Facultad de Ingeniería

Escuela de Ingeniería en Tecnologías de la Información y la Comunicación

Proyecto de grado para optar por el título de:

Ingeniero en Tecnologías de la Información y la Comunicación

Proyecto de grado

IoTarget - Solución a la inseguridad de los dispositivos IoT Wireless en República Dominicana

Autor:

Randy Raúl Mata Olmos 19-0967

Arturo De Jesús Peña 19-0974

Asesor:

Dr. Darwin Muñoz

19/08/2022

Santo Domingo, Distrito Nacional

República Dominicana

Dedicatoria

Le dedico todo mi esfuerzo a mis padres Randy Mata Acosta y Elisa Olmos Grullón quienes desde mi niñez me han guiado por el camino correcto ayudándome a vencer los obstáculos que se interpongan en mi camino y permitiéndome lograr todas las metas que me proponga.

Así como también a mi pareja y a todos mis compañeros quienes me han acompañado en todo este duro trayecto y me han dado las fuerzas necesarias para no rendirme.

Randy R. Mata Olmos

Dedicatoria

A toda mi familia y amigos cercanos, los cuales me han estado apoyando en mis decisiones y buscando lo mejor para mí, han sido un gran motivante para siempre buscar los trabajos de calidad y no rendirme fácilmente. Quisiera agradecer desde el fondo de mi corazón a todos y cada uno de ellos por esa inspiración que han sido para mí.

Arturo De Jesús P.

Agradecimientos

En primer lugar a Dios por ser mi guía en todo este trayecto. Siendo mi norte y guiándome por el camino correcto a través del cual puedo alcanzar mis metas.

A mis padres Elisa Olmos Grullón y Randy Mata Acosta por su paciencia y sus lecciones morales que me han llevado a ser quien soy el día de hoy y me seguirán guiando en el futuro. A mis hermanos que siempre me han brindado apoyo de manera incondicional. A mi pareja que siempre ha estado ahí incluso en los momentos más difíciles, que me ha enseñado a perseverar, a nunca detenerme ante los obstáculos que se interpongan y a siempre conseguir lo que sea que me proponga. A mis maestros quienes han sido los principales impulsores de mi desarrollo educativo en todo este trayecto.

Finalmente pero no menos importante, a mi compañero Arturo de Jesús, quien me ha acompañado en todo este trayecto educativo y laboral, con quien he compartido buenos momentos y que me ha brindado muchas buenas enseñanzas. Siempre ha estado ahí donde sea y cuando sea que se le necesite. Me siento muy agradecido de contar con un compañero como él y espero lo mejor para el en el trayecto de su vida laboral y personal.

Randy R. Mata Olmos

Agradecimientos

A mi madre Helen Yeceny Peña Guzmán, la cual ha sido siempre mi modelo a seguir en la vida, siempre apoyándome con todo lo que puede, siendo mi consejera cuando me veo sin saber qué hacer y dándome esa enseñanza de cómo afrontar la vida y sus distintas adversidades.

A los maestros Rina Familia y Linardo De Jesús Fernández quienes han tenido un gran impacto en mi formación durante este proceso de carrera en la institución, siempre dándonos sus enseñanzas y consejos de cómo ser un profesional de calidad.

A mi compañero Randy Mata Olmos, el cual ha sido un gran amigo y compañero desde ha ya bastantes años y ya estamos más cerca de terminar esta etapa tan importante de nuestras vidas.

Arturo De Jesús P.

Abstract:

For several years, cybersecurity has been a hot topic; it is one of the branches of computer science that has grown in strength over time because of the increasingly complex systems that are developed during the product development process; the more complex the system, it will need to interact with a variety of other appliances within a network, one of these complex systems being IoT devices. Since its release on the market, attacks on this sort of devices have been on the rise, reaching new highs every year, and there has been no discernible drop in attacks to date.

Our proposal consists of making use of the different scripts, frameworks, and technologies available to ensure that Internet of Things devices are protected in some way through good practices. This would make it possible for users to connect and secure their internet of things devices in an understandable way and increase the user's cybersecurity culture through tips, good practices, and manufacturer recommendations.

Keywords: Internet of things, IoT device, Desktop application, Cybersecurity, Data protection, hardening, good practices, Dominican Republic.

Resumen:

La ciberseguridad ha sido un tema que ha estado en tendencia por varios años, es una de las ramas de las ciencias computacionales que ha ido tomando mucha más fuerza con el pasar del tiempo debido a los sistemas cada vez más complejos que se desarrollan durante el proceso de creación de un producto, mientras más complejo el sistema, interactúa con una variedad de equipos interconectados dentro de una red, uno de estos sistemas complejos son los dispositivos de internet de las cosas. Los ataques a este tipo de equipos han ido en aumento desde su introducción en el mercado llegando cada año a una nueva cifra récord y hasta el momento no se ha notado disminución con relación a los ataques a estos dispositivos.

Nuestra propuesta consiste en hacer uso de los distintos scripts, marcos de trabajo y tecnologías disponibles para conseguir que se protejan de alguna manera los dispositivos de internet de las cosas a través de buenas prácticas. Esto haría posible para los usuarios conectar y asegurar sus dispositivos de internet de las cosas de una manera entendible y que además logre también incrementar la cultura de ciberseguridad del usuario a través de tips, buenas prácticas y recomendaciones del fabricante.

Palabras clave: Internet de las cosas, dispositivo IoT, Aplicación de escritorio, Ciberseguridad, Protección de datos, hardening, buenas prácticas, República Dominicana.

Tabla de Contenidos

Tabla de figuras

Lista de Tablas

Capítulo 1: Introducción e información general

1. Introducción e información general

1.1. Introducción

La industria de los dispositivos del internet de las cosas (en lo adelante “dispositivos IoT) ha ido en crecimiento constante desde hace más de 3 años y cada vez más tanto las industrias como los hogares han ido incorporando el uso de este tipo de dispositivos. Sin embargo, así como va en constante crecimiento, los dispositivos se van volviendo un blanco para los atacantes que buscan el robo de información o causar algún daño a un tercero.

A menos que los dispositivos se estén utilizando en un entorno empresarial es posible que el usuario no esté consciente de los riesgos que pueden llegar a presentar estos dispositivos y es necesario tener pendiente el ámbito de la seguridad a la hora de manejar este tipo de dispositivos. Para manejar este tipo de riesgos existen marcos de trabajo y mejores prácticas creados por instituciones reconocidas como OWASP.

Con este proyecto de grado buscamos dar una solución a los riesgos que pueden presentarse a la hora de trabajar con los dispositivos IoT utilizando los marcos de trabajo previamente mencionados y algunos métodos para dar visualización al usuario de cómo podrían ser afectados utilizando estos dispositivos.

1.1.1. Planteamiento del Problema

Los dispositivos de internet de las cosas fueron una revolución en su salida ya que permitieron integrar a los hogares y oficinas facilidades increíbles y mejoras de procesos que hicieron del día a día una experiencia distinta, bien lo describe el portal MuySeguridad en su post publicado en este año (Guillem, 2022):

“Hace ya tiempo que IoT dejó de ser «el futuro». Aunque el impacto del Internet de las Cosas todavía es tenue en hogares y oficinas, hay otros entornos en los que su proliferación ha sido mucho más acusada, al punto de que la conectividad de todo tipo de dispositivos se ha convertido en un factor clave para muchos servicios. Desde elementos de ciudad conectada hasta los surtidores de carga de muchas estaciones de servicio, TPVs de comercios, vehículos conectados y un sinfín de usos industriales son una prueba de la implantación actual de IoT.”

Los dispositivos IoT llegaron para quedarse y estos a medida que iban pasando los años iban teniendo un crecimiento exponencial, sin embargo, la cultura de ciberseguridad de los usuarios no iba en el mismo crecimiento que la cantidad de dispositivos. Muchos usuarios finales y organizaciones se han visto comprometidos con incidentes de seguridad a causa de brechas en sus dispositivos de internet de las cosas debido a que estos no estaban configurados de una manera segura.

1.1.2. Situación Actual

Esta tecnología ha tenido un crecimiento constante desde su inserción en el mercado, de acuerdo con un estudio realizado por Wegner (2022) el mercado de dispositivos y tecnologías de internet de las cosas creció un 22% en 2021 y se ha mantenido con un crecimiento mayor a 20% cada año de los últimos 3 años. Estas estadísticas de por sí demuestran el alto crecimiento que han tenido estos dispositivos sin embargo cuando vemos la cantidad de empresas y hogares que cuentan con al menos 1 de estos dispositivos pues la cifra va tomando sentido.

1.2. Justificación de la investigación

Las empresas de tecnología se ven impulsadas a crear soluciones para la integración de dispositivos de internet de las cosas a menudo, ya sea Alexa, Google home, entre otros. Mientras que el parque de dispositivos IoT aumenta, la cultura de ciberseguridad alrededor de estos se mantiene estática, no se impulsa lo suficiente y los riesgos e implicaciones que traen consigo los dispositivos conectados a internet aumentan.

Es por lo que un software que permita aprender de ciberseguridad y mitigar cualquier brecha que tengan los dispositivos a los cuales tenga alcance sería una solución idónea para esos usuarios y empresas que no cuentan con una cultura de ciberseguridad madura o están insertándose por primera vez en el mundo de los controles y monitoreo de seguridad de la información.

1.3. Importancia e interés del tema

Como hemos mencionado en los puntos anteriores la tendencia hacia la cual se está moviendo el mundo tecnológico es que los dispositivos estén conectados entre ellos o a internet de modo que se facilite el compartir información o brindar servicios adicionales.

Es por eso que nuestra propuesta trae a la mesa una nueva manera de proteger dispositivos de internet de las cosas conectados a una red Wireless. Mediante un software en un dispositivo conectado a la red, se realizarían análisis y recomendaciones de políticas de seguridad de los dispositivos IoT en la red. En el caso de los hogares este tipo de dispositivos suelen quedar poco protegidos y con acceso directo a internet, por lo que, con esta idea, a través del monitoreo y las recomendaciones de seguridad se busca encontrar vulnerabilidades en los dispositivos y aumentar el nivel de seguridad de estos.

1.4. Alcance y Limitaciones

1.4.1. Alcance:

- La propuesta se enfocará en dispositivos de internet de las cosas que se conecten a través de conexiones de red inalámbricas o Ethernet.
- Analizará la información de los dispositivos basado en vulnerabilidades y puertos conocidos y publicados.

1.4.2. Limitaciones:

- El alcance de los descubrimientos estará limitado a dispositivos conectados en la misma red sobre la cual se lance el escaneo.
- Las recomendaciones arrojadas estarán limitadas a estándares y políticas internacionales reconocidas.
- Debido a los sistemas operativos cerrados de los dispositivos las opciones y detecciones pueden estar limitadas.
- Las investigaciones realizadas estarán limitadas a usuarios no empresariales de dispositivos de internet de las cosas residentes del Distrito Nacional, provincia Santo Domingo, República Dominicana.
- Se requerirá al menos 1 dispositivo de internet de las cosas conectado a la red a la hora de realizar el escaneo.

1.5. Hipótesis Preliminar

Mediante el proceso desarrollado, se permitirá a los usuarios incrementar la seguridad de sus dispositivos de internet de las cosas que se conecten a través de redes de internet Wireless, dándoles además un mejor entendimiento de cómo proteger dichos dispositivos en base a mejores prácticas de la industria, creando así un entorno más ciberseguro.

1.6. Objetivos

1.6.1. Objetivo General

Mejorar el nivel de ciberseguridad de dispositivos de internet de las cosas en entornos empresariales y personales incrementando el nivel de cultura de seguridad de la información del usuario, mitigando posibles brechas de seguridad tecnológica que afecten a los dispositivos IoT y disminuyendo los ataques efectuados a causa de estas.

1.6.2. Objetivos Específicos:

1) Ofrecer un software que permitirá mejorar la seguridad para los dispositivos IoT conectados a la red Wireless.
2) Concientizar al usuario de los peligros y riesgos que implican no proteger estos dispositivos en base a lo que el mismo software encuentre.
3) Lograr un monitoreo pasivo de los dispositivos IoT Wireless.
4) Crear un procedimiento de ciberseguridad efectivo y simple que utilizará el propio software para la protección de dispositivos IoT Wireless.
5) Contribuir al cumplimiento de normativas locales e internacionales en cuanto a la regulación de dispositivos IoT.

Capítulo 2: Marco Teórico y Estado del Arte

2. Introducción al capítulo

El siguiente capítulo busca expresar de manera detallada sobre los dispositivos IoT y su historia. Aquí comprenderemos la base teórica sobre la cual se plantea el proyecto en cuestión, tocando así temas como la evolución de los dispositivos IoT y su historia, las aplicaciones de los dispositivos IoT en los diferentes entornos, las principales vulnerabilidades ante las cuales los encargados de seguridad y desarrollo de dispositivos IoT deben enfrentarse y en adición, se detallan las vulnerabilidades presentadas en el OWASP 2021.

2.1. Antecedentes y referencias

2.1.1. Evolución de los dispositivos IoT

Los dispositivos de internet de las cosas son uno de los instrumentos más populares hoy en día para un montón de actividades, desde alarmas en cualquier momento del día, encender o apagar algún equipo compatible con la tecnología, realizar compras por internet utilizando solo voz, entre otra serie de actividades. Sin embargo, esto no siempre fue de esta manera. Si hablamos de la transmisión de datos, en 1874 se dio por primera vez en la historia transmisión de datos a través de un método no convencional para la época. Para este caso gracias a un experimento francés instalaron equipos meteorológicos que transmitían datos a través de enlaces de radio, algo increíble para la época (El origen del IoT, 2017).

Avanzando un poco la historia, a través de las décadas de 1960, 1970 y 1980 se dieron un montón de avances tecnológicos importantes que permitirían la conexión de cualquier dispositivo, inicialmente en 1963 se envió el primer mensaje alguna vez visto en ARPANET, la cual era la red del Departamento de Defensa de los Estados Unidos, esta red fue el origen de lo que hoy conocemos como Internet.

Al pasar los años, para 1973 los científicos Vinton Cerf y Robert E. Kahn desarrollaron un modelo de comunicación que sería el estándar desde ese momento hasta la actualidad, estos desarrollaron el modelo TCP/IP el cual se utiliza para la comunicación en ARPANET en los años futuros.

A medida que iban pasando los años la revolución en las redes se hacía cada vez más evidente, con la entrada de las redes inalámbricas, estas podían ser redes Wifi o Celulares. Este fue el primer impulso que hizo que una gran cantidad de dispositivos. A través de un montón de conceptos conocidos y no tan conocidos como las conexiones Machine to Machine (M2M) fue lo que llevó a el concepto que conocemos hoy como Internet de las Cosas.

El primero en describir el internet de las cosas fue Kevin Ashton, director ejecutivo de Auto-ID Labs en MIT quien en un discurso en el 1999 declaró (DETRI - Escuela Politécnica Nacional, s. f.):

"Hoy las computadoras y, por lo tanto, Internet, dependen casi por completo de los seres humanos para obtener información. Casi todos los aproximadamente 50 petabytes (un petabyte es 1.024 terabytes) de datos disponibles en Internet fueron primero capturados y creados por seres humanos escribiendo, presionando un botón de grabación, tomando una imagen digital o escaneando un código de barras. El problema es que las personas tienen tiempo, atención y precisión limitados. Todo lo cual significa que no son muy buenos para capturar datos sobre cosas en el mundo real. Si tuviéramos computadoras que supieran todo lo que había que saber sobre las cosas, utilizando los datos que reunieron sin nuestra ayuda, podríamos rastrear y contar todo y reducir en gran medida los desperdicios, pérdidas y costos.

Sabríamos cuándo era necesario reemplazar las cosas, repararlas o retirarlas, y si estaba frescas o habían pasado lo mejor posible".

Estas declaraciones asentaron las bases de lo que hoy en día se conoce como IoT. Ayudaron al desarrollo de la identificación por radiofrecuencia (RFID), etiquetado mediante códigos QR, códigos de barra y marcas de agua digitales y el control de inventario, cosas que evidentemente el Internet de las cosas sería capaz de realizar con facilidad.

2.1.2. Aplicaciones similares

Agricultura

Las tecnologías IoT prometen ayudar a los agricultores a cerrar la brecha entre la oferta y la demanda al garantizar buenos rendimientos, rentabilidad y preservación del medio ambiente. La agricultura de precisión es el uso de la tecnología de Internet de las cosas (IoT) para garantizar el uso más efectivo de los recursos con el fin de maximizar la producción agrícola y minimizar los costos operativos. Los equipos especializados, las conexiones inalámbricas, el software y los servicios de tecnología de la información son ejemplos de IoT en las tecnologías agrícolas (IoT Transforming The Future Of Agriculture, 2019).

La agricultura ha sido durante mucho tiempo una parte importante de las civilizaciones humanas en todo el mundo. El rápido progreso de las Tecnologías de la Información y la Comunicación (TIC) ha tenido un impacto significativo en la estructura y administración de la agricultura moderna. A pesar de los beneficios de este desarrollo, una serie de problemas de seguridad presentes y futuros pueden tener una influencia significativa en la agricultura.

El rápido crecimiento de Internet de las cosas (IoT), que ha cambiado el objetivo del sector de enfoques estadísticos a enfoques cuantitativos, ha remodelado prácticamente todas las industrias, incluida la agricultura inteligente. Cambios tan tremendos están sacudiendo los sistemas agrícolas actuales, abriendo nuevas oportunidades al tiempo que plantean una variedad de desafíos. Los sensores inalámbricos y de IoT en la agricultura se vuelven cada vez más utilizados en las granjas, al igual que los desafíos que deberán abordarse a medida que esta tecnología se combine con los enfoques agrícolas tradicionales. La nueva generación de agricultura inteligente creada por IoT está cambiando la cara de la agricultura tradicional para mejorarla, protegerla de peligros como animales e incendios y hacerla más rentable para los agricultores (Bisson, 2021).

Sector Salud

El uso de IoT en la industria hotelera conduce a mejoras significativas en la calidad del servicio. Usando claves electrónicas que se envían directamente al dispositivo móvil de cada huésped, es posible automatizar una variedad de transacciones.

Los médicos pueden monitorear el estado de un paciente fuera del hospital y en tiempo real mediante el uso de dispositivos portátiles o sensores conectados a ellos. El Internet de las cosas ayuda a mejorar la atención al paciente y a prevenir sucesos mortales en pacientes de alto riesgo al monitorear continuamente métricas particulares y proporcionar advertencias automáticas sobre sus signos vitales (The 9 Most Important Applications of the Internet of Things (IoT), 2019).

Otro uso es la incorporación de la tecnología IoT en las camas de los hospitales, dando como resultado camas inteligentes con sensores que monitorean signos vitales, presión arterial, oxímetro y temperatura corporal, entre otros.

Los ciberdelincuentes se dirigen a las organizaciones de atención médica por una variedad de razones. Una es que almacenan enormes volúmenes de datos confidenciales, como la propiedad intelectual y la investigación de vacunas. También incluyen información de identificación personal, como información médica y de seguros, que se puede vender en el mercado negro y de las cibercriminales pueden sacar provecho de muchas maneras tales como afectar de manera reputacional la organización, impactar económicamente la organización y hasta utilizar esa información para robos a terceros o los mismos propietarios de la información (Boyden, 2021).

Uso del consumidor general

Los dispositivos IoT, como los dispositivos portátiles y los hogares inteligentes, son los más utilizados por el consumidor general. Alexa, iPhones, relojes Apple, asistentes inteligentes, lámparas, por mencionar algunos, son ejemplos de dispositivos IoT utilizados por el público general.

Los consumidores suelen estar preocupados por la seguridad y la privacidad de su información personal, pero a menudo carecen de la experiencia que les permita elegir productos con características aceptables de seguridad y privacidad. Los fabricantes se concentran en llevar más productos al mercado lo más rápido posible y no comparten constantemente información sobre las características de seguridad que deben revisarse para

determinar el nivel de seguridad de un dispositivo. Es debido a esto que actualmente existe una gran brecha de seguridad cuando se habla de dispositivos IoT.

2.2. Base teórica

2.2.1. Tecnología IoT

Internet de las cosas, o IoT, es una red global de dispositivos digitales que están conectados a Internet e intercambian los datos entre sí lo que les permite tener diversas funcionalidades. El Internet de las cosas permite realizar una amplia gama de operaciones sin necesidad de interacción humana, lo que permite procesos más eficientes, tecnología más inteligente y una conexión más fluida.

Cualquier tecnología que se utiliza en una red IoT se denomina tecnología IoT. Los dispositivos IoT son un ejemplo de esta tecnología, pero también incluye cosas como servidores, bases de datos, computadoras y sistemas basados en la nube (Oddy, 2021).

2.2.2. Dispositivos IoT

Un dispositivo de Internet de las cosas es cualquier pieza de hardware que se ha configurado para un propósito específico y puede enviar y recibir datos a través de Internet o cualquier otra red digital a la que esté conectado. Estos pueden ser sensores, aparatos, actuadores o dispositivos integrados en maquinaria o equipos más grandes.

En ocasiones, los dispositivos IoT pueden incorporar tecnología inteligente o inteligencia artificial (IA) en un sistema o equipo más grande, lo que le permite volverse más autónomo. En la fabricación industrial, por ejemplo, los robots pueden detectar y responder a

anomalías en un proceso sin necesidad de que un trabajador humano reconozca el problema y apague o redirija físicamente una máquina.

Si está conectado a un microprocesador o chip que pueda conectarse a Internet o a una red digital, casi cualquier objeto o equipo físico puede transformarse en un dispositivo IoT. Los bienes o máquinas más grandes pueden tener varios dispositivos, como varios sensores distintos que proporcionan datos a una única base de datos central.

En la mayoría de las situaciones, el término "dispositivo IoT" se refiere a dispositivos que están conectados a Internet pero que antes no se esperaba que lo estuvieran. Los teléfonos son dispositivos de Internet de las Cosas, pero rara vez se los denomina como tales, ya que es evidente que comunican datos a través de una red. Sin embargo, los dispositivos inteligentes son instancias típicas de dispositivos IoT porque muchas personas no saben que se vinculan a una red digital más grande. (Oddy, 2021).

2.2.3. Evaluación de vulnerabilidades en dispositivos IoT

La evaluación de vulnerabilidades es un examen exhaustivo de las fallas de seguridad de un sistema de internet de las cosas. Determina si el sistema es susceptible a alguna vulnerabilidad conocida, otorga calificaciones de gravedad a esas vulnerabilidades y, si es necesario y cuando es necesario, ofrece remedio o mitigación.

Las evaluaciones de vulnerabilidad pueden proteger contra amenazas como: Inyección SQL, XSS y otros ataques de inyección de código, técnicas de autenticación incorrecta, valores predeterminados inseguros, entre otros (Lowing et al., 2021).

Existen muchos tipos diferentes de evaluación de vulnerabilidades, pero para dispositivos IoT los más comunes son:

- Evaluación de host: una revisión de los servidores cruciales que pueden ser vulnerables a los ataques si no se prueban exhaustivamente o se crean a partir de una imagen de máquina verificada.
- Evaluación Red: Consiste en la evaluación de reglas y procedimientos para prevenir accesos no deseados a redes privadas o públicas y recursos accesibles a la red.
- Evaluación de aplicaciones: Consiste en evaluaciones del Front end o del código fuente estático/dinámico y se utiliza para descubrir vulnerabilidades de seguridad en aplicaciones en línea y su código fuente.

2.2.4. OWASP

El Proyecto de seguridad de aplicaciones abierto, u OWASP (Open Web Application Security Project), es una organización sin fines de lucro comprometida con la seguridad de las aplicaciones web a escala global. Uno de los valores clave de OWASP es que todos los recursos de su sitio web estén disponibles públicamente y sean de fácil acceso, lo que permite a cualquier persona mejorar la seguridad de su propia aplicación en línea. El OWASP Top 10 es quizás su iniciativa más conocida.

El OWASP Top 10 es un estudio actualizado con frecuencia que describe los problemas de seguridad para la seguridad de las aplicaciones web, concentrándose en las diez amenazas más importantes. Un equipo de especialistas en seguridad de todo el mundo colaboró en la investigación. OWASP se refiere al Top 10 como un "documento de concientización" y propone que todas las empresas incorporen el informe en sus procedimientos para evitar y/o mitigar las amenazas a la seguridad (*What Is OWASP? | Cloudflare*, s. f.).

Desde 2003, OWASP ha mantenido el ranking Top 10. La lista se actualiza cada 2 o 3 años para reflejar mejoras y cambios en la industria de AppSec. La importancia de OWASP reside en la información procesable que brinda; actúa como una lista de verificación crítica y una guía interna de desarrollo de aplicaciones web para muchas de las principales empresas del mundo.

Los auditores con frecuencia interpretan la incapacidad de una organización para abordar el OWASP Top 10 como un indicador de que no está cumpliendo con los estándares. Al incorporar el Top 10 en su ciclo de vida de desarrollo de software (SDLC), la empresa muestra un compromiso general con las mejores prácticas de la industria para el desarrollo seguro.

El OWASP top 10 del 2021 trajo cambios significativos para el del año anterior. Estos cambios serán expuestos con detalle ya que los mismos fungen como parte primordial para el desarrollo de este proyecto ya que el escaneo de vulnerabilidades y amenazas se estará realizando, basándose en parte del OWASP top 10 del 2021.

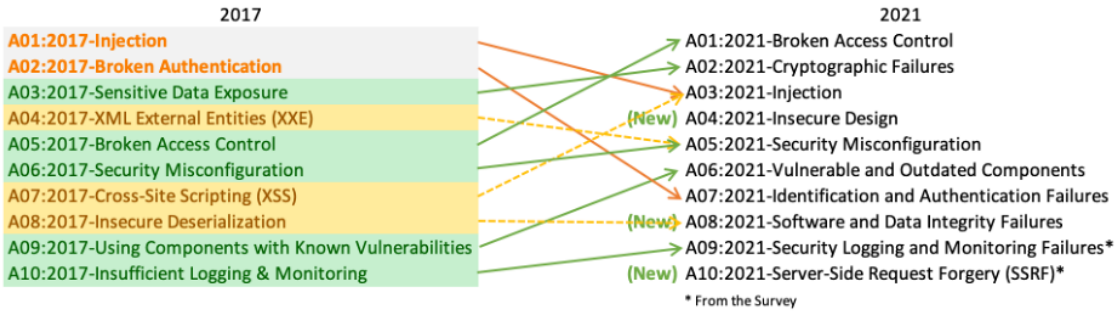


Figura 1: Diagrama de top 10 riesgos de seguridad de aplicaciones del 2021 en comparación al 2017.
Fuente: OWASP top 10

2.2.4.1. A01:2021 – Broken Access Control

La imposición de límites sobre quién (o qué) puede realizar intentos de actividades o acceder a los recursos que han solicitado se conoce como control de acceso (o permiso). El control de acceso en el contexto de las aplicaciones en línea se basa en la autenticación y la gestión de sesiones:

- La autenticación identifica al usuario y válida que es quien dice ser.
- La gestión de sesiones realiza un seguimiento de las solicitudes HTTP subsiguientes realizadas por el mismo usuario.
- El control de acceso evalúa si el usuario está autorizado para realizar la operación que está intentando.

Los controles de acceso que se han visto comprometidos son un problema de seguridad frecuente y, a menudo, grave. El diseño y la gestión del control de acceso es un desafío complicado y dinámico que involucra la aplicación de restricciones corporativas, organizacionales y regulatorias a una implementación tecnológica. Los seres humanos, no la tecnología, deben emitir juicios sobre el diseño del control de acceso, y el potencial de error es considerable (Access control vulnerabilities and privilege escalation | web security academy, s. f.).

Según el blog, los siguientes son ejemplos de fallas comunes de control de acceso:

- Omitir las comprobaciones de control de acceso cambiando la URL, el estado interno de la aplicación o la página HTML, o simplemente empleando una herramienta de ataque API personalizada.
- Permitir que la clave principal se cambie al registro de otro usuario, permitiendo el acceso o la alteración de la cuenta de otro usuario.

- El privilegio está siendo elevado. Operar como usuario sin iniciar sesión o actuar como administrador mientras se inicia sesión como usuario.
- Manipulación de metadatos, como reproducir o alterar un token de control de acceso JSON Web Token (JWT), o manipular una cookie o un campo oculto para elevar los privilegios, o aprovechar la invalidación de JWT.
- El acceso a la API no autorizado es posible debido a una mala configuración de CORS (*What Is and How to Prevent Broken Access Control | OWASP Top 10*, s. f.).

2.2.4.2. A02:2021 - Fallos criptográficos

Cuando los datos confidenciales, como contraseñas, números de tarjetas de crédito e información personal, no están protegidos de forma segura, los atacantes se dirigen a ellos con frecuencia. La causa principal de la fuga de datos confidenciales es la falla criptográfica. Proteger sus datos de fallas criptográficas se ha vuelto más crucial que nunca, según el Proyecto de seguridad de aplicaciones web abiertas (OWASP) 2021.

Una falla criptográfica se puede encontrar cuando:

- Los datos deben almacenarse o enviarse en texto sin formato (lo más común).
- Los datos se protegen mediante un cifrado obsoleto o ineficaz.
- Filtrado o enmascaramiento incorrecto de datos en tránsito

La falla criptográfica puede ser remediada de diversas maneras, entre las que se encuentra:

- Determinar datos sensibles e implementar procedimientos de seguridad adecuados.
- Almacene datos confidenciales solo cuando sea absolutamente necesario; de lo contrario, elimine los datos confidenciales y utilice la tokenización o el truncamiento.

- Utilizando técnicas, protocolos y claves de encriptación sólidas, cifre cualquier información confidencial en reposo.
- Se pueden utilizar protocolos seguros como TLS y HTTP HSTS para cifrar los datos en tránsito.
- Para datos confidenciales, deshabilite el almacenamiento en caché.
- Las contraseñas deben almacenarse utilizando métodos de hash sólidos y salados, como Argon2, scrypt y bcrypt.

2.2.4.3. A03:2021 – Inyección de código

Una vulnerabilidad de inyección en una aplicación web permite a los atacantes pasar datos maliciosos a un intérprete, lo que hace que los datos se compilen y ejecuten en el servidor.

Según el sitio oficial de OWASP (2021) una aplicación es vulnerable a un ataque si y solo si se cumplen las siguientes condiciones:

- El programa no verifica, filtra ni desinfecta los datos proporcionados por el usuario.
- En el intérprete, se utilizan directamente consultas dinámicas o llamadas no parametrizadas sin escape consciente del contexto.
- Para extraer registros confidenciales adicionales, se emplean datos hostiles dentro de los criterios de búsqueda de mapeo relacional de objetos (ORM).
- Los datos hostiles se utilizan directamente o se concatenan. En consultas dinámicas, comandos o procedimientos almacenados, el comando o SQL contiene la estructura y los datos dañinos.

Las acciones por realizar para prevenir ataques de Inyección incluyen (Oh et al., 2021):

1. Utilizar una API segura que no necesite el uso de un intérprete.
2. Utilizar una validación de entradas o “lista blanca” del lado del servidor
3. Los caracteres especiales deben ser escapados.
4. Usar LIMIT y otras restricciones de SQL dentro de las consultas para evitar la divulgación masiva de registros en caso de inyección de SQL.

2.2.4.4. A04:2021 – Diseño inseguro

El diseño inseguro es una categoría amplia que abarca varios defectos, como "diseño de control faltante o inadecuado". Todas las demás categorías de riesgo Top 10 no son causadas por un diseño inseguro. Hay que hacer una distinción entre diseño inseguro e implementación insegura. Distinguimos entre problemas de diseño y fallas de implementación por una razón, tienen diferentes causas y remedios fundamentales. Incluso si un diseño es seguro, las fallas de implementación pueden generar vulnerabilidades que pueden explotarse.

Un diseño defectuoso no se puede reparar con una implementación perfecta, ya que nunca se establecieron las medidas de seguridad necesarias para defenderse de amenazas específicas. Un aspecto que contribuye al diseño inseguro es la falta de un perfil de riesgo empresarial inherente al software o sistema que se está produciendo, lo que provoca que no se decida qué nivel de diseño de seguridad es necesario.

2.2.4.5. A05:2021 - Configuración de seguridad incorrecta

La configuración incorrecta de seguridad es una falta de refuerzo de la seguridad de la pila de aplicaciones. Esto podría implicar la configuración incorrecta de los derechos del servicio en la nube, la activación o instalación de funciones innecesarias y el uso de cuentas o

contraseñas de administrador predeterminadas. Esto ahora incluye entidades externas XML (XXE), que anteriormente se clasificaban como una categoría OWASP separada.

Según el sitio oficial de OWASP (2021) para saber si el sistema es vulnerable, es necesario tomar en cuenta los siguientes elementos:

- Reforzamiento de la seguridad inadecuada en toda la pila de aplicaciones o permisos establecidos incorrectamente en los servicios en la nube.
- Se activan o instalan funcionalidades no deseadas (por ejemplo, puertos, servicios, páginas, cuentas o privilegios innecesarios).
- Las cuentas y contraseñas predeterminadas permanecen activas y sin modificar.
- El manejo de errores muestra a los usuarios rastros de pila u otros mensajes de error innecesariamente descriptivos.
- Las características de seguridad más recientes están desactivadas o mal configuradas en las computadoras actualizadas.
- La configuración de seguridad en los servidores de aplicaciones, los marcos de aplicaciones (por ejemplo, Struts, Spring, ASP.NET), las bibliotecas, las bases de datos, etc., no están configurados para proteger los valores.
- El servidor no envía los encabezados y las directivas de seguridad, o no están configurados en valores seguros.

Para asegurarse contra malas configuraciones en los sistemas según Imperva (2021) es necesario:

- Crear un procedimiento de refuerzo de aplicaciones que sea rápido y sencillo de implementar.
- Configurar el desarrollo, el control de calidad y la producción de la misma manera (con diferentes credenciales).

- Todos los sistemas deben configurarse para que sean lo más simples posible, sin características ni componentes superfluos.
- Se deben aplicar parches y avisos de seguridad a las configuraciones de manera regular.
- Crear un procedimiento automatizado para validar configuraciones seguras en todos los entornos.

2.2.4.6. A06:2021 - Componentes vulnerables u obsoletos

Componentes Vulnerables y Obsoletos, anteriormente conocidos como "Uso de Componentes con Vulnerabilidades Conocidas", se refiere a las vulnerabilidades causadas por software incompatible o desactualizado. Cualquiera que produzca o use una aplicación sin comprender sus componentes principales, versiones o si se han actualizado es vulnerable a este tipo de vulnerabilidad.

Se pueden encontrar problemas de vulnerabilidades:

- Si no está seguro acerca de las versiones de todos los componentes que utiliza (tanto del lado del cliente como del lado del servidor). Esto cubre tanto los componentes utilizados directamente como las dependencias jerárquicas.
- Si el programa no es seguro, no es compatible o está desactualizado. Se incluyen el sistema operativo, el servidor web/de aplicaciones, el sistema de administración de bases de datos (DBMS), las aplicaciones, las API y todos los componentes, los entornos de tiempo de ejecución y las bibliotecas.
- Si no comprueba las vulnerabilidades de forma regular y no se suscribe a los boletines de seguridad de los componentes que utiliza.

- Si la plataforma subyacente, los marcos y las dependencias no se reparan o actualizan de manera oportuna y basada en el riesgo. Esto prevalece en contextos donde la aplicación de parches es una actividad mensual o trimestral bajo control de cambios, lo que deja a las empresas expuestas a vulnerabilidades resueltas durante días o meses.

Para prevenir el uso de componentes vulnerables y desactualizados:

- Las dependencias, características, componentes y archivos no utilizados deben eliminarse de los programas.
- Usando herramientas de análisis de composición de software (SCA), realizar un seguimiento de los componentes y sus versiones tanto en el lado del cliente como en el del servidor.
- Escanear las bibliotecas y sus dependencias de forma regular en busca de componentes inseguros.
- Usar solo componentes oficiales y prefiera paquetes firmados.
- Corregir las vulnerabilidades lo antes posible, eliminar los componentes afectados o instalar un parche virtual.

2.2.4.7. A07:2021 - Fallos de identificación y autenticación

Las áreas de autenticación y autorización son unas de las más importantes de todo el listado. De hecho, las seis principales vulnerabilidades en la lista de OWASP son todas atribuibles a una autenticación o autorización defectuosa.

Cuando las funciones vinculadas a la identidad, la autenticación o la gestión de sesiones de un usuario no se implementan adecuadamente o no están adecuadamente

protegidas por una aplicación, pueden ocurrir problemas de identificación y autenticación. Los atacantes pueden explotar las fallas de identificación y autenticación al comprometer contraseñas, claves, tokens de sesión u otras vulnerabilidades técnicas para asumir de manera temporal o permanente las identidades de otros usuarios.

Se puede decir que existen fallas de autenticación si la aplicación:

- Permite ataques automatizados como el credential stuffing (relleno de credenciales), en el que el atacante tiene una lista de usuarios y contraseñas legítimas.
- Permite la fuerza bruta y otros ataques automatizados.
- Permite contraseñas predeterminadas, débiles o conocidas como "Password1" o "admin/admin".
- Utiliza procedimientos de recuperación de credenciales inseguros o deficientes y de olvido de contraseña, como "respuestas basadas en conocimientos", que no se pueden proteger.
- Almacenamiento de datos que utilizan contraseñas de texto sin formato, encriptadas o mal codificadas (ver A02:2021-Fallas criptográficas).
- La autenticación multifactorial está ausente o es ineficaz.
- La identificación de la sesión se expone en la URL.
- Después de un inicio de sesión exitoso, reutiliza el identificador de sesión.
- Los ID de sesión no se invalidan correctamente. Durante el cierre de sesión o un período de inactividad, las sesiones de usuario o los tokens de autenticación (principalmente tokens de inicio de sesión único (SSO)) no caducan correctamente.

2.2.4.8. A08:2021 – Fallo en el software y la integridad de datos

El código y la infraestructura son propensos a violaciones de integridad en el software y fallas en la integridad de los datos. Esto incluye actualizaciones de software, alteración de datos confidenciales y modificaciones de canalización de CI/CD realizadas sin validación. El acceso no autorizado, la introducción de malware y otras vulnerabilidades importantes pueden resultar de una canalización de CI/CD no segura.

Existe una preocupación generalizada acerca de los programas que reciben actualizaciones automáticas. En algunas situaciones, los atacantes violaron la cadena de suministro y desarrollaron sus propias actualizaciones maliciosas. Miles de empresas fueron pirateadas como resultado de la descarga y aplicación de actualizaciones maliciosas a software previamente confiable sin verificación de integridad.

Con el fin de lograr una prevención oportuna de fallo en el software e integridad de datos es necesario:

- Usar firmas digitales u otros procedimientos similares para asegurarse de que el programa o los datos provengan de la fuente anticipada y no hayan sido alterados.
- Asegurarse de que las bibliotecas y las dependencias, consuman fuentes confiables. Si tiene un perfil de riesgo más alto, considerar alojar un repositorio interno validado y conocido.
- Asegurarse de que se utilice una herramienta de seguridad de la cadena de suministro de software, como OWASP Dependency Check u OWASP CycloneDX, para garantizar que no existan vulnerabilidades conocidas en los componentes.

- Para reducir la posibilidad de que se inyecte código o configuración dañinos en su proceso de desarrollo, asegurarse de que haya un procedimiento de revisión para las modificaciones de código y configuración.
- Asegurarse de que los datos serializados sin firmar o sin cifrar no se proporcionen a clientes que no sean de confianza sin algún tipo de verificación de integridad o firma digital para detectar la manipulación o reproducción de datos serializados.

2.2.4.9. Fallas en el monitoreo y auditoría de seguridad

Las fallas en el monitoreo y auditoría de seguridad, anteriormente conocidas como "auditoría y monitoreos inadecuados", son fallas en la capacidad de una aplicación para identificar y responder a problemas de seguridad. La detección de brechas es imposible sin auditoría y monitoreo. Las fallas en esta categoría tienen ramificaciones para la visibilidad, las alertas y el análisis forense.

Según el sitio oficial de OWASP (2021), Se puede identificar una insuficiencia en el monitoreo auditoría y respuesta activa cuando:

- Los inicios de sesión, los inicios de sesión fallidos y las transacciones de alto valor no se almacenan como eventos auditables.
- Las advertencias y los errores crean mensajes de registro inexistentes, insuficientes o ambiguos.
- Los registros de aplicaciones y API no se verifican en busca de actividades sospechosas.
- Los registros solo se mantienen localmente.
- Los umbrales de alerta apropiados y los protocolos de escalada de respuesta no están en su lugar o no funcionan correctamente.

- Las pruebas de penetración y los análisis realizados con herramientas de pruebas de seguridad de aplicaciones dinámicas (DAST) no proporcionan alarmas.
- En tiempo real o casi en tiempo real, el programa no puede detectar, escalar ni notificar ataques activos.

Con el fin de disminuir la posibilidad de un monitoreo o auditoría deficiente los desarrolladores deben incorporar alguno o todos los siguientes controles, según el riesgo de la aplicación:

- Asegurarse de que todos los errores de inicio de sesión, control de acceso y validación de entrada del lado del servidor se registren con suficiente contexto de usuario para identificar cuentas sospechosas o maliciosas y se retengan durante el tiempo suficiente para permitir una investigación forense retrasada.
- Asegurarse de que los registros se creen en un formato que las soluciones de administración de registros puedan consumir fácilmente.
- Asegurarse de que los datos de registro estén codificados correctamente para evitar inyecciones o ataques a los sistemas de registro o monitoreo.
- Asegurarse de que las transacciones de alto valor tengan un seguimiento de auditoría y medidas de integridad para evitar la manipulación o la eliminación, como tablas de base de datos de solo agregar o algo similar.
- Los equipos de DevSecOps deben crear mecanismos sólidos de monitoreo y alerta para detectar y responder a comportamientos sospechosos lo antes posible.

2.2.4.10. A10:2021 – Falsificación de solicitud del lado del servidor (SSRF)

Cuando una aplicación web obtiene un recurso remoto sin verificar la URL proporcionada por el usuario, se produce una falla de SSRF. Permite a un atacante obligar a

una aplicación a enviar una solicitud manipulada a una ubicación inesperada, incluso cuando está protegida por un firewall, VPN u otro tipo de lista de control de acceso a la red (ACL).

Obtener una URL se ha convertido en un escenario habitual a medida que las nuevas aplicaciones en línea brindan a los usuarios finales funcionalidades útiles. Como resultado, la prevalencia de SSRF está aumentando. Además, la gravedad de SSRF está aumentando como resultado de los servicios en la nube y la complejidad de los diseños.

SSRF se puede evitar empleando algunos o todos los siguientes controles de defensa en profundidad:

Para disminuir el impacto de SSRF desde la capa de red:

- Segmentar las capacidades de acceso a recursos remotos en diferentes redes en la capa de red.
- Implementar la configuración de firewall "denegar de forma predeterminada" o las reglas de control de acceso a la red para evitar todo el tráfico de intranet, excepto el requerido.
- Sugerencias: Asignar propiedad y una vida útil a las reglas de firewall según las aplicaciones.
- En los cortafuegos, mantener un registro de todo el tráfico de red aprobado y prohibido (según la A09:2021: Fallas de registro y monitoreo de seguridad).
- Desde la capa de aplicación es posible:
- Validar y sanear todos los datos de entrada proporcionados por el cliente.
- Utilizar una lista de permitidos positiva para aplicar la estructura de la URL, el puerto y el destino.
- Los clientes no deben recibir respuestas sin procesar.

- Desactivar las redirecciones HTTP.

2.2.5. Marco de trabajo de seguridad de OWASP para IoT (OWASP ISVS)

El estándar de verificación de seguridad de Internet de las cosas (ISVS) de OWASP es un esfuerzo de colaboración para proporcionar un marco de seguridad para las aplicaciones de Internet de las cosas (IoT). Los criterios ISVS se pueden aplicar a varias etapas del ciclo de vida del producto, incluido el diseño, el desarrollo y las pruebas de la aplicación IoT.

Las aplicaciones de IoT con frecuencia se componen de una gran cantidad de aplicaciones interconectadas que trabajan juntas para construir un ecosistema complicado. Como resultado, proteger una aplicación de IoT se reduce a salvaguardar el ecosistema en su conjunto. Como resultado, el ISVS establece criterios de seguridad para los programas integrados y el entorno de IoT en el que viven, basándose tanto como sea posible en los estándares actuales aceptados por la industria (OWASP IoT Security Verification Standard | OWASP Foundation, s. f.).

Según la guía de OWASP ISVS las necesidades de control de seguridad de ISVS se pueden expresar como un stack. Los requisitos de la plataforma de hardware (V5) se mencionan en la parte inferior. La plataforma de hardware se define en todo el ISVS como los muchos componentes de hardware que constituyen la base de su dispositivo conectado. Además de la plataforma de hardware, se encuentran los requisitos para la plataforma de software (V3) y la comunicación (V4), que hacen uso de la plataforma de hardware para permitir un amplio desarrollo de aplicaciones. La capa de requisitos de aplicaciones de espacio de usuario especifica los requisitos para estas aplicaciones (V2). Finalmente, el nivel

Entorno de IoT describe un conjunto de necesidades que sirven como el pegamento que conecta el dispositivo conectado con el ecosistema circundante (V1).

2.2.5.1. V1 - Requerimientos de los ecosistemas

El diseño de seguridad del sistema completado antes del desarrollo, así como un proceso de seguridad que respalde constantemente el desarrollo del sistema y se incorpore en todas las fases de su vida útil, son elementos básicos necesarios para desarrollar implementaciones arquitectónicas de productos seguros. Como parte del ciclo de vida del diseño del producto, el modelado iterativo de amenazas del sistema permite la preparación para intentos maliciosos y el desarrollo de métodos de mitigación.

La cadena de suministro es fundamental para la seguridad de cualquier producto. Un proceso de desarrollo seguro garantiza que se cumplan todos los criterios de seguridad para proveedores y programas de terceros, y que las características del tiempo de desarrollo no se dejen en los dispositivos, exponiéndose a vulnerabilidades (2021).

2.2.5.2. V2 - Requisitos de la aplicación del espacio de usuario

Las reglas de este capítulo están diseñadas para proporcionar acceso seguro a un sistema IoT por parte de humanos y máquinas, así como para proteger los datos confidenciales mediante el uso de las mejores prácticas de seguridad.

El acceso debe ser autenticado y autorizado para que sea seguro. Las restricciones relevantes incluyen una fuerte identificación segura única, segregación de roles de usuario y la idea de privilegio mínimo. La autenticación es el acto de establecer o verificar la

identificación de alguien (o algo) como auténtico, como base para creer que las declaraciones hechas por una persona o sobre un dispositivo son verdaderas y resistentes a la suplantación.

La prevención de la recuperación o interceptación de las credenciales de autenticación, como contraseñas, claves de API y claves privadas, es otro control importante. El acto de crear o validar que alguien (o algo) tiene derechos de acceso a recursos o actividades que cumplen con la política de acceso seguro se conoce como autorización.

Para garantizar el uso seguro de los recursos del sistema, como archivos que contienen datos o código, y el contenido de la memoria, los datos confidenciales, incluidas las contraseñas, deben protegerse y la información privada debe tratarse de manera justa.

La criptografía se utiliza para realizar muchos de los controles de este capítulo. Como resultado, se requieren protecciones adicionales para elegir las primitivas criptográficas apropiadas y configurarlas con almacenamiento seguro de credenciales.

2.2.5.3. V3 - Requisitos de la plataforma de software

El gestor de arranque es la primera pieza de código que se ejecuta cuando se inicia el dispositivo. El fabricante del firmware es responsable de instalar correctamente los gestores de arranque; de lo contrario, sus fallas podrían debilitar la seguridad de todo el dispositivo, lo que podría comprometer y secuestrar el dispositivo. Los controles de este capítulo aseguran la confiabilidad del arranque al verificar las firmas criptográficas en los programas cargados, no permitir la carga de imágenes desde sitios externos y deshabilitar la memoria, el Shell y otros accesos de depuración durante el arranque.

Debido a que operan en modo privilegiado e implementan funciones importantes del dispositivo, incluidas numerosas primitivas de seguridad, el sistema operativo y su núcleo son fundamentales para la seguridad del dispositivo. Se requieren los mejores procedimientos de seguridad para el sistema operativo, la configuración del kernel y el fortalecimiento.

Uno de los sistemas operativos más utilizados en IoT es Linux. Incluye métodos de aislamiento habilitados por espacios de nombres y cgroups, así como módulos de seguridad de kernel adicionales para restricciones de acceso, que van desde la seguridad de primera línea hasta la defensa en profundidad. Al configurar e implementar programas de terceros para operar dentro de un contenedor, es recomendable utilizar estas técnicas de separación.

El software del dispositivo debe actualizarse y mantenerse periódicamente para garantizar la seguridad del producto. Para garantizar que los dispositivos solo ejecuten software firmado criptográficamente sin vulnerabilidades conocidas, los sistemas de actualización deben incorporar las mejores prácticas de seguridad en su diseño e implementación. Los protocolos de administración de vulnerabilidades y parches garantizan que las versiones más recientes se utilicen para publicar compilaciones nuevas con actualizaciones de seguridad ascendentes para evitar que los usuarios finales se comprometan.

2.2.5.4. V4 - Requisitos de comunicación

Dentro de su ecosistema, los dispositivos emplean conectividad de red para intercambiar datos y recibir pedidos. Para asegurar que los contenidos de las comunicaciones sean confiables para las distintas partes, se deben salvaguardar, asegurando la validez de las partes, la integridad contra alteraciones maliciosas y el secreto contra la fuga de información.

En realidad, esto significa adoptar los protocolos de comunicación actuales y configurar sus funciones de seguridad, como la criptografía. Debido a que los estándares de la industria para TLS, Bluetooth y Wi-Fi seguros cambian constantemente, la configuración debe examinarse periódicamente para garantizar que la seguridad de las comunicaciones sea siempre efectiva. Independientemente de la importancia de los datos que se comunican, utilice siempre TLS o un cifrado y autenticación robustos similares.

Se deben tener en cuenta los siguientes puntos para aplicar el requerimiento correctamente:

- Siempre utilizar autenticación basada en certificados con pinning y la autenticación mutua.
- Utilizar la configuración más reciente para activar y seleccionar el orden deseado de cifrados y algoritmos de comunicación.
- Los algoritmos y cifrados obsoletos o inseguros conocidos deben deshabilitarse.
- Para los métodos de comunicación por cable e inalámbricos, utilizar la configuración de seguridad más alta posible.

2.2.5.5. Requisitos de la plataforma de hardware

Comprometer hardware es mucho más costoso y consumidor de tiempo que hacerlo al software. Como resultado, la seguridad del hardware puede servir como una base sólida para la seguridad de los dispositivos integrados. El hardware con puertas traseras o funciones de depuración no documentadas, por otro lado, podría poner en peligro la seguridad de todo el dispositivo, incluso si se han tomado las medidas de seguridad adecuadas en los otros niveles de la pila.

Las reglas de este capítulo están diseñadas para garantizar que, siempre que el hardware esté disponible para una configuración segura, se configure de la manera más segura posible. Esto implica desactivar o proteger los puertos de depuración, configurar todas las alarmas y sistemas de sensores existentes para evitar la manipulación, emplear protección de hardware anti-clonación, como fusibles OTP, y utilizar la MMU (Unidad de gestión de memoria) para el aislamiento seguro del proceso.

El ISVS define tres etapas de verificación de seguridad, y cada nivel aumenta en detalle. Cada nivel incluye un conjunto de requisitos que coinciden con las capacidades y características sensibles a la seguridad.

2.2.5.6. Nivel 1 de ISVS

El propósito de los requisitos de nivel uno es protegerse contra ataques solo de software, es decir, ataques que no requieren acceso físico al dispositivo. Los criterios de nivel uno está destinados a establecer una línea de base de seguridad para los dispositivos conectados en situaciones en las que la violación física del dispositivo no tiene como resultado un efecto de seguridad importante. Estos son dispositivos en los que la dirección IP del dispositivo no debe protegerse, no se guarda información confidencial en el dispositivo y la penetración de un dispositivo no permite que un atacante se mueva lateralmente a otros dispositivos o sistemas en el ecosistema de IoT.

Una bombilla inteligente hecha con hardware y software comercial es un ejemplo de un dispositivo de primer nivel. Un atacante no tendría acceso a tecnología de punta si la bombilla se viera comprometida. No se pueden robar datos si no se guardan datos personales en el dispositivo. Si la autenticación y la autorización se establecen correctamente en la

infraestructura de la nube subyacente, lo menos que puede hacer el atacante es falsificar el estado de la bombilla pirateada.

2.2.5.7. Nivel 2 de ISVS

El propósito de los requisitos de nivel dos es protegerse contra ataques que van más allá del software y tienen como objetivo el hardware del dispositivo. Los dispositivos que cumplen con los estándares de nivel dos son aquellos en los que se debe evitar el compromiso del dispositivo. Estos son dispositivos en los que la propiedad intelectual (IP) del dispositivo debe protegerse razonablemente y los datos confidenciales se mantienen en el dispositivo.

Las cerraduras inteligentes, los sistemas de alarma, las cámaras inteligentes y los dispositivos médicos que recopilan datos de medición y los envían a un médico para su análisis son ejemplos de dispositivos de nivel dos.

2.2.5.8. Nivel 3 de ISVS

Los criterios del nivel tres están destinados a establecer estándares para dispositivos en los que el compromiso debe evitarse a toda costa. Dispositivos que contienen información extremadamente confidencial o donde el compromiso del dispositivo podría resultar en fraude. Los requisitos del nivel tres, además de los requisitos de seguridad proporcionados por los niveles uno y dos, se centran en enfoques de defensa en profundidad que buscan frustrar las operaciones de ingeniería inversa y manipulación física.

Las billeteras criptográficas de hardware, los medidores inteligentes, los automóviles vinculados, los implantes médicos y las máquinas de reciclaje que intercambian latas de aluminio por dinero son ejemplos de dispositivos de nivel tres.

2.3. Marco legal

Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología

La República Dominicana aprobó la Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología el 23 de abril de 2007. Esta ley tiene por objeto proteger contra los delitos cometidos con alta tecnología, así como prevenir y sancionar los delitos cometidos contra los sistemas que utilizan las tecnologías de la información y la comunicación, o cualquiera de sus componentes, que causen daños a las personas físicas o jurídicas, según lo dispuesto en la ley. La integridad de los sistemas de información y sus componentes, la información o datos almacenados o transmitidos a través de estos sistemas, las transacciones y acuerdos comerciales o de otro tipo realizados a través de ellos, y la confidencialidad de estos elementos, están todos protegidos por la ley.

Capítulo 3: Marco Metodológico

3. Introducción al marco Metodológico

Este se destaca por ser aquellas acciones y procesos, los cuales buscan definir y analizar de manera profunda el problema planteado, esto se realiza a través de procedimientos específicos los cuales incluyen las técnicas de observación y recolección de la información, de modo que se pueda describir el 'cómo' se irá a realizar el estudio, el ejercicio tiene como objetivo validar las definiciones y piezas del problema que se está estudiando. Ya lo dice Sabino (2007): "En cuanto a los elementos que es necesario operacionalizar pueden dividirse en dos grandes campos que requieren un tratamiento diferenciado por su propia naturaleza: el universo y las variables" (p.118).

Tamayo y Tamayo (2003), se refiere al marco metodológico como: "Un proceso que, mediante el método científico, procura obtener información relevante para entender, verificar, corregir o aplicar el conocimiento" (p.37), esto en cierta medida tiene como base el método científico, ya que permite a través del método científico validar las hipótesis a través de investigaciones, de modo que estas sean aprobadas o descartadas.

3.1. Tipo de Investigación

Debido a que la meta del estudio será encontrar soluciones a los diversos problemas de seguridad que podrían presentar los dispositivos de internet de las cosas, decidimos que el enfoque de la investigación sea de tipo experimental. De modo que se pueda observar los dispositivos en su estado natural y bajo los esquemas propuestos, de modo que la información pueda ser recolectada en distintos ambientes y estados, ya que de esta manera facilita el proceso de trabajo con la información, su comparación y presentación de resultados.

3.2. Método

El estudio presentará una metodología de investigación cuantitativa. El objetivo de este tipo de método es recolectar informaciones a través datos ya existentes y cuestionarios, este está basado en datos reales y atados al mundo real. Este tiene las características de los datos deben ser medibles y deben existir hipótesis previa a la realización de la investigación, de modo que se puedan concretar los resultados una vez terminado todo el proceso.

Como menciona Cáceres (1996) la Investigación Cuantitativa, se centra fundamentalmente en los aspectos observables y susceptibles de cuantificación de los fenómenos educativos, utiliza la metodología empírico-analítica y se sirve de pruebas estadísticas para el análisis de datos.

Hernández (2006), en la investigación Cuantitativa Los estudios que utilizan este enfoque confían en la medición numérica, el conteo, y en uso de estadística para establecer indicadores exactos.

3.3. Investigación Preliminar

Durante esta investigación cuantitativa, teniendo en cuenta los objetivos que se buscan durante la misma, decidimos que el alcance que conviene adoptar al proceso es el explicativo. Ya que como se menciona en un blog posteado en Inveweb (2016): Son las investigaciones que pretenden darnos una visión general, de tipo aproximativo, respecto a una determinada realidad. Esto se suele dar más que nada cuando el tema elegido para el estudio no ha sido muy explorado, conocido o experimentado sobre él, es difícil formular hipótesis claras o de cierto grado de generalidad sobre ellos.

3.4. Delimitación del problema

Inicialmente solo serán tomados en cuenta aquellos dispositivos de Internet de las Cosas que realicen sus comunicaciones a través de redes de internet. De manera particular aquellos que comparten datos hacia internet para compartir algún tipo de información.

3.4.1. Área geográfica

La población que se estudiará serán aquellas personas o empresas que hacen uso de dispositivos de internet de las cosas de manera frecuente en su día a día o durante sus labores empresariales.

3.4.2. Tiempo

Se utilizará el primer mes para la recopilación de información, realización de entrevistas y cuestionarios. Los próximos 3 meses serán utilizados para desarrollar e implementar un prototipo funcional de la solución. Los últimos 2 meses serán utilizados para la realización de ajustes de acuerdo con los resultados obtenidos y el análisis de las variables recogidas antes y después de que finalizara el proyecto.

3.4.3. Población y muestra

La población estará compuesta por aquellos individuos que hagan uso de dispositivos de internet de las cosas en su vida cotidiana y aquellas empresas que utilizan dispositivos de internet de las cosas para la realización de tareas automatizadas dentro del entorno empresarial. Del lado de los individuos estos deben realizar tareas simples con los dispositivos o monitorear utilizando dispositivos como Cámaras de Seguridad IoT. Del lado de las empresas se tomarán en cuenta aquellas que utilicen dispositivos de internet de las cosas para automatizar procesos empresariales.

De toda esta población se tomará en cuenta el tipo de información que se comparte, como se comparte, puertos y protocolos utilizados para la comunicación, vulnerabilidades y riesgos asociados a dichas vulnerabilidades.

3.4.4. Técnicas e Instrumentos

Como instrumentos principales de recolección y medición utilizaremos cuestionarios y encuestas. Estos servirán como una guía y herramienta de seguimiento de la cultura de ciberseguridad del usuario y si esta está al tanto de los riesgos asociados a estos dispositivos. Como plantea Tomás García, el cuestionario consiste en un conjunto de preguntas, normalmente de varios tipos, preparado sistemática y cuidadosamente, sobre los hechos y aspectos que interesan en una investigación o evaluación (2003). Existen distintos tipos de preguntas que se pueden realizar en los cuestionarios, durante la investigación nos enfocaremos en las preguntas abiertas y cerradas, ya que las preguntas pueden variar dependiendo del contexto sobre el cual se esté evaluando al entrevistado. Se tomarán en cuenta tanto las preguntas abiertas ya que estas permitirán entender la percepción que tiene el entrevistado sobre la ciberseguridad y los impactos que pueda llegar a creer tener en su diario vivir, y también se hará uso de preguntas cerradas, ya que estas ayudan a eliminar la ambigüedad de las respuestas ante algunas situaciones específicas que se requieran consultar.

También se utilizará la observación como método de recolección de información, esto se realiza observando el objeto de estudio en entornos controlados, es decir, dentro de aquellas situaciones específicas bajo las cuales se requiere evaluar el dispositivos o red de dispositivos.

Serán utilizadas entrevistas con expertos de modo que se pueda profundizar dentro del tema de las vulnerabilidades y situaciones de riesgo que afecten a los individuos y las posibles consecuencias que se puedan tener en caso de que se explote alguna de las vulnerabilidades previstas, todo esto con el objetivo de tener el punto de vista experto sobre la situación.

Por último, pero no menos importante, serán utilizados marcos de trabajo internacionales y nacionales como instrumentos de referencia para la realización de recomendaciones, vulnerabilidades conocidas y métodos de escaneo y recolección de datos específicos relacionados a la ciberseguridad.

3.4.5. Técnica de procesamiento de análisis de datos

En esta sección se presentarán los medios que serán utilizados para el registro de la información que se obtenga. Debido a las limitantes de tiempo que existen para la realización de este proyecto, se aplicaran métodos de recolección de información se emplea la metodología cuantitativa de modo que se pueda evaluar el grupo de dispositivos, riesgos, vulnerabilidades y recomendaciones de una manera que permita arrojar un reporte adecuado sobre lo investigado además de todos los recursos relacionados al internet.

Estos procesos serán procesados a través del paquete de oficina de Microsoft, específicamente utilizando Excel de modo que se pueda manejar la data recolectada y procesar los datos de manera estructurada.

3.4.6. Fuentes de datos

Como fuente de información se tomarán para esta investigación se tomarán en cuenta las informaciones relacionadas al tema encontradas a través de internet en artículos, revistas, libros y Bases de datos de vulnerabilidades. Además de esto también serán valoradas las respuestas provistas por los usuario y expertos que se le realicen las encuestas y cuestionarios preparados.

En adición a esto será utilizado el Centro de Recursos para el Aprendizaje y la Investigación (CRAI) de UNIBE de donde extraemos fuentes pertinentes relacionadas al tema a tratar con el fin de que brinden apoyo a la investigación.

Capítulo 4: Plan de mercadeo y Análisis del entorno

4. Plan de mercado y Análisis del entorno

4.1. Introducción al capítulo

El plan de mercadeo y el análisis del entorno son procesos bastante importantes debido a que detallan las acciones que se deben llevar a cabo para alcanzar los objetivos de ventas de una empresa y sirven como herramientas de planeación estratégica que sirve de guía para la toma de decisiones en el área de mercadeo.

El plan de mercadeo debe incluir un análisis del entorno en el que se desenvuelve la empresa, así como un estudio de la competencia y de los clientes potenciales. Asimismo, debe tener en cuenta los objetivos de la empresa y los recursos disponibles para llevar a cabo las acciones de mercadeo.

En este capítulo veremos los diversos elementos de mercado alrededor de los cuales se basará nuestra investigación, como podrían ser los estudios de mercado, benchmarking, presupuesto, modelo de mercado, entre otros.

4.2. Benchmarking

El Benchmarking es la práctica de comparar el rendimiento de los productos, servicios o procesos de una empresa con los de otra empresa que se considera la mejor de la industria, a veces conocida como "la mejor de su clase". El benchmarking se utiliza para encontrar posibilidades internas de mejora. Puede adoptar cambios que generarán beneficios sustanciales mediante el análisis de empresas con un desempeño sobresaliente, desglosando lo que hace que ese desempeño superior sea factible y luego comparando estos procedimientos con la forma en que funciona su negocio.

Esto podría incluir la modificación de las características de un producto para que coincida más con la oferta de un competidor, la alteración del alcance de los servicios que brinda o la implementación de un nuevo sistema de administración de relaciones con los clientes (CRM) para permitir contactos más personalizados con los clientes.

Hay dos tipos de oportunidades de mejora: continuas y espectaculares. La mejora continua es gradual y sólo requiere pequeños ajustes para proporcionar ganancias significativas. Solo mediante la reingeniería de todo el proceso de trabajo interno se pueden lograr mejoras drásticas.

El benchmarking es una técnica de cinco pasos básicos:

1. Para comparar, seleccionar un producto, servicio o departamento interno.
2. Determinar las mejores empresas de su clase con las que debe comparar: las corporaciones con las que medirá su negocio. Recopilar información sobre su rendimiento interno o métricas.
3. Comparar los datos de ambas empresas para encontrar disparidades de rendimiento en su empresa.
4. Adoptar los métodos y prácticas utilizados por los mejores en su clase.
5. La evaluación comparativa mostrará qué mejoras marcarán la mayor diferencia, pero seremos nosotros quienes la implementemos.

Para los fines del análisis del mercado se estudiaron 2 marcas adicionales a nuestro proyecto IoTarget con el fin de estudiar los diversos puntos importantes a destacar de cada una y realizar una comparación objetiva. Dichas marcas fueron Keysight y 7 Layers (Ver tabla 1).

Tabla 1: Análisis y funcionalidades del proyecto.

Funcionalidades	IoTarget	Keysight	7 Layers
Fácil implementación	Si	Si	Si
Fiabilidad	Alta	Alta	Media
Costo	Bajo	Alto	Alto
Rapidez de despliegue	Alta	Media	Alta
Consola centralizada	Si	Si	Si
Diagnóstico	Si	Si	Si
Método de despliegue	Wireless/Ethernet	Wireless/Ethernet	Wireless
Región	Rep. Dom. (temporal)	Global	Global

Fuente: Elaborada por los sustentantes.

4.3. Mecanismo para poblar de información el sistema

Nuestro proyecto se basa principalmente en el análisis de información en base a escaneos de red y a través de la información obtenida realizar una correlación con su base de conocimiento con el fin de poder brindar recomendaciones y comentarios al respecto a quien realice dicho estudio.

Con el fin de obtener información correspondiente de cada dispositivo se realizará un escaneo de red utilizando herramientas integradas al software. Este escaneo brindaría información como el fabricante, el tipo de dispositivo, la IP y los puertos que se encuentran abiertos. Con esta información será posible realizar una búsqueda de información en la base de datos de OWASP y correlacionar el servicio que utiliza el puerto abierto con los servicios vulnerables conocidos y así brindar recomendaciones de lugar al usuario.

4.4. Modelo de negocio

Utilizando el método Canvas podemos especificar y describir el modelo de negocio. Según Alcalde (s. f.) en el blog Economipedia, nos dice que Canvas es una herramienta para analizar y crear modelos de negocio de forma sencilla. Globalmente, se muestra como un lienzo dividido en los principales aspectos que involucran al negocio y gira en torno a la propuesta de valor que se ofrece.

Existen diversas ventajas de utilizar el método Canvas para el desarrollo del modelo de negocio, entre las que se encuentran:

- Mejora la comprensión: Utiliza herramientas visuales. Este proceso anima a los trabajadores que hacen el lienzo a pensar creativamente.
- Enfoques diversos: Esta estrategia preserva una imagen consistente del modelo de negocio desde varios ángulos, como los canales comerciales, de mercado y de distribución.
- Análisis estratégico: En una sola hoja de papel se pueden visualizar todos los aspectos del lienzo. Un enfoque sencillo para lograr la máxima tracción con este instrumento.

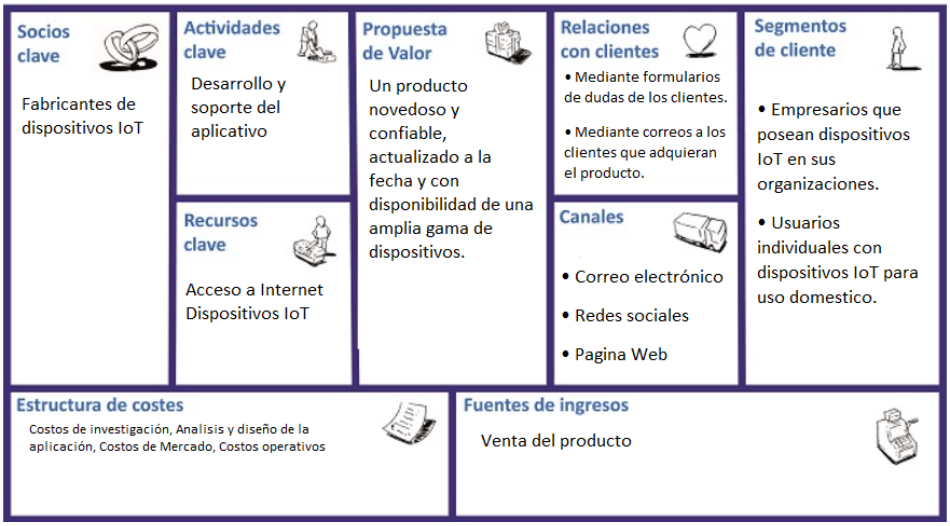


Figura 2: Modelo de negocio utilizando método Canvas
Fuente: Elaborada por los sustentantes utilizando plantilla de Innokabi

4.5. Presupuesto

Para el presupuesto se dividió el proyecto en etapas de desarrollo del mismo con el fin de segmentar los gastos que para cada una se requerirían.

Tabla 2: Presupuesto del proyecto.

#	Etapa	Descripción	Horas de trabajo	Precio/h	Costo en RD$ sin Imp.
1	Análisis	Estudio y levantamiento de los requerimientos del proyecto	48	$ 250.00	$ 12,000.00
2	Diseño	Creación del diseño en base a los requerimientos	72	$ 250.00	$ 18,000.00
3	Base de conocimiento	Se desarrolla la base de conocimiento que utilizará el software	124	$ 250.00	$ 31,000.00
4	Desarrollo	Se desarrolla el software	200	$ 250.00	$ 50,000.00
5	Pruebas	Se realizan pruebas funcionales y de integración del software	132	$ 250.00	$ 33,000.00
6	Documentación	Se realiza la documentación del software	24	$ 250.00	$ 6,000.00
7	Implementación	Se instala y despliega el software en producción	48	$ 250.00	$ 12,000.00
8	Costos de Operaciones	Dominio web y hosting para descarga del software o despliegue en el entorno requerido	1	$40,000.00	$ 40,000.00
9	Ingresos	Ingresos en base a ventas de 5 clientes del primer año	5	$69,000.00	$ 345,000.00
			Subtotal		$ 202,000.00
			Impuestos		$ 36,360.00
			Total de egresos		**$ 238,360.00**

Fuente: Elaborada por los sustentantes

4.6. Retorno de inversión

Según el blog Econopedia, el retorno de la inversión (ROI) es una medida que nos permite evaluar la rentabilidad de una inversión en función del capital puesto y la ganancia obtenida. Se ingresa el beneficio (logrado o deseado) en el numerador y la inversión en el denominador para calcular el ROI. En términos de interpretación, si el indicador es menor que cero, la inversión no es rentable. Si es mayor que cero, implica que se ha reportado una ganancia (Westreicher, 2021).

$$ROI = \frac{Beneficio}{Inversión} = \frac{Ingresos - inversión}{Inversión}$$

Figura 3: Fórmula de ROI

El Principal ingreso a tomar en cuenta está basado en la venta del software, este tendrá un costo final de 49,000 pesos dominicanos, por licencia de un año, adicional a este, se preparó un esquema de licencias adicionales y servicios de mantenimiento y asesoría que tienen costos adicionales que van desde los $25,000 hasta los $40,000 por cada licencia o servicio adicional que se contrate. Debido a esto, el cálculo se realizará en base a 1 (una) licencia por cliente y 1 (un) servicio de mantenimiento con un costo de $20,000 pesos dominicanos siendo de esta manera un ingreso base de $69,000 Pesos dominicanos por cada cliente.

Adicionalmente a los costos de desarrollo del proyecto presentados en la tabla 2, no se requiere de un dispositivo físico que se encargará de realizar el análisis de información por lo que la inversión se basaría principalmente en el presupuesto señalado. Por lo que se estima que el retorno de inversión para el primer año sería como sigue:

Tabla 3: Tabla de ROI

Retorno por inversión del primer año	**Monto**
Ingresos (5 clientes)	$345,000.00
Gastos (Egresos)	$238,360.00
Utilidad Neta	$106,640.00
ROI	**44.7%**

Fuente: Elaborada por los sustentantes

Capítulo 5: Análisis, presentación de Resultados y Conclusiones

5. Introducción al capítulo

Durante este capítulo se conocerán los resultados obtenidos con los instrumentos y técnicas señalados durante el capítulo 3. Luego se detallarán los análisis realizados a los resultados para conocer si se cumple la hipótesis y lograr sacar conclusiones luego de terminado el proceso.

5.1. Encuestas

Luego de haber sido aprobada por el Comité de Ética de la Institución, las siguientes son las preguntas utilizadas para conseguir los datos.

1. ¿Cuál es su rango de edad?
    a. 18-24
    b. 24-30
    c. 31-39
    d. 40 o más

Motivo: Conocer el rango de edad nos permitirá saber el entendimiento de los encuestados de acuerdo con que rango pertenecen de los incluidos en las opciones.

2. ¿Sabe usted que es un dispositivo de internet de las cosas?
    a. Si
    b. No

Motivo: Una pregunta fundamental dentro de nuestra revisión, debido a que nos permitirá saber el entendimiento que tienen los encuestados con relación al tema tratado en la tesis.

3. Tiene usted dispositivos de internet de las cosas que se conecten a su red de hogar/trabajo?
    a. Si
    b. No

Motivo: Con esta pregunta buscamos saber qué número de los encuestados realmente posee los dispositivos de internet de las cosas, de modo que podamos filtrar sobre los casos que son realmente relevantes.

4. ¿Utiliza usted dispositivos de internet de las cosas en su casa o trabajo?
    a. Casa
    b. Trabajo
    c. Ambos

    Motivo: Con esto logramos diferenciar sobre cuál entorno los encuestados hacen uso de sus dispositivos de internet de las cosas.

5. ¿Cuántos dispositivos de internet de las cosas posee?
    a. 1
    b. 2
    c. 3
    d. 4 o más

    Motivo: Pregunta para entender el número de dispositivos de internet de las cosas que tienen cada persona, de esto se tomará al final un promedio de modo que tengamos un estimado de cuántos dispositivos hay por persona en un entorno de hogar o laboral.

6. ¿Qué tipo de dispositivo de internet de las cosas posee? (Seleccionar múltiples)
    a. Cámaras de seguridad
    b. Nevera
    c. Amazon Echo (Dot, Show)
    d. Dispositivos Google home
    e. Apple homekit
    f. Impresora
    g. Aspiradora inteligente
    h. Otro (Especificar)

    Motivo: Con esto podremos determinar cuáles de los dispositivos de internet de las cosas son los más usados por los encuestados.

7. ¿Con qué frecuencia utiliza sus dispositivos de internet de las cosas?
    a. Muy frecuentemente

b. Frecuentemente
c. Ocasionalmente
d. Nunca

Motivo: Con esta pregunta podríamos entender cuál es el nivel de utilización de los dispositivos para cada persona con relación al tipo de dispositivo que tiene y al uso que este le da.

8. ¿Ha recibido concientización sobre los riesgos que presentan los dispositivos de internet de las cosas?
    a. Si
    b. No

Motivo: Con la respuesta a esta pregunta se conocería el nivel de individuos que alguna vez han adquirido algún tipo de concientización sobre los riesgos de sus dispositivos y sobre como mitigarlos.

9. ¿Sus dispositivos de internet de las cosas están debidamente actualizados?
    a. Si
    b. No
    c. No lo sé

Motivo: En base a esta respuesta, podríamos entender si los usuarios poseen un nivel de actualización óptimo de sus dispositivos en función de los tipos de dispositivos y la cantidad que este posee

10. Al momento de instalar su dispositivo, ¿se aseguró de que fueran cambiadas las credenciales por defecto? (Cuenta admin, contraseñas por defecto).
    a. Si
    b. No

Motivo: Gracias a esta pregunta, entenderíamos que cantidad promedio de usuarios se preocupa en realidad por la seguridad de sus dispositivos y en base a esto poder adaptar el prototipo en cuanto a las opciones que este brinde al usuario y su intensidad de operación.

11. ¿Estaría usted dispuesto a utilizar un software que le ayude a asegurar sus dispositivos de internet de las cosas a través de tips, mejores prácticas y configuraciones seguras?
    a. Si
    b. No

Motivo: Con la respuesta a esta pregunta, podríamos realizar una estimación de aceptación del producto en base a las elecciones anteriores de las personas que realicen la encuesta.

5.2. Entrevistas

No fueron realizadas entrevistas durante la realización de este trabajo de tesis.

5.3. Resultados de la Hipótesis planteada.

Mediante el proceso desarrollado, se evidenciaría un incremento en la seguridad de sus dispositivos de internet de las cosas que se conecten a través de redes LAN gracias a que los usuarios tendrán un mejor entendimiento de cómo proteger dichos dispositivos en base a mejores prácticas de la industria, creando así un entorno más ciberseguro.

Los resultados de la encuesta demostraron que la hipótesis es correcta ya que permitiría a los usuarios encuestados mejorar su entendimiento de los riesgos que representan los dispositivos de internet de las cosas y como mejorarlos a través de mejores prácticas, recomendaciones y tips de seguridad alineados con los resultados que buscan de sus dispositivos.

5.4. Verificación y evaluación de Objetivos

5.4.1. Verificación Objetivo General

Siendo el objetivo principal mejorar el nivel de ciberseguridad de dispositivos de internet de las cosas en entornos empresariales y personales incrementando el nivel de cultura de seguridad de la información del usuario, mitigando posibles brechas de seguridad tecnológica que afecten a los dispositivos IoT y disminuyendo los ataques efectuados a causa de estas.

Si observamos y analizamos los resultados de las encuestas sería posible entender que las personas tienen interés en utilizar el diseño propuesto que les permita recibir ese entendimiento y mejores prácticas para usar sus dispositivos de internet de las cosas de manera más segura.

5.4.2. Verificación Objetivos Específicos

1. Ofrecer un software que permitirá mejorar la seguridad para los dispositivos IoT conectados a la red Wireless.
2. Concientizar al usuario de los peligros y riesgos que implican no proteger estos dispositivos en base a lo que el mismo software encuentre.
3. Lograr un monitoreo pasivo de los dispositivos IoT Wireless.
4. Crear un procedimiento de ciberseguridad efectivo y simple que utilizará el propio software para la protección de dispositivos IoT Wireless.
5. Contribuir al cumplimiento de normativas locales e internacionales en cuanto a la regulación de dispositivos IoT.

Analizando los resultados de la encuesta entendimos que las personas están abiertas a utilizar el software propuesto y viendo la manera en la que respondieron, entendemos que será de gran beneficio el utilizar la idea propuesta para asegurar y entender mejor el funcionamiento de sus dispositivos de internet de las cosas.

5.5. Conclusiones

En el proceso de desarrollo del trabajo de investigación pudimos notar que la tendencia a usar dispositivos de internet de las cosas va en incremento, y de la misma manera la preocupación a en el entorno de la seguridad de la información concerniente a este tipo de dispositivos va en gran aumento, estos, vistos como uno de los vectores de ataque que podrían ser más peligrosos debido a la gran cantidad de dispositivos que pueden ser manejados en un entorno y la información que los mismos manejan.

Realizando la encuesta logramos notar el entusiasmo y la viabilidad de un software del tipo que estamos proponiendo tanto para entornos empresariales como personales, permitiendo al usuario entender mejor que riesgos implican el tener este tipo de dispositivos y ayudándolo a mitigar estos problemas utilizando mejores prácticas de la industria y recomendaciones de suplidores y terceros.

5.6. Verificación y evaluación de Objetivos

5.6.1. Líneas Futuras de Investigación

Dentro de las principales líneas futuras de investigación se encuentra darle un seguimiento al estado de la seguridad en los dispositivos IoT posterior a la utilización del sistema propuesto. Esto brindaría una idea del impacto que se podría causar al implementar campañas de seguridad y conocer el estado de seguridad de los dispositivos en una red.

Posteriormente se debe conocer cuáles son aquellos otros vectores de ataque en la infraestructura de las empresas con el fin de profundizar los conocimientos sobre la seguridad en las empresas y cómo podrían mitigarse otros posibles ataques.

Capítulo 6: Análisis y Diseño del Prototipo

6.1. Narrativa General

6.1.1. Objetivos de la empresa al que está dirigido el Proyecto

Como se indicó en los capítulos anteriores de este trabajo investigativo, el panorama de crecimiento en la utilización de los dispositivos de internet de las cosas va en constante crecimiento, sin embargo, en el ámbito de la seguridad no es tan común ver ecosistemas maduros con relación a la ciberseguridad en el que se incluya la protección de este tipo de dispositivos. Los ataques continuarán evolucionando y si no se crea una cultura de ciberseguridad adecuada la posibilidad de que los ataques a estos dispositivos incrementen será bastante alta. De acuerdo con los reportes de honeypots de Kaspersky para septiembre del 2021 los ataques a dispositivos de internet de las cosas se vieron casi duplicados en sus vectores de ataque comunes. (Seals, 2021)

Es por lo que el objetivo principal de la herramienta se encuentra en la concientización del usuario y proveer métodos y acciones que permitan ayudar a los usuarios de los dispositivos de internet de las cosas a que sus dispositivos se mantengan seguros y bien protegidos ante cualquier brecha conocida.

6.1.2. Breve descripción del sistema propuesto

El sistema propuesto consiste en una aplicación dirigida a aquellos usuarios que utilicen dispositivos de internet de las cosas para que estos puedan escanear su red para identificar los dispositivos, revisar sus puertos abiertos, ver posibles vectores de ataques a los que son vulnerables y recibir recomendaciones que permitan mitigar los riesgos presentes o identificados en los dispositivos encontrados.

El sistema se valdrá de buenas prácticas, marcos de trabajo reconocidos a nivel global y recomendaciones de los fabricantes y expertos para la mitigación de vulnerabilidades encontradas, esto con el motivo de estandarizar el método de trabajo e identificación de problemas.

6.1.3. Objetivos del sistema o proyecto

El objetivo general del sistema propuesto es el de desarrollar una aplicación que permita a sus usuarios desarrollar una cultura de ciberseguridad donde se comprenda los riesgos y vulnerabilidades a los que están expuestos estos dispositivos, adicional a esto permitirá el escaneo de dispositivos y puertos abiertos en los dispositivos en cuestión además de dar las recomendaciones para mitigar los riesgos y problemas que presentan estos dispositivos.

6.1.4. Innovaciones del sistema propuesto

El sistema propuesto trae a la mesa una nueva manera de proteger dispositivos de internet de las cosas conectados a una red Wireless. Mediante un software en un dispositivo conectado a la red, se realizarán análisis y recomendaciones de políticas de seguridad de los dispositivos IoT en la red. En el caso de los hogares este tipo de dispositivos suelen quedar poco protegidos y con acceso directo a internet, por lo que, con esta idea, a través del monitoreo y las recomendaciones de seguridad se busca encontrar vulnerabilidades en los dispositivos y aumentar el nivel de seguridad de estos, del lado empresarial tener una manera que permita utilizar y dar seguimiento a través de un marco de trabajo sería ideal para trabajar.

6.1.5. Ventajas y Beneficios

El sistema traerá varios beneficios a los usuarios que lo utilicen como podrían ser:

- Conocimiento de los puertos abiertos en tus dispositivos y los protocolos que utilizan.
- Identificación de vulnerabilidades conocidas basadas en escaneos activos de puertos.
- Recomendaciones de configuración basados en mejores prácticas y estándares internacionales.
- Educar al usuario con conocimiento en materia de ciberseguridad.

6.2. Análisis FODA del sistema propuesto

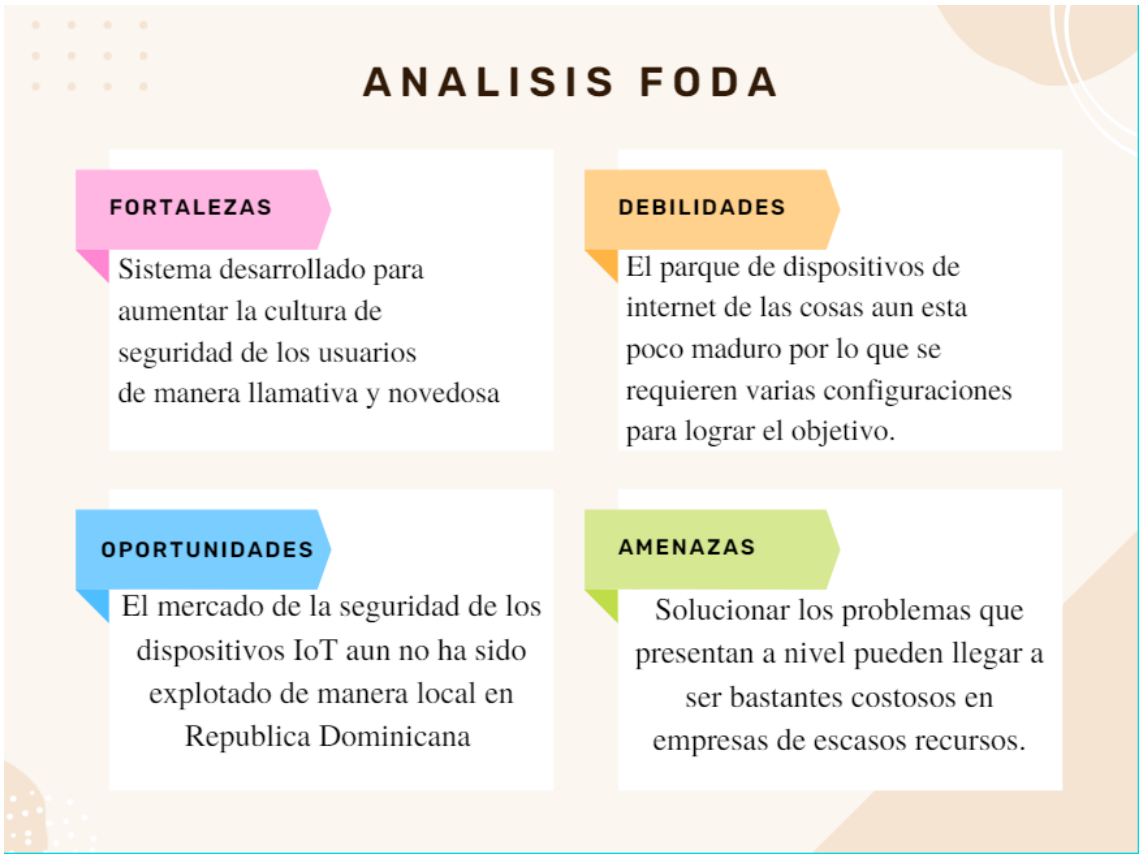


Figura 4: Análisis FODA.
Fuente: Elaborado por los sustentantes

6.2.1. Diagrama de contexto del sistema

IoTarget es un sistema que busca aumentar el nivel de conciencia de ciberseguridad de los usuarios de hogar y/o empresariales. Este sistema cuenta con distintas partes que interactúan bajo una aplicación web que sirve como concentrador para la aplicación y se integran para garantizar el correcto funcionamiento de todas las partes, de manera que los usuarios que utilicen la aplicación puedan tener un conocimiento más a fondo del estado a nivel de seguridad de sus equipos de internet de las cosas conectados a la red. A continuación, listaremos y describiremos las diferentes entidades, ya sean internas o externas, que componen todo el sistema propuesto:

- **Entidad Externa – Usuario de la aplicación**: El mismo hace referencia a todos los usuarios que podrán obtener informaciones sobre el nivel de seguridad de sus dispositivos de internet de las cosas a través de la aplicación web. Además de también las empresas que utilicen la aplicación web para utilizar sus funciones de escaneo, testeo o check de OWASP.
- **Entidad Externa – Dispositivos de internet de las cosas**: Estos son los dispositivos de internet de las cosas que serán utilizados para la revisión de acuerdo con los requerimientos del usuario.
- **Entidad Externa – Base de datos SQLite**: El sistema cuenta con una base de datos SQLite sobre la cual se almacenan toda la información utilizada por la aplicación, desde usuarios hasta datos de almacenamiento sobre los checks de OWASP.
- **Entidad Externa – Canal de uso**: El canal de uso para la aplicación web son los navegadores web.
- **Proceso – Backend del sistema**: En este proceso ocurren todos los procesamientos de datos recibidos a través de las funciones de la aplicación web, almacenando

información en las bases de datos y/o procesando los datos de los dispositivos encontrados.

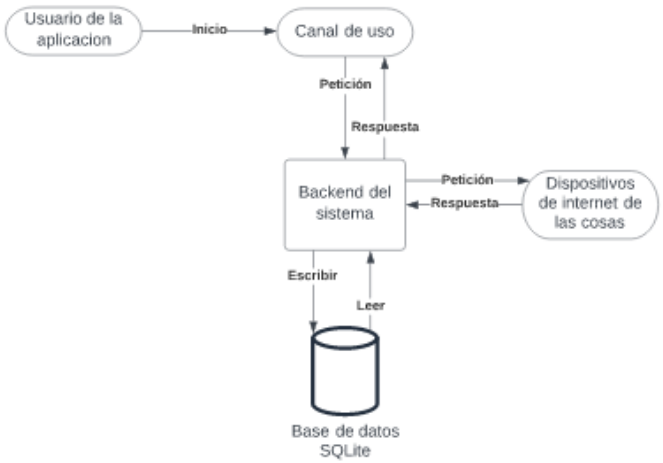


Figura 5: Diagrama de contexto del sistema.
Fuente: Elaborado por los sustentantes

6.3. Análisis funcional del sistema

El sistema es una aplicación web, la cual cuenta con siguientes funcionalidades:

- Registrar e inicio de sesión de los usuarios.
- Obtener información sobre los dispositivos de internet de las cosas de los usuarios, las informaciones recolectadas son las siguientes:
    - Direcciones IP
    - Hostname
    - Puertos abiertos
    - Protocolos expuestos
- Auditoría manual utilizando el estándar OWASP IoT Security Verification Standard ISVS.

6.4. Diagramas de flujo de los procesos:

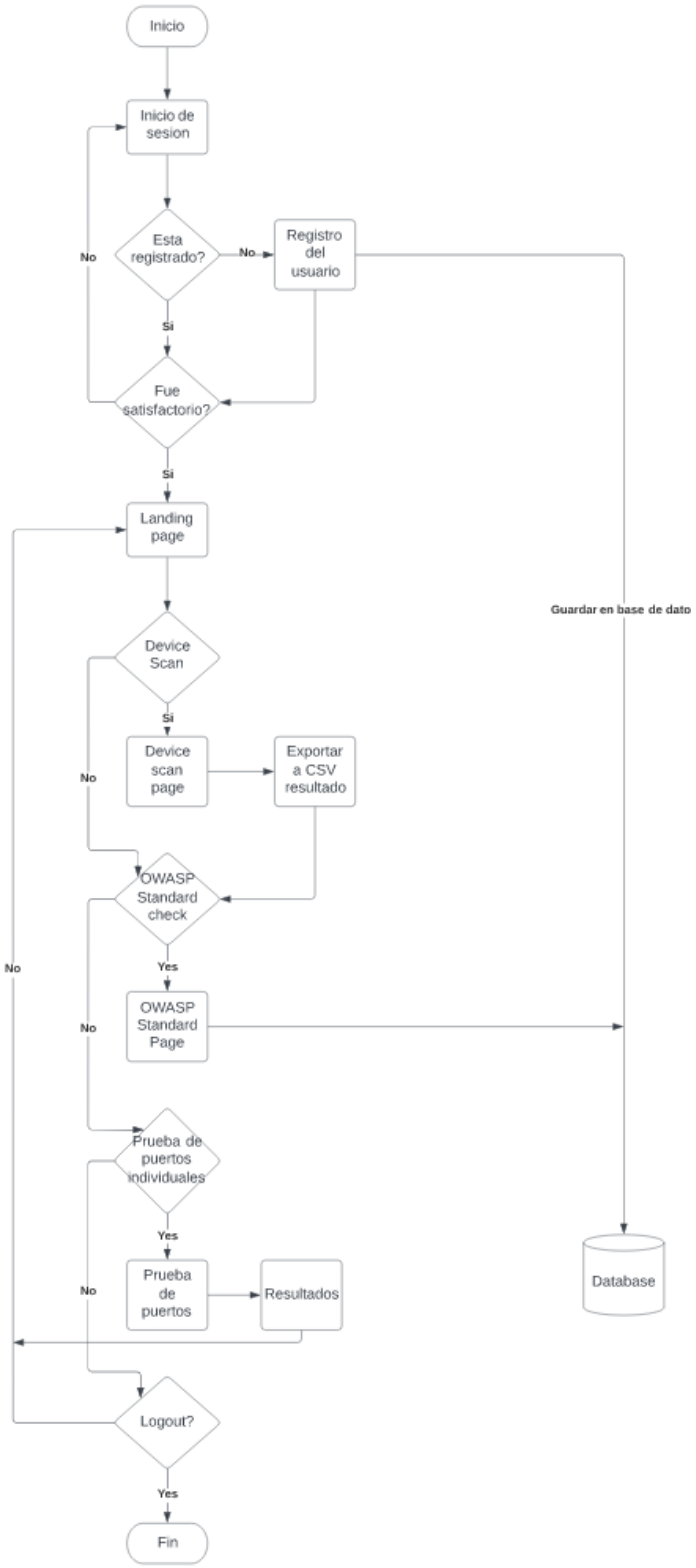


Figura 6: Diagrama de flujo del proceso
Fuente: Elaborado por los sustentantes

6.5. Diagrama de Flujo de Datos (DFD) del sistema propuesto

El sistema cuenta de dos (2) procesos básicos de datos que permiten el correcto funcionamiento de la aplicación web. A continuación, presentaremos una breve descripción y diagramas correspondientes de cada uno de los procesos previamente mencionados.

El primer diagrama describe el flujo del proceso de registro y/o logueo de los usuarios:

Figura 7: Diagrama de flujo de registro.
Fuente: Elaborado por los sustentantes

El segundo diagrama describe el proceso de procesamiento de registro de los cambios realizados al estándar OWASP vinculado al usuario que esté logueado.

Figura 8: Diagrama de flujo de cambios al OWASP ISVS Standard.
Fuente: Elaborado por los sustentantes

6.6. Diseño de la Base de Datos

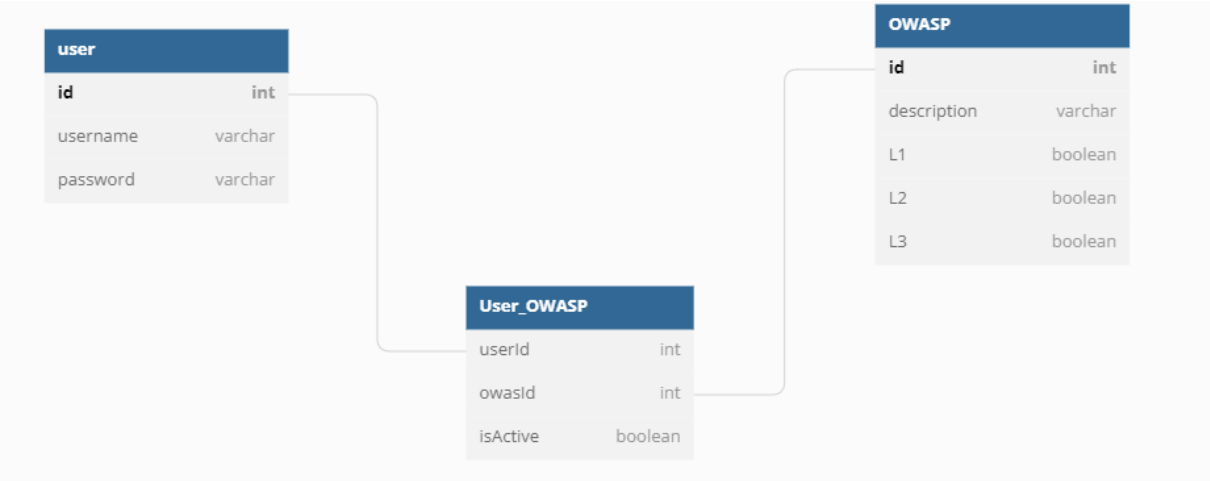


Figura 9: Diagrama E/R de la base de datos.
Fuente: Elaborado por los sustentantes

6.6.1. Esquema de la Base de Datos

```
Table user as U {
  id int [pk, not null, increment]
  username varchar
  password varchar
}

Table User_OWASP {
  userId int [not null, ref: > U.id]
  owasId int [not null, ref: > S.id]
  isActive boolean
}

Table OWASP as S {
  id int [pk, increment]
  description varchar
  L1 boolean
  L2 boolean
  L3 boolean
}
```

Figura 10: Esquema de la base de datos.
Fuente: Elaborado por los sustentantes

6.6.2. Diccionario de datos

Tabla 4: Diccionario de datos de la tabla user

Key	Types	Default	Foreign Key	Description
id	Numeric			Primary Key con el id
username	Text			Campo que almacena el nombre del usuario
password	Text			Campo que almacena la contraseña cifrada

Fuente: Elaborada por los sustentantes.

Tabla 5: Diccionario de datos de la tabla User_OWASP

Key	Types	Default	Foreign Key	Description
userid	Numeric		id de tabla user	Para vincular id de la tabla user
owaspid	Numeric		id de la tabla OWASP	Para vincular id de la tabla OWASP
isValid	Boolean			Campo que almacena el estado del subcontrol de OWASP

Fuente: Elaborada por los sustentantes.

Tabla 6: Diccionario de datos de la tabla OWASP

Key	Types	Default	Foreign Key	Description
id	Numeric			Primary Key con el id
description	Text			Campo con la descripción del subcontrol
L1	Boolean			Propósito que abarca el subcontrol de acuerdo con OWASP
L2	Boolean			Propósito que abarca el subcontrol de acuerdo con OWASP
L3	Boolean			Propósito que abarca el subcontrol de acuerdo con OWASP
subcontrol	Numeric			Campo que contiene el número de subcontrol de acuerdo con OWASP

Fuente: Elaborada por los sustentantes.

6.7. Formato de pantallas para las E/S de datos del sistema

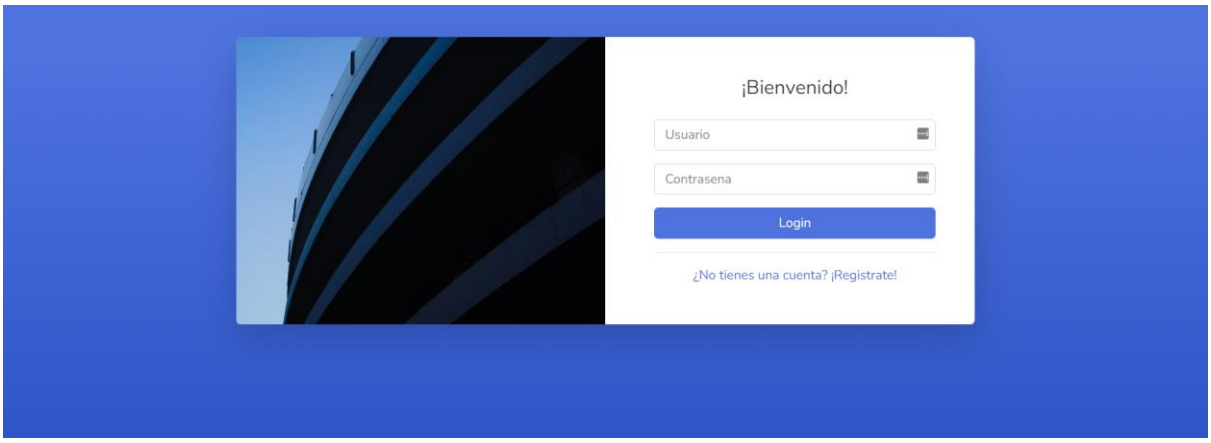


Figura 11: Pantalla de inicio de sesión

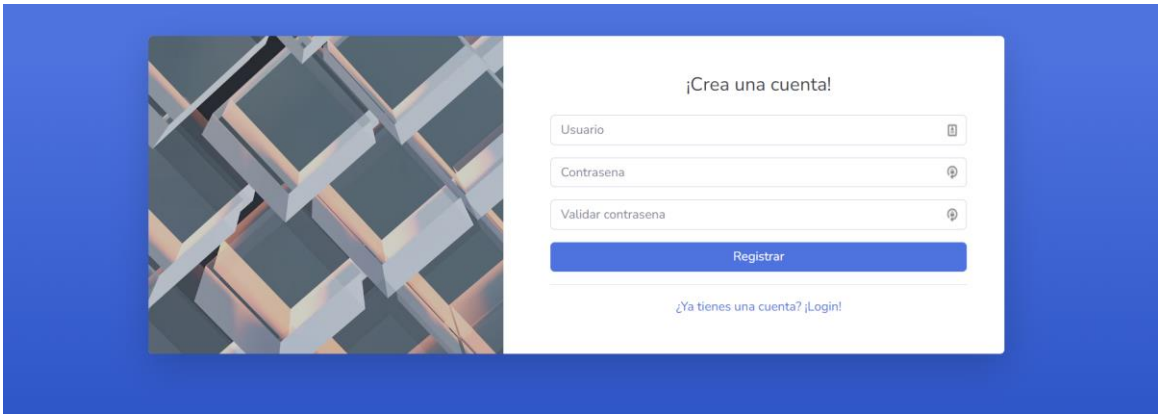


Figura 12: Pantalla de registro

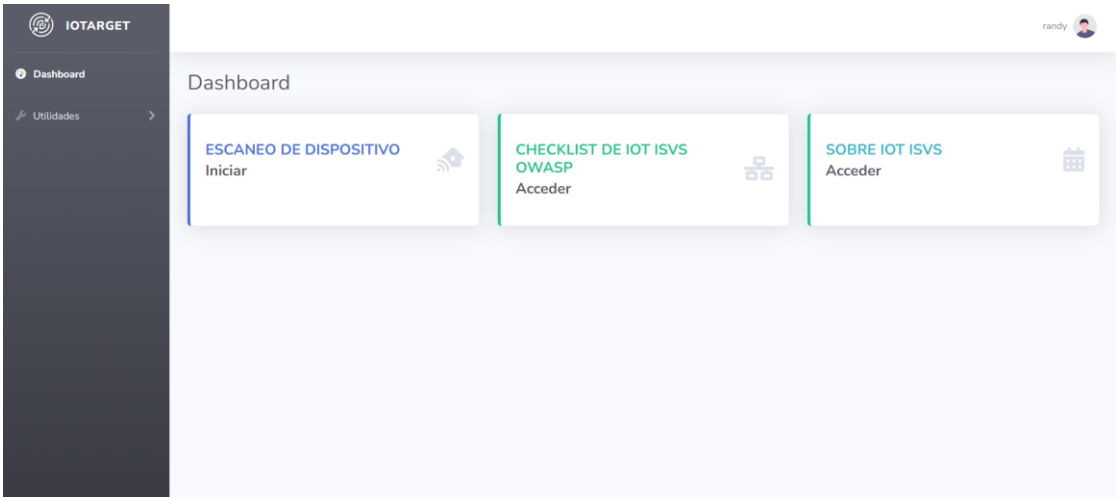


Figura 13: Landing page

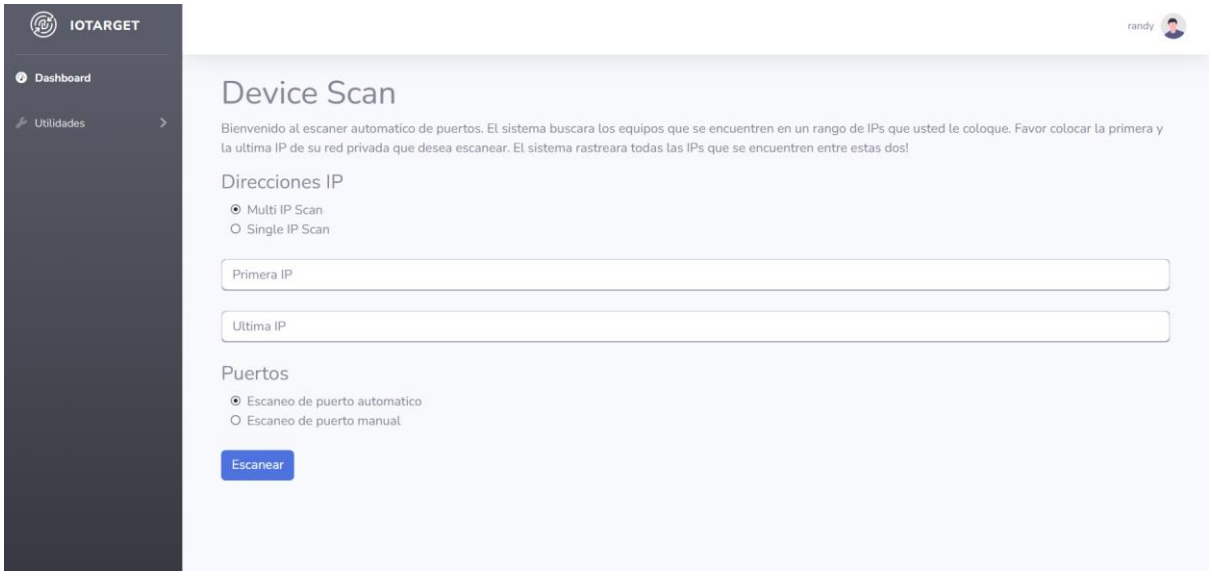


Figura 14: Página de escaneo de dispositivos

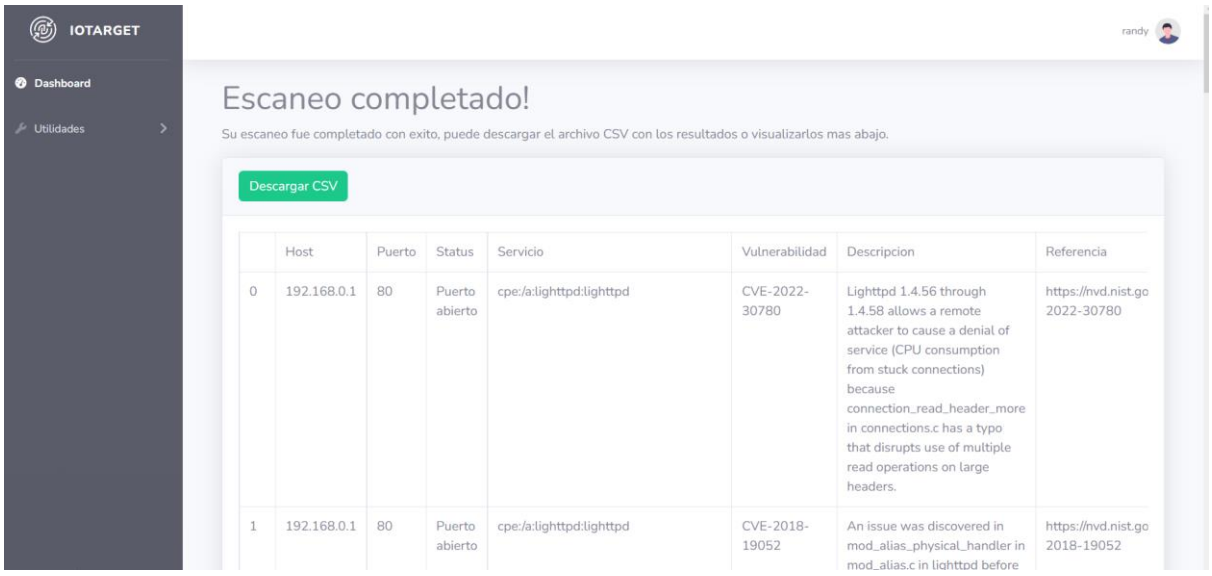


Figura 15: Página de descarga de CSV

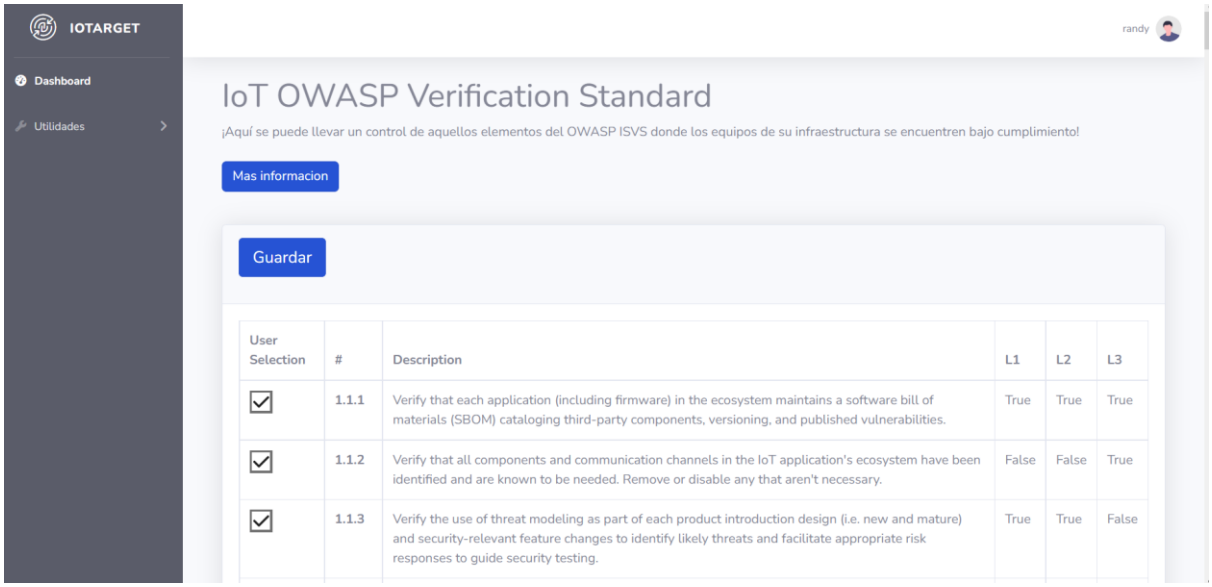


Figura 16: IoT OWASP Verification Standard

6.8. Diagrama jerárquico de programas y/o menús principales

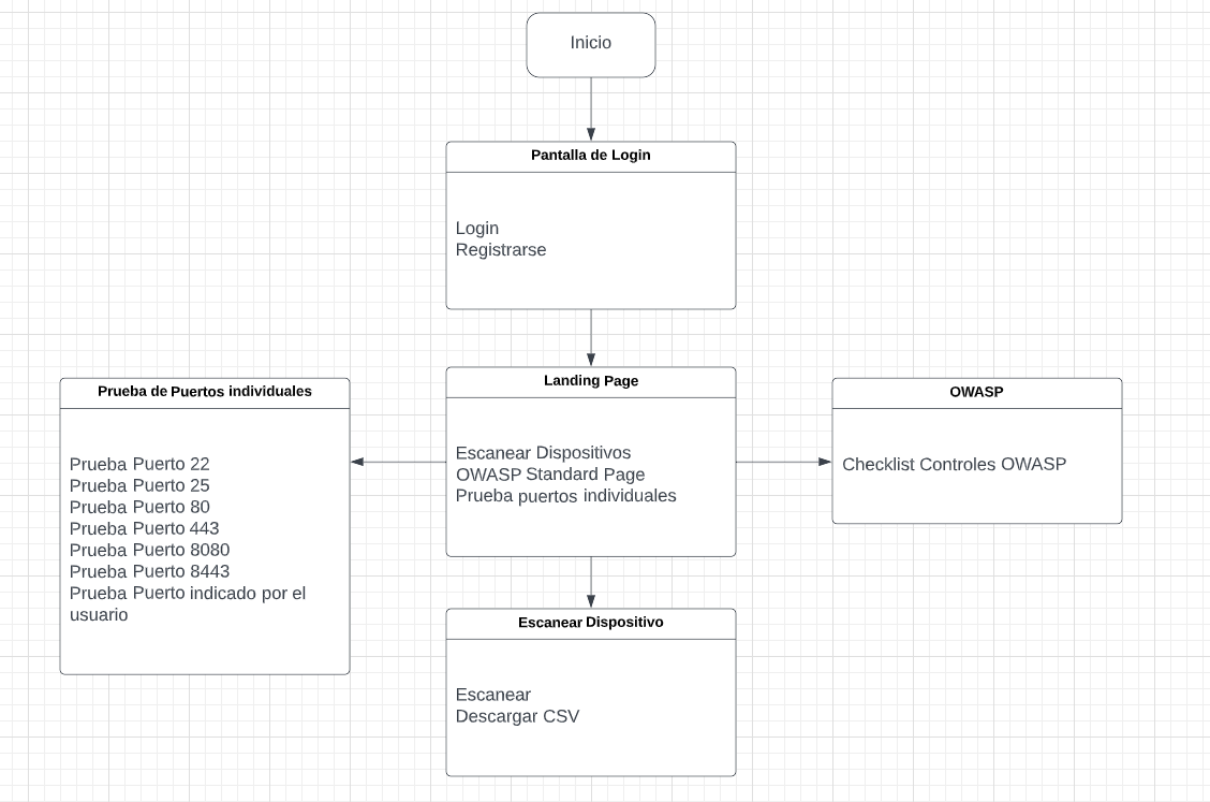


Figura 17: Diagrama jerárquico de programas y/o menús principales

6.9. Seguridad y Control

6.9.1. Políticas de Acceso de Seguridad

Con el fin de mantener la información de los usuarios segura a la hora de utilizar la aplicación se tomaron en cuenta los siguientes puntos durante su creación:

- Todas las contraseñas de usuarios son encriptadas a través del algoritmo de encriptación Bycript.
- Se utiliza sesiones para mantener las conexiones de usuario protegidas.
- El acceso a las bases de datos está protegido con credenciales.

6.10. Especificaciones generales del programa

Se trata de un sistema que integra una base de datos, un servicio web y un motor de escaneo de dispositivos. Para la ejecución del servicio web se debe tener instalado el

programa Python 3.0 el cual es un lenguaje de alto nivel interpretado. Se deben tener instaladas las librerías necesarias para la ejecución del sistema, mismas que vienen ya definidas en el archivo de requerimientos en la carpeta del programa. Finalmente se debe tener instalado un buscador como Google Chrome, Mozilla, Firefox, Microsoft Edge, entre otros. Al ejecutar el programa este se encargará de realizar la gestión necesaria con la base de datos, con el servicio web y el gestor de escaneos.

6.11. Descripción de programas

Para el desarrollo e implementación de la aplicación web planteada se utilizó un conjunto de librerías y herramientas que integradas entre si permitieron la creación de un sistema de escaneo de vulnerabilidades para dispositivos IoT que se encuentren en la red LAN de quien lo utilice. Este sistema integra base de datos, sistema de autenticación, servicio web y su propio sistema de escaneo de vulnerabilidades creando así un ecosistema con diversos elementos individuales pero funcionando en conjunto.

6.11.1. Tecnologías de desarrollo a utilizar

Las principales herramientas utilizadas para el desarrollo de la aplicación web:

- **Python**: De acuerdo con un artículo publicado en la página de Oracle: “Python es un lenguaje de programación orientado a objetos de alto nivel y fácil de interpretar con una sintaxis fácil de leer. Python, ideal para prototipos y tareas ad hoc, tiene un amplio uso en la informática científica, el desarrollo web y la automatización. Como lenguaje de programación para principiantes y con fines generales, Python admite muchos de los mejores científicos de computadoras y desarrolladores de aplicaciones a nivel global.” (Oracle, n.d.)

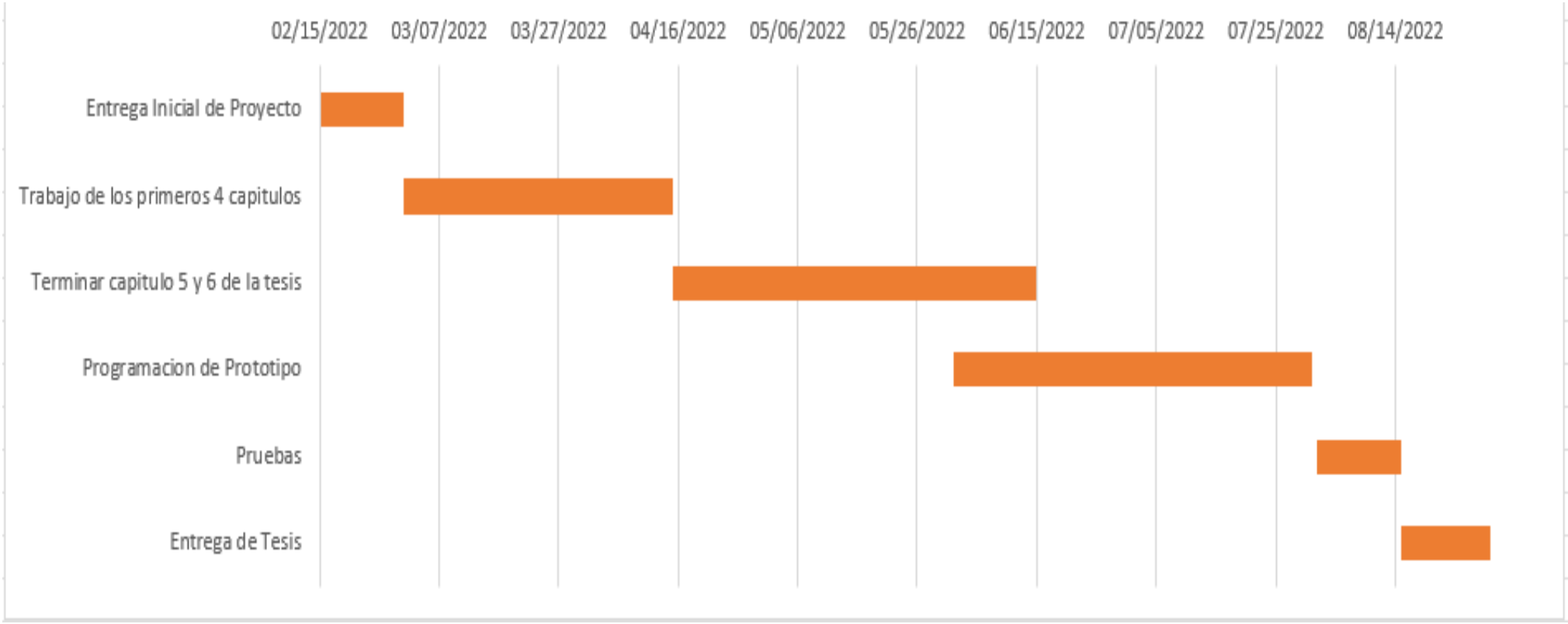
- **HTML:** De acuerdo con el post publicado en la página “Desarrollo web”: “HTML es el lenguaje con el que se define el contenido de las páginas web. Básicamente se trata de un conjunto de etiquetas que sirven para definir el texto y otros elementos que compondrán una página web, como imágenes, listas, vídeos, etc.” (desarrolloweb, 2001)

- **JavaScript:** Podemos decir que JavaScript es uno de los lenguajes de programaciones que permiten adjuntar funciones a páginas web, dándole dinamismo a cualquier página hecha con simple HTML.

- **SQLite:** De acuerdo con el portal HostgatorMX, SQLite puede ser definido de la siguiente manera: **“**SQLite es una de las bases de datos relacionales más conocidas. Básicamente, funciona como un servidor propio e independiente, ya que el Sistema de Gerencia de Base de Datos o SGBD, se puede ejecutar en la misma instancia, eliminando así las consultas y procesos separados.” (HostgatorMX, n.d.)

6.12. Cronograma

Figura 18. Cronograma de actividades



Conclusiones Finales

La seguridad de la información al igual que los dispositivos de Internet de las cosas son temas que ha estado en tendencia ya desde hace varios años. Principalmente el sector IoT ha sido de bastante preocupación en el entorno de la seguridad de la información debido a que estos representan un porcentaje cada vez mayor en las empresas pero el nivel de conocimiento sobre estos y de robustez de sus sistemas operativos no se han visto en crecimiento igual de exponencial. Es por esto que se han convertido en uno de los principales vectores de ataque en la actualidad.

Durante la investigación logramos determinar que la utilización de la herramienta propuesta en la prueba de concepto, será un elemento indispensable ya que ayudará al usuario a identificar debilidades dentro de sus configuraciones de dispositivos del internet de las cosas, le brindará ayuda para mantener un control del nivel de seguridad de sus sistemas y le permitirá tener una infraestructura robusta y segura contra los cibercriminales.

Referencias Web

¿Qué es JavaScript? - Aprende sobre desarrollo web | MDN. (2022, 3 junio). Mozilla.Org. https://developer.mozilla.org/es/docs/Learn/JavaScript/First_steps/What_is_JavaScript

¿Qué es Python? (s. f.). Oracle Developer. https://developer.oracle.com/es/python/what-is-python/

A03 injection - OWASP top 10:2021. (2021). OWASP Top 10. https://owasp.org/Top10/A03_2021-Injection/

Access control vulnerabilities and privilege escalation | web security academy. (s. f.). Port swigger. https://portswigger.net/web-security/access-control

Alcalde, J. C. (s. f.). *Modelo Canvas*. Economipedia. https://economipedia.com/definiciones/modelo-canvas.html

Bisson, D. (2021, 15 diciembre). *IoT security: Protecting food and agriculture organizations*. Security Intelligence. https://securityintelligence.com/articles/iot-security-food-agriculture/

Boyden, P. (2021, 11 noviembre). *Cyber threats: IoT security in the healthcare sector - FraudWatch*. Digital Brand Protection – FraudWatch. https://fraudwatch.com/cyber-threats-iot-security-in-the-healthcare-sector/

conceptodefinicion.net. (2021, 7 enero). ☑ Investigación descriptiva, exploratoria y explicativa. Concepto y Definición. https://conceptodefinicion.net/investigacion-descriptiva-exploratoria-y-explicativa/

DETRI - Escuela Politécnica Nacional. (s. f.). *Historia IoT*. https://detri.epn.edu.ec/historia-iot/

El origen del IoT. (2017, 16 enero). Bruno Cendón. https://www.bcendon.com/el-origen-del-iot/

Guillem, D. S. (2022, 8 marzo). IoT: una puerta abierta al malware. MuySeguridad. Seguridad informática. https://www.muyseguridad.net/2022/03/08/iot-una-puerta-abierta-al-malware/

I. (2016, 12 agosto). INVESTIGACIÓN EXPLORATIVA. INVEWEB. https://inveweb.wordpress.com/2016/08/12/investigacion-explorativa/

I. (2021, 3 diciembre). IoT Security Statistics: 6 Facts. Intersog. https://intersog.com/blog/iot-security-statistics/

IOT TRANSFORMING THE FUTURE OF AGRICULTURE. (2019, 10 julio). IOT Solutions World Congress | 10–12 MAY 2022 BARCELONA. https://www.iotsworldcongress.com/iot-transforming-the-future-of-agriculture/

Lowing, S., Klepfish, N., Hasson, E., Lynch, B., Hewitt, N., Lynch, B., McKeever, G., & Lynch, B. (2021, 11 febrero). *What is vulnerability assessment | VA tools and best practices | imperva*. Imperva. https://www.imperva.com/learn/application-security/vulnerability-assessment/

O. (2021, 28 marzo). *GitHub - OWASP/IoT-Security-Verification-Standard-ISVS: OWASP IoT security verification standard (ISVS)*. GitHub. https://github.com/OWASP/IoT-Security-Verification-Standard-ISVS

Oddy, C. (2021, 20 diciembre). *What are IoT devices? Everything you need to know*. KO2 Recruitment. https://www.ko2.co.uk/what-are-iot-devices/

Oh, J., Lowing, S., Klepfish, N., Hasson, E., Lynch, B., Hewitt, N., Lynch, B., & McKeever, G. (2021, 1 diciembre). *What is OWASP | what are OWASP top 10 vulnerabilities | imperva*. Learning Center. https://www.imperva.com/learn/application-security/owasp-top-10/

OWASP IoT security verification standard | OWASP foundation. (s. f.). OWASP ISVS. https://owasp.org/www-project-iot-security-verification-standard/

Qué es HTML. (2001, 1 enero). Desarrollo Web. https://desarrolloweb.com/articulos/que-es-html.html

Santos, P. R. D. L. (2021, 25 junio). Breve historia de Internet de las cosas (IoT) - Think Big Empresas. Think Big. https://empresas.blogthinkbig.com/breve-historia-de-internet-de-las-cosas-iot/

Seals, T. (2021, 3 septiembre). IoT Attacks Skyrocket, Doubling in 6 Months. Threatpost. https://threatpost.com/iot-attacks-doubling/169224/

SQLite: qué es, cómo funciona y cuál es la diferencia con MySQL. (s. f.). HostgatorMX. https://www.hostgator.mx/blog/sqlite-que-es-y-diferencias-con-mysql/

Tamayo y Tamayo. (2003) El Proceso de la Investigación Científica. Limusa Noriega Editores. 4ta. Edición. México.

The 9 most important applications of the internet of things (IoT). (2019, 24 agosto). Fracttal USA. https://www.fracttal.com/en/blog/the-9-most-important-applications-of-the-internet-of-things

Wegner, P. (2022, 30 marzo). Global IoT market size grew 22% in 2021 — these 16 factors affect the growth trajectory to 2027. IoT Analytics. https://iot-analytics.com/iot-market-size/

Westreicher, G. (2021, 13 abril). *Retorno de la inversión (ROI)*. Economipedia. https://economipedia.com/definiciones/retorno-de-la-inversion-roi.html

What is and how to prevent broken access control | OWASP top 10. (s. f.). HDiv Security. https://hdivsecurity.com/owasp-broken-access-control

What is OWASP? | cloudflare. (s. f.). Cloudflare. https://www.cloudflare.com/learning/security/threats/owasp-top-10/

Referencias Bibliograficas

Hernández, S. y otros (2006): Metodología de la Investigación. México: McGraw Hill.

Jorge Cáceres Urgate (1996) Libro metodología Investigación Cuantitativos

Sabino, Carlos (2007). El Proceso de Investigación. Editorial Panapo. Caracas.

Tomás García (2003): EL CUESTIONARIO COMO INSTRUMENTO DE INVESTIGACIÓN/EVALUACIÓN.

Apéndices

Apéndice a – Preguntas de la encuesta

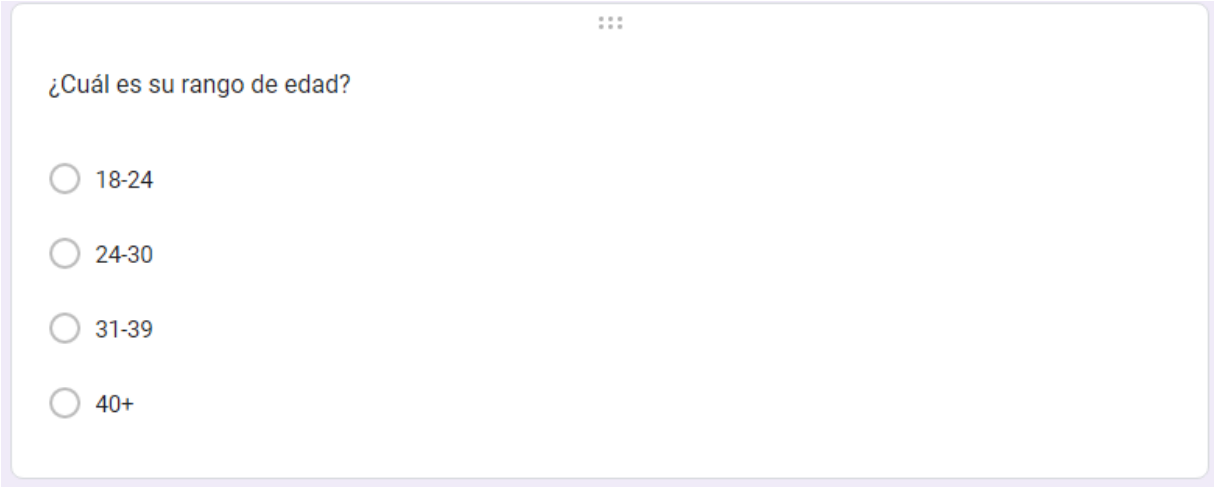


Figura 19: Pregunta 1 de la encuesta.

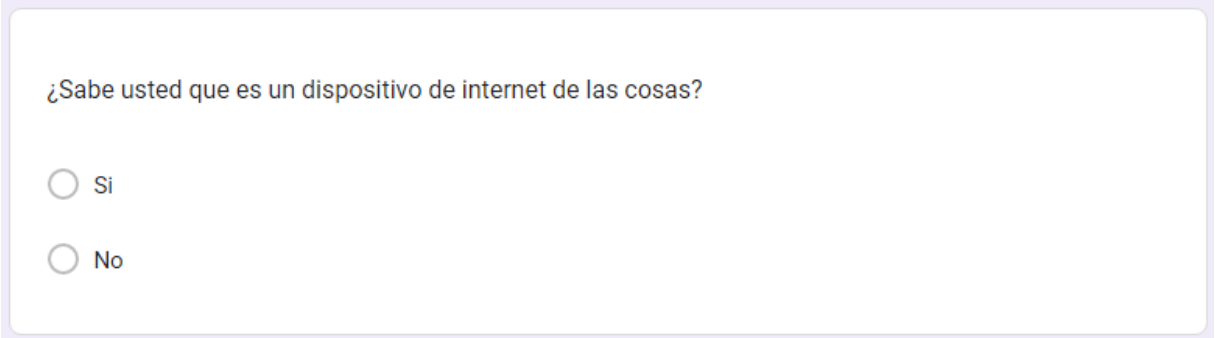


Figura 20: Pregunta 2 de la encuesta.

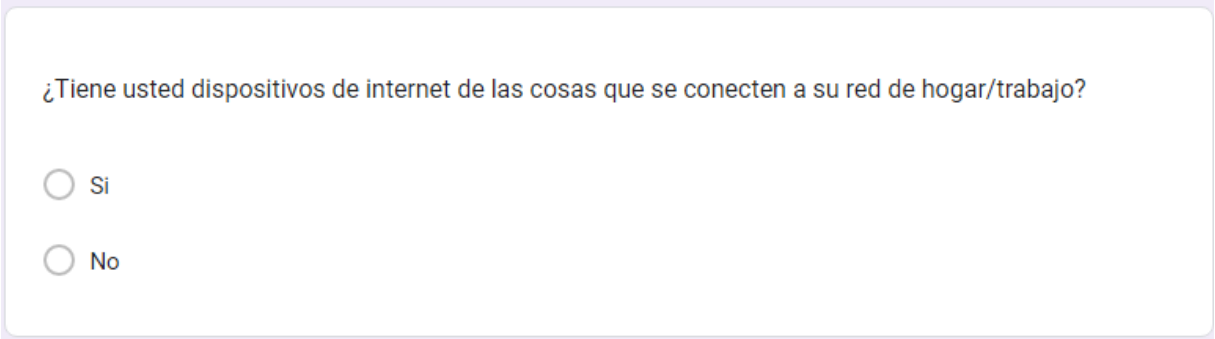


Figura 21: Pregunta 3 de la encuesta.

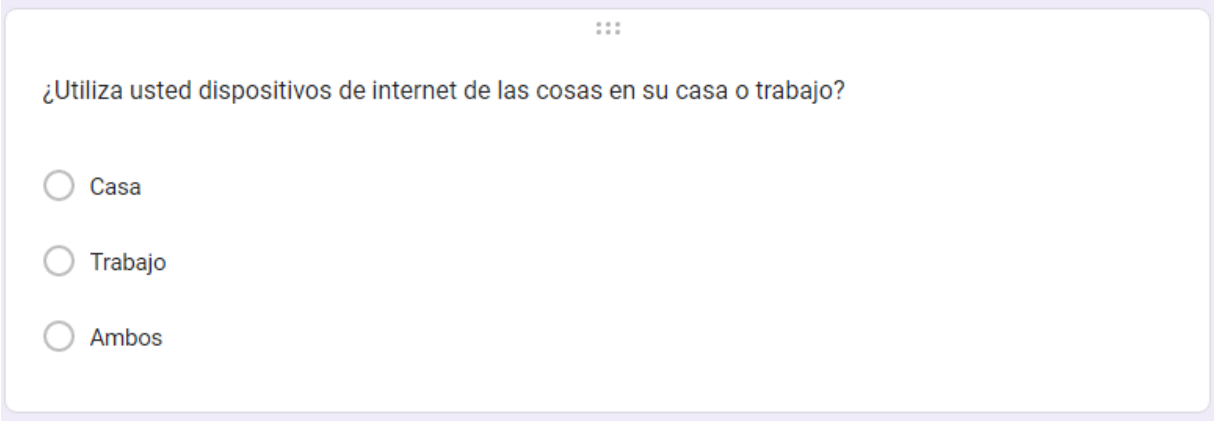


Figura 22: Pregunta 4 de la encuesta.

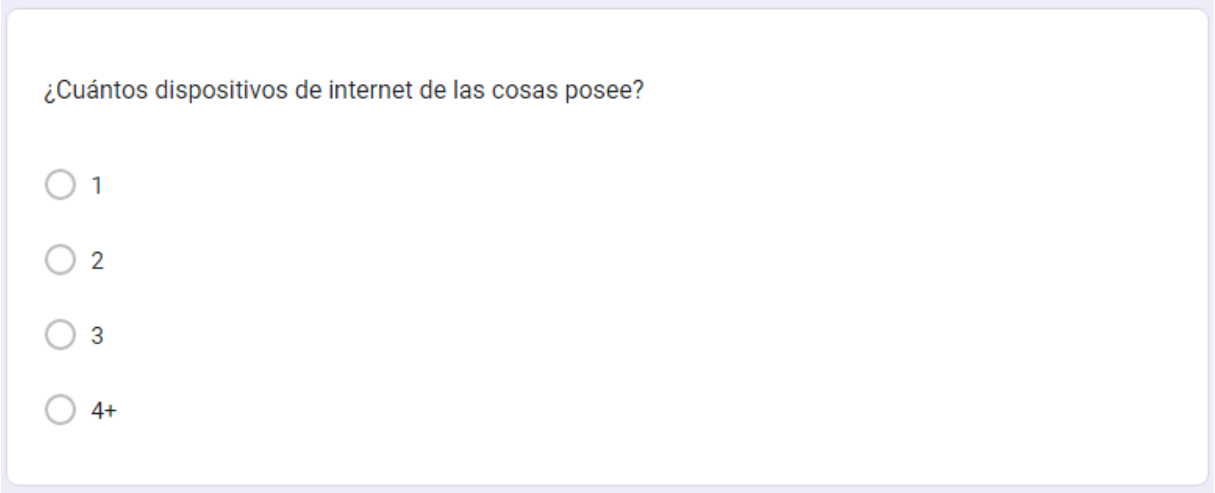


Figura 23: Pregunta 5 de la encuesta.

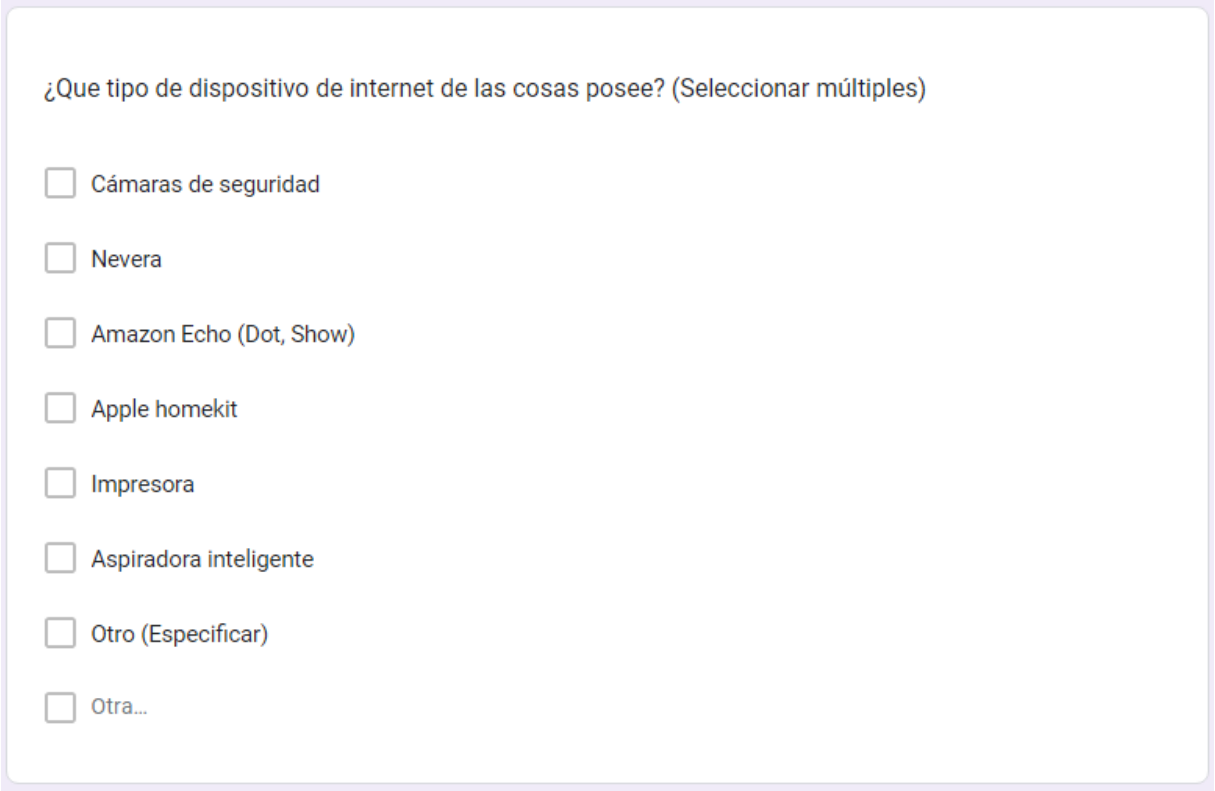


Figura 24: Pregunta 6 de la encuesta.

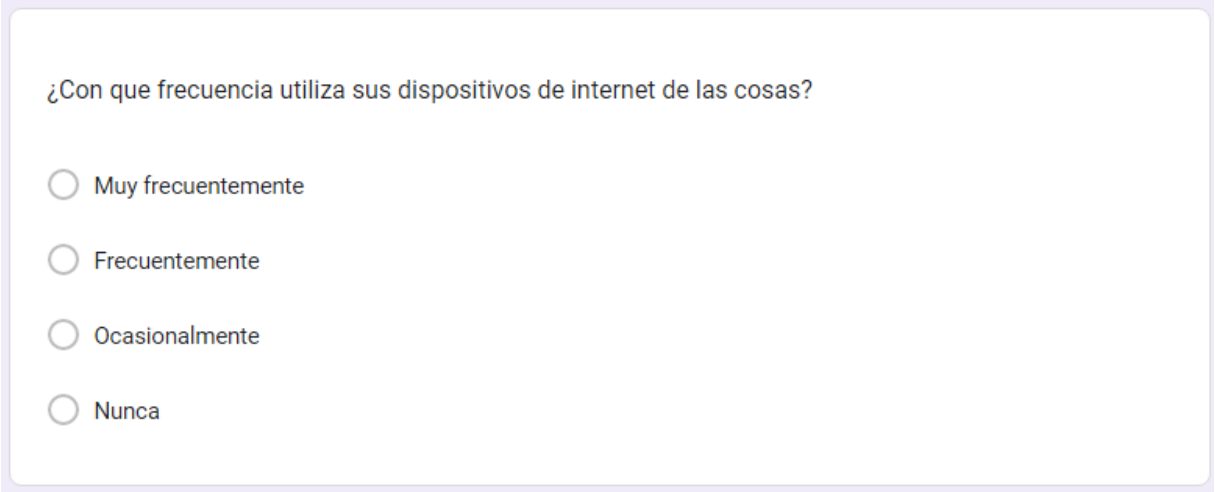


Figura 25: Pregunta 7 de la encuesta.

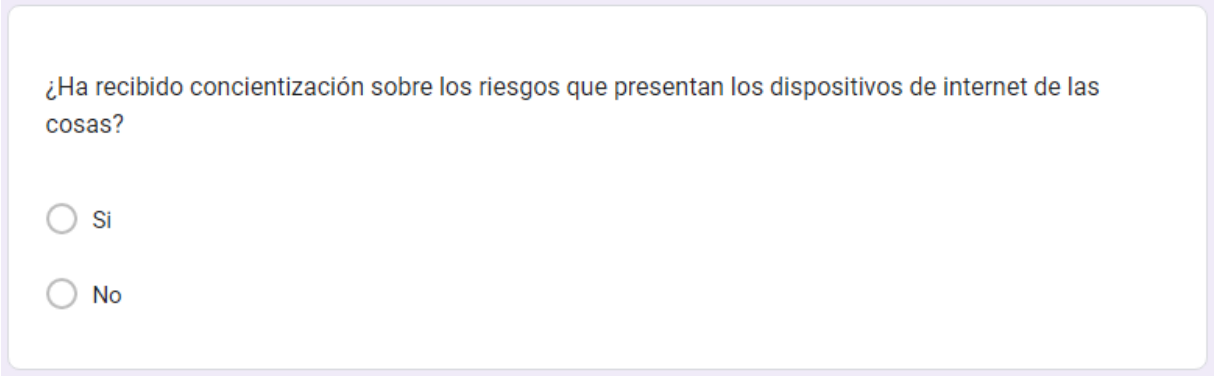


Figura 26: Pregunta 8 de la encuesta.

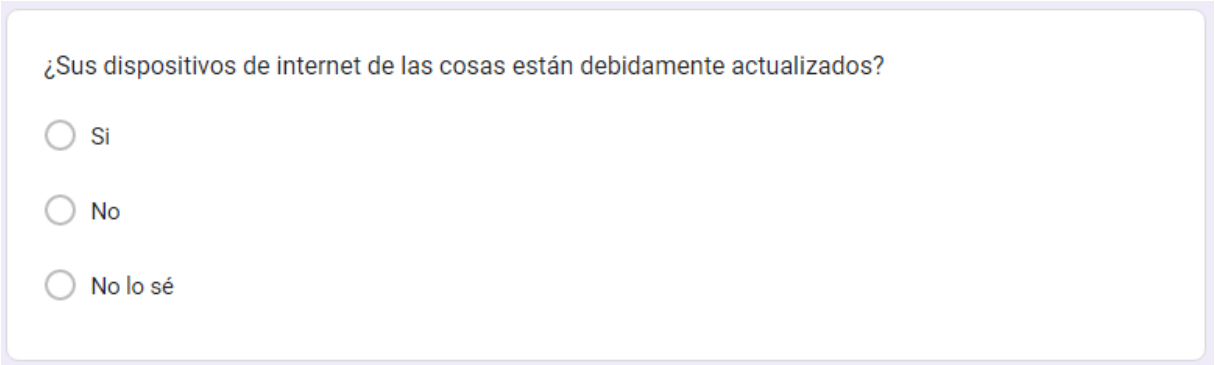


Figura 27: Pregunta 9 de la encuesta.

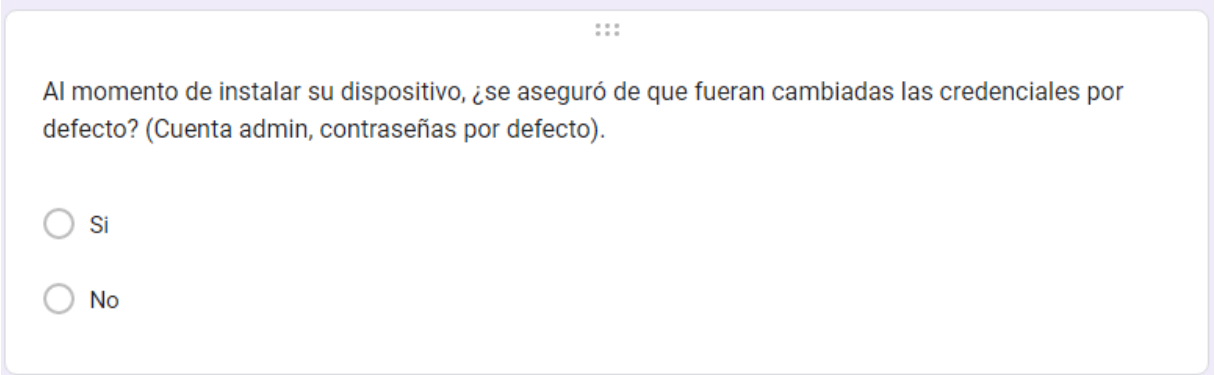


Figura 28: Pregunta 10 de la encuesta.

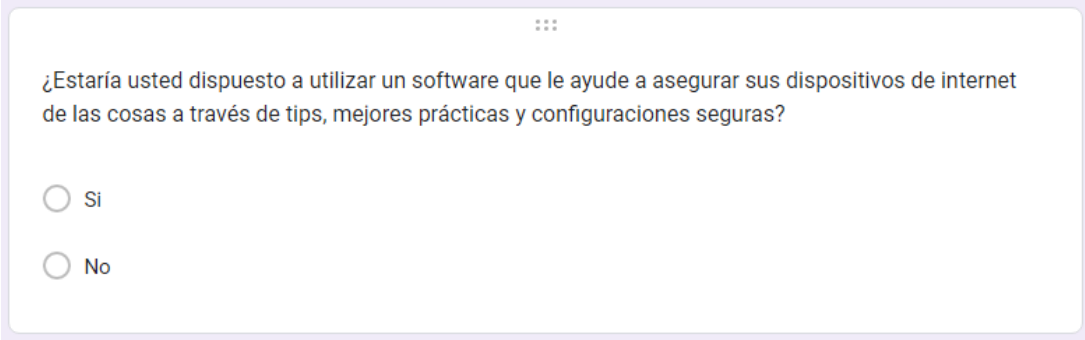


Figura 29: Pregunta 11 de la encuesta.

Apéndice b – Respuestas de la encuesta

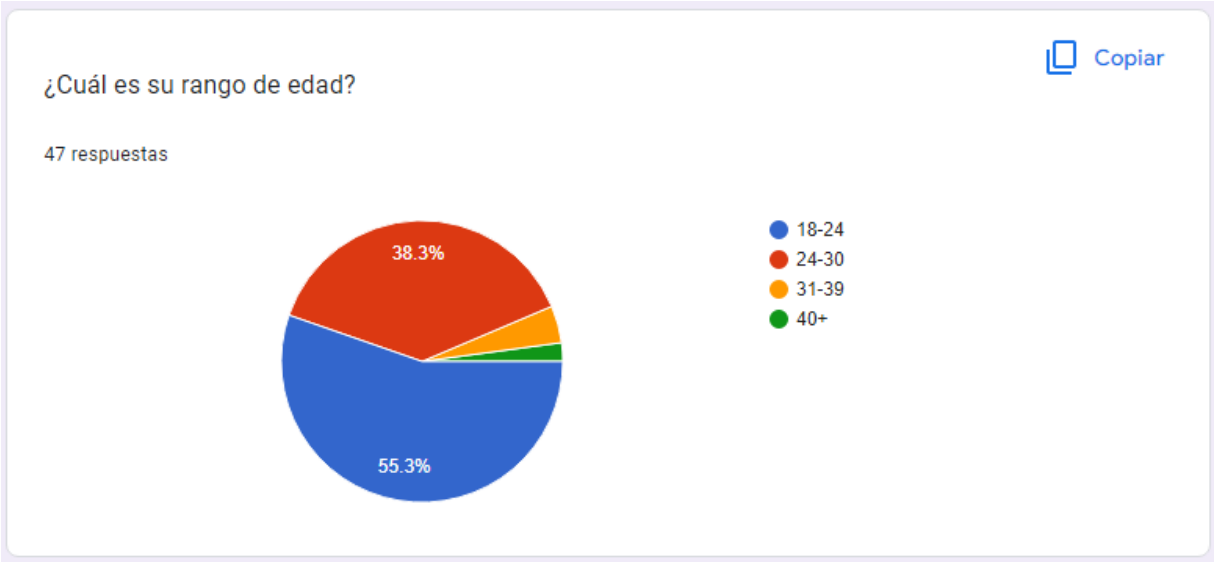


Figura 30: Respuestas de la pregunta 1.

Figura 31: Respuestas de la pregunta 2.

Figura 32: Respuestas de la pregunta 3.

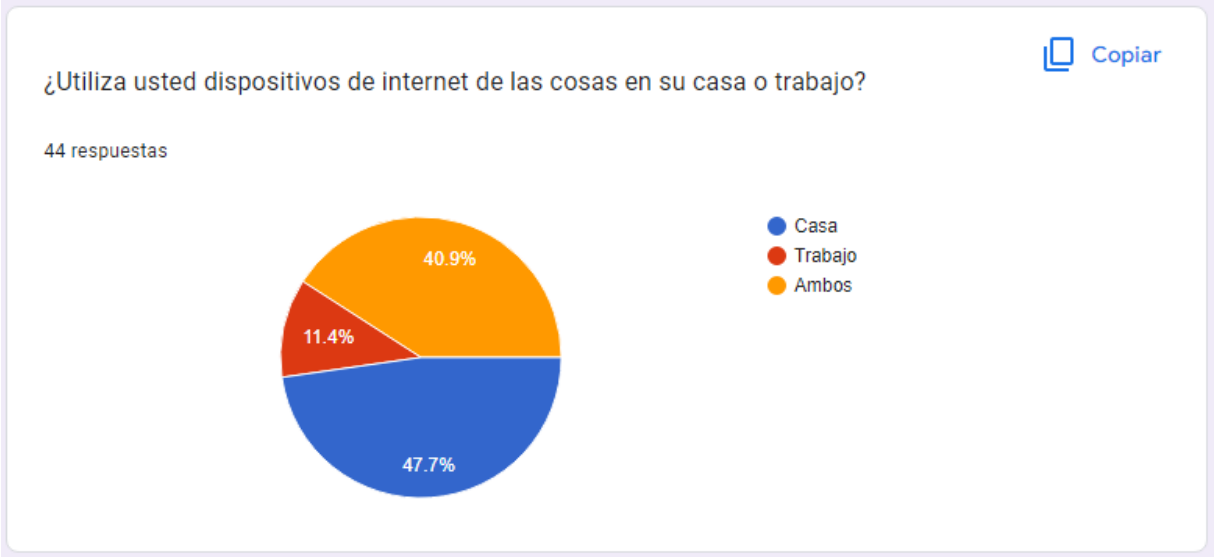


Figura 33: Respuestas de la pregunta 4.

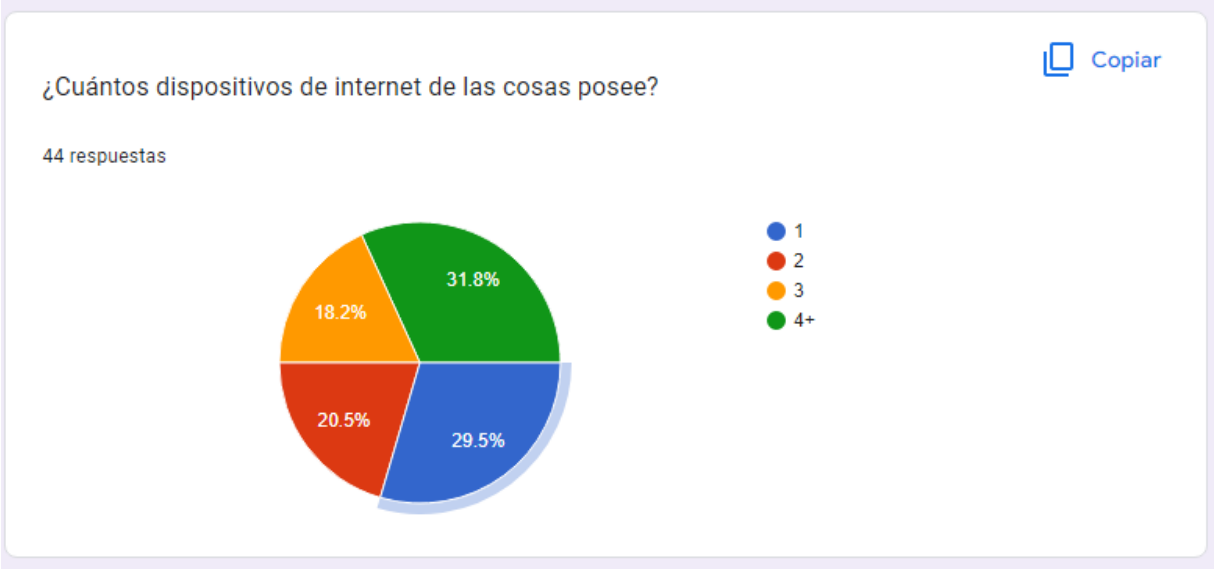


Figura 34: Respuestas de la pregunta 5.

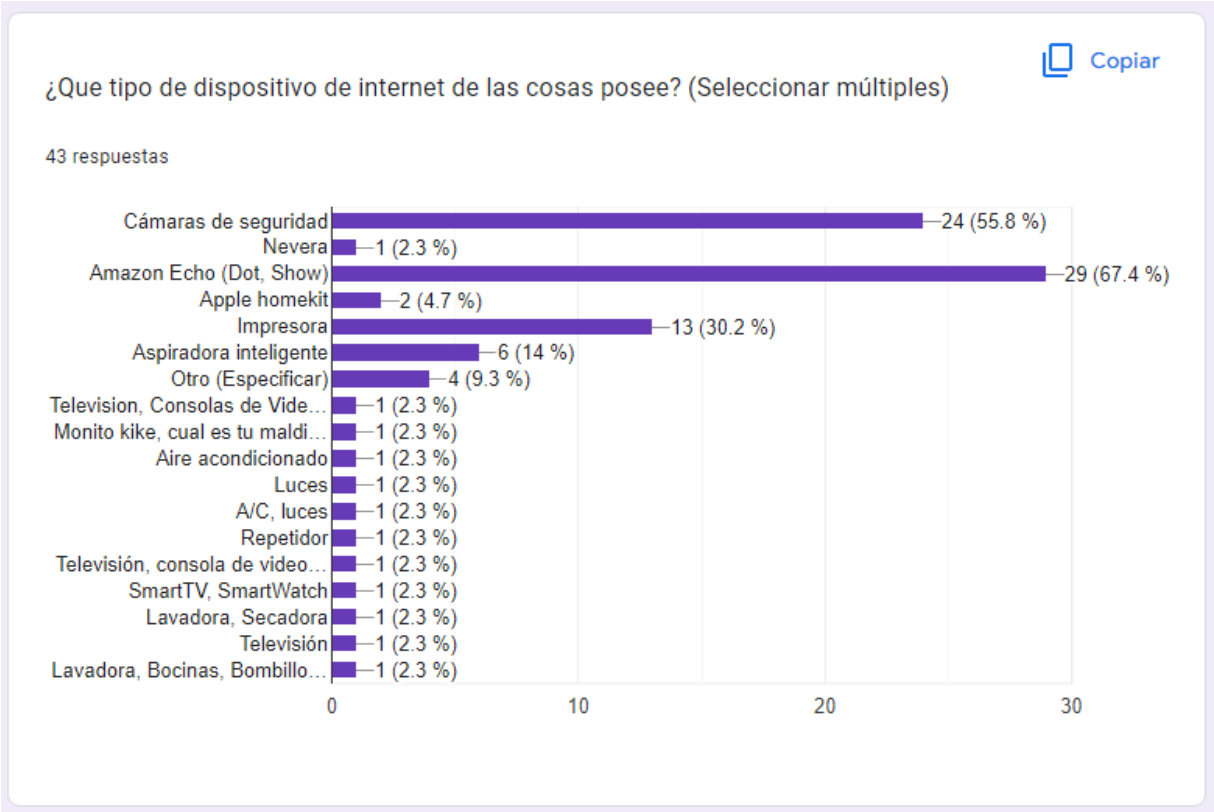


Figura 35: Respuestas de la pregunta 6.

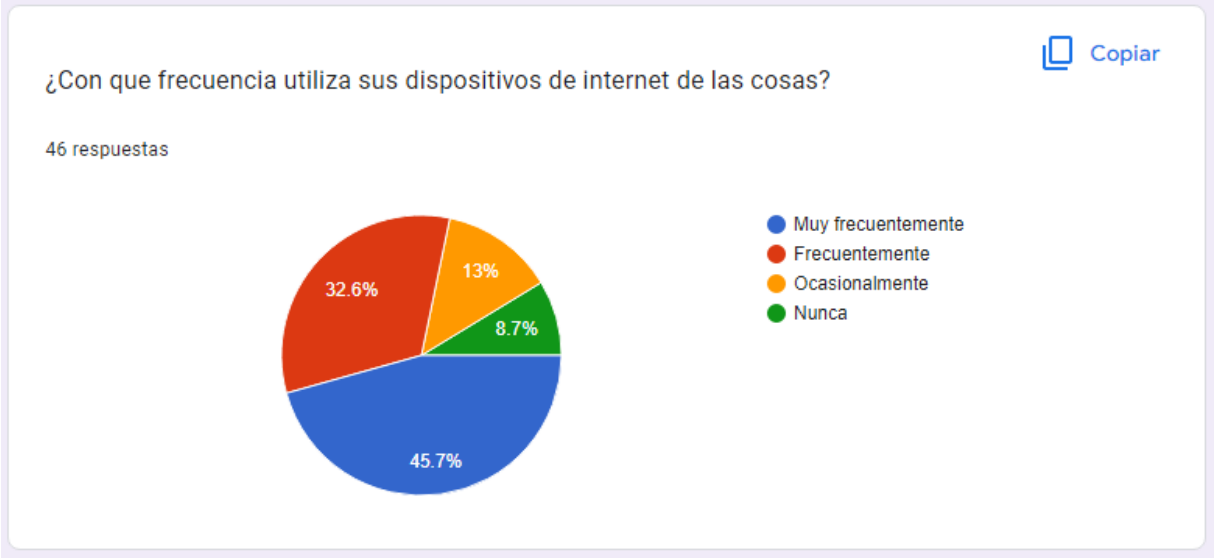


Figura 36: Respuestas de la pregunta 7.

Figura 37: Respuestas de la pregunta 8.

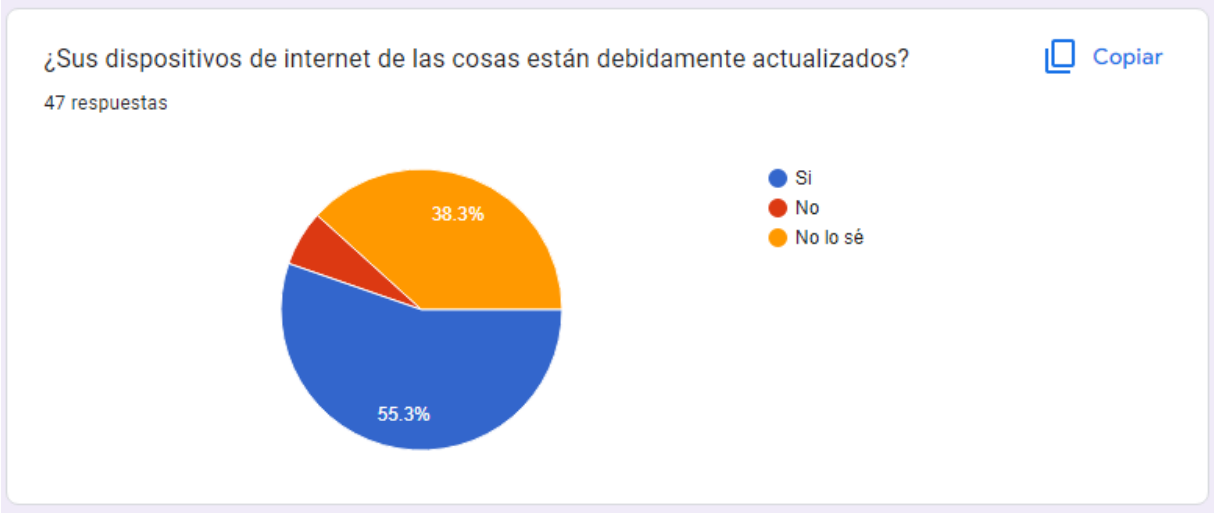


Figura 38: Respuestas de la pregunta 9.

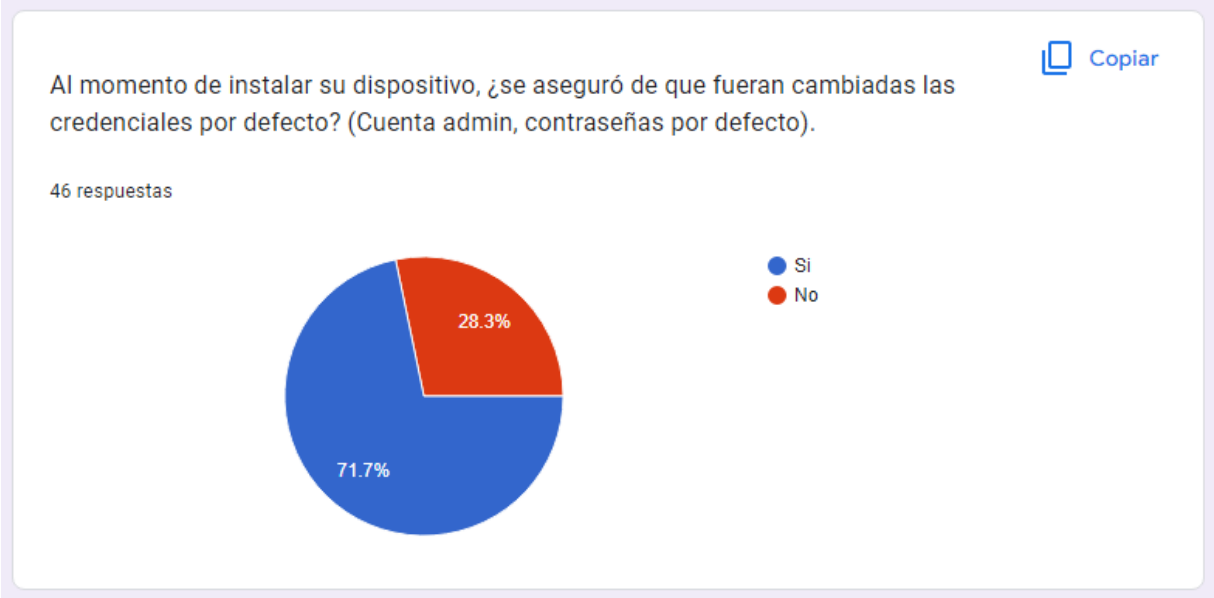


Figura 39: Respuestas de la pregunta 10.

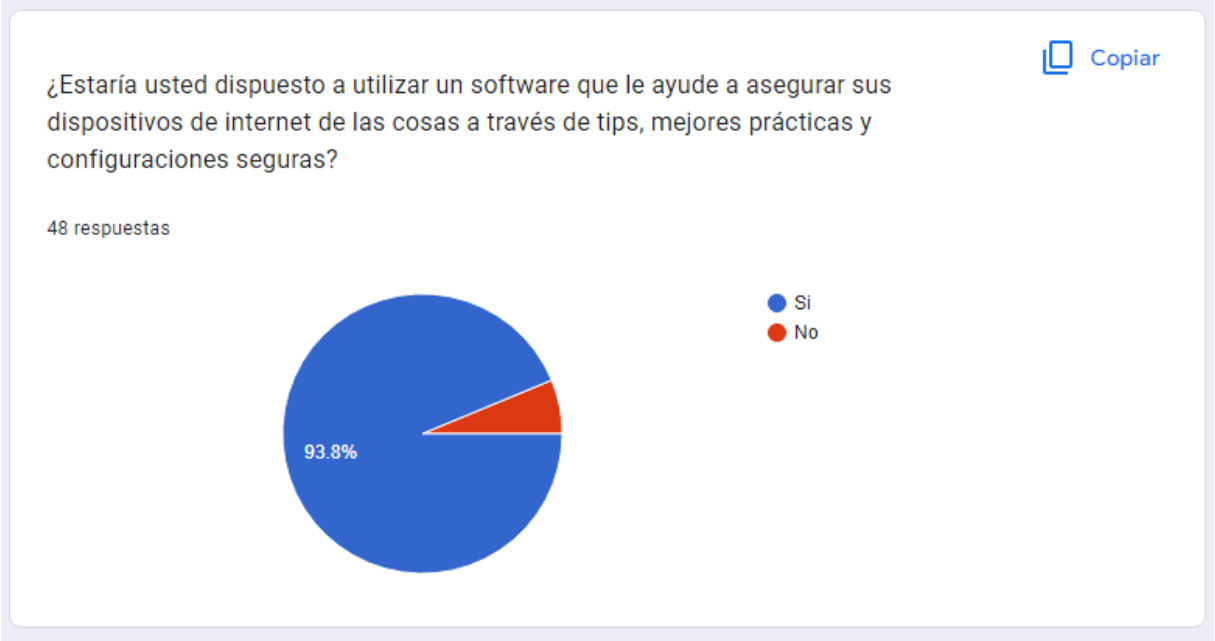


Figura 40: Respuestas de la pregunta 11.

Vita

Randy Raúl Mata Olmos nacido el 9 de junio de 1999 en la ciudad de Santo Domingo. Hijo de Randy Mata Acosta y Elisa Mercedes Olmos. Graduado del título de Técnico en Ciberseguridad en el Instituto Tecnológico de las Américas (ITLA), a la fecha estudiante de la carrera de Ingeniería en Tecnología de la Información y Comunicación en la Universidad Iberoamericana UNIBE.

Desde el año 2019 hasta la fecha labora en el Banco Popular Dominicano desempeñando la función de Líder de monitoreo de Ciberseguridad.

Randy Raúl Mata Olmos

Vita

Arturo De Jesús Peña nacido en el 1998, en la ciudad de Santo Domingo, hijo de Lenin De Jesus Machuca y Helen Yeceny Peña Guzmán, graduado del Instituto Tecnológico de las Américas como Tecnólogo en Seguridad Informática. Actualmente es estudiante de término de la Ingeniería en Tecnología de la Información y Comunicación en la Universidad Iberoamericana (UNIBE).

Certificado de Comptia Security+ (SY0-601), ha cursado varios diplomados, cursos técnicos y capacitaciones durante su tiempo como estudiante. Actualmente labora en el Banco Popular Dominicano en el Área de Seguridad de la Información.

Arturo De Jesús Peña