Descripción General de los Lineamientos de Seguridad IoT de la GSMA

Descripción General de los Lineamientos de Seguridad IoT de la GSMA

Versión 2.0

Febrero 2018

Este es un documento de referencia permanente no vinculante

Clasificación de Seguridad: No confidencial

El acceso y distribución de este documento está restringido a las personas permitidas por la clasificación de seguridad. Este documento es confidencial para la Asociación y está sujeto a la protección de derechos de autor. Este documento se utilizará únicamente para los fines para los que ha sido suministrado y la información contenida en él no debe divulgarse ni ponerse a disposición en ninguna otra forma posible, en su totalidad o en parte, a personas distintas a las permitidas bajo la clasificación de seguridad sin la aprobación previa por escrito de la Asociación.

Table of Contents

1 Introducción 4
1.1 Resumen Ejecutivo 4
1.2 Conjunto de Documentos sobre la seguridad en IoT de la GSMA 5
1.2.1 Lista de control de la GSMA para la verificación de la seguridad en IoT 5
1.3 Objetivo del Documento 6
1.4 Audiencia a la que se dirige el documento 6
1.5 Definiciones 7
1.6 Abreviaturas 8
1.7 Referencias 9
2 Los Desafíos Creados por el Internet de las Cosas 10
2.1 El Desafío de la Disponibilidad 11
2.2 El Desafío de la Identidad 11
2.3 El Desafío de la Privacidad 12
2.4 El Desafío de la Seguridad 13
3 La Solución Celular 14
3.1 Abordando el Desafío de la Disponibilidad 14
3.2 Abordando el Desafío de la Identidad 15
3.3 Abordando el Desafío de la Privacidad y Seguridad 15
4 El Modelo de IoT 16
4.1 Ecosistema de Servicios 16
4.2 Ecosistema de Dispositivos Periféricos 17
5 Evaluación de Riesgos 17
5.1 Objetivo 18
5.2 Referencias del Modelo de Riesgo 19
6 Consideraciones de Privacidad 19
7 Como Usar esta Guía de Manera Efectiva 21
7.1 Evaluando el Modelo Técnico 21
7.2 Revisión del Modelo de Seguridad Actual 22
7.3 Revise y Evalúe las Recomendaciones 22
7.4 Implementación y Revisión 23
7.5 Ciclo de Vida Actual 24
8 Ejemplo – Monitor de Frecuencia Cardíaca Portátil 24
8.1 Descripción General del Dispositivo Periférico 24
8.2 Descripción General del Servicio 25
8.3 El Caso de Uso 26
8.4 El Modelo de Seguridad 26
8.5 El Resultado 28
8.6 Resumen 28
9 Ejemplo – Dron Personal 29
9.1 Descripción General del Dispositivo Periférico 29
9.2 Descripción General del Servicio 30

9.3 El Caso de Uso 31
9.4 El Modelo de Seguridad 31
9.5 El Resultado 32
9.6 Resumen 33
10 Ejemplo – Red de Sensores para Vehículos **33**
10.1 Descripción General del Dispositivo Periférico 33
10.2 Descripción General del Servicio 35
10.3 El Caso de Uso 35
10.4 El Modelo de Seguridad 36
10.5 El Resultado 37
10.6 Resumen 37
Anexo A Consideraciones sobre la Privacidad Recomendadas a Proveedores de Servicios IoT **38**
Anexo B Ejemplo Basado en un Sistema de Rastreo de Vehículos **44**
B.1 Evaluación del Modelo Técnico 44
B.2 Revisión del Modelo de Seguridad 44
B.3 Revisión y Asignación de Tareas de Seguridad 45
B.4 Revisión de las Recomendaciones 46
B.5 Revisión de los Riesgos en los Componentes 46
B.6 Implementación y Revisión 47
B.7 El Ciclo de Vida Actual 48
Anexo C Gestión del Documento **48**
C.1 Historial de Edición del Documento 48
C.2 Otra Información 48

1 Introducción

1.1 Resumen Ejecutivo

El auge del Internet de las cosas (IoT, según sus siglas en inglés) está creando nuevos proveedores de servicios que buscan desarrollar productos y servicios nuevos, innovadores y conectados. Los analistas prevén que cientos de miles de nuevos servicios alrededor del IoT, conectarán miles de millones de nuevos dispositivos IoT entre sí en la próxima década. Este rápido crecimiento del Internet de las cosas representa una gran oportunidad para que todos los participantes en este nuevo ecosistema amplíen sus ofertas de servicios y aumenten su base de clientes.

Los analistas han indicado que los problemas de seguridad son una barrera significativa para el despliegue de muchos servicios nuevos de IoT y, al mismo tiempo, la provisión de conectividad en áreas geográficas cada vez más amplias para una variedad cada vez mayor de servicios de IoT, aumentará la exposición de todo el ecosistema al fraude y ataques malintencionados. Cada vez es más evidente que los atacantes (“hackers”) comienzan a mostrar un interés cada vez mayor en esta industria.

A medida que estos nuevos proveedores de servicios desarrollen nuevos e innovadores servicios para segmentos de mercado específicos, es posible que desconozcan las amenazas que pueden asechar a su servicio. En algunos casos, es posible que el proveedor de servicios no haya desarrollado un servicio que se haya conectado a una red de comunicaciones o Internet anteriormente y que no tenga acceso a los conocimientos y experiencia necesaria para reducir los riesgos que plantea la conexión a Internet en sus dispositivos. Por el contrario, los atacantes manejan la tecnología y localizan las debilidades de seguridad rápidamente, aprovechando las vulnerabilidades de estos nuevos dispositivos. Existe una multitud de ataques que han resultado en dispositivos cuya seguridad ha sido comprometida. Estos últimos pueden exponer datos, ser utilizados para atacar otros dispositivos, o causar una disrupción en aquellos servicios relacionados o no directamente con el dispositivo que ha sido “comprometido”.

Si bien muchos proveedores de servicios, como los de la industria automotriz, atención de la salud, electrónica de consumo y servicios públicos (municipales), pueden considerar que sus requerimientos particulares de seguridad son exclusivos de su mercado, generalmente este no es el caso. Casi todos los servicios de IoT se crean utilizando dispositivos periféricos y componentes de la plataforma de servicios que contienen tecnologías similares a muchas otras soluciones de comunicaciones, informática y Tecnologías de la Información (IT). Además de esto, las amenazas a las que se enfrentan estos servicios y las posibles soluciones para contrarrestar estas amenazas suelen parecerse mucho, incluso en el caso de que la motivación del atacante y el impacto de los ataques de seguridad exitosos sean diferentes.

La industria de las telecomunicaciones, representada por la GSMA, tiene una larga historia de proporcionar productos y servicios seguros a sus clientes. La provisión de productos y servicios seguros, es en sí mismo un proceso y un objetivo. Vigilancia, innovación, capacidad de respuesta y mejora continua son necesarias para estar seguros de que las soluciones adoptadas mitigan las amenazas.

Para ayudar a garantizar que los nuevos servicios IoT que lleguen al mercado sean seguros, los operadores de telecomunicaciones junto con sus socios, proveedores de servicios y dispositivos, desearían compartir su experiencia en seguridad con los proveedores de servicios que buscan desarrollar nuevos servicios de IoT.

Por lo tanto, la GSMA ha editado este conjunto de lineamientos de seguridad para el beneficio de estos nuevos proveedores de servicios.

1.2 Conjunto de Documentos sobre la seguridad en IoT de la GSMA

Este documento representa la primera parte del conjunto de documentos de los lineamientos de seguridad de la GSMA que están destinados a ayudar a la naciente industria del "Internet de las cosas" a establecer una base común de principios alrededor de los problemas de seguridad del IoT. Este conjunto de documentos promueve una metodología para desarrollar servicios de IoT seguros que garanticen el uso de las mejores prácticas de seguridad durante todo el ciclo de vida de un servicio. Los documentos proporcionan recomendaciones sobre cómo luchar contra las amenazas y localizar las debilidades o brechas comunes de seguridad dentro de los Servicios de IoT.

La Estructura del conjunto de documentos se muestra a continuación. Se recomienda a los lectores, empezar por este documento (es decir, Descripción General de los Lineamientos de Seguridad IoT de la GSMA) y luego el resto de los documentos que soportan los principios tratados aquí.

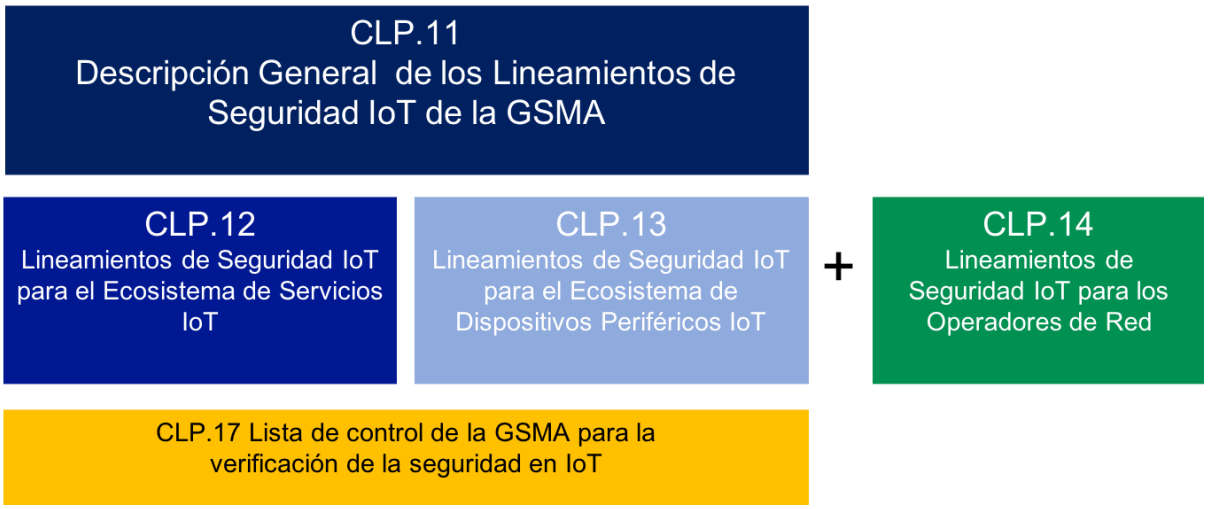

Figura 1 - Estructura del Conjunto de Documentos

Se aconseja a los operadores de red, proveedores de servicios IoT y otros socios en la cadena de provisión, leer el documento GSP CLP.14 "Lineamientos de seguridad del IoT para operadores de red" [13] que proporciona lineamientos de seguridad de alto nivel a operadores de red que pretenden proporcionar servicios a proveedores de servicios IoT, para garantizar la seguridad del sistema y la privacidad de los datos.

1.2.1 Lista de control de la GSMA para la verificación de la seguridad en IoT

Una lista de control y verificación de seguridad IoT se puede encontrar en el documento CLP.17 [16]. Este documento permite a los proveedores de productos, servicios y

componentes de IoT comprobar la conformidad de sus productos con los lineamientos de seguridad IoT de la GSMA.

Al rellenar la lista de verificación arriba mencionada permitirá a cualquier entidad o empresa demostrar las medidas de seguridad que han tomado para proteger sus productos, servicios y componentes de los riesgos de Cyber-seguridad.

Pueden realizarse constancias de verificación enviando a la GSMA una declaración completada con los puntos de la lista. Por favor vea el siguiente link en el portal de la GSMA para más información:

https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/

1.3 Objetivo del Documento

El objetivo de este documento de Descripción General de Lineamientos de Seguridad de Internet de las cosas, es proporcionar al desarrollador de tecnologías o servicios de IoT, un conjunto de lineamientos de diseño para crear un producto seguro. Para lograr esta tarea, este documento servirá como un modelo general para interpretar qué aspectos de una determinada tecnología o servicio son relevantes para su implementación. Una vez que se identifican estos aspectos o componentes, el desarrollador puede evaluar los riesgos asociados a cada componente y determinar cómo tomarlos en cuenta. Cada componente se puede dividir en sub-componentes, donde se describirán los riesgos concretos de una manera pormenorizada. A cada riesgo se le asignará una prioridad para ayudar al implementador a determinar el costo del ataque, así como también el costo de cómo evitarlo y el costo, si corresponde, de no abordar en lo absoluto un riesgo concreto.

La temática que abarca este documento se reduce a las recomendaciones correspondientes al diseño y a la implementación de los servicios de IoT.

Este documento no está concebido para fomentar la creación de nuevas especificaciones o estándares alrededor de IoT, en cambio se harán referencias a las soluciones, estándares y mejores prácticas ya existentes.

Este documento no pretende acelerar la obsolescencia de servicios IoT ya existentes.

Cabe hacer notar que el cumplimiento de las normas a nivel nacional y de las regulaciones en un territorio concreto, son de cumplimiento obligatorio y pueden en cualquier momento anular cualquier pauta que se pueda encontrar en este documento.

1.4 Audiencia a la que se dirige el documento

A quien se dirige este documento:

- Proveedores de servicios de IoT: empresas u organizaciones que buscan desarrollar nuevos e innovadores productos y servicios conectados. Algunos de los muchos campos en los que operan los proveedores de servicios IoT incluyen hogares inteligentes, ciudades inteligentes, industria automotriz, transporte, salud, servicios públicos y productos electrónicos de consumo.
- Fabricantes de dispositivos IoT: desde los desarrolladores de HW IoT a proveedores de servicios IoT para hacer posibles los servicios IoT.

- Desarrolladores de IoT que crean servicios de IoT para los proveedores de servicios de IoT.
- Operadores de red que brindan servicios a proveedores de servicios de IoT o que son a su vez proveedores directos de servicios IoT.

1.5 Definiciones

Término	Descripción
Nombre del punto de acceso	Identificador de un punto de conexión de red al que se conecta un dispositivo periférico. Están asociados a diferentes tipos de servicio, y en muchos casos son configurados por el operador de red.
Atacante o “hacker”	Un pirata informático, un agente inteligente (atacante), un atacante, un estafador u otra amenaza maliciosa para un servicio de IoT. Esta amenaza podría provenir de un solo delincuente, del crimen organizado, por terrorismo, de gobiernos hostiles y sus agencias, por espionaje industrial, de grupos de piratería, de activistas políticos, de hackers 'aficionados', investigadores, así como infracciones de seguridad y privacidad no intencionadas.
La “nube”	Una red de servidores remotos en Internet que aloja, almacena, administra y procesa aplicaciones y sus datos.
Dispositivo Periférico Complejo	Este dispositivo periférico tiene una conexión persistente a un servidor de “back-end” a través de un enlace de comunicaciones, vía la red celular, satelital o una conexión cableada, como Ethernet. Ver CLP.13 [4] para más información.
Componentes	Un componente es un elemento de un objeto digital determinado que, junto con otros componentes, forma un producto o servicio completo. Un componente físico es, por ejemplo, una resistencia, un microcontrolador o una antena. Un componente de un objeto digital, también podría ser una biblioteca de software, un archivo de configuración o un nodo de almacenamiento. Se refiere a los componentes contenidos en los documentos CLP.12 [3] y CLP.13 [4]
SIM embebida	Una SIM que no puede ser eliminada o sustituida físicamente dentro de un dispositivo y permite el cambio seguro de perfiles según la especificación de la GSMA SGP.01 [2].
Dispositivo Periférico IoT	Un dispositivo con capacidad de computo que realiza una función o tarea como parte de un producto conectado o servicio de Internet. Ver sección 3 de CLP.13 [4] para una descripción de las tres clases comunes de dispositivos de IoT y ejemplos de cada clase de dispositivo periférico.
Ecosistema de Dispositivos Periféricos	Cualquier ecosistema de dispositivos sencillos, dispositivos complejos y pasarelas que conectan el mundo físico al mundo digital de formas novedosas. Ver sección 4.2 para más información.
Internet de las cosas	El Internet de las cosas (IoT) describe la coordinación entre múltiples máquinas, dispositivos y aparatos conectados a Internet a través de múltiples redes. Estos dispositivos incluyen objetos cotidianos tales como tabletas y electrónica de consumo y otros dispositivos o máquinas tales como vehículos, monitores y sensores equipados con capacidades de comunicación que les permitan enviar y recibir datos.
Servicio IoT	Cualquier programa de computadora que utiliza datos desde dispositivos de IoT para prestar el servicio.
Proveedor de un Servicio IoT	Las empresas u organizaciones que buscan desarrollar nuevos productos y servicios conectados innovadores.

Término	Descripción
Operador de Red	El operador y propietario de la red de comunicaciones que conecta un dispositivo periférico de IoT a un ecosistema de servicios IoT.
Raíz de Confianza organizacional	Un conjunto de políticas criptográficas y procedimientos que dictan cómo las identidades, las aplicaciones y comunicaciones pueden y deben asegurarse mediante cifrado.
Recomendaciones	Se refiere a las recomendaciones contenidas en los documentos CLP.12 [3] y CLP.13 [4]
Riesgo	Se refiere a los riesgos contenidos en los documentos CLP.12 [3] y CLP.13 [4]
Tareas de Seguridad	Se refiere a las tareas de seguridad contenidas en los documentos CLP.12 [3] y CLP.13 [4]
Punto de Acceso al Servicio	Un punto de entrada en la infraestructura de back-end de un Servicio IoT a través de una red de comunicaciones.
Ecosistema de servicios IoT	El conjunto de servicios, plataformas, protocolos y otras tecnologías necesarias para proporcionar capacidades y recopilar datos de puntos periféricos (servidores) implementados a “pie de campo””. Ver la sección 3.1 para más información.
Módulo de identificación de suscriptor (SIM)	La tarjeta inteligente utilizada por una red móvil para autenticar dispositivos para su conexión a la red móvil y acceso a servicios de red.
UICC	Elemento seguro entendido como plataforma especificada en ETSI TS 102 221 que puede soportar múltiples aplicaciones de autenticación estandarizadas para una red o servicio dentro de distintos dominios de seguridad. Puede ser integrada y encapsulada en varios formatos especificados en ETSI TS 102 671.

1.6 Abreviaturas

Término	Descripción
3GPP	Asociación de proyectos de 3ra generación (“3rd Generation Project Partnership)
API	Interfaz del programa de Aplicación (“Application Program Interface”)
APN	Nombre del punto de Acceso (“Access Point Name”)
CERT	Equipo de Respuesta a Emergencias Informáticas (“Computer Emergency Response Team”)
CLP	Programa de la Vida Conectada (“GSMA’s Connected Living Programme”)
CPU	Unidad de Proceso Central (“Central Processing Unit”)
EAP	Protocolo de Autenticación Extensible (“Extensible Authentication Protocol”)
EEPROM	Memoria de Sólo Lectura Programable con Borrado Eléctrico (“Electrically Erasable Programmable Read-Only Memory”)
GBA	Arquitectura genérica de Bootstrapping (“Generic Bootstrapping Architecture”)
GPS	Sistema de Posicionamiento Global (“Global Positioning System”)
GSMA	Asociación GSM (“GSM Association”)
GUI	Interfaz de Usuario Gráfica (“Graphic User Interface”)
HIPAA	Ley de Transferibilidad y Responsabilidad de los Seguros Médicos (“Health Insurance Portability and Accountability Act”)

Término	Descripción
HRM	Monitor de Frecuencia Cardiaca (“Heart Rate Monitor”)
IoT	Internet de la cosas (“Internet of Things”)
LPWA	Bajo Consumo Area Extendida (“Low Power Wide Area”)
LTE-M	Evolución del Largo Plazo para Máquinas (“Long Term Evolution for Machines”)
NB-IoT	Banda Estrecha-Internet de la Cosas (“Narrowband-Internet of Things”)
NIST	Instituto Nacional de estándares y Tecnología (“National Institute of Standards and Technology”)
OBD	Diagnósticos empotrados (“On Board Diagnostics”)
OCTAVE	Amenaza Crítica Operacional, Activos y Evaluación de la Vulnerabilidad (“Operationally Critical Threat, Asset, and Vulnerability Evaluation”)
OMA	Alianza de moviles abierta (“Open Mobile Alliance”)
PIA	Evaluación del impacto a la Privacidad (“Privacy Impact Assessment”)
PII	Información Personal Identificable (“Personally Identifiable Information”)
RAM	Memoria de Acceso Aleatorio (“Random Access Memory”)
SIM	Módulo de Identificación de Usuario (“Subscriber Identity Module”)

1.7 Referencias

Ref	Número del Documento	Título
[1]	n/a	“The Mobile Economy 2017” http://www.gsmamobileeconomy.com/
[2]	SGP.01	“Embedded SIM Remote Provisioning Architecture” https://www.gsma.com/iot/embedded-sim/
[3]	CLP.12	IoT Security Guidelines for IoT Service Ecosystem https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[4]	CLP.13	IoT Security Guidelines for IoT Endpoint Ecosystem https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[5]	n/a	NIST Risk Management Framework http://csrc.nist.gov/groups/SMA/fisma/framework.html
[6]	CMU/SEI-2007-TR-012	Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process http://www.cert.org/resilience/products-services/octave/
[7]	Not Used	Not Used
[8]	TS 33.220	Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) www.3gpp.org
[9]	RFC 4186	Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM) www.ietf.org
[10]	n/a	Conducting privacy impact assessments code of practice

Ref	Número del Documento	Título
		https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
[11]	n/a	Open Mobile Alliance http://openmobilealliance.org/
[12]	n/a	oneM2M Specifications http://www.onem2m.org/
[13]	CLP.14	IoT Security Guidelines for Network Operators https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
[14]	GE.11-13201	Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue* www.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
[15]	n/a	Right to Internet Access https://en.wikipedia.org/wiki/Right_to_Internet_access
[16]	CLP.17	GSMA IoT Security Assessment Checklist https://www.gsma.com/iot/iot-security-assessment/

2 Los Desafíos Creados por el Internet de las Cosas

Hace varios años un informe especial de las Naciones Unidas recomienda que Internet sea un derecho humano básico y que todas las personas del mundo deberían tener acceso a servicios de banda ancha [14]. Últimamente se están adoptando unas leyes en países como Francia, Grecia, España y otros países [15], para asegurar que el acceso a Internet esté ampliamente garantizado y para evitar que el estado restringa injustificadamente el acceso a un individuo a la información y a Internet.

Estas declaraciones son el resultado de los rápidos cambios sociales y tecnológicos que se derivan del crecimiento de Internet. Esto ha hecho que Internet se convierta en un modo de vida, una de las fuentes primarias a toda clase de información y el método más común para mantener la conectividad entre la gente, amigos y compañeros. Internet no es simplemente una tecnología, se ha convertido en una parte de nosotros.

En consonancia con el creciente deseo de mantenerse conectados, una explosión tecnológica se ha producido en los últimos años. Mientras que los tecnólogos han declarado que "¡El Internet de las cosas está surgiendo!" desde hace más de una década, el interés por acceder a la información desde cualquier sitio y el modelo del costo subyacente no habían logrado combinarse de tal forma que generaran un modelo de negocio práctico hasta hace aproximadamente cinco años. Actualmente, los costos están disminuyendo considerablemente, mientras que el acceso a los servicios inalámbricos y la velocidad de acceso han aumentado dramáticamente. Los protocolos, la duración de la batería e incluso los modelos de negocio han evolucionado para dar cabida a la creciente demanda de información y conectividad.

Esencialmente, lo descrito anteriormente, representa el Internet de las Cosas. No tiene que ver sólo con las “cosas”. Se trata de nosotros. El Internet de nosotros. Las experiencias humanas y digitales ya no conviven codo a codo, están sujetas cada vez más a esta nueva forma de vida.

Y porque la experiencia humana en el mundo físico está ligada cada vez más al mundo digital que nunca, este debe ser protegido, ya que la seguridad digital en estos momentos impacta directamente al mundo físico más que nunca. El Internet de las cosas es una excelente oportunidad para que el mundo avance, para crear bases de datos de conocimientos, de experiencias compartidas cada vez más grandes y que la innovación crezca exponencialmente. Pero para que funcione con eficacia, las tecnologías que impulsan esta conectividad deben ser seguras, para mantener la privacidad, la confianza y la calidad de los servicios necesarios para que esta gran utilidad, esta necesidad básica imprescindible, se mantenga a disposición de todos los que la requieran.

Para que el Internet de las Cosas evolucione con eficacia, debemos resolver los desafíos inherentes a su crecimiento. Estos desafíos son:

- Disponibilidad: Garantizar la conectividad constante entre los extremos (Dispositivos Periféricos) y sus respectivos servicios
- Identidad: Autenticando los Dispositivos Periféricos, los servicios y el cliente o usuario final que opera el dispositivo periférico
- Privacidad: Reducir el daño potencial a los usuarios finales individualmente
- Seguridad: Asegurar que la integridad del sistema puede ser verificada, rastreada y monitorizada

2.1 El Desafío de la Disponibilidad

Para que el internet de las cosas evolucione a su ritmo esperado, los dispositivos periféricos deben poder comunicarse constantemente entre ellos, con los usuarios finales y con los servicios de “back-end”. Para lograr esto, se están implementando nuevas tecnologías como NB-IoT y LTE-M que permiten la conectividad persistente para dispositivos de baja potencia. Esto encaja bien con el desafío del acceso ubicuo a Internet para el mundo moderno. Para que esto tenga éxito, se deben responder varias preguntas:

- ¿Cómo se pueden implementar y operar las redes de baja potencia de área extendida (LPWA) (por ejemplo, NB-IoT y LTE-M) con un nivel de seguridad similar al de los sistemas celulares tradicionales?
- ¿Cómo pueden varios operadores móviles soportar el mismo nivel de seguridad de red cuando los dispositivos periféricos de IoT se estén moviendo de una red a otra?
- ¿Cómo se puede migrar la confianza de red a los puntos periféricos que dependen de pasarelas para comunicarse con los servicios?
- ¿Cómo se pueden abordar las limitaciones de potencia de los dispositivos periféricos “ligeros” (baja capacidad de proceso) en entornos de comunicaciones seguros?

2.2 El Desafío de la Identidad

Para que un dispositivo periférico funcione dentro de un ecosistema de producto o servicio de IoT, debe ser capaz de identificarse de manera segura con sus pares y servicios. Este

aspecto crítico y fundamental de la tecnología de IoT asegura que los servicios y los elementos conectados puedan garantizar a qué, y a quién, se entregan los datos. El acceso a la información y los servicios no es el único problema directamente relacionado con la identidad. También debemos hacer las siguientes preguntas:

- ¿El usuario que opera el dispositivo periférico puede estar fuertemente asociado con la identidad de este dispositivo?
- ¿Cómo pueden los servicios y los elementos empleados en la comunicación verificar la identidad del usuario final al verificar la identidad del dispositivo periférico?
- ¿La tecnología de seguridad de los dispositivos periféricos será capaz de autenticar de forma segura a sus pares en la comunicación y a los servicios?
- ¿Pueden los servicios y pares de comunicación fraudulentos hacerse pasar por los servicios y pares autorizados?
- ¿Cómo se protege la identidad de un dispositivo contra la alteración de los datos o manipulación?
- ¿Cómo pueden los dispositivos periféricos y la red garantizar que un servicio IoT pueda acceder a un dispositivo periférico en concreto?

2.3 El Desafío de la Privacidad

La privacidad ya no se puede ver como un complemento a los productos y servicios existentes. Debido a que el mundo físico se ve directamente afectado por las acciones ejecutadas en el mundo digital, la privacidad debe diseñarse en productos desde el comienzo, para garantizar que cada acción sea autorizada y se verifique cada identidad, garantizando que estas acciones y los metadatos asociados no sean expuesto a elementos no autorizados. Esto solo se puede lograr definiendo una arquitectura adecuada para un producto o servicio, este proceso es excepcionalmente difícil y costoso si se realiza retroactivamente.

Los dispositivos médicos, soluciones para el área automotriz, sistemas de control industrial, domótica, edificios inteligentes y sistemas de seguridad, entre otros, tienen un impacto directo en la vida humana. Es deber de los ingenieros, mantener la seguridad de estos productos y servicios con el más alto nivel de seguridad posible, para reducir la posibilidad de daño físico, así como la exposición de datos privados y personales relevantes.

Por lo tanto, debemos preguntarnos cómo la privacidad afecta no solo al usuario final, sino también a la manera cómo se diseñan las tecnologías de IoT:

- ¿La identidad de un dispositivo periférico está expuesta a usuarios no autorizados?
- ¿Pueden los identificadores exclusivos del servicio y de los dispositivos periféricos IoT permitir que un usuario final o un punto final sean monitorizados o rastreados físicamente?
- ¿Los datos que se transmiten desde un dispositivo periférico o desde un servicio de IoT son indicativos o están directamente asociados con los atributos físicos del usuario final, como la ubicación, los comandos o un estado, como el estar “en reposo” o “activo”?
- ¿Se maneja la confidencialidad y la integridad con la seguridad suficiente como para garantizar que no se observen patrones en el texto de cifrado resultante?
- ¿Cómo el producto o servicio almacena o maneja la información personal del usuario (PII)?

- ¿Puede el usuario final controlar como se almacena o el uso de la PII en el servicio o producto de IoT?
- ¿Se pueden actualizar las claves de seguridad y los algoritmos de seguridad utilizados para proteger los datos?

2.4 El Desafío de la Seguridad

Si bien la seguridad de Internet ha mejorado drásticamente en las últimas décadas, ha habido varias carencias significativas en la tecnología de seguridad empleada en la tecnología moderna. Estas carencias han sido más evidentes en los sistemas embebidos y en los servicios en la nube, los dos componentes principales de la tecnología IoT.

Para que IoT evolucione sin poner en riesgo a grupos masivos de usuarios y de sistemas físicos, las prácticas de seguridad de la información deben aplicarse tanto en dispositivos periféricos como en los servicios de IoT.

- ¿Las mejores prácticas de seguridad se incorporan en el producto o servicio al inicio del proyecto?
- ¿El ciclo de vida de seguridad se incorpora al software o al ciclo de vida de desarrollo del producto?
- ¿La seguridad de la aplicación se aplica tanto a los servicios como a las aplicaciones que se ejecutan en el sistema empotrado?
- ¿Se ha implementado una Base de Computador Confiable (TCB) tanto en el dispositivo periférico como en el Ecosistema de Servicio?
- ¿Cómo hace la TCB para exigir la auto-verificación de las imágenes y servicios de la aplicación?
- ¿Puede el dispositivo periférico o el servicio de IoT detectar si hay una anomalía en su configuración o aplicación?
- ¿Cómo se supervisan los dispositivos periféricos para buscar anomalías que indiquen un comportamiento malicioso?
- ¿Cómo se relacionan la autenticación y la identidad con el proceso de seguridad del producto o servicio?
- ¿Qué plan de respuesta a incidentes se define para detectar anomalías indicativas de un agujero de seguridad?
- ¿Cómo se segmentan los servicios y los recursos para garantizar que se pueda evitar un posible agujero de seguridad de manera rápida y efectiva?
- ¿Cómo se restauran los servicios y los recursos después de la identificación de un agujero de seguridad?
- ¿Se puede detectar un ataque?
- ¿Se puede detectar un componente del sistema que esté comprometido desde el punto de vista de seguridad?
- ¿Cómo pueden los clientes reportar sus inquietudes y dudas sobre la seguridad?
- ¿Se pueden actualizar o reparar los dispositivos periféricos para eliminar vulnerabilidades?

3 La Solución Celular

Si bien ha habido una gran cantidad de tecnologías que ofrecen soluciones de conectividad para IoT, ninguna representa el futuro de la IoT de una manera tan clara como las redes celulares. Las redes celulares ofrecieron los primeros servicios inalámbricos a los consumidores y la industria hace más de veinte años, y desde entonces han estado creando servicios fiables, extensamente disponibles, seguros y rentables. La industria de tecnologías celulares tiene una amplia experiencia en la disponibilidad de red debido a la naturaleza volátil de las redes de radio inalámbricas administradas desde puntos muy lejanos. La identidad de red ha sido un desafío que ha generado numerosos estándares, tecnologías de dispositivos, protocolos y modelos de análisis. La privacidad y la seguridad son preocupaciones constantes de la industria móvil, que han trabajado para disminuir la posibilidad de abusos, robo de identidad y fraude en toda la tecnología celular.

La industria de tecnología celular está ofreciendo tecnologías de redes inalámbricas LPWA (“Low-Power Wire-Area”) con licencia, basadas en estándares, llamadas NB-IoT y LTE-M para cubrir las necesidades de las aplicaciones y servicios de IoT. Estas tecnologías de red LPWA ofrecen la misma (y en muchos casos mayor) conectividad inalámbrica en áreas muy extensas comparadas con las redes celulares tradicionales, utilizando una parte mucho menor de la potencia originalmente requerida para comunicarse efectivamente en este tipo de redes. Muchos operadores de red están implementando servicios LPWA de modo que NB-IoT y LTE-M se convertirán en los estándares de facto para el despliegue de las redes LPWA.

Se puede encontrar más información sobre la implementación de redes NB-IoT y LTE-M en regiones de todo el mundo en el portal de la GSMA: https://www.gsma.com/iot/mobile-iot-initiative/

3.1 Abordando el Desafío de la Disponibilidad

Según el informe de GSMA "The Mobile Economy 2017" [1]:

- A finales del 2016, dos terceras partes de la población mundial tenía una suscripción celular: un total de 4.800 millones de suscriptores únicos. Para el 2020, casi tres cuartas partes de la población mundial, o 5.700 millones de personas, se suscribirán a servicios celulares.
- El cambio a redes de banda ancha móvil y teléfonos inteligentes continúa ganando impulso. Las conexiones de banda ancha móvil (tecnologías 3G y 4G) representaron el 55% de las conexiones totales en el 2016, una cifra que se acercará a las tres cuartas partes de la base de conexiones total para el 2020. Se prevé que la proporción de conexiones 4G solamente se duplique prácticamente del 23% al 41% al final de la década.
- Se prevén 2.300 millones de conexiones adicionales de banda ancha móvil entre 2016 y 2020, y la proporción del total aumentará al 73%. La rápida migración a 4G siguió siendo una característica clave en 2016, con conexiones 4G que aumentaron un 55% durante este año a 1.700 millones. Como resultado, para el 2020, 2G ya no será la tecnología dominante en términos de número conexiones.
- El mercado mundial que pueden abarcar los dispositivos LPWA es grande, con un total de alrededor de 1.400 millones de conexiones en 2020, y algunos observadores de la industria han pronosticado que se llegarán a 5.000 millones en 2022.

3.2 Abordando el Desafío de la Identidad

La gestión de la identidad ha sido un reto desde hace décadas y esto ha fortalecido los estándares de la industria celular y las ofertas de tecnología relacionada de manera significativa. Mientras que la industria de la tecnología celular se asocia típicamente a la tarjeta SIM extraíble, la GSMA ha creado una solución basada en una SIM llamada 'Embedded SIM Remote Provisioning Architecture" [2] (Arquitectura de Provisión Remota de la SIM embebida) que es apropiada para su uso en IoT por permitir una mayor integración a nivel de componente en dispositivos periféricos, reduce los costos de producción y la gestión de conectividad por medio de plataformas "Over The Air" (OTA) para habilitar la conectividad de los dispositivos IoT Periféricos durante toda su vida útil.

Tecnologías de identidad, como la SIM embebida, están diseñadas como anclas de confianza que integran una seguridad por defecto. Se fabrican para resistir a ataques tales como:

- "Glitching"
- Análisis de canal lateral
- Intercepción pasiva de los datos
- Manipulación física
- Robo de identidad

Un avance excelente para esta tecnología ya reforzada por la seguridad es que las nuevas generaciones de estas anclas de confianza y veracidad incorporan una importante mejora en el panorama de IoT. Estas tecnologías serán de doble uso. No se usarán simplemente para verificar la seguridad de la red, sino que también serán capaces de asegurar las comunicaciones de las aplicaciones y la aplicación propiamente dicha, de forma similar a las anclas tradicionales de confianza y veracidad informática.

Esta capacidad de doble uso se verá reforzada por la integración de las especificaciones de seguridad de la industria celular, tales como las provistas por 3GPP GBA [8], OMA [11], oneM2M [12] y otras. Estas tecnologías ayudarán a aprovisionar dispositivos de forma segura en el terreno, a habilitar de forma segura las actualizaciones de firmware inalámbricas y a administrar las capacidades e identidad de los dispositivos.

Estas tecnologías, cuando se utilizan de forma conjunta, facilitan los procesos de ingeniería actualmente muy complejos y se podrán combinar e integrar en un solo componente. En lugar de necesitar ingenieros de aplicaciones desarrollando tecnologías complejas que ellos mismos tienen que administrar, el operador de red, que ya maneja la identidad de red, puede llevar a cabo este proceso en nombre de la aplicación. Esto no sólo reduce la complejidad de la ingeniería, sino también las necesidades diarias de gestión del negocio.

3.3 Abordando el Desafío de la Privacidad y Seguridad

Junto con las capacidades de la tarjeta SIM, la industria móvil ha desarrollado protocolos flexibles, procesos y sistemas de control para activar la seguridad y reducir las posibilidades de fraude y otras actividades maliciosas. Por ejemplo, las tecnologías 3G y 4G utilizan autenticación mutua para verificar la identidad de la red y de los dispositivos periféricos. Este proceso ayuda a asegurar que los atacantes no logren interceptar las comunicaciones.

Además, la tecnología de red se puede asegurar mediante el uso de la SIM y tecnologías como GBA [8] o EAP-SIM [9]. Mediante el uso de estas tecnologías, la SIM se puede aprovisionar con una clave de seguridad de sesión que se puede utilizar en las comunicaciones con los elementos de la red de aplicaciones utilizando protocolos bien conocidos. Este proceso puede disminuir la posibilidad de que los atacantes manipulen el protocolo de la aplicación para poner en peligro los dispositivos o el servicio. Así, es posible asegurar la red y la aplicación conjuntamente con este modelo.

4 El Modelo de IoT

La siguiente figura muestra el modelo de IoT estándar utilizado a lo largo de estos documentos, se representa como una serie de componentes de los Ecosistemas de Servicio y de Dispositivos Periféricos. Cada componente principal está compuesto por sub-componentes, que se detallan en un documento que se centra exclusivamente en el componente principal. Por ejemplo, un componente catalogado como un dispositivo periférico y sus respectivos riesgos, están descritos en el documento de Ecosistema de Dispositivos Periféricos [4] y los componentes de servicio están descritos en el documento del Ecosistema de Servicio [3].

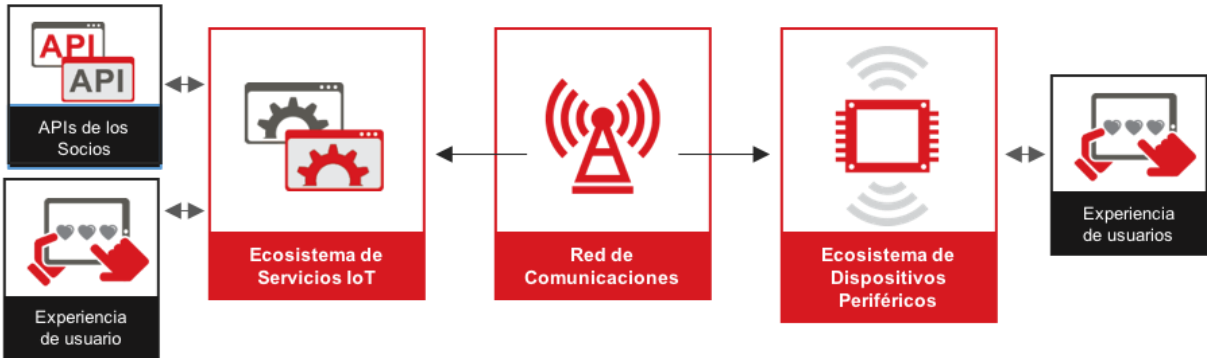

Figura 2 – Ejemplo del Modelo de IoT

En casi todos los modelos de servicios o productos de IoT, este diagrama define los principales componentes que se requieren cuando se despliega una tecnología IoT lista para su implementación o producción.

Los componentes de la red de comunicaciones son inherentes a la IoT y a los efectos de este modelo, proporcionan la conexión entre los dos ecosistemas a través de sus enlaces de comunicación concretos. Estos últimos, están descritos dentro de los documentos del Ecosistema de Dispositivos Periféricos y del Ecosistema de Servicios IoT.

Las Recomendaciones específicas para los lineamientos de seguridad de red para los operadores de red, pueden encontrarse en el documento, "Lineamientos de Seguridad IoT para Operadores de Red de la GSMA" [13].

4.1 Ecosistema de Servicios

El Ecosistema de Servicios representa el conjunto de servicios, plataformas, protocolos y otras tecnologías necesarias para proporcionar capacidades y recopilar datos de dispositivos periféricos desplegados sobre el terreno. Este ecosistema típicamente recoge datos de los Dispositivos Periféricos y los almacena en su entorno de servidor. Estos datos se pueden procesar para el usuario desplegando representaciones visuales elegantes y atractivas de los datos compatibles con varias interfaces de usuario en diferentes terminales. Estos datos, a

menudo en forma de indicadores, parámetros o comandos, también pueden ser entregados a terceras partes autorizadas mediante una API (por ejemplo, oneM2M [12]) originándose en la infraestructura de servicios, que es como los proveedores de servicios de Internet monetizan un servicio comúnmente.

Las directrices de seguridad con respecto al Ecosistema de Servicios utilizado junto al proceso descrito en este documento pueden encontrarse en el documento CLP.12 lineamientos de Seguridad IoT del Ecosistema de Servicio [3]

4.2 Ecosistema de Dispositivos Periféricos

El Ecosistema de los Dispositivos Periféricos [4] puede consistir en dispositivos de baja complejidad, dispositivos complejos y pasarelas que conectan el mundo físico al mundo digital a través de varios tipos de redes cableadas e inalámbricas. Podemos nombrar como ejemplos de Dispositivos Periféricos, sensores de movimiento, cerraduras digitales, sistemas telemáticos automotrices, sistemas de control industrial basado en su sensorización y más. Los Dispositivos Periféricos recogen métricas desde el entorno que les rodea y transmiten los datos en diferentes formatos a través de una red capilar o celular hacia el Ecosistema de servicios, a menudo recibiendo instrucciones o comandos como respuesta. También pueden incluir interfaces de usuario sofisticadas que procesan los datos obtenidos directamente del Dispositivo Periférico, o desde el Ecosistema de Servicios.

Las directrices de seguridad con respecto al Ecosistema de Dispositivos Periféricos para ser utilizadas junto al proceso descrito en este documento, pueden encontrarse en el documento CLP.13 Directrices de Seguridad IoT del Ecosistema de Dispositivos Periféricos [13]

5 Evaluación de Riesgos

Mientras que el concepto de la evaluación de riesgos ha estado presente durante décadas, muchas empresas están más acostumbradas a la reducción de los riesgos para el negocio en general que a tomar en cuenta la seguridad de la información desde un principio. Sin embargo, un proceso de evaluación de riesgos de seguridad sobre la información también es imprescindible para el funcionamiento seguro y mantenimiento en el tiempo de las soluciones tecnológicas que adopta una empresa. Obviamente, en la tecnología del Internet de las cosas, donde el equipo de ingeniería es una parte esencial para el éxito de la empresa, el proceso de evaluación de riesgos debe ser el primer paso que una organización lleve a cabo para la construcción de una práctica de seguridad efectiva.

Mientras que cada organización debe crear una perspectiva pormenorizada del riesgo tecnológico, hay preguntas de alto nivel que se emplean como puntos de partida para el proceso de evaluación de riesgos:

- ¿Qué activos (físicos o digitales) necesitan ser protegidos?
- ¿Qué grupos de personas (tangibles o intangibles) son potencialmente peligrosos?
- ¿Qué es una amenaza para la organización?
- ¿Qué es una vulnerabilidad?
- ¿Cuál sería el resultado si un activo protegido fuera comprometido desde el punto de vista de su seguridad?
- ¿Cuál es la probabilidad de que un activo se vea comprometido?

- ¿Cuál sería el resultado, si se pusiera en un contexto concreto en el cual se dejará expuesto a un conjunto variado de atacantes?
- ¿Cuál es el valor del activo para la organización y sus socios?
- ¿Cuál es el impacto sobre la seguridad del activo que se ve comprometido?
- ¿Qué puede hacerse para remediar o mitigar la posibilidad de encontrar una vulnerabilidad detectada?
- ¿Cómo pueden controlarse nuevas o cambiantes brechas en la seguridad?
- ¿Qué riesgos no se pueden resolver y lo que significan para la organización?
- ¿Qué presupuesto debe dedicarse a la respuesta a incidentes, monitorización y remedio de un riesgo?

Estos puntos de partida ayudarán a los equipos de tecnología de la información (IT) e ingeniería a trabajar más eficazmente dentro de la organización. El objetivo es asegurar que la parte técnica de la empresa esté de acuerdo con los directivos de la empresa (parte ejecutiva) en el tipo de riesgos, valores y planes de reparación. Obligando a los equipos a trabajar juntos se ayudará a crear una perspectiva más realista del riesgo no sólo con respecto el negocio, sino también con respecto al valor de los activos. Esto afectará directamente al presupuesto que debería aplicarse para resolver las brechas que surjan en la seguridad.

Hay algunos riesgos que simplemente no se pueden resolver. Algunos de estos riesgos se mencionan en los lineamientos presentados en este documento. La organización debe evaluar esos riesgos y determinar si son aceptables. Esto proporcionará al negocio un conocimiento realista de sus limitaciones, limitaciones de la tecnología y su capacidad para reaccionar a ciertos tipos de amenazas. No hay nada más costoso que suponer que todas las brechas de seguridad pueden resolverse de una manera rentable.

5.1 Objetivo

El objetivo de una evaluación de riesgos es que la parte técnica de la organización cree (o actualice) un conjunto de políticas, procedimientos y controles que persigan reparar, monitorear y responder a las brechas de seguridad. El resultado de la evaluación de riesgos debe ayudar a la empresa a ajustar no sólo su tecnología, sino la manera en que la tecnología es gestionada, diseñada y desplegada. Una vez que el resultado de la evaluación de riesgos describa mejor el valor de la información y los recursos utilizados por la organización, la empresa en general puede adoptar medidas para mejorar las competencias de su personal, sus procesos y sus políticas.

Recuerde, los beneficios principales de una evaluación de riesgos son:

- Información disponible para el personal de la empresa
- Mejora de los procesos
- Definición de nuevas políticas de seguridad o su actualización
- Implementación de mejoras y remedios
- Monitorización de brechas de seguridad nuevas
- Mejora del producto o servicio

Esto, esencialmente ayuda a la Organización (empresa) a utilizar una plataforma base enfocada a la seguridad que sea accesible al personal y a los procesos de esta. Esta

plataforma entonces debería incluirse en un ciclo que constantemente evalúe y perfeccione las funciones y responsabilidades de toda la organización.

5.2 Referencias del Modelo de Riesgo

En lugar de intentar definir un método nuevo de evaluación de riesgos y un proceso de modelado de las amenazas, por favor, revise las siguientes referencias para un adecuado entendimiento y una presentación general del proceso de evaluación de riesgos:

- Marco de gestión del riesgo del Instituto Nacional de estándares y tecnología (NIST) [5]
- Modelo OCTAVE del “Computer Emergency Response Team (CERT)”[6]

6 Consideraciones de Privacidad

Muchos productos y servicios de IoT se diseñarán para crear, recopilar o compartir datos. Algunos de estos datos no pueden considerarse «datos personales» o afectan la privacidad de los consumidores y, por lo tanto, no estarían sujetos a las leyes de privacidad y protección de datos. Estos datos podrían incluir información sobre el estado físico de las máquinas, datos de diagnóstico internos o métricas sobre el estado de la red.

Sin embargo, muchos servicios de Internet incluyen datos sobre o relacionados con los consumidores y estarán sujetos a las leyes generales de privacidad y protección de datos. No importa donde los operadores móviles ofrezcan servicios de IoT, también estarán sujetos a las reglas de privacidad y seguridad específicas de las redes de telecomunicaciones. Los servicios de IoT enfocados al consumidor implicarán muy probablemente la generación, distribución y uso de datos detallados que puedan afectar la privacidad de un individuo: por ejemplo, al inferir datos acerca de su salud o al desarrollar perfiles basados en sus hábitos de compras y localización. A medida que los servicios de IoT sean más populares, se crearán más datos referentes a los consumidores, que se analizarán en tiempo real y se compartirán entre múltiples “entes” cruzando fronteras.

Cuando los datos se refieran a individuos específicos, este complejo ecosistema 'conectado' suscitará preocupaciones en el consumidor sobre:

- ¿Quién recoge, comparte y utiliza sus datos personales?
- ¿Qué datos concretos se están captando?
- ¿De dónde se obtienen los datos (¿Qué tecnologías o interfaces?)
- ¿Cuándo se recopilan los datos?
- ¿Por qué se recopilan los datos del usuario?
- ¿Cómo se asegura la privacidad (no sólo la seguridad) de la información de las personas?
- ¿Están los individuos controlando cómo se comparten sus datos y cómo las empresas los utilizan?

Todos los proveedores de servicios de IoT que cuentan con los datos de los consumidores - así como los socios que capturen o usen estos datos - tienen la obligación de respetar la privacidad de los individuos y mantener la información personal y aquella que invada su privacidad de manera segura.

Un desafío clave para los proveedores de servicios de Internet es que hay múltiples y a menudo incompatibles, leyes que tratan sobre la privacidad y la protección de datos. Se aplican leyes diferentes en distintos países, dependiendo de los tipos de datos involucrados, así como del sector de la industria y de los servicios que ofrece el proveedor de servicios. Esto tiene implicaciones para un número importante de proveedores de servicios de IoT orientados al consumidor.

Un vehículo conectado, por ejemplo, puede moverse entre países diferentes, lo que significa que la transmisión de datos asociada puede regirse por varias jurisdicciones diferentes. Sensores embebidos que indiquen la ubicación del coche (estática o dinámica) y el rastreo de sus destinos frecuentes podrían utilizarse para inferir una serie de percepciones sobre el estilo de vida del conductor, sus aficiones o religión, que el conductor puede considerar como información privada. Además, el conocimiento acerca de los hábitos de conducción a través de los sensores de diagnóstico del automóvil podría ser compartido con las compañías de seguros que pueden utilizar esos conocimientos para imponer una prima más alta y por lo tanto discriminar al conductor sin su conocimiento.

Los servicios de IoT y sus dispositivos (incluidos coches conectados) también pueden moverse entre diferentes territorios soberanos y por lo tanto diferentes jurisdicciones legales. En muchos casos, los datos personales de un individuo pueden transmitirse o residir dentro de jurisdicciones distintas a la de la persona. Estas son cuestiones importantes que necesitan ser consideradas antes que los servicios IOT se desplieguen de manera multi-nacional.

Otro desafío es que las empresas que recogen datos personales deben, en consonancia con la mayoría de las leyes de protección de datos, requerir el consentimiento de los consumidores en cuestión (también conocido como el «interesado») antes de procesar algunas categorías de esos datos personales – tales como los relacionados con la salud. La mayoría de las leyes define como 'datos personales', cualquier información que se relacione con la vida de una persona concreta 'identificada' o 'identificable'.

Pero a medida que más y más dispositivos se conecten a Internet, más y más datos de individuos serán recogidos y analizados y posiblemente afectarán su privacidad, sin necesariamente ser considerados como datos 'personales' por ley. La combinación de volúmenes de datos masivos, almacenamiento en la nube y análisis predictivo puede proporcionar perfiles detallados de los usuarios. En particular, puede llegar a ser un reto anonimizar la información de manera efectiva ya que los datos personales se pueden deducir a partir de tipos de datos muy variados.

La necesidad de mantener la privacidad de los registros que contengan datos de salud sensibles está bien reconocida, debido al más que posible abuso comercial de dicha información. En el Reino Unido, el “Health Insurance Portability y Accountability Act” de 1996 (HIPAA) incluye requisitos de privacidad y seguridad para mitigar los riesgos de divulgación no autorizada de registros de salud.

HIPAA, como muchas otras regulaciones tales como las de la Unión Europea, sólo se aplica si los datos de salud se pueden ligar a una persona. Los datos almacenados en un dispositivo (que no identifica al usuario) de monitoreo de la sangre no serían cubiertos por estos requisitos, mientras que los mismos datos en una aplicación para “Smartphone” o en un servidor en la nube estarían muy probablemente cubiertos porque se podría vincular a una persona con esa información (en el caso de un Smartphone porque el teléfono casi con toda

seguridad contendrá otros datos que identifiquen al usuario y en un servidor en la nube porque será asociada a una cuenta de usuario identificable). Los legisladores de políticas al respecto en el mundo se están dando cuenta de que la información y conocimientos sobre las personas pueden afectar su privacidad incluso si no se definen como potencialmente 'identificables'. Por lo tanto, están empezando a adoptar enfoques más cercanos al riesgo dentro de los Reglamentos, considerando también las implicaciones más amplias de la privacidad con respecto al uso de datos en lugar de centrarse en las definiciones legales.

Con el fin de generar confianza en el ecosistema de IoT, los gobiernos deberían garantizar que la protección de datos y la legislación de la privacidad sea neutral con respecto a la tecnología empleada y que las reglas se apliquen constantemente a todos los actores en el ecosistema de internet. Además, para que proveedores de servicios de IoT minimicen la necesidad de una intervención regulatoria formal, recomendamos que siga los pasos descritos en el anexo A en las primeras etapas del desarrollo de su producto o servicio de IoT.

7 Como Usar esta Guía de Manera Efectiva

Si bien es mejor implementar la seguridad al inicio de un proyecto de ingeniería, esta guía también puede ayudar a las empresas que ya han diseñado, fabricado e incluso implementado un producto o servicio de IoT. Independientemente de la fase de industrialización en la que se encuentre el producto o servicio del lector, se propone un proceso útil que se debería seguir para obtener el mayor provecho de este conjunto de documentos:

- Evalúe el modelo técnico
- Revise el modelo de seguridad del producto o servicio actual
- Revise y evalúe las recomendaciones
- Implementación y revisión
- El ciclo de vida prosigue

7.1 Evaluando el Modelo Técnico

El primer y más importante paso que debe seguir una organización en el proceso, es comprender muy bien el producto o servicio de IoT. Para realizar una revisión de seguridad y una evaluación de riesgos, el equipo técnico debe estar familiarizado con cada componente utilizado en la solución, cómo interactúan los componentes entre sí y cómo los componentes interactúan con su entorno. Sin una comprensión clara de cómo se construyó (o se construirá) el producto o servicio, la revisión sería incompleta.

Se comienza por hacer un documento que describa cada componente utilizado en el sistema. Identifique cómo se obtiene el componente, cómo se usa, qué nivel de privilegios requiere y cómo se integra en la solución general. Asigne cada componente a las tecnologías descritas en la sección “Modelo” de cada uno de los documentos de lineamientos del Ecosistema de dispositivos periféricos [4] y del Ecosistema de servicio [3]. El documento puede no coincidir exactamente con un componente concreto, pero se debería mapear con una clase general del componente. Simplemente use una de las siguientes clases, por ejemplo, microcontrolador, módulo de comunicaciones o ancla de confianza, esto para encuadrarlo en un contexto general. Considere las siguientes preguntas:

- ¿Qué componentes se usan para construir el producto o servicio?
- ¿Qué entradas y salidas son aplicables al componente en concreto?
- ¿Qué controles de seguridad ya se aplican a estas entradas y salidas?
- ¿Qué nivel de privilegio se aplica al componente?
- ¿Quién en la organización es responsable de implementar el componente?
- ¿Quién en la organización es responsable de monitorear y administrar el componente?
- ¿Qué proceso existe para remediar los riesgos observados en el componente?

Estas preguntas, cuando se responden, proporcionarán una comprensión de cómo los componentes técnicos interactúan entre sí, y cómo el producto o servicio general se ve afectado por cada componente.

Este proceso se corresponde con la primera y la segunda fase del modelo de evaluación de riesgos CERT OCTAVE [6], o del Marco de gestión del riesgo del Instituto Nacional de Estándares y Tecnología NIST [5]. Esto ayuda en el desarrollo de un perfil para cada activo empresarial crítico, en el establecimiento de objetivos de seguridad, y define como la compañía evaluará, supervisará y responderá a los riesgos.

7.2 Revisión del Modelo de Seguridad Actual

A continuación, lea la sección del modelo de seguridad del Dispositivo Periférico o Servicio que se está evaluando. Esta sección ayudará al lector a comprender el modelo que utilizará un atacante para comprometer una tecnología determinada. Este modelo se basa en años de experiencia en la realización de evaluaciones de seguridad, ingeniería inversa y diseño de sistemas integrados.

Una vez que el modelo de seguridad ha sido revisado, el lector debe tener una mejor comprensión de qué tecnologías son más vulnerables, o más deseables para el atacante, en el producto o servicio que se está desarrollando. Esta información debe compartirse con la organización, para garantizar que tanto los ingenieros como los gestores comprendan los riesgos y las amenazas que afectan al modelo actual empleado.

Sin embargo, se debe tener en cuenta que la organización no debe adoptar medidas para modificar su modelo de seguridad en este momento. Es demasiado pronto para hacer cambios concretos en la arquitectura.

Este proceso corresponde de nuevo a la primera y a la segunda fase del modelo CERT OCTAVE [6], o al Marco de gestión del riesgo del Instituto Nacional de Estándares y Tecnología NIST [5]. Revisar el modelo de seguridad ayuda a mejorar el modelo técnico mediante la identificación de brechas potenciales en la seguridad, y a enfocarse hacia los objetivos de seguridad que deberían priorizarse.

7.3 Revise y Evalúe las Recomendaciones

La sección de Recomendaciones debe revisarse en este momento para evaluar cómo se pueden resolver las tareas de seguridad resultantes. Esta sección no solo proporcionará metodologías para la implementación de recomendaciones, sino que también brindará una idea de los desafíos involucrados en la implementación de una recomendación en particular.

Para cada recomendación, se proporciona una sección de Metodología. Esta sección describirá las metodologías que ayudan a remediar o mitigar el riesgo de seguridad correspondiente. Estas metodologías, si bien se presentan desde un alto nivel, delinearán los conceptos que reducen el riesgo desde una perspectiva holística, asegurando que se obtiene una ganancia mayor con una cantidad razonable y práctica de esfuerzo.

Se proporciona una sección de Gastos para analizar, en su caso, los gastos financieros adicionales que la empresa debe tener en cuenta al implementar una recomendación en particular. Si bien la mayoría de los gastos, como el tiempo de ingeniería y las materias primas, son bastante obvios, los gastos menos obvios pueden alterar las finanzas aplicadas a productos y servicios cuyos márgenes de ganancias y límites presupuestarios ya han sido definidos por los gestores empresariales. Si bien no se proporcionan números específicos, se especifican tecnologías y servicios que pueden incurrir en costos adicionales.

También se proporciona una sección de Riesgos para que el lector entienda las lagunas de seguridad que probablemente resulten de no implementar una recomendación en particular. Si bien la empresa puede aceptar que algunos riesgos estén dentro de las pautas operativas de la empresa, el lector debe revisar cada sección dentro de los riesgos, para asegurarse de que la empresa comprende perfectamente los “daños colaterales” de no implementar (o no implementar correctamente) una recomendación concreta. Esto puede parecer sencillo para recomendaciones tales como la de "Encriptar los datos", pero la sutileza de algunas amenazas, como la “reproducción de ataques” contra mensajes que no son criptográficamente únicos, puede ser una sorpresa para el lector en una fecha posterior.

En algunos casos, se proporcionan referencias para una revisión posterior. Si bien este documento no proporciona información detallada sobre cada tecnología, cada riesgo o cada plan de corrección, sí lo hacen otros estándares y estrategias ya comprobadas anteriormente y utilizadas en la industria. Este conjunto de documentos proporcionará referencias a estas fuentes citadas anteriormente, cuando corresponda, dentro de cada recomendación.

El resultado de revisar la sección de Recomendaciones debe vincularse directamente con la sección de Tareas de seguridad. Las Tareas de seguridad ahora deben completarse con Recomendaciones apropiadas para implementar las Tareas de seguridad correctamente. Estas tareas de seguridad se vincularán a componentes específicos asignados a los miembros de la empresa u organización.

La evaluación de las recomendaciones corresponde al paso de Evaluación del Marco de gestión de riesgos del NIST [5] y a los pasos seis, siete y ocho de la metodología CERT OCTAVE [6].

7.4 Implementación y Revisión

En esta etapa, se han definido claramente las Tareas de Seguridad y la empresa comprenderá mejor sus vulnerabilidades de seguridad, su costo y su riesgo. La empresa ahora creará un modelo de arquitectura claro para cada Componente que se esté ajustando y utilizará el proceso de Evaluación de Riesgos elegido por la organización para desarrollar un modelo de amenazas para cada Componente, incorporando las Recomendaciones y Riesgos que son apropiados para cada Componente y Tarea de Seguridad. Cuando se complete el modelo arquitectónico, la organización puede comenzar a implementar cada Recomendación para cumplir con las Tareas de seguridad.

Cuando se termine la implementación, la organización debe revisar los riesgos en la subsección de Recomendaciones y en las secciones de Componentes. La organización debe asegurarse de que la implementación cumpla con los requisitos establecidos por estas secciones. También debe entonces asegurarse de que la implementación resuelve los problemas de seguridad con respecto al contexto en el cual el Componente está diseñado en el producto o servicio de la organización, ya que estos documentos no pueden abordar en su totalidad cada producto o cada servicio diseñado en el mundo real. Si es posible, solicite a una empresa consultora externa que evalúe la implementación para asegurarse de que cumple con las mejores prácticas de seguridad.

La implementación y la revisión se corresponden con el componente “Respond” del Marco de gestión de riesgos del NIST [5] y el paso ocho del modelo CERT OCTAVE [6].

7.5 Ciclo de Vida Actual

El ciclo de vida de seguridad no se detiene en este punto. Por el contrario, la seguridad es una parte inherente de la ingeniería general de un proceso. Los Dispositivos Periféricos y los Servicios de IoT tienen una vida útil y deben ser mantenidos continuamente durante todo ese tiempo, al igual que un ser vivo.

Los requisitos cambian con el tiempo. Los algoritmos criptográficos se vuelven obsoletos o se desactualizan. Los nuevos protocolos y tecnologías de radio deben interactuar con el producto o servicio. Este ecosistema siempre cambiante en el que se implementan nuestros productos embebidos, debe revisarse constantemente para garantizar que se mantenga la confidencialidad, la integridad, la disponibilidad y la autenticidad.

La gestión del ciclo de vida actual de seguridad corresponde con los componentes “Monitor y Frame” del Marco de gestión de riesgos NIST [5], y los pasos uno, cuatro y cinco del modelo CERT OCTAVE [6].

8 Ejemplo – Monitor de Frecuencia Cardíaca Portátil

En este ejemplo, se evaluará un diseño simple de un monitor de frecuencia cardíaca (“HRM”) usando este conjunto de lineamientos. El dispositivo periférico se evaluará utilizando el documento Ecosistema de Dispositivos Periféricos, mientras que la parte concerniente al servicio del diseño se evaluará utilizando el documento Ecosistema de servicio.

8.1 Descripción General del Dispositivo Periférico

Primero, comencemos por evaluar el diseño del hardware del Dispositivo Periférico.

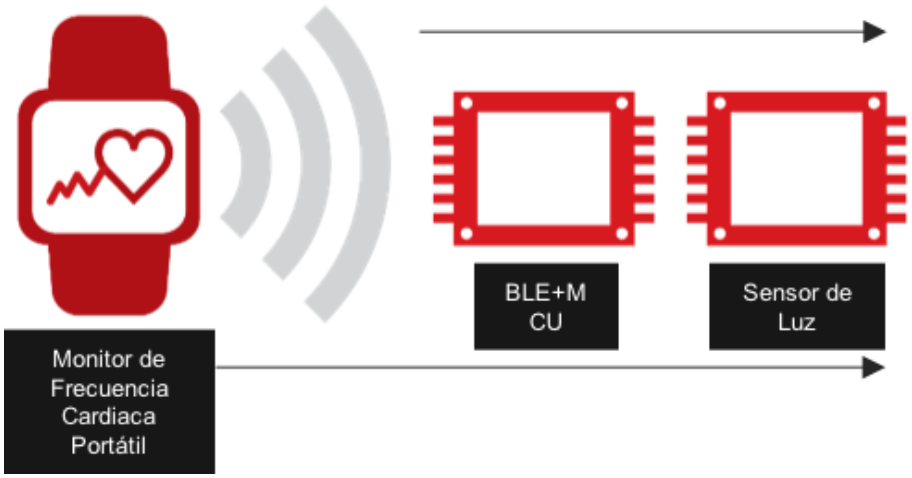

Figura 3– Monitor de Frecuencia Cardiaca y sus Componentes Principales

El HRM consta de componentes estándar para un dispositivo portátil inalámbrico simple: un sensor de luz ambiental y un microcontrolador utilizado con un transceptor Bluetooth de bajo Consumo ("BLE"). El sensor se utiliza para capturar los datos de frecuencia del pulso, mientras que el microcontrolador analiza los datos que se emiten desde el sensor y elige qué datos enviar a través del transceptor BLE incorporado. En este ejemplo, la pila de protocolos BLE utilizada es la versión 4.2.

En este ejemplo, se utiliza una pila tipo botón para alimentar al dispositivo y transmitir datos desde el HRM a otro dispositivo, como en un teléfono inteligente o en una tableta. No se requieren otros componentes para que este dispositivo funcione.

De acuerdo con el documento del Ecosistema de Dispositivos Periféricos, este dispositivo encajaría en la clase de Dispositivos Periféricos Ligeros.

8.2 Descripción General del Servicio

Desde la perspectiva del servicio, la aplicación en el teléfono inteligente o tableta envía las métricas desde el Dispositivo Periférico hasta un servicio de back-end sobre cualquier conexión de red disponible. El servicio de fondo para la aplicación simplemente asocia al propietario del dispositivo con las métricas que se están capturando y las almacena en una base de datos local en el servidor de aplicaciones.

La visualización de los datos se puede obtener utilizando la aplicación móvil o a través del portal del servicio. Los usuarios del HRM pueden iniciar una sesión en el portal del proveedor de servicios para ejecutar procesos sobre las métricas capturadas por el dispositivo periférico.

Este es un modelo de servicio muy simple y común sin complejidades específicas o innecesarias.

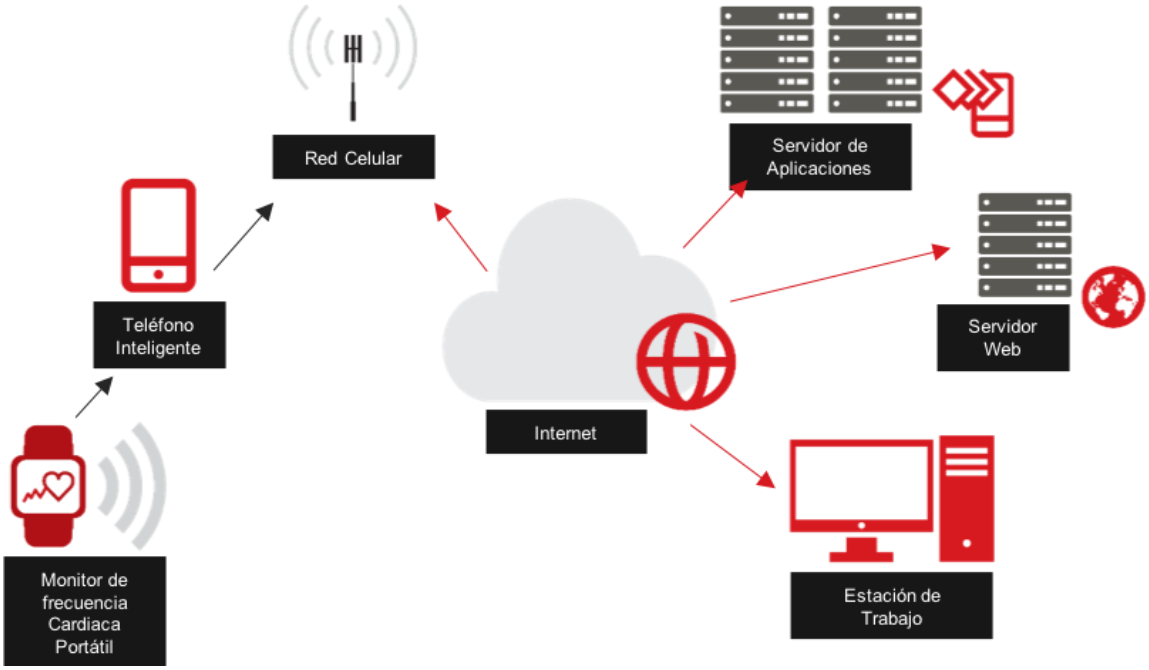

Figura 4– Flujo de Datos hacia un Servicio de Back-end Sencillo

8.3 El Caso de Uso

La empresa que desarrolla esta tecnología tiene la intención de que el usuario final pueda observar los datos relacionados con las medidas de la frecuencia cardiaca a lo largo del día, almacenándolos tanto en la aplicación como en la base de datos del back-end. La intención es permitir a los usuarios revisar su frecuencia cardíaca a lo largo del tiempo para supervisar su salud cardiaca. Los usuarios pueden ver cómo su salud mejora o empeora con el tiempo, dependiendo de si mantienen un estilo de vida saludable o no. Esto permite que los usuarios se motiven mediante la evaluación de las tendencias positivas y negativas en sus datos de monitorización cardiaca.

La empresa tiene la intención de utilizar estos datos para asociarse con fabricantes de dispositivos médicos, proveedores de atención médica y otras organizaciones que pueden usar estas medidas para identificar si un consumidor tiene más o menos probabilidades de incurrir en un “accidente” relacionado con la salud, como un infarto o un derrame.

8.4 El Modelo de Seguridad

El equipo de ingeniería de la empresa comercializadora de esta solución, aprovechó las secciones de “Preguntas Frecuentes” de seguridad en los documentos de Dispositivos Periféricos y de Servicios para determinar qué problemas son más relevantes para su producto y servicio.

Desde una perspectiva de Dispositivo Periférico, el equipo aprendió que las siguientes cuestiones clave son motivo de preocupación:

- Clonación

- Suplantación de Dispositivo Periférico
- Suplantación de servicio
- Garantizar la privacidad

Desde la perspectiva del servicio, el equipo decidió que las siguientes cuestiones clave son motivo de preocupación:

- Clonación
- Servicios pirateados
- Identificación del comportamiento anómalo del Dispositivo Periférico
- Limitación del riesgo de exposición a ataques
- Reducción de la pérdida de datos
- Reducción de la explotación
- Gestión de la privacidad del usuario
- Mejora de la disponibilidad

El equipo revisó las recomendaciones para cada uno de los temas anteriores, según lo sugerido por cada sección de Preguntas Frecuentes de Seguridad. Luego, el equipo optó por implementar las recomendaciones que fueran más rentables y que garantizaran la mayor seguridad.

En este modelo de ejemplo, el Dispositivo Periférico no requeriría un cambio sustancial. Como el Dispositivo Periférico es funcionalmente sencillo, se puede aplicar una seguridad mínima en el Dispositivo Periférico tanto para la aplicación como para la comunicación. Dado que los datos de la aplicación del Dispositivo Periférico se muestran en un solo dispositivo, siempre que el firmware del dispositivo esté bloqueado, no existe una amenaza real de ataque contra el Dispositivo Periférico en un caso de uso determinado.

Sin embargo, dado que la privacidad es un problema, la empresa fabricante debe emplear al menos una versión de PSK personalizada de una base de computación confiable (TCB). Esto garantizaría que los tokens de cifrado fueran únicos para cada Dispositivo Periférico, de modo que un Dispositivo Periférico comprometido no pueda comprometer todo el conjunto de Dispositivos Periféricos. Si las claves personalizadas (únicas) se codificaran en el microcontrolador bloqueado, sería razonable creer que este caso de uso se protegió adecuadamente de la amenaza de clonación, suplantación y problemas de privacidad. Revise los documentos de Servicio de IoT [3] y Dispositivos Periféricos [4] para una explicación más completa sobre qué es una base de computación confiable (TCB) dentro del contexto de cada ecosistema.

La infraestructura del servidor, sin embargo, requiere una cantidad significativa de cambios. Los ingenieros se han dado cuenta de que, de acuerdo con las recomendaciones, corren un serio riesgo de sufrir abusos. Los siguientes problemas se han identificado:

- No hay una solución de seguridad específica en el front-end que disminuya los efectos de un ataque de denegación de servicio
- No hay controles de entrada o salida que limiten el flujo de datos hacia o desde los servicios
- No hay separación de funciones entre niveles de servicio

- No hay una base de datos segura separada que contenga tokens PSK personalizados
- No se implementan medidas de seguridad adecuadas en el sistema operativo del servicio
- No se toman medidas para evaluar el comportamiento anómalo de los puntos finales

8.5 El Resultado

Después de la implementación de las recomendaciones, la empresa tiene un mejor servicio de back-end optimizado y una arquitectura bien definida que aborda adecuadamente los riesgos identificados a través de los lineamientos.

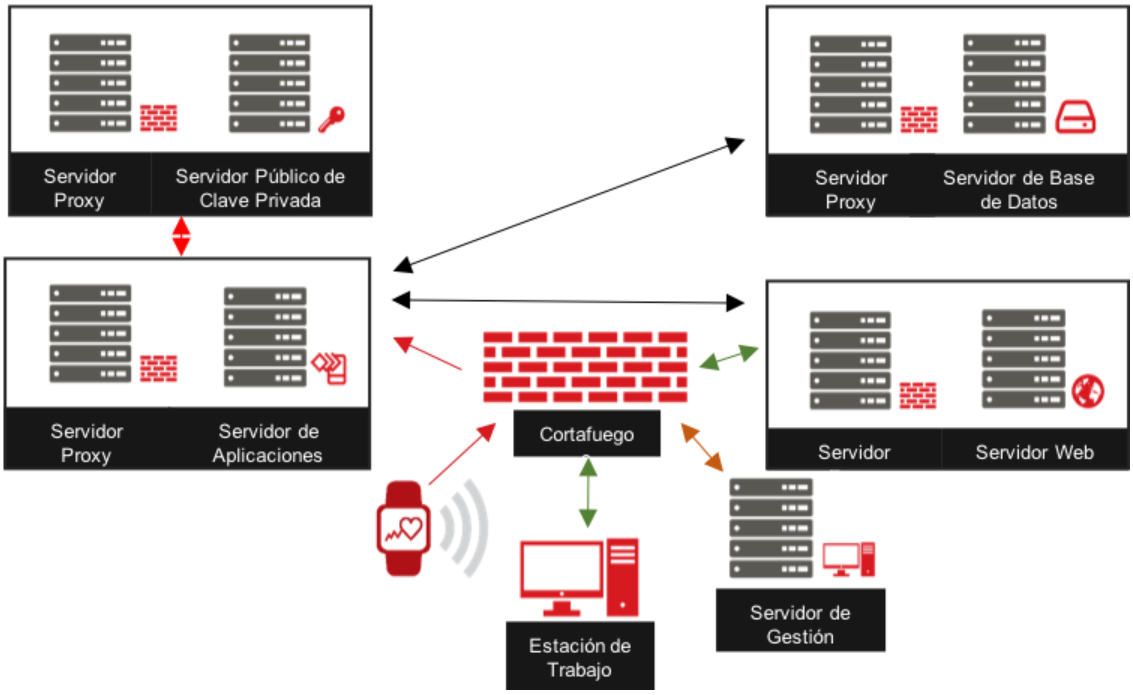

Figura 5– Ecosistema de Servicio Resultante

En la figura anterior, los cambios en el ecosistema de servicio son fácilmente reconocibles. Cada clase de servicio se ha dividido en niveles separados para mejorar la seguridad y la escalabilidad de la tecnología fácilmente en caso de que la demanda se incremente sustancialmente. Dos capas adicionales de servicio en la arquitectura fueron agregadas, una capa de base de datos y otra de autenticación, para separar los sistemas o componentes críticos de los servicios que directamente interactúan con el mundo exterior. Finalmente, se definió un modelo administrativo para permitir el acceso seguro de gestión al entorno de producción. Un componente no está representado en el diagrama, es el que ejecuta un modelo de análisis que observa cuando el comportamiento de un Dispositivo Periférico puede ser indicativo de un ataque en el que se ha comprometido su seguridad o que existe un error en el diseño del hardware o firmware.

8.6 Resumen

En general, esta tecnología que puede ser considerada como sencilla, podría haber sido fácilmente comprometida si la hubieran desplegado "tal cual". Sin embargo, con unos pocos cambios rápidos, sencillos y rentables en el Dispositivo Periférico, se asegura que la solución tecnológica perdure un tiempo mucho mayor en campo sin cambios en la arquitectura.

Con el Ecosistema de Servicio mejorado, hay mucho menos probabilidades de una amenaza de seguridad para los usuarios y para el negocio. La clonación y la suplantación ya no representan una amenaza. La Privacidad está garantizada mediante la asignación a cada Dispositivo Periférico de unos tokens criptográficos únicos. Los componentes del sistema que contienen información crítica se han separado y asegurado con respecto a los componentes que funcionan como interfaz hacia los usuarios que suelen ser atacados. Este modelo, aunque es un poco más complejo, reduce el riesgo global del entorno de producción.

9 Ejemplo – Dron Personal

En este ejemplo, un dron personal de pequeñas dimensiones será evaluado mediante este conjunto de directrices. El Dispositivo Periférico (el dron) se evaluará mediante el documento del Ecosistema de Dispositivos Periféricos, y por parte del servicio, el diseño se evaluará mediante el documento del Ecosistema de Servicio.

9.1 Descripción General del Dispositivo Periférico

Primero, comencemos por evaluar el diseño hardware del Dispositivo Periférico.

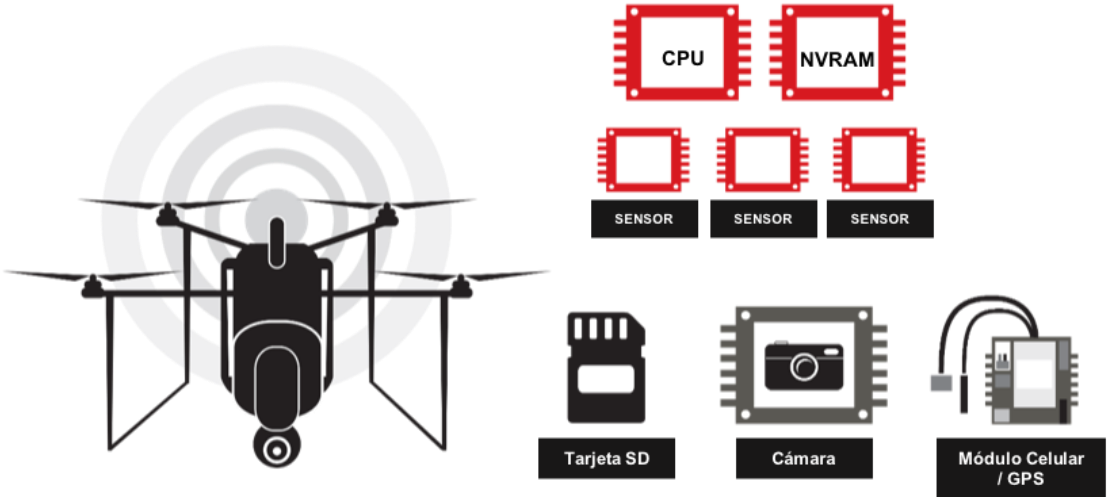

Figura 6– Un Dron y sus Componentes Principales

Este dron personal está compuesto por un conjunto de componentes muy robusto. La capacidad de proceso de los drones no tripulados tiene que ser muy alta debido a la necesidad de controlar varios motores, sensores y otros componentes que deben todos funcionar en perfecta armonía simultáneamente. Este modelo utiliza un procesador ARM Cortex-A8 con un sistema operativo principal (Linux) almacenado en una NVRAM integrada en un chip separado. Una serie de diferentes sensores son necesarios para la detección de movimiento, luz, velocidad y demás variables. Se utiliza una tarjeta SD/MMC para almacenar vídeo, las mediciones de los sensores y metadatos. Se utiliza una cámara para permitir al usuario ver el entorno desde la perspectiva del dron. Un módulo que combina las tecnologías celular y GPS se utiliza para que el dron mantenga la conectividad con su operador incluso cuando está fuera del alcance del protocolo propietario normalmente empleado de comunicaciones. La tecnología GPS también se utiliza para el direccionamiento y para una automatización mínima.

Una batería de polímero de litio (LiPo) se utiliza para alimentar al dron. Su tiempo de autonomía es aproximadamente de dos horas antes de que una nueva carga se requiera para que todas las funciones sigan activas a la vez.

Según el documento del Ecosistema de Dispositivos Periféricos, este dispositivo encajaría en la clase de dispositivos periféricos complejos. A pesar de que contiene un módulo que implementa las comunicaciones celulares, no se considera una puerta de entrada para un ataque ya que no se enrutan mensajes, a, o desde otros dispositivos periféricos.

9.2 Descripción General del Servicio

Desde la perspectiva del servicio, el back-end solo se utiliza para conectar al operador con el dron cuando se detecta una pérdida de conectividad con la interfaz radio propietaria durante el vuelo. Si el dron está en vuelo y la conexión celular se puede habilitar, intentará esperar a que su operador se conecte a través de la red LTE. Sin embargo, si no puede ser controlado por LTE, intentará un aterrizaje automático en el lugar donde despegó por última vez.

Sin embargo, como el dron tiene algunas funciones simples de automatización, se le pueden programar coordenadas y un camino a seguir mientras toma fotos o videos cortos. Estos archivos multimedia se pueden cargar en tiempo real a través de LTE al servicio de back-end para mostrar al operador su itinerario y punto de vista durante la ejecución automatizada.

Por lo tanto, se requiere un servicio de back-end robusto para garantizar un alto grado de disponibilidad del servicio para cada dron que pueda conectarse al sistema. La disponibilidad también es necesaria para poder transmitir ráfagas de muchos datos requeridas para transmitir videos e imágenes de alta resolución a través de un enlace celular. También debe haber una interfaz web que permita al operador ver los ficheros multimedia que se han subido desde un navegador web.

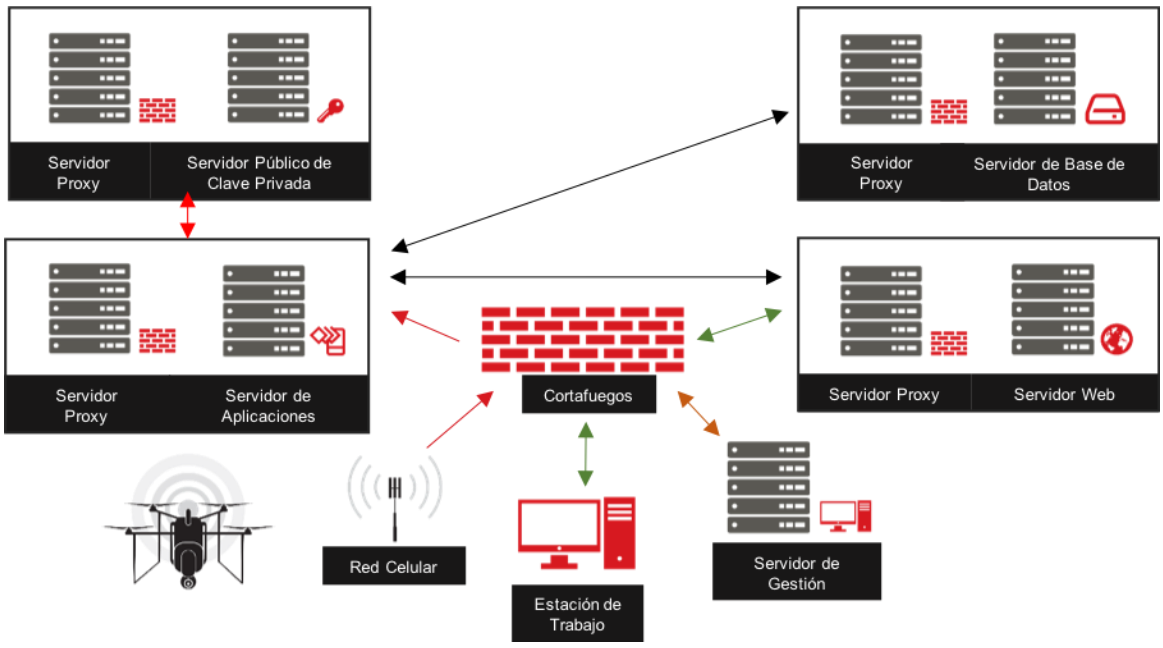

Figura 7– Flujo de Datos hacia los Servicios de Back-end

9.3 El Caso de Uso

La empresa que desarrolla este tipo de tecnología pretende que el usuario final use el dron para filmar imágenes en la naturaleza. Sin embargo, algunos de sus clientes han usado el dron para filmar también escenas en una película por ejemplo, ya que la cámara y las capacidades de estabilización del dron son excepcionales visto el precio que se tiene que pagar por el dron en cuestión. Como resultado, el dron se utilizará en proyectos de filmación costosos donde la propiedad intelectual y la privacidad son las principales preocupaciones.

9.4 El Modelo de Seguridad

El equipo de ingeniería de esta empresa aprovechó las secciones de Preguntas Frecuentes de seguridad en los documentos de Dispositivos Periféricos y de Servicio para determinar qué problemas son los más relevantes para su producto y servicio.

Desde una perspectiva de Dispositivo Periférico, el equipo se dio cuenta de que las siguientes cuestiones clave son motivo de preocupación:

- La Identidad del Dispositivo Periférico
- La Suplantación del Dispositivo Periférico
- Ataques al ancla de confianza
- Modificación del software o firmware
- Administración remota segura
- Detección de Dispositivos Periféricos comprometidos
- Suplantación del servicio
- Garantizar la privacidad

Desde la perspectiva del servicio, el equipo decidió que los siguientes temas son motivo de preocupación:

- Gestionar la privacidad del usuario
- Mejorar la disponibilidad

El equipo revisó las recomendaciones para cada uno de los temas anteriores, según lo sugerido por cada sección de Preguntas Frecuentes de Seguridad. Luego, el equipo optó por implementar recomendaciones que fueran mejoras rentables que garantizaran una mayor seguridad.

En este ejemplo, la infraestructura del servicio no requiere un cambio sustancial. Esto se debe a que la infraestructura del servicio se tuvo que construir desde un inicio de una manera óptima para adaptarse a las ráfagas de tráfico requeridas en el servicio del producto final. La arquitectura ya exigía una arquitectura segura y bien diseñada simplemente para poder escalar de forma efectiva la cantidad de datos transmitida y mantener la disponibilidad de recursos incluso cuando algunos servicios presenten fallos temporales. Sin embargo, la empresa optó por investigar también la cuestión de la privacidad del usuario de manera más profunda, ya que se ha convertido en el principal motivo de controversia dentro del nicho inesperado de negocio de la empresa (filmación).

La infraestructura del Dispositivo Periférico, sin embargo, requiere una cantidad significativa de cambios. Los ingenieros se dan cuenta de que, de acuerdo con las recomendaciones, corren un serio riesgo de sufrir ataques. Los siguientes problemas son identificados:

- El gestor de arranque no valida correctamente la aplicación antes de ejecutar el kernel del sistema operativo, lo que conlleva un riesgo de alteración del SW
- No se utiliza un TCB para administrar la seguridad de la aplicación o de las comunicaciones
- Debido a que no existe un TCB o un ancla de confianza debidamente implementados, la suplantación del Dispositivo Periférico es un problema, que puede conducir a la pérdida de datos
- Sin un TCB bien implementado, el Dispositivo Periférico no puede autenticar correctamente los servicios
- Sin un TCB bien implementado, el punto final no puede autenticar correctamente al operador sobre la interfaz de radio propietaria
- Los ingenieros han confiado en la seguridad de LTE para garantizar que el canal de comunicaciones no se vea comprometido, pero no ha considerado la posibilidad de que se pueda suplantar al Dispositivo Periférico o que se reconfigure fraudulentamente una Femtocell, esto pasaría por alto la seguridad de LTE para poder comprometer esa debilidad de la seguridad del servicio

9.5 El Resultado

Después de implementar las recomendaciones con respecto a los problemas mencionados anteriormente, la empresa ha conseguido una definición mejor de arquitectura del Dispositivo Periférico que aborda adecuadamente los riesgos identificados a través de los documentos de lineamientos.

Para el sistema de drones existente que ya se encuentra en producción, el equipo de ingeniería emite una actualización de firmware que implementa un modelo de seguridad de Pubkey personalizado. La actualización del firmware también mejora el gestor de arranque y brinda seguridad en la arquitectura del núcleo. Dado que se utilizó un modelo de Pubkey personalizado, cualquiera que intente abusar de la falta de seguridad inicial en el Dispositivo Periférico para intentar hacerse pasar por el Dispositivo Periférico de otro usuario fracasará, ya que los ingenieros aprovecharon su base de datos existente de mapeo de usuario a Dispositivo Periférico para crear claves personalizadas para cada usuario. De esta forma, ningún usuario sin las credenciales web adecuadas puede descargar e instalar la actualización del Pubkey personalizada de otro usuario. Si bien este proceso fue complejo y llevó mucho tiempo implementarlo, dará sus frutos.

Las versiones futuras de la tecnología de drones implementarán un ancla de confianza interna en la CPU. Esta ancla de confianza se vinculará a una TCB personalizada de Pubkey, para garantizar que cada punto final cuente con una seguridad excepcional desde el principio.

La implementación de una tecnología criptográfica sólida como la que se propone es imprescindible, ya que también anula el potencial para las otras clases de ataques que la empresa identificó como posibles amenazas. Aprovechando el beneficio de una criptografía sólida y un TCB para la verificación y la autenticación, el equipo de ingeniería puede identificar

fácilmente si hay servicios deshonestos que intenten conectarse al dron. El dron, al detectar servicios deshonestos, simplemente puede aterrizar en el sitio original de despegue.

Cualquier servicio que detecte un dron inseguro en el sistema también puede generar avisos internos. El equipo de administración, en ese momento, puede determinar cómo lidiar con el dron potencialmente comprometido. Esto proporciona un nivel de agilidad con respecto a los eventos de seguridad y también le brinda a la empresa una forma de evaluar si hay problemas de software o hardware que causan un comportamiento anormal en el dispositivo periférico.

9.6 Resumen

Si bien el equipo de ingeniería, obviamente, gastó un tiempo muy importante para crear una arquitectura resistente desde una perspectiva de ingeniería mecánica y servicios de back-end, se debe entender que para crear una tecnología segura en el Dispositivo Periférico se requiere de un trabajo muy complejo. Si bien este escenario no representaba una amenaza crítica para el negocio en general del dron, fue una suerte que hubiera una solución que funcionara lo suficientemente bien para las necesidades de sus clientes. Si estos hubieran requerido una tecnología más crítica para la seguridad, incluso la solución propuesta para su despliegue aquí podría no haber sido suficiente.

Para obtener más información sobre las variantes de Base de Cómputo de Confianza, tales como “Personalized Pubkey TCB” o “Personalized PSK TCB”, revise los documentos del Ecosistema del Servicio IoT [3] y de Dispositivos Periféricos [4].

10 Ejemplo – Red de Sensores para Vehículos

En este ejemplo, una red de sensores para vehículos desplegada en una nueva clase de automóvil será evaluada mediante este conjunto de lineamientos. El Dispositivo Periférico se evaluará mediante el documento del Ecosistema de Dispositivos Periféricos, mientras que la parte del servicio correspondiente al diseño se evaluará mediante el documento del Ecosistema de Servicios.

10.1 Descripción General del Dispositivo Periférico

Primero, comencemos por evaluar el diseño hardware del automóvil con su red de sensores.

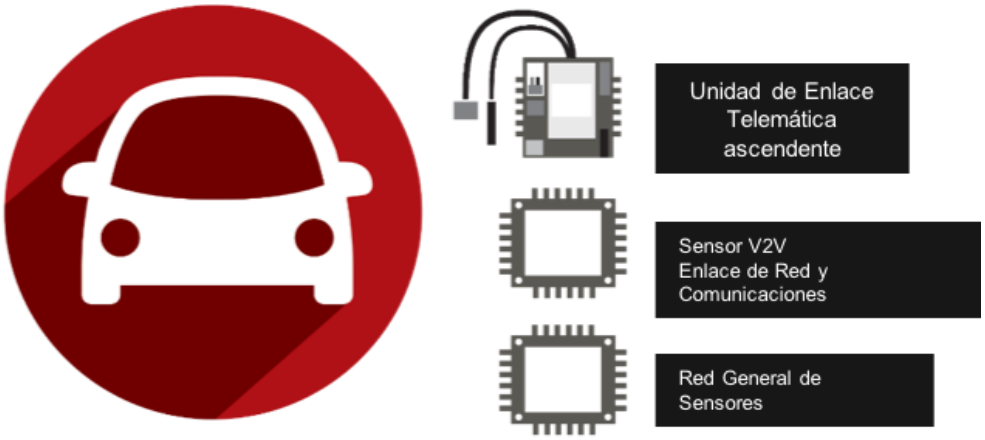

Figura 8– Sistema Completo de una red de Sensores para Vehículos junto con sus Comunicaciones

Como el sistema en la realidad es demasiado complejo para ser representado correctamente con todos los elementos de la solución en un solo diagrama, los tres componentes principales que se han decidido representar son:

- Una unidad de enlace telemática ascendente que gestiona la red de sensores, toma decisiones complejas en nombre del conductor y mantiene una conexión con el sistema de back-end
- Un sistema vehículo a vehículo (V2V) que detecta y reacciona ante los eventos de V2V
- Una red general de sensores que proporciona medidas a la unidad de enlace telemática ascendente

En los sistemas automotrices modernos, la unidad telemática es una parte de la red de informática del automóvil y toma decisiones basadas en datos de los sensores y en las comunicaciones con el back-end. Esta unidad tomará decisiones con, o en nombre de los consumidores que estén conduciendo el vehículo. La unidad telemática asegura que el vehículo está funcionando correctamente, intenta tomar decisiones inteligentes durante las emergencias y recibe comandos de la red conectada al back-end.

La red de sensores V2V identifica vehículos en los alrededores y toma decisiones basadas en las medidas efectuadas por los sensores. Mientras que la unidad telemática principalmente toma decisiones basadas en el estado de los componentes (como los frenos o los medidores de presión de los neumáticos), el sistema V2V toma decisiones basadas en la presencia de otros vehículos, o envía alertas a los vehículos cercanos en el caso de un evento crítico.

La red de sensores general está compuesta por una serie de componentes que proporcionan datos a la unidad telemática y a veces a la unidad V2V. Estas unidades usan la información obtenida en la red general de sensores para tomar decisiones precisas durante eventos críticos.

Según el documento del Ecosistema de Dispositivos Periféricos, este sistema tiene componentes que encajan en cada clase de Dispositivos Periféricos de IoT. La unidad de enlace ascendente de telemática actúa como una “puerta” de entrada. La unidad de V2V actúa como un Dispositivo Periférico complejo. Los dispositivos que implementan la red general de sensores son en realidad todos Dispositivos Periféricos “ligeros”.

10.2 Descripción General del Servicio

Desde la perspectiva del servicio, la red de sensores del vehículo proporcionará medidas hacia el back-end. Esta información puede o no, ser proporcionada a los consumidores. Más bien, el fabricante podría almacenar los datos para observar o identificar posibles problemas con los componentes. Esto puede desencadenar que las alarmas de mantenimiento posteriormente se presenten al consumidor.

El sistema también puede ser mejorado para proporcionar servicios útiles para el consumidor, tales como "desbloquear remotamente la puerta", "arrancar el motor" y servicios con características similares. En un futuro próximo, estos sistemas podrían permitir que los vehículos puedan ser conducidos remotamente a través de sistemas de guiado automatizados.

Mientras que las decisiones más importantes se harán en las unidades de procesamiento en el vehículo propiamente dicho, es razonable pensar que algunas decisiones se tomarán en la nube, donde con mayor facilidad se podrá aplicar el aprendizaje de máquina (ML) y la inteligencia artificial (AI) junto con modelos de comportamiento o estadísticos que puedan permitir tomar decisiones más complejas.

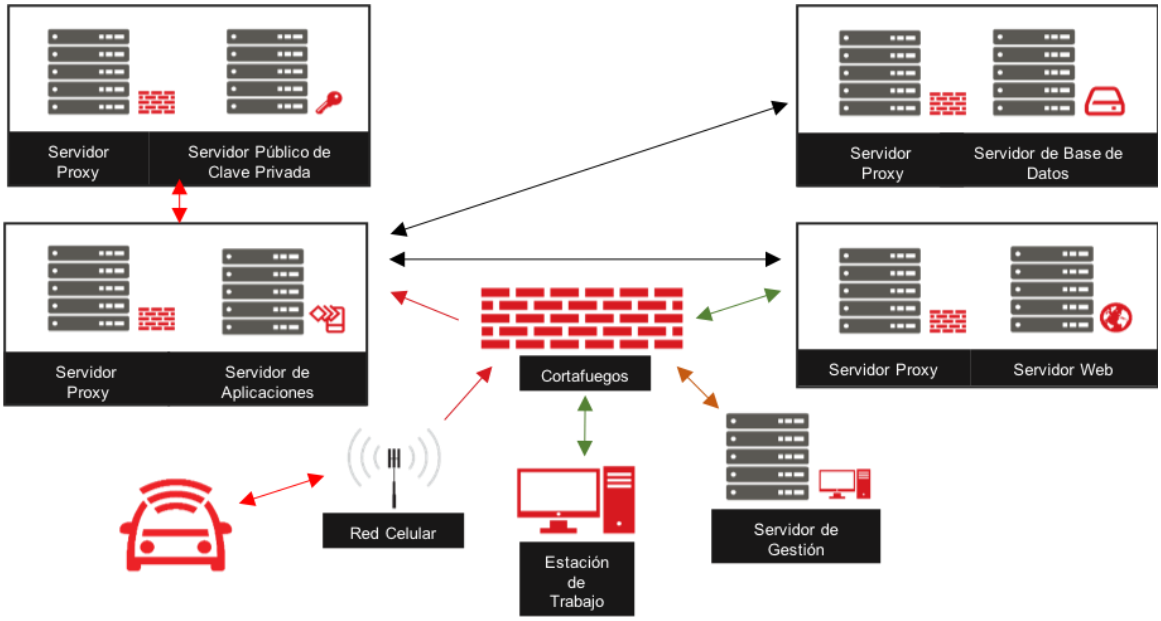

Figura 9– Flujo de Datos hacia los Servicios de Back-end

10.3 El Caso de Uso

El caso de uso de esta tecnología es evidente: y es construir vehículos más inteligentes que puedan tomar decisiones complejas en escenarios críticos. El objetivo es aprovechar la inteligencia de tantos sensores como sea posible para tomar decisiones críticas en ventanas de tiempo muy pequeñas. Frenado automático, difusión de alertas de reventón de neumáticos, desactivación temporal de las advertencias del operador, y otros escenarios potencialmente críticos pueden resolverse mediante el uso de sensores y sistemas informáticos bien diseñados.

Una característica interesante de esta tecnología es que puede ser totalmente transparente para el usuario. El usuario no necesita configurar estos equipos para actuar de cierta manera. Por el contrario, debe ser capaz de controlar unos casos de uso deseados mediante el uso de los parámetros de los sensores. Esto permitirá que las computadoras se comporten correctamente sin importar el entorno.

10.4 El Modelo de Seguridad

El equipo de ingeniería de esta empresa que implementa esta solución, aprovechó las secciones de las Pregunta Frecuentes de seguridad en los documentos de los Ecosistemas de Dispositivos Periféricos y Servicios para determinar qué problemas son más relevantes para su producto y servicio.

Desde una perspectiva de Dispositivos Periféricos, el equipo detectó las siguientes cuestiones clave como motivo de preocupación:

- Suplantación de Dispositivo Periférico
- Suplantación de servicio o de los “socios” en la comunicación V2V
- Ataques de canal lateral
- Detección de Dispositivos Periféricos comprometidos
- Garantizar la protección por encima de un riesgo de seguridad

Desde la perspectiva del servicio, el equipo decidió que los siguientes temas son motivo de preocupación:

- Identificación de comportamiento anómalo en un Dispositivo Periférico
- Gestión de la privacidad de los usuarios

El mayor riesgo en este entorno que no ha sido discutido en los ejemplos anteriores, es el riesgo de suplantación con respecto a los socios de comunicación. Una preocupación que tienen los ingenieros en este tipo de entornos, es el riesgo de que una computadora o servicio tome decisiones críticas utilizando datos que no se autentican correctamente.

Ya que los datos provenientes de los sensores en escenarios críticos como este requieren que se procesen excepcionalmente rápido, la teoría es que puede que no siempre sea factible la implementación de criptografía asimétrica o PKI para las comunicaciones. Sin embargo, esto no puede ser una afirmación siempre cierta. En cambio, un modelo de seguridad preciso debe tomar decisiones por adelantado en escenarios críticos y utilizar claves de sesión previamente guardadas en el caché para Dispositivos Periféricos cercanos. Por ejemplo, si dos objetos se acercan entre sí a un ritmo conocido, las aplicaciones de seguridad en el ecosistema de servicios pueden preparar las claves de sesión específicas de estos dos extremos antes de que lleguen a chocar. Esto garantizaría que una comunicación segura entre los dispositivos periféricos y sensores pueda seguir utilizándose en caso de que no haya tiempo para renegociar una sesión segura instantánea cuando se detecta la posibilidad de un escenario crítico (como un choque inminente).

Por lo tanto, es necesaria una mejora en la implementación del TCB. Una solución interesante es GBA, donde la UICC en la unidad telemática de enlace ascendente puede distribuir claves seguras para Dispositivos Periféricos en todo el sistema. Este protocolo permitirá incluso que

Dispositivos Periféricos ligeros puedan ser identificados con claves de sesión seguras (previamente enviadas) que se pueden utilizar en múltiples escenarios críticos. De esta manera, en el entorno del sistema global siempre se pueden desplegar las claves a partir de una raíz de confianza, aunque los Dispositivos Periféricos ligeros no sean capaces de los cálculos necesarios para la inicialización de una sesión con una clave pública.

Otra cuestión vital en estos entornos es detectar que Dispositivos Periféricos han sido comprometidos desde el punto de vista de la seguridad. Por ejemplo, ¿cómo puede el entorno del sistema reconocer si un sensor simple, como un Monitor de presión de neumáticos (TPM) ha sido comprometido? Si la computadora toma una decisión crítica basada en el TPM señalizando que un neumático ha pinchado, puede surgir un problema de seguridad. Como resultado, el comportamiento de los dispositivos y su confiabilidad, deben ser re-evaluados en cada fase de arranque de sistema. Todos los dispositivos deben ser resistentes a las manipulaciones externas y deben ser capaces de notificar a la red si la seguridad ha sido comprometida. Por otro lado, debe de existir una forma de que otros dispositivos en la red de sensores puedan evaluar la confiabilidad de sus pares en la red al comunicarse.

10.5 El Resultado

Después de haber seguido las recomendaciones, la red de sensores del vehículo estará bien protegida contra los ataques a la red de comunicaciones del vehículo. GBA se utiliza para distribuir las claves de seguridad a todos los Dispositivos Periféricos en el sistema y así lo hace en cada arranque de sistema, asegurando que no se reutilicen las claves antiguas. Esto, junto con la resistencia a manipulaciones externas, una TCB sólida en cada Dispositivo Periférico y una raíz de confianza organizacional, permite que el entorno del sistema funcione con un menor riesgo.

Sin embargo, independientemente de estos cambios, la seguridad es todavía un factor crítico. El equipo de ingeniería y la dirección empresarial, junto con el equipo legal de la empresa y corredores de seguros, deben evaluar la tecnología crítica para la seguridad empleada y determinar si se puede implementar esa tecnología sin arriesgar la seguridad o protección de los usuarios. Aunque a menudo se pueda implementar un sistema seguro, incluso en escenarios críticos, con algunos ajustes en la arquitectura, hay veces que es mejor priorizar la seguridad con respecto a otras preocupaciones en la implementación.

10.6 Resumen

Este tipo de productos normalmente están bien diseñados, y es muy complicado atacar el ecosistema que lo forma. Sin embargo, defectos sutiles en la arquitectura de comunicaciones pueden conducir a un entorno donde la seguridad ha sido comprometida. En “jardines vallados”, como en algunas redes de tipo CANbus, un solo extremo defectuoso puede causar que todo el sistema sea vulnerable. Esto, en entornos de seguridad crítica, es inaceptable.

Anexo A Consideraciones sobre la Privacidad Recomendadas a Proveedores de Servicios IoT

Con el fin de generar confianza en el ecosistema de IoT y minimizar la necesidad de una intervención regulatoria formal, la GSMA propone los siguientes pasos de alto nivel como guía para minimizar cualquier riesgo de privacidad. Recomendamos que los proveedores de servicios de IoT sigan estos pasos y consideren estas preguntas en las primeras etapas de desarrollo de su servicio o producto de IoT.

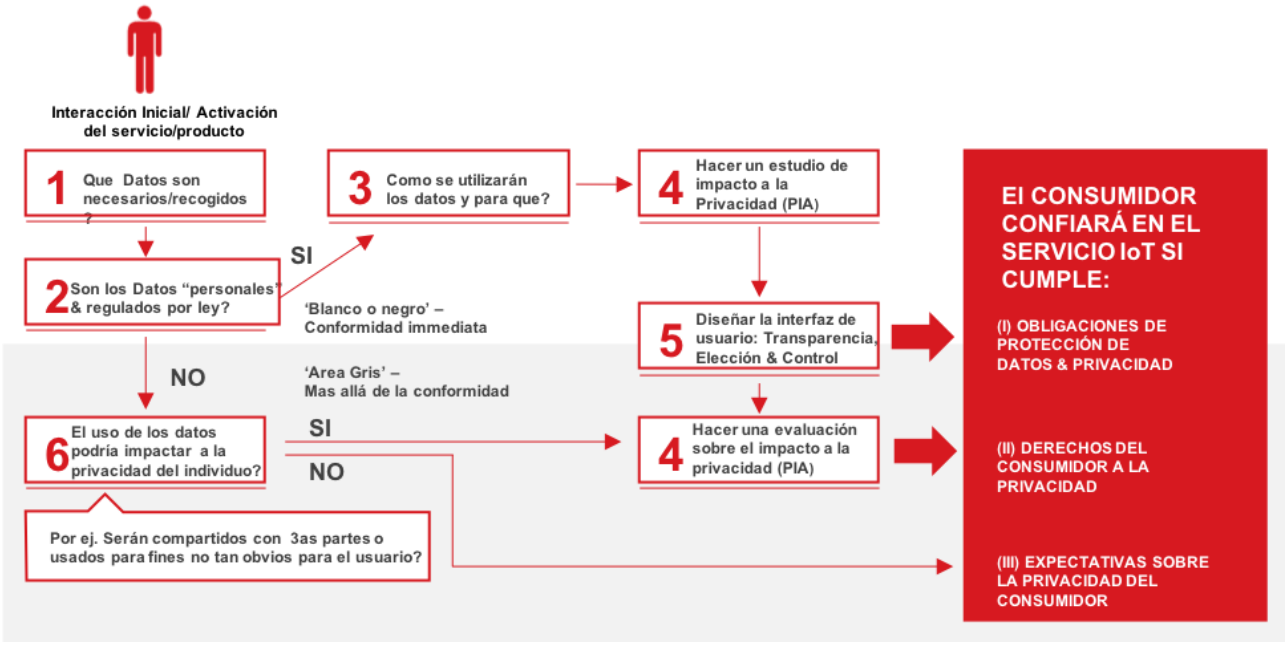

Figura 10– Árbol de Decisión sobre la Privacidad por Diseño de la GSMA

Paso	Consideraciones
Paso 1	**¿Qué datos necesita recopilar de / acerca del usuario para que su producto o servicio de IoT pueda funcionar correctamente?** Uno de los primeros pasos en cualquier modelo de negocio que se basa en datos es identificar qué información se necesita realmente del consumidor o acerca de él, para que el servicio o producto funcione correctamente. Los tipos de datos que requiere un servicio pueden categorizarse como estáticos, como el nombre del consumidor o la dirección particular, y los datos que son dinámicos, como la ubicación en tiempo real. Entonces, si se ofrece, por ejemplo, una pulsera de "fitness" que cuenta los pasos y las calorías que una persona quema, entonces se necesitaría saber el peso, la edad, el sexo, la distancia recorrida y la frecuencia cardíaca del usuario, pero se podría decir que no se necesita la ubicación real del individuo. Al evaluar los tipos de datos necesarios, también es importante decidir si se necesita el consentimiento de las personas para usar esos datos y cómo se obtendría su consentimiento o bien ofrecerles opciones para controlar sus preferencias de privacidad. Un teléfono inteligente podría actuar como un medio para ofrecer al usuario opciones de privacidad (por ejemplo, una aplicación móvil o una página web) cuando el producto en sí no tenga pantalla.

Paso 2	**¿Los datos son 'personales' y están regulados por la ley?**
	
	El siguiente paso debería ser identificar los requisitos de privacidad y protección de datos que la ley impone. Las preguntas por considerar incluyen:
	• ¿Cuál es la definición de datos 'personales' en el país / mercado en cuestión?
	• ¿Los datos son 'personales' y están regulados por la ley? De ser así, ¿ha identificado la base legal que le permite procesar esos datos?
	• ¿Está sujeto a condiciones de licencia relacionadas con la privacidad (por ejemplo, como proveedor de telecomunicaciones)?
	• ¿Existen leyes federales, estatales, locales o sectoriales que se apliquen en relación con su modelo de recopilación de datos propuesto, además de las leyes generales de protección de datos? p. ej.:
	  ○ Servicios financieros / de pago, regulaciones sanitarias
	  ○ Restricciones potenciales en transferencias de datos entre fronteras nacionales

Paso 3	**¿Cómo se usarán los datos y para qué?** Una vez que haya establecido cuáles son sus requisitos legales de cumplimiento, el siguiente paso es determinar cómo se usarán los datos que recopila, y con quién deben ser compartidos, para lograr los resultados previstos como parte de su oferta de servicios. Las siguientes preguntas deberían ayudarlo a abordar consideraciones de seguridad y privacidad en relación con el tratamiento de los datos: • ¿Los datos se mantienen seguros, cuando son almacenados y cuando se transmiten? • ¿Ha establecido claramente los flujos de datos? Es decir, identificar cómo se usarán y compartirán los datos en toda la cadena de valor y con qué fines • ¿Se puede justificar por qué se necesita cada tipo de datos recopilados en el contexto específico en el que se ofrece el servicio deseado? • ¿Ha definido / acordado responsabilidades de privacidad con sus socios desde el principio (y su diseño de producto refleja estas responsabilidades)? • ¿Existen acuerdos contractuales adecuados con las empresas con las que comparte los datos de los consumidores? (Por ejemplo, limitar el uso de datos por parte de los proveedores analíticos para sus propios fines comerciales). Tales acuerdos o restricciones pueden ser bilaterales o podría establecer un código de conducta o directrices y pídales a sus socios que las sigan al pie de la letra, acarreando consecuencias concretas y responsabilidades si no lo hacen.

Paso 4	**Llevar a cabo una evaluación de impacto de privacidad** La realización de una evaluación de impacto en la privacidad (PIA) trata de: • Identificar qué riesgos de privacidad que se plantean en un producto o servicio para las personas. • Reducir el riesgo de daño a las personas que pueda surgir del posible uso indebido de su información personal • Diseñar un proceso más eficiente y efectivo para manejar datos sobre personas Los requisitos de PIA se están volviendo cada vez más comunes en las leyes de protección de datos y privacidad. Hay una serie de guías sobre cómo llevar a cabo una PIA, incluidas las publicadas por la Oficina del Comisionado de Información del Reino Unido [10] y las de la Asociación Internacional de Profesionales de la Privacidad. Las preguntas típicas que deben abordarse al realizar una PIA incluyen: • ¿El resultado del proyecto podrá acarrear que usted / sus socios tomen decisiones o tomen medidas contra personas que de cierta manera puedan tener un impacto significativo sobre ellas? • ¿Es particularmente probable que la información sobre individuos de algún tipo genere inquietudes o dudas sobre la privacidad? Por ejemplo, los registros de salud, los antecedentes penales u otra información que las personas consideren privada. • ¿Requerirá el proyecto que te pongas en contacto con las personas utilizando métodos que puedan ser intrusivos?

Paso 5	**Diseñar la privacidad en la interfaz de usuario**
	
	Después de evaluar los riesgos de privacidad para los consumidores, debe considerar cómo concientizar a los consumidores sobre dichos riesgos y cómo mitigarlos, así como también ofrecerles opciones para expresar sus preferencias de privacidad. En última instancia, este paso consiste en garantizar que ofrezca un servicio que cumpla con las obligaciones legales y las necesidades y expectativas de los consumidores de una manera que sea fácil de usar. Todo esto es para generar confianza en los usuarios asegurándoles que tienen más control sobre su privacidad. Las preguntas a considerar incluyen:
	• ¿Cómo se puede informar a los consumidores sobre los riesgos de su privacidad y cómo pueden tomar decisiones informadas?
	• ¿Ha obtenido su consentimiento, cuando así lo exige la ley? Los elementos clave del consentimiento incluyen: revelación, comprensión, voluntariedad, competencia y acuerdo)
	• ¿Se aseguran los datos cuando están en tránsito y en reposo?
	• ¿Existe un período establecido para el cual necesita conservar los datos del consumidor (y por qué)?
	• ¿La experiencia de uso del consumidor ayuda a ganarse su confianza? Por ejemplo:
	  ○ ¿Entienden que datos comparten a cambio de utilizar el servicio?
	  ○ Los consumidores pueden expresar sus preferencias de privacidad en pasos sencillos como por ejemplo, mediante una página web basada en un 'panel de permisos' con avisos en el ‘momento justo’, un “call centre”, una aplicación móvil, un comando activado por voz, etcétera.

Paso 6	**¿Podría el uso de datos afectar la privacidad de un individuo?** Su producto o servicio puede recopilar datos que no están necesariamente clasificados como 'personales' por ley, pero que pueden tener implicaciones de privacidad para el consumidor y, por lo tanto, deben considerarse desde el principio. Para comprobar si los datos relevantes podrían ser utilizados y afectarían la privacidad del consumidor, considere lo siguiente: • ¿Se podrían combinar los datos (no personales) de su servicio / producto con otros datos de diferentes fuentes para hacer inferencias sobre la vida personal del consumidor? Por ejemplo, inferencias sobre su estilo de vida, hábitos o religión que podrían: o ¿influir en su capacidad de contratar un seguro de salud? o ¿Lo utilizan terceros (minoristas, compañías de seguros) para determinar precios discriminatorios hacia el consumidor específico? • Si es probable que su producto o servicio cambie en algún momento en el futuro, ¿cuáles son las posibles implicaciones de privacidad de dicho cambio en el consumidor? Por ejemplo: o ¿El cambio implica la recopilación de nuevos datos sobre el consumidor (como los datos de localización)? o ¿Los datos del consumidor existentes o nuevos se comparten o se venden a terceros (por ejemplo, los anunciantes) que comenzarían a utilizar los datos del consumidor para fines diferentes a los originalmente destinados? • Si se producen dichos cambios, debe: o Comprobar el posible impacto en su negocio si nuevas leyes serían de aplicación como resultado del cambio o Establezca procesos para informar a los consumidores y obtenga su consentimiento cuando sea necesario o Proporcione los medios para que los consumidores cambien sus preferencias de privacidad • Recomendamos que los proveedores de servicios IoT consideren las siguientes recomendaciones adicionales: o Asegúrese de contar con los acuerdos contractuales adecuados que definan las responsabilidades de cada socio y actor en la cadena de valor o Tenga un proceso claro de corrección de errores para que los consumidores sepan a quién dirigirse si las cosas van mal o si sufren una violación a la privacidad

Anexo B Ejemplo Basado en un Sistema de Rastreo de Vehículos

En este ejemplo, un sistema de rastreo de vehículos se evaluará desde la perspectiva de los Lineamientos de seguridad de IoT. El proceso se extraerá básicamente de la sección siete de este documento general: " Como Usar esta Guía de Manera Efectiva ".

B.1 Evaluación del Modelo Técnico

En el primer paso, "Evaluar el modelo técnico", el equipo de ingeniería evalúa cómo funciona el dispositivo en función de la arquitectura de su producto. El equipo de ingeniería crea un documento que detalla las tecnologías utilizadas en la solución para organizar al personal, asignar tareas de seguridad y realizar un rastreo del progreso de implementación.

En aras de la simplicidad, nuestro sistema de rastreo automotriz tendrá las siguientes capacidades:

- **Ecosistema de Equipos Periféricos:**
  - Una simple interfaz gráfica de usuario (GUI) que permite al usuario:
    - Iniciar sesión con un nombre de usuario y contraseña
    - Deshabilitar el rastreo
    - Habilitar el rastreo
    - Identificar y visualizar la ubicación actual
  - Un módulo celular para conectarse con los servicios de back-end
  - Una tarjeta SIM integrada en el módulo celular
  - Una pila de polímero de litio como alimentación de respaldo
  - Una unidad de procesamiento central (CPU)
  - Una aplicación incorporada en RAM no volátil
  - RAM
  - EEPROM

- **Ecosistema de Servicios:**
  - Conectividad celular para los datos
  - APN privado seguro
  - Punto de acceso al servicio
  - Servicio de administración OTA del módem celular
  - Servicio de administración de tarjeta SIM OTA

Después de identificar la información relevante para cada tecnología, el equipo revisa la sección de Modelo en cada documento de lineamientos e identifica el modelo tecnológico apropiado. El Dispositivo Periférico en este caso puede considerarse como complejo. El modelo de servicio y de red es un servicio estándar de IoT habilitado para dispositivos móviles.

B.2 Revisión del Modelo de Seguridad

Con el modelo técnico descrito, la organización debería estar lista para seguir con la revisión del modelo de seguridad. En el modelo de seguridad, el equipo evaluará como un adversario podría atacar la solución.

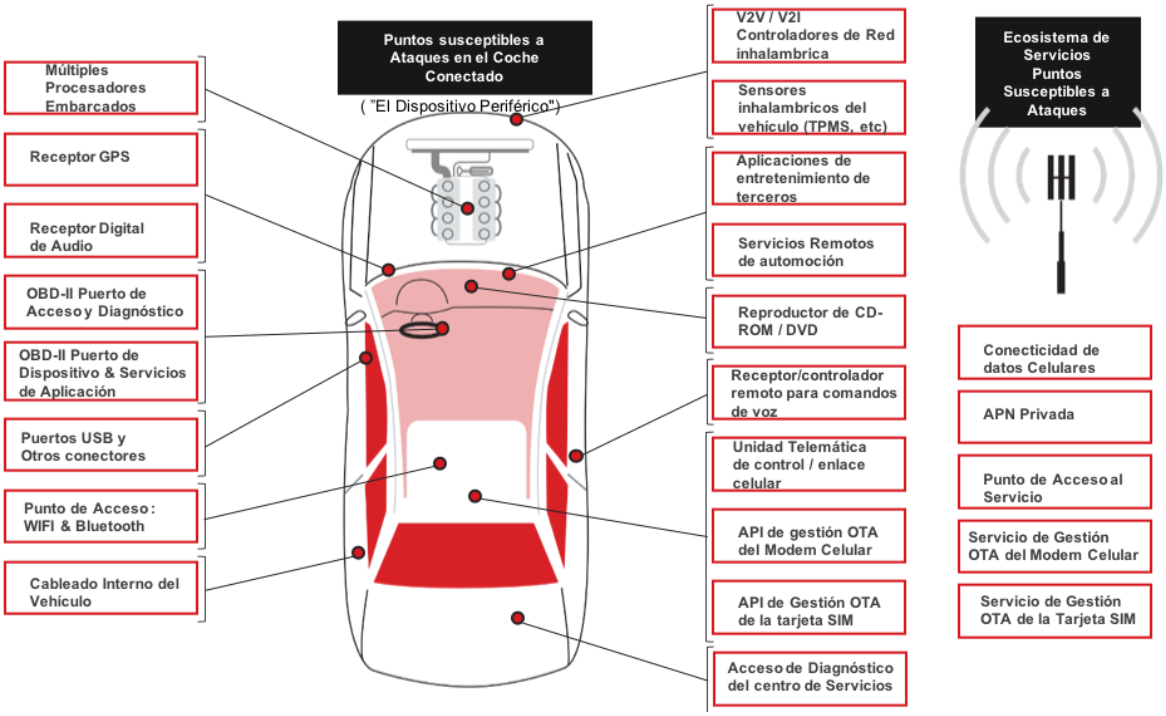

Figura 11– Vectores de Ataque en el Coche Conectado

En nuestra solución de ejemplo, solo hay dos áreas concretas susceptibles de sufrir un ataque de seguridad:

- La red celular
- Un ataque dentro del propio vehículo

Como no hay una conexión de red local, solo una conexión de red móvil, un atacante tendría que comprometer la conexión de red celular, infiltrarse en el canal de comunicaciones desde la APN privada o infiltrarse a través del punto de acceso de servicio, o a través de los servidores de administración OTA del módem celular o de la tarjeta SIM.

La otra forma de comprometer al servicio o dispositivo periférico es a través de un ataque físico ya que existen múltiples puntos de entrada dentro del vehículo (o vectores de ataque), como se muestra en el diagrama, por lo que en el caso de este servicio de IoT, se debería tener especial cuidado y enfocar muchos esfuerzos en el diseño de las interfaces y procesos dentro del vehículo.

B.3 Revisión y Asignación de Tareas de Seguridad

Con el modelo de seguridad evaluado, ahora es sencillo asignar tareas de seguridad. Cada equipo debe asignar una persona específica para cada Componente de la solución que necesita ser evaluado, no solo desde la perspectiva de alto nivel (punto final, red y servicio) sino también desde la perspectiva de cada componente de un elemento en particular. Esto significa que a la CPU se le debe asignar un responsable técnico, al sistema operativo, al servicio de red, etc., de la misma forma.

Una vez que cada Componente se asigna a un responsable, el proceso puede comenzar. Esto significa que, en esta etapa, el equipo entiende:

- De que está compuesta la tecnología
- Qué tecnologías afectan la seguridad
- Qué ingenieros especializados son responsables de cada tecnología identificada dentro de la solución

B.4 Revisión de las Recomendaciones

En la fase de revisión de las recomendaciones, cada miembro del equipo debe leer y comprender tantas recomendaciones de seguridad como sea posible. Esto es por principios de diseño. En lugar de centrarse únicamente en las recomendaciones asignadas a un Componente específico, los ingenieros deben tomarse el tiempo para comprender tantas recomendaciones como sea posible, aunque sea a alto nivel, para obtener una mejor visión de cómo su Componente afecta la seguridad general del producto o servicio. De esta manera, el grupo puede entablar una valiosa discusión sobre qué estrategias para la reparación o reducción del riesgo tendrán el mayor equilibrio desde una perspectiva de efectividad del costo, longevidad y administración.

Una vez que se revisan las recomendaciones, los propietarios del componente pueden determinar si ya se ha aplicado una recomendación o marcar una recomendación pendiente. Esto permitirá al grupo de diseño que debata sobre la aplicabilidad de una recomendación antes de su implementación. Esta es una mejor estrategia a seguir, ya que algunas recomendaciones pueden tener efectos secundarios que afecten al cumplimiento de otras recomendaciones o controles existentes.

En este ejemplo, el equipo habría determinado que:

- Se debe utilizar una base de confianza de aplicaciones
- Se debe definir una raíz de confianza de la organización
- Se debe personalizar al dispositivo
- Se debe implementar la protección contra la manipulación en las cajas o revestimientos de los dispositivos
- Se debe implementar una administración de contraseñas para los Dispositivos Periféricos
- Se deben implementar unas comunicaciones seguras para los Dispositivos Periféricos
- Cualquier imagen procesada debe firmarse criptográficamente
- Se debe implementar la gestión de la privacidad
- Las alertas de consumo de los dispositivos deben estar integradas

B.5 Revisión de los Riesgos en los Componentes

A continuación, la sección Componentes debe evaluarse para identificar los diversos riesgos involucrados en la implementación o integración de un Componente particular en el producto o servicio. En general, esta sección solo puede ser revisada por el responsable del componente para optimizar el trabajo. Sin embargo, siempre es beneficioso leer tanto como sea posible todas las Recomendaciones.

Después de revisar las Recomendaciones y la sección de riesgos del componente, se identificaron las siguientes lagunas de seguridad:

- Los secretos se almacenan sin protección en la EEPROM
- Los secretos no se procesan en la memoria RAM interna
- La interfaz de usuario debe proteger las contraseñas
- La privacidad de usuario debe ser explicada claramente a los usuarios

B.6 Implementación y Revisión

Ahora el equipo puede ajustar la solución para cumplir con los requisitos de seguridad acordados. El equipo vuelve a implementar los componentes, cuando sea necesario, y agrega controles de seguridad, donde sea preciso en el diseño.

En este momento en particular, el equipo ha identificado que están trabajando con un miembro de GSMA que es capaz de aprovisionar una tarjeta SIM que contiene tecnología de ancla de confianza compatible con la aplicación. Esto resolverá la necesidad que habían detectado de utilizar un ancla de confianza utilizando la tarjeta SIM existente. Esto también resuelve la personalización, ya que cada tarjeta SIM se puede personalizar “en el terreno” utilizando la tecnología estándar de la GSMA.

La tecnología SIM también puede ayudar a proporcionar claves de seguridad de comunicación a través de la interfaz de radio, resolviendo el requisito concerniente a implementar la autenticación y la privacidad de las comunicaciones.

La zona específica asignada a la empresa dueña de la solución dentro de la SIM, puede ser programada con una raíz de confianza base que permita a la empresa autenticar a sus pares utilizando una cadena de certificados. Esto resuelve los requisitos de tener una raíz de confianza para la organización y la autenticación de pares.

La caja o empaquetamiento del/los producto/s se actualiza con una solución adecuada, a prueba de manipulaciones.

La EEPROM se codificará con datos cifrados con las claves de seguridad almacenadas en el ancla de confianza de la SIM.

El gestor de arranque se modifica para usar el ancla de confianza para la autenticación de la imagen de la aplicación.

Los Dispositivos Periféricos se reprograman para admitir el uso de una contraseña segura de usuario bloqueando los caracteres de la contraseña a medida que se escriben en la interfaz.

Se agrega una Interfaz Gráfica de Usuario (GUI) para la administración de la privacidad para que el usuario pueda ver y controlar qué información está recopilando la empresa dueña de la aplicación.

Los secretos se procesan solo en la memoria interna del mismo chip.

Una vez que se definan estas implementaciones, el equipo vuelve a evaluar todas las Recomendaciones y Riesgos de seguridad, y revisa el Modelo de seguridad para identificar si los cambios han resuelto sus inquietudes y prioridades de seguridad.

B.7 El Ciclo de Vida Actual

Ahora que el equipo de diseño ha logrado una configuración aprobada por todos, están listos para implementar la solución tecnológica. Sin embargo, la seguridad no se detiene aquí. El equipo negocia con los distintos equipos de diseño una metodología para monitorear los Dispositivos Periféricos y así detectar anomalías de seguridad y una metodología para identificar si la tecnología que están utilizando contiene brechas de seguridad recientemente descubiertas.

El equipo planificará cómo cada incidente o brecha se identifica, se remedia y se recupera. Esto garantizará que, con el tiempo, el avance tecnológico y de la seguridad (ataques y brechas) no tome por sorpresa a la empresa.

Anexo C Gestión del Documento

C.1 Historial de Edición del Documento

Versión	Fecha	Descripción Breve del Cambio	Aprobación Autoridad	Editor / Empresa
1.0	08-Feb-2016	Nuevo PRD CLP.11	PSMC	Ian Smith GSMA & Don A. Bailey Lab Mouse Security
1.1	07-Nov-2016	Se agregaron referencias al esquema de evaluación de seguridad de IoT de GSMA. Correcciones editoriales menores.	PSMC	Ian Smith GSMA
2.0	29-Sep-2017	Agregue información de red LPWA al documento y otras actualizaciones menores.	Grupo de Seguridad IoT	Rob Childs GSMA

C.2 Otra Información

Tipo	Descripción
Dueño del Documento	Programa IoT de la GSMA
Contacto	Rob Childs - GSMA

Es nuestra intención proporcionar un producto de calidad para que nuestros lectores lo usen de manera eficaz. Si encuentra algún error u omisión, contáctenos para hacernos llegar sus comentarios. Puede notificarnos a prd@gsma.com

Sus comentarios o sugerencias serán bien recibidas.