Manejo de datos personales en dispositivos IoT, específicamente en televisores inteligentes

Leidy Zulieth Bonilla Mahecha

Ana Cecilia León Vargas

Trabajo de Grado presentado para optar al título de Especialista en Seguridad de la Información

Asesor: Nelson Augusto Forero Páez, Magíster (MSc) en Educación

Universidad Católica de Colombia

Facultad de Ingeniería

Especialización en Seguridad de la Información

Bogotá D.C., Colombia

2019

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

Es importante considerar que entre más usuarios adquieren dispositivos Smart TV los cuales hacen parte del Internet de las Cosas IoT, mayor es el incentivo que encuentran los ciberatacantes para hallar nuevas formas de atacar y conseguir la información.

El objetivo de este documento es realizar un análisis de los datos que los usuarios registran en los Smart TV y en las aplicaciones de mayor uso que son instaladas en este dispositivo, con el fin de identificar la información susceptible de ataques, así mismo a los Smart TV y las aplicaciones Youtube, Netflix y Spotify, se realizará un comparativo de los datos registrados en estos tanto en el dispositivo como en las aplicaciones frente a los ataques, con el fin de construir los lineamientos de seguridad.

Finalmente se definirán unas recomendaciones sobre la administración de datos personales almacenados en los Smart TV y en las aplicaciones, mediante la elaboración de un manual de buenas prácticas.

Palabras clave: Internet de las Cosas IoT, ataques, Smart TV, datos personales, privacidad, seguridad de datos.

ABSTRAC

It is important to consider that the more users acquire Smart TV devices which are part of the IoT Internet of Things, the greater the incentive that cyber attackers find to find new ways to attack and get information.

The purpose of this document is to perform an analysis of the data that users record on the Smart TVs and in the most commonly used applications that are installed on this device, in order to identify the information susceptible to attacks, as well as to the Smart TVs and the Youtube apps, Netflix and Spotify, will make a comparison of the data recorded in these both on the device and in the applications against attacks, in order to build the security guidelines.

Finally, recommendations on the management of personal data stored on Smart TVs and applications will be defined by developing a best practice manual.

Keywords: IoT Internet of Things, attacks, Smart TV, personal data, privacy, data security.

I. INTRODUCCIÓN

Los Televisores Inteligentes (Smart TV) son hoy en día uno de los dispositivos que conforman el Internet de las Cosas (IoT), los cuales tienen muchas funcionalidades, entre las que se encuentran la navegación por internet para acceder a las redes sociales y a video en streaming a través de sitios web como YouTube y Netflix, acceso a juegos en línea, hacer videollamadas por medio de webcam. Para hacer uso de estas funcionalidades, es necesario realizar el registro de datos personales, en donde posiblemente los usuarios no emplean los mecanismos de seguridad mínimos que ofrecen los fabricantes de las aplicaciones, lo cual hace que estos sean cada vez más susceptibles de ataques por parte de los ciberdelincuentes, quienes están en la capacidad de generar códigos maliciosos para facilitar el acceso y ser una potencial amenaza para la seguridad de la información.

El objeto de estudio de este proyecto es analizar los ataques de ingeniería social realizados a los televisores Smart TV, con el fin de identificar las brechas de seguridad de la información de los usuarios y de las aplicaciones que se utilizan en este tipo de dispositivos durante los últimos tres años y, con este análisis, elaborar un manual de buenas prácticas que contenga los lineamientos generales en el registro de la información y manejo de las aplicaciones en estos dispositivos.

Los Smart TV pasan a estar accesibles al mundo, lo que permite recabar multitud de datos en su entorno, realizar actualizaciones de software para que funcione mejor, y a su vez se expone a ataques que se convierten en un elemento que contribuye, por su efecto multiplicador, a la vulnerabilidad de internet y por tanto a la inseguridad de todos [1]

El trabajo fue estructurado para dar respuesta a la siguiente pregunta de investigación ¿Cómo pueden los usuarios que usan Televisores inteligentes (Smart TV), protegerse de los ataques de ingeniería social al registrar su información personal en las aplicaciones que se instalan en este tipo de dispositivos?, para lo que se definió las actividades establecidas en el cronograma y que se desarrollaran en tres fases.

II. GENERALIDADES

A. Línea de Investigación

El presente anteproyecto se desarrolla bajo la línea de investigación: Software inteligente y convergencia tecnológica

B. Planteamiento del Problema

Actualmente entre los dispositivos que conforman el Internet de las Cosas (IoT) encontramos los Televisores Inteligentes (Smart TV), los cuales forman parte del diario vivir de millones de usuarios. A medida que estos dispositivos adquieren más funcionalidades, la cantidad de datos personales registrados y la susceptibilidad de estos son cada vez más relevantes para los ciberdelincuentes, porque posiblemente los usuarios no hacen uso de los mecanismos de seguridad mínimos que ofrecen los fabricantes para el almacenamiento de los datos personales, y de esta manera evitar ser víctimas de ataques de ingeniería social.

1) Antecedentes del problema

Con los avances tecnológicos de los televisores, "se ha descubierto que millones de Smart TVs de distintos fabricantes distribuidos por todo el mundo podrían ser vulnerables a ataques que derivarían en el control total sobre los dispositivos, abriendo la puerta a acciones como rastrear los hábitos de los usuarios, los cuales pueden ser utilizados para recomendar contenidos según las preferencias de los usuarios, además de enviar publicidad dirigida. Los datos recopilados pueden ser combinados con otros de carácter personal para construir perfiles que podrían ser comercializados con fines desconocidos" [2] y también sirve para realizar ataques de ingeniería social.

Según lo que revelo el estudio desarrollado por Rafael Scheel, investigador de seguridad de la consultora Oneconsult en marzo del 2017 "El 90% de los televisores conectados a Internet que funcionan con el sistema operativo Android son vulnerables a piratería remota, sobre todo aquellos que usan señales de televisión no autorizadas" [3], con lo cual se demostró que se podía tomar completamente el control del televisor inteligente sin necesidad de tener acceso físico al mismo.

Para ese mismo año un investigador de seguridad israelí llamado Amihai Neiderman, descubrió 40 vulnerabilidades de día cero que permitían 'hackear' televisores de forma remota sin necesidad de estar conectado físicamente, en el cual estaban involucrados los televisores de marca Samsung que utilizan el sistema operativo propietario Tizen [4].

Para el 2018, en el marco del Mobile World Congress, la compañía de ciberseguridad ESET a través de Tony Anscombe, informo que luego de hacer un estudio con los técnicos del laboratorio de la misma compañía, establecieron que el malware de las criptomonedas también estaba presente en los SmartTV Los ciberdelincuentes podrían espiar las actividades de una familia, usar la televisión infectada para apropiarse de otros dispositivos del hogar, obtener datos confidenciales o hasta secuestrarla con un ransomware. Hemos visto SmartTV infectadas con malware que mina criptomonedas o que actúa en segundo plano para analizar lo que ves en la televisión", asegura el evangelista global de ESET, Tony Anscombe [5].

Durante el último año se evidencio que la marca más atacada fue Samsung, lo cual quedo demostrado en una noticia publicada por Hardwaresfera en su página web en enero de 2019, en el cual se supo que los atacantes eran una pareja conocida como HackerGiraffe y j3ws3r, quienes consiguieron hackear dispositivos relacionados con Chromecast, Google Home y SmartTV de varias marcas, "Consiguieron acceder a estos dispositivos de manera remota para poder lanzar este contenido multimedia. Además, los atacantes pueden resetear a los valores de fábrica los dispositivos, realizar un reinicio, borrar las redes WiFi almacenadas y otras acciones, mayormente inofensivas", puntualmente lo relevante del ataque fue conseguir molestar a los usuarios al poner imágenes promocionales del youtuber con más seguidores PewDiePie en los SmartTV. [6]

Dentro del informe desarrollado y presentado por ESET SMART TV: ¿una puerta trasera en nuestro hogar?, se menciona que la técnica que se puede usar para ejecutar algún código malicioso en el entorno de la víctima es la Ingeniería social, y el aprovechamiento de las vulnerabilidades como las malas configuraciones y también ataques físicos. Estas técnicas y fallas permiten a los atacantes ganar control del equipo [7].

Los expertos del Laboratorio de Investigación de ESET Latinoamérica han compartido las siguientes medidas preventivas para mitigar los ataques a los Smart TV:

- Contar con alguna solución de seguridad: Estas ofrecen protección contra amenazas para Smart TV, en particular, para aquellas distribuciones basadas en Android, además de módulos capaces de prevenir infecciones por malware y de detectar páginas fraudulentas para bloquear el acceso a ellas (funcionalidad denominada antiphishing).
- Configurar los dispositivos: Reforzar los ajustes del dispositivo para asegurarse de no dejar huecos de seguridad. Restringir los orígenes desconocidos, verificar aplicaciones, no mostrar las contraseñas, crear perfil restringido, deshabilitar la depuración y la recolección de datos por defecto.
- Reforzar la seguridad de la red: utilice protocolos seguros y credenciales fuertes, y que su firmware no presente vulnerabilidades.
- Protección física: se debe tener en cuenta la protección de las entradas físicas del dispositivo. Para ello, se puede activar la protección mediante soluciones de seguridad [7].

2) Pregunta de investigación

¿Cómo pueden los usuarios que usan Televisores inteligentes (Smart TV), protegerse de los ataques de ingeniería social al registrar su información personal en estos dispositivos y en las aplicaciones que se instalan en los mismos?

3) Variables del problema

Vulnerabilidades presentes en los Smart TV para identificar el tipo de información sensible que puede llegar a compartirse y que representan un riesgo para el usuario.

Identificación de los ataques que se pueden realizar a los Smart TV y a las aplicaciones instaladas, para plantear un manual de buenas prácticas que contenga los lineamientos generales en el registro de la información y manejo de las aplicaciones en estos dispositivos.

El registro de los datos personales en las diferentes aplicaciones instaladas en los Smart TV.

C. Justificación

Según estudios realizados por ESET Latinoamérica los cuales revelan que realizar ataques a los Smart TV cada vez es más fácil ejecutarlos, y por lo general sin necesitar un acceso físico al dispositivo o de la interacción con el usuario. También ha sido demostrado en varias ocasiones que, una vez comprometido un Smart TV, este puede servir como punto de partida para ataques a otros dispositivos que se encuentran conectados en la misma red, apuntando finalmente a la información personal del usuario almacenada.

Los Smart TV cada vez son más comercializados, según portal de estadísticas online Statista en 2018 se vendieron más de 114 millones de televisores inteligentes alrededor del mundo. Ese volumen representaría el 70% de todos los televisores vendidos durante ese año, según IHS Markit, empresa proveedora de información global [8].

De acuerdo a este panorama, en Colombia observamos que esta tendencia va en aumento de acuerdo con cifras de Euromonitor, las marcas líderes de este mercado en el país el año pasado fueron Samsung con 34,7%, seguido de LG con 25,7% y Kalley con 7,2%. En cuarta y quinta posición se encuentra Challenger y Hyundai [9].

Cuando un Smart TV se conecta a la red, se debe tener en cuenta que los demás dispositivos que estén conectados pueden ser blancos de ataques, donde el impacto más alarmante es el robo de la privacidad. Basados en que la mayoría de dispositivos de este tipo trabajan hoy en día con alguna distribución del sistema operativo Android, es más sencillo para los atacantes generar códigos maliciosos, realizar ataques dirigidos y amenazas, afectando así equipos de diferentes fabricantes, siendo muy importante para los usuarios que tomen consciencia de que estas amenazas existen, y se requiere más protección en sus dispositivos. Para ello es necesario que realicen un registro adecuado de sus datos personales en las aplicaciones instaladas en los Smart TV, como también tener en cuenta la implementación de buenas prácticas, y al descargar aplicaciones hacerlo a través de tiendas oficiales, desactivar la conexión por Bluetooth cuando no se requiera, crear un perfil restringido, entre otras.

III. OBJETIVOS

A. Objetivo general

Diseñar un manual de buenas prácticas de administración de datos personales registrados en las aplicaciones instaladas en los Smart TV para reducir los ataques de ingeniería social.

B. Objetivos específicos

1. Analizar cuál es la información que los usuarios registran en las aplicaciones instaladas en los Smart TV, para identificar qué información es susceptible de ataques
2. Identificar los ataques más importantes que han sufrido los Smart TV y las aplicaciones Youtube, Netflix y Spotify.
3. Comparar los datos registrados en el Smart TV y las aplicaciones frente a los ataques realizados, para construir los lineamientos de seguridad de los datos.

IV. MARCOS DE REFERENCIA

A. Marco conceptual

IoT (Internet of Things): es el componente tecnológico el término Internet de las Cosas se refiere a escenarios en los que la conectividad de red y la capacidad de cómputo se extienden a objetos, sensores y artículos de uso diario que habitualmente no se consideran computadoras, permitiendo que estos dispositivos generen, intercambien y consuman datos con una mínima intervención humana [10].

IoT se ha desarrollado por medio de la hiperconectividad de diversos instrumentos de la vida cotidiana con las IT, contribuye a maximizar la eficiencia de todas y cada una de las actividades sobre las que se aplican, y es el ejemplo práctico más evidente de la incidencia del ciberespacio en todos los ámbitos de la realidad física [11].

Smart TV: televisión inteligente, dispositivo receptor conectado a internet que puede dar acceso a emisiones televisivas [12]. La conexión a internet puede ser Ethernet directa, por cable o una conexión Wi-Fi y de esta manera acceder a servicios en línea como transmisión de video, redes sociales o simplemente navegar por la web.

Aplicación: Es un programa informático que le permite a los usuarios interactuar con el dispositivo que lo tiene instalado, con el fin de realizar diferentes actividades, entre ellas trabajo, entretenimiento, etc [13].

Dato Personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables [14].

Dato Sensible: son aquellos que pueden producir algún trato discriminatorio. A que afectan la intimidad, tales como la información crediticia, médica, origen étnico, preferencias sexuales, creencias religiosas o políticas, estado de salud o mental [15].

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión [14].

Ataque: Es un intento organizado e intencionado causada por una o más personas para causar daño o problemas a un sistema informático o red [16].

Vulnerabilidad: Es un fallo de seguridad en un programa o en un sistema de información [17].

Vulnerabilidad del día cero: Está relacionada con que un proveedor lanza al mercado un nuevo producto con alguna brecha de seguridad, la cual es de total desconocimiento por los fabricantes [18].

Vulnerabilidad de desbordamiento de búfer: Este se produce cuando se copia una cantidad de datos de manera no controlada sobre un espacio que no es lo suficientemente grande para abarcarlos, sobrescribiendo de esta manera otras zonas de memoria [19].

Ataque Man in the Middle: Son un tipo de ciber-espionaje que intercepta, envía y recibe datos nunca conocidos por las víctimas, hacerse pasar por una de las partes durante una sesión [1].

Malware: un programa malicioso, diseñado para que usuarios no autorizados accedan a un sistema de información sin autorización de su propietario y producir efectos indeseados en este [17].

Ransomware: del inglés *ransom* rescate y *ware* de software, es un tipo de programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado, y demanda un rescate a cambio de quitar una restricción. Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate [20].

Ataques de inyección de comando: Son usados para la ejecución de los mismos en una aplicación, con el fin de extraer información guardada en los dispositivos [21].

Ataque dirigido: Es un proceso a largo plazo que pueden comprometer la seguridad y dan acceso a los atacantes el control de los sistemas TI de la víctima [22]**.**

Amenaza: es cualquier entidad o circunstancia que atente contra el buen funcionamiento de un sistema informático [23].

Ingeniería Social: Es una forma de fraude informático muy utilizado por piratas informáticos y consiste en manipular el comportamiento natural de los usuarios mediante engaños y mentiras [23].

Privacidad de información: comprende las acciones transversales tendientes a proteger la información de acceso, uso, divulgación, interrupción o destrucción no autorizada [24].

Ciberdelincuencia: Se refiere a delitos contra computadoras y sistemas de información, con el objetivo de lograr el acceso no autorizado a un dispositivo o negar el acceso a un usuario legítimo [25].

B. Marco teórico

El presente trabajo de investigación se orienta a analizar los ataques de ingeniería social a los cuales los usuarios de Smart TV se encuentran expuestos al realizar el registro de sus datos personales en las aplicaciones de mayor uso instaladas en estos dispositivos, es necesario identificar cuáles son los datos y la información que se está registrando, dado que estos son considerados como un activo económico de gran importancia para los ciberdelincuentes, como también lo es para los proveedores de las aplicaciones más utilizadas como lo son Netflix y Youtube, HBO GO y Disney Channel [26] para garantizar la protección de estos datos.

Gartner define IoT como "la red de objetos físicos con tecnología embebida que les permite comunicar, sentir e interactuar con su estado interno o con su entorno exterior" [27].

Ampliando el concepto dado por Gartner, se puede decir que IoT suele referirse a una amplia red de dispositivos con sensores, los cuales están diseñados para recopilar datos acerca de su entorno, la mayoría de las veces incluyen datos de las personas. Estos datos posiblemente proporcionan un beneficio al propietario del dispositivo, pero muchas veces también benefician al fabricante o proveedor. La recopilación y el uso de los datos se convierte en una consideración de privacidad cuando las expectativas de privacidad de quienes son observados por los dispositivos de la IoT difieren de las de quienes recogerán y usarán estos datos [10].

En el año 1978 James Martin explicaba que en la sociedad los seres humanos se pueden sentir como osos polares o como un conejillo de indias a los que se les haya conectado un radio transmisor en miniatura con capacidad de enviar continuas señales a un satélite, que van a poder ser registradas y seguidos desde un ordenador [28].

Esta afirmación en la actualidad es cada día más aplicada de lo que parece, en muchos casos por comportamiento y estilo de vida. Cuando los dispositivos o implementaciones no garanticen un

nivel aceptable de seguridad en la identificación, privacidad e integridad en las comunicaciones, es muy probable que estas deficiencias puedan ser aprovechadas por un atacante [29].

En los Smart TV se pueden descargar e instalar aplicaciones de terceros que amplían su funcionalidad. En algunos de estos casos se pueden emplear estas aplicaciones como una puerta de entrada para tomar el control del dispositivo, o para obtener la información registrada. Este tipo de ataque se puede ejecutar de dos formas posibles; la primera explotando vulnerabilidades identificadas en el software, y la segunda descargando aplicaciones maliciosas, bien sea desde una fuente oficial que no analice suficientemente la seguridad de las aplicaciones que incorpora, o bien desde un canal no oficial de aplicaciones [29].

Aunado a lo anterior, los usuarios pueden no ser conscientes de que un dispositivo está recogiendo datos y potencialmente compartiéndolos con terceros. Este tipo de recolección de datos es cada vez más frecuente en los dispositivos de consumo, como por ejemplo en los televisores inteligentes, los cuales tienen características de reconocimiento de voz o de visualización que permanentemente escuchan las conversaciones y selectivamente transmiten los datos recogidos a un servicio en la nube para su procesamiento, donde a veces participa un tercero. Estos tipos de características pueden ser de beneficio para un usuario informado, pero pueden plantear un problema de privacidad para quienes no son conscientes de la presencia de estos dispositivos y no pueden influir significativamente sobre la forma en que se utiliza la información recogida [10].

Los Smart TV almacenan los datos personales, este escenario ponen en evidencia la importancia que tienen este tipo de datos para las empresas y atacantes que buscan sacar la máxima ventaja de la información obtenida a través de estos dispositivos.

Es primordial afrontar esta problemática de privacidad de los datos personales, dado que tienen serias implicaciones sobre los derechos básicos y la capacidad de confiar en Internet y de la información que allí se encuentra.

C. Estado del arte

El estado del arte que se expone en el presente documento, está enfocado básicamente en dos aspectos, el primero de ellos tiene que ver con la privacidad de la información y el segundo con las

vulnerabilidades en los televisores inteligentes Smart TV, ambos aspectos están relacionados con trabajos de investigación realizados internacionalmente.

Investigaciones Internacionales

Los ingenieros Benjamin Michéle y Andrew Karpow, pertenecientes al Grupo de Investigación de Seguridad en Telecomunicaciones del Instituto de Tecnología de Berlín, han participado en varios proyectos de investigación relacionados con la seguridad de dispositivos integrados, especialmente televisores inteligentes y decodificadores. Hacia el año 2014 publicaron un artículo sobre su investigación que titularon "Watch and be Watched: Compromising All Smart TV Generations", en este mostraron que los televisores inteligentes en su estado actual no deben considerarse confiables y, por lo tanto, representan una grave amenaza para la seguridad y la privacidad [30].

Demostraron que el reproductor multimedia integrado, que se ofrece en casi todos los Smart TV del mercado, desde el nivel de entrada hasta los modelos de gama alta e independientemente del proveedor, es altamente vulnerable, para mostrar esto, desarrollaron un ataque práctico de prueba de concepto utilizando un archivo de video malicioso que le da al atacante un control permanente y completo sobre el dispositivo, pero que el usuario no puede detectar por completo. Además, proporcionaron cargas útiles totalmente funcionales para aprovechar sigilosamente la cámara y el micrófono de un televisor, pero es completamente indetectable por el usuario [30].

En cuanto a las aplicaciones que se utilizan en este tipo de dispositivos, sus apreciaciones estuvieron relacionadas a que estas al ejecutarse en un entorno limitado no son fácilmente explotables, sin embargo, pueden almacenar información sensible, que un atacante puede robar una vez que el televisor ha sido comprometido por otros medios.

De esta publicación concluyeron entre otros aspectos, que la mayoría de los modelos de TV cuentan con firmware de actualizaciones solo por unos años. Esto, sin embargo, es mucho más corto que la vida útil promedio de un televisor, por lo tanto, exponiendo finalmente todos los televisores inteligentes a vulnerabilidades recién descubiertas. Por otro lado, Instamos a los proveedores a prestar más atención a la seguridad manejo de archivos multimedia. Los proveedores deben aplicar todas las correcciones de seguridad disponibles utilizando versiones recientes de bibliotecas. Además, en lugar de ejecutarse con todos los privilegios del sistema, el código correspondiente debe seguir el principio del mínimo privilegio [30].

Otra investigación fue la realizada en el año 2017, por Kristina Irion y Natali Helberger titulada como “Smart TV and the online media sector: User privacy in view of changing market realities”, en este mostraron que la recopilación de información sobre el comportamiento de visualización de los usuarios puede proporcionar información muy detallada y e información sensible sobre lo que los usuarios piensan, saben y creen. Por lo tanto, argumentaron el tema de que la privacidad requiere atención especial, no solo desde la perspectiva de la ley de protección de datos, sino también de la ley y política de medios [31].

Después de su investigación sobre los flujos de datos personales de televisores inteligentes, el instituto de pruebas de consumo alemán recomendó que los usuarios deberían deshabilitar la funcionalidad de HbbTV o no conectar el televisor inteligente a Internet (Stiftung Warentest, 2014). Esto no puede ser el camino correcto a seguir, pero debería ser un llamado de atención a los responsables políticos nacionales y de la UE para evaluar los nuevos riesgos para la privacidad de los usuarios. En este artículo, argumentaron que recopilar información sobre los medios de los usuarios el consumo no solo plantea problemas sobre la privacidad y la protección de datos, sino también sobre la ley y política de medios (audiovisuales) en UE y en los estados miembros [31].

La siguiente investigación fue la realizada en el año 2015, denominada “Smart-TV security analysis: practical experiments” [32] en esta el objetivo principal era explorar experimentalmente posibles vectores de ataque e identificar vulnerabilidades y escenarios de ataque prácticamente explotables. En particular, el estudio cubre ataques locales y remotos utilizando diferentes puntos de entrada, incluido el Canal de transmisión de Digital Video Broadcasting (DVB) y el bucle local de par de cobre [31].

En las conclusiones planteadas, abordan varias contramedidas para afrontar las debilidades encontradas. Estos incluyen:

1) Generalizar el uso de métodos criptográficos durante situaciones intercambios críticas. En este estudio pudieron ver que muchos Smart-TV los fabricantes ya han optado por usar el protocolo seguro HTTPS u otros cifrados patentados para asegurar su proceso de actualización de firmware.
2) Medición de la variación de atenuación de señal en la línea ADSL, ya que este valor debería cambiar drásticamente cuando uno inserta nuestra plataforma en la red local.

3) Medición de la variación de la intensidad de la señal de TV, ya que este valor debería cambiar drásticamente cuando uno activa nuestra solución de simulación DVB.
4) Implementar correctamente política en navegadores Smart-TV, como cualquier otra política estándar seguridad. El navegador utilizado por un Smart-TV debe ser al menos tan seguro como los que se usan en las PC.
5) Implementación de cifrado o Técnicas de autenticación en señales DVB. [31].

V. METODOLOGÍA

A. Fases del trabajo de grado

Lo primero que se realizo fue es un análisis de las aplicaciones más usadas en los Smart TV, luego para las aplicaciones del alcance del proyecto, se identificó qué información es susceptible de ataques.

Se identificaron los ataques que han sufrido los Smart TV y las aplicaciones Youtube, Netflix y Spotify, también se compararon los ataques evidenciados en el Smart TV y las aplicaciones, para construir los lineamientos de seguridad de los datos. Finalmente se definieron las buenas prácticas de administración de datos personales almacenados en los Smart Tv, mediante la elaboración de un manual de buenas prácticas con los lineamientos generales del registro de la información personal.

B. Instrumentos o herramientas utilizadas

Se utilizaron un Smart Tv con Netflix y Youtube, y Spotify instalados, los sitios web respectivos para cada una de las aplicaciones definidas en el alcance del proyecto, como también 2 computadores portátiles y los programas de ofimática Word y Excel.

C. Población y muestra

El proyecto está dirigido a la población en general que utiliza Smart TV en los hogares.

D. Alcances y limitaciones

Alcance

- Identificar como por medio de las aplicaciones Netflix, Youtube y Spotify instaladas en un Smart TV se puede presentar la perdida de privacidad de la información, para ser utilizada con fines económicos no autorizados por los usuarios.
- Los Smart TV objeto de estudio abarca solamente los que su conexión es a través de red inalámbrica.

- Buscar una solución a nivel de buenas prácticas de seguridad para proteger la información personal en este tipo de dispositivos.
- Para el estudio se va a tener en cuenta la información de los años 2018 y el 2019.

Limitaciones

- Dificultad en la consecución de la información relacionada a los ataques realizados a las aplicaciones instaladas en los Smart TV y a los propios dispositivos.

VI. PRODUCTOS A ENTREGAR

Para cumplir con el objetivo de esta investigación, los productos que este proyecto entrega son:

- Una relación de las aplicaciones más usadas en los Smart TV, en la cual se da una breve descripción de cada una.
- Una recopilación de los datos personales que solicitan las aplicaciones Youtube, Netflix y Spotify, con el fin de identificar cuáles son los datos que actualmente recogen estas aplicaciones.
- Un reporte de los ataques realizados a Smart TV y a las aplicaciones Youtube, Netflix y Spotify usadas en los mismos durante los años 2018 y 2019, para evidenciar cuales han sido los ataques y si los mismos se han repetido para este período.
- Un análisis comparativo de los datos registrados en los sistemas operativos de los Smart TV de las marcas LG, Samsung y Panasonic el Smart TV y de las aplicaciones, identificar cual es el tipo de información que más estaría expuesta al momento de un ataque.
- Manual de buenas prácticas para la protección de datos registrados en los Smart TV y en las aplicaciones instaladas, dirigido a todos los usuarios que hacen uso de estos dispositivos o que a futuro lo harán.

Los entregables relacionados anteriormente se desarrollarán en el capítulo VII, para cada uno de estos se indica de qué manera se realizó, en donde se consiguió la información y los hallazgos encontrados.

VII. ENTREGA DE RESULTADOS ESPERADOS E IMPACTOS

Para identificar cuáles han sido las aplicaciones más usadas en los Smart TV, se tomó como base una publicación realizada por el Club Insat Android en su página oficial, en la cual se establecen las quince aplicaciones para Smart TV, y para la descripción de cada una de ellas se toma como base la información que se encuentra disponible en sus sitios web correspondientes ver Tabla 1 [33].

Tabla 1 Información de aplicaciones para Smart TV 2019.
Fuente: Elaboración propia.

Aplicación	Descripción
Netflix	Es un servicio de streaming que ofrece una gran variedad de programas, películas y documentales premiados en casi cualquier pantalla conectada a internet. https://www.netflix.com/co/
Youtube	Permite disfrutar los videos y la música, subir contenido original y compartirlo con amigos, familiares y el resto del mundo. https://www.youtube.com
Amazon prime video	Es un servicio de Amazon para ver contenido audiovisual, como series y películas, en streaming y con suscripción de pago. www.primevideo.com
Plex	Permite analizar y organizar los archivos multimedia automáticamente, de forma intuitiva y dándoles un aspecto increíble. https://www.plex.tv/es/your-media/
Spotify	Es un servicio de música digital que da acceso a millones de canciones. https://www.spotify.com
Eurosport player	Brinda acceso ilimitado a los canales de Eurosport, contenido deportivo en vivo y contenido "On Demand" que incluye historias deportivas, biografías deportivas y comentarios desde múltiples dispositivos conectados a Internet, como computadora, teléfono, tableta, TV Samsung o Apple TV (TVOS). https://www.eurosport.es/
Watch tv	Es una aplicación de transmisión de AT&T que brinda más de 35 canales de TV en vivo, además de acceso a un montón de películas y programas a pedido. https://www.attwatchtv.com/
Spb tv	Ofrece a sus usuarios una gran cantidad de canales en varios idiomas con funciones y ajustes fáciles de usar. Sin cuotas de suscripción. https://play.google.com/store/apps/details?id=com.spb.tv.am&hl=es
Series guide	Aplicación mediante la cual se puede seleccionar las series y películas favoritas y marcar lo que se ha visto o lo que se quiere ver en un futuro https://bytelix.com/aplicaciones/lleva-control-tus-series-peliculas-series-guide/
Livetv	Permite ver canales sobre todo de Reino Unido y Estados Unidos, de modo que se puede disfrutar de sus contenidos, e incluso grabar o programar grabaciones. https://mejoresaplicacionesandroid2019.com/mejores-aplicaciones-android-para-smart-tv-2019/
Deezer	Permite escuchar la música que se desea, al instante. Explorar más de 56 millones de canciones y descubrir nuevos artistas.

Aplicación	Descripción
	https://www.deezer.com/es/company
Gamefly	Proporciona la forma más rentable y conveniente de jugar una amplia gama de juegos de consola, sin necesidad de comprar una consola. https://www.gamefly.com/games
Pictionary	Clásico juego de dibujo en familia, permite dibujar en el aire, mirarlo en la pantalla y proyectarlo a la televisión. https://play.google.com/store/apps/details?id=com.mattel.pictionaryair&hl=es_CO
Screen dreams	Ofrece la oportunidad de tener una chimenea brillante sin los problemas de humo, leña y calor. https://appspara.net/smart-tv/
Ss iptv	De manera gratuita permite acceder a la visión de algunos canales de televisión de todo el mundo. https://mejoresaplicacionesandroid2019.com/mejores-aplicaciones-android-para-smart-tv-2019/

Una vez conocidas estas aplicaciones, se evidencia que dentro de estas se encuentran Netflix y Youtube, y Spotify las cuales fueron definidas dentro del alcance del presente proyecto.

Cada día es más común que los usuarios que hacen uso de los Smart TV, utilicen diferentes aplicaciones, lo que implica el registro de sus datos personales con el fin de disfrutar su contenido, es por ello que se hace una recopilación de la información que solicitan las aplicaciones Netflix, Youtube y Spotify al momento de registrarse, así como la forma de realizar el pago. Para el desarrollo de este entregable, se definieron las categorías para cada uno de los tipos de datos de carácter personal, los que se describen a continuación, tomando como referencia la Ley 1266 de 2008 conocida como la “Ley de Habeas Data:

- Dato público. Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas;

- Dato semiprivado. Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley.

- Dato privado. Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular [34].

Adicionalmente, la Ley 1581 de 2012 "Ley de protección de datos personales" establece la siguiente categoría especial de datos personales:

- Datos sensibles: Son "aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos" [35].

Teniendo en cuenta las definiciones, para el caso e Netflix se detalla la información referente a datos personales que es solicitada al momento de crear la cuenta y de registrar el pago, ver tabla 2.

Tabla 2 Información recopilada por Netflix.
Fuente: Elaboración propia

CATEGORIA	TIPO DE INFORMACIÓN	TIPO DE DATO
Información de la cuenta	Correo Electrónico	Privado
	Contraseña	Privado
	Número de teléfono	Privado
Información de facturación y pago	Tarjeta de crédito o débito	Privado
	Nombre	Público
	Apellido	Público
	Número de tarjeta	Privado
	Fecha de vencimiento de la tarjeta (MM/AA)	Privado
	Código de verificación (CVV)	Privado
Configuración	Preferencias de comunicaciones	Privado
Perfiles	Perfiles (Preferencias de reproducción)	Privado
Historial de interacción de contenido	Historial actividad de visualización	Privado
Configuración	Información sobre dirección IP	Privado

La información de los datos personales que se registra en Youtube, se toma teniendo en cuenta que se accede a esta aplicación por medio de una cuenta de Google, se proporciona información personal que incluye el nombre y contraseña. Ver tabla 3.

Tabla 3 Información recopilada por Youtube.
Fuente: Elaboración propia.

CATEGORIA	TIPO DE INFORMACIÓN	TIPO DE DATO
Información de contacto	Nombre	Público
	Correo Electrónico	Privado
	Contraseña	Privado
	Foto	Sensible
	Número de teléfono	Privado
	Fecha de nacimiento	Semiprivado
	Genero	Privado
Intereses	Videos que se suben	Sensible
	Comentarios de Youtube	Semiprivado
	Canales a los que se suscriben	Semiprivado
	Historial de Reproducción	Semiprivado
	Historial de Búsqueda	Semiprivado
	Historial de Ubicaciones	Semiprivado
Sus apps, navegadores y dispositivos	Tipo y configuración del navegador	Semiprivado
	Sistema operativo	Semiprivado
	Información sobre la red móvil (como el nombre del operador y el número de teléfono)	Privado
	Número de versión de la app	Privado
	Actividad del sistema	Privado
	Fecha	Semiprivado
	Hora	Privado
	URL referencia de la petición de fallo	Privado
	Tipo de dispositivo	Privado
	Nombre del proveedor	Privado
Su actividad	Términos que busca el usuario	Privado
	Videos que mira el usuario	Privado
	Vistas e interacciones con contenido y anuncios	Privado
	Información sobre la voz y el audio cuando usa las funciones de audio	Privado
	Actividad de compra	Privado
	Personas con las que se comunica o comparte contenido	Privado
	Actividad en sitios y apps de terceros que usan nuestros servicios	Privado
	Historial de navegación de Chrome que haya sincronizado con su Cuenta de Google	Privado
Información sobre su ubicación	GPS	Privado
	Dirección IP	Privado
	Datos de los sensores del dispositivo	Privado
	Información sobre elementos cerca del dispositivo, como puntos de acceso de Wi-Fi, torres de telefonía y dispositivos con Bluetooth activado	Privado
	Etiquetas de píxel	Privado
	Registros del servidor	Privado

Finalmente, para la aplicación Spotify, se relaciona la información de datos personales que son recopilados al momento de registrarse, como también de pagar una membresía, igual que en los casos anteriores se hace una categorización. Ver Tabla 4.

Tabla 4 Información recopilada por Spotify.
Fuente: Elaboración propia.

CATEGORIA	TIPO DE INFORMACIÓN	TIPO DE DATO
Datos de registro de la cuenta	Nombre	Público
	Correo Electrónico	Privado
	Contraseña	Privado
	Fecha de nacimiento	Semiprivado
	Sexo	Privado
	Código Postal	Público
	País	Público
Datos de uso del Servicio de Spotify	Información acerca del tipo de plan del Servicio	Privado
	Fecha de cualquier solicitud que haga	Semiprivado
	Hora de cualquier solicitud que haga	Privado
	Canciones que ha escuchado	Privado
	Playlists que agrega	Privado
	Contenido de video que ha visto y sus interacciones con otros usuarios de Spotify	Privado
	Mensajes que envía o recibe a través de Spotify	Privado
	URL	Privado
	Datos de cookies	Privado
	Dirección IP	Privado
	Tipos de dispositivos que utiliza para acceder o conectarse al Servicio de Spotify	Privado
	Tipo de conexión de red (p. ej., WiFi, 3G, LTE, Bluetooth)	Privado
	Red	Privado
	Rendimiento del proveedor	Privado
	Tipo de navegador	Privado
	Idioma	Privado
Datos móviles voluntarios	Fotos	Sensible
	Datos de voz	Sensible
	Contactos	Privado
Datos de Pago	Nombre	Público
	Fecha de nacimiento	Semiprivado
	Tipo de tarjeta de crédito o débito	Privado
	Fecha de vencimiento	Privado
	Ciertos dígitos de su número de tarjeta	Privado
	Código postal	Privado
	Número de teléfono móvil	Privado
	Detalles del historial de transacciones	Privado

Para exponer de una manera general y consolidada los tipos de datos que cada una de las aplicaciones solicita para el registro, en la figura 1 se grafica cuáles son por cada una. En esta figura se puede evidenciar que Youtube es la que más recopila datos personales principalmente privados, asociados a los que se registran con una cuenta de Google. Cabe resaltar que se compara la información de tipo personal, sin que esto se entienda como que los datos recopilados sean los mismos para las tres aplicaciones del alcance del proyecto.

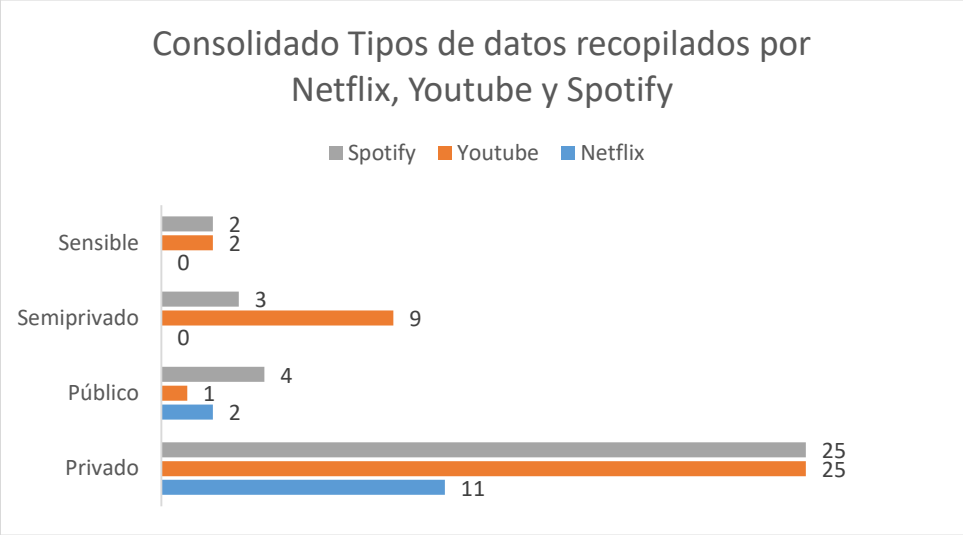

Figura 1 Consolidado Tipos de datos recopilados por Netflix, Youtube y Spotify.
Fuente: Elaboración propia

De lo anterior se puede concluir que la mayoría de los datos personales recopilados hacen referencia a los privados con más del 50% de los mismos en cada una de las aplicaciones, por lo que se debe tener en cuenta las recomendaciones de seguridad, para proteger la información en los Smart TV, de lo contrario la información personal estaría expuesta a diferentes ataques. Por otro lado, para el caso Netflix la información de tipo sensible y semiprivado es del 0%, esta se mantiene dentro de las que menos datos solicita.

Para dar cumplimiento al tercer entregable, a continuación, se detallan los ataques realizados a las aplicaciones y los Smart TV, empezando por el reporte de los ataques realizados a las aplicaciones Netflix, Youtube y Spootify y luego a los televisores inteligentes.

A. Reporte de los Ataques Realizados Aplicaciones

Los ataques de phishing consiste en la suplantación de la identidad, en este los atacantes suelen hacerse pasar por una empresa legitima [36], engañando a la víctima para ganarse la confianza y que el usuario crea que se encuentra en el sitio web oficial y de esta manera lograr conseguir información personal de forma fraudulenta, como las credenciales de usuarios, es por esto que en el desarrollo de esta capítulo, se hace un recuento de los ataques en los cuales se ha comprometido la información personal de los usuarios a través de las aplicaciones definidas en el alcance del proyecto en los últimos dos años [37].

- **Netflix**

Panda Security el 10 de enero de 2018, publico en su página oficial la noticia que denomino "Nueva oleada de phishing para robar cuentas de Netflix", en este indicaban que a través laboratorio anti-malware de Panda Security, habían detectado un ataque masivo a cientos de usuarios en España y Estados Unidos, en el que unos hackers se hicieron pasar por Netflix para robar los datos de acceso de la cuenta [38].

El ataque de phishing se propago por medio de un correo electrónico que llego con el asunto "Notice – Document", seguido por una serie de números como "941-4259" [39]. En el email, que suplanta con bastante acierto la identidad corporativa de Netflix, los piratas informáticos piden a sus víctimas que verifiquen sus datos de acceso a la plataforma audiovisual [38].

En este correo el enlace no dirigía a los usuarios a la web de Netflix, sino a una página falsa. La mayor amenaza de este ataque no era que los hackers robaran los datos de acceso para ver películas y series de forma gratuita. Ni siquiera para vender la cuenta a terceros para que puedan consumir contenidos audiovisuales a costa del usuario registrado. El verdadero riesgo era que los delincuentes revendieran todas estas cuentas en el mercado negro. Además, puedan llegar a llevar a cabo ataques a mayor escala, ya que la mayoría de usuarios reutiliza sus contraseñas y, seguramente a través de los datos robados, otros hackers puedan llegar a las cuentas de correo y redes sociales. Detrás de estos ataques hay bandas organizadas de ciberdelincuentes que van a por dinero", advierte Luis Corrons, Director Técnico de PandLabs [38].

El 21 de septiembre de 2018 en la página oficial de Naked Security publicó una noticia que denominaron "Advertencia emitida cuando los suscriptores de Netflix son golpeados por un ataque

de phishing". Los estafadores de phishing de Netflix vuelven a hacerlo: envían correos electrónicos que intentan robar información confidencial de los suscriptores [40].

Una iniciativa conjunta entre la Policía de la Ciudad de Londres y la Oficina Nacional de Inteligencia contra el Fraude, advirtió a los suscriptores de Netflix sobre una nueva serie de correos electrónicos de phishing. Los estafadores instaban a las víctimas a ingresar la información de su cuenta de Netflix y los detalles de pago [41].

Como muchos estafadores de phishing, este grupo se decepcionó con un lenguaje mal redactado. Debajo de un título que dice "¡Actualice su información de pago!" el correo de phishing decía "Enfrentamos algunas dificultades con la información de facturación actual. Intentaremos nuevamente, pero al mismo tiempo actualice sus datos de pago. Los usuarios se encontraban con que al pie del correo había un botón que insta a los destinatarios a actualizar sus cuentas [41].

El pasado 8 de abril de 2019 la fuente editorial de noticias de seguridad en Internet WeLiveSecurity, publico en su página oficial que la imagen de Netflix seguía siendo utilizada por los cibercriminales para realizar campañas de phishing que suplantaba la identidad de Netflix para engañar a los usuarios y robar sus credenciales de acceso y los datos de su tarjeta de crédito, en este informaban que habían recibido en el laboratorio de ESET Latinoamérica un correo en el que se suplantaba la identidad de Netflix con un mensaje indicando al destinatario que era necesario verificar su información de inicio de sesión debido a que se había registrado una actividad sospechosa en su cuenta, donde a simple vista, un usuario desprevenido podría suponer que se trata de un correo legítimo por parte del proveedor de servicios de series y películas y decidir hacer clic en el botón "ACTUALIZAR" para evitar perder el acceso a su cuenta [42],

Con un diseño igual al del sitio original, la particularidad de la página de Netflix es que independientemente del usuario y clave que se ingresen no se producía ningún tipo de verificación de credenciales y se intentaba llevar al usuario a una instancia en la que se le solicitaba el ingreso de los datos de la tarjeta de crédito asociada a la cuenta [42].

En esta instancia, nuevamente los datos ingresados no eran cuestionados y solo bastaba con cumplir con el requisito de longitud en algunos campos [43]. Es decir que, ante la inclusión de cualquier información y el pedido de confirmar los datos, el sitio finalmente lo redireccionaba al usuario al

portal original de Netflix, habiendo logrado el cometido del robo de credenciales de acceso y los datos de pago de la cuenta” [42].

Nuevamente el 17 de mayo de 2019, la revista digital HayCanal Ciber en su página oficial en internet que titularon “Sobre el ataque de phishing a los usuarios de Netflix, en este manifestaban que existían una nueva y sofisticada estafa de correos electrónicos fraudulentos y que había empezado a circular entre los usuarios de la conocida plataforma de streaming NetFlix con el objetivo de obtener los detalles de la tarjeta de crédito con la que se paga la suscripción mensual [44].

Así lo ha advertido la Oficina de Seguridad del Internauta (OSI) del Instituto Nacional de Ciberseguridad (INCIBE) en un comunicado, en el que detalla que el ataque phishing llega bajo el asunto de "Problemas con tu membresía de Netflix" o "Payment declined", aunque advierte que los ciberdelincuentes pueden utilizar más de un tipo de asunto [44].

En el correo, los ciberdelincuentes señalan que al haber un problema con el pago se debe acceder directamente a un link para actualizar la información de la cuenta. De esta manera el usuario es redirigido a una web que simula ser la web de inicio de sesión de Netflix, solicitando las credenciales de acceso al servicio [44].

- **Youtube**

La noticia más reciente fue la del 23 de septiembre de 2019 en el sitio web de multimedia estadounidense denominaron “Canales de YouTube fueron víctimas de un ataque de phishing: reporte”, en este informaba que varias cuentas de usuarios de YouTube, especialmente las dedicadas a reseñas de automóviles, habían sido hackeadas recientemente según el sitio hermano de CNET en Español, ZDNet [45].

De acuerdo con investigación llevada a cabo por el sitio, varias cuentas con gran número de seguidores como Built, Troy Sowers, MaxtChekVids o Musafir, habían sido víctimas de este hackeo masivo y sus canales aparecían como eliminados de la plataforma de video en streaming. La investigación señala que los hackers utilizaron la estafa de phishing para conseguir las credenciales de las cuentas [45].

Según el propietario de un canal que logró recuperar su cuenta, los hackers usaron correos electrónicos que redireccionan a páginas de inicio de sesión falsas de Google, donde los usuarios introducen sus credenciales y allí las recopilan. Con esta información, los piratas entran en las cuentas de Google de los usuarios, reasignan canales a nuevos propietarios y cambian la URL personalizada del canal de modo que parezca que la cuenta y el canal han sido eliminados [45].

Según la investigación, los hackers están vendiendo estas cuentas de YouTube en OGUsers, un foro en el que se venden credenciales de perfiles de Twitter, Instagram, Snapchat, Skype, Steam, YouTube y más servicios, en muchos casos, robadas [45].

ZDNet cita a un usuario que afirma que estas campañas de hackeo masivas dirigidas a cuentas de automóviles son muy habituales; pues los hackers buscan acceder a una base de datos de correos electrónicos de un sector específico, como es en este caso el del automóvil [45].

El usuario también dijo que los piratas intentarán vender estas cuentas a un nuevo propietario rápidamente antes de que YouTube las devuelva a sus propietarios originales [45].

- **Spotify**

Para el 28 de noviembre de 2018, el portal de noticias de seguridad en Internet WeLiveSecurity publicó un artículo al que denominaron “Campaña de phishing busca robar accesos de cuentas de Spotify”, en este informaban que habían detectado una campaña de phishing que suplantaba la identidad de Spotify en un intento por robar a los usuarios las credenciales de acceso a la plataforma [46].

La campaña se propagaba a través del correo y buscaba engañar a los usuarios para que pincharan en un enlace que dirigía a un sitio fraudulento donde se solicitaba que ingresara su nombre de usuario y contraseña, la cual obviamente queda en manos de los ciberdelincuentes [46].

Si bien el sitio al que redirecciona el enlace parecía bastante convincente, había aspectos clave que permitían corroborar que se trataba de un engaño. De acuerdo a investigadores de AppRiver, que analizaron la campaña, al revisar la dirección de correo del remitente pudieron ver que no era un correo proveniente de Spotify [46].

Caracol Radio el 23 de abril de 2019, dio a conocer la noticia que título “¡Que no pierda su música! No caiga en trampas con su cuenta de Spotify”, en esta informan que Spotify supuestamente

prometía un año de su servicio premium con el cual los usuarios evitan la publicidad durante el cambio de canciones. Esta falsa promesa, que circulaba por WhatsApp, realmente cumplía la función de infectar a la víctima con publicidad y para ello suplantar la identidad del popular servicio de streaming, según la compañía de seguridad informática ESET [47].

A primera vista el mensaje incluía el falso mensaje y un enlace de apariencia similar a la URL oficial de Spotify. Al hacer clic en el enlace, la víctima era redireccionada a una página en la cual se detallan las instrucciones que se deben seguir para obtener la supuesta una cuenta Premium. Inmediatamente el usuario debía responder una serie de preguntas con el objetivo de cumplir con ciertos requisitos y para acceder a la promoción tenía que compartir el mensaje con sus contactos [47].

B. Reporte de los Ataques Realizados a los Smart TV

Durante los años 2018 y 2019 se conocieron diferentes ataques a los Smart TV, los cuales se relacionan a continuación:

- **Ataques Dirigidos**

Estos ataques dirigidos consistían en instalar minadores de la criptodivisa Monero en los Smart TV y enviar todo lo minado a una cartera controlada por los atacantes. En este ESET señala que ya se han detectado ataques dirigidos a explotar criptomonedas. Concretamente, investigadores de Netlab han detectado ataques a través del puerto 5555 (usado en dispositivos Android por la interfaz de debug), que, en el caso de lograr infectar un dispositivo, este seguiría escaneando la red en busca de más dispositivos accesibles a través de este puerto, lo que le confiere capacidades de gusano [48].

En el momento de publicar su análisis, a primeros de febrero, se habían contabilizado más de 5.000 dispositivos afectados, y finalidad de este ataque no era otra que la de instalar un minador de la criptodivisa Monero y enviar todo lo minado a una cartera controlada por los atacantes. Las Smart TV suelen estar conectadas a una fuente de energía de forma continua y, por tanto, podrían estar minando de forma continua durante bastante tiempo hasta que su propietario se diese cuenta [48].

A pesar de tratarse de un ataque limitado, puesto que la amenaza se encontraba localizada mayoritariamente en China y Corea del Sur, podría suponer una tendencia a tener en cuenta de cara

al futuro a corto plazo, e incluso los atacantes podrían modificar el malware para que infectase directamente a aquellas Smart TV que ya incorporan Android como sistema operativo [48].

- **Ataques físicos mediante puertos USB**

Según lo que indica ESET en un artículo al que denominaron Smart TV: ¿una puerta de acceso al hogar para un atacante? Aunque las vulnerabilidades se parcheen y los usuarios se eduquen para la detección de estafas, muchos televisores continúan encontrándose en espacios vulnerables, donde pueden ser alcanzados físicamente por terceros –por ejemplo, en la sala de espera de una oficina o en una sala de estar donde se suelen realizar eventos repletos de extraños [49].

En particular, los puertos USB pueden ser utilizados para la ejecución de scripts maliciosos o la explotación de vulnerabilidades. Algunos gadgets permiten realizar esta tarea de forma rápida y sencilla, como el famoso –o infame– Bash Bunny de Hak5 y su predecesor, el Rubber Ducky, o cualquier hardware de similares características –spoiler alert: no son muy complicados ni costosos de crear de cero. De esta forma, el atacante puede automatizar un variado popurrí de acciones maliciosas basadas en la interacción con la interfaz de usuario y ejecutar el ataque en pocos segundos con tan solo conectar un dispositivo similar en apariencia a una memoria USB [49].

Sin embargo, a pesar de se explica en que consiste el ataque, no se encuentra información de que se haya llevado a cabo el ataque a los televisores inteligentes, bajo esta modalidad.

- **Ataque Recopilación de datos**

Según lo que indica Revista IT Digital Security en su página web, algunos televisores inteligentes llevarían integrado un software que recopilaría datos sobre los programas y los anuncios visualizados, y los videojuegos que se jugaron online, para que los especialistas en marketing puedan orientar sus anuncios a los usuarios [50].

Samba Interactive TV es una compañía que crea perfiles de usuarios basados en análisis de datos para recomendar programas de televisión. Crearon un software que está integrado en Smart TV fabricados por Sony, Sharp, TCL, Philips y otros para recopilar datos de usuarios, a menudo sin un consentimiento claro. Muy a menudo, los usuarios habilitan el servicio sin entender los términos y condiciones, atraídos por la idea de que todo el contenido recibido es personalizado. Obviamente, los datos se envían a los vendedores [50].

El software rastrea toda la información que almacena el televisor sobre los programas y los anuncios visualizados y los videojuegos que se jugaron online, así como la afiliación política de los programas vistos, para que los especialistas en marketing puedan orientar sus anuncios a los usuarios. Los reguladores de la privacidad han llamado la atención sobre esto en múltiples ocasiones, instando a los fabricantes a ser más transparentes en sus prácticas. La compañía no ha publicado estadísticas, pero ha afirmado en el pasado que más del 90% de los usuarios habilitan el servicio [50].

Del análisis de los reportes de los ataques realizados a los Smart TV y a las aplicaciones se puede identificar que para el caso de las aplicaciones estos han sido solo de phishing mediante correo electrónico, en cuantos a los ataques para los Smart TV han sido más variables, encontrando ataques dirigidos, ataques físicos mediante puertos USB y ataques de recopilación de datos mediante software que viene integrado en algunos televisores inteligentes.

Para desarrollar el tercer entregable fue necesario conocer cuáles son los datos personales que se registran en los sistemas operativos que utilizan los Smart TV de las marcas LG, Samsung y Panasonic, ver tabla 5. Luego se comparan estos con los de las aplicaciones e identificar cual es el tipo de información que más estaría expuesta al momento de un ataque, ver tabla 6.

Tabla 5 Información recopilada por los Sistemas Operativos Smart TV.

Fuente: Elaboración propia.

TIPO DE INFORMACIÓN	TIPO DE DATO	SISTEMA OPERATIVO
Correo Electrónico	Privado	WebOS de LG
Contraseña	Privado	WebOS de LG
Fecha de nacimiento	Semiprivado	WebOS de LG
Red	Privado	WebOS de LG
Contraseña	Privado	Tizen Os de Samsung
Red	Privado	Tizen Os de Samsung
Red	Privado	My Home Screen de Panasonic
Contraseña	Privado	My Home Screen de Panasonic
Red	Privado	My Home Screen de Panasonic

De acuerdo a la clasificación de los datos personales para los sistemas operativos de los Smart TV investigados, se logró evidenciar, que es muy poca la información personal que les solicita para

hacer uso de estos dispositivos, para todos solicita la red de internet y una contraseña a la que se van a conectar.

Tabla 6 Información recopilada por las aplicaciones y en los sistemas operativos en los Smart TV.
Fuente: Elaboración propia.

TIPO DE INFORMACIÓN	APLICACIÓN / SISTEMA OPERATIVO
Actividad de compra	Youtube
Actividad del sistema	Youtube
Actividad en sitios y apps de terceros que usan nuestros servicios	Youtube
Apellido	Netflix
Canales a los que se suscriben	Youtube
Canciones que ha escuchado	Spotify
Ciertos dígitos de su número de tarjeta	Spotify
Código de verificación (CVV)	Netflix
Código Postal	Spotify
Comentarios de Youtube	Youtube
Contactos	Spotify
Contenido de video que ha visto y sus interacciones con otros usuarios de Spotify	Spotify
Contraseña	My Home Screen de Panasonic
Contraseña	Netflix
Contraseña	Spotify
Contraseña	Tizen Os de Samsung
Contraseña	WebOS de LG
Contraseña	Youtube
Correo Electrónico	Netflix
Correo Electrónico	Spotify
Correo Electrónico	WebOS de LG
Correo Electrónico	Youtube
Datos de cookies	Spotify
Datos de los sensores del dispositivo	Youtube
Datos de voz	Spotify
Detalles del historial de transacciones	Spotify
Dirección IP	Spotify
Dirección IP	Youtube
Etiquetas de píxel	Youtube
Fecha	Youtube
Fecha de cualquier solicitud que haga	Spotify
Fecha de nacimiento	Spotify
Fecha de nacimiento	WebOS de LG

TIPO DE INFORMACIÓN	APLICACIÓN / SISTEMA OPERATIVO
Fecha de nacimiento	Youtube
Fecha de vencimiento	Spotify
Fecha de vencimiento de la tarjeta (MM/AA)	Netflix
Foto	Youtube
Fotos	Spotify
Genero	Youtube
GPS	Youtube
Historial actividad de visualización	Netflix
Historial de Búsqueda	Youtube
Historial de navegación de Chrome que haya sincronizado con su Cuenta de Google	Youtube
Historial de Reproducción	Youtube
Historial de Ubicaciones	Youtube
Hora	Youtube
Hora de cualquier solicitud que haga	Spotify
Idioma	Spotify
Información acerca del tipo de plan del Servicio	Spotify
Información sobre dirección IP	Netflix
Información sobre elementos cerca del dispositivo, como puntos de acceso de Wi-Fi, torres de telefonía y dispositivos con Bluetooth activado	Youtube
Información sobre la red móvil (como el nombre del operador y el número de teléfono)	Youtube
Información sobre la voz y el audio cuando usa las funciones de audio	Youtube
Mensajes que envía o recibe a través de Spotify	Spotify
Nombre	Netflix
Nombre	Spotify
Nombre	Youtube
Nombre del proveedor	Youtube
Número de tarjeta	Netflix
Número de teléfono	Netflix
Número de teléfono	Youtube
Número de teléfono móvil	Spotify
Número de versión de la app	Youtube
País	Spotify
Perfiles (Preferencias de reproducción)	Netflix
Personas con las que se comunica o comparte contenido	Youtube
Playlists que cree	Spotify
Preferencias de comunicaciones	Netflix
Red	My Home Screen de Panasonic

TIPO DE INFORMACIÓN	APLICACIÓN / SISTEMA OPERATIVO
Red	Spotify
Red	Tizen Os de Samsung
Red	WebOS de LG
Registros del servidor	Youtube
Rendimiento del proveedor	Spotify
Sexo	Spotify
Sistema operativo	Youtube
Tarjeta de crédito o débito	Netflix
Términos que busca el usuario	Youtube
Tipo de dispositivo	Youtube
Tipo de navegador	Spotify
Tipo de tarjeta de crédito o débito	Spotify
Tipo y configuración del navegador	Youtube
Tipos de dispositivos que utiliza para acceder o conectarse al Servicio de Spotify	Spotify
URL	Spotify
URL referencia de la petición de fallo	Youtube
Videos que mira el usuario	Youtube
Videos que se suben	Youtube
Vistas e interacciones con contenido y anuncios	Youtube
Tipo de conexión de red (p. ej., WiFi, 3G, LTE, Bluetooth)	Spotify

Al realizar esta comparación, se evidencia que los tipos de datos que más se solicitan son: las contraseñas, correo electrónico, fecha de nacimiento del usuario, nombre de la red. En cuanto a la red de conexión sin importar que sea para el registro en las aplicaciones o en el sistema operativo, se solicita este dato. Por otro lado, para el dato de nombre, este es solicitado por las tres aplicaciones incluidas en el alcance del proyecto.

El último entregable definido en el presente proyecto es el Manual de buenas prácticas para la protección de datos registrados en los Smart TV y en las aplicaciones instaladas, en el cual se dan las recomendaciones que, en materia de protección de datos deben tenerse presentes en el uso de estos dispositivos, con lo que se pretende mitigar el riesgo de exposición de información personal y sensible a los ciberatacantes, este se puede consultar en el Anexo 1.

Cómo responde a la pregunta de investigación con los resultados

Respondiendo a la pregunta de investigación, ¿Cómo pueden los usuarios que usan Televisores inteligentes (Smart TV), protegerse de los ataques de ingeniería social al registrar su información personal en estos dispositivos y en las aplicaciones que se instalan en los mismos?, se realizó el diseño de un manual de buenas prácticas, el cual se puede consultar en el Anexo 1: Manual de buenas prácticas para la protección de datos registrados en los Smart TV y en las aplicaciones instaladas.

Estrategias de comunicación y divulgación

El presente proyecto de investigación se divulgará en la socialización a los jurados asignados, el cual se encontrará disponible con su anexo en el repositorio de la biblioteca de la Universidad Católica de Colombia.

VIII. CONCLUSIÓN

El derecho a la protección de datos personales corresponde al derecho derivado de la vida privada y de la intimidad de las personas, la cual se ve amenazada con la aparición de nuevas tecnologías. Es por ello que la seguridad de la información es un deber de todos los usuarios de dispositivos IoT, es importante tomar conciencia del rol de cada usuario, teniendo en cuenta recomendaciones y normas de protección de datos personales. En este orden de ideas, Internet de las Cosas requiere un cuidadoso análisis de los riesgos de seguridad presentes, dependiendo de la cantidad de equipos que manejan datos personales y sensibles, y de esta manera poder implementar un efectivo sistema de protección.

A medida que los Smart TV son cada vez más utilizados en los hogares, y mientras se registre información personal y/o sensible, aumenta la probabilidad de ocurrencia de un ataque, así como el impacto y consecuencias. Para prevenirlos, es importante que los usuarios de estos dispositivos entiendan la cantidad de situaciones y acciones que puede poner en riesgo la seguridad de la información que registra y las tecnologías que pueden minimizarlos.

Es muy importante concientizar a los usuarios sobre la protección de los datos personales expuestos en los dispositivos IoT, para evitar ser víctimas de ataques. Más allá de la consciencia y responsabilidad para el cuidado de la privacidad, hay muchos datos que inconscientemente se registran, o que obligatoriamente se ingresan para poder acceder a un servicio en línea (puede ser de entretenimiento, lo que tal vez lo haría "optativo", pero puede ser también un servicio educativo, estatal, de salud, etc.).

REFERENCIAS

[1] P. Llaneza González, Seguridad y responsabilidad en la internet de las cosas (IoT), España: Wolters Kluwer España, S.A., 2018.

[2] C. Borghello, «SmartTV vulnerables a hacking,» 15 Febrero 2018. [En línea]. Available: https://blog.segu-info.com.ar/2018/02/smarttv-vulnerables-hacking.html.

[3] M. Vargas, «Su Smart TV es vulnerable a códigos maliciosos y podría estar en la mira de ciberdelincuentes,» 5 Marzo 2018. [En línea]. Available: https://www.nacion.com/tecnologia/moviles/su-smart-tv-es-vulnerable-a-codigos-maliciosos-y/3UBAUM4DGJFC7EJFBFGC5SVI3I/story/.

[4] Teknautas, «Investigadores avisan: las 'smart TV' de Samsung son un coladero de seguridad,» 4 Abril 2017. [En línea]. Available: https://www.elconfidencial.com/tecnologia/2017-04-04/smart-tv-samsung_1360602/.

[5] Mundo Digital , «El malware de las criptomonedas llega a los Smart Tv,» [En línea]. Available: http://www.mundodigital.net/el-malware-de-las-criptomonedas-llega-a-las-smart-tv/.

[6] R. Solé, «Vulnerabilidades en Chromecast y SmartTV han sido usados para promocionar el canal de PewDiePie,» 06 enero 2019. [En línea]. Available: https://hardwaresfera.com/noticias/software/vulnerabilidades-en-chromecast-y-smarttv-han-sido-usados-para-promocionar-el-canal-de-pewdiepie/.

[7] Elonce, «Smart TV, la nueva puerta de acceso al hogar para los cibercriminales,» 20 Marzo 2019. [En línea]. Available: https://www.elonce.com/secciones/sociedad/582207-smart-tv-la-nueva-puerta-de-acceso-al-hogar-para-los-cibercriminales.htm.

[8] El País , «Smart TV, la nueva puerta de entrada para los ciberataques,» El País , 07 Abril 2019. [En línea]. Available: https://www.elpais.com.uy/vida-actual/smart-tv-nueva-puerta-entrada-ciberataques.html. [Último acceso: 14 Mayo 2019].

[9] V. Cifuentes, «Samsung, LG y Kalley tienen 67,6% del mercado de televisores en Colombia,» *La República,* 22 Abril 2019.

[10] K. Rose, S. Eldridge y L. Chapin, «La internet de las cosas - una breve reseña,» Octubre 2015. [En línea]. Available: https://www.internetsociety.org/wp-content/uploads/2017/09/report-InternetOfThings-20160817-es-1.pdf. [Último acceso: 16 Septiembre 2019].

[11] J. Jimeno Muñoz, Derecho de daños tecnológicos, ciberseguridad e insurtech, Madrid: Dykinson, 2019, p. 314.

[12] N. C. C. Lario, «Minuto uno de la televisión híbrida,» *Historia y comunicación social,* vol. 19, nº Especial, pp. 427-438, 2014.

[13] Ing. Chirinos A, «Diferencia entre aplicación y programa,» [En línea]. Available: https://www.diferencias.cc/aplicacion-programa/. [Último acceso: 18 Septiembre 2019].

[14] «LEY ESTATUTARIA 1581 DE 2012,» Octubre 2012. [En línea]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html. [Último acceso: 16 Septiembre 2019].

[15] C. Fresno Chávez, ¿Se cumplen las leyes del ciberestacio?, Córdoba: El Cid Editor, 2018, p. 35.

[16] ALEGSA , «Ataque informático,» [En línea]. Available: https://www.ecured.cu/Ataque_inform%C3%A1tico. [Último acceso: 18 Septiembre 2019].

[17] E. Chicano Tejada, Auditoría de seguridad informática (MF0487_3), Malaga: ic editorial, 2014.

[18] S. Gaitond y R. S. Patil, «Leveraging machine learning algorithms for zero-day ransomware attack,» *International Journal of Engineering and Advanced Technology,* vol. 8, 2019.

[19] G. Álvarez Marañón y P. P. Pérez García, Seguridad informática para empresas y particulares, Madrid: McGraw-Hill España, 2004, p. 413.

[20] A. M. Barrio, Ciberdelitos: amenazas criminales del ciberespacio, Madrid: Reus, 2017.

[21] F. Spoto, E. Burato, M. D. Ernst, P. Ferrara, A. Lovato, D. Macedonio y C. Spiridon, «Static identification of injection attacks in Java,» *ACM Transactions on Programming Languages and Systems,* vol. 41, nº 18, 2019.

[22] A. Ramírez, «Anatomía de un ataque dirigido,» Redacción Byte TI, 06 Marzo 2018. [En línea]. Available: https://revistabyte.es/actualidad-byte/anatomia-ataque-dirigido/. [Último acceso: 18 Septiembre 2019].

[23] G. Escrivá Gascó, R. M. Romero Serrano, D. J. Ramada y R. Onrubia Pérez, Seguridad informática, Macmillan Iberia, S.A, 2013.

[24] Ministerio de Tecnologías de la Información y las Comunicaciones, «Manual estrategia de gobierno en línea,» Bogotá.

[25] Interpol, «Ciberdelincuencia,» [En línea]. Available: https://www.interpol.int/es/Delitos/Ciberdelincuencia. [Último acceso: 17 Septiembre 2019].

[26] T. Norteamérica, «TOP 25 TV APPS,» 10 Marzo 2017. [En línea]. Available: https://www.tclusa.com/top-tv-apps. [Último acceso: 09 Septiembre 2019].

[27] P. Llaneza González, Seguridad y responsabilidad en la internet de las cosas (IoT), España: Wolters Kluwer España, S.A., 2018.

[28] A. Garriga Dominguez, Nuevos retos para la protección de datos personales en la era del big data y de la computación ubicua, Madrid: DYKINSON, S.L., 2016.

[29] CSIRT-CV, «Seguridad en Internet de las Cosas,» España, 2014.

[30] B. Michéle y A. Karpow, «Demo: Using malicious media files to compromise the security and privacy of smart TVs,» *Consumer Communications and Networking Conference (CCNC) 2014 IEEE 11th,* 2014.

[31] K. Irion y N. Helberger, «Smart TV and the online media sector: User privacy in view of changing market realities,» de *Telecommunications Policy*, Elsevier Ltd, 2017, pp. 170-184.

[32] Y. Bachy, F. Basse, V. Nicomette, E. Alata, M. Kaaniche, J.-C. Courrege y P. Lukjanenko, «Smart-TV security analysis: practical experiments,» *45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks,* 2015.

[33] «Mejores Aplicaciones Android para Smart TV 2019,» 03 Septiembre 2019. [En línea]. Available: https://mejoresaplicacionesandroid2019.com/mejores-aplicaciones-android-para-smart-tv-2019/. [Último acceso: 16 Septiembre 2019].

[34] Superintendencia de Industria y Comercio, «POLÍTICAS DE TRATAMIENTO DE LA INFORMACIÓN PERSONAL EN LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO,» 2014.

[35] «LEY ESTATUTARIA 1581 DE 2012,» 2012.

[36] E. d. L. Gargallo, La seguridad para los menores en Internet, Barcelona: UOC, 2018.

[37] G. Baca Urbina, Introducción a la seguridad informática, México: Grupo Editorial Patria, 2016, p. 344.

[38] Panda Mediacenter, «Nueva oleada de phishing para robar cuentas de Netflix,» Panda Mediacenter, 10 Enero 2018. [En línea]. Available: https://www.pandasecurity.com/spain/mediacenter/seguridad/phishing-netflix-pandalabs/. [Último acceso: 22 Septiembre 2019].

[39] Agencia el Universal, «Hackers se hacen pasar por Netflix y roban acceso a cuenta,» *El Universal,* 2018.

[40] Naked Security, «Warning issued as Netflix subscribers hit by phishing attack,» 21 Septiembre 2018. [En línea]. Available: https://nakedsecurity.sophos.com/2018/09/21/warning-issued-as-netflix-subscribers-hit-by-phishing-attack/. [Último acceso: 23 Septiembre 2019].

[41] Anonymous, «Portaltic.-Una campaña de 'phishing' suplanta a Netflix para conseguir los datos bancarios de sus usuarios,» *DPA International (Spanish),* 2019.

[42] L. Lubeck, «Nuevo Phishing de Netflix busca robar credenciales de acceso y datos de la tarjeta,» Welivesecurity by ESET, 8 Abril 2019. [En línea]. Available: https://www.welivesecurity.com/la-es/2019/04/08/nuevo-phishing-netflix-busca-robar-credenciales-acceso-datos-tarjeta/. [Último acceso: 23 Septiembre 2019].

[43] A. Nikas, E. Alepis y C. Patsakis, «I know what you streamed last night: On the security and privacy of streaming,» *Digital Investigation,* vol. 25, 2018.

[44] R. Maté, «Sobre el ataque de phishing a los usuarios de Netflix,» Hay canal, [En línea]. Available: https://haycanal.com/noticias/11460/sobre-el-ataque-de-phishing-a-los-usuarios-de-netflix. [Último acceso: 20 Septiembre 2019].

[45] E. García, «Canales de YouTube fueron víctimas de un ataque de phishing: reporte,» 23 Septiembre 2019. [En línea]. Available: https://www.cnet.com/es/noticias/youtube-cuentas-hackeo-secuestradas/. [Último acceso: 23 Septiembre 2019].

[46] J. M. Harán, «Campaña de phishing busca robar accesos de cuentas de Spotify,» welivesecurity by eset, 28 Noviembre 2018. [En línea]. Available: https://www.welivesecurity.com/la-es/2018/11/28/campana-phishing-robar-accesos-cuentas-spotify/. [Último acceso: 20 Septiembre 2019].

[47] K. Rozo, «¡Que no pierda su música! No caiga en trampas con su cuenta de Spotify,» Caracol Radio, 23 Abril 2019. [En línea]. Available: https://caracol.com.co/radio/2019/04/23/tecnologia/1556055900_583440.html. [Último acceso: 19 Septiembre 2019].

[48] It Digital Security, «El minado no autorizado de criptodivisas llega a las Smart TV,» 21 Febrero 2018. [En línea]. Available: https://www.itdigitalsecurity.es/vulnerabilidades/2018/02/el-minado-no-autorizado-de-criptodivisas-llega-a-las-smart-tv. [Último acceso: 07 Octubre 2019].

[49] D. Giusto Bilić, «Smart TV: ¿una puerta de acceso al hogar para un atacante?,» Eset, 19 Marzo 2019. [En línea]. Available: https://www.welivesecurity.com/la-es/2019/03/19/smart-tv-puerta-acceso-hogar-atacante/. [Último acceso: 06 Ocubre 2019].

[50] It Digital Security, «Las Smart TV ponen en riesgo la privacidad de los usuarios,» 09 Julio 2018. [En línea]. Available: https://www.itdigitalsecurity.es/endpoint/2018/07/las-smart-tv-ponen-en-riesgo-la-privacidad-de-los-usuarios. [Último acceso: 05 Octubre 2019].

[51] Universidad Autónoma de Madrid, «Citas y elaboración de bibliografía: el plagio y el uso ético de la información: Estilo IEEE,» 26 07 2019. [En línea]. Available: https://biblioguias.uam.es/citar/estilo_ieee. [Último acceso: 29 07 2019].

[52] Wolters Kluwer España SA, Internet of Things y su impacto en los Recursos Humanos y en el Marco Regulatorio de las Relaciones Laborales, Madrid: Kluwer, 2017.