Asistentes personales virtuales: una mirada hacia sus problemas de privacidad

Aron Caballero Macias
Escuela Superior Politécnica del Litoral
Guayaquil, Ecuador
arcamaci@espol.edu.ec

Evelyn Mejia Murillo
Escuela Superior Politécnica del Litoral
Guayaquil, Ecuador
enmejia@espol.edu.ec

Kenny Camba Torres
Escuela Superior Politécnica del Litoral
Guayaquil, Ecuador
kacamba@espol.edu.ec

Steven Araujo Moran
Escuela Superior Politécnica del Litoral
Guayaquil, Ecuador
saraujo@espol.edu.ec

***Resumen*—El auge de los asistentes personales virtuales (VPA) plantea preocupaciones respecto a la protección que ofrecen sobre la privacidad de los usuarios. Esta investigación revela si las personas están conscientes del uso y administración que tanto ellos como terceros pueden realizar con los datos compartidos con sus VPAs. Mediante una encuesta realizada a 43 personas usuarios de VPAs, se obtuvo que más del 50 % desconoce sobre el acceso de terceros y menos del 25 % ha administrado los datos almacenados en el historial de su VPA. Adicionalmente, se realizó la revisión de los historiales de 14 participantes, con el propósito de detectar como influyen las interacciones accidentales en su privacidad y cuál VPA (Google Assistant o Amazon Alexa) realiza un mejor manejo de ellas. Se detectó que Google Assistant respetó más la privacidad de sus usuarios, ya que evitó almacenar las grabaciones producidas por activaciones accidentales, al contrario de Alexa que en los historiales presentó grabaciones no deseadas.**

I. Introducción

Actualmente los asistentes personales virtuales o VPA por sus siglas en inglés se encuentran presentes en la sociedad, principalmente mediante dispositivos móviles inteligentes o smartphones. Existen 5.190 millones de usuarios únicos de smartphones, lo que representa el 67 % de la población mundial [22]. En Ecuador el 76,8 % de las personas que poseen un celular activado, tienen un smartphone [1]. También se pueden encontrar a los VPAs en otros dispositivos inteligentes tales como televisores, vehículos autónomos, dispositivos médicos y sistemas de navegación.

Los VPAs permiten llevar a cabo diversas interacciones, por ejemplo, solicitar el pronóstico del clima, realizar una transacción o controlar un dispositivo IoT como luces, alarmas, cerraduras, etc [13]. En el proceso de interacción el VPA almacenará información sensible, direcciones, contactos, listas de compras, entre otros. Las principales empresas detrás de los VPAs con más presencia de mercado son Google y Amazon. Ambas empresas han revelado que sus empleados escuchan las grabaciones almacenadas, Amazon para asegurar respuestas correctas de su VPA [18] y Google para mejorar su tecnología de reconocimiento del idioma [12].

Las principales preocupaciones de los usuarios de VPA son la confianza, privacidad y escucha pasiva [19]. Los VPAs se han diseñado para permanecer en espera hasta reconocer un comando de voz de activación [2]. Existen varios casos donde terceras personas han intentado aprovechar esta característica. Por ejemplo, para estrategias de marketing como el caso de Burger King cuando lanzó una publicidad en donde se pronunciaba la frase "Ok Google, what is the Whopper burger?" cuya intención era activar el asistente de Google para que diera más información sobre el producto anunciado [4], o cuando un atacante accedió remotamente a un dispositivo Alexa haciendo uso de la autenticación de un solo factor para realizar un pedido a la tienda de Amazon [15].

Esta investigación pretende descubrir el nivel de conocimiento que poseen los usuarios sobre la administración de los datos almacenados por los VPAs y describir cómo puede verse afectada la privacidad de los usuarios debido a las activaciones accidentales. Finalmente, con la intención de generalizar la metodología aplicada a cualquier VPA, la investigación se realizará con usuarios de Google Assistant y Amazon Alexa.

II. Revisión Literaria

Las investigaciones anteriores relacionadas a la seguridad y privacidad que ofrecen los VPAs pueden englobarse en las siguientes categorías: 1) captura de voz no intencionada, 2) falta de transparencia al momento de utilizar los datos y 3) brechas de seguridad que pueden ser explotadas por hackers. A continuación se procederá a explicar cada una estas categorías y posteriormente se expondrá el funcionamiento de los VPAs y cómo se manejan respecto a la privacidad y uso de terceros.

II-A. Captura de voz no intencionada

Un estudio llevado a cabo en usuarios de Alexa reveló que el 91 % de los participantes tuvo al menos una conversación almacenada sin consentimiento [14]. La conversación de una pareja que se grabó accidentalmente y se envió a un contacto aleatorio con el dispositivo Amazon Echo, es un claro ejemplo de cómo una conversación desacertada puede ser utilizada erróneamente [9]. Los VPAs no logran diferenciar cambios de contexto, esto permitió que un VPA llevara a cabo la compra

de 4 libras de galletas y una casa de muñecas, derivada de la conversación con una niña. [6].

II-B. Falta de transparencia por parte de las empresas al momento de utilizar los datos

Las empresas detrás de los VPAs ofrecen kits para el desarrollo de aplicaciones, estos otorgan acceso a la información interpretada por el VPA mientras la aplicación se encuentra en uso. Un skill o action es una aplicación que puede activarse mediante una palabra clave. Un estudio reveló que el 75 % de los skills alojados en la tienda oficial de Amazon carecen de políticas de privacidad [3]. Esto es alarmante debido a que el usuario está instalando una aplicación que no indica cómo serán manejados los datos que recolecte. Adicionalmente, se ha observado el uso de grabaciones almacenadas por los VPAs en procesos legales, tomando por sorpresa a los usuarios implicados [21].

De igual manera, la falta de políticas de privacidad ocasiona que la comprensión de los datos compartidos con aplicaciones de terceros sea escasa [5]. Existe evidencia de casos donde conversaciones realizadas en casa son utilizadas para presentación de publicidades[11]. Incluso personal de Amazon afirmó que los contactos se almacenan en el dispositivo, permitiéndoles acceder a esta información sin su consentimiento[11].

II-C. Brechas de seguridad que pueden ser explotadas por hackers.

Dado que los VPAs son dispositivos de escucha activa son propensos a enviar información de manera accidental a través de skills o actions desarrollados por terceros. Al decir de manera accidental la palabra que activa la aplicación, el VPA podría comenzar a recolectar audio del usuario, incluso si el usuario no se percata de ello. [17].

Los usuarios presentan preocupaciones en relación con la divulgación de información privada, sin embargo, esta información es necesaria para aprovechar los servicios de los VPAs. Un estudio que analiza los beneficios en relación con los riesgos percibidos, concluye que para alentar a los usuarios a compartir su información personal, es más efectivo reducir la gravedad percibida de la pérdida de información que equipar los VPAs con controles de seguridad más estrictos para mejorar los niveles de confianza. [20].

II-D. Funcionamiento de los asistentes personales

Los asistentes de Amazon y Google se activan a través de un método de autenticación de un solo factor, basado en una o varias palabras, similar a una contraseña (“Alexa”, “Ok Google”). Cualquier persona o máquina está en capacidad de activar un VPA, siempre y cuando se pronuncie la palabra de autenticación correcta. La activación es efectiva para sonidos con niveles de presión sonora superiores a 60dB [15].

Alexa y Google Assistant poseen un mecanismo de escucha permanente, capaces de recibir comandos de voz todo el tiempo. Existe una diferencia fundamental entre los asistentes del hogar y los asistentes de dispositivos móviles, estos últimos solo pueden recibir comandos de voz, después de que el teléfono se haya desbloqueado [15].

En el caso de Alexa, después de su activación, los comandos de voz que recibe los envía a una nube de procesamiento, por medio de la red Wifi, los comandos reconocidos como válidos son enviados a un servidor llamado “smart home skill adapter”, el cual a su vez los reenvía a otra nube que se encarga de realizar la petición del usuario[15]. Ver Fig. 1.

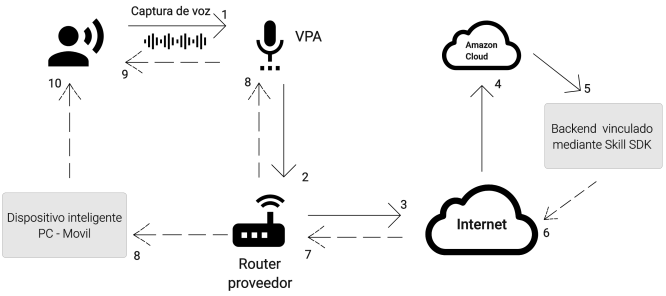

Figura 1. Servicio de voz de Alexa

Se ha comprobado que mientras Alexa está silenciada, no graba audio. Sin embargo, cuando no está silenciada, Alexa en ocasiones interactúa con el servicio de Amazon, aun cuando no se ha usado el comando de activación.[10].

Un estudio realizado a Google Home y Amazon Alexa, determina los datos en común almacenados que se pueden encontrar por comando de voz, los cuales son: (1) el texto del comando, (2) la marca de tiempo y (3) el nombre del dispositivo. Esta información fue extraída de la “actividad del asistente”, en el caso de Google Home y de la nube de Amazon en el caso de Alexa [5].

Los VPAs actualmente poseen características similares, pero de forma general estos pueden realizar tareas diversas como: (1) leer y enviar mensajes de textos o correos electrónicos, (2) realizar llamadas telefónicas, (3) responder a consultas básicas (Pronóstico del clima, hora o fecha actual, el resultado de una operación matemática), (4) establecer recordatorios, alarmas y eventos de calendario, (5) contar chistes e historias, (6) reproducción de medios conectados Netflix y Spotify, y (7) controlar dispositivos IoT como luces, alarmas, cerraduras de puertas, entre otros [13].

II-E. Privacidad y usos de terceros

La incertidumbre relacionada con las características de funcionamiento de los VPAs, tienen implicaciones en temas de privacidad y seguridad. El tiempo de almacenamiento, análisis, uso y vinculación de la información recolectada, entre otras, son factores determinantes. Los asistentes dependen en gran medida de los datos potencialmente privados, recopilados de los usuarios [16]. En un experimento previo se realizó un análisis de los datos almacenados por dispositivos Alexa, afirmando que esta información aumenta la posibilidad de entender el estilo de vida del usuario, además se ha logrado identificar patrones de horarios, intereses y lugares donde ha estado el usuario [7].

Aún si se deposita toda la confianza sobre el hardware y el sistema operativo esto no impide que los datos sean accedidos por terceros. Las empresas fabricantes buscan continuamente mejorar sus VPA's, por tal razón les otorgan acceso a sus empleados a los datos de los usuarios. También al dar acceso a un API o interfaz de desarrollo para estos VPAs, podrían permitir conocer información privada de los usuarios [17].

El que otras aplicaciones puedan activar el asistente también se convierte en un peligro. Una investigación que ofrece un método de omisión de permisos mediante una aplicación de Android, utiliza Google Voice Search para que realice operaciones provenientes de archivos de audio preparados por la aplicación en segundo plano. Sin necesidad de permisos, GVS-Attack, como lo denominaron sus creadores, puede obtener el control remoto del dispositivo permitiéndole acceder y transmitir información confidencial [8]. El estudio demostró que aunque una aplicación no requiere permisos, puede ser insegura.

III. Metodología

La presente investigación se centra en examinar el grado de conocimiento que poseen los usuarios sobre la administración y uso de los datos biométricos recolectados por los VPAs. Además, se realiza una comparativa, en relación con el nivel de privacidad y preservación de los datos obtenidos por los asistentes de Google y Amazon.

El proceso de investigación comenzó con la aplicación de un cuestionario denominado *Encuesta inicial*, la cual a través de una serie de preguntas permitió conocer el grado de conocimiento que tienen los usuarios sobre el uso de los datos recolectados por los VPAs. Además, esta encuesta permitió determinar quiénes serían las personas que participarían en la siguiente etapa de la investigación.

La *Encuesta inicial* fue realizada por 63 personas, la primera sección fue destinada a conocer datos demográficos, tales como edad y género. La segunda sección fue utilizada para conocer si los participantes han usado o están usando actualmente los VPAs, además de saber desde que dispositivos los usan y qué tipo de actividades acostumbran a ejecutar con los VPAs. Las siguientes secciones se describen a continuación.

Conocimiento sobre el funcionamiento de los VPAs:

- ¿Tiene conocimiento de que los VPAs lo están escuchando constantemente?
- ¿Tiene conocimiento de que sus conversaciones con el asistente personal se están grabando permanentemente?
- ¿Tiene conocimiento de que existe un historial de sus conversaciones con el asistente? ¿Ha revisado este historial?
- ¿Tiene conocimiento de que las conversaciones en el historial del asistente pueden ser eliminadas? ¿Ha eliminado conversaciones del historial?

Conocimiento sobre acceso a datos almacenados por el VPA por terceras personas:

- ¿Tiene conocimiento de que los empleados de las empresas desarrolladoras de los VPAs revisan sus conversaciones con el asistente?
- ¿Sabía usted que desarrolladores de aplicaciones (ajenos a la compañía fabricante) pueden reconocer las interpretaciones de sus comandos de voz, mientras usted interactúa con su aplicación?

Al finalizar la *Encuesta inicial* se seleccionó a un grupo voluntario de 14 usuarios actuales de VPAs para continuar con la siguiente fase.

La segunda fase consistió en aplicar durante un periodo de 4 semanas, un instrumento denominado *Encuesta semanal*. El objetivo era comparar el nivel de protección y preservación de los datos de los asistentes de Google y Amazon, considerando lo almacenado en sus historiales. Para esto, se utilizaron las preguntas que se enumeran a continuación:

- Total de interacciones reconocidas
- ¿Qué tipo de información encontró en las interacciones reconocidas?
- Total de interacciones no reconocidas
- ¿Qué tipo de información encontró en las interacciones no reconocidas?
- Total de activaciones accidentales

Para efectos del estudio, los datos almacenados como producto de una activación accidental fueron tratados como parte de la información encontrada en interacciones no reconocidas.

Para evitar confusiones, antes que iniciara el proceso, el equipo de investigación proporcionó a los participantes un vídeo tutorial en donde se indica como realizar el proceso de recolección de datos de forma correcta, también se enfatizó que las activaciones accidentales son aquellas que se producen cuando el asistente se activa sin haber recibido un comando de voz y esta activación es detectada por el usuario.

Luego, los participantes procedieron a registrar la información solicitada en la *Encuesta semanal*. Las fechas durante las cuales se desarrolló este proceso se describen en la Fig. 2. Los investigadores ofrecieron acompañamiento virtual cada fin de semana a los participantes, de tal forma que se asegure la integridad de la información.

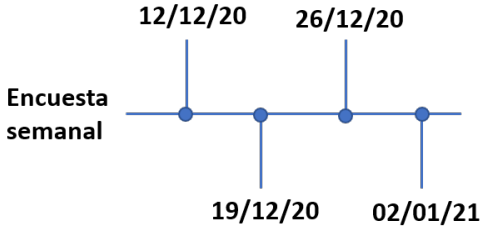

Figura 2. Fechas de ejecución de encuesta semanal

El proceso llevado a cabo en la investigación se describe en la Fig. 3.

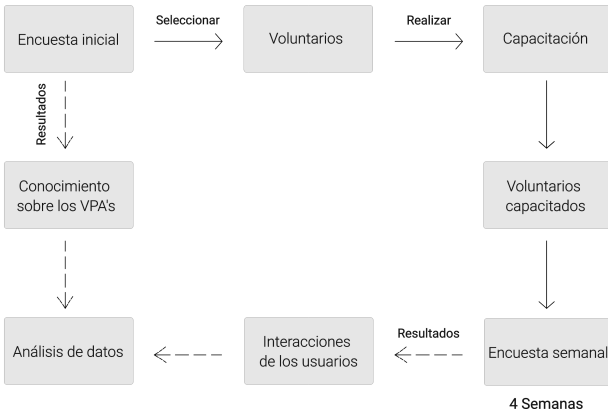

Figura 3. Proceso de la investigación

IV. Resultados

En esta sección se presentan los resultados obtenidos en la investigación.

La tabla I muestra las proporciones de los datos demográficos, obtenidos a partir de la aplicación de la encuesta inicial.

Tabla I
Datos demográficos de los encuestados

Rango de años	Femenino (%)	Masculino (%)
<18	1.59	1.59
19-28	**25.39**	**65.08**
39-48	3.17	0
49-58	1.59	1.59

IV-A. Uso del VPA

Para los resultados descritos a continuación solo se consideran a los participantes que son usuarios activos de los VPAs, los cuales representan el 44 % (28 personas) de encuestados.

De los dispositivos más usados para interactuar con los VPAs, se encontró que se usan celulares y parlantes inteligentes por igual. Los dispositivos menos utilizados son las tablets y Smart TVs, como se evidencia en la Fig. 4.

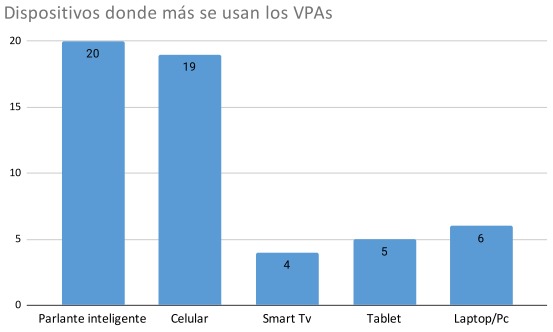

Figura 4. Respuesta a la pregunta de la encuesta inicial sobre los dispositivos en donde usa los VPAs

Entre las actividades que más realizan los participantes con sus VPAs se encuentran las opciones “Consultar información”, “Música” y “Gestionar alarma” y entre las menos realizadas “Domótica” y “Conversaciones”. En la Fig. 5 se puede apreciar los usos que se realiza con los VPAs.

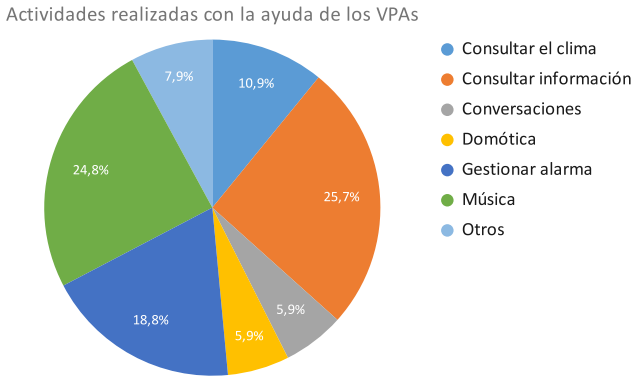

Figura 5. Respuestas de los participantes a la pregunta de la encuesta inicial sobre las actividades que realizan con los VPAs

IV-B. Conocimientos del usuario

En este apartado se describen los resultados considerando el 68.3 % de participantes (43 personas), los cuales corresponden a los usuarios que han usado o están usando VPAs.

La mayor cantidad de participantes aseguran conocer sobre la escucha constante de los VPAs, así mismo más de la mitad de encuestados desconocen sobre el almacenamiento permanente y la existencia de un historial en los asistentes, ver Fig. 6.

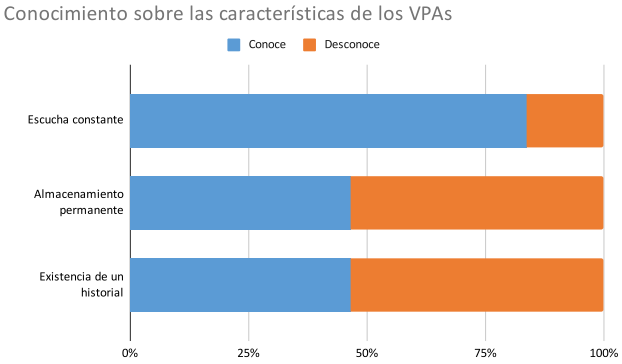

Figura 6. Respuestas de los participantes a las preguntas de la encuesta inicial sobre la escucha constante, el almacenamiento permanente y la existencia de un historial en los VPAs

Se examina el conocimiento que se tiene sobre el historial, descubriendo que menos de la mitad de los encuestados conocían la existencia de un historial en los VPAs, además solo un quinto de estos ha eliminado conversaciones de este historial, como se muestra en la Fig. 7.

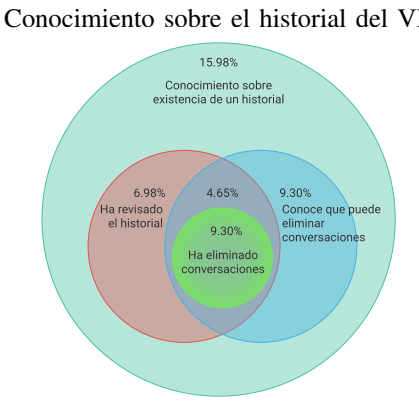

Figura 7. Respuestas de los participantes a las preguntas de la encuesta inicial sobre revisión y eliminación de conversaciones en el historial de los VPAs

La mayoría de los participantes no conocen que los empleados de las empresas fabricantes pueden escuchar sus conversaciones con el asistente. De forma similar desconocen que los desarrolladores pueden acceder a las interpretaciones de los datos capturados por los VPAs, ver Fig. 8.

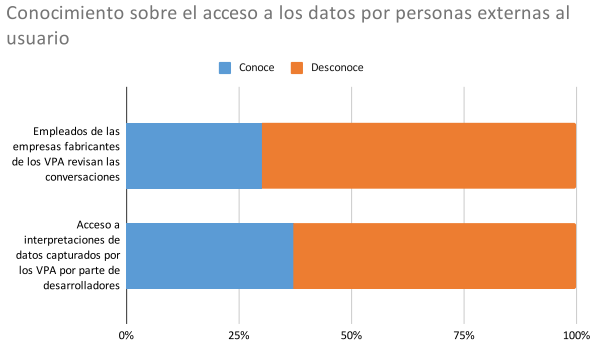

Figura 8. Respuestas de los participantes a las preguntas de la encuesta inicial sobre el acceso de empleados y desarrolladores a los datos recolectados por los VPAs

IV-C. Protección y preservación de los datos

En este apartado se describen los datos considerando 14 participantes, que son aquellos que decidieron involucrarse voluntariamente en la investigación. Del total de participantes, el 50 % de ellos poseen el asistente de Amazon y el otro 50 % el asistente de Google.

La tabla II muestra las proporciones de tipos de interacciones realizadas por los participantes en los respectivos asistentes.

Tabla II
PORCENTAJE DE INTERACCIONES POR TIPO DE ASISTENTE

Interacción	Amazon Alexa	Google Assistant
Reconocidas	**94.6 % (3143)**	79.1 % (763)
No reconocidas	3.4 % (113)	**8.8 % (85)**
Accidentales	2.0 % (65)	**12.0 % (116)**

Las actividades en las interacciones reconocidas con mayor frecuencia y comunes en ambos asistentes fueron: Búsqueda de información en la web y ejecución de aplicaciones y recordatorios, como se aprecia en la Fig. 9.

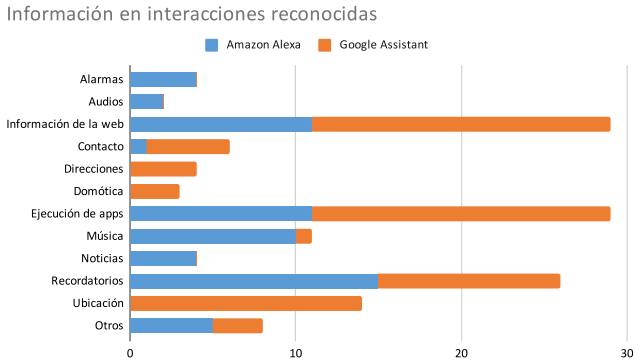

Figura 9. Respuestas a la pregunta de la encuesta semanal sobre la información encontrada en interacciones reconocidas

La actividad encontrada mayor cantidad de veces en las interacciones no reconocidas y común en ambos asistentes fueron los audios accidentales. La interacción menos registrada y común en ambos asistentes fueron los audios no entendibles, ver Fig. 10.

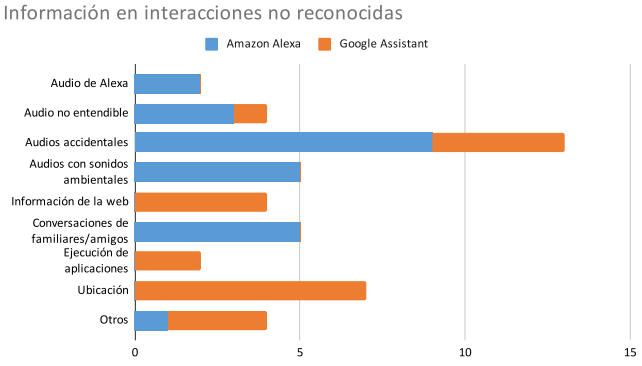

Figura 10. Respuestas a la pregunta de la encuesta semanal sobre la información encontrada en interacciones no reconocidas

Indiferente al VPA utilizado, más de la mitad de los participantes prensentó al menos una activación accidental. Solo el 34.5 % afirmó haber reconocido todas sus interacciones dentro de sus historiales.

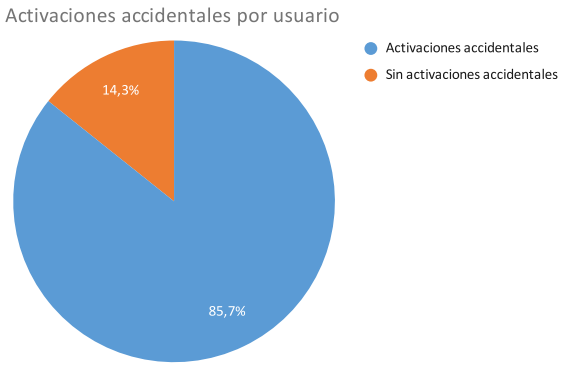

Figura 11. Porcentaje de usuarios que registraron por lo menos una activación accidental durante las 4 semanas

V. Discusión

Los usuarios participantes de la investigación son personas mayoritariamente jóvenes adultos con edades de entre 19 y 28 años (90.5 %) que acceden a los asistentes virtuales por medio de dispositivos celulares y parlantes inteligentes. Este segmento de usuarios realiza actividades de uso cotidiano como escuchar música o buscar información en la web con la asistencia del VPA.

Las personas son conscientes que los VPAs permanecen en escucha pasiva a la espera de un comando de voz de activación. Aun así, un poco mas de la mitad (53.3 %), no conocen que los asistentes almacenan permanentemente sus interacciones, mucho menos conocen que estos datos almacenados pueden ser accedidos desde un historial.

La proporción de usuarios que conocen sobre la existencia de un historial no es considerable (46.51 %), a pesar de esto son mucho menos los que lo han revisado (20.93 %). El conocimiento sobre la administración de los datos almacenados por el asistente va en función de un correcto manejo del historial. La investigación evidencia que son muy pocos los usuarios que revisan su historial y a la vez entienden que pueden eliminar datos de este (13.95 %). La correcta administración del historial permite a los usuarios decidir si la información registrada por el asistente debe ser eliminada o permanecer almacenada. Es importante señalar que aquellas personas que gestionan correctamente su información en el VPA, en su mayoría han optado por remover datos del historial.

Es importante para la privacidad que los usuarios sepan que terceros pueden tener acceso a sus datos. En el caso de los VPAs aproximadamente un tercio de los usuarios (30.2 %) conocen que las propias empresas desarrolladoras de los asistentes revisan sus conversaciones. Del mismo modo el 37.2 % de los usuarios llegan a conocer que los desarrolladores pueden acceder a interpretaciones de sus datos capturados por el VPA.

La responsabilidad de proteger los datos que se comparten con el VPA no solo recae sobre el usuario, el propio asistente debe asegurar que la información almacenada sea consistente, en sentido que el usuario pueda reconocer cada una de sus interacciones. Los asistentes de Amazon y Google poseen un porcentaje aceptable de interacciones reconocidas como realizadas (94.6 % y 79.1 % respectivamente). Aun así, hay un pequeño margen de error que se traduce en interacciones no reconocidas para ambos asistentes, resaltando Google Assistant por ser el más propenso a registrar interacciones sin consentimiento del usuario.

La información que se almacena en el historial de los VPAs, como resultado de las interacciones reconocidas como realizadas, se debe a la realización de actividades de uso cotidiano, esto es cierto para ambos asistentes. Al evaluar las interacciones no reconocidas por los usuarios, en el caso de Alexa, se presentan datos que se alejan completamente del perfil de usuario utilizado en esta investigación, mientras que Google Assistant muestra información que es comparable con las interacciones reconocidas.

Las interacciones no reconocidas son producto de activaciones accidentales del asistente no percibidas por los usuarios. Estas activaciones son muy comunes entre usuarios de VPAs (85.7 %), siendo Google Assistant el más propenso a salir de su estado de escucha pasiva sin recibir un comando de activación, en comparación con Amazon Alexa.

VI. Conclusiones

Los resultados obtenidos demuestran que los usuarios poseen conocimiento sobre la escucha constante, la existencia del historial y la posibilidad de administración de sus datos, pero no realizan una correcta gestión de su información demostrando un alto grado de desconocimiento sobre el cuidado de sus datos producto de interacciones con los asistentes. Del mismo modo se demuestra poco conocimiento sobre el acceso que terceros pueden llegar a tener a los datos almacenados por los VPAs.

Con respecto a la protección presentada por cada VPA, Google Assistant es más propenso a activarse sin el consentimiento del usuario, pero presentó un mejor cuidado con el almacenamiento de las interacciones a diferencia de Amazon Alexa, que registró información que está fuera de lo considerado normal para los usuarios.

VII. Recomendaciones

La presente investigación se realizó con una cantidad equivalente de dispositivos Alexa y Google Assistant. No obstante, se recomienda llevar a cabo la investigación en dos partes una para smart phones y otra para parlantes inteligentes. Los smart phones acompañan todo el tiempo al usuario aun cuando salen de su hogar, a diferencia de los parlantes inteligentes los cuales permanecen en el hogar, además, no ofrecen una capa adicional de seguridad (bloqueo o suspensión del dispositivo). Por ello es recomendable reducir esta disparidad de tipo al máximo, buscando comparar en igualdad de condiciones ambos VPAs.

VIII. Reconocimientos

Nos gustaría agradecer a los participantes de la investigación, los cuales respondieron las encuestas semanalmente y

llevaron un control con respecto a sus interacciones. También agradecer al MSc. Rafael Bonilla y a la PhD. Otilia Alejandro por su guía y mentoría en la elaboración de esta investigación.

Referencias

[1] Instituto nacional de estadÍsticas y censos, encuesta multipropósito - tic diciembre 2019.

[2] Seguridad y privacidad de los datos de dispositivos que funcionan con asistente - ayuda de google nest.

[3] Abdulaziz Alhadlaq, Jun Tang, Marwan Almaymoni, and Aleksandra Korolova. Privacy in the amazon alexa skills ecosystem. *Star*, 217(11), 1902.

[4] Allot. Vulnerabilities of digital assistants — threat bulletin. 2019.

[5] Tawfiq Ammari, Jofish Kaye, Janice Y Tsai, and Frank Bentley. Music, search, and iot: How people (really) use voice assistants. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 26(3):1–28, 2019.

[6] Hyunji Chung, Michaela Iorga, Jeffrey Voas, and Sangjin Lee. Alexa, can i trust you? *Computer*, 50(9):100–104, 2017.

[7] Hyunji Chung and Sangjin Lee. Intelligent virtual assistant knows your life. *CoRR*, abs/1803.00466, 2018.

[8] Wenrui Diao, Xiangyu Liu, Zhe Zhou, and Kehuan Zhang. Your voice assistant is mine: How to abuse speakers to steal information and control your phone. In *Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices*, pages 63–74, 2014.

[9] Ben Dickson. Beware the privacy and security risks of smart speakers, 2018.

[10] Marcia Ford and William Palmer. Alexa, are you listening to me? an analysis of alexa voice service network traffic. *Personal and Ubiquitous Computing*, 23(1):67–79, 2019.

[11] Nathaniel Fruchter and Ilaria Liccardi. Consumer attitudes towards privacy and security in home assistants. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–6, 2018.

[12] Google. How google protects your privacy if you choose to save audio data, 2020.

[13] Matthew B Hoy. Alexa, siri, cortana, and more: an introduction to voice assistants. *Medical reference services quarterly*, 37(1):81–88, 2018.

[14] Yousra Javed, Shashank Sethi, and Akshay Jadoun. Alexa's voice recording behavior: A survey of user understanding and awareness. In *Proceedings of the 14th International Conference on Availability, Reliability and Security*, pages 1–10, 2019.

[15] Xinyu Lei, Guan-Hua Tu, Alex X Liu, Chi-Yu Li, and Tian Xie. The insecurity of home digital voice assistants-vulnerabilities, attacks and countermeasures. In *2018 IEEE Conference on Communications and Network Security (CNS)*, pages 1–9. IEEE, 2018.

[16] Yuting Liao, Jessica Vitak, Priya Kumar, Michael Zimmer, and Katherine Kritikos. Understanding the role of privacy and trust in intelligent personal assistant adoption. In *International Conference on Information*, pages 102–113. Springer, 2019.

[17] Nathan Malkin, Serge Egelman, and David Wagner. Privacy controls for always-listening devices. In *Proceedings of the New Security Paradigms Workshop*, pages 78–91, 2019.

[18] Giles Turner Matt Day and Natalia Drozdiak. Amazon listening to what you tell alexa, 2019.

[19] Christi Olson. New report tackles tough questions on voice and ai.

[20] Debajyoti Pal, Chonlameth Arpnikanondt, and Mohammad Abdur Razzaque. Personal information disclosure via voice assistants: The personalization–privacy paradox. *SN Computer Science*, 1(5):1–17, 2020.

[21] Anne Pfeifle. Alexa, what should we do about privacy: Protecting privacy for users of voice-activated devices. *Wash. L. Rev.*, 93:421, 2018.

[22] Yi Min Shum. Situación global mobile 2020 - 5.190 millones de usuarios únicos.