UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE CUENCA

CARRERA DE COMPUTACIÓN

Trabajo de titulación previo a la obtención del título de Ingeniera en Ciencias de la Computación

ARTÍCULO ACADÉMICO:

"DISEÑO DE UN FRAMEWORK PARA LA SEGURIDAD Y PRIVACIDAD EN LA IMPLEMENTACIÓN DE SERVICIO DE PAQUETERÍA MEDIANTE DRONES PARA EL COMERCIO ELECTRÓNICO EN EL ECUADOR"

AUTORA:

TATIANA DOMÉNICA CÁRDENAS JHO

TUTORA:

ING. JENNIFER ANDREA YÉPEZ ALULEMA, MSc.

CUENCA - ECUADOR

2021

CESIÓN DE DERECHOS DE AUTOR

Yo, Tatiana Doménica Cárdenas Jho con documento de identificación N° 0503206377, manifiesto mi voluntad y cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autora del trabajo de titulación: **"DISEÑO DE UN FRAMEWORK PARA LA SEGURIDAD Y PRIVACIDAD EN LA IMPLEMENTACIÓN DE SERVICIO DE PAQUETERÍA MEDIANTE DRONES PARA EL COMERCIO ELECTRÓNICO EN EL ECUADOR"**, mismo que ha sido desarrollado para optar por el título de: *Ingeniera en Ciencias de la Computación*, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en mi condición de autora me reservo los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hago entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Cuenca, octubre de 2021.

Tatiana Doménica Cárdenas Jho

C.I. 0503206377

CERTIFICACIÓN

Yo, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: **"DISEÑO DE UN FRAMEWORK PARA LA SEGURIDAD Y PRIVACIDAD EN LA IMPLEMENTACIÓN DE SERVICIO DE PAQUETERÍA MEDIANTE DRONES PARA EL COMERCIO ELECTRÓNICO EN EL ECUADOR"**, realizado por Tatiana Doménica Cárdenas Jho, obteniendo el *Artículo Académico*, que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana.

Cuenca, octubre de 2021.

Jennifer Andrea Yépez Alulema, MSc.

C.I. 0104207238

DECLARATORIA DE RESPONSABILIDAD

Yo, Tatiana Doménica Cárdenas Jho con documento de identificación: N° 0503206377, autora del trabajo de titulación: **"DISEÑO DE UN FRAMEWORK PARA LA SEGURIDAD Y PRIVACIDAD EN LA IMPLEMENTACIÓN DE SERVICIO DE PAQUETERÍA MEDIANTE DRONES PARA EL COMERCIO ELECTRÓNICO EN EL ECUADOR"**, certifico que el total contenido del *Artículo Académico*, es de mi exclusiva responsabilidad y autoría**.**

Cuenca, octubre del 2021.

Tatiana Doménica Cárdenas Jho

C.I. 0503206377

Resumen

Como resultado del alcance de la transformación digital y el notable crecimiento del comercio electrónico y tras el auge de distintos factores y acontecimientos que vivimos en la actualidad como la crisis sanitaria del COVID-19, se evidencia un notable impacto en el flujo creciente de consumidores y cantidad de pedidos u órdenes de compra. De tal manera que, industrias, empresas, microempresas, PYMEs y/o minoristas electrónicos requieren de soluciones de servicios innovadoras, a menudo impulsadas por avances tecnológicos, para mejorar la gestión de la experiencia del cliente y de igual manera, ayudar a la toma de decisiones gerenciales al diseñar nuevos servicios de paquetería para el comercio electrónico.

La automatización del servicio de paquetería de productos es una tendencia que se percibe con más frecuencia en forma de Vehículos Aéreos no tripulados, también conocido como drones. En Latinoamérica, la presencia de drones para transportar pedidos a domicilio es una realidad que podría concretarse a mediano plazo, ya que aún está en proceso de adaptación, entre los cuales se encuentran países como Colombia, Brasil y Perú. Por otra parte, en Ecuador en el año de 2020 se estrenó un plan piloto para las entregas con drones desde el centro de Quito hasta los suburbios de la capital, según declara Espinoza (2020) en el diario Expreso.

Un Framework que defina delineamientos de seguridad y privacidad para el potencial uso de drones como servicio de paquetería, aplicando como caso de estudio el sector farmacéutico en el comercio electrónico de la ciudad de Cuenca, permitirá a los distintos sectores económicos del país contar con una guía que les facilitará la implementación de un nuevo mecanismo de tecnología innovadora de transporte aéreo. Además, ayudará a estos negocios a alinear y priorizar sus actividades de seguridad con sus requisitos empresariales o de misión, tolerancias de riesgos y recursos en cuanto al servicio de entrega de sus productos, ya que el Framework presenta leyes que las empresas deben cumplir con respecto a la protección de datos y/o información de sus consumidores.

Palabras clave: Servicio de paquetería, seguridad y privacidad de datos, dron, comercio electrónico, Framework, UAV.

Abstract

The era of digital transformation, the growth of e-commerce and the rise of several factors and events that society has been experiencing through the COVID-19 sanitary crisis have caused a notable impact on the increasing number of consumers and purchase orders. Thus, industries, enterprises, microenterprises, SMEs and electronic retailers require service solutions to improve customer experience. Technological advances can usually drive these innovations. Also, it could be necessary to help managerial decision-making when those businesses are designing new packing services for e-commerce.

Product delivery automation is a trend perceived more frequently in UAV, also known as drones. In Latin America, although delivery services through drones are a reality, it is still in an adaptation process in the medium term among countries like Colombia, Brazil and Peru. Contrarily, according to Espinoza (2020) in the newspaper Expreso, in Ecuador, in 2020, a delivery service with a drone was launched as a pilot plan, from the Quito centre to the capital's suburbs.

The Security and Privacy Framework presents guidelines for the potential use of drones as a packaging and delivery service, applied as a study case of e-commerce in the pharmaceutical sector in the city of Cuenca. This Framework will allow different economic sectors of the country to have a guide that will facilitate the implementation of a new innovative air transport technology mechanism. It is necessary to consider that these sectors are currently carrying out their deliveries by land transportation, consuming large amounts of fuel, negatively impacting the environment. In addition, the Framework presents laws that companies must comply with concerning the protection of data and information of its consumers. Therefore, it will help businesses align and prioritise their security activities with their business or mission requirements, risk tolerances, and resources regarding service delivery of their products.

Keywords: Delivery, data security and privacy, drone, e-commerce, Framework, UAV.

Índice de contenido

1. Revisión de literatura.

Tras el creciente uso de internet, el advenimiento de nuevas tecnologías y el desarrollo de las Tecnologías de la Información y Comunicación (TIC), han posibilitado la generación de métodos innovadores para la comercialización de productos y servicios, posibilitando a varias empresas a solventar barreras geográficas y de tiempo. El comercio electrónico es el resultado natural de esta situación, ofreciendo diversos "beneficios para las empresas, consumidores, la sociedad y para la economía de un país, ya que permite reducir costos y tiempos de operaciones, fomenta la producción con valor agregado y genera fuentes de empleo" (SGCAN & Caicedo, 2021). Además, permite una prevalencia de la logística sobre las fronteras.

Frente a esta situación, es evidente la necesidad de adquirir destrezas digitales para el uso del e-commerce, sin embargo, de acuerdo con el análisis del Ministerio de Producción, Comercio Exterior, Inversiones y Pesca (MPCEIP) y, el Ministerio de Telecomunicaciones y Sociedad de la Información (2021), en el Ecuador se ha diagnosticado que "existe una notable brecha digital con relación a los países de la región y el mundo, lo que representa una desventaja competitiva en este nuevo escenario comercial"(p. 4).

La SGCAN (2021), acredita este diagnóstico tras un estudio realizado entre los países que conforman la Comunidad Andina (CAN), indicando que el porcentaje de utilización de herramientas digitales en el sector productivo para la adquisición de insumos es bajo en la región andina (igual o menor al 37%); Ecuador presenta un porcentaje de 13,90%. El porcentaje de empresas que usan banca electrónica con excepción de Colombia (con el 95.4%), es inferior al 47% en los demás países de la CAN, de tal manera que Ecuador se considera dentro de ese porcentaje.

En la Estrategia Nacional de Comercio Electrónico 2021, se indica que "durante el estado de emergencia sanitaria causado por la propagación mundial del virus del COVID-19, se ha impulsado el comercio electrónico y la transformación digital en gran escala a nivel global" (Ministerio de Telecomunicaciones y Sociedad de la Información et al., 2021, p. 6). En relación con la problemática expuesta y el aumento de contagios de manera exponencial en varias partes del mundo, se ha forzado a los consumidores a efectuar sus compras habituales a través de transacciones electrónicas. Por consecuente, el e-commerce se posiciona en un sector privilegiado, aun cuando continúa en un proceso evolutivo de desarrollo y madurez debido al surgimiento y transformación de las necesidades de las empresas con la finalidad de conocer a los potenciales consumidores y satisfacer sus necesidades.

En la presentación de la Estrategia Nacional de Comercio Electrónico (ENCE), efectuada el 11 de marzo del 2021, se señala que, a través de una investigación del análisis de oferta y demanda con relación a las compras por internet, elaborada por la Universidad de Especialidades Espíritu Santo y la Cámara Ecuatoriana de Comercio Electrónico, "en el Ecuador, las compras por canales digitales, incluidos sitios web, se han incrementado al menos en 15 veces desde el inicio del distanciamiento social". Además, el auge del SARS-CoV-2 generó una oportunidad de apertura del e-commerce, impulsando a un "34% de los usuarios de plataformas digitales como medios de compra, a usar estas plataformas de manera frecuente" (Ministerio de Telecomunicaciones y Sociedad de la Información et al., 2021, p. 6).

Así mismo, en la investigación realizada por la Gerente de E-Commerce y Logística de De Prati, Jessica Dávila (2021), se presenta un aumento en la frecuencia de compra pre y post COVID-19, de tal manera que de 2 a 3 veces por semana aumentó 9%; una vez por semana aumentó 9% del 6%; una vez por semana aumento 13% del 13%; cada 15 días aumentó 7% del 10% anterior. Finalmente, una vez al mes tuvo un crecimiento del 21% frente a un 19% que se presentaba pre-pandemia con una presencial total en cuanto a compras del 40%.

Es evidente que el comercio electrónico y la transformación digital ha tenido un gran alcance durante los últimos años y más aún tras la situación sanitaria mundial que estamos viviendo actualmente; no obstante, a medida que el flujo creciente de pedidos de comercio electrónico continúa generando nuevos registros, es necesario aumentar los volúmenes de transporte para poder satisfacer las necesidades del consumidor electrónico y que este transporte sea rápido, eficiente y no genere perdidas para la industria, empresa y/o microempresa que lo requiere.

Vakulenko, Shams, Hellström, y Hjort (2019) consideran en su investigación que "los minoristas electrónicos y los proveedores de servicios de logística buscan soluciones de servicios innovadoras, a menudo impulsadas por avances tecnológicos".

Marcelo Albuja (2021), Gerente FastFarma y Exgerente de Territorio en Uber Eats, en la presentación de la ENCE indica que el futuro para trasporte de paquetería son los drones como servicio de entrega.

El desarrollo de tecnologías autónomos aplicado como servicio de entrega de mercancías, es una tendencia que se percibe con más frecuencia en forma de Vehículos Aéreos no Tripulados (UAV), también conocido como drones, en varios países y algunas ciudades generalmente de Europa, Norteamérica, Centroamérica y China.

Amazon Prime Air, UPS Flight Forward y DHL son algunas de las grandes grandes industrias a nivel mundial que han utilizado el concepto de dron mensajero en sus acciones. Por otro lado, el 1 de noviembre de 2019, la división de entrega de drones de UPS, UPSFF y CVS Pharmacy realizaron las primeras entregas comerciales de drones residenciales de medicamentos recetados en los Estados Unidos (Tabatabai, 2020). Para el vuelo inaugural, los farmacéuticos cargaron los drones con medicamentos recetados en una farmacia CVS en Carolina del Norte. Los drones Matternet M2 volaron a residencias cercanas y bajaron lentamente los paquetes al suelo sobre las propiedades. Un operador de drones remoto estaba en espera para intervenir, en caso de ser necesario.

El Fondo de las Naciones Unidas para la Infancia (UNICEF) utilizó drones para enviar vacunas a niños en zonas remotas de Vanuatu. Con esto, se pretende solventar la problemática de la temperatura específica para garantizar la eficacia de vacunas y el trasporte ágil y rápido. De tal manera que, "cada dron lleva una caja de espuma de poliestireno con las vacunas, hielo y sensores electrónicos para monitorear la temperatura en todo momento. Una vez enviados, las enfermeras certificadas los reciben y vacunan a los niños"(Sánchez, 2018).

En Latinoamérica, "recibir pedidos a domicilio a través de drones es una realidad que, si bien aún está en proceso de adaptación, podría concretarse a mediano plazo" (Economía, 2019). Entre los países que han implementado esta tecnología se encuentran Colombia, Brasil y Perú. Por otra parte, en Ecuador en el año de 2020, según declara Espinoza (2020) en el diario Expreso, se estrenó un plan piloto para las entregas con drones que conectará la capital del Ecuador, Quito, con varios clientes que habitan en zonas periféricas de la ciudad como Cumbayá, Tumbaco, el Valle de los Chillos o Pomasqui.

Hoy en día, los servicios de entrega de mercancía en el Ecuador realizan esta actividad por medio de transporte terrestre, aéreo y marítimo, "consumiendo un alto índice de combustible en transportación y distribución de mercadería, generando un incremento en la deterioración medio ambiental, tráficos por carretera, dificultad de entrega en zonas menos accesibles y accidentes" (Luzuriaga, 2017, p. 14). La situación descrita sigue en ascenso, ya que perjudica la satisfacción al cliente por la larga espera en recibir su pedido.

Melissa Luzuriaga (2017), en su investigación acerca del "Análisis del uso de drones en los servicios de entrega dentro de la ciudad de Guayaquil", señala que la entrega de productos a domicilio mediante drones resultaría idónea, ya que puede acortar los tiempos de espera, dentro de los 30 minutos a partir de las solicitudes de los clientes en línea; por ende, mantener

las garantías de tiempo de entrega, lo cual suele ser un factor clave en este servicio y podría resultar esencial para el éxito de este modelo de negocio (Lotz, 2015).

Mediante la situación descrita y el uso de impulsores de negocios en el Ecuador, el Framework es una metodología con un enfoque para reducir el riesgo vinculado a las amenazas de seguridad y privacidad que puede comprometer con la información e integridad física de los drones, en el escenario de servicio de paquetería en el comercio electrónico del sector farmacéutico en la ciudad de Cuenca. Permitiendo a estos negocios, alinear y priorizar sus actividades de seguridad con sus requisitos empresariales o de misión, tolerancias de riesgos y recursos en cuanto al servicio de entrega de sus productos.

De igual manera, el Framework permitirá a los distintos sectores económicos del país entre los cuales se encuentran: alimentos, correos, belleza, moda, medicina, etc., contar con una guía que les facilitará la implementación de un nuevo mecanismo de transporte de paquetería, puesto que actualmente dichos sectores llevan a cabo sus entregas mediante transporte terrestre consumiendo grandes cantidades de combustibles fósiles, lo cual genera un impacto negativo en el medioambiente.

Considerando que la implementación de este nuevo servicio de transporte se involucra directamente con la integridad de los datos del consumidor, es importante considerar la perspectiva de Seguridad de la Información, aplicado en los drones para que, a partir de los resultados obtenidos, se logre determinar vulnerabilidades frente a ataques y amenazas de seguridad a los que pueden estar expuestos los drones.

Es por ello por lo que el Framework presenta leyes que las empresas deben cumplir con respecto a la protección de datos y/o información de sus consumidores, apoyando así a las farmacias en la aplicación de medidas preventivas y reactivas para la seguridad de la información, con el fin de proteger la privacidad de los clientes, empleados y terceros. De esta manera, se facilitaría la promoción de un nuevo mecanismo de transporte que proporcione a más de rapidez, seguridad frente a ataques y que resguarde la integridad de la información del consumidor.

2. Metodología.

El proyecto se basó en el desarrollo de seis fases con la ejecución de diferentes actividades que se detallan a continuación:

FASE 1: Estudio de las necesidades del mercado en el sector farmacéutico para la entrega de sus productos.

La ciudad de Cuenca, capital de la provincia del Azuay, se caracteriza por poseer una cultura atípica a comparación del resto del país, principalmente fundamentada en prácticas y costumbres de hace centenares de años que se han mantenido hasta a la actualidad, de tal manera que es importante conocer el comportamiento del consumo de los ciudadanos, para poder realizar una propuesta de valor en todo ámbito.

Las preferencias de las farmacias en la ciudad de Cuenca se adquirieron a través de la aplicación del método subjetivo de la encuesta (Oncins de Frutos, 1991), la misma que se realizó sobre una muestra de 233 farmacias representativas de un colectivo de 319. Cabe indicar que la información de la población de farmacias corresponde al número total de permisos otorgados a farmacias y boticas en la ciudad de Cuenca en el año 2019, los cuales fueron solicitados y entregados por el Control Municipal de la ciudad, disponible a través de la URL: https://github.com/tatcjho/Framework-Ciberseguridad/blob/main/Farmacias/CATASTRO%20FARMACIAS.xls.

Se realizó la encuesta mediante un formulario web que fue distribuido mediante redes sociales y el correo electrónico institucional, con el objetivo de tener un mayor alcance de encuestados ya que por motivo de distanciamiento social provocado por la pandemia mundial, COVID-19, no era recomendable visitar presencialmente las instalaciones de las entidades farmacéuticas.

Además, con la técnica de recolección de información se utilizó la herramienta de preguntas bifurcadas, la cual está basada en respuestas anteriores de la persona que está contestando una encuesta, con la finalidad de no redundar preguntas que al usuario no le competen.

FASE 2: Estudio de los requerimientos técnicos de los drones como servicio de paquetería.

En esta fase se procedió a hacer un análisis de las especificaciones técnicas que deben poseer los UAV para consolidarse como un servicio de paquetería. Para ello, se utilizó

investigación documental, siendo esta "una técnica de investigación cualitativa que se encarga de recopilar y seleccionar información a través de la lectura de documentos, libros, revistas, grabaciones, filmaciones, periódicos, bibliografías, entre otros" (Ortega, 2020).

Los requerimientos técnicos se presentan como parte del Framework, en una tabla donde se indica el nombre de la especificación, descripción y valor que debe cumplir esa especificación con respecto a una condición dada. Para la obtención de la información requerida se trabajó con la investigación de Jung y Kim (2017), denominado "Analysis of Amazon Prime Air UAV Delivery Service".

La empresa estadounidense de comercio electrónico, Amazon, lanzó el proyecto de Prime Air, "un futuro sistema de entrega diseñado para enviar paquetes de manera segura a los clientes en 30 minutos o menos utilizando vehículos aéreos no tripulados" (Welch, 2015). Amazon Air ahora realiza un promedio de 140 vuelos por día y está expandiendo su cantidad, por lo que esta empresa puede entrar a competir con compañías como FedEx y UPS , según informa Palmer (2021).

También, se realizó el análisis del reglamento de advertencia para los propietarios de los Vehículos Aéreos no Tripulados en el Ecuador empleado por la Dirección General de Aviación Civil (2020), el cual aplica en aeronaves "cuyo peso máximo de despegue sea superior a 0,25 kilogramos y menor o igual a 150 kilogramos" (p. 8). Esta información es de importancia y utilidad ya que, el propietario del dron debe seguir y cumplir estas condiciones en caso de que su dispositivo esté dentro de este rango de peso establecido.

Posterior a la obtención de los requerimientos técnicos, se realizó una comparativa entre 8 drones conocidos en el mercado para analizar si estos drones se podrían utilizar como función de delivery.

FASE 3: Análisis y selección de un grupo de drones que pueden ser utilizados en la implementación del servicio de paquetería dentro del sector farmacéutico.

Se seleccionó el grupo de drones a partir de la comparativa realizada en la fase 2, con el objetivo de realizar las pruebas con un dron que satisfaga con todos los requerimientos técnicos y otro, que no presente en su totalidad el cumplimiento de todas las especificaciones.

En el estudio de Organización Médica Colegial de España (2009), se indica que "el peso medio del envase de un medicamento dispensado en farmacia es de 26,8 g. y que contiene de media 49,5 g. de medicamento"; por lo que se realizó las pruebas de requerimientos técnicos

en base a la carga útil que debe presentar el dron para poder transportar el peso mínimo de medicamentos en una farmacia. La carga útil corresponde al peso que puede transportar el dron fuera de su peso originario, es decir, cualquier objeto o artículo adicional al dron, como cámaras, sensores o paquetes adicionales para la entrega (Jackson, 2021).

FASE 4: Ataques y amenazas de seguridad a los que pueden estar expuestos el grupo de drones seleccionados.

Se implementa la revisión bibliográfica basada en la investigación documental para lo cual se definió 3 subsecciones en esta fase:

1. **Espacio de amenaza de seguridad cibernética en UAS:** comprensión del posible espacio de amenazas; de tal manera que, se indica la importancia de que los usuarios de los drones estén bien informados de las capacidades de ataque de sus adversarios.

   Las amenazas pueden ser descubiertas y clasificadas a través de distintas tecnologías y/o métodos, utilizándose la Taxonomía de STRIDE, la cual es un modelo de amenazas implementado para ayudar a considerar e identificar amenazas potenciales a un sistema (Hussain et al., 2014). Además, su objetivo es garantizar que una aplicación cumpla con las directivas de seguridad de la tríada CIA (Confidencialidad, Integridad y Disponibilidad), junto con Autenticación, Autorización y No Repudio.
2. **Escenario de ataque:** identifica los canales centrales que definen los límites de la comunicación con el dron, entre los cuales se encuentran el canal de comunicación entre el dron y el canal de comunicación entre el entorno operativo y el dron.
3. **Descripción de ataques:** detalla brevemente los métodos para implementar un ciberataque en un UAV.

FASE 5: Diseño y desarrollo del Framework con respecto a la seguridad y privacidad de los drones como servicio de paquetería en el comercio electrónico.

El diseño del Framework se fundamenta en el "Marco para la mejora de la seguridad cibernética en infraestructuras críticas" del Instituto Nacional de Estándares y Tecnología (NIST), ya que este documento ofrece una forma flexible de abordar la seguridad cibernética, incluyendo las dimensiones físicas, cibernéticas y de personas (Stine et al., 2014).

Los drones, pueden ofrecer grandes ventajas en cuanto a entregar productos farmacéuticos; por otro lado, los Vehículos Aéreos no Tripulados también promueven problemas de privacidad, por lo que pueden hackearse o utilizarse para atacar otros dispositivos

electrónicos. Es así que, en la sección de delineamientos de protección ante amenazas que establece el Framework, se indican 11 delineamientos que el usuario debe considerar para poder protegerse frente a un ciberataque en el UAV que está utilizando como servicio de paquetería de productos farmacéuticos.

FASE 6: Validación del Framework mediante el grupo selecto de drones

En esta fase se valida el Framework a través del grupo de drones seleccionados en la fase 3, para los cuales, se definió un escenario de pruebas a fin de realizar los respectivos ataques que fueron especificados en la quinta fase.

La validación de Framework contempla la puesta en práctica de los delineamientos de protección en los drones para posteriormente realizar las pruebas de ataques hacia ellos.

Aplicados los delineamientos de protección de los drones, se define el lugar donde se van a aplicar las pruebas de vuelo de los drones. Existen varias aplicaciones a más de DJI, que poseen una función para permitir al usuario visualizar las zonas restringidas en la localidad donde se quiere emprender el vuelo. Estas zonas son presentadas a través de una geovalla.

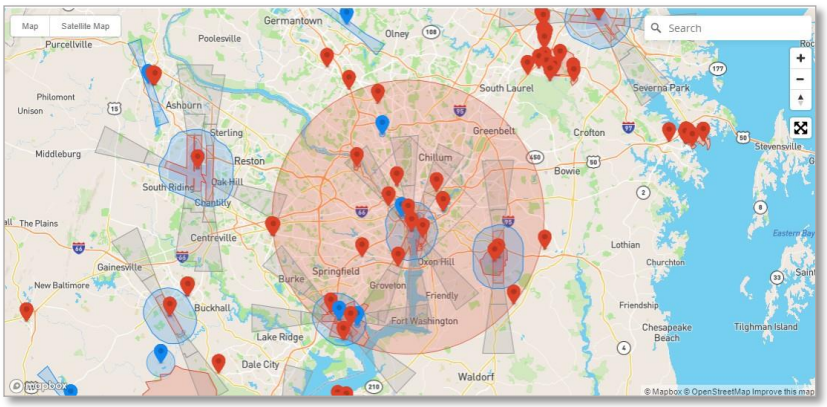

Ilustración 1 Geovalla de DJI para DJI MINI 2 en Estados Unidos

Nota. Adaptado de DJI. (s. f.). Geo Zone Map - Fly Safe - DJI. DJI Official. https://www.dji.com/flysafe/geo-map

Las geovallas crean una frontera virtual alrededor de un lugar específico al usar un software basado en GPS o RFID. “Esto genera una respuesta cada vez que un dron no autorizado entra en la zona, y los controles conectados a los drones, impiden que vuelen hacia zonas con geovallas o despeguen en ellas” (Infotecs, 2021).

Ilustración 2 Simbología de color de restricción de vuelo de drones en la geovalla de DJI

Ilustración 3 Simbología de color de restricciones de vuelo en drones basado en leyes y normativas locales en la geovalla de DJI

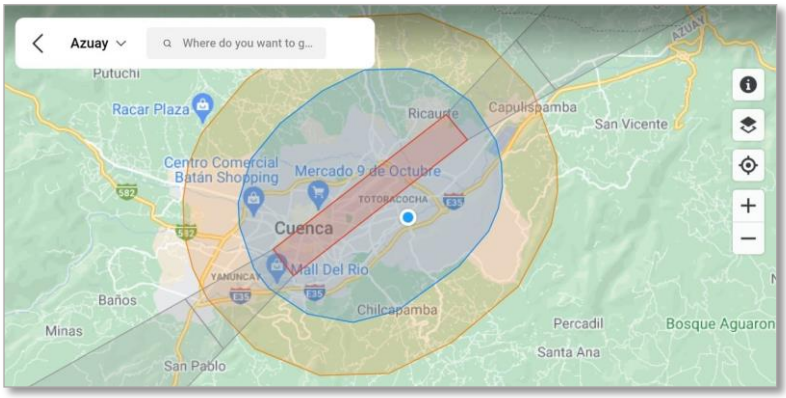

Ilustración 4 Geovalla para drones según DJI para el Azuay

Las pruebas de vuelo se realizaron en la ubicación que se encuentra dentro de la zona de autorización establecida en la ilustración 4 ya que esta, presenta una fuerte señal de GPS para establecer un punto de inicio y garantizar la estabilidad de posicionamiento. De igual manera, no existen interferencias magnéticas cerca de la ubicación, evitando que se pierda temporalmente el control del dron, o por último de los casos, que el dron se bloquee.

3. Interpretación de resultados.

3.1 Necesidades del sector farmacéutico para la entrega de sus productos

La encuesta realizada al sector farmacéutico permite inferir que, en la ciudad de Cuenca, 162 de 233 farmacias (69.5%), no poseen una página web con e-commerce para promocionar sus productos y servicios; frente a un 30.5% de entidades farmacéuticas que si gozan de la oportunidad de vender sus productos por medio de la web. Cabe destacar que esta encuesta contempla un 3,34% de error en el muestreo aleatorio.

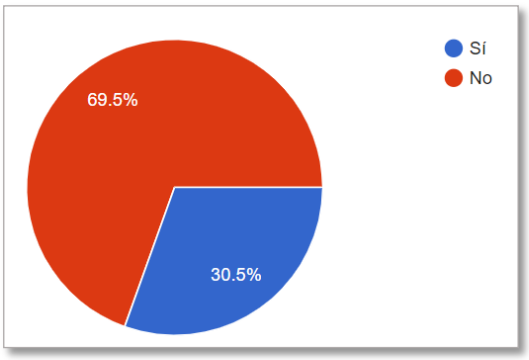

Ilustración 5 ¿Su centro farmacéutico tiene página web y puede vender sus productos a través de ella?

El 30,5% de farmacias representantes de la ilustración 5, trasladan los productos solicitados por sus clientes mediante transporte que consume combustible para su movilización. Lo que representa un gasto extra para el comerciante. Además, indican “la rapidez” como característica importante para cumplir con las necesidades de sus clientes en cuanto al servicio de entrega de paquetería; estimando de menor importancia, la confidencialidad y seguridad del producto con un 57,75% de acogida por los votantes.

Tomando en cuenta la temperatura ambiental como un factor muy importante para preservar al producto en una condición estable, el 97,2% de las entidades encuestadas que proporcionan a sus clientes el servicio de compra en línea, considerarían implementar un medio de transporte que posea un cajón que cumpla con la temperatura establecida y no deteriore el producto farmacéutico ni sus componentes.

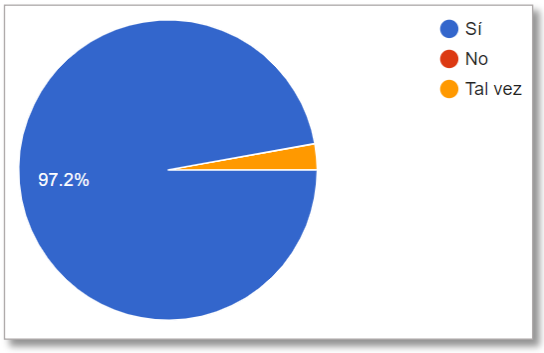

Ilustración 6 ¿Consideraría usted implementar un nuevo servicio de paquetería propio, a un módico precio, seguro y además que le permita generar un pago extra por el cliente que desee comprar sus productos?

Según la ilustración 6, casi la totalidad de las farmacias que venden sus productos en línea, consideran implementar una opción de medio de transporte que les genere ingresos extras para la farmacia. Además, este transporte de paquetería sería seguro, bajo en costo y propio para dicha entidad. Así mismo, generalmente estas locaciones farmacéuticas califican su nivel de seguridad para transportar los productos farmacéuticos hasta la ubicación indicada por el cliente, con una puntuación de 4/5. Solamente 10 farmacias consideran que satisfacen la seguridad del producto al 100%.

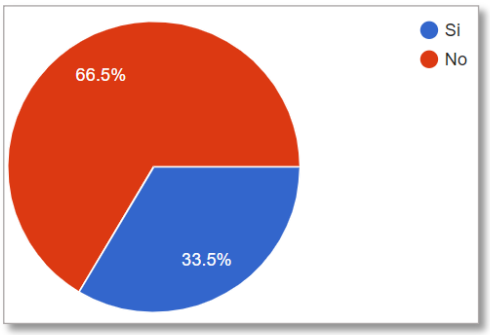

Ilustración 7 ¿Sabía usted que el e-comerse en el Ecuador creció el 300 % este año en comparación con el 2019?

El 66,5% de las entidades encuestadas que no presentan una página web que le permita vender sus productos farmacéuticos, no posee conocimiento acerca del crecimiento del e-commerce en el Ecuador desde el año 2019 hasta el 2021. Por otro lado, el 33,5% de esta población presentadas en la ilustración 7, teniendo conocimiento de este incremento, no han optado por vender sus productos de manera online.

De igual manera, tras el informe de las ventajas que puede presentar el comercio electrónico dentro de una empresa, el 66,5% de las farmacias sin página web, implementaría esta nueva metodología de venta de sus productos. No obstante, el 18% de esta población

no considera aplicar esta opción. Se infiere que se debe ofrecer más información con referencia al comercio electrónico para que el 15,5% de la población encuestada tenga una posición más clara en cuanto a esta elección.

El servicio de paquetería mediante drones es una metodología que las empresas sí están dispuestas a implementar, ya que la reducción de costos fue el segundo atributo con mayor acogida por la población y que se presenta de color azul en la ilustración 5. De igual manera, una de las opciones más seleccionadas fue la presencia de un cajón donde se transporte el producto a temperatura ambiente evitando causar estropeos en la mercancía.

Por otro lado, es necesario informar a la población cuencana acerca del crecimiento tecnológico por el que está pasando el Ecuador con el fin de "potenciar un entorno adecuado que permita incentivar el desarrollo en el comercio electrónico" (Ministerio de Telecomunicaciones y Sociedad de la Información et al., 2021, p. 10) en la ciudad, a través del empleo intensivo de las tecnologías de comunicación e información.

3.2 Comparativa de requerimientos técnicos en los drones

En el mercado existen varios tipos de drones con un objetivo establecido. En el caso de los drones para llevar peso, es decir, útil para el servicio de paquetería, se debe considerar que existen drones de uso común y drones profesionales.

Cuando se trata de drones de uso común o también conocidos como UAV de hobby, cuyo objetivo principal es el público en general, los fabricantes están tratando de hacer los modelos más sofisticados donde su objetivo es aumentar la duración del tiempo de vuelo y el rango de vuelo, sin embargo, los drones de hobby no están diseñados ni equipados para llevar una carga adicional, aunque según el estudio de (Poljak, 2019), tienen la capacidad de levantar cargas útiles en relación con su tamaño.

Por lo contrario, los drones profesionales se utilizan para entornos industriales o militares, y están diseñados principalmente para llevar peso extra mientras vuelan. Estos drones pueden transportar cargas impresionantes, porque es su propósito original y sus baterías están diseñadas para soportar ese peso extra y no perder tiempo de vuelo.

Posterior a la obtención de los requerimientos técnicos presentados en la fase 2 de la metodología, se realizó una comparativa entre 8 drones conocidos en el mercado para analizar si estos drones se podrían utilizar como función de delivery en el sector

farmacéutico. Esta comparativa posee tanto drones profesionales como drones de hobby para poder establecer una diferencia de valor.

Ilustración 8 Comparativa de los requerimientos de la FASE 2 frente a un grupo de drones reconocidos en el mercado

En la Ilustración 8 se puede apreciar que la gran mayoría de drones cumplen con los requerimientos solicitados para consolidarse en el servicio de entrega de paquetería. No obstante, se debe considerar que existen varios factores que perjudican la capacidad de carga útil del dron. Entre ellos, los más importantes son la potencia del motor, el tamaño y número de hélices, el tipo de batería y el peso del dron. Uno de los factores que se debe tener en cuenta es que el empuje de la hélice debe ser el doble del peso total del dron y la carga útil (Poljak, 2019).

De la ilustración 8 se seleccionó al DJI PHANTOM 3 PROFESSIONAL y al DJI MINI 2, con el objetivo de realizar las pruebas con un dron que satisfaga con todos los requerimientos técnicos y otro, que no presente en su totalidad el cumplimiento de todas las especificaciones.

3.3 Validación de carga útil en el grupo selecto de drones

Las validaciones de carga útil se enumeran en la tabla 1, donde se realiza cuatro experimentos. El cumplimiento de la prueba es marcado con un ✓ en cada columna de los drones empleados para la prueba.

#	PESO CAJA	PESO PRODUCTO	PESO TOTAL	CUMPLIMIENTO DE PRUEBA	
				DJI PHANTOM 3 PROFESSIONAL	DJI MINI 2
1	0 gramos	0 gramos	0 gramos	✓	✓
2	36 gramos	31 gramos	97 gramos	✓	✓
3	36 gramos	63 gramos	99 gramos	✓	✓
4	36 gramos	76 gramos	112 gramos	✓	✓

Tabla 1 Pesos para la prueba de carga útil en los drones DJI MINI 2 y PHANTOM 3 PROFESSIONAL

El primer peso de la tabla 1, corresponde al vuelo inicial con la cuerda donde se sostendrá el paquete. Se realizó esta prueba con el propósito de verificar que el armazón donde se transportará el producto farmacéutico no tenga problemas con los sensores propios del UAV.

Ilustración 9 Vista superior de la caja donde se almacena el producto farmacéutico

Ilustración 10 Prueba de carga útil de 112g en DJI PHANTOM 3 PROFESSIONAL

Ilustración 11 Prueba de carga útil de 112g en DJI MINI 2

En las ilustraciones 9, 10 y 11 se visualiza la ausencia de un armazón especializado para transportar el producto farmacéutico. Este objeto es de gran importancia para el delivery con drones ya que al no contar con un artefacto confiable, estable y apto para los diferentes tipos de clima que posee la ciudad de Cuenca, se está atentando contra la seguridad física del paquete a transportar.

De igual manera, se debe considerar la velocidad del viento, humedad y la presión del aire con el que tiene que lidiar el dron, ya que, al ser un armazón sin una estructura establecida, el viento fue un gran factor de arrastre del dron, por lo que el vehículo aéreo no tripulado contó con dificultades para aterrizar.

3.3.1 Categorización de amenazas de seguridad a los que pueden estar expuestos el grupo de drones seleccionados

Todos los ataques de la revisión bibliográfica se enumeran en la tabla 2 como filas, mientras que los tipos de ataque STRIDE se representan como columnas. El tipo de ataque específico es marcado con un en el cruce de la fila con la columna que corresponde a untipo de ataque.

Es evidente que los tipos más comunes de ataques contra UAV son la suplantación y DoS. No se encontraron ataques de los tipos Repudio en la búsqueda de literatura. La distribución de los ataques se ilustra en un gráfico circular.

ATAQUE	S	T	R	I	D	E
Ataque 1.1	✓					
Ataque 1.2	✓					
Ataque 1.3	✓					
Ataque 2.1	✓					
Ataque 2.2	✓					
Ataque 2.3	✓					
Ataque 2.4	✓					
Ataque 2.5	✓					
Ataque 2.6	✓					
Ataque 3	✓					
Ataque 4					✓	
Ataque 5					✓	
Ataque 6					✓	
Ataque 7	✓					

Tabla 2 Clasificación de los ataques a los drones en la Taxonomía de STRIDE

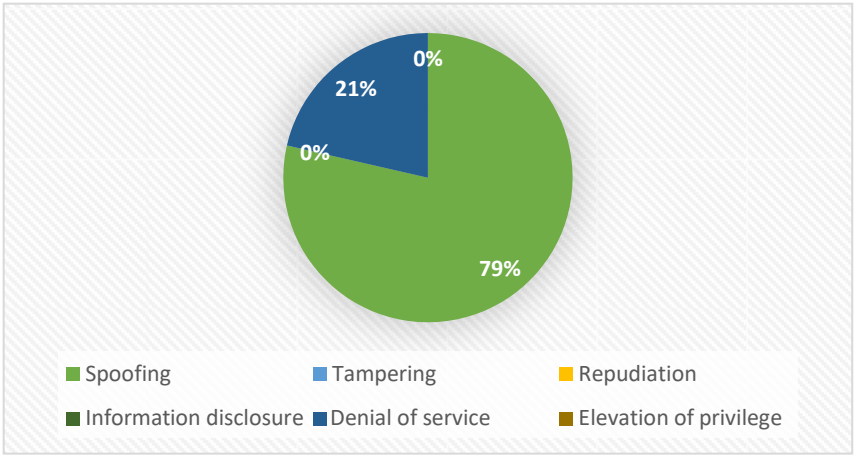

Ilustración 12 Porcentajes de distribución de la tabla 14

3.3.2 VALIDACION DEL FRAMEWORK MEDIANTE EL GRUPO SELECTO DE DRONES

3.3.2.1 Delineamientos de protección:

Los delineamientos de protección hacen referencia a las medidas de seguridad que deben estar aplicadas en los drones para protegerlos frente a los ataques cibernéticos

establecidos en la fase 5. A continuación se detalla cómo se fue aplicando las medidas de seguridad en cada uno de los drones utilizados para las pruebas.

- **Primera medida de protección: Actualización de Firmware.** Se realizó la actualización del programa encargado de controlar todos los circuitos electrónicos de ambos drones, es decir del DJI MINI 2 y del DJI PHANTOM 3 PROFESSIONAL. Las actualizaciones son propuestas por la marca del dron, DJI.

1. **DJI MINI 2:** se efectuó la actualización del firmware por medio del dispositivo donde se encuentra la aplicación que permite que el dron vuele. Este UAV al ser uno de los dispositivos más actuales por la empresa DJI, no requiere que se apliquela actualización de manera manual como sucede con otros drones anteriores a este. Por otra parte, la actualización se realiza de manera automática al presionar el botónde actualizar. Estas actualizaciones se presentan en la pantalla principal antes de realizar el vuelo.

Ilustración 13 Requerimiento y actualización de Firmware de batería en el DJI MINI 2

Cabe destacar la importancia de seguir las instrucciones presentadas en la pantalla puesto que, si se cierra la aplicación o se modifica el dron por algún motivo podía generar algún conflicto en la actualización.

Ilustración 14 Actualización de Firmware del DJI MINI 2

2. **DJI PHANTOM 3 PROFESSIONAL:** este modelo de dron lanzado en abril de 2015 (DJI Official, 2016), presenta una actualización de manera manual por lo que es necesario leer la guía instructiva de este modelo de UAV y ver los videos que la aplicación del dron nos proporciona. Al igual que el DJI MINI 2, las actualizaciones de firmware aparecen en el dispositivo que manejará el dron:

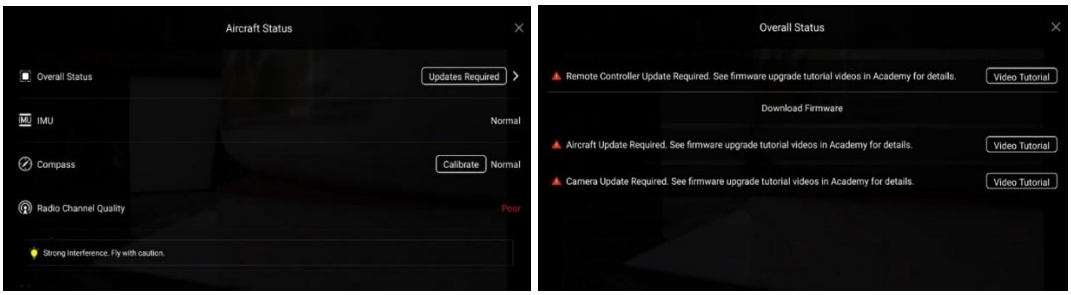

Ilustración 15 Requerimiento de actualizaciones en el DJI PHANTOM 3 PROFESSIONAL

A comparación de la ilustración 13, en la ilustración 15 no existe un botón de actualizar como lo indicó el modelo DJI MINI 2, por lo que se tiene que ingresar al video para conocer la actualización que requiere el vehículo aéreo no tripulado.

Al ser un dron con una versión antigua, por consecuente, actualización manual, se requiere ingresar a la página oficial de DJI, a la sección de descargas y posterior a ello, identificar el modelo a actualizar. Para el DJI PHANTOM 3, se necesita actualizar al firmware, donde descargaremos la primera opción que muestra la sección de descargas.

Ilustración 16 Descarga del nuevo firmware para el Phantom 3 Professional desde la página del DJI Phantom 3 Professional - Product Information – DJI

Posterior a la descarga, se cargó en la tarjeta microSD del dron el archivo .bin que contiene el reajuste del Firmware. Al finalizar la instalación, el DJI PHANTOM 3 PROFESSIONAL proporciona un archivo de texto plano donde se indica si el dron ha completado la actualización y cuando fue su última mejora.

Ilustración 17 Actualización del Firmware completa del DJI PHANTOM 3 PROFESSIONAL

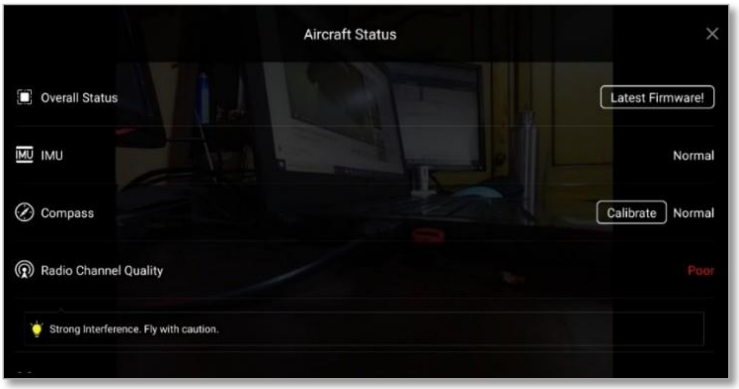

Ilustración 18 Verificación del estado del Aircraft para el PHANTOM 3 PROFESSIONAL

- **Segunda medida de protección: Contraseña segura para la aplicación de la estación base.** La longitud y complejidad de una contraseña son factores fundamentales para que su crackeo sea difícil o casi imposible. “Dependiendo de la longitud y complejidad de la clave, podemos saber más o menos el tiempo que se tardaría en crackear una contraseña” (Lorenzo, 2020). Hive Systems desarrolló un gráfico útil para ilustrar el tiempo que tarda un pirata informático en aplicar la fuerza bruta a una contraseña de inicio de sesión.

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

Ilustración 19 Tiempo de ataque de fuerza bruta según el número de caracteres de su contraseña.

Nota. Adaptado de Fripp, C. (2021, March 22). Use this chart to see how long it'll take hackers to crack your passwords. Komando.Com. https://www.komando.com/security-privacy/check-your-password-strength/783192/#:%7E:text=On%20average%2C%20it%20takes%20a,into%20a%20seven%2Dcharacter%20password.

DJI presenta dos aplicaciones de estación base para cada uno de los drones según su modelo de UAV, para lo cual el DJI MINI 2, se maneja mediante la aplicación de "DJI Fly", mientras que el dron DJI PHANTOM 3 se opera desde la aplicación de "DJI GO – For products before P4". Estas aplicaciones están disponibles en las tiendas de aplicaciones móviles. Play Store para el sistema operativo Android, y App Store para iOS.

Para la aplicación de estación base, se estableció una misma cuenta de DJI. Además, se utilizó una combinación de letras, números y caracteres especiales con la finalidad de crear una contraseña segura para disuadir a los atacantes; de esta forma, se espera que la mayoría de los atacantes desista y busque una víctima más fácil, ayudando así a evitar que el atacante hackee la señal del dron.

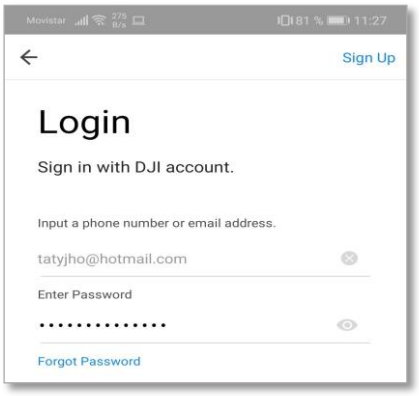

Ilustración 20 Inicio de sesión desde la aplicación de DJI GO

Como se puede observar en la Ilustración 20, se visualiza una contraseña de 14 caracteres que poseen mayúsculas, minúsculas, números y caracteres especiales, presentando un tiempo estimado de 200 millones de años según la ilustración 19, en que la contraseña sea crackeada por ataque de fuerza bruta.

- **Tercera medida de protección: Limitación a la estación base.** Se estableció un router únicamente para la aplicación móvil que se va a conectar con los drones. Mediante el comando de Nast aplicado en Linux, se puede observar las direcciones MAC e IP de los hosts que están conectados a la red.

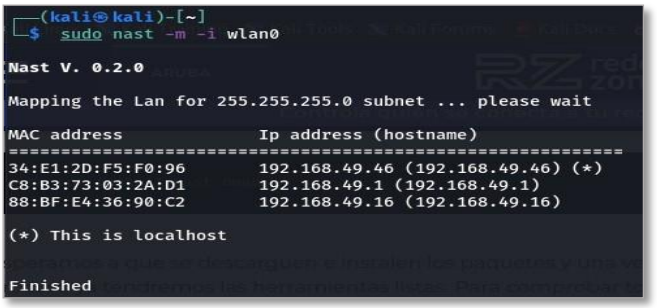

Ilustración 21 Aplicación de comando nast en Kali Linux

En la ilustración 21, se visualiza 3 host que están conectados a la red. La dirección IP 192.168.49.1, hace referencia a la dirección IP del router; la IP 192.168.49.46 representa la maquina local de Kali y finalmente, la IP 192.168.49.16 simboliza al dispositivo móvil que está conectado con la aplicación del dron.

Es importante destacar que la conexión a Internet es activada únicamente en caso de que exista alguna actualización pendiente en el dron. Esta buena práctica lo indica el delineamiento de protección número 1 establecido en el Framework, descrito como “Conexión a Internet desactivada al volar el UAV”.

- **Cuarta medida de protección: Suscripción a VPN.** Se realizó la descarga de una VPN obtenida en Play Store, denominada “Secure VPN”, con el objetivo de mantener una conexión a Internet de manera segura frente a los atacantes cibernéticos.

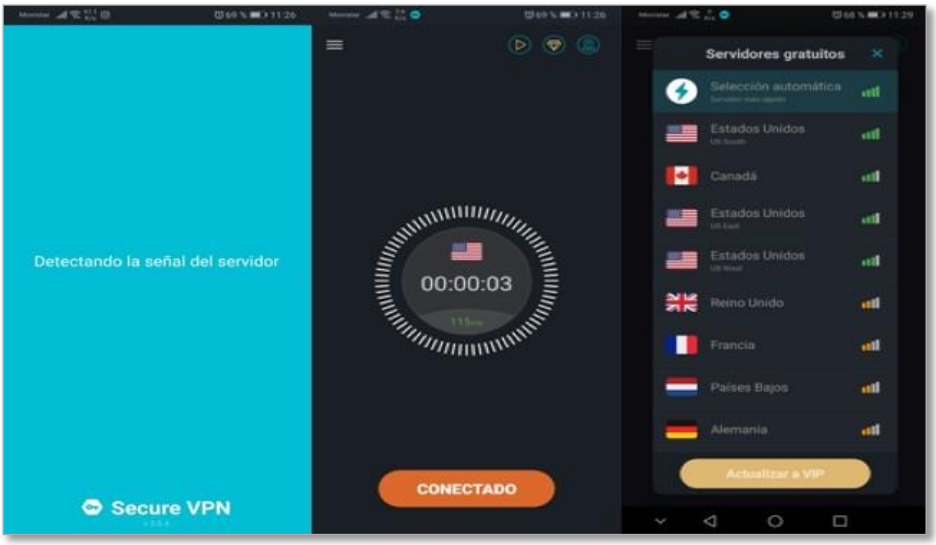

Ilustración 22 Conexión a Secure VPN con servidor de Estados Unidos desde el dispositivo que contiene la aplicación para manejar el dron

3.3.2.2 Espacios de prueba:

Se realizó las pruebas de vuelo tanto en la zona restringida, como en la zona autorización. La prueba en la zona restringida obtuvo un resultado que no se puede efectuar el vuelo, de tal manera que se requiere solicitar permiso al aeropuerto Mariscal La Mar.

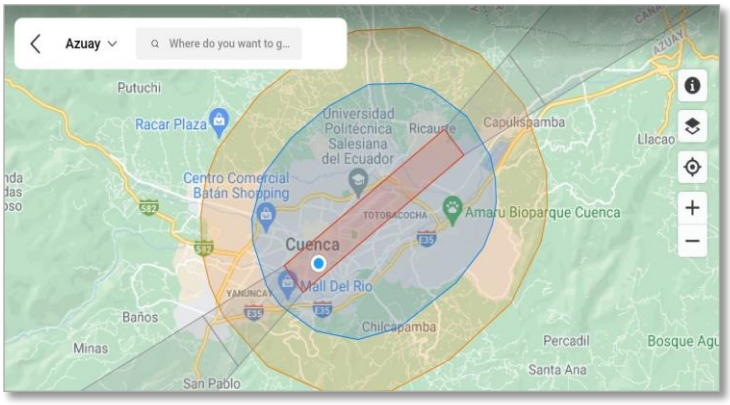

Ilustración 23 Prueba de espacio en zona restringida dentro de la geovalla de DJI

Como se presenta en la Ilustración 24, se encuentran varios centros farmacéuticos, casas hogares y hospitales. Los iconos naranjas hacen referencia a los hospitales; los azules indican los asilos de ancianos y por último, los iconos color morado representan las entidades farmacéuticas. Estos sitios son importantes porque pueden requerir de medicamentos. Finalmente, el icono amarillo representa la ubicación donde se realizó las pruebas de vuelo.

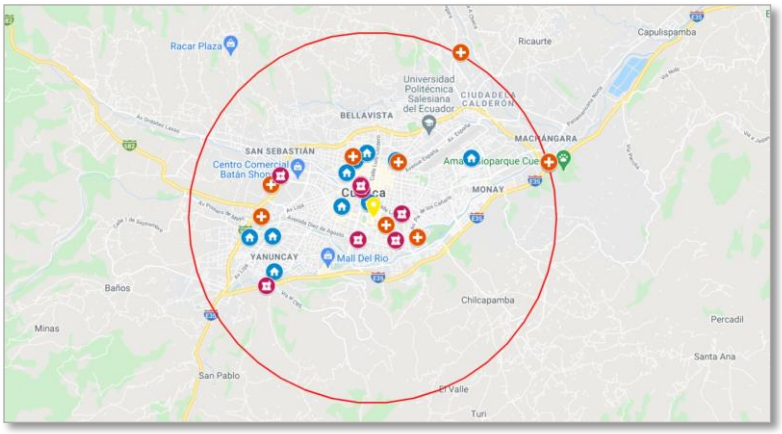

Ilustración 24 Trazo de rango de 5km de la ubicación presentada en la ilustración 36

Nota: Radio graficado en https://kml4earth.appspot.com/circlegen.html e implementado en https://www.google.com/intl/es/maps/about/mymaps/. Disponible en: https://www.google.com/maps/d/edit?mid=1tDmatuucNZAfG4KnvvvQzC-UJQeFNS6Q&usp=sharing

Por otra parte, en la zona de autorización se pudo realizar el vuelo, mediante un código de permiso propuesto por la empresa DJI. Este código fue solicitado mediante una llamada.

Ilustración 25 Prueba de espacio en zona de autorización dentro de la geovalla de DJI

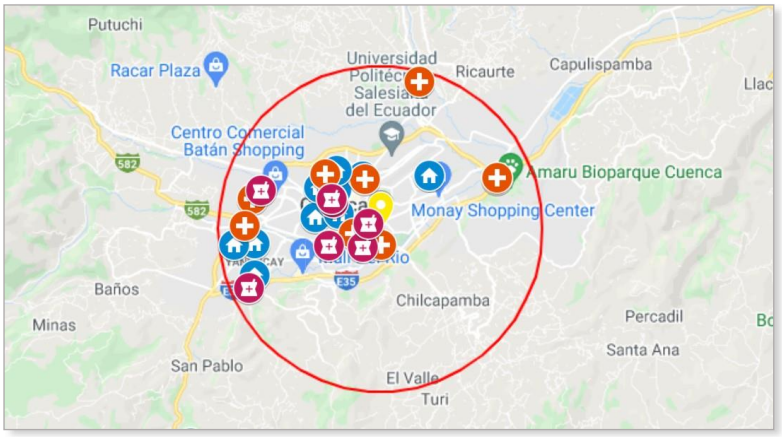

Ilustración 26 Trazo de rango de 5km de la ubicación presentada en la ilustración 38

Nota: Radio graficado en https://kml4earth.appspot.com/circlegen.html e implementado en https://www.google.com/intl/es/maps/about/mymaps/. Disponible en: https://www.google.com/maps/d/edit?mid=101rzwjP9eoFyi6eUVu7_gS3eHbXZv-Ud&usp=sharing

3.3.2.3 Ejecución de ataques:

Se procede a realizar los distintos ataques para validar que los delineamientos propuestos en el Framework sean útiles para resguardar la seguridad del vehículo aéreo no tripulado, además de los datos que este posee. Para ello, se ha realizado una investigación documental de las principales ciberamenazas presentes en el Ecuador y que se resume en la tabla 3.

N°	Ciberamenazas en Ecuador	Desviación de la clasificación según tendencias internacionales	Ciberamenazas 2018 de la *ENISA
1	Suplantación de identidad	↑	Software malicioso
2	Correo no deseado	↑	Ataques basados en la web
3	Software malicioso	↓	Ataques de aplicaciones web
4	Fuga de información	↑	Suplantación de identidad
5	Amenaza interna	↑	Negación de servicio
6	Manipulación física/daño/robo	↑	Correo no deseado
7	Robo de identidad		Redes de bots
8	Ataques de aplicaciones web	↑ ↓	Violación de datos
8	Programa de secuestro de datos	↑	Amenaza interna
10	Negación de servicio	↓	Manipulación física/daño/robo
11	Ataques basados en la web	↓	Fuga de información
12	Violación de datos	↓	Robo de identidad
13	Redes de bots	↓	Minería de criptomonedas maliciosa
14	Minería de criptomonedas maliciosa	↓	Programa de secuestro de datos
15	Espionaje cibernético	→	Espionaje cibernético

Tabla 3 Ataques de ciberseguridad según las principales amenazas en el Ecuador.

Nota: Obtenido de Vera, S. (2019, 3 septiembre). Principales Ciberamenazas en Ecuador. Gobierno Electrónico de Ecuador. https://www.gobiernoelectronico.gob.ec/principales-ciberamenazas-en-ecuador/

Posterior a ello, se realizó la clasificación de la columna de "Ciberamenazas en Ecuador" correspondiente a la Tabla 2, en la taxonomía de STRIDE para poder realizar las

pruebas de ataques a la categoría que más ataques tenga.

N°	Ciberamenazas en Ecuador	S	T	R	I	D	E
1	Suplantación de identidad	✓					
2	Correo no deseado	✓					
3	Software malicioso	✓					
4	Fuga de información	✓					
5	Amenaza interna	✓					
6	Manipulación física/daño/robo		✓				
7	Robo de identidad	✓					
8	Ataques de aplicaciones web	✓					
8	Programa de secuestro de datos	✓					
10	Negación de servicio					✓	
11	Ataques basados en la web	✓				✓	
12	Violación de datos			✓			
13	Redes de bots						
14	Minería de criptomonedas maliciosa	✓					
15	Espionaje cibernético	✓					

Tabla 4 Clasificación de las Ciberamenazas en Ecuador según la Taxonomía de STRIDE

Entre la tabla 2 y 4, se puede diferir que las categorías que más ataques presentan según la Taxonomía de STRIDE son: "Suplantación de Identidad" y "Denegación de Servicios". Por consecuente, se realizaron las pruebas de ataque con referencia a estas categorías señaladas.

Para la realización de los ataques se utilizó un conjunto de herramientas diseñadas para ataques de ingeniería social denominado The Social-Engineer Toolkit (SET). Esta herramienta permite suplantar, de manera sencilla, "la identidad de un sitio determinado, o enviar ataques por mail a las cuentas de correo de la compañía" (Krombholz et al., 2015)., infectar memorias USB o CDs/DVDs, entre otros. Los resultados de la ejecución de los ataques se detallan a continuación.

1. **Ataque interno de suplantación de identidad por ataque web:**

   Este ataque tiene la finalidad de obtener las credenciales de la cuenta de DJI, ya que antes de poder volar el vehículo aéreo no tripulado, es necesario iniciar sesión dentro de la aplicación.

   Se realizó un ataque web mediante la utilización del SET, seleccionando la opción de Ataques de Ingeniería Social → Credential Harvester Attack Method. Para este ataque se utilizó la opción de "Custom import", puesto que la página de inicio de sesión de DJI, no se clona de manera completa.

Verificación del ataque web sin VPN:

Se realizó el ataque a un navegador web de un dispositivo que se encontró conectado a la misma red Wi-Fi. Se ingresó la dirección IP del computador donde se levantó el ataque web mediante SET, es decir la dirección 192.168.1.9.

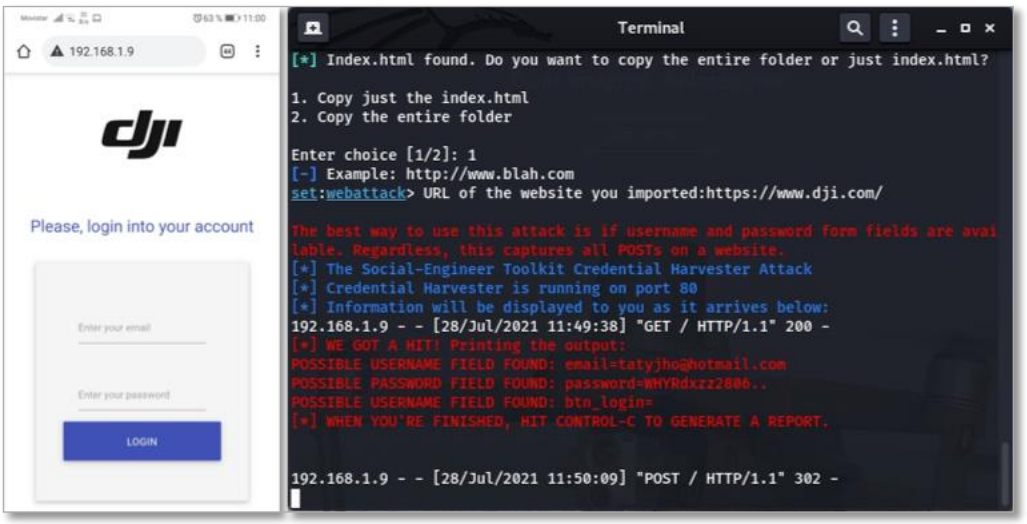

Ilustración 27 Ingreso a la página web bajo la dirección IP donde se tiene levantando el ataque web.

Verificación del ataque web con VPN:

Se procedió a activar la VPN de la aplicación en el dispositivo móvil. En la ilustración 28, al recargar la página se puede apreciar que ahora ya no nos sale la página de iniciar sesión y se mantiene cargando hasta que se interrumpe la conexión.

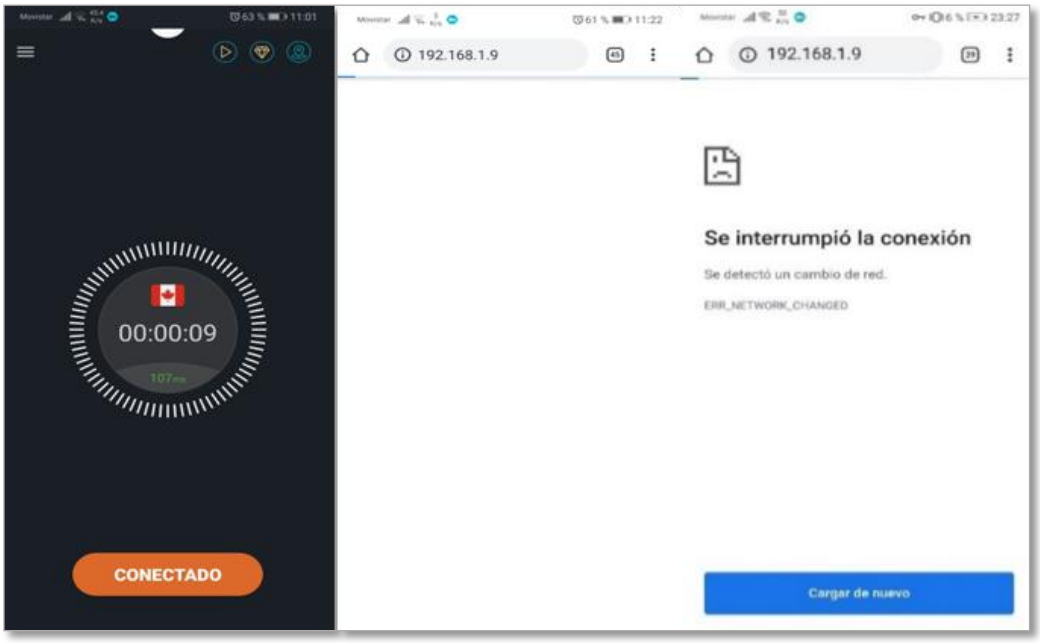

Ilustración 28 Verificación de ataque en dispositivo móvil activado la aplicación VPN

2. Ataque interno de suplantación de identidad por ataque web enviado a través de correo no deseado.

Tras la implementación de la suplantación de identidad por ataque web que se mencionó anteriormente, se realiza un ataque de correo electrónico donde se involucra el nombre de la empresa de la marca DJI, indicando que se ha detectado actividad sospechosa y, para lo cual, debe ingresar a un enlace para verificar su cuenta.

Este ataque se realizó a una sola persona y se lo realizará mediante Gmail, habilitando el acceso a aplicaciones menos seguras dentro de la cuenta de Google.

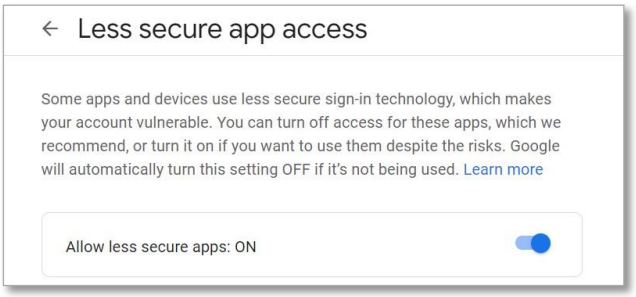

Ilustración 29 Activación de Acceso a aplicaciones menos seguras en Google

Posterior a ello, se ingresó el remitente del mensaje y se estructuró el mensaje de phishing donde se presencia un enlace para la obtención de las credenciales de la cuenta de DJI.

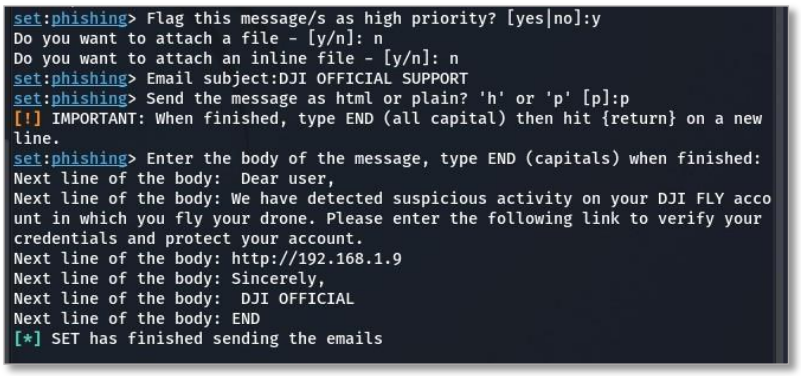

Ilustración 30 Mensaje en texto plano con el enlace de la página web para atacar las credenciales

Verificación del ataque:

Se comprobó que el mensaje haya llegado exitosamente con la configuración que se realizó en la herramienta utilizada. Cabe destacar que el ataque de phishing y web fue interrumpido de manera exitosa por la VPN ya que el SET está trabajando sobrela dirección IP asignada por DHCP. La VPN permite una conexión segura y cifrada entre un usuario determinado y la red a la que está conectado.

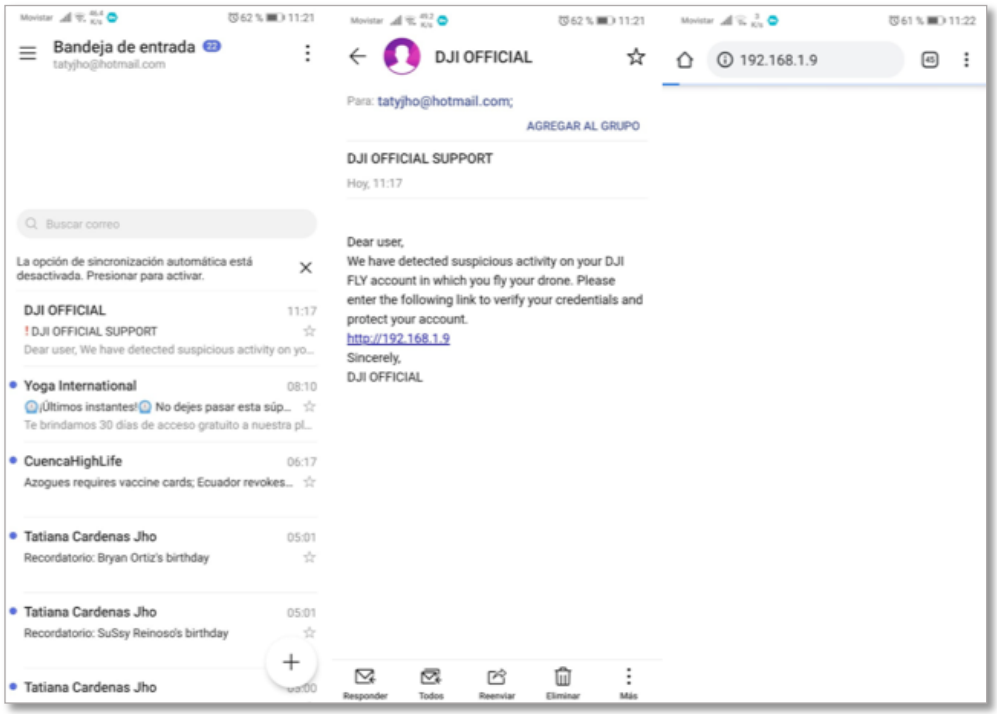

Ilustración 31 Verificación de ataque phishing y web activado el VPN del dispositivo móvil

3. **Ataque de denegación de servicio:**

Actualmente existen varias tecnologías de transmisión que permiten la comunicación entre el controlador del dron y el UAV. El Wi-Fi es una de las comunicaciones más utilizadas por grandes compañías de drones como es DJI. Sin embargo, esta empresa creó un sistema de transmisión denominado Ocusync 2.0, el cual permite un rango de comunicación de hasta 7000 m (Iñiguez, 2020). El dron DJI MINI 2, posee este tipo de tecnología por lo que realizar un ataque a este no es muy posible hasta la actualidad.

Por otro lado, el DJI PHANTOM 3 PROFESSIONAL según su manual de usuario no presenta una conexión Wi-Fi, por lo que no se puede obtener una dirección IP para poder realizar esta prueba de ataque.

Todos los ataques realizados en el experimento se enumeran en la Tabla 5 como filas, mientras que la defensa de los drones tras aplicar el Framework se representa como columnas. Si el Framework fue efectivo frente a los ataques es marcado con un ✓, para el caso contrario, se lo identifica con una ✕.

Los ataques de suplantación de identidad fueron bloqueados de manera exitosa según los delineamientos de seguridad propuesto por el Framework. Sin embargo, el ataque de correo no deseado es un ataque de ingeniería social para el cual es indispensable concientizar a todo el personal de la entidad farmacéutica puesto que, si un empleado, dirigente o personal administrativo cae en los engaños sometidos en phishing, el impacto puede ser muy importante en cuanto a la pérdida de información del cliente que adquiere los servicios de paquetería mediante drones y además el hurto del vehículo aéreo no tripulado.

El ataque 2 realizado en este experimento de validación del Framework indica como se puede adjuntar un enlace para obtener las credenciales del usuario. Con esa información se puede acceder, iniciar un vuelo y secuestrar al dron en caso de que el UAV este prendido en ese entonces.

Ataque	Delineamientos de seguridad del Framework	
	DJI PHANTOM 3 PROFESSIONAL	DJI MINI 2
Amenaza interna	✓	✓
Suplantación de identidad	✓	✓
Correo no deseado	✓	✓
Suplantación de identidad	✓	✓
Denegación de servicio	✗	✗

Tabla 5 Resultados de ciberataques a drones implementado el Framework de Seguridad

4. Discusión.

El resultado de la validación del Framework indica que los ataques de suplantación de identidad y denegación de servicio son los tipos de ataques más comunes contra los vehículos aéreos no identificados. Los objetivos para atacar un dron con estos métodos son tomar el control total sobre la ruta de vuelo y provocar que el dron se estrelle contra su voluntad. Estos hechos tienen graves consecuencias para los conductores y/o propietarios del dron, así como para la sociedad en general, ya que puede herir directamente a una persona. De igual manera, se atenta contra la integridad de datos, puesto que los archivos del UAV secuestrado también son robados.

Hay una fuerte conexión entre el tipo de ataque de suplantación y secuestro del dron, así como entre el choque del dron y los ataques DoS. Por consecuente, las compañías productoras de los vehículos aéreos no tripulados deben centrarse en estas vulnerabilidades más que en cualquier otra, debido a los peligros que plantean para la sociedad. Este es un tema relativamente nuevo porque la propia tecnología es nueva y ha creado un aumento en la demanda de estos. Las predicciones del mercado sólo muestran que esta demanda crecerá, lo que significa que se necesita más investigación en este tema para mitigar los posibles riesgos que un creciente uso de los UAV podría representar para las personas.

La rigurosidad de parámetros y reglamentos con respecto al uso de UAVs en el Ecuador propuesta por la Dirección General de Aviación Civil (2020), podría considerarse una gran desventaja para los operadores de esta tecnología aplicada en trabajos aéreos, ya que la actual normativa presenta varias restricciones en cuanto al sobrevuelo en ciertos lugares de la zona urbana de la ciudad; no presenta una ley de protección para la entidad que provee servicio de

paquetería mediante UAV; costos excesivamente altos para la adquisición de seguro de vuelo, entre otros.

El Framework funciona para ataques de DoS y de Spoofing. Sin embargo, como trabajo futuro se puede validar el Framework con el resto de los ataques que tienen exposición en la ciberseguridad del Ecuador y con los ataques presentados en la tabla 2, con la finalidad de que exista una mejora en el Framework y que distintas entidades del sector económico a más de la farmacéutica puedan utilizar este medio para implementar los drones como servicio de paquetería.

5. Conclusiones.

Las MIPYMEs del sector farmacéutico en Ecuador requieren de plataformas digitales que las mantengan conectadas con sus clientes de manera local e internacional, la cual proporcione servicios innovadores para mejorar la gestión de la experiencia del cliente desde la búsqueda del producto hasta la gestión de envío, almacenamiento, distribución y entrega de este, con la finalidad de mantener la competitividad en un mercado golpeado por la expansión del virus SARS-COV-2.

El servicio de entrega con drones es un paradigma prometedor en la próxima era de IoT. En este documento, se ha analizado el uso de un Framework desarrollado para la seguridad en los servicios de entrega con drones enfocado en el sector farmacéutico de la ciudad de Cuenca, ya que el uso de drones se está desarrollando rápidamente y existe una necesidad urgente de establecer el marco y las herramientas para garantizar un manejo adecuado y la confianza en su aplicación para la entrega de productos farmacéuticos.

Las metodologías de prueba de estabilidad del UAV deben expandirse para incluir las tensiones únicas que se pueden encontrar durante el transporte de estos y del peso extra a trasladar, como vibraciones, fuerza g, cambios rápidos de presión, humedad y variaciones de temperatura, que pueden afectar los atributos de los materiales críticos de los medicamentos. De igual manera se debe explorar los distintos ataques tras la clasificación de la taxonomía de STRIDE para una validación más certera.

Existen varios impedimentos para abordar el uso de drones destinados a la distribución de medicamentos. No es sencillo que, a corto plazo, esta metodología de transporte de mercadería esté implantado en las empresas con servicio de comercio electrónico, puesto que

más de la mitad de la población farmacéutica de la ciudad de Cuenca que no posee página web con ventas en línea, presenta desconocimiento acerca de las ventajas del e-commerce y el crecimiento que este método de compra y venta está tenido en el país. No obstante, la problemática de la económica, legislativa y de seguridad, que impide el adecuado auge del comercio electrónico y por consecuente, el empleo de drones como servicio de paquetería para este, parecen remediable. Con inversiones en estas materias, la aparición de drones en la vida cotidiana de los cuencanos sería más probable a medio o largo plazo.

Las fabricantes de estos dispositivos también deben utilizar este resultado y más resultados acerca de la seguridad en los drones como una indicación de que necesitan desarrollar un software más seguro en el futuro.

6. Bibliografía

Albuja, M. (2021, marzo). Delivery en tiempos de COVID - 19. https://eservicios.mintel.gob.ec/wp-content/uploads/2021/03/Marcelo-Albuja.pdf

De Prati, & Dávila, J. (2021, marzo). ¿Cómo cambió el Comercio Electrónico durante la pandemia? https://eservicios.mintel.gob.ec/wp-content/uploads/2021/03/De-Prati.pdf

Dirección General de Aviación Civil. (2020). Operación de Aeronaves Pilotadas a Distancia (RPAs) no DGAC-DGAC-2020-0110-R. https://www.aviacioncivil.gob.ec/wp-content/uploads/downloads/2020/11/5-DGAC-DGAC-2020-0110-R-Reglamento-de-RPAs.pdf

DJI Official. (2016, 16 febrero). DJI Adjusts Pricing for Phantom 3 Professional Globally - DJI. https://www.dji.com/newsroom/news/dji-adjusts-price-for-phantom-3-professional#:%7E:text=The%20Phantom%203%20Professional%20launched,to%20get%20into%20aerial%20videography.%E2%80%9D

Economía. (2019, 14 noviembre). El futuro del delivery: la entrega a través de drones. Revista Economía. https://www.revistaeconomia.com/el-futuro-del-delivery-la-entrega-a-traves-de-drones/

Espinoza, G. (2020, 16 octubre). Ecuador estrena plan piloto para entregas con drones desde Quito a suburbios. www.expreso.ec. https://www.expreso.ec/ciencia-y-tecnologia/ecuador- estrena-plan-piloto-entregas-drones-quito-suburbios-91727.html

Gobierno Electrónico. (2019, 3 septiembre). Principales Ciberamenazas en Ecuador. Gobierno Electrónico de Ecuador. https://www.gobiernoelectronico.gob.ec/principales-ciberamenazas-en-ecuador/ https://eservicios.mintel.gob.ec/wp-content/uploads/2021/02/ESTRATEGIA- NACIONAL_ENCE2.pdf

Hussain, S., Kamal, A., Ahmad, S., Rasool, G., & Iqbal, S. (2014). Threat modelling methodologies: a survey. Sci. Int.(Lahore), 26(4), 1607-1609.

Infotecs. (2021, 25 mayo). Seguridad en Drones (Parte 2). https://infotecs.mx/blog/seguridad_en_drones_parte_2.html

Iñiguez, A. (2020, 24 noviembre). ¿Qué diferencias hay entre WIFI vs OcuSync 2?0? Drones, Cámaras, Acción. https://drones-camaras-accion.com/blog/wifi-vs-ocusync-diferencias/

Jackson, B. (2021, 26 febrero). Understanding Drone Payloads. COPTRZ. https://coptrz.com/understanding-drone-payloads/#:%7E:text=Payload%3A%20The%20Definition,sensors%2C%20or%20packages%20for%20delivery.

Jung, S., & Kim, H. (2017). Analysis of amazon prime air uav delivery service. Journal of Knowledge Information Technology and Systems, 12(2), 253-266.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and applications, 22, 113-122.

Lorenzo, J. A. (2020, September 16). Este es el tiempo que se tarda en crackear tu contraseña. RedesZone. https://www.redeszone.net/tutoriales/seguridad/tiempo-hackear-contrasena/

Lotz, A. (2015). Drones in Logistics: A Feasible Future or a waste of effort.

Luzuriaga Romero, M. N. (2017). Análisis del uso de drones en los servicios de entrega dentro de la ciudad de Guayaquil (Doctoral dissertation, Universidad de Guayaquil. Facultad de Ingeniería Industrial. Carrera de Ingeniería en Teleinformática.).

Ministerio de Telecomunicaciones y Sociedad de la Información, Ministerio de Producción, Comercio Exterior, Inversiones y Pesca, & Estrategia Nacional de Comercio Electrónico. (2021, marzo). ESTRATEGIA NACIONAL DE COMERCIO ELECTRÓNICO. https://eservicios.mintel.gob.ec/wp-content/uploads/2021/02/ESTRATEGIANACIONAL_ENCE2.pdf

Oncins de Frutos, M. (1991). NTP 283: Encuestas: metodología para su utilización. Nota Técnica de Prevención, Madrid: Instituto Nacional de Seguridad e Higiene en el Trabajo (INSHT).

Organización Médica Colegial de España. (2009, 18 junio). El volumen y peso de los envases de medicamentos se ha reducido en un 15%. Médicos y Pacientes.

http://www.medicosypacientes.com/articulo/el-volumen-y-peso-de-los-envases-de-medicamentos-se-ha-reducido-en-un-15

Ortega, C. (2020, 13 agosto). ¿Qué es la investigación documental? QuestionPro. https://www.questionpro.com/blog/es/investigacion-documental/#:%7E:text=La%20investigaci%C3%B3n%20documental%20es%20una,%2C%20peri%C3%B3dicos%2C%20bibliograf%C3%ADas%2C%20etc.

Palmer, A. (2021, 18 febrero). Amazon Air will have a «growth spurt» this spring and could eventually resemble an airline, study says. CNBC. https://www.cnbc.com/2021/02/17/amazon-air-fleet-growing-fast-could-resemble-airline-study.html

Poljak, M. (2019, 3 diciembre). How Much Weight Can a Drone Carry? Drone Tech Planet. https://www.dronetechplanet.com/how-much-weight-can-a-drone-carry/#:%7E:text=So%20How%20Much%20Weight%20Can,are%2020%20to%20220%20kg

Secretaría General de la Comunidad Andina, SGCAN, & Caicedo, D. (2021, marzo). DESAFIOS PARA EL COMERCIO ELECTRÓNICO EN AMÉRICA LATINA. https://eservicios.mintel.gob.ec/wp-content/uploads/2021/03/diego-caicedo.pdf

Stine, K. M., Quill, K., & Witte, G. A. (2014). Framework for improving critical infrastructure cybersecurity.

Sánchez, G. (2018, 19 diciembre). UNICEF hace historia: utiliza drones para entregar vacunas para niños. Insights. https://www.insights.la/2018/12/19/unicef-utiliza-drones-entregar-vacunas-ninos/

Tabatabai, M. (2020, 29 enero). Drone-to-Door – The Ascent of The Airborne Pharmacy. Magellan Health Insights. https://magellanhealthinsights.com/2020/01/27/drone-to-door-the-ascent-of-the-airborne-pharmacy/

Vakulenko, Y., Shams, P., Hellström, D., & Hjort, K. (2019). Service innovation in e-commerce last mile delivery: Mapping the e-customer journey. Journal of Business Research, 101, 461–468. https://doi.org/10.1016/j.jbusres.2019.01.016

Welch, A. (2015). A cost-benefit analysis of Amazon Prime Air.