4 Modelo Planear-Hacer-Verificar-Actuar

ISO 27001 utiliza el conocido modelo Plan, Do, Check, Act (PDCA), que significa lo siguiente:

Planear: Establece objetivos, procesos, procedimientos para la seguridad de la información, de manera que se logren entregar resultados de acuerdo con los objetivos y políticas de la organización.

Hacer: Representa la forma como se debe de operar, implementar, las políticas, controles y procesos.

Revisar: Analiza y mide dónde es aplicable los procesos, evaluación de objetivos e informar los resultados a la administración para su revisión.

Actuar: Realiza las acciones correctivas y preventivas, basados en auditorías y cualquier información relevante que permita la mejora continua en la seguridad de la información.

Tiene como finalidad poder desarrollar el estándar de manera óptima, en donde se asegura cierto grado de coherencia con otras normas de Sistemas de Gestión de Seguridad de la Información (SGSI).
La norma aplica este modelo de la siguiente manera:

1. Planear: En las secciones 4, 5, 6, y 7 de la norma se procede con el planeamiento de un SGSI.
2. Hacer: En la sección 8 se espera que se desarrolle e implemente el SGSI.
3. Verificar: En la sección 9 se espera que se lleve a cabo la evaluación del SGSI.
4. Actuar: En la sección 10 se espera que se hagan las mejoras necesarias para el SGSI.

Capítulo III

Marco Metodológico

3. Marco Metodológico

El marco metodológico establece el procedimiento general por seguir durante la investigación, así como las fuentes y sujetos de información. Consta de una serie de pasos los cuales se deben seguir para poder efectuar un estudio correcto y ordenado. En él no solo se analizan los pasos a seguir para la solución del problema planteado, sino que también las herramientas a emplear.

En un proceso de investigación se deben tomar en cuenta todos los factores que influyan en el problema, tales como contexto, condiciones, cambios y principios (Sabino, 2014). Es por esta razón que en este capítulo se estudia el problema tanto a nivel práctico como a nivel teórico, de manera que se analicen los diversos elementos que afecten la situación actual.

3.1 Contexto del lugar donde se realiza el proyecto

Este proyecto de graduación se lleva a cabo en el Instituto Costarricense de Electricidad y Telecomunicaciones (ICE), en las instalaciones del Edificio ubicado en Sabana Norte en San José Costa Rica. Específicamente en el departamento de Dirección de Tecnologías de la Información, donde se encargan de resguardar los archivos IPDR y CDR de todos los abonados de la red telefónica celular.

3.2 Información general de la institución donde se realiza el proyecto

3.2.1 Misión:

Somos la Corporación propiedad de los costarricenses, que ofrece soluciones de electricidad y telecomunicaciones, contribuyendo con el desarrollo económico, social y ambiental del país.

3.2.2 Visión:

Ser una Corporación líder, innovadora en los negocios de electricidad y telecomunicaciones en convergencia, enfocada en el cliente, rentable,

eficiente, promotora del desarrollo y bienestar nacional, con presencia internacional.

3.2.3 Valores:

- Integridad
- Compromiso
- Excelencia

3.3 Procedimiento Metodológico

3.3.1 Tipo de investigación

La investigación por realizar es de carácter evaluativo, se debe investigar y analizar la manera en que se recolectan y manipulan los archivos IPDR y CDR, además se pretende utilizar el estándar ISO IEC 27001 con el fin de obtener un resultado metodológico claro y sistemático. A manera de complemento se pretende elaborar una serie de recomendaciones para mejorar la forma en que se manipulan los datos actualmente, de modo que la información se accese cuidadosamente y siempre esté segura.

3.3.2 Diseño de la investigación

Esta es una investigación de campo, debido a que es apoyada en fuentes documentales a partir de las cuales se elaboran fundamentos teóricos que permiten sustentar el estudio del proyecto. El estudio se basa en la recolección y análisis de datos procedentes de las torres celular.

La información por analizar será extraída de manera directa de la realidad y por el investigador en el sitio en donde se llevará a cabo el estudio, en este caso, en la empresa ICE.

3.3.3 Enfoque de la investigación

La presente investigación presenta un enfoque cualitativo, debido a que estudia la realidad en su contexto natural y como se desenvuelve; todo esto permite interpretar fenómenos, según las personas y servicios implicados por medio de la utilización de instrumentos de recolección de información. Este análisis permitirá evaluar la importancia de tener una metodología de buenas prácticas para la manipulación de los archivos IPDR y CDR.

3.3.3.1 Población

La población del proyecto de investigación la constituye el personal del ICE, sede Sabana Norte.

3.3.3.2 Muestra

La investigación centra su unidad de análisis en el departamento de Dirección de Tecnologías de la Información. Este departamento gestiona la seguridad de la información a nivel Institucional y es quien posee la responsabilidad, el personal operativo y administrativo para iniciar un proceso de mejora en la gestión de archivos IPDR y CDR.

3.4 Técnicas e instrumentos de recolección de datos

La información para esta investigación se obtiene por medio del análisis de la gestión de los archivos IPDR y CDR. También, mediante la aplicación de cuestionarios a los colaboradores del departamento de Dirección de Tecnologías de la Información. Además, se pretende realizar una entrevista al encargado del departamento y también a personal que previamente trabajó con estos datos, finalmente se pretende la observación en sitio para ampliar y verificar algunos datos suministrados por los colaboradores del departamento.

3.4.1 Entrevista

Es una técnica enfocada en la obtención de información de manera oral y personalizada, su principal objetivo es conocer sobre acontecimientos y aspectos subjetivos; generalmente las entrevistas poseen un objetivo implícito, el cual es dado por la investigación por realizar.

Para efectos de este trabajo de investigación, la entrevista se realizará al encargado del departamento de Dirección de Tecnologías de la Información, lo cual permite conocer un poco sobre sobre la gestión actual de los archivos IPDR y CDR y verificar o confirmar datos brindados por los colaboradores del subproceso.

3.4.2 Técnica de observación

La técnica de la observación es una técnica del proceso investigativo que consiste en observar personas, acciones y hechos, entre otros, con el objetivo de determinar información requerida para poder realizar una investigación. Esta técnica es muy utilizada para observar el comportamiento de clientes o usuarios frente a sus labores cotidianas.

Para el caso de este proyecto se pretende observar el modo en que se gestionan los datos, estrategias de manipulación y manera en que se resguardan.

3.5 Fuentes de información

Las fuentes de información utilizadas para el desarrollo de la presente investigación fueron obtenidas por medio de sitios especializados en el tema Internet de las Cosas, legislación en Costa Rica, GPS y privacidad. Las mismas ayudaron en la compresión del entorno y complejidad organizacional en la gestión de los archivos IPDR y CDR, brindando un sustento teórico y metodológico al trabajo.

Estas fuentes consisten en informes relacionados con los sistemas de las tecnologías de la información, tales como fuentes documentales, las cuales incluyen

manuales de procedimientos, informes, procesos y fuentes digitales, entre otros. Estas últimas fueron uno de los principales medios de consulta, por la gran cantidad de sitios web relacionados con Internet de las Cosas.

3.6 Procedimientos para la elaboración del proyecto

El presente trabajo de investigación tiene como finalidad elaborar una guía de buenas prácticas que permita una correcta gestión de los archivos de IPDR y CDR recolectados por el Instituto Costarricense de Electricidad y Telecomunicaciones basado en la norma ISO IEC 27001:2013.

Es necesario conocer el entorno actual y la manera en que se gestionan estos archivos y a la vez la forma en que se gestiona la seguridad de la información en el departamento a cargo, todo esto es vital para poder desarrollar este trabajo de manera exitosa. Por esto, previo a la confección de la guía, se ejecutan las siguientes acciones:

- Análisis de datos mediante la recolección de información por medio de cuestionarios y entrevistas realizados a personal clave de la institución.
- Análisis de resultados de los métodos de investigación, los cuales permiten la definición de variables para la guía metodológica.

Una vez obtenidos los datos y valorado el estado actual en cómo se gestionan los archivos IPDR y CDR, se procede a desarrollar el diseño de la guía metodológica donde se definen los pasos y requisitos necesarios para evitar una incorrecta manipulación de dichos archivos.

Capítulo IV

Propuesta y Resultados

4. Propuesta y Resultados

4.1 Resultados

4.1.1 Riesgos para la privacidad

Después de realizar un análisis de los datos solicitados al Instituto Costarricense de Electricidad por medio del formulario de la PROHAB, podemos observar que nuestra privacidad está en manos de las empresas y aplicaciones que almacenan nuestros datos de geolocalización, particularmente los proveedores de servicio de telefonía. Dentro de los datos que se almacenan están los datos de geolocalización de los terminales móviles dados por las antenas de comunicación celular, que son resguardados hasta por tres años en bases de datos resguardadas, según la normativa legal costarricense.

4.1.1.1 Privacidad a cambio de servicio

Cuando Mark Zuckerberg, fundador de Facebook, advirtió en una entrevista en 2010 que la privacidad había muerto, le acusaron de exagerado (Tsotsis, 2010). Con el tiempo, además de un visionario, aquel presagio lo ha hecho multimillonario. Las personas, hoy en día, usan las nuevas tecnologías para su diario vivir, estas tecnologías permiten tomar fotografías de lo que hacen, los lugares que visitan, las personas con las que se conviven, entre otras cosas.

Los usuarios brindan datos con previo consentimiento porque, si bien es cierto cada vez que se instala una aplicación la misma pide permisos para utilizar ciertas funcionalidades del dispositivo, el consentimiento se brinda sin conocimiento, simplemente se quiere obtener la aplicación y damos aceptar sin leer detalladamente las condiciones que se nos presentan. Por ejemplo, para instalar una aplicación para tomar notas, la misma pide acceder la ubicación, la cámara y los contactos, entre otras funcionalidades; ¿y para qué esta aplicación solicitará acceso a funcionalidades que ni siquiera se utilizan en ella?

Una investigación realizada por Quartz en el 2017 arrojó un dato muy interesante, ellos afirman que, desde comienzos del 2017, los teléfonos Android registran las ubicaciones de torres de celulares cercanas al dispositivo, incluso cuando se desactiva el servicio de localización (INFOBAE, 2017). Lo más interesante de esta investigación es que Google no desmiente tal afirmación, dentro de la política de privacidad de Google se aclara que la compañía reunirá información sobre la ubicación de los equipos que usen su servicio:

> *"Cuando utiliza los servicios de Google, podemos recolectar y procesar información sobre su ubicación actual. Utilizamos varias tecnologías para determinar la ubicación, incluyendo la dirección IP, GPS y otros sensores que, por ejemplo, puede proporcionar a Google información sobre dispositivos cercanos, acceso a puntos wifi y torres de celulares"*

La ventaja más obvia de la geolocalización es la mejora de eficiencia en muchos servicios digitales. Si buscamos un determinado servicio en algún motor de búsqueda, ya sea desde el móvil o desde el ordenador, es más fácil que el buscador nos ayude si conoce nuestra posición o ubicación. Nos dará entonces datos relativos a locales cercanos y evitará otros demasiado alejados. Lo mismo sucede si buscamos una determinada calle, si el servicio de mapas sabe dónde estamos, nos podrá indicar la forma más rápida de llegar.

También podemos considerar una ventaja que si un comercio on-line al que solemos visitar sabe a qué tipo de locales acudimos, pueda analizar nuestros gustos y darnos consejos sobre qué producto nos puede interesar más. Nos ahorramos así publicidad de bajo interés.

Entonces podríamos preguntarnos, ¿dónde está lo negativo de todo esto?

Es justamente esta eficiencia que presta la geolocalización lo que resulta inquietante. Ahora que hay automóviles, electrodomésticos y hasta cepillos de

dientes inteligentes que generan un volumen de datos exponencial, hay empresas que se dedican exclusivamente a la construcción de bases de datos y perfiles de consumo con los millones de datos que vamos regalando por la red gracias a este tipo de tecnología. Analizan, por ejemplo, todo lo que publicamos en las redes sociales para vender estudios de mercado y de perfiles políticos.

Los “Data Broker”, que así se llaman estas compañías, son como reventas de información (Masa, 2015). Estas empresas quieren conocer qué hicimos ayer para vender esa información a las compañías que quieren predecir qué haremos mañana, qué compraremos mañana, por quién votaremos mañana.

El resultado de todo esto es una publicidad cada vez más personalizada. De hecho, los propios Data Broker, igual que Facebook y Google, aseguran que el gran beneficiado es el propio usuario, ya que solo recibe publicidad que le resulte útil, ajustada a sus gustos y sus intereses.

Pero, ¿qué pasa cuando no queremos una mejor publicidad, tan solo porque no queremos que se utilicen nuestros datos para elaborar perfiles ni estudios de marketing? Pueden ser muchos los motivos por los que no deseemos que todo el mundo sepa dónde estamos en cada momento, pero para ello prácticamente tendríamos que renunciar a las nuevas tecnologías.

Los datos son “el nuevo petróleo” que las empresas están empezando a explotar sin que el usuario sea consciente de la rentabilidad que eso ofrece. Solo Google Maps sabe a qué hora se sale de casa, dónde se ha estado, en qué lugares se compra, qué marca de carro se tiene, y hasta cuándo se llega a casa, aunque no seas consiente de brindar estos datos. De esta forma, cuando Google tiene que segmentar publicidad sabe exactamente qué necesitan sus usuarios; no es magia, ya estos datos se han adquirido con previo consentimiento. La base de la privacidad es el consentimiento informado.

La empresa KPMG realizó un estudio en el que muestran por medio de gráficos circulares varias situaciones en las que los consumidores analizan si son útiles o inquietantes (KPMG, 2017). El resultado arroja datos interesantes, por ejemplo, el 54% de las personas encuestadas indicó que le parece inquietante (color verde) adquirir un televisor en descuento siempre y cuando la persona permita que monitoreen sus hábitos, por el contrario, el 46% restante lo considera útil (color azul). Entonces, los consumidores prefieren obtener un televisor a bajo costo sin importar que su privacidad esté en manos de un desconocido. En el siguiente cuadro se muestran otras situaciones que fueron analizadas en el estudio.



Imagen 5. Situaciones útiles o inquietantes. Fuente: Crossing the line. KPMG (KPMG, 2017)

Entonces vemos que las personas sí se preocupan en su mayoría por la privacidad, pero también están dispuestas a brindar la privacidad a cambio de un servicio.

4.1.1.2 Operadores móviles: ¿Aseguran mi privacidad?

Como se mencionó al principio de este apartado, las empresas de telecomunicación obtienen mucha información gracias a sus antenas de comunicaciones, esta

información es guardada en archivos tales como los IPDR o CDR. Estos archivos pueden estar en varios formatos, ya sea formato decimal o hexadecimal.

Al realizar un análisis de estos archivos, podemos observar que las empresas de telecomunicaciones tienen en sus manos la privacidad de sus clientes, tienen acceso a los datos reales de dónde están sus clientes, qué compran, con quién hablan y hasta con quién se relacionan. Y es que no es nada extraño que estos datos se utilicen para hacer publicidad y hasta para hacer mercadeo.

La creciente sofisticación de la tecnología parece ir de la mano de la incapacidad de los usuarios para tener control de su información, se deja en manos de empresas proveedoras de tecnología y entidades como el gobierno la confianza de que estos datos no serán mal utilizados. En el artículo 6 del reglamento sobre medidas de protección de la privacidad de las comunicaciones se indica que:

> *"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 instalación y operación de los sistemas y las medidas técnicas y administrativas para cumplir ese propósito".*

Según Adrián Chacón, encargado de la gestión de arquitectura tecnológica del Instituto Costarricense de Electricidad (ICE), estos archivos son protegidos bajo estrictas medidas de seguridad tanto a nivel lógico como físico. El acceso lógico a los mismos está restringido, solamente las personas autorizadas pueden manipularlos. A nivel físico, el datacenter donde se encuentran estos archivos cuenta con seguridad perimetral y solamente algunas personas pueden acceder a ellos, por consiguiente, los servidores donde se almacenan estos datos heredan los mismos controles.

Puede que estas medidas sean suficientes para resguardar los archivos IPDR y CDR, pero tal vez no sean suficientes para cuidar la privacidad de los usuarios.

GSMA es una asociación que representa los intereses de operadores de telefonía móvil, proveedores de servicios, fabricantes, desarrolladores y compañías de comunicación y entretenimiento de todo el mundo.

En enero del año 2011 la GSMA publicó sus Mobile Privacy Principles (GSMA, 2011), estas directrices se basan en el principio de Privacy by design[1] que promueve entre las compañías del sector una actitud proactiva en la protección de la privacidad del consumidor desde el inicio y no en el último momento. La guía aborda cuestiones tales como la necesidad de ser transparente con el usuario y ayudarle a gestionar su privacidad, limitar la obtención y retención de sus datos, garantizar la seguridad de la información, tener en cuenta las especiales características de las redes sociales, ser especialmente claro en el tratamiento de datos de localización, proteger a los niños y adolescentes e implementar el principio de *accountability*[2] o responsabilidad en la protección de la privacidad de los usuarios. El ICE, al ser un proveedor miembro de esta asociación, debe tomar en cuenta estas medidas que promueve la GSMA para que de esta forma se asegure la protección de la privacidad de los usuarios.

El cruce de datos entre localización y producción de información desde dispositivos celulares puede revelar datos sensibles, y compone un rompecabezas entre la esfera de lo íntimo y lo público.

Para efectos de esta investigación se solicitó al ICE los datos personales que se encuentran en sus bases de datos. Dentro de la información brindada están los datos de geolocalización, estos se muestran en términos de latitud y longitud, esto quiere decir que se manejan los puntos exactos de la trayectoria de una persona. Procedimos a realizar una tabulación de esta información para proyectarla en un

[1] La *Privacy by Design,* PbD o Privacidad desde el Diseño, consiste en la implementación y desarrollo de procesos, pautas y medidas de seguridad que vayan acorde con los principios de calidad, licitud, seguridad y finalidad y con ello el respeto a Derechos y Libertades Fundamentales (Ceara, 2017).

[2] En un contexto general, responsabilidad demostrada puede definirse como: "la obligación de un individuo o de una organización de rendir cuentas sobre sus actividades, aceptar responsabilidad sobre ellas y divulgar los resultados de manera transparente" (businessdictionary, s.f.).

mapa, en la siguiente figura se puede visualizar el recorrido de una persona durante un mes:

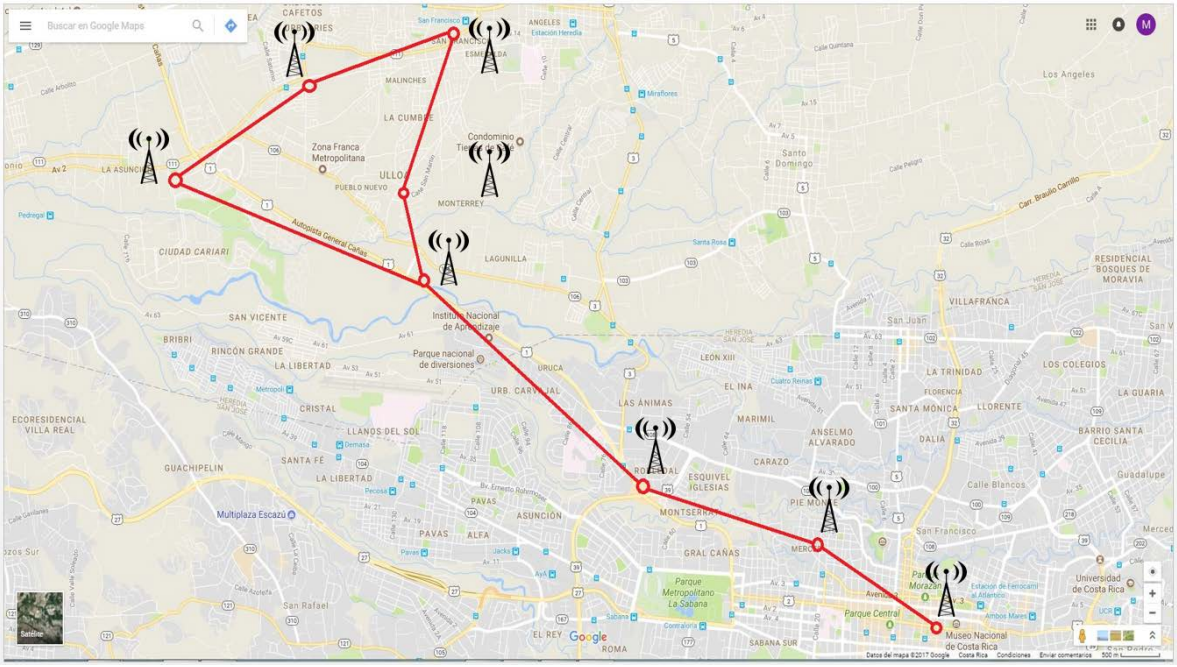


Imagen 6. Trayectoria proyectada por medio de geolocalización. Fuente: Propia.

Un dato importante es que esta localización se obtiene por medio de las torres telefónicas, por lo tanto, aunque se deshabilite la función de localización en el dispositivo móvil, la información siempre va a ser capturada por parte de las antenas.

La imagen anterior permite recorrer un mes de vida sobre el mapa y, al mismo tiempo los datos obtenidos permiten conocer el tiempo que estuvo hablando la persona, cuántos mensajes envió y recibió, o durante cuánto tiempo estuvo conectado a Internet. Todo esto es porque la persona llevaba todo el día consigo un teléfono móvil, que va emitiendo una señal cada cierto tiempo.

Es un hecho que la compañía o proveedor de telefonía tiene en sus manos datos sumamente sensibles, los cuales podrían ser utilizados con fines lucrativos, o peor aún caer en manos de personas o empresas no autorizadas. Para evitar la mala

manipulación de los datos personales, en nuestro país existen leyes y normativas que protegen estos datos, las cuales se enfocan en el derecho de autodeterminación.

4.1.1.3 Protección de datos personales

Las tecnologías modernas de la información y la comunicación han transformado profundamente la forma como la humanidad crea y distribuye sus conocimientos, así como la posibilidad de acceso a plataformas en las que se acumulan gran cantidad de datos personales. El riesgo que se genera para la intimidad de los individuos tiene que ser controlado en términos de defender su libertad e igualdad del tratamiento automatizado o manual de sus datos personales cuando figuren en bases de datos tanto de organismos públicos como privados. En la actualidad, la sociedad costarricense ha tenido que enfrentarse al mundo digital y ello ha generado que el ciudadano experimente lo que se conoce como la sociedad de la información.

Es el Derecho a la Autodeterminación Informativa el cual con base en el valor y relevancia actual de los datos personales establece la facultad que tiene cada persona en proteger su intimidad y decidir qué datos personales pueden ser o no tratados, almacenados, transferidos, divulgados y comercializados en el territorio de la República de Costa Rica. En virtud de este derecho, a cada persona le asisten derechos especiales enmarcados en la Ley 8968. Estos derechos especiales a nivel internacional son identificados como los “Derechos Arco”, los cuales permiten que el ciudadano pueda ejercer el derecho de Acceso, Rectificación, Cancelación y oposición frente al tratamiento de sus datos personales.

Según Wendy Rivera Román, directora de la PRODHAB de nuestro país,

> “*en Costa Rica los derechos se definen por medio de otra nomenclatura (AR), esto porque en el apartado de Rectificación se incluye la Cancelación y Oposición. Es importante mencionar también que a los derechos ARCO se*

ha adicionado la acción de portabilidad (ARCOP), lo que permite llevar mis datos a otro operador para hacer el cambio".

4.1.1.3.1 Datos que protege la Ley

A raíz de la aprobación de la normativa de protección de datos, se han generado varias interpretaciones e interrogantes en relación con el ámbito de aplicación de esta.

Inicialmente se consideró que su aplicación se limitaba única y exclusivamente a quienes comercializan datos (personas físicas o jurídicas, públicas o privadas), es decir, que solo estos debían inscribir sus bases de datos, se excluía así cualquier base de datos cuya información de carácter personal no sea comercializada. Por otro lado, y a partir de la interpretación de la Agencia de Protección de Datos de los Habitantes (PRODHAB), la discusión tomó otro rumbo y se centró en determinar cuáles empresas debían inscribir sus bases de datos ante dicha institución.

La Agencia de Protección de Datos de los Habitantes consideró que están sujetas a inscripción además de las bases de datos que se comercializan, todas aquellas que se utilicen con fines de prospección comercial (publicidad) y las que sean transferidas; lo que ha llevado a entender que deben inscribirse prácticamente todas, y en ese tanto, todas deben someterse a la citada normativa.

Cuando una empresa inscribe una base de datos se solicita que se indique el sistema, programa y método o proceso utilizado para el tratamiento de los datos, así como los mecanismos de seguridad que la empresa utilizará para proteger estos datos. Además, la directora de la PRODHAB indicó que

"*cuando se hace la inscripción se realiza una verificación jurídica y técnica, esto está sujeto a revisión en cualquier momento, si la PROHAB decide revisar en cierto momento lo puede hacer por medio de un oficio. A demás*

periódicamente se solicita a las empresas que realicen actualización de dicha información."

Dentro de las atribuciones de la Agencia de Protección de Datos se encuentra el poder verificar el cumplimiento de la normativa, independientemente si se trata de una institución pública o privada. La ley en el artículo 16, le da a la PRODHAB, como competencia, el hecho de poder acceder a las bases de datos siempre y cuando sea para realizar un estudio ante la noticia de que hay un tipo de irregularidad. La agencia tiene recursos limitados, por lo tanto, lo que se realiza es un tipo de muestreo y de acuerdo de esas muestras o hallazgos se procede a realizar algún otro proceso de verificación más exhaustivo.

4.1.1.3.2 Solicitud de datos personales

Para efectos de esta investigación se procedió a hacer el uso del derecho de solicitud de datos personales, dicha solicitud se realizó al Instituto Costarricense de Electricidad. Para ello se utilizó el formulario que facilita la PRODHAB dentro de su página web (ver anexo 1).

Fue evidente el desconocimiento por parte del personal del ICE con respecto a la Ley de Protección de Datos personales y así también de la solicitud que se estaba realizando. Dentro de las condiciones que se indican en el formulario se encuentra el tiempo de entrega de los datos solicitados, el cual es de 5 días hábiles. Después de un mes y una denuncia interpuesta ante la Agencia de Protección de Datos (Ver Anexo 2) se recibió respuesta por parte del ICE, dentro de la que indican lo siguiente:

"Según el Reglamento sobre Medidas de Protección de la Privacidad de las Comunicaciones (RMPPC) reitera ese derecho a la intimidad y la protección de los datos de carácter personal de los usuarios finales y el deber correlativo de los operadores y proveedores de garantizar que los datos de tráfico asociados a sus comunicaciones no serán grabadas, registradas, almacenadas, intervenidas o vigiladas por terceros.

Este reglamento es tajante respecto a la posibilidad de conservar datos sobre el contenido de las comunicaciones, por cuanto menciona que "ningún dato que revele el contenido de la comunicación podrá conservarse en virtud de la legislación vigente", pues estaríamos en presencia de una intervención telefónica, que solo se puede realizar por orden judicial.

De acuerdo con la Ley General de Telecomunicaciones no se establece la entrega de información relacionada con Georreferenciación, datos de navegación de su servicio celular (rutas de una antena a otra) como una obligación del operador y un derecho del cliente, máxime que no es un servicio disponible al público, y como tal, no forma parte de la oferta comercial del ICE, por lo cual no se puede brindar la información solicitada"

Ante esta respuesta, nace la inquietud de si una Ley predomina sobre otra, ¿será entonces que las empresas que brindan servicios de comunicaciones se rigen solamente por la Ley de Telecomunicaciones e ignorarán la Ley de Protección de Datos? ¿Acaso esos datos de geolocalización no son datos personales y nos pertenecen como tal?

Son muchas las inquietudes que genera esta respuesta por parte de este operador, pero la más importante es: si ellos alegan que solamente resguardan este tipo de información cuando existe una orden judicial, ¿cómo es que se determina la trayectoria que realizó una persona si por ejemplo se realiza una denuncia de secuestro? Gracias a la investigación realizada a los archivos IPDR se determina que estos datos sí son resguardados por el operador, pero a los mismos no se les da utilización para brindar algún servicio al abonado y no se determina el tiempo en que estos son resguardados. Pero por su naturaleza, este tipo de archivos resguardan las coordenadas de las antenas donde se ha conectado el dispositivo móvil, por lo tanto, los datos de geolocalización de una persona sí son resguardados.

Ante tal hallazgo, se procedió a informar a la Agencia de Protección de Datos, la cual al momento de finalización de esta investigación se encuentra haciendo los

estudios respectivos para determinar si esta información debe ser brindada al investigador o no.

De igual forma, ante la solicitud no se realizó entrega de ningún dato personal, ya que no solo se pedían los datos de geolocalización, sino más bien cualquier dato personal que se encontrase en las bases de datos del ICE.

4.1.2 Implicaciones Legales

Como hemos mencionado a lo largo del desarrollo de esta investigación, la localización se puede realizar a través de un dispositivo móvil que puede ser rastreado por la empresa que provee servicios. Estas empresas pueden dar en tiempo real la ubicación de una persona, con solo la petición expresa de un juez para una investigación, esto de conformidad con el artículo 24 de la Ley N°7425, "Ley de Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones[3]".

Esta situación fue acusada en México por la Comisión Nacional de Derechos Humanos[4], argumentando que se daba demasiado poder a los agentes del Ministerio Público para investigar la localización de las personas a través de sus teléfonos móviles y que por lo tanto se promovía una violación al derecho de privacidad al dar demasiada libertad sin control alguno a dicho Ministerio. Además, representaba una facultad demasiado grande, que sin un control adecuado puede ser usado de manera poco adecuada (Mexico, 2014).

Al respecto se puede mencionar que el objetivo de investigar la localización persigue un fin legítimo, y podría representar una oportunidad de capturar a un criminal o impedir un hecho ilícito, por tal se entendería y se tendría por justificada la intromisión en la privacidad, pero precisamente para eso se requiere un control.

[3] Ley de Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones N°7425. Diario Oficial la Gaceta, 09 de agosto de 1994. Disponible en: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=16466&nValor3=17615&param2=1&strTipM=TC&lResultado=3&strSim=simp

[4] Acción de Inconstitucionalidad 32/2012. Disponible en: http://www.cndh.org.mx/sites/all/doc/Acciones/Acc_Inc_2012_32_Demanda.pdf

En nuestro país, la Ley N°7425 se promulgó mucho tiempo antes que la Ley N°8968, por lo tanto, se podría analizar si ahora se requiere de alguna modificación que regule en qué momento o qué controles se deben llevar a cabo para que este derecho que se otorga a un Poder Judicial sea utilizado de la mejor forma, resguardando y cumpliendo lo que dictan las Leyes en Costa Rica en referencia a la privacidad y el resguardo de los datos personales.

El marco regulatorio de telecomunicaciones establece como una infracción muy grave utilizar la información de los usuarios finales para fines no autorizados en la Ley y violar la privacidad o intimidad de las comunicaciones de los usuarios finales. Las sanciones asociadas dependerán de la gravedad de la infracción y los efectos que estas hayan causado. Específicamente, las infracciones muy graves serán sancionadas mediante una multa de entre 0,5% y hasta 1% de los ingresos brutos del operador o proveedor obtenidos durante el período fiscal anterior. Asimismo, cuando a juicio de la SUTEL, la infracción revista de una gravedad particular, esta podrá imponer como sanción una multa de 1% y hasta un 10% de las ventas anuales obtenidas durante el ejercicio fiscal anterior, o el valor de los activos.

De igual manera, a nivel de protección de datos personales, es considerado una falta grave negarse injustificadamente a dar acceso a un interesado sobre los datos que consten en archivos y bases de datos, y será sancionada con una multa de cinco a veinte salarios base del cargo de auxiliar judicial I, según la Ley de Presupuesto de la República.

La experiencia hará que se modifiquen las leyes y se pongan límites más estrictos a situaciones como la geolocalización, que los controles de confianza sean más estrictos, y que se respete la privacidad y legalidad. Se espera que lo que hay dentro del celular, así como la ubicación, sean una cuestión privada, o al menos así se pretende, ya que a través de la geolocalización se pueden obtener datos privados de una persona.

Propuesta

4.2 Pruebas de Penetración

El propósito de este proyecto es poder desarrollar un documento con diversos planes que contengan instrucciones específicas sobre cómo mejorar y proteger la privacidad de los usuarios del ICE. Si bien es cierto la institución ya cuenta con una infraestructura segura, no se puede confiar y siempre se puede mejorar para evitar futuros inconvenientes. Su contenido puede variar de una unidad de negocio a otra o bien de una subestación a otra.

Debido a la dependencia de los usuarios con equipos de IoT, muchas veces se desconoce la información que podrían estar entregando y/o revelando por el uso de estos dispositivos, la privacidad y los riesgos que esta conlleva cobra día con día mayor importancia. Es por esto que es indispensable que cualquier institución sin importar si es grande o pequeña posea planes aptos para poder brindar confidencialidad e integridad a toda la información que gestionan.

Como fin principal de este capítulo está el proponer diversos planes que ayuden a futuros proyectos que posee el ICE, específicamente en el departamento de Dirección de Tecnologías de la Información. Se pretende describir documentos para realizar auditorías, especificar las fases que se requieren para la implementación de pruebas de penetración, y la creación de plantillas basadas en el estándar ISO/IEC27001 y NIST frameworks, de manera que se logre asegurar la operación de la organización y el servicio a sus clientes minimizando el impacto financiero, y evitando efectos negativos que puedan producirse en los planes estratégicos previamente establecidos por la compañía.

A continuación, se presentan las diferencias entre una prueba de penetración y un escaneo de vulnerabilidades:

	Escaneo de Vulnerabilidades	**Prueba de Penetración**
Propósito	Identificar, clasificar e informar vulnerabilidades que, si se explota, puede dar como resultado accesos intencionales o involuntarios de un sistema.	Identificar formas de explotar vulnerabilidades para prevenir o limitar ataques de ciberseguridad a la arquitectura de seguridad de la compañía.
Cuando	Trimestralmente o cada vez que se hagan cambios en la organización como actualización de sistemas o compra de equipos, entre otros.	Anualmente o cada vez que ocurran cambios significativos dentro de la organización.
Como	Por lo general se lleva a cabo mediante el uso de una variedad de herramientas automatizadas junto con verificaciones manuales de problemas previamente identificados.	Es un proceso manual que puede incluir el uso de escaneo de vulnerabilidades y el uso de otra gran cantidad de herramientas automatizadas que permiten obtener datos sensibles de la organización.
Reportes	Los reportes generalmente se obtienen automáticamente por las herramientas utilizadas para llevar a cabo el escaneo de vulnerabilidades. Este reporte categoriza las	Descripción de cada vulnerabilidad encontrada. Más riesgos específicos que puede presentar la vulnerabilidad,

	vulnerabilidades y provee números de identificación para cada una.	incluyendo métodos específicos. Ejemplos de vulnerabilidades incluyen SQL Injection, privilegio escalamiento, Cross-site scripting o protocolos inseguros, entre otros.
Duración	El tiempo es relativamente corto, típicamente puede tardar algunos minutos por cada servidor escaneado.	Las pruebas pueden durar días o semanas, dependiendo del alcance de la prueba y tamaño del ambiente a ser vulnerado. Las pruebas pueden crecer en tiempo y complejidad si los esfuerzos descubren problemas no contemplados.

Tabla 1: Diferencia entre escaneo de vulnerabilidades y pruebas de penetración. Fuente: Propia

Se sugiere antes de iniciar con las pruebas de penetración hacerlo en un ambiente controlado (infraestructura espejo), de esta manera no se ponen en riesgo los distintos servicios de producción de la organización.

A continuación, se enumera una lista de acciones previa a las pruebas de penetración:

1. Inventario de riesgos
2. Análisis de vulnerabilidades (puertos, protocolos, CVEs)
3. Rangos de direcciones IPs
4. Fuentes de información
5. Análisis de las páginas WEB
6. Existencia de redes inalámbricas
7. Detección de equipos activos

8. Horario de realización de las pruebas (dentro horas laborales o fuera de horas laborales)
9. Red virtual de pruebas

4.2.1 Objetivos de una prueba de penetración

1. Determinar si un usuario malintencionado puede obtener acceso no autorizado a los diversos activos de la organización.
2. Confirmar la existencia de controles en la organización que sean capaces de reaccionar ante algún evento o irregularidad que se presente en la compañía.
3. Verificar que la información es gestionada correctamente sin que se llegue afectar la confidencialidad, integridad y acceso.

Hay tres tipos de pruebas de penetración: black-box, white-box y gray-box. En una evaluación de black-box, el cliente no proporciona información antes del inicio de la prueba. En una evaluación de White-box, la entidad puede proporcionar al encargado de realizar la prueba de penetración detalles completos de la red y las aplicaciones. Para la prueba gray-box la entidad puede proporcionar detalles parciales de los sistemas objetivos.

4.2.2 Requerimientos mínimos para la creación de un laboratorio de Pruebas de Penetración

Hardware:

- Computadoras/Servidores de 5ta generación con procesador Core I5 o I7
- Memoria RAM de 8 a 16 gigas
- Disco duro de 500 gigas
- Sistema Operativo Windows/Linux
- 3 puertos Ethernet
- 1 Router Wifi
- 1 Switch capa 2
- 1 Router (2800, 2811) Cisco

- 2 Firewalls para asegurar el laboratorio
- 2 o 3 monitores
- 5 llaves mayas booteables con distintos sistemas operativos

Software:

- Mozilla Firefox con add-ons (Hackbar, Cookie Stealer, Temper Data, Request Header Modifier)
- Java para Windows
- Software para equipos virtuales (Virtual Box, VMware)
- Microsoft .net Framework 4.5
- WinRAR
- Virtual Studio versión 2010 o mayor
- Suite de Microsoft SYS Internals
- Adobe Acrobat Reader
- Microsoft Office 2010 o mayor

Sistemas Operativos:

- Kali Linux Versión 2.0 o 3.0
- DEFT (Digital Evidence Forensics Toolkit)
- Backtrack 5 R3
- Windows 7 booteable desde un USB
- Wifi Slax

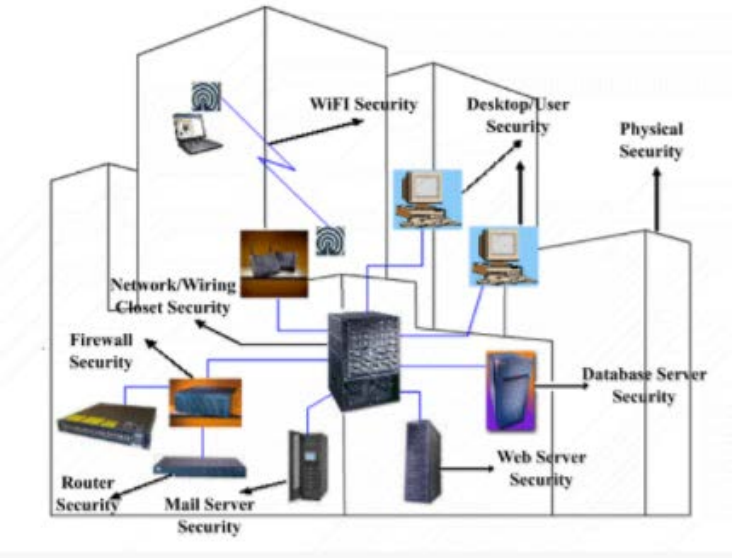


Imagen 7: Infraestructura segura. Fuente: Pen-tests.com (s.f.).

4.2.3 Requisitos de software especializado para evaluación de vulnerabilidades y pruebas de penetración



Imagen 8: Infraestructura segura. Fuente: Propia

Se recomienda manejar las pruebas de penetración de la compañía por medio de diversas fases, de manera que se pueda mejorar la seguridad de las tecnologías de la información de la organización y se tomen acciones que permitan solucionar las deficiencias con las que cuenta la empresa.

1. Fase - Identificación:
    - Escaneo y análisis de vulnerabilidades de equipos de red
    - Escaneo de puertos de red
    - Revisión de instalaciones físicas
    - Sistemas críticos
    - Información de la organización
    - Proveedores
    - Auditoría

2. Fase - Análisis
    - Análisis de impacto del negocio
    - Análisis de riesgos
    - Documento de Recomendaciones

3. Fase – Acción
    - Creación de políticas de seguridad de TI
    - Plan de continuidad del negocio
    - Remediación de vulnerabilidades
    - Conformación de equipo de emergencia
    - Configuración o compra de equipo o aplicaciones
    - Asesoramiento para la creación de documentos de funcionamiento de los sistemas
    - Sugerencia de mejoras en la seguridad física

4. Fase – Monitoreo y revisión
    - Capacitación de empleados

- Ejecución de pruebas

5. Fase – Controles
    - Proceso de concientización
    - Auditoría interna
    - Revisión mensual de vulnerabilidades de los sistemas
    - Centralización de los sistemas

4.2.4 Pasos para efectuar un buen plan de pruebas de penetración

- Paso 1: Planeamiento

La realización de una buena prueba de penetración requiere una planificación previa que tiene como mínimo los siguientes pasos:

- Tipo de prueba de penetración a realizar
- ¿Se permitirá ataques DoS o DDoS?
- Instalación de Backdoors
- ¿Se permite la eliminación de logs?
- ¿Se permite la ingeniería social?

Una vez que se haya obtenido los detalles de lo que se puede hacer y no se puede realizar, se recomienda la creación de un documento en donde se especifique el alcance de la prueba y en donde se otorgue el permiso necesario al personal que vaya a llevar a cabo la iniciativa.

- Paso 2: Enumeración y mapeo de redes

Este primer paso a menudo implica el escaneo de puertos y determinar qué computadoras están conectadas a ella, además de obtener información del sistema operativo y los servicios que ofrecen.

- Paso 3: Reconocimiento

Esto implica revisar las máquinas en la red y extraer información de ellas, como las aplicaciones que están ejecutando. El reconocimiento también puede involucrar el uso de Google para obtener información sobre la organización que se está evaluando, por ejemplo, para conocer los nombres del personal de TI y los ejecutivos. Las cuentas de redes sociales para esas personas también pueden revelar información, como los nombres de las mascotas, que a menudo se usan en las contraseñas.

- Paso 4: Captura y análisis de paquetes de la red

La captura y análisis de paquetes de red se utiliza para examinar el tráfico que circula por la red y para buscar datos no cifrados, incluidas las contraseñas o el tráfico voz.

- Paso 5: Escaneo de vulnerabilidades

Un análisis de vulnerabilidad puede revelar si alguna máquina tiene versiones inseguras de software u otras vulnerabilidades conocidas que pueden explotarse, o si los puntos de acceso inalámbricos están abiertos o tienen contraseñas débiles. Una herramienta popular de vulnerabilidad de código abierto es OpenVAS, o inclusive se puede optar por una herramienta más poderosa como Nessus, sin embargo, esta aplicación tiene un costo de $2100 al año. Otros escáneres más especializados también pueden dirigirse a los servidores web para buscar vulnerabilidades como errores de secuencias de comandos entre sitios (XSS).

- Paso 6: Explotación de vulnerabilidades

Esta etapa intenta explotar cualquier vulnerabilidad conocida para obtener el control de un sistema. Es importante recordar que, aunque una exploración de vulnerabilidades puede revelar una vulnerabilidad, no todas las vulnerabilidades pueden explotarse con éxito o conducir necesariamente a una violación grave. Un marco de explotación como Metasploit contiene una base de datos de “exploits”

listos para usar que puede coincidir con vulnerabilidades, así como herramientas para crear y lanzar sus propios exploits.

- Paso 7: Ataque masivo

Una vez que un sistema vulnerable se ve comprometido, se puede aprovechar esto para penetrar aún más en la red. Por ejemplo, si es posible acceder al archivo de contraseñas de un servidor, una herramienta de descifrado de contraseñas puede generar contraseñas valiosas. Usando el conocimiento obtenido de la fase de reconocimiento, estas contraseñas pueden usarse para comprometer más sistemas y acceder a más datos.

Una herramienta de descifrado de contraseñas reconocida es John the Ripper, para procesar archivos de contraseñas que se extraen de la red que está probando. También se puede utilizar la herramienta Hydra, la cual es utilizada para generar un ataque de fuerza bruta de inicio de sesión paralelizada que puede intentar iniciar sesión en servicios como ftp al intentar diversas combinaciones múltiples de inicio de sesión y/o contraseñas en un corto tiempo.

- Paso 8: Phishing / Ingeniería social

Uno de los eslabones más débiles en una organización sigue siendo su propio personal, por lo que se debería intentar engañar a los usuarios mediante diversas técnicas. Eso significa enviar correos electrónicos de phishing o simplemente llamarlos para tratar de convencerlos para revelar detalles de inicio de sesión u otro tipo de información confidencial.

Revisiones generales:

1. Aplicaciones WEB: Revisar si las aplicaciones son capaces de identificar ataques SPAM en los formularios de contactos utilizados en las páginas web.
2. Servidores Proxy: Revisar si el tráfico de red está siendo monitoreado por dispositivos proxies, estos dispositivos complican a los hackers la obtención de información interna de la organización.

3. Filtros AntiSpam: Revisar si el tráfico de correo entrante y de salida es valorado por una aplicación antispam de manera que se bloquee correo no deseado.
4. Firewalls: Corroborar la existencia de Firewalls en la red de manera que se logre bloquear acceso no autorizado a las diversas redes que existan en la compañía.
5. Exploits: Tratar de generar ataques utilizando la herramienta Metasploit de manera que se logre encontrar diversos problemas en las aplicaciones y equipos de la organización.
6. Passwords: Verificar que los nombres de usuario y contraseñas viajan encriptados por la red utilizando protocolos seguros como HTTPS o SSH, entre otros. Los passwords del personal deben ser mínimo de 8 caracteres con números y caracteres especiales.
7. Nombres de usuario: Evitar el uso de usuarios por defecto como admin, administrador o cisco, entre otros.
8. Cookies: Corroborar que la información almacenada en las cookies de la página web no se encuentre en texto plano.
9. Vulnerabilidades: Uso de herramientas como NESSUS u OpenVas para el análisis de vulnerabilidades de los equipos.
10. Puertos: Analizar que solo puertos específicos se encuentran abiertos en la red de la empresa, corroborar que puertos como HTTP, Telnet o FTP, entre otros, se encuentran deshabilitados.
11. Red Inalámbrica: Revisar que la red Wireless utilice protocolos como WPA2 y la contraseña es relativamente segura.
12. Métodos HTTP: Revisar que los comandos PUT y DELETE no están habilitados en el servidor WEB.
13. Accesos aplicaciones: Revisar que las aplicaciones se bloquean después de 3 o 4 intentos de acceso fallidos.
14. Detalles internos de los sistemas: En caso de fallas o problemas de los sistemas o aplicaciones de la organización, por ningún motivo se debe revelar información sensible a usuarios no administradores.

15. Escaneo de archivos: Todos los archivos deben ser escaneados por un antivirus antes de ser subidos a servidores internos.
16. SQL Injection: Verificar que los servidores no son vulnerables a problemas de SQL injection.
17. Cross-Site Scripting (XSS): Revisar que las aplicaciones WEB no tienen problemas de XSS.
18. Permisos de acceso: El acceso a los diversos servicios de la organización debe ser gestionado por un administrador de sistemas que valore el acceso que requieren los distintos usuarios de la compañía.
19. Terminación de sesiones: Corroborar que existe un tiempo máximo de conexión a las diversas aplicaciones, de manera que una vez concluido el tiempo el usuario deba reautenticarse.
20. Versiones actualizadas: Revisar que los sistemas operativos y aplicaciones están corriendo la última versión del sistema.
21. Buffer overflow: Hacer un constante monitoreo de la memoria y CPU de los dispositivos de red de manera que se logre detectar problemas anómalos por medio de estos detalles.
22. Ataques por fuerza bruta: Analizar si los sistemas son seguros a ataques por fuerza bruta.
23. Ataques DoS: Revisar que los equipos son capaces de mitigar problemas por ataques DoS o DDoS.

4.3 Hallazgos

- El área de servicio al cliente del ICE no tiene conocimiento acerca de las leyes de protección de datos (ley 8968).
- Pocos recursos y personal por parte de la PRODHAB para auditar a las empresas que inscriben las bases de datos y determinar si estas cumplen con los requisitos de seguridad de la información.
- Desconocimiento por parte del personal del ICE del funcionamiento de los servicios que se brindan.
- Poca inscripción de bases de datos personales por parte de las empresas ante la PRODHAB, el ICE no tiene sus bases de datos personales inscritas ante este ente.
- Falta de validación por parte del departamento de tecnologías de información mediante pruebas de penetración, de las medidas de seguridad que se implementan en los data centers principales.
- La deshabilitación del GPS en dispositivos móviles no exime a los usuarios de que se conozca su ubicación real.
- Falta de unificación en los distintos departamentos del ICE a nivel de seguridad de la información. Si bien es cierto existe un departamento encargado de esta área para velar por la seguridad de toda la institución, no se logró identificar que exista unificación a nivel de los departamentos.

Capítulo V

Diagnóstico

5. Diagnóstico

Entrevista a personal del departamento DCTI, encargados de la gestión de los archivos IPDR y CDR.

1. **¿El servidor asignado para la gestión de los archivos CDR recibe mantenimiento periódicamente?**

Sí, por contrato cada 6 meses, existen 2 tipos de mantenimiento, correctivo y preventivo. El preventivo por lo menos 2 veces por año, el cual es aplicación de parches (por parte del proveedor, en este caso HPE), si sale algo crítico la aplicación es de inmediata, el correctivo es por ejemplo un disco duro se descompuso y se debe reemplazar, cambios de kernel, y situaciones similares se aplican más seguidamente.

2. **¿Existe un Sistema de Gestión de Seguridad Informática en la Empresa?**

Sí existen, hay diversas oficinas encargadas de aplicar la gestión de seguridad informática y también hay regulaciones a lo interno como aplicación de bitácoras de seguridad.

3. **¿Conoce sobre la norma ISO 27001? ¿Ha utilizado o implementado algún control de seguridad de la información basado en la norma ISO27001?**

Sí se ha aplicado, por auditoría se tuvo que hacer, las auditorías se realizan 2 veces al año, actualmente KPMG es quien realiza estas acciones a lo externo.

4. **¿La compañía capacita al personal en temas de seguridad informática?**

Sí, se tienen aproximadamente 3 años y medio donde se dan charlas de seguridad y ciberseguridad en toda la corporación.

5. **¿Existe alguna política para el cambio regular de las contraseñas?**

Sí, dependiendo de los sistemas (capacidad y criticidad). Para el servidor que gestiona los CDR existen varios tipos de usuarios, se utiliza LDAP para el cambio de las contraseñas.

6. **¿Existe un manual de funciones y responsabilidades de seguridad de la información?**

Sí existen, todos los usuarios conocen sus roles y responsabilidades, hay dueños de la información, administradores entre otros muchos más usuarios que necesitan conocer bien sobre esto.

7. **¿Qué personal tiene acceso al servidor que guarda los archivos CDR?**

En general solo los administradores, solo el grupo que le da servicio de soporte al Sistema Operativo y Hardware del equipo; en estos momentos solo este grupo es administrador, somos 4 personas. El acceso físico queda registrado en cámaras y se debe rellenar una bitácora cada vez que se ingresa.

8. **Cuándo ocurre un evento relacionado con seguridad de la información, ¿sabe a quién reportarlo?**

No hemos tenido problemas de seguridad en nuestra infraestructura debido a que se tiene bien delimitado los accesos, solo ciertas IPs pueden acceder a los servidores, pero en caso de algún problema se debe reportar al departamento de DPSI (Dirección Protección y Seguridad Institucional).
El ICE tiene un software (NESSUS) que se encarga de ver las vulnerabilidades que tiene un servidor, pero hasta la fecha no se ha contratado a un experto en seguridad para que realice pruebas de penetración.

9. **¿Considera necesario que la compañía invierta en el análisis para la implementación de un Sistema de Gestión de Seguridad de la Información?**

Sí claro, en el ICE nos basamos en ITIL para procesos, ISO 27001 para la parte de seguridad de información, ISO 14000 para el proceso de calidad total y está en proceso de aplicarse a toda la corporación.

10. ¿Qué tipo de seguridad se utiliza para el servidor que maneja los archivos CDR? Antivirus, Antispyware

Es un servidor UNIX, la seguridad lógica a nivel de usuario se limita la información que pueden ver los usuarios, además de la seguridad física que es obviamente restringido, a nivel de ambientes corporativos no se utiliza Windows.

11. ¿Existe alguna política anticorrupción?

Nosotros como funcionarios públicos se tiene prohibido el tráfico de influencias, la venta de información empresarial es sinónimo de cárcel o espionaje de información empresarial, que es darle datos a la competencia, nos aplican todas las leyes y por lo tanto no se debería de recurrir a estas prácticas.

Todo lo que se haga en estos sistemas queda registrado y es auditado por el departamento de auditoría. Las auditorías se hacen en tiempo real y se guardan los registros por 2 años aproximadamente.

12. ¿Existen zonas restringidas de acceso de personal?

Se usa badge institucional, para los departamentos SOC se debe meter badge, luego clave y finalmente se utiliza huella digital, a la parte del data center no se puede ingresar sin autorización previa y probablemente no se logre entrar a la parte donde están los servidores.

13. ¿Tienen controles? Uso de internet, correo electrónico, control de acceso.

Sí hay, de todo.

A nivel de red institucional no se puede ingresar a redes sociales, se necesita autorización previa, solo personal de Dirección de Comunicación tiene acceso a

redes sociales, esto debido a que ellos en su mayoría son periodistas, hacen anuncios, entre otros.

La red de servidores no tiene acceso a internet. En caso de Windows para hacer actualizaciones se utiliza WSUS.

Para la parte de correo electrónico no hay control, últimamente el ICE va a adquirir un DLP (Data Loss Prevention) y esto ayudará a eliminar todos aquellos correos que no sean de uso institucional, todo esto con el fin de prevenir la fuga de información.

14. ¿Todo el software que se maneja en los servidores se encuentra licenciado?

Sí, es obligatorio. Los fabricantes también hacen auditorías para ver el cumplimiento de licenciamiento.

15. ¿Se ha hecho algún tipo de análisis de riesgos en los últimos meses? Como se mitigan los riesgos

Efectivamente se realizan análisis de riesgos, se realizó hace poco un análisis de riesgos para la parte física, pero no se realizan muy a menudo. Los auditores de seguridad de la información son los que se encargan de realizar ese análisis, pero no existe suficiente personal para realizar este trabajo. Debido a que la cantidad de equipos es muy grande, el análisis de riesgos no se puede realizar a todos los equipos. Algunas revisiones se realizan de la mano del proveedor de los equipos de cómputo, el cual brinda la posibilidad de utilizar herramientas de análisis para dicho fin. No existen fechas o periodos definidos para realizar este tipo de análisis.

16. ¿La privacidad y la seguridad para los archivos CDR se ampara bajo alguna ley?

Ley de Telecomunicaciones, por ser empresa pública también debe ampararse bajo varias leyes las cuales definen el nivel de responsabilidad que se tiene.

17. Maneras de acceder al servidor que gestiona los archivos CDR.

Se debe tener permiso para acceder de manera remota, los servidores físicos no se encuentran en Costa Rica, el acceso es por medio de SSH.

18. ¿Cómo funciona la política de respaldos?

Los respaldos se manejan de diferentes formas, los datos más críticos se respaldan periódicamente, por ejemplo, los registros donde se guardan las transacciones de la base de datos, pero si la base de datos es muy pesada no se respalda todos los días. En general la política se basa en el tipo de dato, la criticidad, el objetivo, entre otras cosas. La política también debe basarse en algunas regulaciones.

19. ¿Existe algún manual de sanciones en caso de divulgación de datos privados por parte de algún funcionario?

Se cuenta con un código de ética y la Ley Orgánica del ICE, además de las regulaciones a nivel nacional para los profesionales informáticos.

20. ¿Qué tipo de motor de base de datos utilizan?

Son muchos los tipos de bases de datos, pero no podemos indicar la información específica.

21. ¿Los datos capturados son analizados por el ICE o por un tercero?

Los archivos CDR son manipulados por muchos departamentos en la empresa, pero solo el ICE manipula los datos como tal.

22. ¿Los datos de geolocalización que capturan son resguardados por el ICE o por terceros?

Son resguardados por el ICE y no se utilizan servicios en la nube para resguardarlos.

23. ¿Existe un sitio alterno donde respalden los datos de los usuarios?

Sí, existen muchos sitios alternos en el territorio nacional donde se replica la información e infraestructura.

24. ¿Qué categoría de TIER es el Datacenter del ICE?

Se cuenta con varias categorías de TIER, los más críticos son TIER 3, aunque no se cuenta con la certificación respectiva.

Entrevista Wendy Rivera, Directora Nacional de la Agencia de Protección de Datos de los Habitantes (PRODHAB).

1. **¿Un operador de telefonía celular debe registrar sus bases de datos de sus usuarios ante la PROHAB?**

De acuerdo con la normativa vigente en esos momentos, independientemente a lo que se dedique una empresa, si comercializa esos datos o bien dicho obtiene ganancia sobre esos datos, sí tiene que registrar su base de datos. Importante recalcar que no se toma como transferencia si es bajo el mismo grupo comercial, es decir si es dentro del mismo grupo de interés económico, si la organización es externa si debe registrar la base de datos.

2. **¿El derecho de acceso de información en operadores de servicio de telefonía celular incluiría brindar la información sobre los datos de geolocalización?**

Es muy importante que, en el caso de acceso de la información, cuando un titular solicita los datos que se tienen registrados sobre él, tienen que incluirse absolutamente todos los datos que se tienen dentro de la base de datos. En tema tradicional esto quiere decir nombre y cédula, entre otras, y lo no tradicional como imágenes, ubicaciones, videos (en caso de cámaras de video vigilancia) son datos

inherentes de la persona que la hacen identificable y debe incluirse dentro de la información que solicita.

3. **¿Cuánto tiempo puede guardar un operador de telefonía celular la información de sus clientes?**

Si una persona tiene una relación comercial con una empresa en este caso de telefonía, mientras dure la relación comercial puede mantenerlo en sus bases de datos, la situación cambio cuando esa relación culmina, mientras no haya deuda y no se dejó nada pendiente, a partir de ese momento se habla de derecho de olvido el cual es de 10 años. El otro tiempo que se aplica en término comercial, aplicable en organizaciones como SUGEF, es de 4 años, pero en términos generales se puede guardar hasta 10 años excepto que en el contrato se establezca un tiempo menor, pero no puede sobrepasar los 10 años.

4. **¿Realiza la PROHAB algún tipo de auditoría que regule o fiscalice las instituciones públicas que utilizan bases de datos que contienen información personal?**

Dentro de las atribuciones de la agencia se encuentra el poder de solicitar información o poder verificar el cumplimiento de la normativa, independientemente si se trata de una institución pública o privada. La ley en el artículo 16 le da competencia para que personas físicas o jurídicas o entidades públicas, se tiene la posibilidad de acceder (siempre y cuando para que sea para verificación o que estemos ante la noticia de que haya algún tipo de irregularidad). En este caso los recursos son limitados, por lo tanto, se realizan muestreos en el tipo de actividad y de acuerdo con esa información se replantean o se hace otro tipo de verificación.

5. **La ley indica que el tiempo que puede conservar una empresa mis datos luego de haber terminado la relación comercial es de 10 años, ¿por qué tanto tiempo si ya la relación terminó?**

El motivo es que es una disposición legal y es un estándar internacional, el derecho al olvido como tal si se busca en distintas normativas es de 10 años. En material laboral se guardan datos de exempleados, pero en el caso de la Caja en tema de obrero personal el plazo de prescripción es sumamente largo. Esto se ve como respaldo jurídico en las transacciones, ya que puede haber reclamos en la parte comercial, en lo civil, penal y los plazos de prescripción son amplios. Es por esto que no se pueden establecer tiempos cortos, porque el que haga el tratamiento como el titular de los datos estaría en un estado de indefensión, entonces se ve como un respaldo de seguridad jurídica. Se debe recordar que los 10 años se establecen como un tope para una cuestión que no hay pena perpetua, o sea, no hay una sanción permanente y que debe establecerse algún plazo, y el plazo por norma internacional es ese, por lo tanto, se decidió tomar ese tiempo.

6. **Cuando se inscribe una base de datos se solicita que se indique el sistema, programa y método o proceso utilizado para el tratamiento de datos, ¿una vez recibida esa información se verifica el cumplimiento de sus controles?**

Cuando se hace la inscripción como tal se hace una revisión jurídica y técnica, y eso está sujeto a revisarse en cualquier momento. Además, queda sujeto a que periódicamente se solicite que se haga actualización de esa información y que se pueda verificar, o también en cualquier momento de oficio la agencia puede ir a solicitar la verificación, no es una cuestión para el momento de la inscripción.

7. **¿Apoya la PROHAB en los derechos ARCO?**

La base de nosotros de protección de datos personales es lo que internacionalmente se conoce como ARCO, lo que pasa es que en el caso de

nuestro país es que el ARCO como tal no está sino se le conoce con otra nomenclatura. A nivel de Costa Rica se le podría conocer como "AR" debido a que en la "R" se metió la parte de Rectificación, Cancelación y oposición, también de acuerdo con las últimas modificaciones en la materia a los derechos ARCO se le ha agregado la portabilidad. Algunos ven este punto como una parte del ejercicio del acceso de la información como una forma diferente de hacerlo, pero se reconoce como un derecho adicional que es justamente poder solicitar los datos en un formato interoperable donde se pueda transportar a otro operador y se pueda realizar, por lo tanto, los derechos ARCO se están transformando en ARCOP. En nuestro país es la base de los derechos de los habitantes, aunque no está consignado con esas siglas debido a que en rectificación se incluyeron los otros conceptos.

8. **¿Qué sucede con el tema de aplicar la normativa de protección de datos en los casos de empresas no domiciliadas en Costa Rica por ejemplo compañías de aplicaciones móviles como nos aseguramos de que respeten nuestra ley?**

En cuestión de la normativa siempre hay una cuestión de territorialidad sujetos activos y pasivos en el cual está muy determinado el principio de territorialidad, por lo tanto, no podemos extender nuestras competencias. Además, en el caso de funcionarios públicos estamos sujetos a un principio de legalidad, el cual tenemos que respetar siempre, y no podemos ir más allá. Sin embargo, en la parte de educación sí es importante recordar e inculcar en el habitante que al momento que uno descarga una aplicación hay una serie de condiciones que esa aplicación trae, como política de privacidad, dirimir conflictos y otras y eso me dice a mí si yo acepto condiciones o no acepto. Eso es una fase contractual en la cual la persona accede a esas condiciones. Cabe destacar que no es una cuestión de firmar y así quedó, ya que las personas no pueden renunciar a sus derechos, pero en el caso de esa materia contractual sí es muy importante siempre leer las condiciones de seguridad y condiciones generales de la aplicación debido a que en esos casos se aceptan los escenarios propuestos.

Tenemos también el comercio electrónico, en este tema hace aproximadamente un mes se dio una modificación en el reglamento del consumidor donde se viene a regular y a establecer muy de la línea de protección de datos personales una serie de condiciones de acceso de la información, de mantener sede, garantías y demás, que eso también le da al consumidor garantías adicionales para poder proteger no solo sus datos, sino también la parte económica. Hay otro tipo de aplicaciones en las que por cuestión de ayuda entre las agencias (nosotros pertenecemos a la Red Iberoamericana en Protección de Datos Personales), a veces entre agencias se dan apoyo para verificar si se cumplen con los requisitos necesarios.

En el caso de UBER nosotros estamos haciendo las verificaciones o en cualquier otro tipo de vulnerabilidades o brechas que se han conocido a través de los medios de comunicación, sí es muy importante que en el caso de nosotros obviamente le apostamos a la revisión y que estén debidamente registradas las empresas que deban registrarse, pero también hay una cuota sumamente importante que está en la educación de los habitantes de que sepan cuáles son las consideraciones que deben tener, que lean acerca del tema. Si se habla acerca de dispositivos de internet de las cosas, todavía es mucho más importante porque se nos van presentando panoramas donde no solo debemos hacer regulaciones en términos del estado como tal, sino que también tenemos que asumir una actitud de auto regulación porque la primera línea de protección somos nosotros mismos. Y no solo es una cuestión de nosotros como adultos, sino que también debemos pensar en las nuevas generaciones que ya toman como naturaleza este tipo de dispositivos, pero las condiciones de seguridad, protección y demás es una parte que debemos inculcar. Inclusive en adultos mayores, que quedan más expuestos ya que deben adaptarse a una nueva forma de hacer las cosas. Por lo tanto, sí es un trabajo arduo que hay que hacer, pero no solo una cuestión de la agencia o cuestión estatal sino algo que debe venir de la ciudadanía por ser la primera línea de protección. Todos estos temas están relacionados con un cambio de cultura, un cambio grande de la forma en que hemos visto que podemos confiar; pero también se debe preguntar, no solo es una cuestión de confiar sino conocer nuestros derechos y las instancias a las que podemos recurrir.

Conclusiones y Recomendaciones

Conclusiones

- Las empresas telefónicas capturan muchos datos personales. Luego de realizar el análisis de los archivos CDR e IPDR podemos concluir que la privacidad está en manos de estas empresas, pero podemos confiar en que las mismas resguardan esta información, por lo tanto, no es el mayor riesgo a la privacidad.

- Uno de los mayores riesgos a la privacidad es el uso de aplicaciones móviles, las cuales utilizan información personal para generar ganancias y esto con el consentimiento de los usuarios. Y es que los usuarios están dispuestos a brindar sus datos personales a cambio de un servicio que ayudará a agilizar el diario vivir, pero muchos de ellos no son conscientes del peligro que esto representa.

- Con el análisis de los archivos CDR e IPDR a los que se tuvo acceso, se concluye que existen formas variopintas de rastreo de información de usuarios de los sistemas de telefonía, que no necesariamente tienen que ver con sistemas GPS, y por su naturaleza técnica, los usuarios no tienen manera de evitar:

    - Se puede conocer la ubicación relativa de una persona con base en el registro de las celdas almacenadas en el CDR, ubicadas en las torres de telefonía a las cuales el terminal se conectó en un lapso determinado.
    - Se puede conocer la ubicación relativa de una persona con base en el registro de las IP de salida almacenadas en el IPDR, que pertenecen a los puntos de acceso a Internet donde el terminal se conectó en un lapso determinado.
    - Se puede conocer la ubicación relativa de una persona con base en el registro de las coordenadas de latitud y longitud almacenadas en el

IPDR, que pertenecen a los puntos de acceso a Internet donde el terminal se conectó en un lapso determinado.

- Estos registros basados en archivos IPDR y CDR de rastreo pasivo sirven para ayudar a fuerzas policiales en caso de secuestros extorsivos y ubicación relativa de personas extraviadas.
- Se puede conocer la ubicación aproximada de un usuario de telefonía celular gracias a la triangulación de las señales de radio de los terminales. Esto se debe a que las torres celulares controlan constantemente la fuerza de las señales de telefonía móvil. Los celulares o terminales poseen rangos en los cuales se puede obtener y enviar llamadas. Este intercambio de información constante permite juzgar la ubicación de dichos terminales en tiempo real.

- Son muchas las regulaciones a las que se enfrentan las empresas en nuestro país, pero estas no son acatadas o conocidas por dichas empresas. La ley de protección de datos a la persona obliga a inscribir las bases de datos de uso comercial, pero son muy pocas las empresas que realizan la inscripción de estos datos. Además, la PRODHAB no cuenta con suficiente personal para realizar un estudio de cuáles son las empresas que deben inscribir estas bases de datos, por lo tanto, el cumplimiento de esta ley no se lleva a cabo. Este tipo de falta no tiene ninguna implicación, ya que lo único que se sanciona es el mal uso o tratamiento que se le dé a los datos personales de un cliente.

- La implementación por fases de la guía metodológica es un proceso metódico, guiado y estratégico que permite al departamento DPSI garantizarse y asegurarse la correcta aplicación y calidad de las pruebas de penetración. La alineación e integración de la estructura documental genera una cultura de sensibilización hacia los colaboradores en el ámbito de la ciberseguridad y permite seguir el estándar ya instaurado y la madurez del proceso de gestión de la calidad.

- La elaboración de una guía de pruebas de penetración le permite a la organización conocer cuáles son los sistemas críticos que se van a probar y prepararse con anticipación en caso de algún ataque cibernético que pueda llegar afectar el correcto funcionamiento de los mismos. Esta guía también delimita lo que se puede hacer y lo que no se puede realizar durante la ejecución del proceso (previamente aprobado por la gerencia), de manera que se evitan improvisaciones innecesarias.

  Es muy importante que estas pruebas se realicen en ambientes virtualizados, esto evita que se manipulen los equipos de producción y previene posibles afectaciones típicas de la realización de estas pruebas a nivel de hardware o software de los sistemas.

Recomendaciones

- Se recomienda que el equipo que trabaje en los procesos propuestos en este proyecto reciba capacitaciones acerca de la norma ISO 27001 e ISO 27002, con el fin de que el personal conozca más sobre el estándar, además de adquirir experiencia en cómo implementarlo y siempre efectuar una mejora continua.

- La alta gerencia debe estar involucrada activamente en el proceso de pruebas de penetración de manera que exista un compromiso y liderazgo en su ejecución.

- Se recomienda emprender campañas para crear una cultura de sensibilización en todo el personal de la organización, y generar así conciencia sobre la importancia de notificar incidentes o cualquier anomalía que se presente, de manera que se prevengan vulnerabilidades o problemas en la compañía.

- Para poder gestionar una crisis y mantener la confianza del personal y de sus clientes, las organizaciones deben garantizar que existe un flujo de comunicación transparente y apegado al ordenamiento jurídico costarricense.

- La realización de pruebas de penetración al menos 2 veces al año es necesaria y prácticamente una necesidad para corroborar que la seguridad de la organización funciona correctamente; esto evitará sanciones a la compañía y resguardará los datos a todos los usuarios del ICE.

- Mantener una capacitación continua por parte del personal del ICE de las leyes de protección de datos para garantizar el cumplimiento de las mismas.

Glosario de términos

Amenaza: Causa de un incidente no esperado el cual puede impactar sistemas o equipos de la organización.

Análisis de impacto: Proceso de análisis de los efectos negativos que una interrupción podría causarle a una organización.

Análisis de riesgos: Proceso de análisis para entender la naturaleza y el nivel de impacto que un riesgo puede ocasionarle a una organización.

Auditoría: Proceso sistemático utilizado para obtener evidencia como documentación que permita emitir una opinión independiente y adecuada.

Backdoor: En español significa puerta trasera. Programa que se introduce en el ordenador y establece una puerta trasera a través de la cual es posible controlar el sistema afectado, sin conocimiento por parte del usuario.

Buffer Overflow: En español significa desbordamiento de buffer. Error de software que se produce cuando un programa no controla adecuadamente la cantidad de datos que se copian sobre un área de memoria reservada, excediendo el uso de cantidad de memoria asignado. Los hackers aprovechan estos problemas para ejecutar código malicioso en el equipo de una víctima.

Confidencialidad: Propiedad o atributo que consiste en proporcionar acceso a los sistemas de información únicamente a aquellos usuarios autorizados en tiempo y forma determinados y negar el acceso a terceros no autorizados.

Cross-Site Scripting (XSS): Tipo de inseguridad informática típico de las aplicaciones Web, que permite a una tercera persona inyectar en páginas web visitadas por el usuario código JavaScript o en otro lenguaje similar evitando medidas de control.

CVE: Common Vulnerabilities and Exposures. En español significa vulnerabilidades y exposiciones comunes. Esta es una lista de información registrada sobre vulnerabilidades de seguridad conocidas, en la que cada referencia tiene un número de identificación único.

Disponibilidad: Capacidad de un proceso o servicio, a ser accesible y útil por los usuarios autorizados cuando estos lo requieran.

DDoS: Siglas para Distributed Denial of Service. En español significa denegación de servicio distribuida, es un tipo especial de DoS de manera conjunta y coordinada entre varios equipos.

Estos ataques consiguen el objetivo de hacer inaccesible la máquina víctima agotando el ancho de banda o sobrepasando la capacidad de procesamiento.

DoS: Siglas para Denial of Service. En español significa Denegación de Servicio. Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

Estándar: Conjunto de medidas o requisitos mínimos aceptables para que una operación en específico pueda funcionar de manera correcta asegurando la calidad en los servicios**.**

Eventualidad: Situación o hecho que sucede sin previo aviso, e impacta de manera negativa una organización.

Guía metodológica: Documento técnico compuesto por un conjunto de conceptos, sugerencias e instrucciones para poder realizar con éxito una tarea en específico.

Hacker: Persona que a través de medios técnicos o de ingeniería social consigue acceder o introducirse en un sistema informático con intenciones diversas, ya sea por simple entretenimiento o con la intención de descifrar el funcionamiento interno

de los equipos y servidores de Internet. Asalta así los sistemas de seguridad sin ocasionar daños en ellos.

Incidente: Circunstancia o suceso que ocurre de manera inesperada ocasionando problemas de afectación de servicios al negocio de una organización.

Información: Conjunto de datos procesados utilizados para construir un mensaje. La información es la base del conocimiento del ser humano.

Ingeniería Social: Mecanismo social para obtener información o datos de naturaleza sensible.

Integridad: Conjunto de medidas de seguridad que se incluyen en un sistema de información, que garantizan la exactitud de los datos transportados o almacenados, evitando su alteración, pérdida o destrucción, ya sea de forma accidental, por fallos de software o hardware, por condiciones medioambientales o bien, por intervención de terceros con fines fraudulentos.

IoT: Internet de las cosas.

ISO: (Organización Internacional de Normalización) Es una organización no gubernamental internacional independiente, esta organización se dedica para la creación de estándares internacionales.

ISO 27001: Estándar o norma de la Organización Internacional de Estandarización que define los objetivos de control para la gestión de la seguridad de la información.

ISO 27002: Estándar o norma de la Organización Internacional de Estandarización que proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información para iniciar, implantar o mantener un SGSI.

SGSI: Sistema de Gestión de Seguridad de la Información.

Matriz de riesgos: Es una herramienta utilizada para identificar los riesgos más significativos que pueden afectar a una organización, esta herramienta ayuda a ejercer un mejor control de riesgos y brinda seguridad a la compañía.

Mitigación de riesgos: Proceso en donde se eliminan, disminuyen o transfieren riesgos a los que se encuentra expuesta la organización de manera que su afectación no cause daños importantes en el negocio.

Plan de continuidad del negocio: Medidas tomadas por una organización para recuperar y restaurar los servicios críticos del negocio en un tiempo determinado después de un incidente.

Phishing: Técnica de ingeniería social utilizada por los hackers para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito/débito, y que se hace pasar por una comunicación confiable y legítima.

Privacidad: Ámbito de la vida personal de un individuo o de un grupo que debe ser reservado y mantenerse confidencial.

Política: Directriz que debe ser divulgada y acatada por el personal de la organización, en ella se encuentra los lineamientos por seguir para la toma de decisiones, facilitando la implementación de estrategias.

Procedimientos: Conjunto de acciones documentadas que contiene la descripción de cómo debe ser desarrollada una actividad dentro de la organización.

Riesgo: Potencial de que una amenaza específica logre explotar las debilidades de un activo o servicio, causando daños a la organización.

SQL Injection: Tipo de ataque a una base de datos en el cual, por la mala filtración de las variables, se puede inyectar un código creado por el atacante al propio código fuente de la base de datos.

Vulnerabilidad: Debilidad de un sistema informático o activo que puede ser explotada por una amenaza, y que es utilizada para generar daños a una organización.

Bibliografía

Álvarez, J. A. (s.f.). *ASIFUNCIONA.* Obtenido de ASIFUNCIONA: http://www.asifunciona.com/electronica/af_gps/af_gps_10.htm

ALVEAR, R. (2 de FEBRERO de 2017). *ENFOQUEUTE.* Obtenido de ENFOQUEUTE: http://ingenieria.ute.edu.ec/enfoqueute/index.php/revista/article/view/121/127

ARROW. (1 de 7 de 2015). Obtenido de ARROW: https://www.arrow.com/es-mx/research-and-events/articles/protocols-for-the-internet-of-things

Bartley, K. (s.f.). *onsip*. Obtenido de onsip: https://www.onsip.com/blog/what-are-call-detail-records-cdrs

Cendon, B. (16 de ENERO de 2017). *BCENDON*. Obtenido de BCENDON: http://www.bcendon.com/el-origen-del-iot/

CISCO. (2014). *CISCO.* Obtenido de CISCO: https://www.cisco.com/c/dam/assets/global/ES/offers/datacenter/potential/dc-05-attaining-iot-value-wp-cte-es-eu.pdf

Cruz, E. V. (09 de 05 de 2016). *securingtomorrow.* Obtenido de securingtomorrow.: https://securingtomorrow.mcafee.com/languages/espanol/la-vulnerabilidad-del-iot-un-riesgo-para-las-empresas/

Española, R. A. (s.f.). *RAE*. Obtenido de RAE: http://www.rae.es/

EVANS, D. (4 de 2011). *CISCO.* Obtenido de CISCO: https://www.cisco.com/c/dam/global/es_mx/solutions/executive/assets/pdf/internet-of-things-iot-ibsg.pdf

González, G. (27 de 9 de 2014). *HIPERTEXTUAL.* Obtenido de HIPERTEXTUAL: https://hipertextual.com/archivo/2014/07/protocolo-xmpp/

GSMA. (11 de ENERO de 2011). *GSMA*. Obtenido de GSMA: https://www.gsma.com/publicpolicy/wp-content/uploads/2016/02/GSMA2016_Guidelines_Mobile_Privacy_Principles.pdf

H, G. (14 de 6 de 2015). *acdemocracy.* Obtenido de acdemocracy: http://acdemocracy.org/gps-vulnerability-options-and-alternatives/

INFOBAE. (22 de 11 de 2017). Obtenido de INFOBAE: https://www.infobae.com/america/tecno/2017/11/22/por-que-google-registra-la-ubicacion-de-los-usuarios-aun-cuando-la-localizacion-del-celular-este-apagada/

Iraola, A. (2016). *Teleco world*. Obtenido de Teleco world: http://telecoworld.org/sistemas-de-navegacion-gps-vs-glonass-vs-galileo/

ISO27000. (s.f.). *ISO27000*. Obtenido de ISO27000: http://www.iso27000.es/sgsi.html

Keeling, S. D. (2015). *IBM.* Obtenido de IBM: http://www-05.ibm.com/services/es/bcs/pdf/Ciudades_mas_inteligentes.pdf

Latinoamérica, R. G. (s.f.). *Red Gráfica Latinoamérica.* Obtenido de Red Gráfica Latinoamérica: http://redgrafica.com/Breve-historia-de-los-celulares-y

Madrigal, A. (9 de 2 de 2016). *costarica2050*. Obtenido de costarica2050: http://costarica2050.cr/el-internet-de-las-cosas-tiene-gran-relevancia-en-el-consejo-de-innovacion.html

Manaure, A. (22 de FEBRERO de 2017). *PC WORLD.* Obtenido de PC WORLD: http://www.pcworldenespanol.com/2017/02/22/vulnerabilidad-dispositivos-iot-acelera-ataques-ddos/

Mexico, C. (2014). *CNDH*. Obtenido de CNDH: http://www.cndh.org.mx/sites/all/doc/Acciones/Acc_Inc_2012_32_Demanda.pdf

Olguín, M. (16 de 8 de 2016). *GACETA MEXICO.* Obtenido de GACETA MEXICO: http://www.gaceta.unam.mx/20160815/hay-22-mil-millones-de-dispositivos-digitales-conectados-a-internet/

Paganini, P. (23 de 2 de 2012). *securityaffairs*. Obtenido de securityaffairs: http://securityaffairs.co/wordpress/2845/hacking/gps-spoofing-old-threat-and-new-problems.html

PalazzesI, A. (23 de 7 de 2010). *NEOTEO.* Obtenido de NEOTEO: http://www.neoteo.com/historia-del-gps-como-el-mundo-dejo-de-perderse/

Paniagua, E. (28 de 4 de 2017). *RETINA.* Obtenido de RETINA: https://retina.elpais.com/retina/2017/04/27/tendencias/1493283914_759472.html

PARTNER, C. (20 de 12 de 2016). *CHANNEL PARTNER.* Obtenido de CHANNEL PARTNER: http://www.channelpartner.es/seguridad/noticias/1094530002502/los-ataques-a-iot-el-ransomware-o-el-phising-seran-tendencia-en-2017.1.html

PENTEST. (2017). *PENTEST*. Obtenido de PENTEST: http://www.pen-tests.com/

PRODHAB. (s.f.). *Agencia de Protección de Datos de los Habitantes*. Obtenido de Agencia de Protección de Datos de los Habitantes: http://prodhab.go.cr/reformas/

Ramírez, A. (14 de 9 de 2015). *LA PRENSA LIBRE*. Obtenido de LA PRENSA LIBRE: http://www.laprensalibre.cr/Noticias/detalle/39904/383/alonso-ramirez:-internet-de-las-cosas-en-costa-rica,-generalidades-que-deben-tenerse-presentes

RIOACHA. (5 de 3 de 2007). *ftp.ciat.cgiar.org.* Obtenido de ftp.ciat.cgiar.org: ftp://ftp.ciat.cgiar.org/DAPA/planificacion/GEOMATICA/GPS/GPS_Modulo.pdf

SUTEL. (2008). *Superintendencia de Telecomunicaciones*. Obtenido de Superintendencia de Telecomunicaciones:

https://sutel.go.cr/sites/default/files/normativas/ley_general_de_telecomunicaciones.pdf

SUTEL. (2009). *Superintendencia de Telecomunicaciones*. Obtenido de Superintendencia de Telecomunicaciones: https://sutel.go.cr/sites/default/files/normativas/reglamento_sobre_medidas_de_proteccion_de_la_privacidad_de_las_comunicaciones_decreto_ejecutivo_35205-minaet.pdf

Whittaker, J. (s.f.). *dcps*. Obtenido de dcps: https://dcps.instructure.com/courses/9336/pages/2-slash-5-the-internet-of-things

Anexos

Anexo 1: Formulario de solicitud de datos personales.

PRODHAB
AGENCIA DE PROTECCIÓN DE DATOS DE LOS HABITANTES
MINISTERIO DE JUSTICIA Y PAZ

AGENCIA DE PROTECCIÓN DE DATOS DE LOS HABITANTES (PRODHAB)

FORMULARIO PARA EJERCER EL DERECHO DE ACCESO A DATOS PERSONALES

Este formulario ha sido confeccionado por la AGENCIA DE PROTECCION DE DATOS DE LOS HABITANTES, cédula jurídica número 3-007-655746, de conformidad con lo dispuesto en la Ley N° 8968, de 7 de julio de 2011, de Protección de la Persona Frente al Tratamiento de sus Datos Personales y el Decreto Ejecutivo No. 37554-JP, de 30 de octubre de 2012, Reglamento a la Ley N° 8968. El mismo ha de ser completado por el administrado, con la información necesaria y debe ser presentado ante el Responsable de la Base de Datos.

Datos del Solicitante

Nombre completo: Marcela Hernández Ugarte.

Documento oficial de identidad: 113160460.

Teléfono: 8992-8587

Responsable de la Base de Datos o el Tratamiento

Nombre de la entidad (privada o pública): Instituto Costarricense de Electricidad.

Dirección física: Sabana Norte, San José.

Correo electrónico: atuladoice@ice.go.cr.

Teléfono: 2003-5423.

Por este medio, **EJERZO MI DERECHO DE ACCESO A DATOS PERSONALES DE LOS CUALES SOY TITULAR**, conforme a lo previsto en la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, N° 8968 y su respectivo Reglamento, solicitando:

Se me proporcione en forma gratuita toda la información que sobre mí se encuentre en su(s) base(s) de datos de los meses de octubre y noviembre, incluyendo información de geolocalización, en el plazo máximo de CINCO DÍAS HÁBILES (5) a partir de la recepción de esta solicitud, con base en el artículo 7, inciso 1) de la Ley. Vencido el plazo sin que esta solicitud sea satisfecha o fuese denegada sin justa causa, ***podrá iniciarse ante la Agencia de Protección de Datos de los Habitantes, el respectivo Procedimiento para la Protección de Derechos, con las eventuales consecuencias legales que la Ley y su Reglamento establecen.***

PRODHAB
AGENCIA DE PROTECCIÓN DE DATOS DE LOS HABITANTES
MINISTERIO DE JUSTICIA Y PAZ

AGENCIA DE PROTECCIÓN DE DATOS DE LOS HABITANTES (PRODHAB)

FORMULARIO PARA EJERCER EL DERECHO DE ACCESO A DATOS PERSONALES

Este formulario ha sido confeccionado por la AGENCIA DE PROTECCION DE DATOS DE LOS HABITANTES, cédula jurídica número 3-007-655746, de conformidad con lo dispuesto en la Ley N° 8968, de 7 de julio de 2011, de Protección de la Persona Frente al Tratamiento de sus Datos Personales y el Decreto Ejecutivo No. 37554-JP, de 30 de octubre de 2012, Reglamento a la Ley N° 8968. El mismo ha de ser completado por el administrado, con la información necesaria y debe ser presentado ante el Responsable de la Base de Datos.

Notificaciones:

Las mías en la siguiente dirección de correo electrónico marze2118@gmail.

Ruego proceder de conformidad.

Firma: _____

Fecha: 4/12/17

ICE GRUPO ICE
AGENCIA CALLE BERRO
Nombre del Funcionario
Fecha 04/12/17

Eyenill Medina.

Solicitud: 1-752582055 7.

Anexo 2: Denuncia ante la PRODHAB.

PRODHAB
AGENCIA DE PROTECCIÓN DE DATOS DE LOS HABITANTES
MINISTERIO DE JUSTICIA Y PAZ

AGENCIA DE PROTECCIÓN DE DATOS DE LOS HABITANTES (PRODHAB)

PROCEDIMIENTO DE PROTECCIÓN DE DERECHOS

1) **Datos del Denunciante.**

Nombre del denunciante:

Marcela Hernández Ugarte

Dirección exacta:

Heredia, San Francisco. Del Walmart 500 metros oeste, 300 metros sur, casa color mostaza a mano derecha.

No. Cédula o No. de Identificación: 113160460 No. Telefono: 89928587

Correo electronico: marzu2118@gmail.com

2) **Contenido de la Denuncia.** (según lo previsto en el Artículo 60 del Reglamento de la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, No.8968 publicado en La Gaceta No. 170 del 5 de setiembre de 2011).

a) Nombre del dueño o responsable de la base de datos, o bien cualquier elemento que permita identificar al denunciado (persona física o jurídica a quien se denuncia):

Instituto Costarricense de Electricidad.

b) Hechos en los que se funda la denuncia, deben ser expuestos uno por uno, enumerados y bien especificados, en forma clara y precisa:

El dia 4 de diciembre del año 2017 procedi a entregar el formulario para ejercer el derecho a datos personales en la sucursal del ICE-KOLBI de San Jose ubicado en calle 3, el dia que entregue el formulario ninguna persona que laboraba en la sucursal(ni siquiera el administrador) tenia conocimiento del procedimiento que se debia llevar a cabo y me indicaron que solo me podian entregar los datos de llamadas y no los datos que solicitaba(vease copia de solicitud adjunta), ademas me indicaron que debia realizar un pago para que esos datos me fueran entregados a lo que les indique que segun la Ley N° 8968, esos datos deben de ser entregados a mi persona de forma gratuita, por lo que procedieron a ingresar la solicitud en el sistema indicandome que no iban a entregar los datos en el plazo de 8 dias ya que ellos por ley(SUTEL) tienen un plazo mayor.
Al dia de hoy 8 de enero del año 2017 no he recibido respuesta por parte de la institución, por lo que procedo a interponer denuncia formal ante la Agencia de Protección de Datos Personales para que se proceda a investigar este caso.

c) Aportar las pruebas documentales pertinentes (es decir, toda aquella información que considere el denunciante sirva de sustento a los hechos denunciados).

d) Pretensión que formule (indicar claramente qué es lo que solicita por medio de la presente denuncia, según lo que establece la Ley 8968):

Agradezco interponer sus buenos oficios para que la información personal que fue solicitada sea entregada a mi persona lo antes posible ya que esta es requerida para una investigación académica.

e) Señalamiento de medios para recibir notificaciones: (indicar qué medio se utilizará –Correo Electrónico, Fax; en el caso del medio para notificar al Denunciado debe indicarse una dirección física exacta, según lo que establece el Art. 19 de la Ley de Notificaciones Judiciales).

e.1) Al Denunciante

Correo Electrónico: marze2110@gmail.com

e.2) Al (o los) Denunciado(s)

f) REQUISITOS ADICIONALES

f.1) En caso de señalar prueba testimonial, deberá aportarse declaración jurada de los testigos, debidamente autenticada notarialmente.

f.2) En caso de que se haya ejercido el derecho de rectificación, inclusión o supresión de datos personales, aportar copia del respectivo formulario, y la respuesta a dicha gestión en caso de existir.

f.3) Aportar fotocopia completa de la denuncia y sus pruebas, un juego de éstas para recibido y tantas fotocopias como denunciados haya.

f.4) Todos los documentos deberán ser presentados directamente en las oficinas de la Agencia de Protección de Datos de los Habitantes, sita en: Módulo 8, Edificio Administrativo, Registro Nacional, Zapote.

MARCELA CRISTINA HERNANDEZ UGARTE (FIRMA)

Firmado digitalmente por MARCELA CRISTINA HERNANDEZ UGARTE (FIRMA)

FIRMA

Fecha: 08 / 01 /2018

Anexo 3: Archivo con datos capturados por antenas de telecomunicaciones.

Documento de Geolocalización

Tec	startTime	callerNumber	servedIME	servedPDPAddress	LAC	cellID	Antena	Latitude	Longitude
LTE	46:25.0	89928587	353802089069 60	10.240.48.105	3105	28622	NULL	NULL	NULL
3g	46:32.0	89928587	353802089069 60	10.240.48.105	2105	44081	Guatuso	9.99935	-84.11484
LTE	46:43.0	89928587	353802089069 60	10.240.48.105	3105	28622	NULL	NULL	NULL
3g	34:15.0	89928587	353802089069 60	10.240.48.105	2105	44081	Guatuso	9.99935	-84.11484
3g	34:15.0	89928587	353802089069 60	10.240.48.105	2105	44081	Guatuso	9.99935	-84.11484
LTE	00:12.0	89928587	353802089069 60	10.240.48.105	3105	28622	NULL	NULL	NULL
3g	00:31.0	89928587	353802089069 60	10.240.48.105	2105	44081	Guatuso	9.99935	-84.11484
LTE	38:18.0	89928587	353802089069 60	10.240.48.105	3105	28622	NULL	NULL	NULL
3g	38:30.0	89928587	353802089069 60	10.240.48.105	2105	44081	Guatuso	9.99935	-84.11484
LTE	50:20.0	89928587	353802089069 60	10.240.48.105	3105	28622	NULL	NULL	NULL
3g	15:52.0	89928587	353802089069 60	10.240.48.105	2105	44081	Guatuso	9.99935	-84.11484
LTE	16:26.0	89928587	353802089069 60	10.240.48.105	3105	28622	NULL	NULL	NULL
3g	17:51.0	89928587	353802089069 60	10.240.48.105	2105	44081	Guatuso	9.99935	-84.11484
LTE	18:15.0	89928587	353802089069 60	10.240.48.105	3105	28622	NULL	NULL	NULL
3g	28:16.0	89928587	353802089069 60	10.240.48.105	2105	44081	Guatuso	9.99935	-84.11484
LTE	29:14.0	89928587	353802089069 60	10.240.48.105	3105	22860	NULL	NULL	NULL
3g	30:52.0	89928587	353802089069 60	10.240.48.105	2105	31701	Guatuso	9.99226	-84.14061
LTE	30:59.0	89928587	353802089069 60	10.240.48.105	3105	31701	CALLE MAYORGA AURORA HEREDIA	9.99226	-84.14061
LTE	38:36.0	89928587	353802089069 60	10.240.48.105	3105	22920	NULL	NULL	NULL
3g	41:26.0	89928587	353802089069 60	10.240.48.105	2105	22913	Guatuso	9.986042	-84.148809
LTE	41:38.0	89928587	353802089069 60	10.240.48.105	3103	35646	SUBESTACION LA CAJA	9.965353	-84.1652
3g	45:54.0	89928587	353802089069 60	10.240.48.105	2105	36370	Guatuso	9.98272	-84.16346
LTE	47:17.0	89928587	353802089069 60	10.240.48.105	3104	30721	MARRIOT	9.988361	-84.1755273
LTE	50:59.0	89928587	353802089069 60	10.240.48.105	3105	27612	NULL	NULL	NULL
3g	51:10.0	89928587	353802089069 60	10.240.48.105	2105	30173	Guatuso	9.97543	-84.15435
LTE	52:08.0	89928587	353802089069 60	10.240.48.105	3105	30178	CARIARI HEREDIA	9.975432	-84.1543466
3g	52:26.0	89928587	353802089069 60	10.240.48.105	2105	30173	Guatuso	9.97543	-84.15435
LTE	52:47.0	89928587	353802089069 60	10.240.48.105	3105	30172	CARIARI HEREDIA	9.975432	-84.1543466
LTE	01:39.0	89928587	353802089069 60	10.240.48.105	3105	30170	CARIARI HEREDIA	9.975432	-84.1543466
3g	02:33.0	89928587	353802089069 60	10.240.48.105	2105	30171	Guatuso	9.97543	-84.15435
3g	02:54.0	89928587	353802089069 60	10.192.212.131	2105	22873	NULL	NULL	NULL
LTE	03:39.0	89928587	353802089069 60	10.192.212.131	3105	22872	CARIARI	9.973115	-84.14022
3g	04:29.0	89928587	353802089069 60	10.192.212.131	2105	22873	NULL	NULL	NULL

Anexo 4: Plantilla de análisis de Riesgos.

Información General

Plan de Gestión de Riesgos	
Fecha:	
Versión:	
Encargado:	
Comentarios:	

Amenazas

Clasificación	Tipo Amenaza
Naturales	Fuego Huracán Inundación Terremoto Tormenta Tornado
Información	Alteración de datos Corrupción de datos Destrucción de información Fuga de datos Robo de información
Instalaciones	Altas temperaturas Daño en tuberías de agua Fallo de servicios de comunicaciones Humedad Interrupción de otros servicios y suministros esenciales Problemas con el suministro eléctrico
Acceso	Abuso de privilegios de acceso Ataque de intermediario (man in the middle) Caida del sistema por sobrecarga Degradación de los soportes de almacenamiento de la información Difusión de software dañino Errores de mantenimiento / actualización de equipos (hardware) Errores de mantenimiento / actualización de programas (software) Espiación Indisponibilidad del personal Pérdida de equipos Sabotaje informático Virus/Malware
Errores de configuración	Error de usuarios Error del administrador
Ingeniería social	Denegación de servicio Robo Descuido del personal Extorsión
Social	Epidemia Huelgas Pérdida de personal clave Problemas de transporte Terrorismo Vandalismo Violencia laboral

Clasificación de Riesgos

Clasificación de Riesgos		
	Riesgo	Niveles
1	Insignificante	1 - 2
2	Bajo	3 - 6
3	Moderado	7 - 9
4	Alto	10 - 16
5	Critico	17 - 25

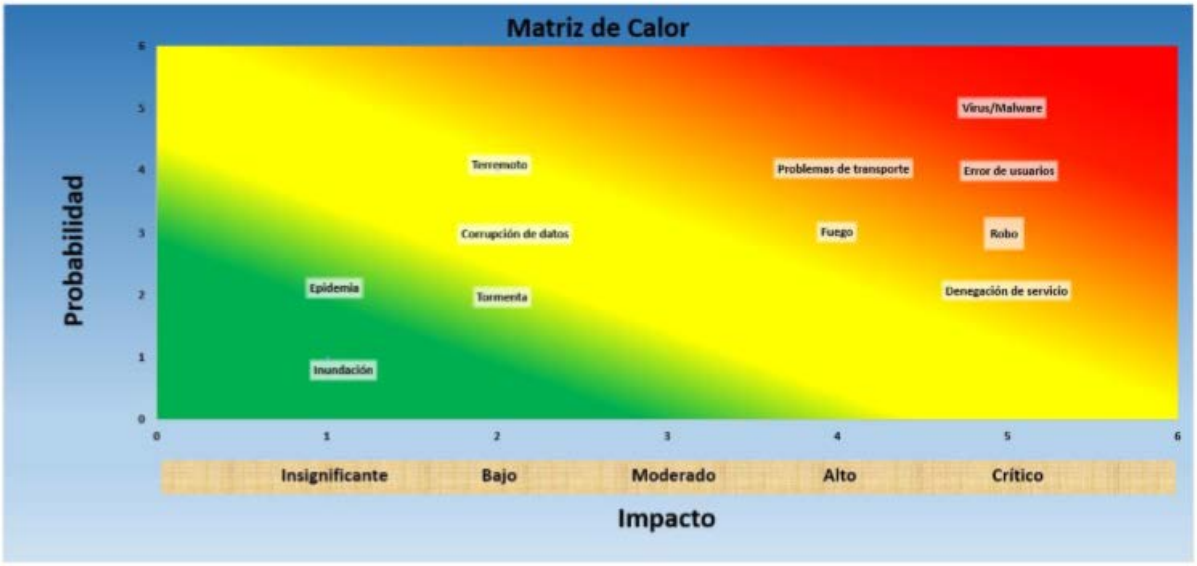
Análisis de Riesgos

Matriz de Riesgos					
Nombre Amenaza	Impacto	Probabilidad	Resultado	Clasificación	Evaluación
Inundación	1	1	1	Insignificante	Asumir
Tornado	1	1	1	Insignificante	Asumir
Difusión de software dañino	1	1	1	Insignificante	Asumir
Huelgas	1	1	1	Insignificante	Asumir
Epidemia	1	2	2	Insignificante	Asumir
Terrorismo	1	2	2	Insignificante	Asumir
Espiación	1	3	3	Bajo	Asumir
Violencia laboral	1	3	3	Bajo	Asumir/Eliminar
Huracán	2	2	4	Bajo	Asumir
Tormenta	2	2	4	Bajo	Asumir
Humedad	2	2	4	Bajo	Asumir
Caída del sistema por sobrecarga	2	2	4	Bajo	Eliminar
Error del administrador	2	2	4	Bajo	Eliminar
Corrupción de datos	2	3	6	Bajo	Transferir
Ataque de intermediario (man in the middle)	3	2	6	Bajo	Mitigar
Degradación de los soportes de almacenamiento de la información	2	3	6	Bajo	Mitigar
Terremoto	2	4	8	Moderado	Transferir
Alteración de datos	3	3	9	Moderado	Mitigar
Robo de Información	3	3	9	Moderado	Mitigar
Interrupción de otros servicios y suministros esenciales	3	3	9	Moderado	Transferir
Abuso de privilegios de acceso	3	3	9	Moderado	Eliminar
Errores de mantenimiento / actualización de programas (software)	3	3	9	Moderado	Transferir
Sabotaje Informático	3	3	9	Moderado	Transferir
Extorsión	3	3	9	Moderado	Asumir
Vandalismo	3	3	9	Moderado	Transferir
Daño en tuberías de agua	5	2	10	Alto	Mitigar
Denegación de servicio	5	2	10	Alto	Mitigar
Fuego	4	3	12	Alto	Transferir
Fuga de datos	4	3	12	Alto	Mitigar
Fallo de servicios de comunicaciones	4	3	12	Alto	Transferir/Mitigar
Pérdida de equipos	3	4	12	Alto	Transferir/Mitigar
Destrucción de información	5	3	15	Alto	Mitigar
Altas temperaturas	5	3	15	Alto	Transferir
Robo	5	3	15	Alto	Transferir/Mitigar
Errores de mantenimiento / actualización de equipos (hardware)	4	4	16	Alto	Transferir/Mitigar
Problemas de transporte	4	4	16	Alto	Asumir
Indisponibilidad del personal	5	4	20	Critico	Asumir
Error de usuarios	5	4	20	Critico	Mitigar
Pérdida de personal clave	5	4	20	Critico	Asumir
Problemas con el suministro eléctrico	5	5	25	Critico	Mitigar
Virus/Malware	5	5	25	Critico	Mitigar
Descuido del personal	5	5	25	Critico	Mitigar

Herramienta

Matriz de Riesgos					
Nombre Amenaza	Impacto	Probabilidad	Resultado	Clasificación	Evaluación Riesgos (Recomendaciones según la calificación del riesgo)
Inundación	1	1	1	Insignificante	1.Asumir / 2. Transferir
Epidemia	1	2	2	Insignificante	1.Asumir / 2. Transferir
Tormenta	2	2	4	Bajo	1.Asumir / 2.Eliminar / 3. Transferir
Corrupción de datos	2	3	6	Bajo	1.Asumir / 2.Eliminar / 3. Transferir
Terremoto	2	4	8	Moderado	1.Transferir / 2. Mitigar / 3.Eliminar
Denegación de servicio	5	2	10	Alto	1.Mitigar / 2. Transferir / 3.Eliminar
Fuego	4	3	12	Alto	1.Mitigar / 2. Transferir / 3.Eliminar
Robo	5	3	15	Alto	1.Mitigar / 2. Transferir / 3.Eliminar
Problemas de transporte	4	4	16	Alto	1.Mitigar / 2. Transferir / 3.Eliminar
Error de usuarios	5	4	20	Crítico	1.Mitigar / 2. Transferir
Virus/Malware	5	5	25	Crítico	1.Mitigar / 2. Transferir

Ejecutar Proceso



Anexo 5: Plantilla de Auditoría.

Auditoria Base de Datos			
Empresa			
Cuestionario de control de Bases de Datos			
Dominio	Base de Datos		
Proceso	Seguridad de la Información		
Objetivo Control	Seguridad de la información de las Bases de Datos		
Cuestionario			
Pregunta		**Si**	**No**	**N/A**
¿Existe archivos logs donde se guarde la información referida a las operaciones que realiza la Base de Datos?			
¿Se realizan Backups (diariamente, semanalmente, mensualmente, trimestralmente, anualmente)?			
¿Existen usuarios que no sean DBA pero que tengan asignado el rol DBA del servidor?			
¿Existen usuarios que no sean DBA pero que tengan asignado el rol DBA del servidor?			
¿Existe un administrador de sistemas en la organización que lleve un control de los usuarios?			
¿Los perfiles de usuarios se gestionan por medio del administrador de la Base de Datos?			
¿Los accesos a las instancias de la Base de Datos son gestionados?			
¿Las instancias que contienen el repositorio, tienen acceso restringido?			
¿Se renuevan las claves de los usuarios de la Base de Datos?			
¿Se obliga el cambio de la contraseña de manera automática?			

¿Se encuentran resguardados todos los intentos de accesos no satisfactorios o denegados a tablas físicas y lógicas del repositorio?			
¿Se manejan estándares para la configuración de la base de datos?			
¿Posee la base de datos un diseño físico y lógico?			
¿Los datos utilizados en el ambiente de desarrollo, son reales?			
¿Las copias de seguridad se efectúan diariamente?			
¿Las copias de seguridad son encriptados?			
¿Se ha probado restaurar alguna vez una copia de seguridad, para probar que las mismas se encuentren bien hechas?			
¿Los dispositivos que tienen las copias de seguridad, son almacenados fuera del edificio de la empresa?			
¿En caso de que el equipo principal sufra una avería, existen equipos en redundancia?			
¿Cuándo se necesita restablecer la base de datos, se le comunica al administrador?			
¿Se lleva a cabo una comprobación, para verificar que los cambios efectuados son los solicitados por el interesado?			
¿Se documentan los cambios efectuados?			
¿Hay algún procedimiento para dar de alta a un usuario?			
¿Hay algún procedimiento para dar de baja a un usuario?			
¿Es eliminada la cuenta del usuario en dicho procedimiento?			

¿Cuáles son las IPs de los servidores?			
¿El motor de Base de Datos soporta herramientas de auditoría?			
¿Existe algún plan de contingencia ante alguna situación no deseada en la Base de Datos?			
¿Existen logs que permitan tener pistas sobre las acciones realizadas en los objetos de las bases de datos?			
Total			

Auditoría Control Ambiental				
Empresa				
Cuestionario de Control Impacto Ambiental				
Dominio	Entrega de Servicios y Soportes			
Proceso	Protección contra Factores Ambientales			
Objetivo Control	Controles Ambientales			
Cuestionario				
Pregunta		**Si**	**No**	**N/A**
¿El Data Center tiene alguna sección con sistema de refrigeración?				
¿Con que frecuencia se valoran y calibran los controles ambientales?				
¿Existe algún contrato de mantenimiento para los equipos que proporcionan el control ambiental?				
¿Existen instalados y se limpian regularmente los filtros de aire?				
¿Con que frecuencia se limpian los filtros de aire?				
¿Se tiene plan de contingencia en caso de que fallen los controles ambientales?				
¿Se cuenta con políticas claras y definidas al finalizar la vida útil de los elementos informáticos que se dan de baja?				
Total				

Auditoria Inventarios				
Empresa				
Cuestionario de Control Inventario				
Dominio	Adquisición e Implementación			
Proceso	Adquirir y Mantener la Arquitectura Tecnológica			
Objetivo Control	Evaluación de Nuevo Hardware			
Cuestionario				
Pregunta		**Si**	**No**	**N/A**
¿Se cuenta con un inventario de todos los equipos que son parte de la organización?				
¿Con que frecuencia se analiza el inventario?				
¿Se poseen bitácoras de fallas encontradas en los equipos?				
¿La bitácora es llenada por personal conocimiento en el tema?				
¿Se incluye la fecha de detección de la falla?				
¿Señala fecha de corrección de la falla y revisión de que el equipo funcione correctamente?				
¿Se poseen registros individuales de los equipos?				
¿La bitácora incluye información, en donde se detalla la falla, las causas que la originaron, así como las herramientas utilizadas?				
¿Se lleva un control de los equipos en garantía, para que a la finalización de ésta, se integren a algún programa de mantenimiento?				
¿Existen servicios de mantenimiento para todos los equipos?				
¿Con que frecuencia se realiza el mantenimiento a los equipos?				
¿Se cuenta con procedimientos definidos a lo interno para la adquisición de nuevos equipos?				
¿Se tiene una estructura de evaluación para determinar el rendimiento de los equipos a adquirir y así poder elegir el mejor?				
Total				

Auditoria Redes				
Empresa				
Cuestionario de Redes				
Dominio	Redes y Comunicaciones			
Proceso	Instalación y Diseño de Redes			
Objetivo Control	Evaluación de la Infraestructura de Redes de Comunicación			
Cuestionario				
Pregunta		**Si**	**No**	**N/A**
¿Todos los hosts se encuentran bajo un mismo estándar de modo que no se reduzca la velocidad de transmisión?				
¿Se ponen a prueba los enlaces de la red frecuentemente?				
¿La longitud de los cables de red no excede los 90 metros sin que exista un repetidor?				
¿El patch panel cumple con los requerimientos básicos del estándar 568-A y 568-B?				
¿El etiquetado implementado en la organización es sencillo de en entender en caso que se necesite rastrear una conexión?				
¿El cable cuenta con los recorridos horizontales correctos para el backbone y sus subsistemas?				
canaletas?				
¿Se cuenta con firewalls y/o IPS para la protección de la red perimetral?				

¿Las direcciones IPs de los equipos de la red son implementadas de manera dinámica?			
¿Se cuentan con Routers, para la expansión de redes locales de la organización?			
¿Existe conexión a tierra para protección de equipos ante posibles descargas eléctricas que puedan afectar los equipos?			
¿Se cuenta con dispositivos para la regulación del voltaje?			
¿Se tiene implementado un sistema de control de acceso a los centros de cableado y dispositivos?			
¿Los equipos se encuentran instalados en áreas con temperaturas adecuadas para su funcionamiento?			
¿Existe implementado un modelo de calidad de servicio en la red?			
¿La red cuenta con los equipos y aplicaciones necesarias para tener un mayor resguardo de personal no autorizado (hackers)?			
¿Existen planes de contingencia y continuidad del negocio que garanticen el buen funcionamiento de la red?			
¿Las terminaciones del cable de red están correctamente configuradas en base al código de colores de los pares trenzados?			
¿La red se encuentra segmentada?			
¿Se cuenta con un análisis de vulnerabilidades en la implementación y configuración de los dispositivos de red?			
¿Los datos que viajan por internet son cifrados?			
Total			

Auditoria Respaldo Eléctrico			
Empresa			
Cuestionario de Control Respaldo Eléctrico			
Dominio	Entrega de Servicios y Soportes		
Proceso	Administración de Instalaciones		
Objetivo Control	Suministro Ininterrumpido de Energía		
Cuestionario			
Pregunta	**Si**	**No**	**N/A**
¿Existe una instalación a tierra física para todos los equipos?			
¿La instalación eléctrica se realizó específicamente para el centro de cómputo?			
¿Existe otra instalación dentro el centro de cómputo diferente de la que alimenta a los equipos de cómputo?			
¿La instalación eléctrica llega a un tablero de distribución?			
¿El tablero de distribución está en la sala, visible y accesible?			
¿El tablero considera espacio para futuras ampliaciones de hasta de un 30 % (Considerando que se dispone de espacio físico para la instalación de más equipos)?			
¿La Instalación eléctrica es independiente para el centro de cómputo?			
¿La misma instalación con tierra física se ocupa en otras partes del edificio?			
¿Los ventiladores y aire acondicionado están conectados en la misma instalación de los equipos a la planta de emergencia?			
¿Los ventiladores y aire acondicionado están conectados en la misma instalación de los equipos a los no-break?			
¿Se cuenta con interruptores generales?			
¿Se cuenta con interruptores de emergencia en serie al interruptor general?			
¿Se cuenta con interruptores por secciones ó aulas?			
¿Se tienen los interruptores rotulados adecuadamente?			
¿Se tienen protecciones contra corto circuito?			
¿Se tiene implementado algún tipo de equipo de energía auxiliar?			
¿Se cuenta con Planta de emergencia?			
¿Se tienen conectadas algunas lámparas del centro de cómputo a la planta de emergencia?			
¿Qué porcentaje de lámparas están conectadas a la planta de emergencia (recomendable el 25%)			
Total			

Auditoria Seguridad de la Información				
Empresa				
Cuestionario de Control de Seguridad Lógica e Informática				
Dominio	Manejo de Información y Elementos			
Proceso	Seguridad de la Información			
Objetivo Control	Seguridad de la Información			
Cuestionario				
Pregunta		**Si**	**No**	**N/A**
¿Se utilizan metodologías para el respaldo de información?				
¿Se realizan respaldos de información diariamente?				
¿Existe un administrador de sistemas que controle las cuentas de los usuarios?				
¿Existe algún estándar interno para la creación de contraseñas?				
¿Las contraseñas se configuran con letras, números y símbolos?				
¿Se obliga, cada 2 meses cambiar la contraseña?				
¿Se tienen software antivirus instalados en los equipos de cómputo?				
¿Cuentan con antivirus actualizado?				
¿Se tienen instalados anti malware en los equipos de cómputo?				
¿Se cuenta con licencias de software?				
¿Existe un proceso para mantener las licencias actualizadas?				
Existen procesos internos para la adquisición de nuevas licencias?				
¿Existen sanciones para el personal que instale software no permitido?				
¿Los usuarios de bajo nivel tienen restringido el acceso a las partes más delicadas de las aplicaciones?				
¿Se realizan mantenimiento preventivo a los equipos de cómputo?				
¿Se realizan mantenimiento correctivo a los equipos de cómputo?				
¿El equipo de cómputo cuenta con suficiente espacio en Disco Duro en función de los servicios que otorga?				
¿El equipo de cómputo cuenta con suficiente memoria RAM en función de los servicios que otorga?				
¿La velocidad del procesador es el adecuado para los programas que son utilizados en los equipos?				
Total				

Auditoria Seguridad Física

Empresa	
Cuestionario de Control y seguridad Instalaciones y Cubículos	
Dominio	Entrega de Servicios y Soportes
Proceso	Administración de Instalaciones
Objetivo Control	Instalaciones y Seguridad

Cuestionario

Pregunta	Si	No	N/A
¿Las instalaciones (cubículos y oficinas) fueron diseñadas o adaptadas específicamente para funcionar como un centro de equipo de cómputo?			
¿Se tiene una distribución del espacio adecuada, de forma tal que facilite el trabajo y no existan distracciones?			
¿Se cuentan con lugares de acceso restringido?			
¿Existen sistemas de seguridad que restrinja el paso?			
¿Existen sistemas de emergencia como detectores de humo, alarmas, u otro tipo de censores?			
¿Se posee una buena señalización de las salidas de emergencia y se tienen establecidas rutas de evacuación?			
¿Se cuenta con medios adecuados para extinción de fuego en el centro de cómputo?			
¿Se cuenta con una iluminación adecuada y con iluminación de emergencia en caso de alguna emergencia?			
¿Se cuenta con sistemas de seguridad para evitar el robo de equipo de las instalaciones?			

¿Existe un lugar asignado para papel y herramientas de trabajo?			
¿Los muebles instalados dentro del centro de cómputo son funcionales? ¿Cintas de respaldo, archiveros, mesas de trabajo, etcetera?			
¿Existen prohibiciones para fumar, consumir alimentos y bebidas en el centro de datos?			
¿Se cuenta con suficientes rótulos en lugares visibles que recuerdan las diversas prohibiciones propuestas por la empresa?			
¿Con cuanta frecuencia se limpian las instalaciones?			
¿Con cuanta frecuencia se limpian los ductos de aire y la cámara de aire que existe debajo del piso falso (si existe)?			
Total			

Anexo 6: Documentos de buenas prácticas.

6.1 Alcance

Instituto Costarricense de Electricidad y Telecomunicaciones

Alcance del SGSI

Código	*## - ICE - Alcance SGSI*
Versión	*<Versión del documento>*
Fecha de Creación	*<Fecha de elaboración de documento>*
Creado por	*<Nombre de persona o personas creadores del documento>*
Aprobado por	*<Nombre de persona que aprueba el documento>*
Nivel de confidencialidad	*<Público, Confidencial, Privado>*

Modificaciones del PCTIC

Fecha	Versión	Modificado por	Descripción
<mm/dd/aa>	*<Número versión documento>*	*<Nombre de persona que modifico el documento>*	*<Descripción de la modificación>*

1. Objetivo del documento

<Definir en esta sección el objetivo de este documento, con el fin de definir los límites del SGSI>

2. Alcance

<Definir en esta sección el alcance de este documento dentro del SGSI>

3. Usuarios

<Definir en esta sección los usuarios miembros del equipo de proyecto que implementa el SGSI y los miembros de la alta dirección patrocinadora del proyecto>

4. Definición del alcance del SGSI

<Definir en esta sección los límites del SGSI para decidir qué información se quiere proteger. Esta protección será independientemente de la forma de gestión: almacenada, procesada o transferida. El alcance debe determinar las partes o procesos del Instituto Costarricense de Electricidad y Telecomunicaciones que van a ser incluidas. Igualmente, el ICE debe determinar cuáles son los procesos críticos para que la Institución decida qué es lo que quiere proteger y por dónde se debe empezar. Dentro del alcance debe quedar definido las actividades de la Institución, ubicaciones físicas que van a ser involucradas, la tecnología de la Institución y las áreas que podría quedar excluidas del SGSI. Es importante que el documento del alcance se defina de acuerdo con los siguientes aspectos: Procesos y servicios, unidades organizativas, ubicaciones, redes infraestructura de TI, exclusiones del alcance >

6.2 Plan de Concienciación

Plan de Concienciación	
Fecha:	*<Fecha de elaboración del documento>*
Versión:	*<Número de versión del documento>*
Encargado:	*<Nombre del funcionario que aprueba el documento>*

Contenido

1. **Propósito** 3
2. **Descripción de talleres de concienciación** 3
3. **Estrategia de implementación** 3
4. **Planeación** 4
5. **Responsables** 5
6. **Actividades** 5
7. **Detalles de los talleres** 7
8. **Encuesta de satisfacción** 7

1. Propósito

<Propósito general del plan de concienciación>

2. Descripción de talleres de concienciación

<Describir lo que se quiere llevar a cabo en cada uno de los talleres >

3. Estrategia de implementación

<Elaborar una estrategia de implementación de la concienciación que involucre actividades en donde el personal participe activamente promoviendo una cultura de gestión de riesgos>

- *Talleres*
- *Comunicación vía correo electrónico*
- *Campaña de publicación de banners en pasillos*
- *Entrega de vouchers*

4. Planeación

<Elaborar una planeación anual sobre las actividades que se estarían realizando y el mes en que se llevarían a cabo>

Actividad	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Setiembre	Octubre	Noviembre	Diciembre
Prueba de continuidad Afectación de Servicio de Internet												
Análisis de nuevos riesgos del negocio												
Revisión de documento de plan de gestión de riesgos												
Impartición de taller # 1												
Impartición de taller # 2												
Entrega de material impreso												
Envió de plan de SGSI vía correo electrónico												

5. Responsables

<Establecer los responsables para cada actividad de concienciación>

Actividad	Nombre Responsable	Correo Electrónico	Teléfono
<Nombre Actividad>	*<Nombre responsable de impartir actividad>*	*<Correo electrónico de responsable>*	*<Número telefónico de responsable>*

6. Actividades

<A continuación un ejemplo de la preparación de 2 distintos talleres>

6.1 Taller # 1 - Visión general y funcionamiento de la gestión de riesgos

6.1.1 Objetivo del taller/actividad

<Objetivos del taller, que se quiere lograr, metas, oportunidades, debilidades>

6.1.2 Temario

- ***Sensibilización:***
  - *¿Qué es un incidente?*
  - *¿Tipos de desastres?*
  - *Causas*
  - *Impactos*
  - *Importancia de contar con un Plan de Gestión de Riesgos*
  - *Procesos/Servicios críticos*
- ***Alcance***
- ***Funciones y Responsabilidades***

        - *Nombre de encargados*
        - *Funciones*
        - *Información de contacto*
    - ***Elementos utilizados en la Gestión de Riesgos***
        - *Nombre de elementos*
        - *Ubicación*
        - *Ejemplos*
    - ***Estrategia de recuperación***
        - *Evaluación*
        - *Prioridades*
        - *Tiempos*
        - *Compromisos*
        - *Pruebas*
    - ***Declaración de desastre***
        - *Comportamiento frente un desastre*
        - *Recolección de información de desastre*
        - *Análisis*
    - ***Comunicación***
        - *Medios utilizados para comunicar un desastre*
        - *Medios utilizados para mantenerse en contacto después de un desastre*
    - ***Activación del Plan***
        - *Encargado de activar el plan*
        - *Reuniones*
        - *Acatamiento de instrucciones*
    - ***Pruebas y mantenimiento del plan***
        - *Tipos de pruebas*
        - *Evaluación de resultados*
        - *Mejoras*
        - *Sugerencias/Preguntas*

6.2 Taller # 2 - Revisión de los procedimientos de recuperación

6.2.1 Objetivo del taller/actividad

<Objetivos del taller, que se quiere lograr, metas, oportunidades, debilidades>

6.2.2 Temario

- ***Concepto de amenaza, vulnerabilidad y riesgo***
- ***Asignación de responsabilidades***
- ***Ejecución de procedimientos para recuperación de servicios críticos***

7. Detalles de los talleres

- **Cantidad de asistentes:**
  - *Nombre:*
  - *Departamento:*
  - *Jefe:*
- **Material informativo:**
  - *Presentación Power Point*
  - *Videos*
  - *Brochures*
- **Duración:**
- **Personal al que va dirigido el taller:**
  - *Personal en general*
  - *Personal de T.I*
- **Fecha:**
- **Hora:**
- **Lugar:**
  - *Nombre de sala de reuniones*

8. Encuesta de satisfacción

<Elaborar una encuesta para obtener retroalimentamentación por parte del personal, esto servirá para mejorar las actividades, obtener resultados y revisar disconformidades>

6.3 Política

Política del SGSI

Versión	*<Versión del documento>*
Fecha	*<Fecha de creación del documento>*
Elaborado por	*<Nombre de la persona encargada de la creación del documento>*
Firma	*<Firma del funcionario>*
Revisado por	*<Nombre de la persona encargada de la revisión del documento>*
Firma	*<Firma del funcionario>*

Modificaciones del SGSI

Fecha	Versión	Modificado por	Objetivos	Descripción
<mm/dd/aa>	*<Número versión documento>*	*<Nombre de persona que modifico el documento>*	*<Objetivos documento>*	*<Descripción de la modificación>*

Tabla Contenido

1. Objetivo 3
2. Marco Jurídico/Normativo 3
3. Alcance 3
4. Gestión de la Política 3
4.1 Objetivos 3
4.2 Requisitos 3
4.3 Procedimientos 3
4.4 Responsables 6
4.5 Comunicación 6
5. Supervisión/Auditoria 7
6. Sanciones 7

1. Objetivo

<Establecer el objetivo del SGSI>

2. Marco Jurídico/Normativo

<Definir el marco legal y normativo relacionado con el SGSI>

3. Alcance

<Definir el alcance de la política>

4. Gestión de la Política

<Definir cómo se va a gestionar la política>

4.1 Objetivos

<Establecer los objetivos que deben ser cumplidos para poder gestionar la política correctamente>

4.2 Requisitos

<Definir los requisitos necesarios para poder gestionar la política>

4.3 Procedimientos

<Definir los procedimientos a seguir para poder ejecutar la política de la manera esperada>

1. *La instalación y desinstalación de hardware es responsabilidad total de departamento de TIC y la necesidad materia prima para dichas actividades serán proveídas por el*

departamento y bajo el presupuesto de infraestructura, bajo la división de infraestructura informática.

2. *En ningún caso el colaborador intentará reparar algún error en el equipo, únicamente informará la posible falla al departamento de TIC. De ser requerido, el equipo se desplazará a la oficina de soporte para su debida revisión.*
3. *Queda totalmente prohibido, excepto a los encargados del departamento de TIC autorizados, manipular los componentes activos de la red tales como switches, routers, artefactos inalámbricos, entre otros.*
4. *No se permitirá la instalación de puntos de acceso de redes inalámbricas con conexión a la red de la empresa sin la debida información y autorización de TIC.*
5. *Ningún usuario está autorizado a utilizar herramientas de rastreo de puertos o que permitan detectar vulnerabilidades. El uso de estas herramientas sólo está permitido a los administradores de la red y bajo situaciones especiales.*
6. *El Departamento de TIC pondrá en funcionamiento herramientas de control que posibiliten detectar, analizar y bloquear accesos no permitidos que pongan en riesgo la seguridad de la información y atenten contra el desempeño.*
7. *El procedimiento de control de cambios debe ser realizados apegados a los controles necesarios para no comprometer la seguridad de los sistemas.*
8. *Se prohíbe crear perfiles o dominios para personas externas a la empresa*
9. *El departamento de TIC debe reportar a la alta dirección cualquier anomalía detectada en la aprobación de creación o modificación de usuarios.*
10. *En caso de que un trabajador se encuentre bajo investigación sobre alguna irregularidad se le suspenderá los permisos de usuario hasta que recursos humanos comunique que estos pueden ser habilitados nuevamente.*
11. *Todas las partes interesadas y terceras partes que manejen información de la empresa, están obligados a salvaguardarla en los sitios dispuestos para tal fin, para garantizar la disponibilidad, confidencialidad y respaldo de la misma.*
12. *Cualquier perdida de información propiedad del cliente, manipulación indebida, traslado, transformación o mala utilización de la misma corresponden a una falta grave por la que esta debe ser comunicada inmediatamente al departamento encargado.*
13. *Se prohíbe totalmente manipular información propiedad del cliente en computadoras externas a la empresa, así sea en teletrabajo o fuera de la oficina.*
14. *En caso de que un trabajador por negligencia o uso indebido ocasione perdida de información propiedad del cliente o atente contra esta deberá asumir las responsabilidades civiles y penales que legalmente esto conlleve.*

4.4 Responsables

<Definir los responsables o encargados de desarrollar la política>

4.5 Comunicación

<Definir cómo le comunicara al personal los procedimientos a seguir según lo establecido en la política>

5. Supervisión/Auditoria

<Definir responsables o encargados de velar que la política se cumpla según lo esperado>

6. Sanciones

<Definir el procedimiento para las sanciones o amonestaciones causado por la violación a la política>