UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE ARQUITECTURA E INGENIERÍAS

Trabajo de fin de carrera titulado:

DESARROLLO DE UN MODELO PARA EL ANÁLISIS DE VULNERABILIDADES DE DISPOSITIVOS INTELIGENTES DE RECONOCIMIENTO DE VOZ, BASADO EN LA NORMA ISO/IEC 27005:2011, CASO DE ESTUDIO AMAZON ECHO (ALEXA)

Realizado por:

OTILIA PATRICIA GUZMÁN VILLAGÓMEZ

Director del proyecto:

DR. DANIEL RIOFRÍO

Como requisito para la obtención del título de:

MÁSTER EN TECNOLOGÍAS DE LA INFORMACIÓN

DECLARACIÓN
JURAMENTADA

Yo, OTILIA PATRICIA GUZMÁN VILLAGÓMEZ, con cédula de identidad # 170607405-9 declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y, que ha consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

Otilia Patricia Guzmán Villagómez

C.C.: 170607405-9

DECLARATORIA

El presente trabajo de investigación titulado:

“DESARROLLO DE UN MODELO PARA EL ANÁLISIS DE VULNERABILIDADES DE DISPOSITIVOS INTELIGENTES DE RECONOCIMIENTO DE VOZ, BASADO EN LA NORMA ISO/IEC 27005:2011, CASO DE ESTUDIO AMAZON ECHO (ALEXA)”

Realizado por:

OTILIA PATRICIA GUZMÁN VILLAGÓMEZ

Como Requisito para la Obtención del Título de:

MÁSTER EN TECNOLOGÍAS DE LA INFORMACIÓN

Ha sido dirigido por el profesor

DR. DANIEL RIOFRÍO

Quien considera que constituye un trabajo original de su autor

Dr. Daniel Riofrío

DIRECTOR

LOS PROFESORES INFORMANTES

ING. VERÓNICA RODRÍGUEZ, MBA

DR. DIEGO RIOFRÍO

Después de revisar el trabajo presentado, lo han calificado como apto para su defensa oral ante el tribunal examinador

Ing. Verónica Rodríguez, MBA

Dr. Diego Riofrío

Quito, abril, 2018

DEDICATORIA

.

Dedico el presente trabajo de investigación a:

La mujer más importante de mi vida, mi mamita Amalia, quien siempre creyó en mí, y que pese a que hoy no está conmigo físicamente, estoy segura que hoy, en el cielo, ella está muy feliz y orgullosa de mí. Te amo mami.

A mi papá Jorge, para que éste logro de su hija, alivie en algo el dolor que lleva en su corazón por la partida de mi mami.

AGRADECIMIENTO

A mi Dios, por estar conmigo y darme la fortaleza necesaria para afrontar todos los duros momentos que tuve que vivir a lo largo del desarrollo de este proyecto; por toda la sabiduría que me ha dado y su infinito amor. A Él toda la gloria y honra.

A mi familia, por todo su apoyo y motivación para llevar a cabo este trabajo. Gracias por haberme permitido tomar tiempo que les pertenecía a ustedes, para poder llevar a cabo este trabajo. Gracias por creer en mí.

Un especial agradecimiento a mi director de tesis, Daniel Riofrío, por todo su tiempo, ayuda, colaboración, apoyo, y motivación para poder realizar el presente trabajo. Sin su ayuda simplemente no lo hubiese podido lograr. Sin duda, la mejor decisión fue trabajar junto a usted. Gracias Daniel.

A Fabiola Moyón, por su invaluable ayuda y conocimientos de seguridad compartidos para la elaboración de este trabajo de investigación. Gracias Faby.

Tabla de Contenidos

Lista de Figuras

Lista de Tablas

Lista de Fórmulas

Lista de Matrices

RESUMEN

El presente trabajo de investigación pone de manifiesto las vulnerabilidades a las que como usuarios estamos expuestos al utilizar dispositivos de reconocimiento de voz, en particular, el caso de estudio de este trabajo: Amazon ECHO, Alexa. Pese a que el objetivo de este dispositivo es facilitar actividades cotidianas a sus usuarios, éstos no están exentos de ser manipulados por terceros, vulnerando así no solo la seguridad de nuestros hogares, sino también poniendo en riesgo nuestra privacidad. Con el estudio preliminar, de vulnerabilidades de estos dispositivos, se plantea un modelo de gestión seguridad de éstas, el cual busca asegurar el entorno del usuario de estos dispositivos. El modelo se basa en la norma ISO-IEC 27005:2011, la cual proporciona directrices, para gestionar riesgos, a través de la identificación de activos, amenazas, vulnerabilidades, eventos existentes y los controles de seguridad a aplicarse. Con la ayuda de esta norma, y con la opinión de los usuarios obtenida a través de una serie de entrevistas semiestructuradas, se elaboran matrices de riesgos y sugieren controles de seguridad, con el fin de que puedan ser adoptados por los mismos y asegurar su entorno actual. Por otro lado, con el fin de evidenciar una vulnerabilidad física y lógica de interés por sus características técnicas, se llevó a cabo un experimento, en donde se reproduce un ataque a través de comandos inaudibles de voz, logrando visualizar de forma clara un tipo de ataque al que los usuarios están expuestos. Como conclusión, se pudo evidenciar una reacción positiva por parte del usuario, al considerar los controles sugeridos que tratan de mitigar el riesgo existente en su entorno. Finalmente, planteamos trabajos a futuro que puedan abarcar la implementación y monitoreo del modelo propuesto.

Palabras Clave

Amazon ECHO, vulnerabilidad, sistemas de reconocimiento de voz, ISO/IEC27005:2011.

ABSTRACT

This research paper exposes the vulnerabilities to which we as users are exposed to use of voice recognition devices, in particular the case study of this paper: Amazon ECHO, Alexa. Even though the objective of this device is to provide daily activities to its users, they are no exempt from being manipulated by third parties, this violating not only the security of our homes, but also jeopardizing our privacy. With the preliminary study of vulnerabilities of these devices, a vulnerability security management model is proposed in order to ensure the user environment of these devices. The model is based on ISO-ICE 27005:2011, which provides guidelines for risk management through the identification of assets, threats, existing vulnerabilities, events and security controls to be applied. With the help of this norm, and with the user's opinion obtained through a series of semi-structured interviews, risk matrices and security controls are elaborated, in order to be adopted by them, and to ensure their current environment. On the other hand, in order to demonstrate a physical and logical vulnerability of interest due to its technical characteristics, we carry out an experiment, where an attack is reproduced through inaudible voice commands, thus clearly visualizing a type of attack to which users are exposed. As a conclusion, it was possible to demonstrate a positive reaction on the part of the user, when considering the suggested controls that try to mitigate the existing risk in their environment. Finally, we propound future works that may include the implementation and monitoring of the proposed model.

Keywords

Amazon ECHO, vulnerability, speech recognition system, ISO/IEC27005:2011

CAPÍTULO I

INTRODUCCIÓN

En las últimas décadas, gracias al acceso a Internet, el desarrollo de la Inteligencia Artificial, la interconectividad, y con el auge del Internet de las Cosas, (*Internet of Things* IoT, por sus siglas en inglés) han surgido una gran variedad de dispositivos inteligentes. Entre éstos dispositivos interconectados se destacan, aquellos que son capaces de interpretar y procesar comandos de voz, los cuales están siendo utilizados en ambientes cada vez más íntimos, como oficinas, hogares, lugares de descanso, entre otros. No cabe duda que el avance tecnológico que ha experimentado la sociedad con el IoT ha sido positivo, ayudando a establecer una comunicación más efectiva entre el hombre y este tipo de dispositivos inteligentes. Su función de alguna manera está enfocada en cumplir con una serie de tareas útiles, las cuales tratan de facilitar la vida de las personas que lo utilizan. Sin embargo, es evidente que el énfasis que se ha dado a estos dispositivos se basa en añadir y mejorar características y funcionalidades, antes que reforzar la seguridad en los mismos; dejando así brechas o puertas abiertas que pueden ser aprovechadas por individuos malintencionados o por errores involuntarios, comprometiendo la privacidad de quienes lo utilizan.

1.1 El Problema de Investigación

1.1.1 Planteamiento del Problema

Hoy en día, con el surgimiento del Internet de las Cosas, los usuarios prefieren utilizar aplicaciones que interactúan con ellos simulando a humanos, los cuales están siendo incorporados en sistemas telefónicos, aplicaciones web y asistentes personales virtuales conocidos como VPAs (*Virtual Personal Assistant*, por sus siglas en inglés). Tal es la

tendencia, que el reporte *Forecast Snapshot: VPA-Enabled Wireless Speakers, Worldwide*, indica que: “El gasto del usuario final para el mercado mundial de altavoces inalámbricos habilitados por el asistente personal virtual (VPA) alcanzará los $2,100 millones en 2020, frente a $ 360 millones en 2015. Para 2020, se pronostica que el 3,3 por ciento de los hogares habrá adoptado un altavoz inalámbrico habilitado para VPA” (Gartner, 2016).

Sin embargo, junto a este crecimiento nacen preocupaciones de seguridad y privacidad asociadas con el uso de estos dispositivos inteligentes, surgiendo varias preguntas tales como: ¿Estos dispositivos son seguros? ¿Están grabando nuestras conversaciones? ¿Nos están espiando? ¿A qué riesgos de seguridad estamos expuestos como usuario? Preguntas que necesitan respuestas claras con el fin de brindar tranquilidad a sus usuarios.

Entre los asistentes personales virtuales de reconocimiento de voz, está el popular Amazon ECHO, “Alexa”. Este dispositivo, de acuerdo a la retroalimentación dada en las páginas de revisiones de compra de Amazon (Johnson, 2017), estudios de seguridad realizados por consultores de MWR *InfoSecurity* (Barnes, 2017), así como también diversos estudios y documentos técnicos publicados, tales como lo realizado por Clinton, Cook, & Banik (2017), Roy, Hassanieh, and Choudhur (2017), Song and Mital (2017), Zang G., Yan, Ji, and Zhang T. (2017), Yang Hui & Leong (2017), han dejado en evidencia la existencia de brechas de seguridad. Las vulnerabilidades reportadas van desde físicas y lógicas en su uso, posibles violaciones en la privacidad de sus dueños, la no distinción entre voces, llevar a cabo compras no autorizadas por sus dueños, así como también la manipulación física de los dispositivos Amazon ECHO (Clinton, Cook, & Banik, 2017; Barnes, 2017).

Lo expuesto lleva a pensar, que a pesar de las consideraciones de diseño y los intentos de ofrecer un ambiente de uso seguro, el dispositivo de reconocimiento de voz Amazon ECHO presenta vulnerabilidades físicas y lógicas que demandan mayores esfuerzos en su

implementación de controles de seguridad. Además, desde el punto de vista de sus usuarios, es pertinente estudiar estas brechas de seguridad para asegurar su entorno.

1.1.1.1 Diagnóstico

A continuación, se detallan varios eventos que se caracterizan como síntomas detectados en el uso de los dispositivos de reconocimiento de voz Amazon ECHO:

1. En Texas, Estados Unidos, una niña de seis años, mientras jugaba con el dispositivo Amazon ECHO "Alexa" en su casa, le pidió comprarle una casa de muñecas. "Alexa" obedeció las órdenes de la niña y procedió con la compra. Adicionalmente y en referencia a esta compra, cientos de dispositivos fueron activados por equivocación por el famoso reportero Jim Patton de CW6, en San Diego California, el pasado enero del 2017, al transmitir la noticia de la niña, cuando dijo "Amo a esta pequeña niña diciendo 'Alexa cómprame una casa de muñecas'" (Bhattacharya, 2017). Todos los dispositivos Amazon ECHO de los televidentes procedieron a la compra de una casa de muñecas al escuchar al reportero.
2. En la página de Amazon sobre las revisiones de compra de los dispositivos Amazon ECHO; Johnson (2017), reportó el pasado 5 de febrero del 2017 una vulnerabilidad al darse cuenta que el dispositivo ECHO no solicita el modo de emparejamiento para su conexión con *bluetooth*. El cliente menciona en su comentario, que dos de sus vecinos pudieron establecer conexión con su dispositivo Amazon ECHO sin ninguna autorización, apareciendo como un dispositivo más de la lista *bluetooth*. Lo más preocupante es, que el dispositivo Amazon ECHO está plenamente vinculado con la cuenta de Amazon del cliente, lo que significa que podrían tener acceso a su cuenta sin ningún problema.
3. De acuerdo al estudio realizado por Barnes (2017), indica que los dispositivos Amazon Echo son vulnerables a ataques físicos, permitiendo al atacante conseguir acceso a la raíz del sistema operativo Linux e instalar un malware, sin dejar evidencia física de

manipulación del mismo. El consultor en seguridad procedió con su prueba y convirtió al dispositivo Amazon ECHO en un dispositivo de escucha afectando su funcionalidad. La vulnerabilidad fue confirmada para las ediciones 2015 y 2016 de Amazon Echo.

En resumen, los dispositivos de reconocimiento de voz, Amazon ECHO, presentan vulnerabilidades físicas y lógicas que exponen a sus usuarios a problemas de seguridad y privacidad. Los ejemplos expuestos aportan como evidencia de estas vulnerabilidades, por lo cual se realiza una revisión de varios estudios científicos publicados sobre pruebas de seguridad, métodos de análisis realizados a los dispositivos Amazon ECHO, así como también de la retroalimentación de los dueños de los dispositivos Amazon ECHO, sobre problemas presentados en su funcionamiento, todo esto, con el fin de proporcionar el diagnóstico respectivo.

Producto de la investigación "*Alexa are You listening*?" (Barnes, 2017), se han publicado varios artículos técnicos sobre las vulnerabilidades físicas encontradas en este tipo de dispositivos inteligentes. Se debe recordar, que la investigación demostró que los modelos Amazon Echo 2015-2016 son susceptibles de ser vulnerados físicamente, permitiendo al atacante tener acceso al sistema operativo Linux del dispositivo e instalar un malware, sin dejar evidencia de manipulación. Según el estudio, una vez que el malware ha sido instalado, éste permite a los atacantes tener acceso remoto persistente al dispositivo, permitiéndole transmitir audio de micrófono en vivo hacia servicios remotos, sin que esto altere el funcionamiento del dispositivo, y peor aún sin que sus dueños conozcan sobre esto. Pese a que la compañía Amazon solucionó el problema para los dispositivos Amazon Echo 2017, es importante tener presente lo que menciona la publicación "Las fallas de seguridad en Amazon Echo que permiten a los piratas informáticos obtener acceso a la raíz no pueden ser reparados" (Jay, 2017), referente a que la vulnerabilidad encontrada, no puede ser parchada usando actualizaciones de software,

lo que significa que los casi 11 millones de dispositivos ECHO 2015-2016, seguirán siendo vulnerables de por vida (Consumer Intelligence Research Partners, LLC. (CIRP), 2017).

Adicional a esto, Roy, Hassanieh, and Choudhur (2017), Song and Mital (2017), y Zang G., Yan, Ji, and Zhang T. (2017), proponen un ataque mediante la transmisión de ondas de ultrasonidos (inaudibles para humanos) para controlar los asistentes comunes como Siri, Google Home y Amazon ECHO "Alexa". Lo interesante de estos estudios es que los comandos de voz inyectados son inaudibles para los humanos, pero audibles para los dispositivos de reconocimiento de voz. Los resultados obtenidos arrojaron altas tasas de éxito en los dispositivos atacados.

Por otro lado, Yang Hui & Leong (2017), indica que los dispositivos como Amazon ECHO están en constante escucha, con el fin de tener un auto entrenamiento constante, de manera que la próxima vez, estos den una respuesta con apariencia más inteligente. Sin embargo, estos dispositivos podrían estar rastreando información sensible de sus dueños. Lo que puede significar que, durante este constante periodo de escucha, agentes externos pueden estar obteniendo información desde estos dispositivos, violando así la privacidad de sus usuarios.

Adicionalmente, en base a la recolección de información de la compañía Amazon sobre las revisiones de compra de los dispositivos Amazon ECHO, varios usuarios con compras verificadas, ponen de manifiesto problemas encontrados en el uso de los dispositivos. Tal es el caso del cliente Johnson (2017), quien reportó el pasado 5 de febrero del 2017 una vulnerabilidad (tal como se lo mencionó en el apartado anterior de detección de síntomas), al darse cuenta que el dispositivo ECHO no solicita el modo de emparejamiento para su conexión con *bluetooth*. De acuerdo a lo manifestado por el

cliente, no se ha dado solución por parte de la compañía Amazon, por lo que procedió a apagar el dispositivo hasta obtener una solución efectiva.

Cabe recalcar, que al tratarse de una tecnología emergente, varias investigaciones ponen de manifiesto, la falta de estudios profundos relacionados al tema de seguridad en este tipo de dispositivos inteligentes. Tal es el caso de Alhadlaq, Tang, Almaymoni, & Korolova (2017), el cual explica que es uno de los primeros que se lleva a cabo sobre la privacidad en el ecosistema de las funcionalidades de Alexa.

Es importante mencionar, que varios estudios identifican como pertinente la realización de trabajos futuros que traten una investigación más profunda sobre la seguridad de este tipo de dispositivos. Por ejemplo, lo manifestado por Haack, Severance, Wallace, & Wohlwend (2017) y Clinton *et al* (2017) que proponen llevar a cabo más estudios a profundidad.

De acuerdo a todo lo mencionado anteriormente, el diagnóstico es que los dispositivos de reconocimiento de voz Amazon ECHO, pese a contar con una arquitectura de seguridad, ésta presenta brechas, lo que le lleva a ser susceptible de sufrir vulnerabilidades tanto físicas como lógicas. A todo esto se debe incluir, la falta de estudios profundos de modelos de seguridad relacionados a este tipo de dispositivos inteligentes.

1.1.1.2 Pronóstico

Al existir continuas vulnerabilidades que enfrentan los dispositivos de voz Amazon ECHO, reportadas ya sea por la continua retroalimentación en las páginas de revisiones de compra verificadas, diferentes pruebas realizadas por empresas de seguridad, así como también por varios estudios de investigación; las mismas *continuarán* incrementándose y los usuarios *seguirán* siendo susceptibles a ataques en cualquier momento, comprometiendo así la seguridad y privacidad de los individuos que utilicen dichos dispositivos.

Los dispositivos Amazon ECHO, pueden conectarse e interactuar con otros dispositivos inteligentes, y el hecho de que los primeros sean susceptibles de vulneración *abrirá* la puerta para que estos otros puedan ser controlados por alguien más. En el caso de que no se solucione este inconveniente, lo siguiente que puede suceder será la manipulación de dichos dispositivos, con lo que se podría cometer robos y atracos. Por ejemplo: en el caso de dispositivos que controlan los seguros de puertas de acceso; sería como entregar las llaves de la casa a cualquier extraño.

No es desconocido que los dispositivos Amazon ECHO están relacionados con las cuentas de Amazon de sus dueños; teniendo a su alcance el manejo de información sensible de sus propietarios. Al existir la posibilidad de manipulación de los mismos, dicha información sería susceptible de vulneración y su privacidad se vería comprometida.

Al vender dispositivos poco seguros, y/o no confiables, la imagen de la empresa Amazon se podría verse afectada; por ende, podría disminuir sus ventas, y más grave aún, podría perder su credibilidad.

1.1.1.3 Control Pronóstico

Al tener plenamente identificados los puntos débiles de seguridad de los dispositivos Amazon ECHO, se busca que las próximas versiones de los mismos, sean más seguros; reduciendo así, la posibilidad de vulneración tanto física como lógica de los mismos.

Una vez que se cuente con dispositivos Amazon ECHO más seguros, la conexión con otros objetos inteligentes, como es el caso de aquellos que controlan los seguros de puertas de acceso podrá ser llevada a cabo sin mayores preocupaciones concernientes a las vulnerabilidades presentadas en los mismos.

Se busca ofrecer una visión nueva desde el punto de vista del usuario y cómo proteger su entorno de las vulnerabilidades que presentan los dispositivos Amazon ECHO. La intención es aportar académicamente a la discusión de cómo asegurar el IoT, con el fin de

que empresas como Amazon, puedan mejorar la arquitectura de seguridad de este tipo de dispositivos de forma integral. Sin dejar de lado las políticas de seguridad, los términos de uso y el tipo de servicio que ofrecen.

Si se cuenta con dispositivos Amazon ECHO confiables y seguros, los usuarios se sentirían a gusto utilizándolos, y recomendarían su uso a otros; con lo que las ventas de los mismos se incrementarán y por ende la imagen de la empresa Amazon mejoraría.

1.1.2 Formulación del Problema

Los dispositivos de reconocimiento de voz, Amazon ECHO (Alexa), presentan brechas de seguridad que afectan a cerca de 18 millones de personas, lo cual debería ser tomado en cuenta tanto por sus fabricantes como sus usuarios, con el fin de adoptar medidas para la gestión de riesgos que se derivan de las mismas.

1.1.2 Sistematización del Problema

Una vez planteado el problema objeto de esta investigación, es importante poder abordar al mismo desde diferentes perspectivas, con el fin de brindar una solución más completa. Es por tal motivo, que se plantean las preguntas a continuación:

- ¿Cómo conocer la problemática actual de seguridad en la que están inmersos los dispositivos de reconocimiento de voz Amazon ECHO?
- ¿Cómo conocer el funcionamiento de los dispositivos de reconocimiento de voz Amazon ECHO?
- ¿Cómo definir un grupo de controles que necesitan ser aplicados en el análisis de vulnerabilidades de los dispositivos de reconocimiento de voz Amazon ECHO, y así ser aplicado en el caso de estudio propuesto?
- ¿Cómo proceder con el grupo de controles definidos, para que estos puedan ser tomados en cuenta en el caso de estudio propuesto?

- ¿Cuál es el método científico que se puede emplear para demostrar vulnerabilidades en los dispositivos de reconocimiento de voz Amazon ECHO?

1.2 Objetivos

1.2.1 Objetivo General

Elaborar un modelo para el análisis de vulnerabilidades de dispositivos de reconocimiento de voz, en particular, para el dispositivo Amazon ECHO (Alexa), mediante el uso de la norma ISO/IEC 27005:2011 con el fin de que sus usuarios, conozcan las medidas que pueden adoptar ante estas brechas de seguridad, en entornos cotidianos.

1.2.2 Objetivos Específicos

- Realizar un estudio, estado del arte, sobre el ambiente en el que están inmersos los dispositivos de reconocimiento de voz, Amazon ECHO, para conocer la problemática actual de seguridad de los mismos.
- Realizar un análisis documental de la arquitectura lógica y física del sistema Amazon ECHO, para conocer el funcionamiento del dispositivo.
- Identificar el grupo de controles de la norma ISO/IEC 27005:2011, a ser aplicados en el análisis de vulnerabilidades derivado del estudio del estado del arte.
- Aplicar el grupo de controles previamente identificados en el análisis de vulnerabilidades para el caso de estudio propuesto.
- Realizar un experimento a través del cual, se logre reproducir un ataque con comandos de voz inaudibles, a los dispositivos de reconocimiento de voz, Amazon Echo (Alexa), basado en lo realizado por: Roy *et al*. (2017), Song and Mittal (2017), y Zhang *et al.* (2017).

1.3 Justificación

La popularización de la Internet, y el mejoramiento en su acceso, han contribuido a que la Internet de las Cosas (IoT) ya esté presente en nuestras vidas. Poco a poco consumidores están aprovechando las ventajas que ofrece esta tecnología emergente de interconectividad, y han empezado a dar cabida a dispositivos inteligentes interconectados entre sí en ambientes cada vez más íntimos, como son nuestros hogares. Dispositivos como línea blanca, luces, sensores, seguros de puertas de acceso, asistentes personales de reconocimiento de voz, entre otros; son aquellos con los que los usuarios pueden interactuar en el día a día. Es más, no se puede negar la utilidad que pueden proporcionar los dispositivos inteligentes y su impacto positivo sobre sus usuarios finales. De cierta forma, estos otorgan comodidad, ahorran tiempo, y pueden llegar a facilitar la vida de quienes lo utilizan. Sin embargo, permanece latente la preocupación de que sus consumidores puedan verse afectados en su privacidad y seguridad. Hoy en día, los fabricantes, pensando en las ventajas que pueden proporcionar a sus clientes, están ocupados en reforzar y aumentar nuevas tareas y funcionalidades a los dispositivos, muchas veces en detrimento de la seguridad. Si bien no se puede afirmar que los dispositivos inteligentes carecen de una arquitectura de seguridad, se debe mencionar, que la actual, no es lo suficientemente robusta como para prevenir ser vulnerada.

Dentro de esta gama de dispositivos inteligentes, se encuentran los dispositivos de reconocimiento de voz Amazon ECHO. Uno de los asistentes inteligentes más utilizados en la actualidad, con ventas sobre los 18 millones de unidades en los Estados Unidos desde su lanzamiento en noviembre del 2014 (Consumer Intelligence Research Partners, LLC., 2017). Dado que estos dispositivos utilizan información sensible sobre sus dueños, como son datos financieros y privados, la vulneración de los mismos sea esta lógica o física pondrían en riesgo la seguridad y privacidad de sus dueños.

1.3.1 Justificación Teórica

El presente proyecto pertenece a la categoría de Ingenierías y Tecnologías y se justifica teóricamente mediante diversos estudios de investigación, documentos técnicos publicados, así como también varias pruebas de seguridad realizadas por consultores de MWR *InfoSecurity* (2017), los cuales han dejado en evidencia la existencia de vulnerabilidades en la arquitectura física y lógica de los dispositivos Amazon ECHO.

Dentro de los estudios de investigación publicados, el realizado por Dewri, Nguyen, Chen, Lin, & Gupta (2017), menciona que los asistentes personales como Amazon ECHO son sensores ubicuos en un hogar conectado a IoT que constantemente monitorean y recolectan datos. Esto conlleva a la preocupación de seguridad sobre la posibilidad que hackers tomen el control en algún momento, sin que sus dueños se percaten de aquello.

De igual manera, de acuerdo a lo que indica Yang Hui & Leong (2017), los dispositivos de reconocimiento de voz, como Amazon ECHO están en constante escucha pese a no estar activados (mediante palabra de activación). Esto se da, según el estudio, con el fin de prepararse a sí mismos de una forma inteligente, y así poder responder de una mejor manera las solicitudes de los usuarios. Sin embargo, estos dispositivos podrían estar rastreando información sensible de sus dueños. Lo que puede significar que, durante este constante periodo de escucha, agentes externos puedan estar monitoreando estos dispositivos, obteniendo información y violando así la privacidad de sus usuarios.

Por último, algo importante que mencionan Yang Hui & Leong (2017) “Mientras los usuarios responden de manera entusiasta a esta nueva tecnología, ellos también necesitan estar seguros que sus dispositivos trabajen para ellos y no contra ellos”.

1.3.2 Justificación Metodológica

El trabajo de investigación utiliza la metodología de investigación documental, la cual permite levantar toda la información que requiere el uso y aplicación de la norma ISO/IEC

27005:2011 Tecnologías de la Información - Técnicas de Seguridad - Gestión de Riesgos de Seguridad de la Información, sobre la cual está basado el modelo de análisis de vulnerabilidades propuesto. El levantamiento de la información a través de la técnica documental, se lo lleva a cabo por medio de la revisión de papers, libros, tesis, y documentos técnicos, para así poder suplir lo que requiere la norma seleccionada.

Adicional a esto, se utilizan otras técnicas como son las entrevistas semiestructuradas, las mismas que a través de la opinión emitida por un grupo de expertos, sirven para poder levantar información, y así poder validar el modelo propuesto.

1.3.3 Justificación Práctica

La norma ISO/IEC 27005:2011 Tecnologías de la Información - Técnicas de Seguridad - Gestión de Riesgos de Seguridad de la Información define una tecnología madura que se usa ampliamente en la práctica de organizaciones. El modelo de seguridad planteado hereda la fortaleza de la norma, con la diferencia que utiliza como punto de referencia la realidad del usuario de los dispositivos de voz Amazon ECHO, por lo que, este modelo al ser puesto en práctica por cualquier usuario de estos dispositivos, permitirá asegurar su entorno. Adicional a esto, el modelo sirve como base para el desarrollo de otros modelos similares, o de aquellos que tengan un mayor alcance de seguimiento y control.

1.3.4 Justificación Legal

El presente trabajo de investigación, presenta un caso de estudio a ser realizado en Ecuador; y se justifica de forma legal en base a lo que menciona la Constitución del Ecuador, en su Capítulo sexto. Derechos de libertad Art. 66.- Numeral 19.

> El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente

> protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. (Asamblea Constituyente, 2015, p.49)

Y también lo que establece el Código Orgánico Integral Penal, COIP, en su sección Tercera, Delitos contra la seguridad de los activos de los sistemas de información y comunicación. Artículo 230.- Interceptación ilegal de datos.-

> Será sancionada con pena privativa de libertad de tres a cinco años: "1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible." (Asamblea Nacional del Ecuador, 2014, p.37)

1.3.5 Relevancia Social

Este proyecto contribuirá a la sociedad para que los consumidores puedan conocer los riesgos a los que están expuestos al utilizar dispositivos inteligentes de reconocimiento de voz con los que interactúan día a día en sus ambientes cotidianos. Muchas veces, las personas adquieren dispositivos inteligentes, sea esto por moda, por novelería o simplemente por curiosidad; sin saber en realidad las implicaciones del uso del mismo, y lo que es más grave aún, desconociendo sus derechos de privacidad y seguridad. A esto se debe añadir la poca cultura de seguridad que tiene el público en general.

Es más, la sociedad necesita saber que tan expuestos están con el uso de estos dispositivos, que tan seguros son, qué información es la que está siendo recolectada a través de estos, y cual información sobre sus clientes es permitida recolectar por las compañías, así como también que pueden hacer con la misma. Si el estudio no se lleva a cabo, los dueños seguirán utilizando e interactuando con este tipo de dispositivos, sin tomar ninguna medida de control y estarán expuestos a que se violen sus derechos de

privacidad y seguridad en su ambiente cotidiano sin que ellos, ni siquiera se percaten de aquello.

1.4 Marco Teórico

Para poder entender de mejor manera el ambiente en el cual se desenvuelven los dispositivos inteligentes de reconocimiento de voz Amazon ECHO, así como el uso de las normas ISO/IEC 27005, 27001 y 27002 para el análisis propuesto, es necesario abordar varios conceptos relacionados. Es por esto que este apartado detalla a los dispositivos de reconocimiento de voz dentro del contexto de la Internet de las Cosas (IoT) y aborda los aspectos más importantes de las normas ISO previamente mencionadas.

Internet de las Cosas

El origen de los objetos conectados no puede ser considerado como algo reciente, puesto que sus inicios se remontan a estudios tecnológicos realizados en el siglo XIX, con los primeros experimentos de telemetría y con los pensamientos y escritos de científicos como Nikola Tesla y Alan Turing, los cuales anticiparon el sorprendente crecimiento de la conectividad global. Tesla, uno de los padres de las comunicaciones inalámbricas, manifestó en una entrevista a la revista *Colliers* (como se cita en Cendón, 2017):

> Cuando lo inalámbrico esté perfectamente desarrollado, el planeta entero se convertirá en un gran cerebro, que de hecho ya lo es, con todas las cosas siendo partículas de un todo real y rítmico… y los instrumentos que usaremos para ellos serán increíblemente sencillos comparados con nuestros teléfonos actuales. Un hombre podrá llevar uno en su bolsillo.

Este gran cerebro al que hace referencia Tesla, conlleva en primer lugar a la interconexión de todo y a la evolución que hemos tenido desde el uso de ordenadores personales, teléfonos inteligentes, hasta llegar a ese “gran cerebro” que hoy en día es el Internet. Pero no fue hasta los años noventa donde la Internet tuvo su expansión definitiva.

Y con la utilización de protocolos como el TCP/IP, permitieron que la red que en un inicio fue creada únicamente para uso militar, la conocida ARPANET (Cendón, 2017), se convirtiera en Internet; dando paso a un nuevo concepto de interconectividad. Fue a partir de este momento, en el que la idea de conectar objetos a esta "Red de Redes" comenzó a tomar forma. Sin embargo, pese a tener una manera diferente de entender las redes, toda la comunicación estaba basada en una estructura física de cables, que de alguna manera ensombreció la idea de la conexión de objetos. Sin embargo, a inicios del siglo XXI, con el surgimiento de la conectividad inalámbrica a través de red celular o *Wi-Fi*, se pudo evidenciar el surgimiento y crecimiento de los objetos conectados.

Antes de poder referirse a los objetos conectados, es necesario conocer sobre la Internet de las Cosas (IoT), la cual es una red que usando la infraestructura de comunicación existente, permite la conexión de varios objetos inteligentes. Es necesario indicar, que las dos tecnologías base del IoT son: la identificación por radiofrecuencia (RFID), y las redes de sensores inalámbricos. A través de la tecnología RFID, se puede identificar de manera única a un objeto, con el fin de obtener información de este, así como también de su entorno; esto se logra a través de la etiqueta RFID que lleva el objeto. En lo referente a los sensores, éstos son aquellos que permitirán percibir las características físicas del entorno en el que se encuentra el dispositivo; con lo que son capaces de recoger toda la información de su entorno.

Una vez conocido el entorno del IoT, se puede hablar acerca de los objetos conectados, los cuales no son simplemente dispositivos, sino objetos inteligentes. Objetos que poseen software, circuitos, sensores y sistemas de red que les permiten monitorear, recolectar y enviar información a la Internet, así como también interactuar con sus usuarios. Los primeros dispositivos inteligentes datan de los años 70, con la aparición de los cajeros automáticos conocidos como ATM; y su evolución ha sido tan rápida que hoy

en día se cuenta con un amplio rango de los mismos, y que son parte de la Internet de las Cosas (Clinton *et al*., 2017).

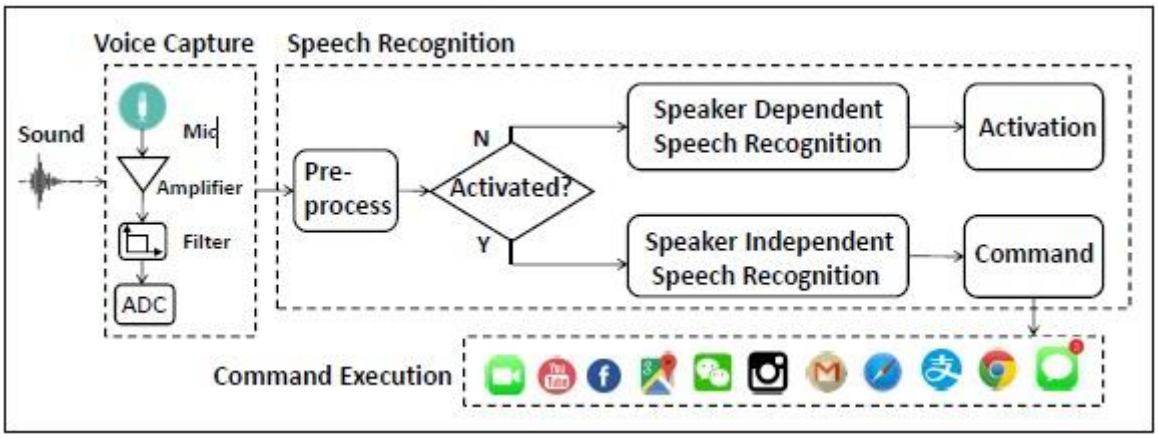
Adicional a esto, un dato interesante que se menciona es que "durante el 2008, el número de objetos conectados a Internet excedió el número de personas en la tierra, y está estimado que para el año 2020 existirán más de 50 billones de dispositivos inteligentes" (Clinton *et al*., 2017).

Sistemas de Reconocimiento de Voz

Dentro de la gama de los dispositivos inteligentes del IoT, están aquellos que utilizan sistemas de voz controlable. Un sistema de este tipo, consiste básicamente en tres subsistemas: captura de voz, reconocimiento de voz y ejecución de comandos. "El subsistema de captura de voz graba voces ambientales, que se amplifican, filtran y digitalizan, antes de pasarlas a los sistemas de reconocimiento de voz" (Zhang *et al*., 2017).

La figura 1 muestra la arquitectura de un sistema de voz controlable, la cual toma como entrada comandos de voz para la respectiva ejecución de comandos.

Figura 1. Arquitectura de un Sistema de Voz Controlable (Zhang *et al*., 2017)



Según Bolt (1980), el reconocimiento de comandos de voz tiene sus inicios a finales de los años 70 a través del proyecto denominado "*put that there*", en el cual, los comandos son utilizados para interactuar con una computadora.

"Un sistema de reconocimiento de voz es una herramienta computacional capaz de procesar la señal de voz emitida por el usuario y reconocer la información contenida en ella, traduciéndose luego a texto o comandos que ejecuten una acción sobre un proceso" (Keimel, 2016).

Por lo que se puede decir que, el sistema de reconocimiento de voz trabaja en dos fases que son la activación y el reconocimiento. Durante la primera fase, el sistema espera el ser activado. Un ejemplo de esta activación es la palabra "Alexa", para el caso de los dispositivos Amazon ECHO. Y en la segunda fase, el sistema utiliza algoritmos de reconocimiento de voz para reconocer las palabras de activación (Zhang *et al*., 2017).

Los asistentes de voz como es el caso del dispositivo Amazon Echo están basados en el aprendizaje de máquina. La idea detrás del aprendizaje de máquina es mejorar la interacción existente entre este tipo de dispositivo y sus dueños mediante su uso; es decir, mientras más sea utilizado el dispositivo, más aprenderá y se adaptará al vocabulario empleado, y a las preferencias de sus dueños.

Amazon ECHO, Alexa

El dispositivo de reconocimiento de voz Amazon ECHO, es uno de los productos estrella de la empresa Amazon Inc., la cual es una de las compañías más grandes de compras en línea a nivel mundial. Fundada en 1995, por Jeff Bezos, comenzó con la venta de libros en línea, a través de su conocida página web, convirtiéndose en uno de los mayores minoristas en línea del planeta.

Alexa es el cerebro de los dispositivos Amazon ECHO en sus diferentes versiones ECHO: *Dot, Tap, Show y Look*. Se trata de un dispositivo de reconocimiento de voz el

cual está implementado en la nube, cuya característica principal es su activación al llamado de “Alexa” (la cual es la palabra de activación) para responder preguntas, reproducir música, controlar dispositivos inteligentes, hacer llamadas, envío de mensajes y mucho más. Sin embargo, pese a toda esta gama de nuevas características, los dispositivos ECHO siguen manteniendo una limitante: el lenguaje, ya que solo reconocen el idioma inglés. Por otro lado, independientemente del idioma que se maneje, surgen varias preguntas por parte de los usuarios de Alexa, referentes al tema de seguridad. ¿Qué tan seguro es tener Alexa en casa? ¿Me están espiando? ¿Puedo ser víctima de un fraude? Preguntas y preocupaciones válidas que son necesarias analizarlas a través de un estudio de investigación.

A todo esto, se debe añadir, que no cabe duda de la gran popularidad y aceptación que tiene hoy en día esta tecnología inteligente como lo es el IoT; sin embargo, a la par de su crecimiento, han surgido varias preocupaciones referentes a la seguridad en este tipo de tecnología, los cuales han sido plasmados en varios estudios de investigación científica. De acuerdo a lo mencionado en el estudio “Seguridad de la Internet de las Cosas”, “La seguridad, en su aspecto más técnico, se puede definir como aquellas actividades enfocadas a proteger un determinado dispositivo o servicio, así como todo aquello con lo que interactúa e intercambia con otros dispositivos o servicios, ya sea información, datos, señales, etc.”. Utilizando como base la anterior definición, la seguridad de IoT se podría definir como aquellas actividades encaminadas a la protección de los objetos y sus comunicaciones o interacciones con otros objetos. Es necesario tener presente este concepto, con el fin de que todos aquellos individuos que están interactuando con estos dispositivos inteligentes a diario, en ambientes cada vez más íntimos, estén conscientes de los riesgos que su uso conlleva el usarlos.

Estándares de Seguridad

Antes de abordar el tema de los estándares de seguridad, es necesario saber que la información es un recurso de gran valor para las empresas, el cual necesita ser gestionado de manera adecuada; con el fin de que aporte de manera positiva a las organizaciones. Y es la seguridad de la información la que se encarga de dicha gestión, a través de un conjunto de normas, técnicas, procedimientos y estrategias, con el fin de mantener este valioso activo protegido, tratando de minimizar amenazas existentes, y riesgos continuos garantizando los principios de confidencialidad, disponibilidad e integridad del activo conocido como información (Universidad Nacional de Luján, 2017).

Adicional a esto, es importante tener claro varios conceptos que van a ser utilizados dentro de la seguridad de la información. Ya que el modelo para el análisis de vulnerabilidades planteado en el presente trabajo se basa en la norma ISO/IEC 27005:2011. Los conceptos a continuación son expuestos desde el punto de vista de la seguridad.

Amenaza *(Threat):* "Una amenaza tiene el potencial de dañar a los activos como lo son la información, procesos y sistemas y por lo tanto organizaciones. Las amenazas pueden ser de origen natural o humano, y pueden ser accidentales o deliberadas" (ISO/IEC 27005, 2011). Por lo que una amenaza representa una situación potencial que supone un daño a los activos.

Vulnerabilidad *(Vulnerability):* "Las vulnerabilidades pueden ser explotadas por las amenazas para causar daño a los activos o la organización. La presencia de una vulnerabilidad no causa daño en sí misma, ya que debe haber una amenaza presente para explotarla" (ISO/IEC 27005, 2011). Con lo que se puede decir que una vulnerabilidad es una debilidad de un bien o de un control, a la cual se la puede ver como una característica negativa del bien, la misma que puede ser aprovechada por una amenaza.

Riesgo *(Risk):* "La materialización de una amenaza que aprovecha una vulnerabilidad y que expone a las organizaciones y sus sistemas informáticos es lo que se conoce como riesgo" (Prandini & Pallero, 2013). La norma ISO/IEC 27002 (2013), lo define como la probabilidad de ocurrencia de un determinado hecho y sus consecuencias (el impacto).

La figura 2 muestra la relación entre los tres conceptos antes descritos.

Figura 2. Amenaza – Vulnerabilidad – Riesgo (Prandini & Pallero, 2013)

Una vez abordados varios de los conceptos relacionados con la seguridad, es tiempo de mencionar la existencia de normas, estándares o guías que pueden ser utilizadas para la aplicación de controles en un sistema de seguridad. Estas normas forman parte de los estándares internacionales publicados por la Organización Internacional de Estandarización (ISO, por sus siglas en inglés) y la Comisión Electrotécnica Internacional (IEC). ISO es una organización internacional no gubernamental e independiente creada para "facilitar la coordinación internacional y la unificación de las normas industriales"(ISO). Cuenta con miembros de 161 países y cuenta con 779 comités y subcomités técnicos que se encargan del desarrollo de estándares. Los estándares ISO

aseguran que los servicios, productos sean seguros, confiables y de buena calidad, los cuales son creados para las personas que los necesitan (ISO). Es así como el presente trabajo utiliza las siguientes normas:

ISO/IEC 27005:2011, Tecnologías de la Información – Técnicas de Seguridad - Gestión de Riesgos de Seguridad de la Información (ISO/IEC 27005, 2011).

La norma ISO/IEC 27005:2011, establece las directrices para la gestión de riesgos de seguridad; la misma que puede ser aplicada a diferentes tipos de organizaciones que pretendan gestionar todos aquellos riesgos, que de alguna manera puedan comprometer la seguridad de la información de la organización. Esta norma, da soporte a los conceptos especificados en la norma ISO/IEC 27001:2013.

ISO/IEC 27001:2013, Tecnologías de la Información – Técnicas de Seguridad – Sistema de Gestión de Seguridad de la Información – Requisitos (ISO/IEC 27001, 2013).

La norma ISO/IEC27001:2013, "especifica los requerimientos para el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora de un SGSI debidamente formalizado" (Valencia-Duque & Orozco-Alzate, 2017). El Sistema de Gestión de Seguridad de la Información (SGSI por sus siglas en inglés), es la base sobre la cual se centra la ISO27001. Cuenta con 14 dominios y 114 controles, la misma que es utilizada como guía para la identificación de amenazas, vulnerabilidades y otros elementos que servirán para la Gestión de Riesgos.

ISO/IEC 27002:2013, Tecnologías de la Información – Técnicas de Seguridad – Código de Prácticas para Controles de Seguridad de la Información (ISO/IEC 27002, 2013).

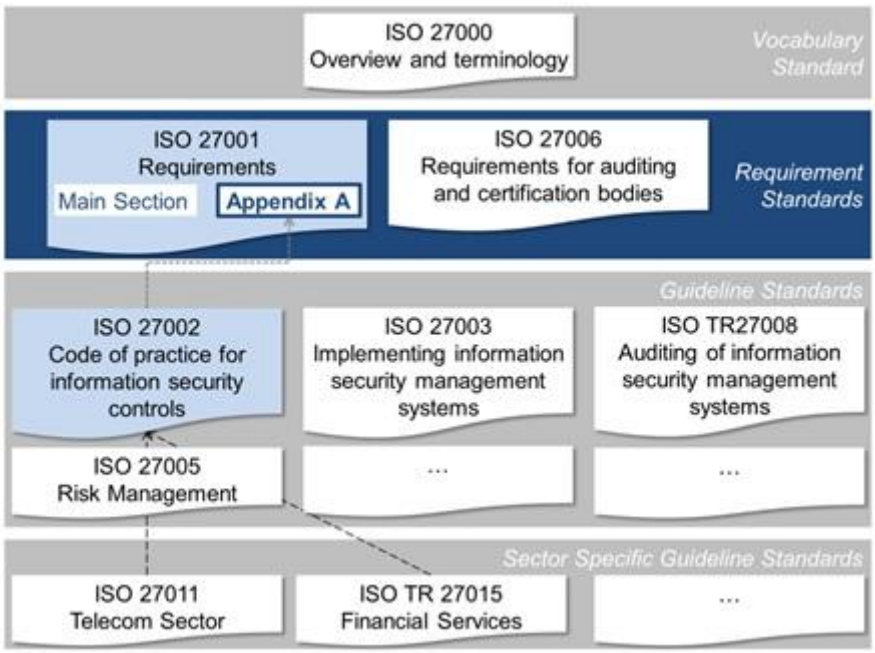
La norma ISO/IEC27002:2013 proporciona la guía para la identificación y aplicación de controles de seguridad, para la mitigación de los riegos encontrados, una vez que han

sido identificadas las amenazas y vulnerabilidades que presentan un escenario de riesgo. Cuenta con 14 dominios, 35 objetos de control y 114 controles.

Por lo que, el conocimiento de los conceptos, modelos, procesos, y terminologías existentes en las norma ISO27001 ayudará al establecimiento, implementación y mejoramiento de los controles de la ISO27002, tal cual lo muestra la figura 3. Es decir que el trabajo en conjunto de éstas dos, proporcionará el debido soporte que ayudará a una mejor comprensión de la norma ISO/IEC27005, como lo muestra la figura 4.

Figura 3. Relación entre ISO/IEC27001 e ISO/IEC27002 (PECB, 2016)

Figura 4. Relación normas ISO27001, ISO27002 e ISO27005 (Klaus, 2014)



1.5 Estado del Arte

Amazon “Alexa” es un asistente personal inteligente y el cerebro de los dispositivos Amazon Echo en sus diferentes versiones *ECHO, DOT, TAP, Echo Show* y el nuevo *Echo Look*. Se trata de un dispositivo de reconocimiento de voz el cual está implementado en la nube, cuya característica principal es su activación al llamado de “Alexa” (palabra clave aceptada por los parlantes independientes que son parte del dispositivo), el cual una vez que ha reconocido el comando, procede a la ejecución de una gran variedad de tareas, tales como: dar información en vivo sobre el clima y tráfico, reproducir música, controlar dispositivos inteligentes del hogar, ordenar productos desde el almacén online de Amazon, interacción con aplicaciones de terceros, entre otros (Amazon, 2017).

Figura 5. Dispositivos Amazon ECHO (Amazon, 2017)

De acuerdo al estudio “*Security Analysis of the Amazon Echo*” (Haack *et al*., 2017), dentro de los componentes que conforman la arquitectura de los dispositivos Amazon ECHO están:

ECHO, es el dispositivo que provee la interfaz para el usuario que a través de comandos de voz realiza preguntas y Echo responde. ECHO está siempre en escucha, y

sólo responderá cuando escuche la palabra de activación “Alexa” transmitiendo el audio subsecuente al servicio de nube Alexa.

Servicio en la Nube de Alexa, recibe el audio desde los dispositivos ECHO y es el responsable de manejar el reconocimiento de voz y asociar los comandos de voz con los “*intents*” (el término *intent* representa una acción que es realizada ante un pedido del usuario) y la información asociada. Basado en determinado *intent*, el servicio de nube Alexa delega el comando al servidor de *Skills*, sea este operado por Amazon o por terceros. Una vez que el servicio de nube de Alexa recibe una respuesta por parte del servidor de *Skills*, este le trae a los dispositivos ECHO.

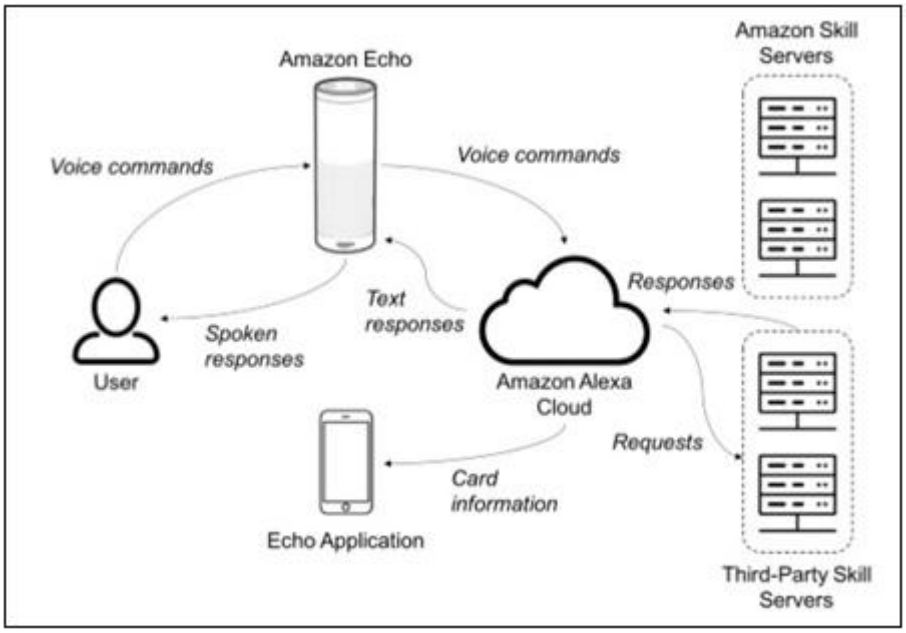
Servidores de Skills de Amazon, los *Skills* son las tareas esenciales que el servicio de Alexa puede dar a un usuario, como por ejemplo el chequeo del tráfico, clima, etc. Algunas de estas tareas son desarrolladas para todos los usuarios de Amazon Alexa y son manejadas en los servidores de *Skills* de Amazon.

Servidores de Skills de terceros, todas aquellas funcionalidades o *Skills* que son implementadas por desarrolladores externos (no de la compañía Amazon), serán manejados en estos servidores.

Aplicación Echo, es la aplicación móvil que Amazon ofrece para que los usuarios puedan realizar ajustes a la configuración de Alexa. A través de esta, será posible visualizar históricos de las iteraciones que se han realizado con el dispositivo.

La figura 6 muestra los componentes de la arquitectura de los dispositivos Amazon Echo antes mencionados.

Figura 6. Sistema de Arquitectura de los dispositivos Amazon Echo. (Haack *et al*., 2017)



Adicionalmente, el estudio identifica cuatro categorías de actores con sus respectivas acciones. Usuarios primarios, cuya cuenta es la primera registrada en el dispositivo ECHO y son aquellos los que tienen el control de uso del dispositivo; usuarios secundarios, que son registrados en el dispositivo siempre y cuando el usuario primario lo permita; otros usuarios, los cuales pueden interactuar con el dispositivo ECHO sin registrar sus cuentas en este; y los afiliados de Amazon, que son todos aquellos que trabajan para Amazon y que pueden tener acceso a información propietaria; sin embargo, estos actores no deberían tener acceso a información sensible de los usuarios de ECHO. También da a conocer una política ideal para los dispositivos Amazon Echo focalizada en confidencialidad, integridad y disponibilidad.

Es más, el estudio realiza pruebas de seguridad basadas en 4 canales: sonido, red, API y *Skills* de terceros. Se realizó un trabajo previo en el que pudieron encaminar el dispositivo a través de un proxy y poder ver el tráfico generado por Echo, del cual se puede mencionar que la mayor parte del tráfico viene en forma de petición HTTPS el cual está encriptado, pero notando también la generación de algunas solicitudes HTTP.

En referencia al ataque basado en voz, el primer intento en el estudio fue el tratar de hablar en diferentes idiomas y acentos. “Alexa” no entiende otros idiomas que no sea inglés y reconoce acentos británicos y australianos. Concluyen indicando un aspecto negativo en la disponibilidad del dispositivo, puesto que es limitado a angloparlantes.

El segundo intento, hace referencia a la respuesta de comandos en forma indirecta ya sea por grabaciones, mensajes de voz o generados por computadora. Con esta prueba se evidenció que “Alexa” puede ser influenciada por personas externas, es decir que no estén dentro de casa. Adicionalmente, se pudo evidenciar que ECHO no tiene diferenciación de voz o protección contra discurso no humano o repetitivo. Lo que hace que sea más difícil la distinción entre los usuarios primarios, secundarios y otros. Sin embargo, una forma que el dispositivo tiene para autorizar tareas restringidas es el ingreso de un pin de 4 dígitos. Sin embargo, se encontró que el valor por default en el dispositivo para la realización de compras no solicita el pin. Lo que compromete la integridad, al permitir que usuarios puedan realizar órdenes de compras desde otras cuentas de usuarios.

En referencia a los ataques de red, el estudio utiliza la herramienta *Wireshark* para interceptar tráfico de red. La dirección MAC del dispositivo ECHO fue fácilmente recuperada desde la aplicación de Alexa. Se pudo capturar un gran número de paquetes enviados entre el dispositivo ECHO y otras direcciones. Lo notable de esta prueba es que se evidenció un gran número de paquetes transferidos cuando se interactuaba con el dispositivo ECHO, pero también se enviaron paquetes sin interactuar con el dispositivo. Lo que puede significar que estas transmisiones son producto de actualizaciones en el firmware, lo cual resulta motivo para futuras investigaciones.

Por otro lado, la publicación “*Alexa, Can I trust You*?” (Chung *et al*., 2017), pone de manifiesto que, el llevar a cabo mejores pruebas de diagnóstico del ecosistema de los

asistentes virtuales inteligentes (IVA por sus siglas en inglés), puede revelar vulnerabilidades existentes, obteniendo así sistemas confiables. La publicación lleva a cabo varios análisis enfocados en los siguientes puntos: nube-nativa, análisis de paquetes, pruebas de comandos de voz, análisis de aplicaciones y análisis del firmware. Una de las pruebas realizadas, se enfocó en un ataque de escuchas en el ecosistema de un IVA. Para este tipo de ataque, se utilizaron herramientas de intercepción de paquetes para analizar las peticiones y respuestas HTTPS, y así determinar cuáles *APIs* son usadas para enviar y recibir información de un IVA. Se pudo evidenciar que en la comunicación entre el dispositivo inteligente y los servicios host de la nube, no todo el tráfico es transmitido sobre un protocolo seguro. También se evidenció que la imagen de datos del firmware puede ser transferida sobre paquetes no encriptados, exponiendo de esta manera, al sistema a ataques de un hombre en el medio (*Man-in-the-Middle Attack*). Adicional a esto, la publicación hace referencia a lo difícil que le resulta al sistema de este tipo de dispositivos, distinguir entre voces similares; lo que puede engañar al dispositivo cuando otro usuario que no es el dueño solicite realizar algo con el mismo. La publicación concluye en que a medida que este tipo de asistentes virtuales se vuelven más inteligentes es necesario entender la seguridad y privacidad de esta tecnología emergente, puesto que, con mejores pruebas de diagnóstico, se podrán lograr sistemas más confiables.

Por otra parte, en referencia a las vulnerabilidades físicas que pueden tener los dispositivos Amazon ECHO, de acuerdo a la investigación realizada por la compañía de seguridad MWR *InfoSecurity*, a través de la prueba de laboratorio realizada por Barnes (2017), se demostró que los modelos Amazon Echo 2015-2016 son susceptibles de ser vulnerados físicamente, permitiendo al atacante tener acceso al sistema operativo Linux del dispositivo e instalar un malware, sin dejar evidencia de manipulación. El estudio indica también, que una vez que el malware ha sido instalado, éste permite a los atacantes

tener acceso remoto persistente al dispositivo, permitiéndole transmitir audio de micrófono en vivo hacia servicios remotos, sin que esto altere el funcionamiento del dispositivo, y peor sin que sus dueños conozcan sobre esto. Pese a que la compañía Amazon solucionó el problema para los dispositivos Amazon Echo 2017, el estudio concluye en que es necesario tener presente a los dispositivos Amazon ECHO (2015-2016) que todavía están en el mercado y que siguen siendo susceptibles de este tipo de ataque.

Adicional a este tipo de ataques físicos, el documento técnico "*A Survey of Various Methods for Analyzing the Amazon Echo*" (Clinton *et al*., 2017), enfocado en analizar el modelo de privacidad de los dispositivos Amazon ECHO, pone de manifiesto diferentes enfoques de ataques físicos que se pueden realizar en los dispositivos Amazon ECHO, mediante los cuales se podría tener un mayor acceso al sistema de archivos del dispositivo Amazon ECHO. Se identifican tres enfoques de ataques físicos: primero, la conexión de una tarjeta SD externa a través del circuito integrado (*pinout*) del dispositivo, en donde se consiguió cargar la tarjeta con un sistema operativo y arrancar el mismo. Segundo, el acceso a través del estilo raíz *eMMC* como se lo ha realizado antes con *FireTV* (producto de Amazon); sin embargo, esta prueba fue diferida para futuras investigaciones, y tercero, mediante el uso de una herramienta de depuración llamada *Joint Test Action Group* (JTAG por sus siglas en inglés), idea tomada de Finlayson (2017), quien indica en una publicación en su cuenta de *twitter* sobre la posibilidad de tener acceso a depuración y características de programación normalmente no disponibles en los dispositivos Amazon ECHO; sin embargo, los investigadores de este estudio no tuvieron la posibilidad de comprar esta herramienta, por lo que se lo difirió para un trabajo futuro prometedor que permitirá tener un acceso completo al dispositivo. Por todo lo anteriormente expuesto, el estudio concluye que los dispositivos Amazon ECHO son vulnerables a ataques físicos

incluyendo posibles comandos de inyección a través del puerto UART y vulnerable a denegación de servicios (DoS, por sus siglas en inglés) durante el arranque. Sin embargo, el estudio también señala que la seguridad en general de este dispositivo es relativamente fuerte comparada con otros dispositivos sujetos de investigaciones anteriores.

Por otro lado, en referencia a las aplicaciones realizadas por terceros para los dispositivos Amazon ECHO, el estudio "*Privacy in the Amazon Alexa Skills Ecosystem*" (Alhadlaq *et al*., 2017), menciona que es uno de los primeros estudios que se lleva a cabo sobre la privacidad en el ecosistema de las funcionalidades de Alexa, conocidos como "Alexa *Skills Kit*". Este servicio está disponible desde el 2015, y actualmente existen más de 10,000 *Skills* disponibles; y lo que pretende es permitir a desarrolladores crear una serie de funcionalidades manejadas por comandos de voz (llamadas *Skills*) para que puedan ser utilizadas por Alexa. El dispositivo inteligente Amazon ECHO actúa como un agente entre el usuario y el *backend* basado en la nube donde se encuentra el *Skill*. Cuando el *Skill* es invocado, al usuario no se le da a conocer sobre las políticas de seguridad, ni tampoco se le pregunta si está de acuerdo con los términos de uso o políticas de privacidad. En caso de que el usuario desee conocer sobre estas, deberá acceder a ellas manualmente.

El estudio está enfocado en las elecciones de privacidad llevadas a cabo por Amazon al establecer el ecosistema *Skills*, y las prácticas de privacidad actuales de los desarrolladores dentro de este. El estudio analizó las políticas de privacidad de todos los *Alexa Skills* y encontró que el 75% de estos no tienen ninguna. Adicionalmente, de las 2,860 *Skills* que tienen un enlace de política de privacidad, 269 no son alcanzables debido errores HTTP, acceso denegado o tiempo de espera. A esto se debe añadir que 35 de los enlaces de políticas de privacidad no conducen a información relacionada con esta, sino a información de la página web del desarrollador. Esto habla que del porcentaje de sitios

que tienen que tienen problemas de acceso, el 3.5% requieren un enlace a la cuenta de Amazon.

Es más, se encontró que la empresa Amazon no requiere a los desarrolladores de los *Skills* solicitar permisos que incluyan políticas de seguridad a menos que el *Skill* solicite un enlace con la cuenta de Amazon. Es por esto que no todos los *Skills* tienen políticas de privacidad implementadas. Algo interesante de los resultados mostrados en este estudio, es el hecho de que los *Skills* más populares y que tienen mejor calificación, son los que menos políticas de seguridad tienen registradas. Los resultados obtenidos en este estudio, indican que la actitud frente a las políticas de privacidad por parte de Amazon y los desarrolladores de *Skills* no es la más adecuada.

Adicional a esto, el estudio "A *Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic*" (Apthorpe, Reisman, & Feamster, 2017), desarrolla una estrategia en el que demuestra que un observador pasivo de red puede inferir en el comportamiento del consumidor a través de la captación de tráfico de los dispositivos del IoT. Entre los dispositivos que se escogieron para ser esta prueba está el dispositivo Amazon Echo. Lo interesante del proyecto es que se crea un laboratorio simulando una casa inteligente; utilizando un dispositivo *Raspberry* Pi 3 como enrutador para poder capturar el tráfico de los dispositivos. Los resultados indicaron que el tráfico generado de todos los dispositivos examinados revelan las actividades de los usuarios, y que pese a que los datos se encuentren encriptados, esto no garantiza la protección de privacidad en los hogares inteligentes.

Por otro lado, el estudio "*Inaudible Voice Commands*" (Song & Mittal, 2017), pone de manifiesto, que dado el continuo uso de comandos de voz para la iteración con los dispositivos del IoT, es posible realizar ataques a través de estos comandos. El estudio

propone un método de ataque novedoso, puesto que lo realiza mediante la transmisión de ultrasonidos inaudibles para los humanos (frecuencias mayores a 20kHz), y así controlar a los asistentes de reconocimiento comunes como *Siri, Google Home* y Amazon Echo "Alexa", sin que sus dueños se percaten de aquello, y sin que sea necesaria la modificación física de los mismos. El ataque explota dos características esenciales de estos dispositivos: sus micrófonos no lineales (para el lector interesado, el Anexo 1 desarrolla este tema a mayor profundidad) y la escucha continua.

El estudio también menciona un trabajo similar realizado en "*BackDoor: Making Microphones Hear Inaudible Sounds*" (Roy *et al*., 2017), en el cual aprovechan la no linealidad de los micrófonos, para llevar a cabo información inaudible acústica y vulnerar micrófonos espías. Sin embargo, el método utilizado necesita de procedimientos de codificación adicionales, para llevar a cabo su objetivo. Por lo que el estudio de Song and Mittal (2017) propone algo diferente, donde el micrófono no necesita ser alterado físicamente y sus salidas son interpretadas como comandos de voz. El estudio concluye indicando, que a través de la distorsión de intermodulación y la modulación de amplitud, el ataque a través de comandos de voz es inaudible, y los resultados obtenidos arrojan altas tasas de éxito en los dispositivos Amazon ECHO a más de dos metros de distancia.

Adicional a estos dos estudios, se cuenta también con "*DophinAttack: Inaudible Voice Commands*" (Zhang *et al*., 2017), estudio que diseña un ataque denominado "DolphinAttack", el cual modula comandos de voz inaudibles a través de portadores ultrasónicos, para lograr inaudibilidad. Y aprovechando la no linealidad de los circuitos en los micrófonos, en la que los comandos de audio modulados en baja frecuencia, pueden ser de-modulados satisfactoriamente, y más importante aún, pueden ser reconocidos por los sistemas de reconocimiento de voz. El estudio valida "*DolphinAttack*", en populares sistemas de reconocimiento de voz como *Siri, Google Now, Samsung S Voice, Huawei*

HiVoice, Cortana y Alexa, inyectando una serie de comandos inaudibles; logrando activar *Siri* para que inicie una llamada de *FaceTime* en un *iPhone*, activar *Google Now* para cambiar el teléfono a modo de avión, e incluso manipular el sistema de navegación de un automóvil *Audi*.

Por otra parte, la publicación "*The Era of Ubiquitous Listening: Living in a World of Speech-Activated Devices*" (Yang Hui & Leong, 2017), pone de manifiesto un enfoque ubicuo, con la existencia de una era de escucha continua en la que los dispositivos inteligentes de reconocimiento de voz como son los dispositivos Amazon ECHO, que constantemente están en busca de comandos de voz por parte del usuario, para llevar a cabo tareas, dejando atrás formas manuales de control, como el uso de botones de hardware. Capaces de aprender de previas iteraciones con usuarios y en constante aprendizaje inteligente, este tipo de desarrollo de tecnologías activadas por comandos de voz está siendo vista como extensiones naturales de los individuos. A todo esto se debe añadir que de alguna u otra forma se los ha comenzado a ver como un miembro más de la familia. Sin embargo a través de su uso se tienen consecuencias no deseadas; tales como, que los dispositivos se activen por error y se tengan instancias accidentales de grabación de audio; la existencia de una explotación intencional, convirtiendo a los dispositivos con propósitos de espionaje. Lo que conduce a pensar en que mientras los usuarios responden con entusiasmo a una nueva tecnología, ellos también necesitan asegurarse con sus dispositivos trabajen para ellos y no contra ellos.

A todo esto se debe añadir lo que menciona el estudio "*Cybersecurity & Internet of Things*" (Dewri *et al*., 2017), a una sociedad con sensores ubicuos en sus hogares conectados todo el tiempo al IoT, y que constantemente monitorean y recolectan datos; lo que conlleva a una serie de preocupaciones de seguridad por parte de sus usuarios sobre la posibilidad de que hackers tomen el control en cualquier momento. A la par del

seguimiento de esta nueva tecnología, surgirán problemas éticos por la vulneración de estos sistemas. La sociedad necesita conocer que información le es permitida recolectar a las compañías como Amazon a través de sus dispositivos, así como también que hacen con esta.

En cuanto a la gestión de riesgos a través de la norma ISO/IEC 27005, el estudio "Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios" (Ramírez & Ortiz, 2011), propone crear una metodología para el manejo de riesgos tecnológicos, basada en los estándares ISO/IEC 31000 e ISO/ IEC 27005.

Figura 7. Alineación de estándares ISO 31000 e ISO 27005 con modelo PHVA (Ramírez & Ortiz, 2011).

<table>
<tr><th>PHVA</th><th colspan="3">ISO 27005</th><th colspan="2">ISO 31000</th></tr>
<tr><td rowspan="12">Planear</td><td colspan="2" rowspan="2">Definir plan de gestion de riesgos</td><td rowspan="12">Proceso de gestión del riesgo</td><td colspan="2">Mandato y compromiso de la dirección</td></tr>
<tr><td colspan="2">Diseño del marco de trabajo para gestión de riesgos</td></tr>
<tr><td colspan="2">Establecimiento del contexto</td><td colspan="2">Entender la organización y su contexto</td></tr>
<tr><td colspan="2" rowspan="3"></td><td colspan="2">Definir responsabilidades</td></tr>
<tr><td colspan="2">Recursos</td></tr>
<tr><td colspan="2">Integración con procesos</td></tr>
<tr><td>Identificación del riesgo</td><td rowspan="3">Valoración Riesgo</td><td colspan="2">Establecer mecanismo de comunicación</td></tr>
<tr><td>Estimación del riesgo</td><td colspan="2" rowspan="3"></td></tr>
<tr><td>Evaluación del riesgo</td></tr>
<tr><td colspan="2">Desarrollar el plan de tratamiento del riesgo</td></tr>
<tr><td colspan="2">Aceptación del riesgo</td></tr>
<tr><td rowspan="3">Hacer</td><td colspan="2"></td><td colspan="2">Establecer políticas para la gestión de riesgo</td></tr>
<tr><td colspan="2">Implementar el plan de tratamiento</td><td>Implementación del marco de trabajo para la gestión de riesgos</td><td>Implementar el proceso de gestión de riesgos</td></tr>
<tr><td colspan="2">Implementar el plan de comunicacón del riesgo</td><td colspan="2"></td></tr>
<tr><td>Verificar</td><td colspan="2">Monitoreo y revisión del riesgo</td><td colspan="2">Monitoreo y revisió del marco de trabajo</td></tr>
<tr><td>Actuar</td><td colspan="2">Mantener y mejorar el proceso de gestión</td><td colspan="2">Mejora continua del marco de trabajo</td></tr>
</table>

Es más, se sugiere el uso de buenas prácticas y guías internacionales para el correspondiente manejo de riesgos y seguridad de las organizaciones. Los sistemas de gestión propuestos en la metodología tienen su base en la ISO 31000 (Manejo de Riesgos),

la gestión de riesgos es tomada de la ISO 27005 (Gestión de Riesgos de Seguridad de la Información), y las fases propuestas del modelo PHVA (Planear, Hacer, Verificar y Actuar). Por lo que, la metodología realiza una alineación entre estos estándares con el modelo previamente dicho. La figura 7 muestra dicha alineación.

Adicional a esto, las etapas que contempla la metodología propuesta, se basan en la ISO 27005, y son:

- Establecimiento de plan de comunicación interno y externo.
- Definición del contexto organizacional interno y externo.
- Valoración de riesgos tecnológicos.
- Tratamiento de riesgos tecnológicos.
- Monitoreo y mejora continua del proceso de gestión.

El estudio concluye indicando que, es necesario robustecer la seguridad bajo tres aspectos: el físico, el lógico y el factor humano; con lo que se busca un marco de protección integral para las organizaciones.

Por otro lado, el estudio "Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000" (Valencia-Duque & Orozco-Alzate, 2017), propone una nueva metodología basada en la interrelación de cuatro normas de la ISO/IEC27000. Toma los fundamentos de la ISO27001, los controles de seguridad de la ISO27002, la gestión de riesgos de la ISO27005, y los pasos recomendados en la ISO27003. Todo esto, con el fin de generar un proceso metodológico basado en estándares internacionales y que sirva como aporte para la implementación de un Sistema de Gestión de Seguridad (SGSI) de manera exitosa en cualquier empresa.

La metodología propuesta en el estudio mencionado anteriormente (Valencia-Duque & Orozco-Alzate, 2017), plantea cinco fases secuenciales para hacer posible la implementación de un SGSI en una organización adoptando una perspectiva sistemática. Las fases planteadas se distribuyen en base a la ISO27001.

La Fase 4: "Valoración de riesgos y planificar el tratamiento de riesgos", se aborda a más detalle puesto que es de mayor aporte para el desarrollo del presente trabajo de investigación. Para esta fase, se utiliza la norma ISO27005. Establecimiento del contexto, en el cual se hace referencia a los parámetros de probabilidad, impacto, vulnerabilidad y criterios de aceptación de riesgo.

En lo que refiere a los parámetros de probabilidad, se necesita establecer la frecuencia de la posible ocurrencia de las amenazas. Se utilizan rangos de tres y cinco niveles. A cada nivel se le asigna un valor de referencia. Para los parámetros de impacto, estos se definen en función de las consecuencias que se pueden producir ante cualquier amenaza sobre los activos en referencia a la confidencialidad, disponibilidad e integridad.

Para la determinación de la vulnerabilidad, establecen una nueva medida para el impacto que una amenaza podría tener sobre la organización afectando la disponibilidad, integridad y confidencialidad de la información. La determinación de la vulnerabilidad en este caso, corresponde a que tan sensible es la organización frente a la posible materialización de una amenaza sobre a la información de la misma. Para el cálculo, el estudio utiliza dos parámetros: probabilidad e impacto, y aplica la fórmula 1 a continuación.

Fórmula 1. Vulnerabilidad del escenario de riesgo (Valencia-Duque & Orozco-Alzate, 2017)

$$V_x = (P \times I)/\max(P \times I)$$

Posteriormente, el modelo trabaja en la aceptabilidad del riesgo en la organización, para lo cual se requiere conciliar de forma coherente los diferentes intereses de la empresa.

A continuación, se estima el riesgo que consiste en estimar la vulnerabilidad (inherente y residual). La vulnerabilidad inherente estima la vulnerabilidad sin considerar los controles de seguridad, mientras que, en la estimación de la vulnerabilidad residual se toma en cuenta los controles.

Finalmente, se realiza la evaluación y el tratamiento del riesgo. La evaluación compara el riesgo y el nivel de aceptación del riesgo de cada vulnerabilidad. Mientras que el tratamiento del riesgo, hace alusión a todas las acciones a tomar con la ayuda de los controles identificados, con el fin de que el riesgo llegue al nivel aceptado por la empresa.

El estudio concluye indicando que gracias al uso y a la interrelación de cuatro de las normas de la familia ISO/IEC 27000, es posible llevar a cabo un proceso metodológico, el mismo que puede dar una respuesta de seguridad que se ajusta a la necesidad de las empresas, sin mucha demora pero aplicando estándares internacionales ya establecidos.

1.6 Adopción de una perspectiva teórica

La perspectiva teórica adoptada en este estudio, está dirigida a lo establecido en la norma ISO/IEC 27005:2011 Tecnologías de la Información – Técnicas de Seguridad - Gestión de Riesgos de Seguridad de la Información (ISO/IEC 27005, 2011), la cual es utilizada, para llevar a cabo el modelo para el análisis de vulnerabilidades de dispositivos inteligentes de reconocimiento de voz Amazon ECHO, empleando la gestión de riesgos. La misma que servirá de guía para la identificación de los requerimientos para la gestión de riesgos, basada en la norma ISO/IEC 2001:2005 Tecnologías de la Información – Técnicas de Seguridad – Sistema de Gestión de Seguridad de la Información – Requisitos (ISO/IEC 27001, 2013). Y la identificación de controles de seguridad adecuados, apoyada

en la norma ISO/IEC 2002:2013 Tecnologías de la Información – Técnicas de Seguridad - Código de Prácticas para Controles de Seguridad de la Información (ISO/IEC 27002, 2013), los mismos que serán aplicados en el correspondiente análisis.

Adicional a esto, se toma como referencia teórica el estudio "*Security Analysis of the Amazon Echo*" (Haack *et al*., 2017), en el que cual se realiza una investigación profunda sobre la arquitectura y funcionamiento de los dispositivos Amazon ECHO, la identificación de los diferentes actores y funciones permitidas; y, se plantea un modelo seguridad enfocado a la disponibilidad, confiabilidad e integridad.

Por último, en lo que refiere a la experimentación planteada, se toma como referencia lo realizado por Roy *et al*. (2017), Song and Mittal (2017), y Zhang *et al*. (2017), los cuales proponen un ataque mediante la transmisión de ultrasonidos (inaudibles), para controlar los asistentes comunes de reconocimiento de voz, como lo son los dispositivos Amazon ECHO.

CAPÍTULO II

MÉTODO

2.1. Nivel de Estudio

El presente trabajo de titulación, abarca el desarrollo de un modelo para el análisis de vulnerabilidades para los dispositivos de reconocimiento de voz, caso de estudio Amazon ECHO (Alexa); el cual, utiliza el método *exploratorio*, con el objetivo de examinar adecuadamente los parámetros y actores que intervienen en la manipulación de los dispositivos de reconocimiento de voz Amazon ECHO. Para ello, se lleva a cabo un estudio documental, sobre los diferentes escenarios de vulneración, sean estos físicos o lógicos, en los que pueden estar involucrados los dispositivos Amazon ECHO.

La técnica aplicada es el análisis bibliográfico de varios estudios de investigación tales como; las pruebas de vulnerabilidad física realizadas por consultores de la compañía de seguridad MWR *InfoSecurity* (Barnes, 2017), las diferentes experimentaciones de seguridad lógica encontradas en el estudio "*Security Analysis of the Amazon Echo*" (Haack, *et al*., 2017), el novedoso ataque a dispositivos de reconocimiento de voz, como lo son Amazon ECHO, a través de la transmisión de comandos inaudibles de alta frecuencia, puesto de manifiesto en el estudio "*Inaudible Voice Commands*" (Song & Mittal, 2017), así como también la retroalimentación de compras verificadas sobre los dispositivos Amazon ECHO, encontradas en el sitio web oficial de la compañía Amazon.

Adicionalmente, se lleva a cabo un experimento que combina el estudio sobre la arquitectura del dispositivo Amazon ECHO, "*Security Analysis of the Amazon Echo*" (Haack *et al*. 2017), y las pruebas de seguridad lógica que aprovechan las vulnerabilidades

de dos características esenciales de los dispositivos de reconocimiento de voz: la no linealidad en los micrófonos y la escucha continua, "*Inaudible Voice Commands*" (Song & Mittal, 2017).

2.2. Modalidad de investigación

La modalidad de investigación adoptada en el presente trabajo es documental. Basado en la recolección del estado del arte, relacionando estudios temáticos al problema que se quiere solucionar. La contribución, se centra en cómo este modelo de análisis de vulnerabilidades contribuye a mitigar los problemas de seguridad existentes en este tipo de dispositivos.

Es necesario indicar, que varios estudios empleados en el estado del arte, han adoptado esta modalidad de investigación. Por ejemplo, Yang Hui & Leong (2017) utiliza una investigación cualitativa cuya información ha sido recolectada a partir de artículos de noticias, sitios web oficiales de empresas de tecnología, así como también hace uso de fuentes secundarias como literatura académica y reportes tecnológicos.

2.3. Método

En el presente trabajo de investigación se utiliza el método Deductivo, el cual se origina a partir del análisis realizado a todos los documentos que forman parte del estado del arte, sobre las vulnerabilidades en los dispositivos de reconocimiento de voz Amazon ECHO.

El estudio, "*A Survey of Various Methods for Analyzing the Amazon Echo*" (Clinton *et al*., 2017), y lo realizado por la compañía de seguridad MWR *InfoSecurity*, a través de pruebas de laboratorio (Barnes, 2017), demuestran que los dispositivos de reconocimiento de voz, Amazon ECHO, son susceptibles de ser vulnerados físicamente.

Así como también, lo realizado por Roy *et al*. (2017), Song and Mittal (2017), y Zhang *et al*. (2017), los mismos que demuestran que los dispositivos de reconocimiento de voz, Amazon ECHO, son susceptibles de ser vulnerados lógicamente.

Con estos antecedentes, se determina que los dispositivos de reconocimiento de voz Amazon ECHO, presentan brechas de seguridad en su arquitectura lógica y física; las cuales pueden ser aprovechadas por agentes externos, para vulnerarlos, sin que sus dueños se percaten de ellos, comprometiendo así su privacidad.

2.4. Selección de instrumentos de investigación

El presente trabajo de investigación utiliza un método exploratorio y lleva a cabo una revisión documental; por lo que, los instrumentos utilizados para la elaboración de los diferentes apartados del plan son: papers, tesis universitarias y artículos de investigación. Adicionalmente, se consideran otros instrumentos como lo son, las páginas de revisión de compras verificadas de la compañía Amazon, las páginas oficiales de la compañía Amazon, y pruebas de seguridad realizadas y publicadas en laboratorios de empresas de seguridad.

2.5. Validez y confiabilidad de instrumentos

La validez de los documentos utilizados en el presente trabajo de investigación se detalla a continuación:

Los papers utilizados en el presente trabajo de investigación, son documentos científicos que han sido publicados y avalados previamente por entidades de la comunidad científica a través de validación por pares. Los documentos utilizados en este trabajo cuentan con la validación de las Librerías Digitales *IEEEXplore*, y de la *Association for Computing Machinery* (ACM), el motor de búsqueda académico de *Bielefeld* (BASE), Universidad de Princeton, El Colegio Militar de Carolina del Sur (USA), Universidad del

Sur Este de California (USA), Laboratorios de Investigación Digital Forense, Universidad de Tecnología de *Auckland*, Universidad de Korea (South Korea), Universidad Edith Cowan (Australia); así como también, publicaciones en revistas reconocidas, tal es el caso, del artículo de la Universidad Nacional de Singapur, publicado en la Revista Asiática de Asuntos Públicos (*Asian Journal of Public Affairs*), y el estudio realizado en la Universidad de Korea, el cual fue publicado en la revista *Cybertrust*.

Las tesis utilizadas en el presente trabajo de investigación, han sido publicadas y avaladas por universidades reconocidas como son: Universidad Nacional del Centro de la Provincia de Buenos Aires (Argentina) y la Universidad Politécnica de Madrid (España).

En lo referente a la categoría de otros instrumentos, toda la información correspondiente a la página de revisión de compras de los dispositivos Amazon ECHO, políticas de uso, términos de uso y privacidad, provienen directamente de la página oficial de la compañía Amazon, fabricante de dichos dispositivos. Cabe recalcar, que la retroalimentación proviene de la página de compras verificadas. Así mismo, producto de las pruebas de seguridad realizadas por la compañía de seguridad MWR InfoSecurity, han surgido publicaciones en TEISS Cracking Cyber Security de Londres.

Por último, las guías utilizadas para el análisis de vulnerabilidades provienen de las los estándares internacionales publicados por la Organización Internacional de Estandarización (ISO, por sus siglas en inglés) y la Comisión Electrotécnica Internacional (IEC).

2.6. Procesamiento de datos

Todo el análisis llevado a cabo en el presente trabajo de investigación, a través del estudio documental, muestra la existencia de brechas de seguridad en la arquitectura de los dispositivos de reconocimiento de voz Amazon ECHO; por lo que, dichos dispositivos están expuestos a ser manipulados de manera lógica como física.

En lo referente a las vulnerabilidades lógicas, estudios como "*Security Analysis of the Amazon Echo*" (Haack *et al*., 2017), realiza diferentes pruebas de seguridad de la arquitectura lógica de los dispositivos Amazon ECHO, analizan el tráfico generado y proponiendo trabajos futuros. Adicional a esto, la publicación "*Alexa, Can I trust You*?" (Chung *et al*., 2017), propone varios análisis enfocados en nube-nativa, análisis de paquetes, pruebas de comandos de voz, análisis de aplicaciones y análisis del firmware; los resultados de las mismas, ponen de manifiesto que, el llevar a cabo mejores pruebas de diagnóstico del ecosistema de los asistentes virtuales inteligentes (IVA), como son los dispositivos de reconocimiento de voz Amazon ECHO, pueden revelar vulnerabilidades existentes, lo cual puede encaminar a tener sistemas más confiables.

Es más, lo realizado por Roy *et al*. (2017) en "*Backdoor: Making microphones hear inaudible sounds*", Song and Mittal (2017) en "*Inaudible Voice Commands*", y Zhang *et al*. (2017) en "*Dolphin Attack: Inaudible Voice Commands*", da a conocer un método de ataque novedoso, mediante la transmisión de ultrasonidos inaudibles para controlar los asistentes comunes como *Siri, Google Home* y Amazon Echo "Alexa"; a sus micrófonos no lineales que son parte esencial de los mismos. Los resultados obtenidos, arrojaron altas tasas de éxito en los dispositivos Amazon ECHO.

Por otro lado, en referencia a la manipulación física de los dispositivos Amazon ECHO, el estudio realizado por la compañía de seguridad MWR *InfoSecurity*, a través de pruebas de laboratorio (Barnes, 2017), demostró que los modelos Amazon Echo 2015-2016 son susceptibles de ser vulnerados físicamente, permitiendo al atacante tener acceso al sistema operativo Linux del dispositivo e instalar un malware, sin dejar evidencia de manipulación. Cabe anotar, que pese a que la empresa Amazon solucionó esta vulnerabilidad para los dispositivos ECHO 2017; siguen existiendo más de 11 millones de dispositivos 2015-2016, que seguirán siendo susceptibles de ser vulnerados.

Adicional a esto, el documento técnico "*A Survey of Various Methods for Analyzing the Amazon Echo*" (Clinton *et al*., 2017), enfocado en analizar el modelo de privacidad de los dispositivos Amazon ECHO, pone de manifiesto diferentes enfoques de ataques físicos que pueden tener los dispositivos Amazon ECHO, los cuales podrían tener un mayor acceso al sistema de archivos del dispositivo Amazon ECHO.

Por otro lado, en referencia a las aplicaciones realizadas por terceros para los dispositivos Amazon ECHO, el estudio "*Privacy in the Amazon Alexa Skills Ecosystem*" (Alhadlaq *et al*., 2017), señala que es uno de los primeros estudios que se lleva a cabo sobre la privacidad en el ecosistema de las funcionalidades de Alexa, conocidos como "Alexa *Skills Kit*". El estudio está enfocado en las elecciones de privacidad llevadas a cabo por Amazon al establecer el ecosistema *Skills,* y las prácticas de privacidad de los desarrolladores que contribuyen a la creación de los *Skills*. Vale mencionar que la empresa Amazon, solicita políticas de privacidad únicamente a aquellos *Skills* que tienen un enlace a la cuenta de Amazon. Lo que llama la atención de los resultados obtenidos es que los *Skills* mejor calificados, son los que más carecen de políticas de privacidad. Todo esto evidencia que el asunto de privacidad en este aspecto es tomado muy a la ligera.

Adicionalmente, en referencia al experimento planteado, se pretende reproducir el ataque realizado por Roy *et al*. (2017), Song and Mittal (2017), y Zhang *et al*. (2017), los mismos que proponen un método de ataque inaudible, a través de la emisión de señales de ultrasonido a los dispositivos de reconocimiento de voz, como es el caso de Amazon ECHO.

Por último, en lo referente al desarrollo del modelo para el análisis de vulnerabilidades de dispositivos inteligentes de reconocimiento de voz Amazon ECHO, se toma lo establecido en la norma ISO27005:2011; la misma que se apoya en las normas

ISO2001:2005 e ISO2002:2013, para la identificación de los elementos y controles de seguridad necesarios, que serán aplicados en el correspondiente análisis.

Por todo lo anteriormente expuesto, se cuentan con todos los elementos necesarios para proponer un modelo para el análisis de vulnerabilidades de dispositivos de reconocimiento de voz utilizando la norma ISO/IEC27005:2011.

CAPÍTULO III

ARQUITECTURA DE LOS DISPOSITIVOS AMAZON ECHO

El dispositivo de reconocimiento de voz Amazon ECHO, es uno de los productos estrella de la empresa Amazon Inc., la cual es una de las compañías más grandes de compras en línea a nivel mundial. Fundada en 1995, por Jeff Bezos, comenzó con la venta de libros en línea, a través de su conocida página web, convirtiéndose en uno de los mayores minoristas en línea del planeta. Alexa, es el cerebro de los dispositivos Amazon ECHO en sus diferentes versiones *Echo 1st Generation* (1), *Echo 2nd Generation* (2), *Echo Show* (3), *Echo Plus* (4), *Echo Spot* (5), *Echo Tap* (6), *Echo Dot* (7), y el nuevo *Echo Look* (8) (ver figura 8).

Figura 8. Dispositivos Amazon ECHO (Amazon, 2017)

Se trata de un dispositivo de reconocimiento de voz el cual está implementado en la nube, cuya característica principal es su activación al llamado de “Alexa” (la cual es la

palabra de activación, aunque puede ser cambiada), y una vez que ha reconocido el comando, procede a la ejecución de una gran variedad de tareas, tales como: dar información en vivo sobre el clima, tráfico y noticias, reproducir música, controlar dispositivos inteligentes del hogar, ordenar productos desde el almacén online de Amazon, interacción con aplicaciones de terceros, entre otros. Sin embargo, pese a toda esta gama de nuevas características, los dispositivos ECHO siguen manteniendo una limitante: el lenguaje, ya que solo reconocen el idioma inglés. Pero su uso, se ha extendido fuera de Estados Unidos llegando a Reino Unido y Alemania.

Para poder utilizar el dispositivo, es necesario conectarlo, tener una conexión a Internet para poder descargar aplicación Alexa, realizar las configuraciones respectivas, y proceder con los comandos de voz, con el fin de que se lleven a cabo las tareas respectivas.

3.1 Arquitectura Física

Dentro de los modelos de los dispositivos de reconocimiento de voz de Amazon, se toma como referencia al modelo ECHO para un mayor detalle de su arquitectura física. De acuerdo a lo que menciona Amazon, y tal como lo muestra la figura 9, los dispositivos Amazon ECHO poseen las siguientes características técnicas:

- Tamaño: 5.8 x 3.4 x 3.4 pulgadas. Peso: 29.0 onzas.
- Altavoz de sonidos graves (*Woofer*) de 2.5 pulgadas. Altavoz de sonidos agudos (*Tweeter*) de 0.6 pulgadas.
- Arreglo de siete micrófonos.
- Anillo de luz para ajuste de volumen.
- Conexión *Wi-Fi* con banda dual que soporta redes 802.11 a/b/g/n (2.4 y 5 GHz). No soporta conexiones *ad-hoc*.

- Conexión *Bluetooth* para la transmisión de audio desde dispositivos móviles.

Figura 9. Detalles Técnicos Amazon ECHO (Amazon, 2017)

Adicionalmente, de acuerdo al estudio "*Amazon Echo Teardown*" (IFIXIT, 2014), los dispositivos Amazon ECHO constan de las siguientes partes:

Las figuras 10 y 11 muestran lo referente a la placa de alimentación y el controlador del altavoz, los mismos que se encuentran ubicados en la parte inferior del dispositivo. En esta sección se encuentran los siguientes componentes:

- El regulador descendente TPS53311 3A, *Texas Instruments* TPS53312 con conmutador integrado (recuadro rojo).
- El Códec de audio estéreo de baja potencia, *Texas Instruments* TLV320DAC3203 (recuadro naranja).
- El amplificador estéreo sin filtro clase D, *Texas Instruments* TPA3110D2 15W (recuadro amarrillo).

Figura 10. Componentes de la placa de alimentación Amazon ECHO (IFIXIT, 2014)

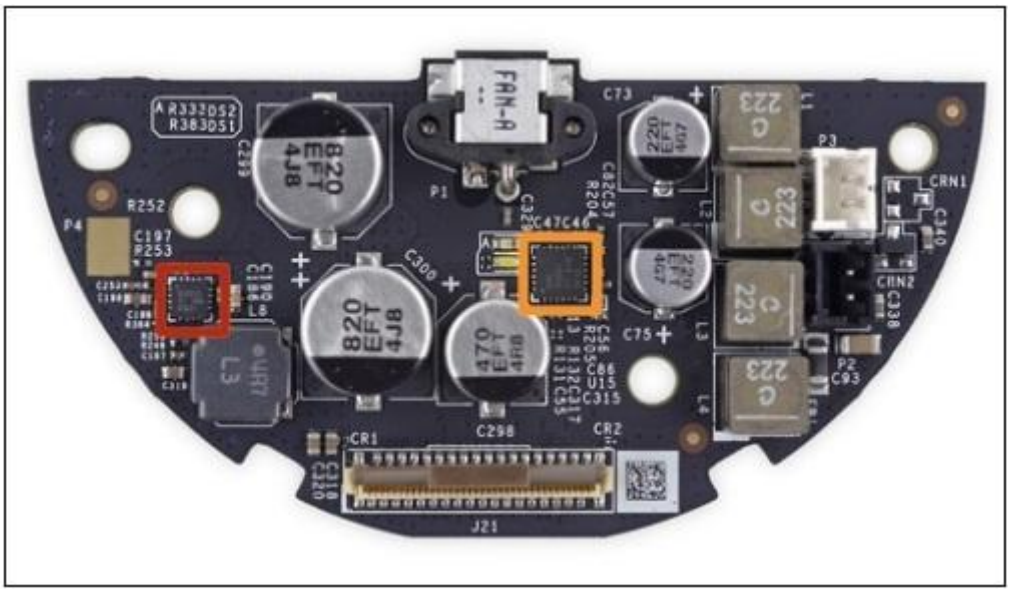
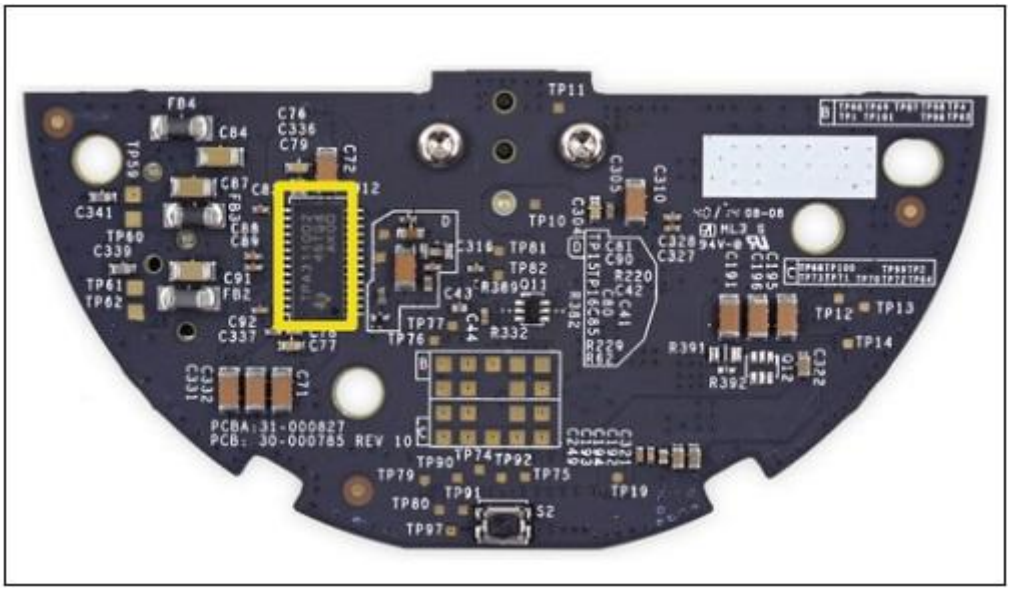


Figura 11. Componentes del controlador del altavoz Amazon ECHO (IFIXIT, 2014)

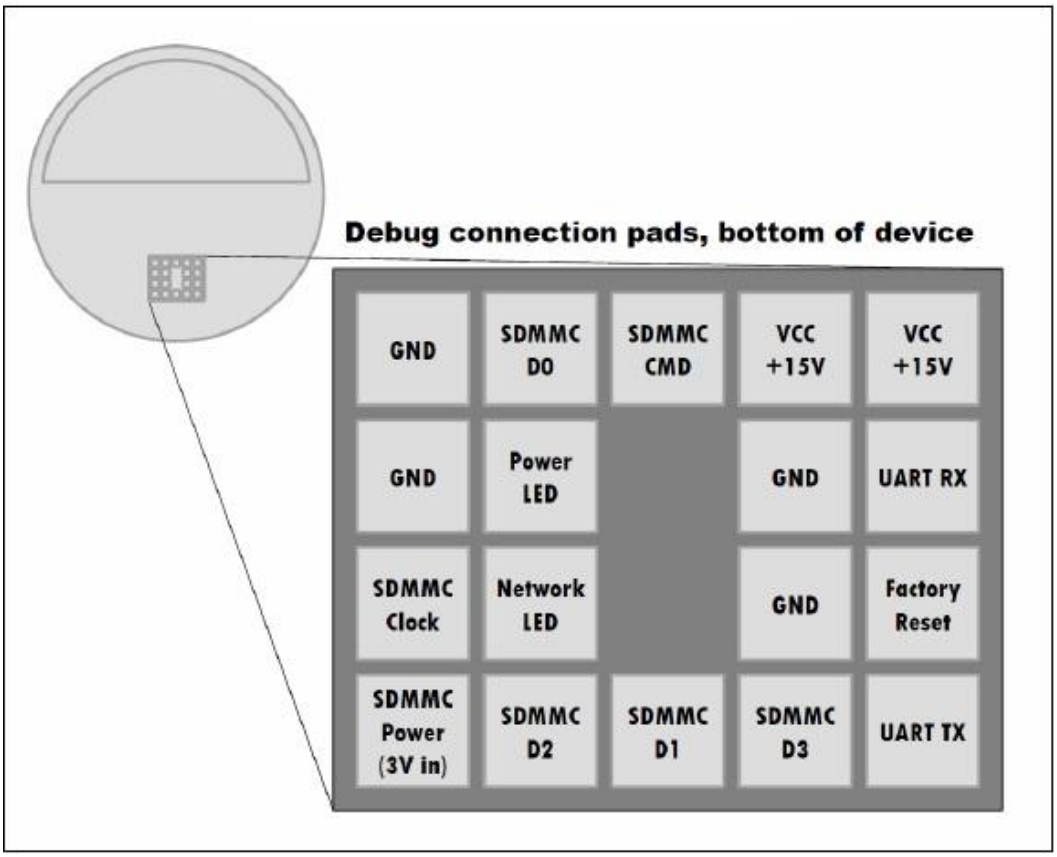


Cabe destacar, que dentro de esta placa de alimentación, se puede identificar un *pinout* o disposición de pines, el cual contiene 18 diferentes pines. Este permite la conexión de una tarjeta externa SD. Es importante señalar, que los dispositivos ECHO están configurados para ser arrancados desde este *pinout*, si es detectado durante la iniciación.

Por lo que, se podrá utilizar una tarjeta SD externa la cual contenga un sistema operativo y arrancar el dispositivo Amazon ECHO. Esta característica permitió que los dispositivos Amazon ECHO puedan ser vulnerados de manera física, tal como lo menciona Barnes (2017).

La figura 12 muestra la distribución de pines antes mencionada. Estos proveen poder de 15V, 3V, UART TX, RX y tierra; así como también todo lo necesario para la conexión de una tarjeta externa SD.

Figura 12. *Pinout* para los puertos de depuración (Clinton, Cook, & Banik, 2017)

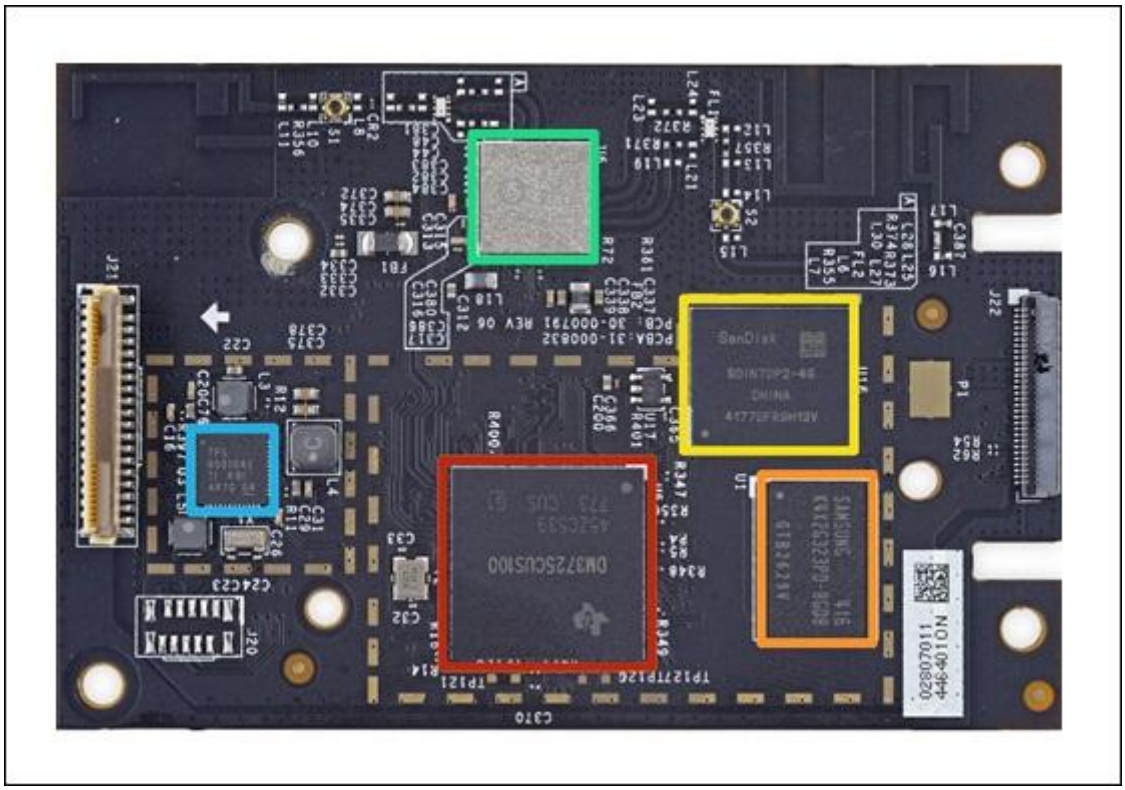


Adicionalmente, la figura 13 muestra la placa base (*motherboard*) que da vida a los dispositivos ECHO.

- Procesador digital de medios, *Texas Instruments* DM3725 (recuadro rojo).
- Chip de memoria *SanDisk* de 4GB (recuadro amarrillo).

- Chip RAM *Samsung* K4X2G323PD-8GD8 de 256MB (recuadro naranja).
- Chip *Qualcomm Atheros* QCA6234XAM2D para la conexión *Wi-Fi*, y módulo Bluetooth (recuadro verde).
- Y por último, el chip para el Manejo Integrado de Poder, *Texas Instruments* TPS65910A1 (recuadro azul).

Figura 13. *Motherboard* de los dispositivos Amazon ECHO (IFIXIT, 2014)

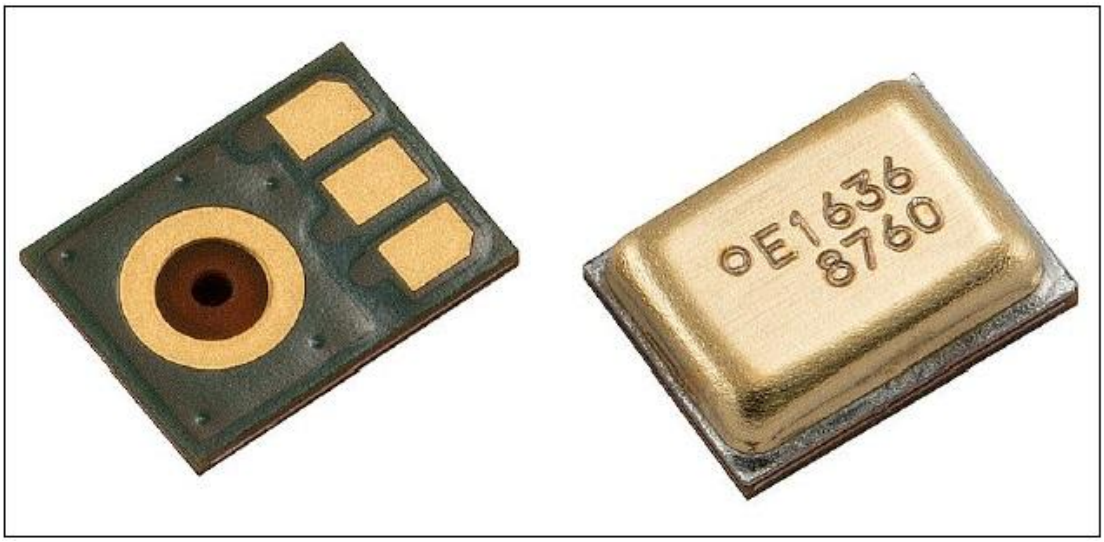


Otro componente muy importante que merece ser mencionado es el arreglo de siete micrófonos que utilizan los de los dispositivos Amazon ECHO.

De acuerdo a lo que menciona IFIXIT (2016), los dispositivos Amazon ECHO DOT utilizan micrófonos *Knowles*: *SiSonic*^{TM} (Knowles Electronics, LLC, 2017), muy probablemente el modelo SPA1687LR5H-1, puesto que estos se conectan a las entradas diferenciales de ADC, a más de cumplir con las debidas especificaciones y dimensiones requeridas para este tipo de dispositivo. Este modelo, consiste de un sensor acústico, un

buffer de entrada de bajo ruido y un amplificador de salida diferencial. La figura 14 muestra el micrófono *Knowles SiSonic™* en mención.

Figura 14. Micrófono Knowles SiSonic™ modelo SPA168LR5H-1 (Knowles Electronics, LLC, 2017)



El micrófono *Knowles SiSonic™* utiliza tecnología MEMS (*Micro Electro Mechanical Systems*), el cual debido a sus características "domina los dispositivos de control de voz, incluyendo teléfonos inteligentes y dispositivos portátiles" (Zhang, Yan, Ji, & Zhang, 2017). Los dispositivos Amazon ECHO, utilizan este tipo de micrófonos (Amazon Developer, 2017).

Cabe destacar, que los componentes del micrófono son sistemas lineales, lo que significa que las señales de salida son combinaciones lineales de la señal de entrada. Sin embargo, la linealidad tanto en los micrófonos como en los parlantes que transmiten las ondas mecánicas del sonido, solamente se conserva en el rango de frecuencia audible (20Hz – 20kHz), y fuera de este rango exhiben no linealidad (Roy, Hassanieh, & Choudhur, 2017). "Los dispositivos con no linealidad son capaces de generar nuevas frecuencias y con una señal de entrada elaborada, pueden reducir la señal y recuperar la señal de banda base" (Zhang *et al.*, 2017).

Es importante señalar, que para llevar a cabo el experimento descrito en el Anexo 1, las características de escucha continua, así como, la no linealidad de arquitectura del micrófono de los dispositivos Amazon ECHO son parte esencial del mismo.

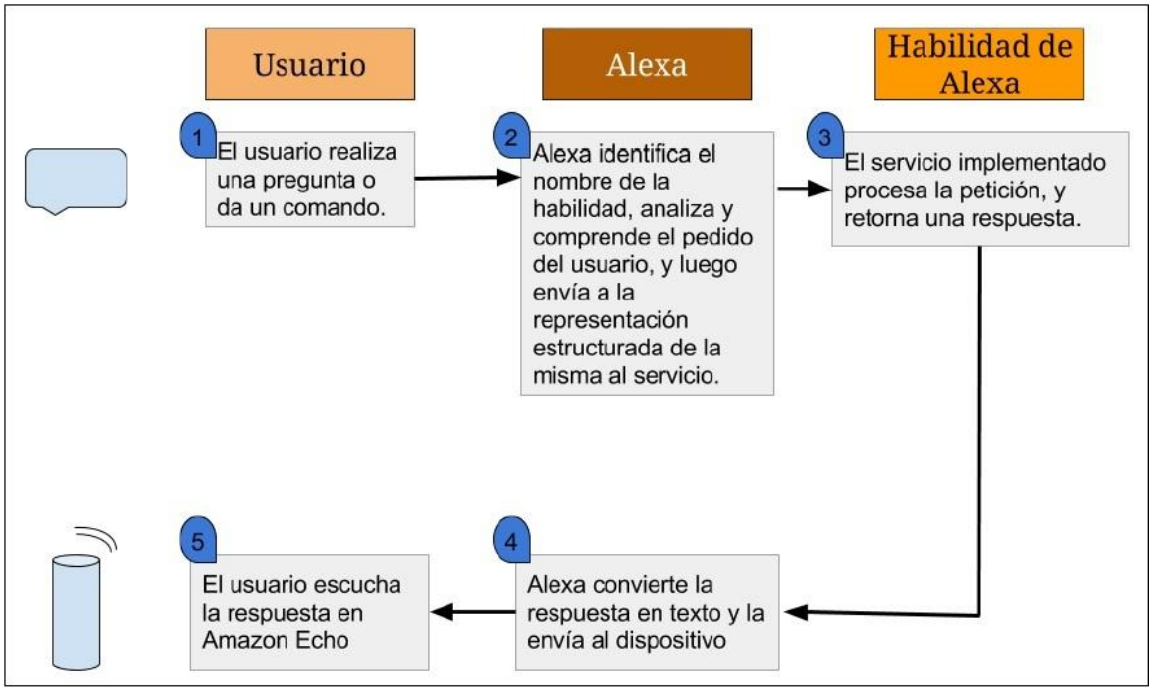
3.2 Arquitectura Lógica

De acuerdo al estudio "*Security Analysis of the Amazon Echo*" (Haack *et al*., 2017), dentro de los componentes que conforman la arquitectura lógica de los dispositivos Amazon ECHO están:

ECHO: dispositivo que provee la interfaz para el usuario a través de comandos de voz.

Servicio en la Nube de Alexa: software/servicio responsable de relacionar los comandos de voz con los *intents* o acciones a ejecutar por Alexa. La figura 15 muestra la interacción entre el usuario y Alexa previamente descrita.

Figura 15. Interacción del dispositivo Amazon ECHO con el servicio de Alexa (Keimel, 2016)



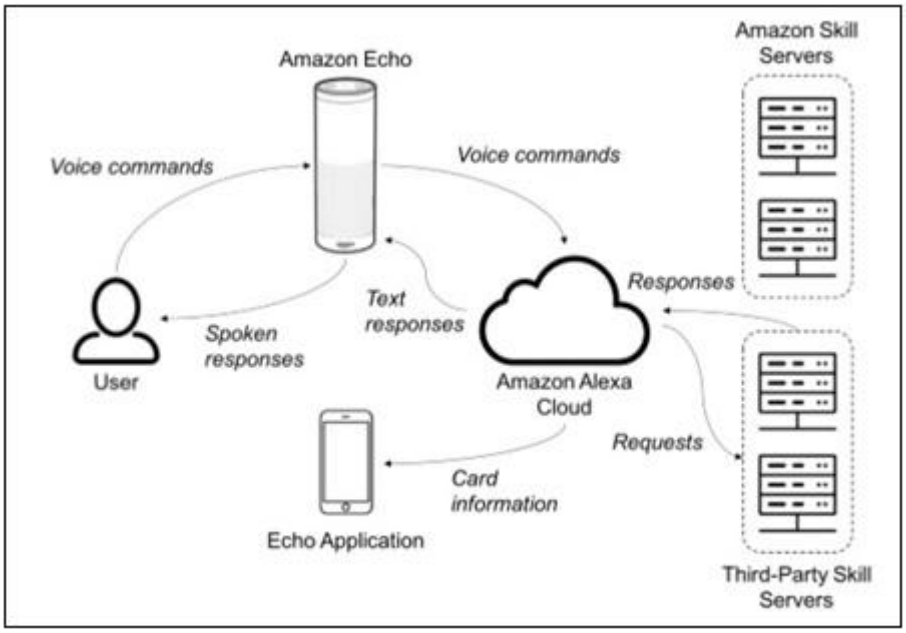
Servidores de Skills de Amazon, donde se alojan los *Skills* (habilidades / funcionalidades) de Alexa, desarrollados por Amazon para sus usuarios.

Servidores de Skills de terceros, donde se alojan los *Skills* que son implementados por desarrolladores externos.

Aplicación Echo, aplicación a través de la cual los usuarios pueden realizar ajustes a la configuración de Alexa.

La figura 16 muestra la arquitectura de los dispositivos Amazon ECHO antes mencionada.

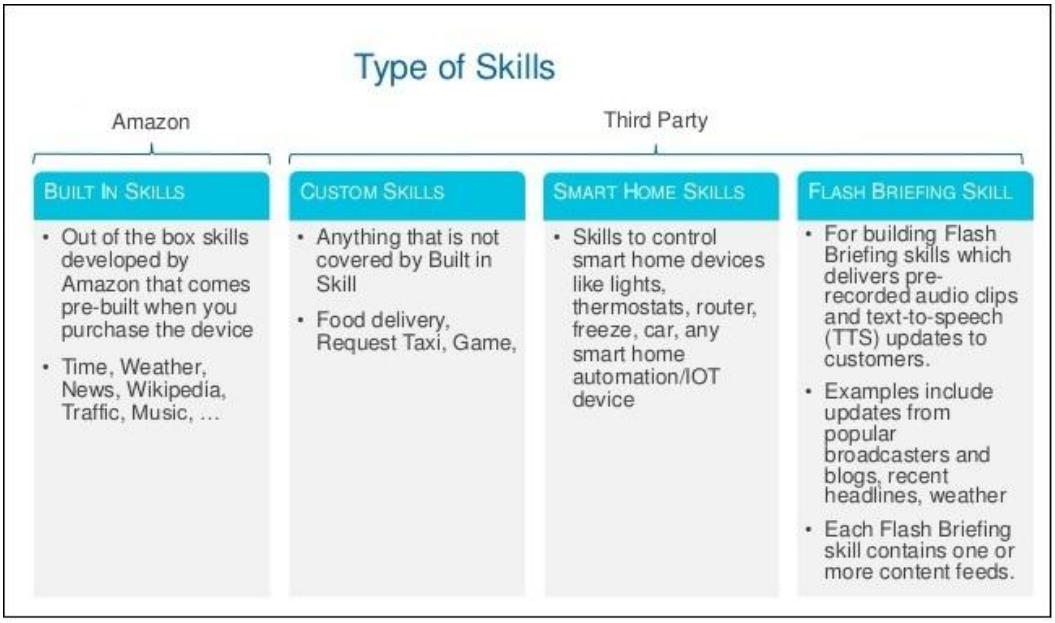
Figura 16. Sistema de Arquitectura de los dispositivos Amazon Echo. (Haack *et al*., 2017)



3.2.1 *Alexa Skills Kit* (ASK)

Alexa *Skills Kit*, es una colección de APIS (Interfaces de Programación de Aplicaciones), herramientas, documentación y ejemplos, que permiten a desarrolladores externos de la compañía Amazon añadir funcionalidades personalizadas a los Amazon ECHO; los mismos que le permitirán a estos dispositivos ser más inteligentes y brindar más servicios a sus usuarios a través de comandos de voz (Amazon, 2017). La figura 17 muestra varios tipos de *Skills* que pueden adicionarse a Alexa.

Figura 17. Tipos de *Skills* para Alexa (Chakrabarti, 2017)



Estas nuevas funcionalidades o *Skills* desarrollados por terceros, deben habitar en la nube, con lo que los usuarios podrán hacer uso de las mismas en cualquier momento, pudiendo estar alojados en dos lugares: Amazon Web Services, AWS Lambda (el cual es ofrecido por Amazon), o un punto de acceso HTTPS, accesible a través de Internet con un certificado de seguridad.

3.2.2 *Alexa Voice Services* (AVS)

Los Servicios de Voz de Alexa, proporcionan las herramientas de hardware y software necesarias, para que los desarrolladores puedan integrar a Alexa con sus productos, con lo que AVS brinda un control de voz de manos libres conveniente para cada dispositivo conectado. A través de AVS, se pueden adicionar nuevas interfaces inteligentes a productos, con lo que los usuarios podrán usar y así beneficiarse de las funcionalidades de Alexa. Se trata de un servicio escalable que se aloja en la nube, que provee interfaces de fácil uso, trata de simplificar la tarea a los desarrolladores al momento de la construcción de productos, que pueden ser activados mediante comandos de voz, los cuales manejan Reconocimiento Automático de Voz (ASR) y el Entendimiento del Lenguaje Natural

(NLU), lo cual es procesado en la nube. La figura 18 muestra la integración de AVS con tres dispositivos conectados.

Figura 18. Integración de AVS con otros dispositivos (Amazon Developer, 2017)

3.3 Formas de Conexión

En lo referente a la conexión de redes Wi-Fi, los dispositivos Amazon ECHO pueden conectarse a redes de doble banda Wi-Fi (2,4 GHz / 5 GHz), las cuales utilizan el estándar 802.11 a / b/ g / n (Amazon, 2017). Sin embargo, los dispositivos Amazon ECHO, no trabajan en redes *ad-hoc* (o *peer-to-peer*).

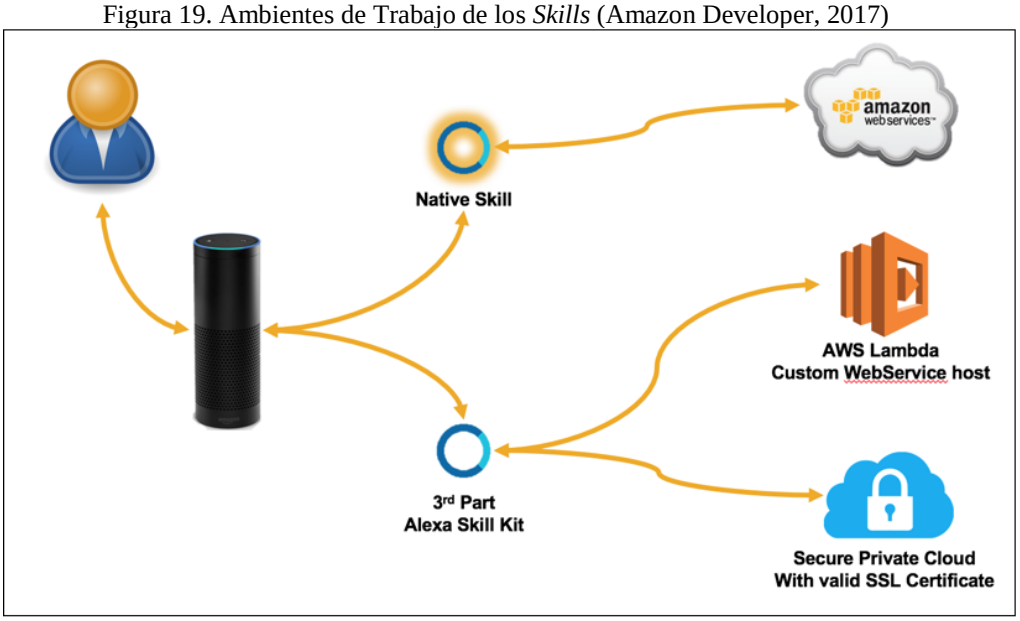
Adicional a esto, los dispositivos Amazon ECHO, pueden conectarse y controlar otros objetos inteligentes en casa. Una de las formas de conexión es a través de un *Hub* (Amazon Developer, 2018). El protocolo *ZigBee* (*Light Link ZigBee*) es el estándar global utilizado para el control de productos de iluminación de fácil uso. Lo que permite a sus usuarios el tener control inalámbrico sobre todos sus accesorios LED, bombillas, temporizadores, controles remotos, interruptores, entre otros (Amazon Inc., 2018). Es a través de este estándar, que se puede realizar cambios de manera remota a los dispositivos inteligentes en casa de una manera más efectiva y centralizada.

Adicional a esto, otra forma para la conexión con dispositivos, es la nueva categoría conocida como *Alexa Gadgets* (Amazon Developer, 2018), que a través de SDK y el API *Skills*, permiten a los desarrollados construir productos y experiencias que convierten al dispositivo Echo en un centro de juegos interactivo en el que se construyen y se conectan dispositivos.

3.4 Ambientes de Trabajo

Al referirse a los *Skills* o funcionalidades que pueden ser añadidas al dispositivo Amazon ECHO, los desarrolladores cuentan con dos servicios de Alexa, los cuales residen en la nube. En lo que refiere a los *Skills* nativos, se cuenta con Amazon *Web Services* AWS, y para aquellos *Skills* desarrollados por terceros, Amazon ofrece *AWS Lambda*. En el caso de que los desarrolladores cuenten ya con un sitio en la nube, éstos también podrán hacer uso de ésta, siempre y cuando cumpla con los respectivos certificados de seguridad requeridos por la compañía Amazon. La figura 19 muestra los ambientes de trabajo mencionados.

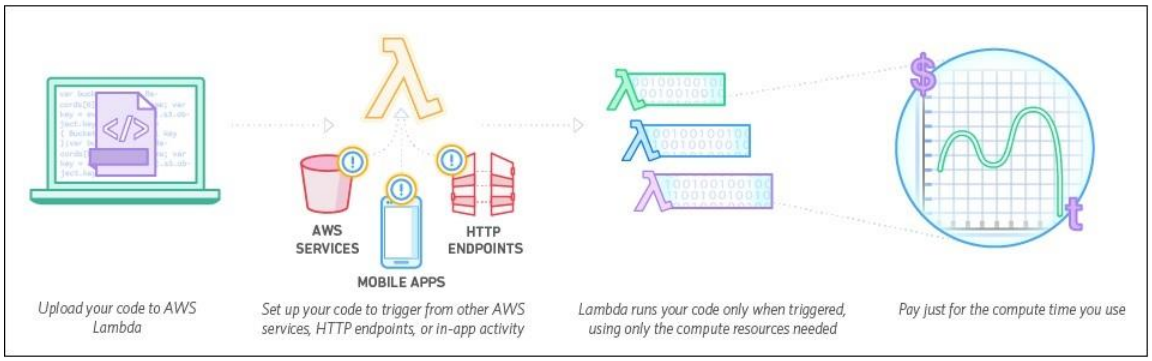
Figura 19. Ambientes de Trabajo de los *Skills* (Amazon Developer, 2017)



AWS Lambda, como lo menciona Amazon (2017), es un servicio de cómputo que permite ejecutar código generado por programadores en respuesta a eventos. A su vez gestiona automáticamente y de manera efectiva todos los recursos informáticos necesarios para llevar a cabo el servicio; esto facilita a que las aplicaciones puedan responder de manera más rápida a la nueva información.

Su funcionamiento es de la siguiente manera: el desarrollador sube el código a *AWS Lambda*, posteriormente se debe configurar el código que va ser ejecutado desde otros servicios AWS, puntos HTTP finales, o actividades en aplicaciones. Posterior a esto, Lambda corre el código subido solo cuando es llamado y usando solo aquellos recursos necesarios. Finalmente, se paga solo por el tiempo de uso. La figura 20 muestra el flujo de trabajo de AWS Lambda descrito.

Figura 20. Funcionamiento AWS Lambda (Amazon, 2017)



CAPÍTULO IV

MODELO DE SEGURIDAD

El desarrollo del modelo de seguridad planteado en el presente trabajo de investigación, se basa en la necesidad que tiene el usuario de proteger el ambiente en el cual interactúa de forma diaria con dispositivos inteligentes del tipo de Amazon ECHO. La idea es que los usuarios puedan sentirse seguros al mantener conversaciones frente a estos dispositivos, el poder realizar transacciones a través de éstos de manera confiable, el interactuar de forma segura con otros dispositivos inteligentes interconectados, en casa, entre otros. Es por tal motivo, que la identificación de los activos (explicados en la sección 4.1 de este capítulo) está relacionado a la información que el usuario maneja a través del dispositivo Amazon ECHO, bajo este tipo de ambientes.

Adicionalmente, para llevar a cabo el modelo para el análisis de vulnerabilidades de dispositivos de reconocimiento de voz Amazon ECHO, se emplean las directrices especificadas en la norma ISO27005:2011, “Gestión de Riesgos de Seguridad de la Información” (ISO/IEC 27005, 2011), con el soporte de las normas ISO2001:20013, “Requerimientos” (ISO/IEC 27001, 2013), para la identificación de los elementos involucrados en el análisis, e ISO27002:2013, “Código de Prácticas para Controles de Seguridad de la Información” (ISO/IEC 27002, 2013), para la identificación y selección de controles de seguridad adecuados; los cuales servirán como base y referencia para los controles sugeridos a los usuarios, de tal manera que, al ser implementados, se puedan

evitar violaciones a la seguridad y privacidad de las personas que manejan este tipo de dispositivos.

La figura 21 muestra el esquema de la Gestión de Riesgos basado en la norma ISO27005, la cual expone los elementos que necesitan ser identificados como lo son los activos, amenazas, vulnerabilidades, riesgo y las contramedidas (salvaguardas) para mitigar los riesgos encontrados.

Figura 21. Esquema de Gestión de Riesgos basado en la ISO27005 (Cao Avellaneda, 2008).

Los pasos a seguir para el desarrollo del modelo, basados en la norma ISO27005:2011 son los siguientes:

1. Identificación de los activos.
2. Identificación de las amenazas.
3. Identificación de las vulnerabilidades y sus tipos.
4. Valoración de activos.

5. Estimación del riesgo a través de los criterios de probabilidad de ocurrencia y valoración de impacto.
6. Creación matriz de riesgos inherente (adaptada).
7. Identificación de controles de seguridad basados en la norma ISO 27002.
8. Identificación de controles sugeridos al usuario.
9. Creación de matriz de riesgos residual (con controles aplicados).

Es necesario indicar que el trabajo para el desarrollo de las matrices, se lo llevó a cabo mediante la técnica de entrevista semiestructurada (Shull, Singer, & Sj_berg, 2007), con la participación de tres usuarios de los dispositivos Amazon ECHO, Alexa. La información de los usuarios y su relación con el dispositivo, se detalla en la tabla 1 a continuación.

Tabla 1. Usuarios – Alexa. Elaborado por el autor.

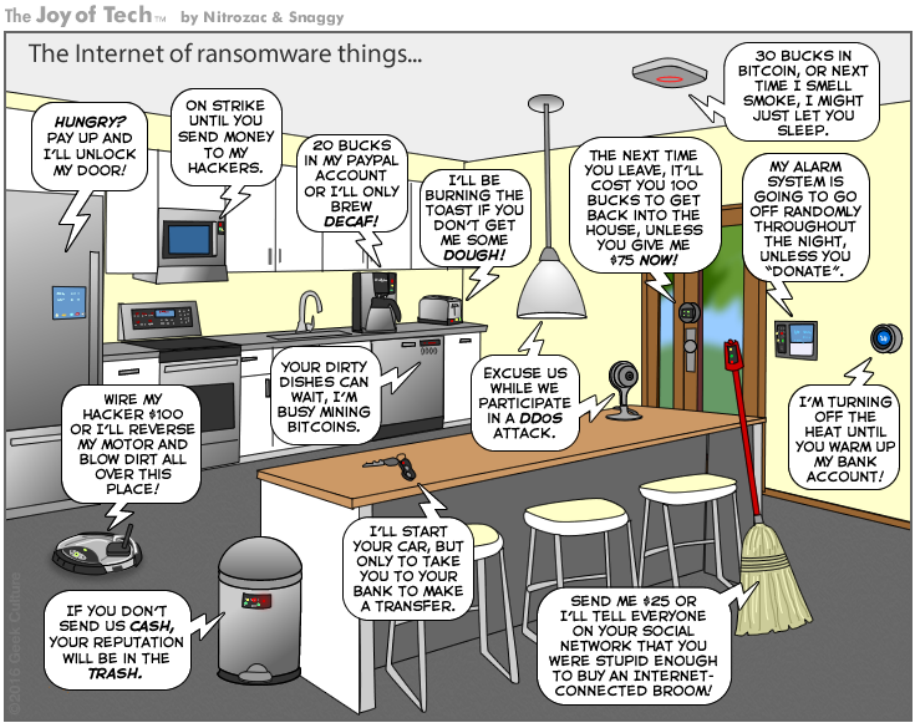
Usuario	**Actividad**	**Uso de Alexa**
Usuario 1	Profesional en sistemas. Docente universitario con doctorado en Ciencias de la Computación.	Dispositivo en casa. Maneja otros dispositivos inteligentes a través de este.
Usuario 2	Experto en TI con maestría en Ciencias de la Computación.	Dispositivo en casa. Interactúa con el dispositivo para solicitarle actividades diarias tales como el clima, horarios de tren y buses, etc.
Usuario 3	Experto en TI con maestría en Ciencias de la Computación.	Dispositivo en casa. Interactúa con el dispositivo y tiene planes de evaluarlo a mayor profundidad.

4.1 Identificación

4.1.1 Identificación de Activos

Como se mencionó anteriormente, la identificación de los activos está relacionada con la información que el usuario maneja a través del dispositivo Amazon ECHO en su entorno actual. La figura 22 muestra en forma divertida la interacción entre varios dispositivos de reconocimiento de voz en su entorno familiar.

Figura 22. Usuario – Dispositivos inteligentes en el hogar. (Nitrozac & Snaggy, 2016)



Si bien es cierto y de acuerdo a lo establecido en la norma ISO/IEC 27005:2011, sección 8.2.2 "Identificación de Activos", se deben identificar los activos con alcance establecido en la organización. Para el caso del presente estudio, proponemos cambiar este paradigma, identificando a los activos desde el punto de vista del usuario. Puesto que la norma ISO/IEC27005:2011 utiliza un enfoque tradicional de Seguridad de la Información en organizaciones que aún no se adapta a los entornos del ciberespacio, en dónde, el modelo de seguridad tiene que integrar de forma más robusta a personas, procesos y

tecnología de manera más íntima a todos los entornos en dónde se utiliza información digitalizada. Así, los activos identificados van en relación a los activos que el usuario del dispositivo de reconocimiento de voz Amazon ECHO pretende proteger en el entorno en el que se desenvuelve. La tabla 2 muestra los activos en mención.

Tabla 2. Identificación de Activos. ISO27005:2011. Elaborado por el autor.

ACTIVOS	
Dispositivo AMAZON ECHO	• Información sensible que se tiene en la cuenta de Amazon. • Transacciones en línea. • Manejo de otros dispositivos inteligentes en casa; tales como: luces, temperatura, bloqueo de puertas, encendido de auto, etc. • Conversaciones privadas (mantenidas en casa)

4.1.2 Identificación de Amenazas

De acuerdo a lo establecido en la norma ISO/IEC 27005:2011, sección 8.2.3 Identificación de Amenazas, las amenazas y sus fuentes deben ser identificadas (ISO/IEC 27001:2013 Clausula 4.2.1 d) 2), "Identificar las amenazas para los activos identificados". Las amenazas pueden ser de origen natural o humano y pueden ser ocasionadas de manera accidental o deliberada. Estas deben ser identificadas de manera genérica y por tipo. La tabla 3 muestra las amenazas identificadas por tipo, las cuales fueron tomadas de la norma ISO/IEC 2005:2011 en su anexo C. Cabe recalcar que se tomaron aquellas amenazas a las que pueden estar expuestos los dispositivos Amazon ECHO.

Tabla 3. Identificación de Amenazas. (ISO/IEC 27005, 2011)

Tipo	Amenaza
Compromiso de la información	• Espionaje Remoto • Escuchas • Manipulación de Hardware • Manipulación de Software • Robo de información • Acceso no autorizado • Pérdida de confidencialidad
Comunicaciones	• Obtención de información extraída de los paquetes que se transmiten por la red Interceptación pasiva de la información • Análisis de tráfico
Acciones no autorizadas	• Uso no autorizado del equipo • Proceso ilegal de datos

4.1.3 Identificación de Vulnerabilidades

Se necesita identificar a las vulnerabilidades existentes, de acuerdo a lo que establece la norma ISO/IEC 27005:2011, sección 8.2.5 “Identificación de vulnerabilidades”, en la que dice que “se deben identificar las vulnerabilidades que pueden ser explotadas por las amenazas y así causar daño a los activos de la organización” (ISO/IEC 27001:2013 Clausula 4.2.1 d) 3) “Identificar las vulnerabilidades que pueden ser explotadas por amenazas”.

Para lo cual, la norma ISO/IEC 27005:2011, en su Anexo D, numeral D.2 “Vulnerabilidades y Métodos de Evaluación de Vulnerabilidades” (ISO/IEC 27005, 2011), describe varios métodos para la identificación y evaluación de vulnerabilidades, como lo son: las herramientas automáticas de escaneo de vulnerabilidades, pruebas de seguridad y evaluación, pruebas de penetración y revisión de código. Los resultados que se obtengan

de todos los tipos de pruebas de seguridad, nos ayudarán a identificar un sistema de vulnerabilidades. Dentro de los métodos que dan soporte a las pruebas de seguridad descritas anteriormente están: entrevistas a personas y usuarios, cuestionarios, inspecciones físicas y análisis de documentos.

Para el presente trabajo, se emplea el análisis de documentos como método para la identificación de vulnerabilidades existentes en los dispositivos de reconocimiento de voz, Amazon ECHO; el cual, es el resultado del estudio del estado del arte llevado a cabo. Adicional a esto, se toman en consideración las revisiones de compras verificadas de la empresa Amazon, por parte de los usuarios, a través de la página web oficial de la compañía. Por último, se utiliza la inspección física, la misma que se ejecuta a través del experimento planteado (para mayor información ver sección Anexos 1.Experimentación).

Con lo que, a través del análisis documental se lograron identificar las vulnerabilidades que pueden ser explotadas en los dispositivos de reconocimiento de voz, Amazon ECHO. La tabla 4 muestra las vulnerabilidades encontradas, así como también el estudio correspondiente que la sustenta.

Tabla 4. Identificación Vulnerabilidades - Amazon ECHO. ISO27005:2011. Elaborado por el autor.

	Vulnerabilidades	**Estudio**
V1	Falla de hardware / software.	Prueba de laboratorio realizada por Barnes (2017)A Survey of Various Methods for Analyzing the Amazon Echo (Clinton et al., 2017)
V2	Control de acceso no autorizado / inadecuado.	'Alexa cómprame una casa de muñecas' (Bhattacharya, 2017), Analysis of the Amazon Echo (Haack et al., 2017), Privacy in the Amazon Alexa *Skills* Ecosystem (Alhadlaq *et al*., 2017), Analysis of the Amazon Echo" (Haack et al., 2017), Alexa, Can I trust You? (Chung *et al*., 2017)

	Vulnerabilidades	Estudio
V3	Conexión no autorizada al equipo.	Página de revisión de compras de Amazon, Johnson (2017)
V4	Uso no controlado / impropio	Inaudible Voice Commands (Song & Mittal, 2017), BackDoor: Making Microphones Hear Inaudible Sounds (Roy et al., 2017), DophinAttack: Inaudible Voice Commands (Zhang et al., 2017), "Cybersecurity & Internet of Things" (Dewri *et al*., 2017)
V5	Líneas de comunicación desprotegidas / Protección inadecuada de tráfico sensible / Transferencia de información en texto visible.	Security Analysis of the Amazon Echo" (Haack et al., 2017), Can I trust You? (Chung et al., 2017)

4.1.3.1 Tipo de Vulnerabilidades

Dentro de los diferentes tipos de vulnerabilidades especificados en la norma ISO/IEC 27005:2011, en su Anexo D, numeral D.1 "Ejemplos de vulnerabilidades", se cuenta con los siguientes tipos de vulnerabilidades: hardware, software, red, personal, sitio y organización (ISO/IEC 27005, 2011). La tabla 5 presenta las vulnerabilidades identificadas en los dispositivos de reconocimiento de voz Amazon ECHO con su respectivo tipo.

Tabla 5. Vulnerabilidades - Tipos. ISO/IEC 27005:2011. Elaborado por el autor.

	Vulnerabilidades	Tipo
V1	Falla de hardware / software	• Hardware • Software

	Vulnerabilidades	Tipo
V2	Control de acceso no autorizado / uso inadecuado	• Personal • Organización
V3	Conexión no autorizada al equipo	• Red
V4	Uso no controlado / impropio	• Personal • Organización
V5	Líneas de comunicación desprotegidas. Protección inadecuada de tráfico sensible. Transferencia de información en texto visible.	• Red

4.2 Relación Amenaza – Vulnerabilidad

Una vez que han sido identificadas las amenazas y las vulnerabilidades que afectan a los dispositivos de reconocimiento de voz Amazon ECHO, es necesario relacionarlos. La tabla 6 muestra la relación entre las mismas.

Tabla 6. Relación Amenaza – Vulnerabilidades. Elaborado por el autor.

Amenaza	Vulnerabilidad
• Manipulación de hardware / software	V1 Falla de hardware / software
• Uso no autorizado del equipo • Proceso ilegal de datos • Pérdida de confidencialidad	V2 Control de acceso no autorizado / inadecuado
• Acceso no autorizado al equipo • Escuchas • Espionaje remoto • Robo de información	V3 Conexión no autorizada al equipo V4 Uso no controlado/ impropio
• Interceptación pasiva de la información • Obtención de información extraída de	V5 Protección inadecuada de tráfico. Transferencia de información en texto

Amenaza	Vulnerabilidad
los paquetes que se transmiten por la red.	visible.

4.3 Relación Amenaza – Vulnerabilidad – Evento

Para poder trabajar con las matrices de riesgo (ver sección 4.6 Matrices), es necesario identificar los eventos que están relacionados con las amenazas y vulnerabilidades, para de esta manera tener un escenario de riesgo. Los eventos identificados en los diferentes estudios del estado del arte, así como su relación con las amenazas y vulnerabilidades, se detallan en la tabla 7.

Tabla 7. Amenaza – Vulnerabilidad – Evento. Elaborado por el autor.

Amenaza	Vulnerabilidad	Evento
• Manipulación de hardware / software	V1 Falla de hardware / software	Manipulación física del dispositivo, acceso al sistema operativo e instalación de malware (en modelos 2015-2016)
• Uso no autorizado del equipo • Proceso ilegal de datos • Pérdida de confidencialidad	V2 Control de acceso no autorizado / inadecuado	Personas no autorizadas pueden activar a Alexa a través de comandos de voz sean audibles o inaudibles.
• Acceso no autorizado al equipo	V3 Conexión no autorizada al equipo	Personas no autorizadas pueden conectarse al dispositivo vía bluetooth.

Amenaza	Vulnerabilidad	Evento
• Escuchas • Espionaje remoto • Robo de información • Interceptación pasiva de la información • Obtención de información extraída de los paquetes que se transmiten por la red.	V4 Uso no controlado/ impropio V5 Protección inadecuada de tráfico. Transferencia de información en texto visible.	Personas no autorizadas pueden monitorear el dispositivo y obtener acceso a información privada.

4.4 Criterios utilizados para el Análisis de Vulnerabilidades

Para llevar a cabo el análisis de vulnerabilidades, en primer lugar es necesario conocer la importancia que tienen los activos identificados por los usuarios, y así poder decidir sobre cuáles activos se llevará a cabo la gestión de riesgos, sobre el cual está basado el análisis de vulnerabilidades propuesto.

4.4.1 Valoración de los Activos

Una vez que han sido identificados los activos, es necesario conocer la importancia que tienen para los usuarios, es así como se lleva a cabo la valorización de los mismos. El rango de valoración empleado se detalla en la tabla 8.

Tabla 8. Rango de Valoración de Activos. Elaborado por el autor.

Valoración Numérica	Valoración	Descripción
1	Muy Bajo	El activo tiene un valor muy bajo para el usuario.
2	Bajo	El activo tiene un valor bajo para el usuario.
3	Medio	El activo tiene un valor medio para el usuario.
4	Alto	El activo tiene un valor alto para el usuario.
5	Muy Alto	El activo tiene un valor muy alto para el usuario.

Una vez definido el rango de valoración, se emplea la técnica de entrevista semiestructurada, con la participación de tres usuarios (ver Anexo 2. Entrevistas. Valoración Activos), y así conocer la importancia que tiene para ellos cada uno de los activos identificados.

Como se puede observar en la tabla 9, los activos: (A3) Conversaciones Privadas (valor 5) e (A1) Información Sensible Cuenta Amazon (valor 4.3), tienen la valoración más alta entre todos los activos por parte de los usuarios entrevistados.

Tabla 9. Valoración de Activos. Elaborado por el autor.

	ACTIVOS	Valor Activo	Calificación Usuario (1)	Calificación Usuario (2)	Calificación Usuario (3)
A1	Información sensible cuenta Amazon	4.3	5	4	4
A2	Transacciones en línea	3.3	3	3	4
A3	Conversaciones privadas	5	5	5	5
A4	Control de otros dispositivos	2.7	4	1	3

Sin embargo, el activo (A4) Control de Otros Dispositivos es considerado para el trabajo en las matrices, dada su importancia en la Internet de las Cosas (IoT).

4.4.2 Criterios de probabilidad de ocurrencia y valoración de impacto

Una vez que han sido identificadas las amenazas, vulnerabilidades y eventos de los dispositivos de reconocimiento de voz Amazon ECHO, es necesario realizar la estimación del riesgo, para lo cual se emplea una metodología cualitativa acompañada de una valoración numérica, la misma que utiliza dos criterios:

1. Criterio de probabilidad de ocurrencia
2. Criterio de valoración de impacto

En lo que refiere a la probabilidad de ocurrencia del evento en el que una amenaza explote una vulnerabilidad, se emplean los criterios de valoración detallados en la tabla 10.

Tabla 10. Criterios de probabilidad de ocurrencia de amenazas – vulnerabilidad – dispositivos Amazon ECHO. Elaborado por el autor.

Valoración Numérica	Probabilidad	Descripción
1	Muy Baja	Probabilidad muy baja de que una amenaza explote una vulnerabilidad.
2	Baja	Probabilidad baja de que una amenaza explote una vulnerabilidad.
3	Media	Probabilidad media de que una amenaza explote una vulnerabilidad.
4	Alta	Probabilidad alta de que una amenaza explote una vulnerabilidad.
5	Muy Alta	Probabilidad muy alta de que una amenaza explote una vulnerabilidad.

En lo que se refiere al impacto, los criterios de valoración para la disponibilidad, confiabilidad e integridad se detallan en la tabla 11.

Tabla 11. Criterios de valoración de impacto disponibilidad – confiabilidad – integridad – Amazon ECHO. Elaborado por el autor.

Valoración Numérica	**Impacto**	**Descripción**
1	Bajo	El impacto entre la disponibilidad, confiabilidad e integridad es bajo.
2	Medio	El impacto entre la disponibilidad, confiabilidad e integridad es medio.
3	Alto	El impacto entre la disponibilidad, confiabilidad e integridad es alto.

Los criterios de probabilidad de ocurrencia así como el impacto generado serán utilizados en las matrices de riesgos inherente y residual que se describen en la siguiente sección.

4.5 Matrices

Una vez valorizados los activos, establecidos los criterios de probabilidad e impacto, se procede a la elaboración de las matrices de riesgos inherente y residual. Para esto, se obtuvo la calificación para la probabilidad de ocurrencia y para el impacto generado (una por cada usuario, en total 3), por cada uno de los dos activos seleccionados, A3 y A4. Esto se logró a través de la entrevista semiestructurada (ver Anexo 2. Entrevistas. Probabilidad Ocurrencia e Impacto Generado). El promedio de las calificaciones obtenidas dieron como resultado, los valores finales para las dos variables en mención. Con estos valores, se procede con el cálculo del riesgo, para lo cual se utiliza la fórmula 2.

Fórmula 2. Cálculo del Riesgo. Elaborado por el autor.

$$R = P \times I$$

Donde: R = Riesgo. P = Probabilidad. I = Impacto.

Una vez calculado el riesgo, se necesita definir el valor cualitativo de la criticidad; para lo cual, a partir del resultado obtenido en el cálculo del riesgo, se establecen 3 rangos equitativamente distribuidos (cinco valores cada uno). Cuyo valor mínimo es uno (1) y valor máximo es quince (15), obteniendo de esta manera los tres valores cualitativos necesarios para la obtención de la criticidad. Bajo, medio y alto. La tabla 12 muestra los rangos establecidos y los valores de la criticidad en mención.

Tabla 12. Cálculo de la criticidad. Realizado por el autor.

Cálculo	Criticidad
Si el riesgo está entre 1 a 5	Bajo
Si el riesgo está entre 6 a 10	Medio
Si el riesgo está entre 11 a 15	Alto

4.5.1 Matriz de Riesgos Inherente

Una vez que se cuenta con el sistema de valoración, se procede a llenar dos matrices de Riesgos Inherente (para A3 y A4), las mismas que fueron adaptadas para medir el nivel de criticidad y el riesgo por cada uno de los activos seleccionados.

La matriz de riesgo 1 representa al activo (A3) y la matriz de riesgo 2 representa al activo (A4). Las mismas que contienen, todos los elementos anteriormente detallados en el modelo propuesto.

Matriz 1. Matriz de Riesgos Inherente – Conversaciones Privadas. Elaborado por el autor.

MATRIZ DE RIESGOS INHERENTE
DISPOSITIVOS DE RECONOCIMIENTO DE VOZ AMAZON ECHO "ALEXA"

Probabilidad de ocurrencia: 1 Muy baja, 2 Baja, 3 Media, 4 Alta, 5 Muy alta

Impacto: 1 Bajo, 2 Medio, 3 Alto

						CONVERSACIONES PRIVADAS		
						5		
EVENTO	**VALOR RIESGO**	**CRITICIDAD**	**PROBABILIDAD DE OCURRENCIA**	**IMPACTO**	**VOTO / CARGOS**	**Calificación Usuario Nro. 1**	**Calificación Usuario Nro. 2**	**Calificación Usuario Nro. 3**
Manipulación física del dispositivo,acceso al sistema operativo e instalación de malware para escucha de conversaciones (en modelos 2015-2016)	4	Bajo	1.3	3.0	VOTO IMPACTO	3.0	3.0	3.0
					VOTO PROBABILIDAD DE OCURRENCIA	1.0	1.0	2.0
Personas no autorizadas pueden activar a Alexa a través de comandos de voz sean audibles o inaudibles para escucha de conversaciones.	12	Alto	4.0	3.0	VOTO IMPACTO	3.0	3.0	3.0
					VOTO PROBABILIDAD DE OCURRENCIA	3.0	5.0	4.0
Personas no autorizadas pueden conectarse al dispositivo vía bluetooth, para escucha de conversaciones	12	Alto	4.0	3.0	VOTO IMPACTO	3.0	3.0	3.0
					VOTO PROBABILIDAD DE OCURRENCIA	4.0	3.0	5.0
Personas no autorizadas pueden monitorear el dispositivo y obtener acceso a conversaciones privadas.	12	Alto	4.0	3.0	VOTO IMPACTO	3.0	3.0	3.0
					VOTO PROBABILIDAD DE OCURRENCIA	4.0	5.0	3.0

Matriz 2. Matriz de Riesgos Inherente – Control de Otros Dispositivos. Elaborado por el autor.

MATRIZ DE RIESGOS INHERENTE
DISPOSITIVOS DE RECONOCIMIENTO DE VOZ AMAZON ECHO "ALEXA"

Probabilidad de ocurrencia: 1 Muy baja, 2 Baja, 3 Media, 4 Alta, 5 Muy alta

Impacto: 1 Bajo, 2 Medio, 3 Alto

						CONTROL DE OTROS DISPOSITIVOS		
						2.67		
EVENTO	**VALOR RIESGO**	**CRITICIDAD**	**PROBABILIDAD DE OCURRENCIA**	**IMPACTO**	**VOTO / CARGOS**	**Calificación Usuario Nro. 1**	**Calificación Usuario Nro. 2**	**Calificación Usuario Nro. 3**
Manipulación física,acceso al sistema operativo e instalación de malware, para control de otros dispositivos inteligentes en casa.	3	Bajo	1.0	3.0	VOTO IMPACTO	3.0	3.0	3.0
					VOTO PROBABILIDAD DE OCURRENCIA	1.0	1.0	1.0
Personas no autorizadas pueden activar a Alexa a través de comandos de voz sean audibles o inaudibles, para control de otros dispositivos intelegentes en casa.	12	Alto	4.7	2.7	VOTO IMPACTO	3.0	2.0	3.0
					VOTO PROBABILIDAD DE OCURRENCIA	5.0	5.0	4.0
Personas no autorizadas pueden conectarse al dispositivo vía bluetooth, para control de otros dispositivos en casa.	12	Alto	4.0	3.0	VOTO IMPACTO	3.0	3.0	3.0
					VOTO PROBABILIDAD DE OCURRENCIA	2.0	5.0	5.0
Personas no autorizadas pueden monitorear el dispositivo y obtener acceso al mismo para control de otros dispositivos en casa.	12	Alto	4.3	2.7	VOTO IMPACTO	3.0	3.0	2.0
					VOTO PROBABILIDAD DE OCURRENCIA	4.0	5.0	4.0

4.5.2 Matriz de Riesgos Residual

Al igual que en el caso de la matriz de riesgos inherente, se elaboran dos matrices de riesgo residual, una por cada activo seleccionado (A3 y A4). Para este caso, es necesario la identificación y selección de los controles de seguridad que serán utilizados como contramedidas para la mitigación de los riesgos encontrados.

En el modelo propuesto, la norma ISO 27002 proporciona la guía de los controles que pueden ser considerados para identificar, evaluar y mitigar los riesgos encontrados. Es decir, que a través del uso de éste estándar de seguridad, se pueden seleccionar los controles para el mejoramiento de las prácticas de seguridad.

Los dominios de la ISO 27002:2013 utilizados para la identificación de los controles en el modelo propuesto son los siguientes:

- Clausula 9: Control de Acceso.
- Clausula 12: Seguridad en la Operativa.
- Clausula 13: Seguridad en las Telecomunicaciones.
- Clausula 14: Adquisición, Desarrollo, y Mantenimiento de los Sistemas de Información.
- Clausula 15: Relaciones con Suministradores.
- Clausula 16: Gestión de Incidentes en la Seguridad de la Información.
- Clausula 18: Cumplimiento.

Adicionalmente, la descripción de los controles de seguridad identificados dentro de cada dominio se detalla en la tabla 13. La descripción de los controles pertenece a la norma ISO27002 (ISO/IEC 27002, 2013)

Tabla 13. Vulnerabilidad – Evento- Control ISO27002:2013. Elaborado por el autor.

Control ISO 27002	**Descripción**
V1 Falla de hardware / software	
12.6.1 Gestión de las vulnerabilidades técnicas.	Se debería obtener información sobre las vulnerabilidades técnicas de los sistemas de información de manera oportuna para evaluar el grado de exposición de la organización y tomar las medidas necesarias para abordar los riesgos asociados.
12.2.1 Controles contra el código malicioso.	Se deberían implementar controles para la detección, prevención y recuperación ante afectaciones en combinación con la concientización adecuada de los usuarios.
9.4.2 Procedimientos seguros de inicio de sesión.	Cuando sea requerido por la política de control de accesos se debería controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de *log-on*.
18.2.2 Cumplimiento de las políticas y normas de seguridad.	Los gerentes deberán revisar regularmente el cumplimiento del procesamiento y los procedimientos de información dentro de su área de responsabilidad respecto a las políticas, normas y cualquier otro tipo de requisito de seguridad correspondiente.
V2 Control de acceso no autorizado / inadecuado	
9.1.1 Política de control de acceso.	Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.
9.2.2 Gestión de los derechos de acceso asignados a usuarios.	Se debería implantar un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios.

Control ISO 27002	Descripción
9.2.3 Gestión de los derechos de acceso con privilegios especiales.	La asignación y uso de derechos de acceso con privilegios especiales debería ser restringido y controlado.
9.2.4 Gestión de información confidencial de autenticación de usuarios.	La asignación de información confidencial para la autenticación debería ser controlada mediante un proceso de gestión controlado.
9.2.5 Revisión de los derechos de acceso de los usuarios.	Los propietarios de los activos deberían revisar con regularidad los derechos de acceso de los usuarios.
9.2.6 Retirada o adaptación de los derechos de acceso.	Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio.
9.3.1 Uso de información confidencial para la autenticación.	Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad de la organización en el uso de información confidencial para la autenticación.
9.4.3 Gestión de contraseñas de usuario.	Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar contraseñas de calidad.
18.2.2 Cumplimiento de las políticas y normas de seguridad.	Los gerentes deberán revisar regularmente el cumplimiento del procesamiento y los procedimientos de información dentro de su área de responsabilidad respecto a las políticas, normas y cualquier otro tipo de requisito de seguridad correspondiente.

Control ISO 27002	Descripción
V3 Conexión no autorizada al equipo	
9.1.1 Política de control de acceso.	Se debería establecer, documentar y revisar una política de control de accesos en basa a las necesidades de seguridad y de negocio de la Organización.
9.2.6 Retirada o adaptación de los derechos de acceso.	Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio.
9.3.1 Uso de información confidencial para la autenticación.	Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad de la organización en el uso de información confidencial para la autenticación.
9.4.3 Gestión de contraseñas de usuario.	Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar contraseñas de calidad.
12.4.1 Registro y gestión de eventos de actividad.	Se deberían producir, mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información.
14.1.2 Seguridad de las comunicaciones y servicios accesibles por redes públicas.	La información de los servicios de aplicación que pasan a través de redes públicas se debería proteger contra actividades fraudulentas, de disputa de contratos y/o de modificación no autorizada.
18.2.2 Cumplimiento de las políticas y normas de seguridad.	Los gerentes deberán revisar regularmente el cumplimiento del procesamiento y los procedimientos de información dentro de su área de responsabilidad respecto a las políticas, normas y

Control ISO 27002	Descripción
	cualquier otro tipo de requisito de seguridad correspondiente.
V4 Uso no controlado / impropio	
V5 Protección inadecuada de tráfico. Transferencia de información en texto visible	
13.1.2 Mecanismos de seguridad asociados a servicios de red.	Se deberían identificar e incluir en los acuerdos de servicio (SLA) los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se entregan de manera interna o están externalizados.
13.2.1 Políticas y procedimientos de intercambio de información.	Deben existir políticas, procedimientos y controles formales de transferencia para proteger la información que viaja a través del uso de todo tipo de instalaciones de comunicación.
13.2.4 Acuerdos de confidencialidad y secreto.	Se deberían identificar, revisar y documentar de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la organización para la protección de la información.
14.1.2 Seguridad de las comunicaciones y servicios accesibles por redes públicas.	La información de los servicios de aplicación que pasan a través de redes públicas se debería proteger contra actividades fraudulentas, de disputa de contratos y/o de modificación no autorizada.
14.1.3 Protección de las transacciones por redes telemáticas.	La información en transacciones de servicios de aplicación se debería proteger para evitar la transmisión y enrutamiento incorrecto y la alteración, divulgación y/o duplicación no autorizada de mensajes o su reproducción.

Control ISO 27002	Descripción
15.2.1 Supervisión y revisión de los servicios prestados por terceros.	Las organizaciones deberían monitorear, revisar y auditar la presentación de servicios del proveedor regularmente.
18.1.4 Protección de datos y privacidad de la información personal.	Se debería garantizar la privacidad y la protección de la información personal identificable según requiere la legislación y las normativas pertinentes aplicables que correspondan.
18.2.2 Cumplimiento de las normas y políticas de seguridad.	Los gerentes deberán revisar regularmente el cumplimiento del procesamiento y los procedimientos de información dentro de su área de responsabilidad respecto a las políticas, normas y cualquier otro tipo de requisito de seguridad correspondiente.

Una vez identificados los controles de seguridad que van a ser aplicados para mitigar los riesgos ocasionados por la explotación de las vulnerabilidades encontradas a través de las amenazas, se procede identificar controles sugeridos a los usuarios en base a los controles identificados en la norma ISO 27002. Estos controles ayudarán a los usuarios a tomar medidas para reforzar la seguridad en sus activos. La tabla 14 muestra los riesgos, los controles de la ISO27002 y los controles sugeridos para el usuario.

Tabla 14. Evento – Control ISO 27002 – Control Sugerido. Elaborado por el autor.

Evento	Control ISO 27002	Control sugerido
Manipulación física del dispositivo, acceso al sistema operativo e instalación de malware (en modelos 2015-2016).	12.6.1 Gestión de las vulnerabilidades técnicas. 12.2.1 Controles contra el código malicioso. 9.4.2 Procedimientos seguros de inicio de sesión.	• Cambiar el modelo de Alexa. • Y/o mantener un control físico de sello de seguridad y monitorear.

Evento	Control ISO 27002	Control sugerido
	18.2.2 Cumplimiento de las políticas y normas de seguridad.	
Personas no autorizadas pueden activar a Alexa a través de comandos de voz sean audibles o inaudibles.	9.1.1 Política de control de acceso. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.2.5 Revisión de los derechos de acceso de los usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso. 9.3.1 Uso de información confidencial para la autenticación.	• Cambiar la palabra de activación. • Crear un *profile* de voz en Alexa • Revisar el histórico de las interacciones de voz con Alexa. • Habilitar solo los *Skills* que voy a utilizar en Alexa. • Poner en off la opción *Drop in* (todo esto desde Alexa app). • Poner en silencio el botón del micrófono de Alexa. • Ubicar el dispositivo en un lugar estratégico en casa (no cerca de ventanas, puertas, televisor, etc.). • Leer las condiciones de uso y noticias de privacidad de los *Skills* habilitados. • Y/o mantener siempre

Evento	Control ISO 27002	Control sugerido
	9.4.3 Gestión de contraseñas de usuario. 18.2.2 Cumplimiento de las políticas y normas de seguridad.	actualizado el *firmware* de Alexa
Personas no autorizadas pueden conectarse al dispositivo vía bluetooth.	9.1.1 Política de control de acceso. 9.2.6 Retirada o adaptación de los derechos de acceso. 9.3.1 Uso de información confidencial para la autenticación. 9.4.3 Gestión de contraseñas de usuario. 12.4.1 Registro y gestión de eventos de actividad. 14.1.2 Seguridad de las comunicaciones y servicios accesibles por redes públicas. 18.2.2 Cumplimiento de las políticas y normas de seguridad.	• Tener una red Wi-Fi segura en casa (con contraseña robusta). • Conectar el dispositivo Alexa solo a redes Wi-Fi seguras. • Revisar el histórico de las conexiones Wi-Fi y Bluetooth realizadas a Alexa. • Crear un *profile* de voz en Alexa. • Poner en off la opción *Drop in* (todo esto desde *Alexa app*). • Y/o mantener siempre actualizado el *firmware* de Alexa.
Personas no autorizadas	13.1.2 Mecanismos de	• Poner en silencio el botón del

Evento	Control ISO 27002	Control sugerido
pueden monitorear el dispositivo y obtener acceso a conversaciones privadas.	seguridad asociados a servicios de red. 13.2.1 Políticas y procedimientos de intercambio de información. 13.2.4 Acuerdos de confidencialidad y secreto. 14.1.2 Seguridad de las comunicaciones y servicios accesibles por redes públicas. 14.1.3 Protección de las transacciones por redes telemáticas. 15.2.1 Supervisión y revisión de los servicios prestados por terceros. 18.1.4 Protección de datos y privacidad de la información personal. 18.2.2 Cumplimiento de las políticas y normas de seguridad.	micrófono de Alexa. • Borrar el histórico de lo realizado con Alexa. • Revisar el histórico de conexiones Wi-Fi y Bluetooth (todo esto desde *Alexa app*). • Mantener siempre actualizado el firmware de Alexa. • Leer sobre las políticas y términos de uso de los *Skills* habilitados. • Y/o ubicar el dispositivo en un lugar estratégico en casa (no cerca de ventanas, puertas, televisor, etc.)

Una vez identificados los controles dentro de la norma ISO27002 y definidos los controles sugeridos, se procede con el trabajo en la matriz de riesgo residual. Para obtener la nueva calificación, se volvió a preguntar a los usuarios a través de la entrevista semiestructurada, sobre el valor de la probabilidad de ocurrencia, para los dos activos A3 y A4, pero esta vez considerando el control de seguridad sugerido. Con lo que, se obtuvieron los nuevos valores para las columnas de probabilidad de ocurrencia y criticidad. La matriz 3 muestra los valores de la matriz residual para el activo A3, y la matriz 4 muestra los valores para el activo A4. Es necesario indicar, que el valor del impacto generado se mantiene igual que en las matrices de riesgo inherente. Por último, se mantiene la columna de criticidad de la matriz inherente en las matrices de riesgo residuales, para poder observar el cambio de criticidad una vez considerados los controles de seguridad.

Matriz 3. Matriz de Riesgos Residual – Conversaciones Privadas. Elaborado por el autor.

MATRIZ DE RIESGOS RESIDUAL (CON CONTROLES)

DISPOSITIVOS DE RECONOCIMIENTO DE VOZ AMAZON ECHO "ALEXA"

Probabilidad de ocurrencia: 1 Muy baja, 2 Baja, 3 Media, 4 Alta, 5 Muy alta

Impacto: 1 Bajo, 2 Medio, 3 Alto

										CONVERSACIONES PRIVADAS		
										5		
EVENTO	CONTROL ISO/IEC 27002		CONTROL SUGERIDO	VALOR RIESGO	CRITICIDAD INHERENTE	CRITICIDAD RESIDUAL	PROB OCURR.	IMPACTO	VOTO / CARGOS	Calificación Usuario Nro. 1	Calificación Usuario Nro.2	Calificación Usuario Nro. 3
Manipulación fisica del dispositivo, acceso al sistema operativo e instalación de malware, para escucha de conversaciones (en modelos 2015-2016).	12.6.1	Gestión de las vulnerabilidades técnicas	* Cambiar el modelo de Alexa. * Y/o mantener un control físico de sello de seguridad y monitorear.	3	Bajo	Bajo	1.0	3.0	VOTO IMPACTO	3.0	3.0	3.0
	12.2.1	Controles contra de código malicioso.							VOTO PROBABILIDAD DE OCURRENCIA	1.0	1.0	1.0
	9.4.2	Procedimientos seguros de inicio de sesión.										
	18.2.2	Cumplimiento de las normas y políticas de seguridad.										
Personas no autorizadas pueden activar a Alexa a través de comandos de voz sean audibles o inaudibles para escucha de conversaciones.	9.1.1	Políticas de control de accesos.	* Cambiar palabra de activación. * Crear un profile de voz en Alexa. * Revisar el histórico de las interacciones de voz con Alexa. * Habilitar solo los skills que voy a utilizar en Alexa. * Poner en off la opción Drop in (todo esto desde Alexa app). * Poner en silencio el botón del micrófono de Alexa. * Ubicar el dispositivo en un lugar estratégico en casa (no cerca de ventanas, puertas, televisor,etc.) * Leer las condiciones de uso y noticias de privacidad de los skils habilitados. * Y/o mantener siempre actualizado el firmware de Alexa.	4	Alto	Bajo	1.3	3.0	VOTO IMPACTO	3.0	3.0	3.0
	9.2.2	Gestión de los derechos de acceso asignados a usuarios.							VOTO PROBABILIDAD DE OCURRENCIA	1.0	1.0	2.0
	9.2.3	Gestión de los derechos de acceso con privilegios especiales.										
	9.2.4	Gestión de información confidencial de autenticación de usuarios.										
	9.2.5	Revisión de los derechos de acceso de los usuarios.										
	9.2.6	Retirada o adaptación de los derechos de acceso.										
	9.3.1	Uso de información confidencial para la autenticación.										
	9.4.3	Gestión de contraseñas de usuario.										
	18.2.2	Cumplimiento de las normas y políticas de seguridad.										

EVENTO	CONTROL ISO/IEC 27002		CONTROL SUGERIDO	VALOR RIESGO	CRITICIDAD INHERENTE	CRITICIDAD RESIDUAL	PROB OCURR.	IMPACTO	VOTO / CARGOS	Calificación Usuario Nro. 1	Calificación Usuario Nro.2	Calificación Usuario Nro. 3
Personas no autorizadas pueden conectarse al dispositivo vía bluetooth, para escucha de conversaciones	9.1.1	Políticas de control de acceso.	* Tener una red Wi-Fi segura en casa(con contraseña robusta). * Conectar el dispositivo Alexa solo a redes Wi-Fi seguras. * Revisar el histórico de las conexiones Wi-Fi y Bluetooth realizadas a Alexa. * Crear un profile de voz en Alexa. * Poner en off la opción Drop in (todo esto desde Alexa app). * Y/o mantener simpre actualizado el firmware de Alexa.	10	Alto	Medio	3.3	3.0	VOTO IMPACTO	3.0	3.0	3.0
	9.2.6	Retirada o adaptación de los derechos de acceso.							VOTO PROBABILIDAD DE OCURRENCIA	3.0	4.0	3.0
	9.3.1	Uso de información confidencial para la autenticación.										
	9.4.3	Gestión de contraseñas de usuario.										
	12.4.1	Registro y gestión de eventos de actividad.										
	14.1.2	Seguridad de las comunicaciones y servicios accesibles por redes públicas.										
	18.2.2	Cumplimiento de las normas y políticas de seguridad.										
Personas no autorizadas pueden monitorear el dispositivo y obtener acceso a conversaciones privadas.	13.1.2	Mecanismos de seguridad asociados a servicios de red.	* Poner en silencio el botón del micrófono de Alexa. * Borrar el histórico de lo realizado con Alexa. * Revisar el histórico de conexiones Wi-Fi y Bluetooth (todo esto desde Alexa app). * Mantener siempre actualizado el firmware de Alexa * Leer sobre las políticas y términos de uso de los skills habilitados. * Y/o ubicar el dispositivo en un lugar estratégico en casa (no cerca de ventanas, puertas, televisor,etc).	7	Alto	Medio	2.3	3.0	VOTO IMPACTO	3.0	3.0	3.0
	13.2.1	Políticas y procedimientos de intercambio de información.							VOTO PROBABILIDAD DE OCURRENCIA	3.0	2.0	2.0
	13.2.4	Acuerdos de confidencialidad y secreto										
	14.1.2	Seguridad de las comunicaciones y servicios accesibles por redes públicas.										
	14.1.3	Protección de las transacciones por redes										
	15.2.1	Supervisión y revisión de los servicios prestados por terceros.										
	18.1.4	Protección de datos y privacidad de la información										
	18.2.2	Cumplimiento de las normas y políticas de seguridad.										

Matriz 4. Matriz de Riesgos Residual – Control de Otros Dispositivos. Elaborado por el autor.

MATRIZ DE RIESGOS RESIDUAL (CON CONTROLES)

DISPOSITIVOS DE RECONOCIMIENTO DE VOZ AMAZON ECHO "ALEXA"

Probabilidad de ocurrencia: 1 Muy baja, 2 Baja, 3 Media, 4 Alta, 5 Muy alta

Impacto: 1 Bajo, 2 Medio, 3 Alto

										CONTROL DE OTROS DISPOSITIVOS		
										2.7		
EVENTO	**CONTROL ISO/IEC 27002**		**CONTROL SUGERIDO**	**VALOR RIESGO**	**CRITICIDAD INHERENTE**	**CRITICIDAD RESIDUAL**	**PROB OCURR.**	**IMPACTO**	**VOTO / CARGOS**	**Calificación Usuario Nro. 1**	**Calificación Usuario Nro.2**	**Calificación Usuario Nro.3**
Manipulación fisica del dispositivo, acceso al sistema operativo e instalación de malware, para control de otros dispositivos inteligentes en casa (en modelos 2015-2016).	12.6.1	Gestión de las vulnerabilidades técnicas	Cambiar el modelo de Alexa y/o mantener un control físico de sello de seguridad y monitorear	3	Bajo	Bajo	1.0	3.0	VOTO IMPACTO	3.0	3.0	3.0
	12.2.1	Controles contra de código malicioso.							VOTO PROBABILIDAD DE OCURRENCIA	1.0	1.0	1.0
	9.4.2	Procedimientos seguros de inicio de sesión.										
	18.2.2	Cumplimiento de las normas y políticas de seguridad.										
Personas no autorizadas pueden activar a Alexa a través de comandos de voz sean audibles o inaudibles, para control de otros dispositivos inteligentes en casa.	9.1.1	Políticas de control de accesos.	* Cambiar palabra de activación. * Crear un profile de voz en Alexa. * Revisar el histórico de las interacciones de voz con Alexa. * Habilitar solo los skills que voy a utilizar en Alexa. * Poner en off la opción Drop in (todo esto desde Alexa app). * Poner en silencio el botón del micrófono de Alexa. * Ubicar el dispositivo en un lugar estratégico en casa (no cerca de ventanas, puertas, televisor,etc.) * Leer las condiciones de uso y noticias de privacidad de los skils habilitados. * Y/o mantener siempre actualizado el firmware de Alexa.	4	Alto	Bajo	1.7	2.7	VOTO IMPACTO	3.0	2.0	3.0
	9.2.2	Gestión de los derechos de acceso asignados a usuarios.							VOTO PROBABILIDAD DE OCURRENCIA	1.0	2.0	2.0
	9.2.3	Gestión de los derechos de acceso con privilegios especiales.										
	9.2.4	Gestión de información confidencial de autenticación de usuarios.										
	9.2.5	Revisión de los derechos de acceso de los usuarios.										
	9.2.6	Retirada o adaptación de los derechos de acceso.										
	9.3.1	Uso de información confidencial para la autenticación.										
	9.4.3	Gestión de contraseñas de usuario.										
	18.2.2	Cumplimiento de las normas y políticas de seguridad.										

EVENTO	CONTROL ISO/IEC 27002		CONTROL SUGERIDO	VALOR RIESGO	CRITICIDAD INHERENTE	CRITICIDAD RESIDUAL	PROB OCURR.	IMPACTO	VOTO / CARGOS	Calificación Usuario Nro. 1	Calificación Usuario Nro.2	Calificación Usuario Nro.3
Personas no autorizadas pueden conectarse al dispositivo vía bluetooth, para control de otros dispositivos inteligentes en casa.	9.1.1	Políticas de control de acceso.	* Tener una red Wi-Fi segura en casa(con contraseña robusta). * Conectar el dispositivo Alexa solo a redes Wi-Fi seguras. * Revisar el histórico de las conexiones Wi-Fi y Bluetooth realizadas a Alexa. * Crear un profile de voz en Alexa. * Poner en off la opción Drop in (todo esto desde Alexa app). * Y/o mantener simpre actualizado el firmware de Alexa.	4	Alto	Bajo	1.3	3.0	VOTO IMPACTO	3.0	3.0	3.0
	9.2.6	Retirada o adaptación de los derechos de acceso.							VOTO PROBABILIDAD DE OCURRENCIA	1.0	1.0	2.0
	9.3.1	Uso de información confidencial para la autenticación.										
	9.4.3	Gestión de contraseñas de usuario.										
	12.4.1	Registro y gestión de eventos de actividad.										
	14.1.2	Seguridad de las comunicaciones y servicios accesibles por redes públicas.										
	18.2.2	Cumplimiento de las normas y políticas de seguridad.										
Personas no autorizadas pueden monitorear el dispositivo y obtener acceso al mismo para control de otros dispositivos en casa.	13.1.2	Mecanismos de seguridad asociados a servicios de red.	* Poner en silencio el botón del micrófono de Alexa. * Borrar el histórico de lo realizado con Alexa. * Revisar el histórico de conexiones Wi-Fi y Bluetooth (todo esto desde Alexa app). * Mantener siempre actualizado el firmware de Alexa * Leer sobre las políticas y términos de uso de los skills habilitados. * Y/o ubicar el dispositivo en un lugar estratégico en casa (no cerca de ventanas, puertas, televisor,etc).	6	Alto	Medio	2.3	2.7	VOTO IMPACTO	3.0	3.0	2.0
	13.2.1	Políticas y procedimientos de intercambio de información.							VOTO PROBABILIDAD DE OCURRENCIA	3.0	2.0	2.0
	13.2.4	Acuerdos de confidencialidad y secreto										
	14.1.2	Seguridad de las comunicaciones y servicios accesibles por redes públicas.										
	14.1.3	Protección de las transacciones por redes telemáticas.										
	15.2.1	Supervisión y revisión de los servicios prestados por terceros.										
	18.1.4	Protección de datos y privacidad de la información personal.										
	18.2.2	Cumplimiento de las normas y políticas de seguridad.										

CAPÍTULO V

RESULTADOS

5.1 Conclusiones

El modelo de seguridad planteado se apoya en la familia de las normas ISO con un enfoque diferente en el que generalmente se utiliza, como es el de la seguridad en una organización. Se cambia el enfoque y se hace énfasis en el punto de vista del usuario y su papel protagónico en el cuidado de los activos que se encuentran en su entorno familiar. Con esto se logra que el usuario conozca sobre la importancia de la seguridad de su información así como su responsabilidad en el cuidado de la misma.

Es necesario indicar que la norma ISO/IEC 27005 proporciona las directrices y lineamientos para llevar a cabo una gestión de riesgos efectiva. Un aspecto interesante que se debe rescatar, es la fusión existente con las normas ISO27001, que proporciona la guía base para diagnosticar la situación actual, y la ISO27002, que proporciona los controles de seguridad necesarios a ser aplicados.

Sin embargo, los dispositivos Amazon ECHO, Alexa, están ligados a una cuenta de la empresa Amazon, con lo que no hay dueño de la información. Esto hace difícil que se puedan aplicar normas de la familia 27000, ya que estas piden la definición del dueño del activo de información, el mismo que será el encargado de administrar los accesos.

Por otro lado, el modelo de seguridad planteado muestra la necesidad que tienen los usuarios de proteger el entorno actual en el que interactúan con dispositivos como

"Alexa". Es importante resaltar que los entornos en referencia son ambientes íntimos como nuestros hogares u oficinas privadas, en dónde no basta tener al alcance funcionalidades que faciliten algunas actividades y proporcionen comodidad; sino que necesitamos garantizar su seguridad. Sobre todo al tener un asistente inteligente que tiene la capacidad de hacer cosas por nosotros, interactuar y manejar otros dispositivos inteligentes en casa, sin que esto implique ningún nivel de intromisión, monitoreo que vulnere o ponga en peligro nuestra privacidad.

Es más, a través del modelo propuesto, el usuario tiene la posibilidad de sugerir a la empresa Amazon, tener una visión de seguridad en los dispositivos Amazon ECHO no solamente desde el punto de vista técnico, sino desde el punto de vista del usuario. Se debe recordar, que no basta la implementación de seguridad únicamente en procesos y tecnología; los usuarios hoy en día son parte esencial de una implementación de seguridad más integral.

Cabe resaltar, que la opinión del usuario es importante y siempre tendrá un peso significativo en el avance de la tecnología. Al igual que su compromiso y actuación frente a los problemas de seguridad que el uso de los mismos puede acarrear.

Más aún, al hablar de los activos del usuario en su entorno familiar al manejar Alexa, resulta interesante observar que a ellos les interesa más que estén escuchando las conversaciones que mantienen en casa, a que les roben. Por lo que, se puede evidenciar que la privacidad de las personas, independientemente de su estatus, es lo que más importa.

También resulta atractivo ver el cambio de la criticidad mostrada en la matriz de riesgos inherente (que fluctúa de media a alta), y la criticidad en la matriz de riesgos residual (baja) una vez sugeridos los controles que puede adoptar el usuario. Lo que

evidencia que al tener controles de seguridad, la probabilidad de que una amenaza explote una vulnerabilidad disminuirá.

Por último, esta investigación sirve como referencia para otros estudios que se lleven a cabo en el país. Pese a que en el Ecuador, el uso de este tipo de asistentes personales, como lo es Amazon ECHO, Alexa, está iniciando, en algún momento este tipo de tecnología estará presente en los hogares ecuatorianos, y es necesario conocer cómo usarla de una manera responsable, sin poner en riesgo nuestra privacidad y seguridad.

5.2 Recomendaciones

Si bien es cierto que la compañía Amazon ha vendido más de 18 millones de dispositivos Amazon ECHO, lo que los convierte en el líder de ventas en el mercado actual. A más de las funcionalidades que ha implementado en estos dispositivos, se sugiere que el aumento de las funcionalidades vaya de la mano con la seguridad para el uso de los mismos.

Adicional a esto, se sugiere que la empresa Amazon, tome en consideración las recomendaciones que hacen sus usuarios, a través del modelo de seguridad planteado; tal como lo ha venido realizando en el aspecto de las funcionalidades implementadas (creadas por terceros). Se plantea la necesidad de que la empresa Amazon, visualice a la seguridad en este tipo de dispositivos inteligentes de reconocimiento de voz, como una funcionalidad básica que debe estar incorporada y disponible a todos sus usuarios.

Por último, no es suficiente el que se adopten y apliquen controles de seguridad propuestos. Es necesario dar un seguimiento oportuno y eficiente a los controles una vez implementados, con el fin de saber si se tiene una protección efectiva. Es necesario indicar, que así como la tecnología avanza, también las nuevas formas de ataques que presentan nuevas amenazas, ante los cuales todos debemos estar preparados.

5.3 Trabajos a Futuro

En lo que se refiere a la experimentación desarrollada en el presente trabajo, para los ataques a través de comandos inaudibles de voz, no solamente para Amazon, sino para todos los fabricantes de este tipo de dispositivos inteligentes; se plantea la necesidad de un trabajo técnico que ayude a brindar una solución. Para el caso de los nuevos modelos de éstos dispositivos, el cambio de hardware de los micrófonos para reducir la sensibilidad de las ondas emisoras de ultrasonido, puede ser una solución viable. Sin embargo, para los modelos ya existentes en el mercado actual, se plantea la necesidad de desarrollar filtros (desarrollo de software), que permitan diferenciar a los comandos inaudibles de los audibles, permitiendo así solo la emisión de frecuencias deseadas, evitando de esta manera ataques de este estilo por parte de *hackers* o personas mal intencionadas.

Finalmente, el modelo planteado sirve como base para la realización de otros modelos de seguridad, los mismos que pueden abarcar la implementación de los controles identificados y sugeridos, así como también el respectivo seguimiento y control. Todo esto, con el fin de proporcionar una seguridad integral para cualquier ambiente en el que éste sea considerado.

Lista de Referencias

Alhadlaq, A., Tang, J., Almaymoni, M., & Korolova, A. (2017). Privacy in the Amazon Alexa Skills Ecosystem. *Proceedings on Privacy Enhancing Technologies (PoPETs)*.

Amazon. (2017). *Alexa Skills Kit*. Retrieved from Amazon: https://developer.amazon.com/alexa-skills-kit

Amazon. (2017). *Amazon Privacy Notice*. Retrieved from Amazon: https://www.amazon.com/gp/help/customer/display.html?nodeId=468496

Amazon. (2017). *AWS*. Retrieved from AWS Lambda: https://aws.amazon.com/es/lambda/

Amazon. (2017). *Echo & Alexa Devices.* Retrieved from Amazon: https://www.amazon.com/Amazon-Echo-And-Alexa-Devices/b/ref=sv_devicesubnav_0?ie=UTF8&node=9818047011

Amazon Developer. (2017). *Alexa Blogs*. Retrieved from The Advantages of Using Piezoelectric MEMS Microphones in Your Alexa-Enabled Product: https://developer.amazon.com/blogs/alexa/post/bcef47f5-f1ca-4614-8a57-6af7eabfd1eb/the-advantages-of-using-piezoelectric-mems-microphones-in-your-alexa-enabled-product. Access Date (2017, 09 20)

Amazon Developer. (2017). *Alexa Voice Service.* Retrieved from Amazon Developer: https://developer.amazon.com/alexa-voice-service

Amazon Developer. (2018). *Connected Devices*. Retrieved from Connect Your Devices to Alexa: https://developer.amazon.com/alexa/connected-devices. Access Date (2018, 01 16).

Amazon Inc. (2018). *Communication Protocols*. Retrieved from Home Automation: Communication Protocols: https://www.amazon.com/Communication-Protocols-Guide/b?ie=UTF8&node=10533375011. Access Date (2018, 01 16).

Apthorpe, N., Reisman, D., & Feamster, N. (2017). *A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic.* Retrieved from ARXIV: https://arxiv.org/pdf/1705.06805.pdf

Asamblea Constituyente. (2015). Contitución de la Repúbllica del Ecuador. Capítulo sexto. Derechos de libertad Art. 66.- Numeral 19. Pag.49. Ecuador.

Asamblea Nacional del Ecuador. (2014, February 10). Código Orgánico Integral Penal (COIP). Sección Tercera, Delitos contra la seguridad de los activos de los sistemas de información y comunicación. Artículo 230.-. Numeral 1. Pag. 37. *Suplemento Registro Oficial No. 180*. Quito, Pichincha, Ecuador.

Atzori, L., Iera, A., & Morabito, G. (2010, October 28). *The Internet of Things: A survey. Computer networks.* Retrieved from Science Direct: http://www.sciencedirect.com/science/article/pii/S1389128610001568

Audacity. (2017). *Audacity*. Retrieved from Audacity: https://www.audacityteam.org/

Barnes, M. (2017). *Alexa, Are you listening?* Retrieved from Labs MWRInfoSecurity: https://labs.mwrinfosecurity.com/blog/alexa-are-you-listening

Bhattacharya, A. (2017). *Amazon's Alexa Accidentally Ordered a Ton of Dollhouse across San Diego*. Retrieved from QUARTZ: https://qz.com/880541/amazons-amzn-alexa-accidentally-ordered-a-ton-ofdollhouses-across-san-diego/

Bolt, R. (1980). "Put-That-There: Voice and Gesture at the Graphics Interface". *Proceedings of the 7th annual conference on Computer graphics and interactive techniques.*

Cao Avellaneda, J. (2008, June 10). *Publicada la ISO 27005:2008.* Retrieved from Gobierno de la Ciberseguridad: http://seguridad-de-la-informacion.blogspot.com/2008/06/publicada-la-iso-270052008.html

Cendón, B. (2017). *El origen del IoT*. Retrieved from Bruno Cendón Pensamientos y Tecnología: http://www.bcendon.com/el-origen-del-iot/ Access Date (2017, 01 16)

Centro Humbolt. (2004, June). El ABC de la Gestión de Riesgos. *El ABC de la Gestión de Riesgos*. Centro Humbolt.

Chakrabarti, A. (2017, February 9). Amazon alexa - building custom skills.

Chung, H., Iorga, M., & Voas, J. (2017, September 22). "Alexa, Can I trust You?". *IEEE Computer Society*, *50*(9, 2017), 100-104. doi:10.1109/MC.2017.3571053

Clinton, I., Cook, L., & Banik, S. (2017). *A Survey of Various Methods for Analyzing the Amazon Echo.* Retrieved from https://vanderpot.com/Clinton_Cook_Paper.pdf

Consumer Intelligence Research Partners, LLC. (CIRP). (2017, May 8). *Amazon Echo Dot Drives Fast Growth.* Chicago: Consumer Intelligence Research Partners, LLC.

Cusack, B., & Khaleghparast, R. (2016). A privacy gap around the internet of things for open-source projects. *The Proceedings of 14th Australian Information Security Management Conference* (pp. 14-20). Perth, Western Australia: Edith Cowan Universit. Retrieved from AUSTRALIAN INFORMATION SECURITY MANAGEMENT CONFERENCE: http://ro.ecu.edu.au/ism/191/

Dewri, A., Nguyen, A., Chen, F., Lin, M., & Gupta, S. (2017, Marzo 20). *Cybersecurity & Internet of Things.* Retrieved from https://kfrankc.me/files/ethics_w17.pdf

Gartner. (2016, October 3). *"Forecast Snapshot: VPA-Enabled Wireless Speakers, Worldwide, 2016."*. Retrieved from Gartner: https://www.gartner.com/newsroom/id/3464317

Haack, W., Severance, M., Wallace, M., & Wohlwend, J. (2017, May 18). *Security Analysis of Amazon Echo.* Retrieved from MIT Computer Science and Artificial Intelligence Laboratory: https://courses.csail.mit.edu/6.857/2017/project/8.pdf

IFIXIT. (2014, December 16). *Amazon Echo Teardown.* Retrieved from IFIXIT: https://www.ifixit.com/Teardown/Amazon+Echo+Teardown/33953

IFIXIT. (2016, 04 19). *Amazon Echo Dot Teardown.* Retrieved from IFIXIT: https://www.ifixit.com/Teardown/Amazon+Echo+Dot+Teardown/61304

ISO. (n.d.). *International Organization for Standardization.* Retrieved from International Organization for Standardization: https://www.iso.org/about-us.html

ISO/IEC 27001. (2013, September 25). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements.* Retrieved from ISO/IEC 27001:2013: www.iso.org

ISO/IEC 27002. (2013). *ISO27002.es El portal de ISO27002 en español.* Retrieved from ISO27000.es: http://www.iso27000.es/iso27002.html

ISO/IEC 27005. (2011, 06). *ISO/IEC 27005:2011 Information Technology. Security techniques. Information security risk management.* Retrieved from ISO.ORG: https://www.iso.org/standard/56742.html

Jay, J. (2017, August 2). *Security flaws in Amazon Echo that let hackers gain root access cannot be patched.* Retrieved from TEISS Cracking cyber security: https://teiss.co.uk/iot/security-flaws-amazon-echo-let-hackers-gain-root-access-cannot-patched/

Johnson, M. (2017, February 5). *Mayor Security Flaw.* Retrieved from Amazon Customer Review: https://www.amazon.com/review/RZCKADI4L1JCI/ref=cm_cr_dp_cmt?ie=UTF8&ASIN=B015TJD0Y4&channel=detail-glance&nodeID=9818047011&store=amazon-home#wasThisHelpful

Keimel, M. G. (2016, Junio). *Integración de dispositivos en una plataforma de vida cotidiana asistida por computadora.* Retrieved from RIDAA UNICEN: http://www.ridaa.unicen.edu.ar/xmlui/handle/123456789/646

Klaus, H. (2014). ISO 27001 for Developers and Testers. *Testing Experience.*

Knowles Electronics, LLC. (2017). *Knowles Microphones*. Retrieved from Knowles: http://www.knowles.com/eng/Products/Microphones

Morning Consult. (2017, June 12). *National Tracking Poll #170603.* Morning Consult. Retrieved from https://morningconsult.com/wp-content/uploads/2017/06/170603_crosstabs_Brands_v3_TB-1.pdf

Nitrozac, & Snaggy. (2016). *The Joy of Tech.* Retrieved from http://www.joyoftec.com

PECB. (2016, February 23). *PECB.* Retrieved from ISO/IEC 27002:2013 Information Technology - Security Techniques Code of Practice for Information Security Controls : https://pecb.com/whitepaper/isoiec-270022013-information-technology---security-techniques-code-of-practice-for-information-security-controls

Prandini, P., & Pallero, M. (2013, Mayo 05). Vulnerabilidades, amenazas y riesgo en "texto claro". *Magazcitum*.

Ramírez, A., & Ortiz, Z. (2011). Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *En: Ingeniería, Vol. 16, No. 2, pág. 56-66., 16*(2), 56-66.

Reinoso, G. (2015). *Electrónica y ciencia.* Retrieved from Blog técnico sobre proyectos caseros de electrónica, informática y física.: http://electronicayciencia.blogspot.com/2013/03/la-distorsion-armonica-total-thd.html

Roy, N., Hassanieh, H., & Choudhur, R. R. (2017, June). BackDoor: Making Microphones Hear Inaudible Sounds. *MobiSys '17 Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services* (pp. 2-14). Nigara Falls: ACM. doi:10.1145/3081333.3081366

Sacerdoti, E. (2014, September 22). *Equaphon University. La distorsión.* Retrieved from Equaphon University: http://www.equaphon-university.net/la-distorsion/

Shull, F., Singer, J., & Sj_berg, D. I. (2007). Guide to Advanced Empirical Software Engineering. Secaucus, New Jersey, USA: Springer-Verlag New York, Inc.

Song, L., & Mittal, P. (2017, August 24). *Inaudible Voice Commands.* Retrieved from ArXiv: https://arxiv.org/pdf/1708.07238.pdf

Tejero, A. (2014). *Seguridad en el Internet de las Cosas.* Retrieved from Universidad Politécnica de Madrid: http://www.upm.es

Tesla, N. (1926, January). When Woman is Boss. (K. Colliers, Interviewer)

Universidad Nacional de Luján. (2017). *Departamento de Seguridad Informática - Seguridad de la información.* Retrieved from Universidad Nacional de Luján: http://www.seguridadinformatica.unlu.edu.ar

Valencia-Duque, F. J., & Orozco-Alzate, M. (2017, Junio 01). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *Revista Ibérica de Sistemas y Tecnologías de la Información*, 73-87. doi:10.17013/risti.22.73-88

Yang Hui, J., & Leong, D. (2017, August 18). The Era of Ubiquitous Listening: Living in a World of Speech-Activated Devices. *Asian Journal of Public Affairs 10(1): e5*, 1-19.

Zhang, G., Yan, C., Ji, X., & Zhang, T. (2017, August 31). DolphinAtack: Inaudible Voice Commands. *CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on*

Computer and Communications Security (pp. 103-117). Dallas: ACM. doi:10.1145/3133956.3134052

ANEXOS

Anexo 1. Experimentación

El experimento propuesto reproduce lo realizado por: Roy *et al*. (2017) en "*Backdoor: Making microphones hear inaudible sounds*", Song and Mittal (2017) en "*Inaudible Voice Commands*", y Zhang *et al.* (2017) en "*Dolphin Attack: Inaudible Voice Commands*"; los cuales tratan acerca de la generación e inyección de comandos inaudibles (alta frecuencia, sobre los 20kHz) para el oído humano, pero que son reconocidos por los dispositivos inteligentes de reconocimiento de voz, sin que sus dueños de percaten de aquello.

Este tipo de ataque, utiliza una técnica que afecta directamente a las membranas de los micrófonos incorporados los dispositivos de reconocimiento de voz, como lo es Amazon ECHO DOT (que es utilizado en este experimento), haciendo que las mismas vibren cuando son alcanzadas por las ondas de sonido. Permitiendo así, que el hardware del micrófono pueda captar estas señales pese a ser inaudibles.

Es más, este tipo de ataque, aprovecha, la característica de no linealidad que poseen este tipo de dispositivos, logrando así, que el micrófono una vez que reciba la señal de alta frecuencia, pueda grabar la misma como normal (audible), permitiendo así que el dispositivo reconozca la orden (Song & Mittal, 2017).

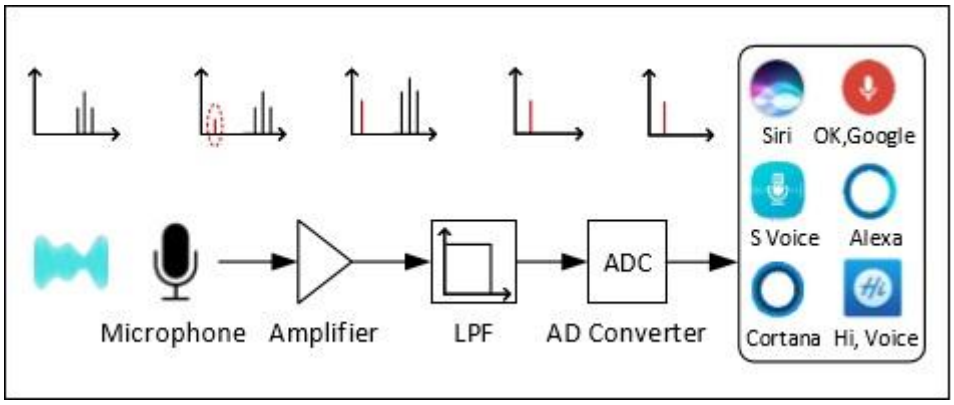
Para un mejor entendimiento, se detallan a continuación varios conceptos relacionados al tema.

Micrófonos

El primer componente de la arquitectura de un sistema de voz controlable, es la captura de voz, por lo que es necesario describir cómo funciona dicho componente para un mejor entendimiento.

El funcionamiento de un micrófono es el siguiente: el transductor o sensor electro acústico, genera una variación de voltaje proporcional a la presión del sonido. La señal debe pasar a través de un amplificador, el mismo que permitirá amplificar la señal de salida emitida por el transductor. Cabe señalar que sin esta amplificación, la señal será muy débil. A continuación, se cuenta con un Filtro de Bajos LPF (*Low Pass Filter*) el cual se encargará de filtrar los componentes de alta frecuencia, y por último el convertidor de Análogo a Digital, ADC (*Analog Digital Converter*), utilizado para digitalización y cuantificación; el cual mide la variación de voltaje (frecuencia de muestreo fija) y almacena los muestreos en memoria. Debido a que el rango de frecuencia audible va desde 20Hz hasta 20kHz, el filtro LPF generalmente usa 20kHz, mientras que la taza de muestreo en el cual trabaja un ADC, será de 48kHz o 44kHz. La figura 23 muestra el funcionamiento de un micrófono antes descrito.

Figura 23. Funcionamiento de un micrófono (Roy, Hassanieh, & Choudhur, 2017)



Distorsión no lineal

Una característica importante de los micrófonos que utilizan los dispositivos de reconocimiento de voz, es la propiedad de no linealidad, la cual, permite crear nuevas

frecuencias a partir de una señal de entrada; la misma que puede reducir la señal, así como también recuperar la señal de banda base (Zhang *et al.*, 2017). Es más, de acuerdo a lo que se menciona el estudio "*Backdoor: Making microphones hear inaudible sounds*" (Roy *et al*., 2017), la salida no lineal es una serie de poder infinito.

Adicionalmente, es necesario indicar, que la propiedad de linealidad y no linealidad presenta distorsión. Se considera distorsión a todas aquellas diferencias que se tenga entre la señal de entrada y la señal resultante o de salida (Sacerdoti, 2014). Para el caso de esta investigación, se considera la distorsión presente en la arquitectura no lineal. "Las distorsiones no lineales, son aquellas que generan componentes de frecuencias nuevas, que pueden o no tener relación con la señal inyectada, afectando así su componente espectral" (Sacerdoti, 2014). Dentro de este tipo de distorsión, se tiene la distorsión armónica y la distorsión por intermodulación.

La distorsión armónica conocida también como distorsión total, THD por sus siglas en inglés (*Total Harmonic Distortion*), se produce cuando la señal de salida de un sistema no equivale a la señal que entró en este. Esta mide la cantidad de armónicos que el equipo introduce, pero que no existían en la señal original (Reinoso, 2015). Dentro de las utilidades que se obtiene al tener distorsión armónica, está la generación funciones de alta frecuencia, la cual, es aprovechada en la realización del experimento propuesto.

Por otra parte, la distorsión por intermodulación, IMD por sus siglas en inglés (*Inter Modulation Distortion*), la cual, a diferencia de la distorsión armónica, aquí no se mantiene una relación armónica entre las nuevas frecuencias generadas y la señal de origen. Pudiendo así ser percibidas de manera más notoria (Sacerdoti, 2014).

Como se mencionó anteriormente, el dispositivo de reconocimiento de voz que se utiliza en este experimento es Amazon ECHO DOT. Cabe recalcar que durante la

ejecución del experimento no se necesitó realizar ninguna manipulación física a los micrófonos del dispositivo en mención. El ataque aprovecha dos características de este tipo de objeto inteligente: la no linealidad presente en su arquitectura, y la escucha continua. Lo que se necesita es mantener una distancia prudente con referencia al dispositivo inteligente y ejecutar el comando de voz de alta frecuencia.

De acuerdo a lo manifestado por Song and Mittal (2017), en el estudio "*Inaudible Voice Commands*", las señales de salida contienen nuevas frecuencias. "Estas nuevas frecuencias no son tan solo múltiplo de enteros de la frecuencia original, es la suma y la diferencia de la frecuencia original de entrada". Para demostrar aquello, Song and Mittal (2017) plantean una serie de fórmulas, las mismas que se analizan a continuación:

Fórmula 3. Señal de salida luego de ser amplificada (Song & Mittal, 2017)

$$Sout = \sum_{i=1}^{\infty} G_i S_{in}^i = G_1 S_{in} + G_2 S_{in}^2 + G_3 S_{in}^3 + \cdots,$$

El primer término de la fórmula 1 es un término lineal el cual domina el sonido de entrada en un rango normal. Sin embargo, los otros términos reflejan no linealidad, siendo el segundo término el más fuerte comparado con los otros (Song & Mittal, 2017). La salida del segundo término es expresada en la fórmula 2, en la cual se puede apreciar la distorsión armónica $2f_1, 2f_2$ y distorsión por intermodulación $(f_1 \pm f_2)$ presentes en una arquitectura no lineal.

Fórmula 4. Término de segundo orden (Song & Mittal, 2017)

$$G_2 S_{in}^2 = G_2 + \frac{G2}{2}(\cos(2\pi(2f_1)t) + \cos(2\pi(2f_2)t))$$

$$+ \ G_2(\cos(2\pi(f_1 + f_2)t) + \cos(2\pi(f_1 - f_2)t))$$

Las acciones llevadas a cabo en el experimento son:

- Obtención de recursos de hardware y software necesarios.
- Configuración de los diferentes equipos utilizados.
- Implementación del código para la generación de comandos en alta frecuencia a través de algoritmos, utilizando la herramienta *Matlab*.
- Generación de comandos audibles de voz a través de la herramienta *Audacity* e *iPhone*.
- Pruebas.

Recursos de Hardware y Software

Para poder llevar a cabo el experimento, fueron necesarios recursos de hardware y software que aparecen en la tabla 15.

Tabla 15. Hardware y Software experimento. Elaborado por el autor.

Equipo	**Características**	**Gráfica**
Amazon ECHO	ECHO DOT 2nd *edition* 2017	
Teléfonos inteligentes con activación de voz	*iPhone* 4S IOS 9.3.5 *iPhone 7*	 
Laptop	*Sony Vaio*	
Parlante ultrasonido	*Fostex* FT17H Horn Super *Tweeter*	

Equipo	Características	Gráfica
Parlante	Pioner TS-S250	
Amplificador de sonido que opere en rango de ultrasonido	Sony DN-1050	
Amplificador de sonido análogo	TEAC RV-30	
Amplificador de sonido de alta calidad	Yamaha Stereo Receiver R-S202	
Cable parlante	Conexión parlante – amplificador	
Cable RCA (Audio)	RCA	
Osciloscopio	Para la medición de señales (tiempo – voltaje)	
Software para generación de señales	*Matlab*	Matlab
Software para reproducción de audio	*Audacity*	Audacity®

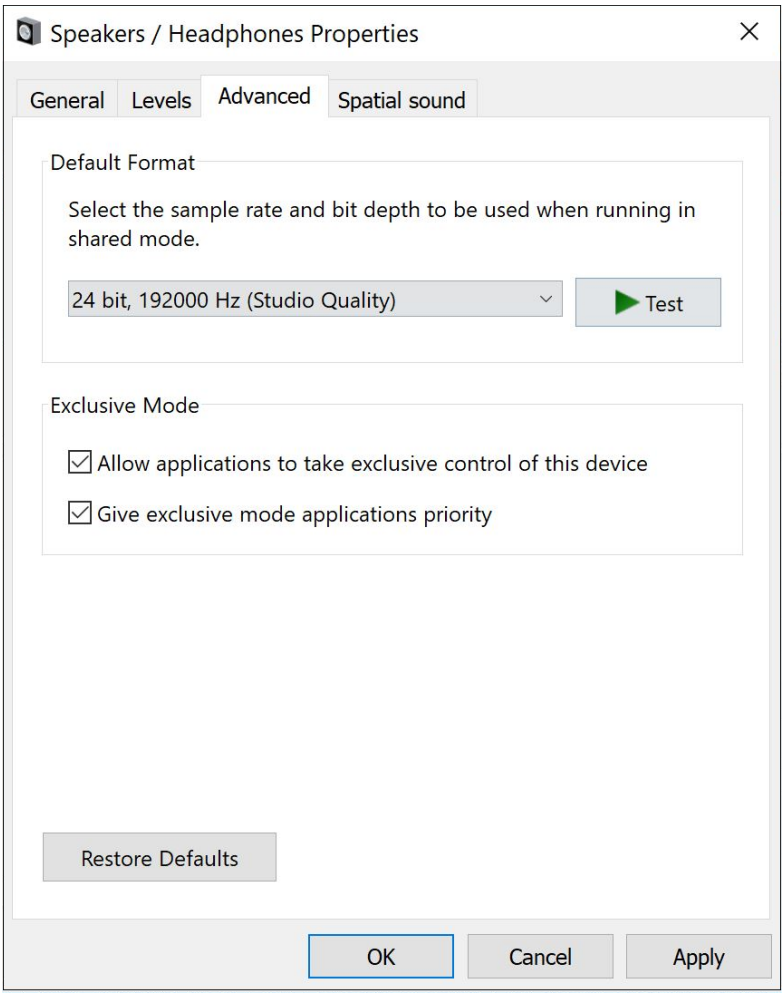
Desarrollo e Implementación

Para poder llevar a cabo el experimento y las pruebas respectivas, se necesitan configurar varios dispositivos.

Configuración de Laptop

La laptop será utilizada para generar las señales de audio. En este caso, se trata de un computador portátil *Sony Vaio*. La tarjeta de sonido debe tener el valor más alto posible (en este caso de 24 bit, 192,000 Hz), para poder luego amplificar la señal, y reproducirla a través del parlante. La figura 24 muestra la configuración en mención.

Figura 24. Configuración parlante Sony Vaio. Elaborado por el autor.

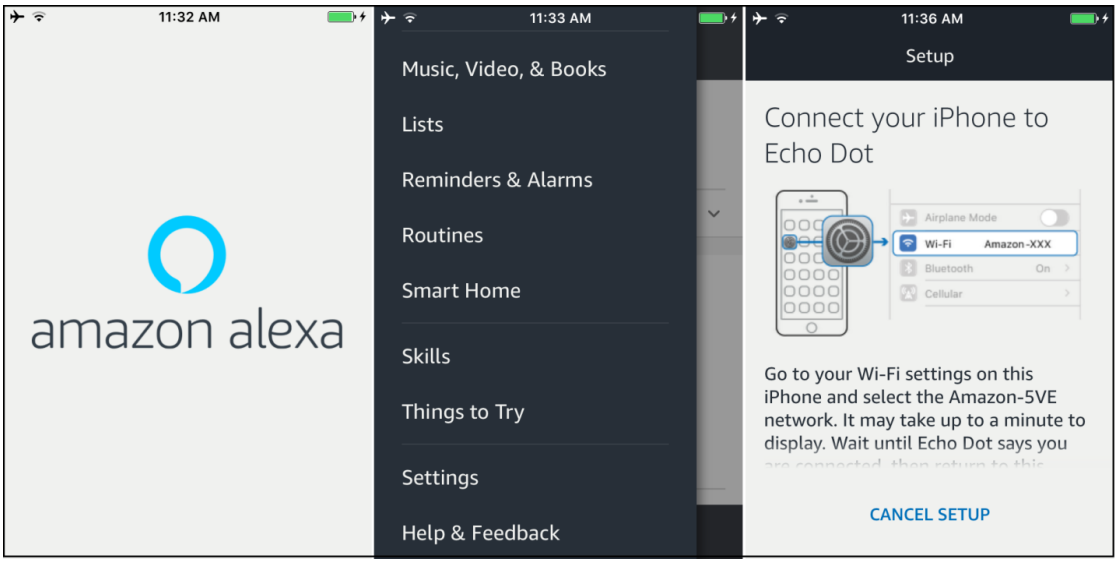


Configuración del dispositivo Amazon ECHO

El dispositivo Amazon ECHO, debe ser configurado previamente, es decir debe estar asociado a una cuenta Amazon (del dueño), seleccionar ubicación, entre otras; y debe estar conectado a la red *wireless* desde donde va a trabajar. Para poder realizar la conexión, se utiliza la aplicación Alexa APP, la misma que debe ser instalada en cualquier teléfono inteligente. Para este caso, la aplicación fue instalada en un *iPhone* 4S.

Como el experimento se lleva a cabo en la Universidad Internacional SEK del Ecuador, se procede con la conexión en la red *Wi-Fi* de la misma. La figura 25 muestra la aplicación Alexa y su configuración de *Wi-Fi*.

Figura 25. Amazon Alexa Ap. Elaborado por el autor.



Comandos de voz

Se necesita generar comandos de voz audibles, (rango hasta 20Mhz), de extensión .WAV; los mismos que, serán traducidos a comandos de voz inaudibles (30-40kMz). Para la grabación de dichos comandos, se utiliza la herramienta *Audacity* 2.2.1 (2017), así como también, se realizan grabaciones utilizando el *iPhone* 4S. La tabla 16, muestra los comandos de voz audibles generados.

Tabla 16. Comandos de voz audibles. Elaborado por el autor.

Ref.	Comando de Voz	Path
CA1	Alexa, what time is it?	Anexos\comandos_audibles\alexa_time.wav
CA2	Alexa, are you spying on me?	Anexos\comandos_audibles\alexa_spy.wav
CA3	Alexa, how is the weather	anexos\comandos_audibles\alexa_weather.wav
CA4	Alexa, play some music	anexos\comandos_audibles\alexa_music.wav
CA5	Hey Siri, call 1,2,3,4,5	anexos\comandos_audibles\siri_call.wav
CA6	Hey Siri, play some music	anexos\comandos_audibles\siri_music.wav

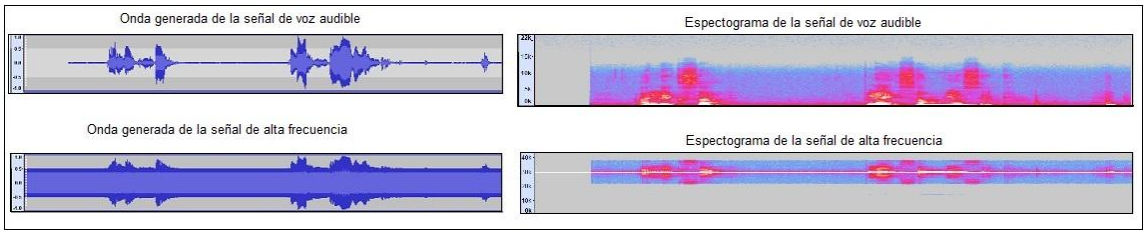
Adicionalmente, se generan los respectivos comandos de voz inaudibles, tal como lo muestra la tabla 17.

Tabla 17. Comandos inaudibles generados. Elaborado por el autor.

Ref	Comando de Voz	Path
CI1	Alexa, what time is it?	Anexos\comandos_inaudibles\inaudible_alexa_time.wav
CI2	Alexa, are you spying on me?	Anexos\comandos_inaudibles\inaudible_alexa_spy.wav
CI3	Alexa, how is the weather?	Anexos\comandos_inaudibles\inaudible_alexa_weather.wav
CI4	Alexa, play some music	Anexos\comandos_inaudibles\inaudible_alexa_music.wav
CI5	Hey Siri, call 1,2,3,4,5	anexos\comandos_inaudibles\inaudible_siri_call.wav
CI6	Hey Siri, play some music	anexos\comandos_inaudibles\inaudible_siri_music.wav

Las señales generadas por los comandos de voz audible e inaudible pueden ser apreciadas de mejor manera en la figura 26.

Figura 26. Onda y espectrograma comando de voz audible e inaudible. Elaborado por el autor.



Aplicación de fórmulas y algoritmos

La tabla 18 muestra los filtros usados y los algoritmos implementados en MATLAB, con el fin de poder generar los comandos de voz inaudibles. El código generado para realizar el ataque fue tomado de Liwei Song (2017), coautor del estudio de investigación "Inaudible Voice Commands".

Las fórmulas utilizadas para la elaboración del algoritmo de ataque implementado, se detallan a continuación.

Fórmula 5. Filtro Pasa Bajos (Song & Mittal, 2017)

$$S_{filter}$$

Fórmula 6. Aumento del Sampling (Song & Mittal, 2017)

$$S_{up}$$

Fórmula 7. Modulación Ultrasonido (Song & Mittal, 2017)

$$S_{modu=}\, n_1 S_{up} \cos\,(2\pi f_{ct})$$

Fórmula 8. Algoritmo de Ataque (Song & Mittal, 2017)

$$S_{attack} = \; n_2 \;\; (S_{modu} \; + \; \cos\,(2\pi f_{ct})$$

Tabla 18. Algoritmos generación comandos inaudibles. Elaborado por el autor.

Fórmulas – Filtros	**Algoritmo en MATLAB**
Lectura de comandos de voz audibles Se define una variable que contendrá el archivo .wav que se desea leer.	voice_command = 'siri_order.wav'; [vs,vsf] = audioread(voice_command);

Fórmulas – Filtros	Algoritmo en MATLAB
Vs contendrá el arreglo mientras Vsf contendrá la frecuencia de muestreo	
Fórmula 3. Filtro Pasa Bajos Una vez que se tiene el audio, es necesario pasarlo por un filtro de pasa bajos para remover los componentes de alta frecuencia. El filtro permitirá la baja frecuencia para la modulación manteniendo suficiente información de la señal original.	[b,a] = butter(50, 2*8000/vsf,'low'); [voice_with_filter] = filter(b,a,vs(:,1));
Fórmula 4. Aumento del Sampling. Filtro para aumentar la tasa de muestreo (sampling rate) La idea aquí, es aumentar el sampling rate. El sampling rate de un comando de voz normal es de 48kHz, lo mismo que el del filtro. La máxima frecuencia de ultrasonido no debería ser menos de 28kHz, por lo que se necesita un mayor sampling rate.	High_sampling_freq = 192000;

Fórmula 5. Modulación Ultrasonido
Aqui se adopta como carrier frecuency 40kHz.
Y se obtiene ultrasound AM modulation
El valor para el carrier frecuency es de 40000. Cabe recalcar que durante las pruebas, el valor fue modificado. Se trabajó con 30kHZ.
	Dt = 1/high_sampling_freq;
	len = size(voice_with_upsampling,1);
	t = (0:dt☹len – 1)*dt)';
	carrier_freq = 40000;
	ultra_modu_DSB_AM=
	voice_with_upsampling.*cos(2*pi*carrier_freq*t);

Fórmulas – Filtros	Algoritmo en MATLAB

Normalización
Función de normalización
 	
Llamado a la función de normalización
	function [output] = normalizacion(input)
	max_value = max(abs(input));
	output = 1./max_value .* input;
	end
	ultra_input_DSB_AM
	normalizacion(ultra_modu_DSB_AM)
	cos(2*pi*carrier_freq*t);

Fórmula 6. Algoritmo de ataque	destination_file = 'inaudible_voice_command.wav'; audiowrite(destination_file,normalizacion(ultra_input_DSB_AM), high_sampling_freq);

Pruebas y Resultados

Luego de la configuración de los equipos, así como también de la generación de los comandos de voz y el desarrollo del código en Matlab con la aplicación de fórmulas, para la generación de las órdenes inaudibles; se procede con las pruebas correspondientes.

Los resultados esperados del experimento son:

- Generación de los comandos inaudibles
- Que los dispositivos de reconocimiento de voz utilizados, reconozcan los comandos inaudibles generados.
- Que a través de la ejecución satisfactoria del experimento propuesto, se pueda comprobar la vulnerabilidad existente en este tipo de dispositivos.

Pruebas realizadas del 11 al 19 de enero 2018

1. Se grabaron varios comandos de voz con la herramienta *Audacity*. Se debe tomar en cuenta que el dispositivo Alexa reconoce el idioma inglés únicamente. Los comandos generados son CA1, CA2 y CA3 (ver tabla 16).

2. Se generan los correspondientes comandos de voz inaudibles a través de los algoritmos implementados en la herramienta MATLAB. Los comandos inaudibles son CI1, CI2 Y CI3 (ver tabla 17).
3. Se procede con la conexión de los equipos

   a) Laptop – Amplificador. Se conecta el cable RCA desde la laptop al amplificador. El cable desde la laptop sale desde los audífonos, mientras que en el amplificador en la sección AUDIO, se realizó la prueba con las tres entradas existentes: SAT/CATV, VIDEO 1 y SA-CD/CD. La figura 27 muestra la conexión en mención.

Figura 27. Conexión Sony Vaio con amplificador. Elaborado por el autor.

   b) Parlante – Amplificador. Se conecta el cable desde el parlante al amplificador. Se utiliza el parlante frontal del amplificador, puesto que este es el que posee menos filtros. Cabe destacar, que para las pruebas se probó con cada una de las opciones existentes (*front, center, subround*). La figura 28 muestra la conexión en mención.

Figura 28. Conexión entre parlante y amplificador. Elaborado por el autor.

c) Dispositivo Amazon ECHO DOT. El dispositivo Alexa debe estar ubicado a una distancia no tan lejana del parlante. El micrófono del mismo, deben ubicarse frente a los micrófonos del parlante, tal como lo muestra la figura 29.

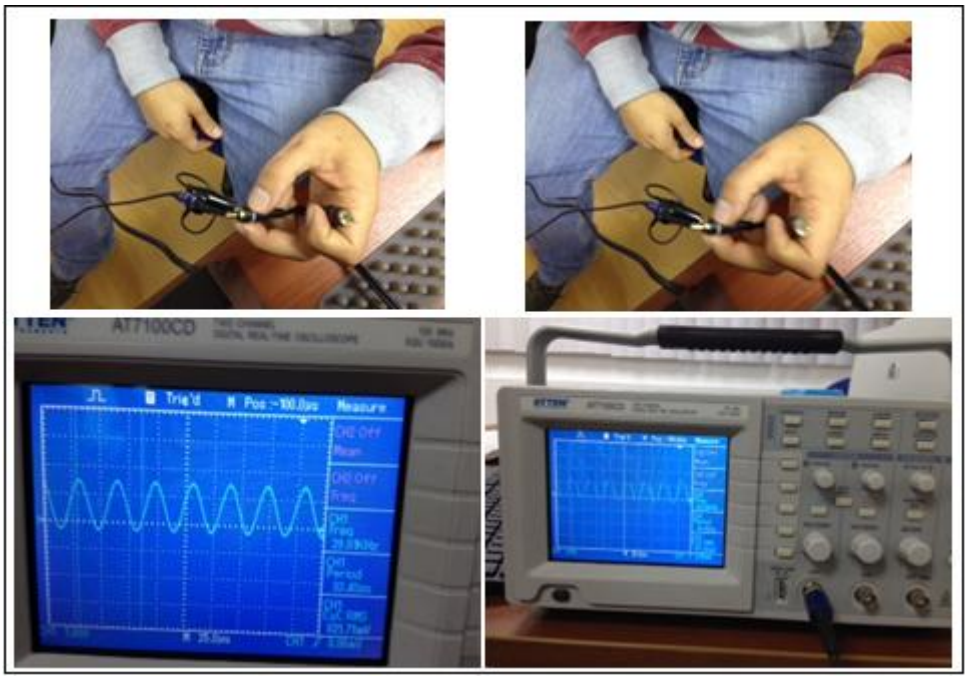
Figura 29. Ubicación Amazon ECHO DOT y parlante. Elaborado por el autor.

4. Una vez que los equipos han sido instalados y conectados, se procede con las pruebas.
   - El volumen de la laptop, así como del amplificador están al máximo.
   - Se reproducen uno por uno los comandos de voz inaudible CI1, CI2 y CI3 desde la aplicación *Audacity*.
   - Sin embargo, cuando se reproducen los comandos inaudibles, no se tiene el resultado deseado. Es decir los comandos CI1, CI2 y CI3, no son reconocidos por el

dispositivo Amazon ECHO. Para poder solucionar este inconveniente, se procede con lo siguiente:

- Se procede a probar cada una de las entradas de Audio en el amplificador SAT/CATV, VIDEO 1 y SA-CD/CD, y se reproducen los comandos CI1, CI2 y CI3 generados, pero tampoco se tiene éxito. Por lo que, para descartar que el problema provenga desde el amplificador, se necesita utilizar un osciloscopio para medir la potencia de la señal generada.
- Pruebas con el osciloscopio. Se conecta el cable RCA que sale desde la laptop hacia el amplificador, tal como lo muestra la figura 30.

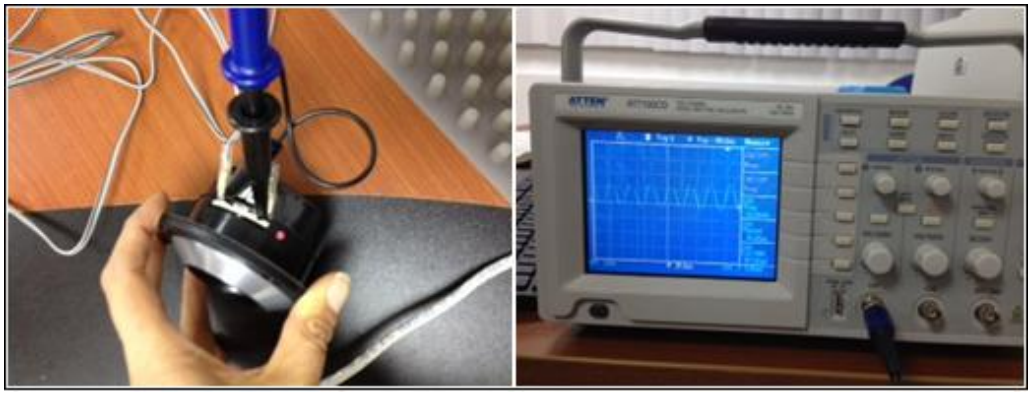
Figura 30. Pruebas osciloscopio – cable RCA. Elaborado por el autor.



- Sin embargo, la señal generada desde la laptop, pudo ser visualizada correctamente desde el osciloscopio; por lo que se descarta que el problema provenga desde la laptop.
- Se realiza la prueba con el cable que se utiliza para conectar el parlante y el amplificador. La figura muestra 31 la prueba correspondiente. Sin embargo, se

pudo evidenciar que el cable transmite y la señal es generada sin problema en el osciloscopio.

Figura 31. Pruebas osciloscopio – cable parlante – amplificador. Elaborado por el autor.



- Se procede a probar la señal que sale del cable desde el amplificador. Tal como lo muestra la figura 32. Sin embargo, en este caso no se evidenció señal de salida en la pantalla del osciloscopio, lo cual comprueba que el amplificador es el que ocasiona que la señal no sea emitida. Esto puede deberse a los filtros incorporados que posee.

Figura 32. Pruebas osciloscopio – cable amplificador. Elaborado por el autor.

Pruebas realizadas el 23 de Enero del 2018

1. Con lo detectado en las pruebas anteriores, se procede a cambiar de amplificador. Se opta por un amplificador análogo, simple, el cual no posee ningún filtro sofisticado. La figura 33 muestra en cuestión.

Figura 33. Amplificador análogo TEAC. Elaborado por el autor.

2. Se realiza la conexión de todos los equipos, tal como se lo hizo con las pruebas anteriores.
3. Cabe recalcar, que para las pruebas se incorpora un nuevo dispositivo, un teléfono *iPhone*, al cual se pretende activar, tal como se lo realiza con el dispositivo Amazon ECHO, DOT. Las figuras 34 y 35 muestran el ambiente implementado y la conexión de los equipos respectivamente.

Figura 34. Ambiente de pruebas implementado. Elaborado por el autor.

Figura 35. Conexión de equipos para pruebas. Elaborado por el autor.

4. Se procede a la grabación de los comandos de voz CA4, CA5 y CA6. La grabación y reproducción de cada comando se lo realiza a través de la herramienta *Audacity*.
5. Se procede a la generación de los comandos inaudibles CI4, CI5 y CI6 a través de la herramienta *Matlab*.
6. Se procede con la configuración del amplificador, en referencia a volumen y filtros (bajo y triple). La figura 36 muestra la configuración en mención.

Figura 36. Configuración amplificador análogo. Elaborado por el autor.

7. Se emite las señales inaudibles CI4, CI5 y CI6 una por una.
8. Afortunadamente, una vez emitida la señal, ésta es reconocida por el dispositivo Amazon ECHO, con lo que la prueba fue satisfactoria.
9. La distancia utilizada entre el dispositivo de reconocimiento de voz y el parlante es de aproximadamente 20 centímetros.
10. El dispositivo Amazon ECHO DOT, reconoció la orden de reproducir música (CI4), sin problema.
11. El *iPhone* reconoció la orden de llamar (CI5) y de tocar música (CI6) sin ningún problema.

Con lo que se cumple lo propuesto en este experimento, lo cual es probar la vulnerabilidad existente en este tipo de dispositivos.

Pruebas 02 y 08 de Febrero 2018

1. Para optimizar los resultados obtenidos, se utiliza un nuevo amplificador. La figura 37 muestra el amplificador utilizado.

Figura 37. Amplificador Yamaha. Elaborado por el autor.

2. Se utiliza un nuevo set de parlantes *Pioner*. Tal como se lo aprecia en la figura 38.

Figura 38. Parlantes Pioner. Elaborado por el autor.

3. Se realiza la conexión de todos los equipos, de la misma forma en la se lo hizo con las pruebas anteriores. La figura 39 muestra la conexión entre el amplificador Yamaha y la laptop Sony a través del cable RCA. Y la figura 40 muestra la conexión entre el amplificador Yamaha y el parlante.

Figura 39. Conexión amplificador – laptop. Elaborado por el autor.

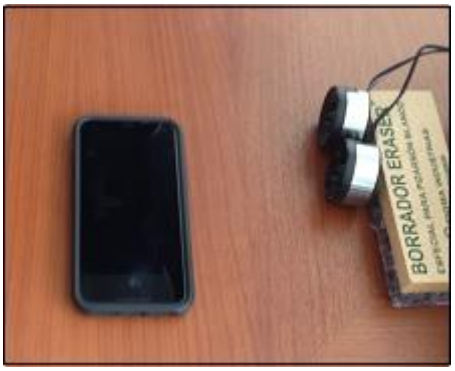
Figura 40. Conexión amplificador Yamaha – parlante. Elaborado por el autor.

4. Se utilizan los comandos de voz inaudibles generados en las pruebas anteriores CI1, CI2, CI3 y CI4 para las pruebas con el dispositivo Amazon ECHO DOT.
5. Se procede con la emisión de los mismos uno por uno.
6. El ambiente creado se lo puedo visualizar en la figura 41.

Figura 41. Ambiente de pruebas. Elaborado por el autor.

7. El dispositivo Amazon ECHO DOT reconoce las órdenes emitidas desde los comandos reproducidos.
8. Se realiza las pruebas con el dispositivo *iPhone*. El cual también reconoce las órdenes CI5 y CI6. La figura 42 muestra la iteración entre el *iPhone* y el parlante.

Figura 42. iPhone 7 – parlante. Elaborado por el autor.



Anexo 2. Entrevistas

Valoración Activos

Responda las siguientes preguntas teniendo en cuenta la siguiente escala:

1 Muy bajo

2 Bajo

3 Medio

4 Alto

5 Muy alto

1 ¿Qué valor tiene para usted la información personal y privada (como por ejemplo, tarjetas de crédito, direcciones, compras realizadas, etc.) que mantiene en su cuenta Amazon?

2 ¿Qué valor tiene para usted las transacciones que realiza a través de su dispositivo Alexa, como por ejemplo compras en línea?

3 ¿Qué valor tiene para usted las conversaciones que mantiene en casa?

4 ¿Qué valor tiene para usted el manejo y control de otros dispositivos en casa (como por ejemplo control de luces, tv, temperatura, etc.) a través de su dispositivo Alexa?

Probabilidad de Ocurrencia

Responda las siguientes preguntas teniendo en cuenta la siguiente escala:

1 Muy baja

2 Baja

3 Media

4 Alta

5 Muy alta

1. ¿Qué tan probable es que personas externas a su hogar manipulen físicamente su dispositivo Alexa y logren tener acceso a su configuración?

2. ¿Qué tan probable es que terceras personas puedan activar a su dispositivo Alexa a través de comandos de voz, y realizar transacciones sin que usted se percate de aquello, es decir que usted no escuche cuando le dan órdenes a su Alexa?

3. ¿Qué tan probable es que personas externas, como por ejemplo sus vecinos, puedan conectarse a su dispositivo Alexa a través de bluetooth sin que usted lo haya autorizado o se haya dado cuenta?

4. ¿Qué tan probable es que personas externas lo estén monitoreando, y escuchando continuamente las conversaciones que mantiene en su entorno a través de su dispositivo Alexa?

Impacto Generado

Confiabilidad – Disponibilidad – Integridad

Responda a las siguientes preguntas utilizando la siguiente escala

1 Bajo

2 Medio

3 Alto

1. ¿Cuál sería el impacto generado si personas externas a su hogar pueden manipular físicamente a su dispositivo Alexa y logren tener acceso a su configuración?

2. ¿Cuál sería el impacto generado si terceras personas pueden activar a su dispositivo Alexa a través de comandos de voz, y realizar transacciones sin que usted se percate de aquello, es decir que usted no escuche cuando le dan órdenes a su Alexa?

3. ¿Cuál sería el impacto generado si personas externas, como por ejemplo sus vecinos, pueden conectarse a su dispositivo Alexa a través de bluetooth, sin que usted lo autorice o se haya dado cuenta?

4. ¿Cuál sería el impacto generado si personas externas lo están monitoreando, y escuchando continuamente las conversaciones que usted mantiene en su entorno, a través de su dispositivo Alexa?