Método para la detección de exfiltración de información sobre los datos transmitidos por ultrasonido entre dispositivos computacionales a través de la captura, identificación y clasificación de la información.

Clay Schneider Vallejo Pinilla

Carlos Augusto Ruiz Patiño

Instituto Tecnológico Metropolitano

Facultad de ingeniería

Medellín, Colombia

2019

Método para la detección de exfiltración de información sobre los datos transmitidos por ultrasonido entre dispositivos computacionales a través de la captura, identificación y clasificación de la información.

Clay Schneider Vallejo Pinilla

Carlos Augusto Ruiz Patiño

Tesis o trabajo de investigación presentada(o) como requisito parcial para optar al título de:

Magister en seguridad informática

Director (a):

Msc.Héctor Fernando Vargas Montoya

Línea de Investigación: Ciencias de la Computación

Instituto Tecnológico Metropolitano

Facultad de Ingeniería

Medellín, Colombia

2019

Dedicatoria

Les dedicamos esta tesis a nuestras familias por todo su apoyo y ayuda durante este proceso, en especial a mi Madre Luz Mary Patiño y Padre Carlos Arturo Ruiz Tabares, que me han apoyado en cada paso que realizo y me han entregado todo de sí. Este proceso va dedicado a las personas que dieron su apoyo en unos momentos difíciles de mi vida, a mi madre: Luz Gloria Pinilla, mi padre: Orlando Antonio Vallejo Restrepo, a mi hijo: Miguel Alejandro Vallejo Sánchez y a mi compañero Carlos Augusto Ruiz por su constante motivación y apoyarme en seguir adelante.

Agradecimientos

Total gratitud a nuestros directores iniciales Srs. Manuel Santander y Javier Mauricio Duran que en su momento entregaron grandes aportes a nuestro proyecto y que creyeron en cada momento de nuestra tesis; además por su acompañamiento.

Al director Héctor Vargas, que confió en nuestras capacidades y nos entregó su apoyo en todo el resto del proceso, aportándonos sus conocimiento técnicos, metodológica y logrando también en nosotros una gran motivación e interés de nuestra tesis.

También le agradecemos a todas las personas que directa o indirectamente aportaron y fueron de gran apoyo, como lo fueron compañeros y profesores de la maestría, en especial los profesores Gloria Mercedes Díaz Cabrera y Fernando Quintero los cuales nos reflejaron ese gran liderazgo que poseen y nos orientaron a continuar en este proceso y al no desertar de nuestra propuesta de tesis.

1. Resumen

En proyecto se entregan los resultados concernientes a la exfiltración de información a través de ultrasonido entre equipos computacionales, esto es, lograr enviar información (de un equipo A a un equipo B) que puede ser sensible a través de un medio no convencional como lo es el ultrasonido. La información y los datos pueden ser vulnerados por diferentes medios, este proyecto analiza cómo es posible transmitir información con ultrasonido, a través del uso de los sistemas periféricos de estaciones de trabajo, con lo cual, el principio de confidencialidad se ve vulnerado. Para lograr el objetivo se usaron 2 escenarios, uno libre de ruido y el otro, un ambiente de oficina, así mismo, se contó el uso del software GNU Radio, QuietNet y un desarrollo propio, el cual permitió a través de la definición de unos niveles de clasificación, visualizar el proceso de exfiltración de información.

Con la ejecución de las diferentes pruebas, se logró la trasmisión, recepción y visualización de datos, éstos una vez recepcionados, se les aplicó un proceso de clasificación de información, que, aunque es un ambiente de prueba, puede ser aplicada a cualquier elemento informático que pueda transmitir por ultrasonido. Las pruebas realizadas se enfocaron en el uso de hardware básico no modificado (equipos portátiles sin modificaciones), para simular condiciones de los escenarios respectivos.

Palabras clave: Canal Encubierto, Ultrasonido, Exfiltración, Clasificación de información, confidencialidad

Abstract

In this project, the results concerning the exfiltration of information through ultrasound between computer equipment are delivered, that is, to be able to send information (from equipment A to equipment B) that can be sensitive through an unconventional means such as It is the ultrasound. The information and data can be violated by different means, this project addresses how from workstations, a user can transmit information using peripheral systems that support ultrasound, whereby the principle of confidentiality is violated. To achieve the objective, 2 situations were used, one free of noise and the other, an office environment, likewise, the use of GNU Radio software, QuietNet and its own development was counted, which is connected through the definition of Some levels of classification, visualize the process of exfiltration of information.

With the execution of the different tests, the transmission, reception and visualization of data is controlled, it is detected once received, an information classification process was applied, which, although it is a test environment, can be applied to any computer element that can be transmitted by ultrasound. The tests carried out focused on the use of basic unmodified hardware (portable equipment without modifications), for simulate conditions of specific controls.

Keywords: Undercover Channel, Ultrasound, Exfiltration, Classification of information, confidentiality

Contenido

2. Lista de figuras

Pág.

3. Lista de tablas

Pág.

4. Lista de Símbolos y abreviaturas

BIOS: Basic Input/Output System.

CM: Centímetro

CMF: Content Monitoring Filtering

DB: Decibelio

DLP: Data Loss Prevention

FSK: Frequency Shift Keying.

GHZ: Gigahertz.

GnuPG: GNU Privacy Guard.

HZ: Hercio.

I: Investigación (Parque I).

IDS: Intrusion detection system.

ILP: Information Leak Prevention.

ITM: Instituto Tecnológico Metropolitano-

KHZ: Kilohertzio.

MHZ: Megahercios.

MTRS: Metros

MTS: Metros

NFC: Near Field Communication.

PC: Personal Computer

RSA: Rivest, Shamir y Adleman.

SO: Sistema Operativo.

UML: Unified Modeling Language.

WLAN: Wireless local área network

CVEI: Clasificador y visualizador de exfiltracion de información

Introducción

El trabajo realizado en proyecto de grado lo compone una estructura secuencial donde se refleja el cumplimiento de los siguientes objetivos propuestos.

Objetivo General:

Proponer un método para la detección de exfiltración de información basado en los datos transmitidos por ultrasonido entre dispositivos computacionales a través de la captura, identificación y clasificación de la información.

Objetivos Específicos:

1) Definir un conjunto de componentes y características en hardware de computadores portátil y de escritorio que permitan transmisión ultrasónica susceptible de permitir exfiltración de información.
2) Desarrollar un método para la detección de eventos de transmisión de datos a través de fuentes ultrasónicas en un ordenador portátil y de escritorio.
3) Desarrollar un procedimiento de clasificación que permita establecer si los datos que se está transmitiendo son información relevante.
4) Evaluar el método diseñado para la detección de exfiltración de información.

Los avances tecnológicos en campos tales como las comunicaciones y la electrónica, han permitido innovar e implementar canales de comunicación utilizando como base las conexiones ópticas, eléctricas o las ondas electromagnéticas; éstas últimas, siguen potencializándose por la facilidad de viajar a través del vacío, además de ser ondas transversales que pueden ser polarizadas y alcanzar unas velocidades muy altas. Al poseer estas propiedades, los fenómenos físicos que afectan la

propagación de la onda (transmisión, absorción, reflexión, refracción, difracción o dispersión, difusión) son muchos menores en comparación con la afectación que se produce en la transmisión de las ondas acústicas. Las ondas acústicas, a diferencia de las anteriores, son mecánicas, elásticas y requieren un medio para viajar; además son ondas longitudinales, no pueden ser polarizadas y su velocidad de propagación depende de las características del medio en el que se transmite (presión, temperatura, densidad, humedad), y pueden extenderse hasta el rango de los gigahertz [1].

Dado lo anterior, la tecnología de comunicación inalámbrica utiliza ondas electromagnéticas que, variando su operación de frecuencia y protocolos de comunicación, determinan el rango máximo de cobertura y la tasa de transferencia de datos. Actualmente se encuentran tecnologías estandarizadas de conexión inalámbrica tales como el estándar 802.11 WI-FI, NFC, Bluetooth, Infrarrojos, Redes 2g, 3g, 4g, entre Otros [2].

Estos mecanismos son constantemente regulados y analizados en materia de vulnerabilidades, con el fin de reducir las distintas amenazas, que son creadas por personas con diferentes motivaciones y objetivos, por ejemplo, ciberterroristas, hacktivistas, delincuentes informáticos, delincuencia organizada, entre otros.

Como objetivos primarios de la seguridad informática se encuentran la integridad, disponibilidad y confidencialidad seguido de objetivos secundarios, pero no menos importantes como son la autenticidad, el no repudio o el aislamiento de la información. La integridad se refiere a que la información debe ser precisa, coherente y completa, la disponibilidad que debe estar accesible en el

momento que sea requerida; y la confidencialidad que debe ser protegida de accesos o divulgaciones no autorizadas. El detrimento de cualquiera de estos aspectos afecta a los dueños de la información y puede resultar en la pérdida de credibilidad, privacidad, e incluso legalidad de los datos de usuario; afectando tanto a personas naturales como a organizaciones [4].

Los sistemas informáticos son vulnerables a muchas amenazas que pueden ocasionar pérdidas insignificantes o catastróficas, desde riesgos de desastres naturales hasta dificultades técnicas; las pérdidas pueden aparecer por la actividad de intrusos externos a la organización, por accesos fraudulentos, por accesos no autorizados, por el uso erróneo de los sistemas por parte de empleados propios, o por la aparición de eventualidades en general destructivas [5]. Los efectos de las distintas amenazas posibles son variados, unos pueden comprometer la integridad de la información, otros degradar la disponibilidad de los servicios y otros estar relacionados con la confidencialidad. Una de las amenazas evidenciadas en el boletín estadístico de Kaspersky Labs para el año 2018 según la red de nube global Kaspersky Security Network (KSN) es el sabotaje o robo de información sensible a través de filtración de datos, caso en el que se ve afectada directamente la confidencialidad, aspecto de interés para esta investigación[6].

En el campo de seguridad se denomina exfiltración, a la filtración de datos o de información a una salida no autorizada de datos y que pueda generar pérdida del control de ésta por parte del propietario; en el mundo de la informática normalmente están relacionadas con ataques a sistemas informáticos para la sustracción de datos, y las consecuencias son cada vez mayores debido a la creciente importancia que se otorga a la información a nivel mundial y a la dependencia de las comunicaciones en las organizaciones. Una exfiltración se asocia directamente a la pérdida de

confidencialidad, de modo que la información que pertenece a un sistema informático termina siendo accesible para otros sistemas, su impacto despierta preocupación en organizaciones y particulares debido a que puede afectar la imagen pública, producir desconfianza e inseguridad o generar consecuencias a terceros [7].

Esa exfiltración puede deberse a asuntos técnicos o humanos, y usualmente implican la falla de procedimientos, herramientas, entre otros, que generan una falta de control de la información. Desde lo humano pueden presentarse malas prácticas, espionaje, entrega directa de información a terceros, falta de formación (exfiltración por desconocimiento), entre otras; mientras que desde lo técnico el problema radica en la dificultad de administrar los mecanismos de transmisión mediante los cuales viaja la información, debido a causas como las grandes cantidades de datos o la falta de maniobrabilidad de los sistemas, es por ello que la exfiltración de información es una amenaza grave a la seguridad [8].

Por otro lado, la creación de redes acústicas como una tecnología de comunicación que puede ser usada como un canal encubierto para transportar datos, es una amenaza considerable para la seguridad informática e incluso podría romper los objetivos de seguridad de los sistemas informáticos de alta seguridad, que no consideran la creación de redes acústicas como posible vector de ataque, así lo muestra el estudio reciente de los investigadores de la Universidad de Zhejiang en comandos de voz inaudibles; el reconocimiento de voz (SR) sistemas como Siri o Google Nowhave se ha convertido en un método cada vez más popular de interacción hombre-máquina, el desarrollo de DolphinAttack es un caso donde se presenta una técnica para hacerse con el control de los

asistentes de voz de los dispositivos. El equipo de investigación transformó los comandos de voz en ondas ultrasónicas, con frecuencias demasiado elevadas para los humanos, pero totalmente reconocibles por los micrófonos de los dispositivos actuales.

Este estudio, el ultrasonido se convierte en un impulso eléctrico en el dispositivo receptor (por ejemplo, un teléfono inteligente) y se restaura la señal original que contiene el comando de voz, no hay ninguna función especial en el dispositivo, es simplemente una característica del proceso de conversión. Como resultado, el dispositivo atacado escucha y ejecuta el comando de voz, facilitando el ataque, "DolphinAttack: comandos de voz inaudible" [9] a pesar de que estadísticamente no se encuentra que exista una tasa alta que reporte eventos de incidente de este tipo no significa que no pueda estar sucediendo tal es el caso del Malware BadBios que tiene la capacidad de hacer transferencia de datos a través de la acústica [10].

Así mismo, los accesos no autorizados suelen estar relacionados con los mecanismos de comunicación y almacenamiento más populares como son los dispositivos, redes y servidores, en los que se accede a la información a través de ondas electromagnéticas; sin embargo, hay algunos medios alternativos que han sido ciertamente menos explorados como las ondas ultrasónicas, por la inestabilidad que presentan para la transmisión de datos debido a su nivel de confiabilidad, velocidad y medio de transporte, se ha trabajado poco en la maniobrabilidad de este tipo de onda para la transmisión de datos [11].

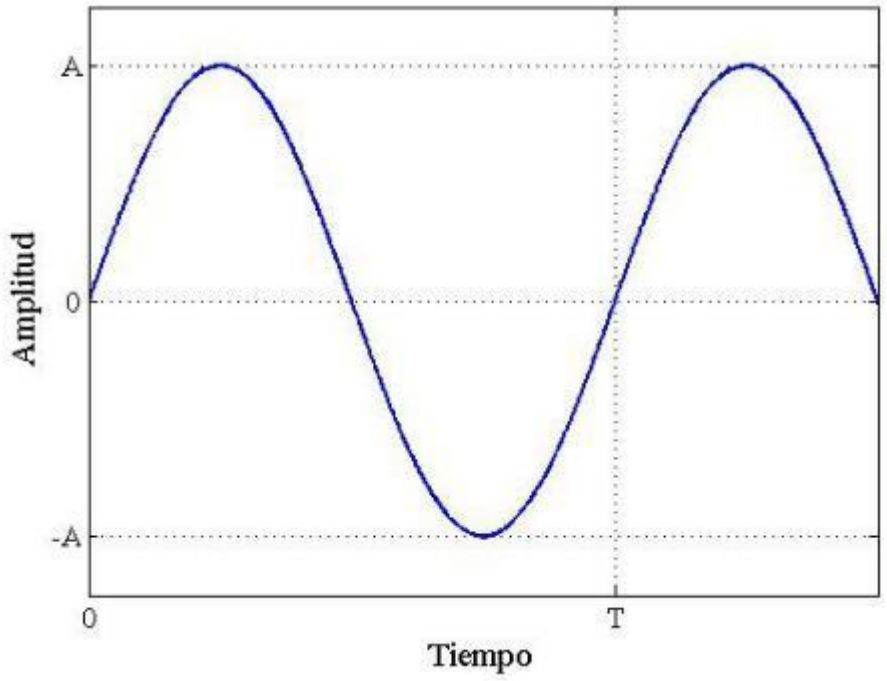
Para nuestro interés en particular, los equipos y sistemas de información pueden presentar exfiltración a través de variados mecanismos. Se puede decir que la multiplicidad de datos y ubicaciones presenta una situación de vulnerabilidad, pues la información descentralizada requiere

tratamientos especiales que permitan mantenerla a salvo, desde aspectos de hardware como la protección de los dispositivos, hasta el software y el aseguramiento de redes y servidores. También pueden presentarse pérdidas a través de programas maliciosos, ya que estos permiten acceder a los equipos y afectar la privacidad de forma directa, ejemplo de esto son los spyware y los keylogger. Además, pueden generarse debidas a errores técnicos o de configuración que dejan expuesta la información en espacios físicos o virtuales; por ejemplo, los protocolos sin cifrar que circulan en Internet pueden ser fácilmente interceptados por atacantes [12], pero vale recordar que los computadores presentan una exposición a la pérdida de información a través de sus periféricos de emisión y recepción de sonido que no solo se limitan a los altavoces y a los micrófonos, sino además a dispositivos como los ventiladores y discos duros que pueden ser manipulados para que dentro de su operatividad logren reproducir sonidos a un nivel ultrasónico permitiendo así la exfiltración de la información [11].

Teniendo en cuenta las múltiples amenazas a los sistemas, es posible que en el mercado se tenga una serie de soluciones contra la pérdida de datos, que pueden detectar los lugares en los que está almacenada la información, supervisarlos y evitar exfiltración o robos; entre estas se encuentran el Data Loss Prevention (DLP), Information Leak Prevention (ILP) y Content Monitoring Filtering (CMF), sin embargo este tipo de soluciones funcionan de diferentes formas, desde la clasificación de la información, hasta la aplicación de políticas preventivas acorde a un patrón de filtrado, pero no asociadas directamente al ultrasonido [12].

Adicional para complementar el trabajo propuesto, se utilizó para mostrar las medidas gráficamente de las frecuencias de sonido, ondas sinudoidal, gráficas y funciones, que se aprecia en la siguiente figura.

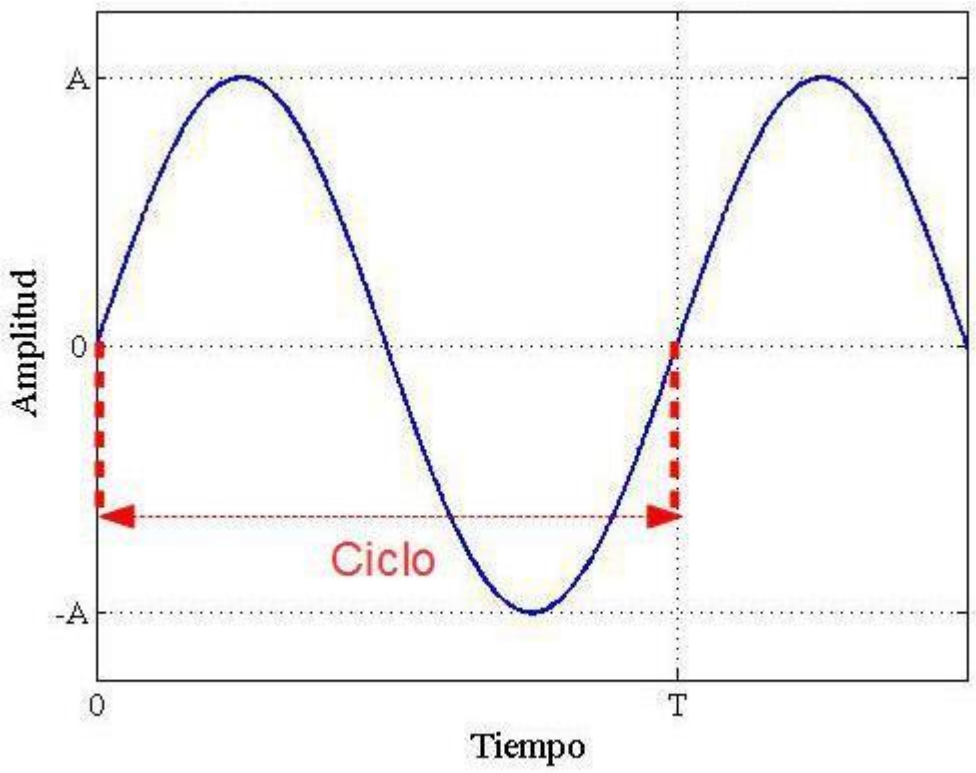
Figura 1: Onda Sinusoidal [13]**.**



En realidad, es una función que utiliza dos dimensiones de como varia la función seno en determinados valores de una variable, para nuestro trabajo es utilizada la función como caso en el tiempo. En la figura 1, se visualiza en el eje Y que se representa la amplitud, mientras que el eje X se representa el tiempo. De lo anterior se puede observar la variación y amplitud que se produce en determinado tiempo.

Normalmente indican las medidas que existen, ejemplo; en tiempos se puede encontrar segundos y en amplitud cualquier cosa que se desee graficar entre (decibelios d algún tipo, presión sonora, voltaje o intensidad eléctrica). Con lo anterior se tiene un mayor concepto básico de los trabajos que pueden ser usados con el sonido [13].

Figura 2: Ciclo, periodo y frecuencia [13]



En la imagen anterior está definido como ciclo, cuando se trata con señales que se repiten a lo largo del tiempo, se define un ciclo a todo lo que se comprende desde el punto de inicio hasta que se vuelve el mismo punto en la misma condición. El periodo es el tiempo que se tarda en producirse un ciclo y la frecuencia es el nuero de ciclos que se dan en un segundo, el periodo y la frecuencia están relacionadas cuanto menor sea el periodo más ciclos se van a dar en un segundo, y por lo tanto mayor será la frecuencia.

Los equipos computacionales de forma nativa pueden intercambiar ciertos datos e información a través de ultrasonido (programada o no), dichos datos podrían tener una relevancia en cuanto al

tipo y calidad, por lo cual, detectar posible información que sea transmitida por dichos medios no convencionales y que pueda considerarse reservada, genera una vulnerabilidad en términos de seguridad de la información, cuya mitigación es un reto para el área de las ciencias computacionales.

Lo anterior posee un agravante referido a los servicios actuales que están siendo orientados a las ejecuciones por comandos de voz, permitiendo el constante flujo, sin control y monitoreo, de ondas sonoras que son emitidas y receptadas por un dispositivo, comprometiendo eventualmente así la confidencialidad, integridad y disponibilidad de la información.

El trabajo de grado inicia con el marco teórico, el estado del arte que da soporte al desarrollo de la propuesta. Luego se continúa mostrando la metodología usada para dar cumplimiento a los objetivos, seguido de esta, se muestran los resultados obtenidos en cada uno de los objetivos propuestos. Así mismo se desarrolla en cada capítulo el estudio para la creación del software (marco de trabajo), la ejecución de este y los resultados de prueba generados a partir de un caso real.

El software que se propuso es la recopilación de buenas prácticas existentes en el sector de la seguridad de la información y de la informática, puesto que a través de este se definieron los artefactos, herramientas y aspectos metodológicos que permitirán al administrador del equipo de cómputo tomar medidas para vigilar su información, que le permitan mitigar la fuga de información transmitida a través de ondas ultrasónicas., por último se entregan conclusiones, recomendaciones y trabajo futuro en el desarrollo de la tesis.

5. Marco Teórico y Estado del Arte

5.1 Marco teórico

El ultrasonido es una onda mecánica que se encuentra por encima de los 20 000 Hz umbral que es imperceptible para el odio humano ya que este es capaz de reconocer frecuencias acústicas hasta los 20 000 Hz [14]. Actualmente las computadoras poseen características físicas en sus componentes electrónicos que permiten a través de una alteración de su comportamiento, generar este tipo de ondas en alta frecuencia, como ejemplo encontramos los altavoces, los ventiladores de los disipadores, los discos duros mecánicos y como dispositivos de recepción de este sonido se encuentran los micrófonos que vienen incorporados dentro de dichos dispositivos.

Por las anteriores características de estos dispositivos de hardware es posible que los usuarios de las máquinas finales tengan la posibilidad de desarrollar software que permita generar canales encubiertos de comunicación ya que el propósito por el cual fue desarrollado el dispositivo logra realizar una tarea o actividad adicional, en este caso crear un canal de comunicación que finalmente no es autorizado o informado por el dispositivo para lograr un propósito [15].

El canal encubierto es el medio que permite que se realice exfiltración de información, entiéndase por este término como el medio que le otorga funcionalidades al hardware de permitir que la información sea extraída del dispositivo sin ser este avisado ni autorizado por el usuario o el software administrador del dispositivo. Por tal motivo desde la década de los 70 se han implementados complejos estructurales que aíslan los dispositivos o computadoras de las redes de conexión para tratar de evitar

que se produzcan fugas o exfiltración de información a esto se le conoce como técnicas TEMPEST [16].

Con el propósito de lograr lo anterior, se ha definido una serie de fases que se describen a continuación:

Clasificación de información.

La clasificación de la información permite establecer una serie de patrones que permiten dar cuenta de qué tan sensible es la información que existe, para obtener una clasificación, se puede basar en el estudio de temas y metodologías neutrales y de reconocimiento nacional e internacionales del tipo: habeas data, información o secreto empresarial, información adaptable sobre técnicas tipo foot-printing o de reconocimiento en seguridad y que pueda revelar vulnerabilidades según la CVE [17], DLP, entre otras, para lo cual se realizará una adaptación e integración de la metodología diseñada para la detección de eventos de transmisión de datos sobre este tipo de canal de comunicación [12].

La clasificación de seguridad como concepto, resulta ser muy variable según la objetividad de las corporaciones, que a su vez se basan en normas de varios años atrás, lo que, para este momento digital, se pueden quedar cortas en el alcance de materia de seguridad ya que cada año el volumen informático crece en tamaño.

Se implementará una nueva definición de clasificación basado en el paper: "Una definición de la clasificación de seguridad de la información en Contexto de seguridad cibernética." En donde se aplicara una nueva base de clasificación de información basada en la recopilación de los diferentes

métodos como: COBIT, NIST, ISO, ISA, RFC, NERC en la que se actualiza y mejora de los componentes en la seguridad informática, la clasificación de la información digital es el resultado de la asignación de una categoría de seguridad a la información de acuerdo con los aspectos contextuales de esta información. Una categoría de seguridad deberá ayudar a proteger la información de eventos de filtración que podrían afectar involuntariamente los propietarios de esta información. La clasificación contextualizada debe tener en cuenta los cuatro riesgos: Riesgo atado por la naturaleza intrínseca de la información; Riesgos asociados con la propiedad de esta información; Riesgo legal; riesgo de almacenamiento de información"

Basada en la recopilación y reestructuración propuesta por los autores en la literatura se proporciona una nueva definición de la clasificación que se agrupa en 6 categorías de restricción de acceso a la información en la cual se toma las mejores prácticas de las normas: COBIT, NIST, ISO, ISA, RFC, NERC, y se definen los patrones que partiendo de una definición macro se pueda ajustar a la normativa singular según la forma de trabajo en las diferentes organizaciones privadas o gubernamentales. Con lo anterior se logrará una mayor atención enriqueciendo la clasificación de seguridad de información interdisciplinaria en la dialéctica de seguridad informática de una manera actualizada a la nueva gestión de la información.

Los 6 nuevos niveles para realizar una clasificación de información efectiva:

- Noción de: protección, la sensibilidad, la criticidad, valor, ciclo de vida, contextualización, uso, disponibilidad, integridad, evaluación de riesgos, el riesgo del propietario, y el riesgo de almacenamiento de información, riesgo legal que es el tema predominante en la definición del NIST.

- Noción de: información, protección, riesgo legal, sensibilidad, ciclo de vida, contextualización, uso, disponibilidad, la integridad, la evaluación de riesgos, el riesgo del propietario, y el riesgo de almacenamiento de información.
- Noción de: protección, del ciclo de vida, contextualización, uso, disponibilidad, integridad, evaluación de riesgos, el riesgo del propietario, y el riesgo de almacenamiento de Información.
- Noción de: contextualización, uso, evaluación de riesgos, el riesgo del propietario, y el riesgo de almacenamiento de información.
- Noción de: Sensibilidad, criticidad, Ciclo vital, Contextualización, Riesgo Legal, uso, disponibilidad, integridad, evaluación de riesgos, el riesgo del propietario, y el riesgo de Almacenamiento de Información.
- Noción de: protección, criticidad, del valor, del ciclo de vida, contextualización, uso, disponibilidad, integridad, evaluación de riesgos, el riesgo del propietario, y el riesgo de almacenamiento de información.[18]

Entenderemos el concepto de nivel de clasificación como: un componente basado en seguridad informática tradicional, del mismo modo en que es definido por Craigen, Diakun- Thibault y Purse en 2014: “La ciberseguridad es la organización recopilación de recursos, procesos y estructuras utilizados para proteger el ciberespacio y los sistemas habilitados para el ciberespacio de ocurrencias que no coinciden con jure de los derechos de propiedad de facto “. Esta definición resalta lo interdisciplinario de la seguridad cibernética. Nos muestra que este tipo de seguridad ahora tiene un alcance más amplio que la seguridad informática tradicional [18] .

Dada una recopilación de la literatura para redefinir el mejor procedimiento de clasificación extrayendo de cada teoría lo que es aplicable, se realiza una definición de grupos de clasificación a los cuales se les realiza un nombramiento basado en la norma ISO 27001 al cual corresponda un identificador que conglomere la mayoría de los atributos que califican los grupos. De tal manera a consideración se realiza el siguiente nombramiento:

Como concepto de secreto se entiende como: compartir información entre un grupo de personas, en la que se oculta a otros grupos la información. Dado esta definición es la representación dentro de las características de la noción de nivel más alto de importancia al grupo 1[18].

- Grupo 1: Secreto: Nivel más alto de clasificación de material en un nivel nacional o gubernamental. Como concepto de secreto se entiende como: derecho de la información, por la que se garantiza solo accesibilidad al personal autorizado a consultar la información. Dado esta definición es la representación dentro de las características de la noción del primer nivel de importancia.
- Grupo 2: Confidencial: Nivel de confidencialidad de la información se decrementa. Como concepto de confidencial se entiende como: limitar y disminuir la capacidad de acceso en un grupo considerable de participantes. Dado esta definición es la representación dentro de las características de la noción del segundo nivel de importancia al grupo 2.
- Grupo 3: Restringido: Para niveles medios de confidencialidad. Como concepto de restringido se entiende como: lo que está en la parte de adentro y que no tiene acceso externo. Dado esta definición es la representación dentro de las características de la noción del tercer nivel de importancia al grupo 3.

- Grupo 4: Uso interno: Información con un nivel bajo de confidencialidad. Como concepto de uso interno se entiende como: lo que puede ser accedido por todos. Dado esta definición es la representación dentro de las características de la noción del cuarto nivel de importancia al grupo 4.
- Grupo 5: Público: Todas las personas pueden ver la información. Como concepto de público se entiende como: cualquier tipo de información no perteneciente a ningún grupo con características particulares. Dado esta definición es la representación dentro de las características de la noción del quinto nivel de importancia al grupo 5.
- Grupo 6: Sin clasificar: Captación de información que no está en ninguno de los 5 grupos clasificatorios.

En la era de la información electrónica, las personas pueden compartir, acceder y difundir información en un volumen aparentemente ilimitado. La capacidad de difundir información en formato electrónico es enorme, al mismo tiempo la fuerza laboral se ha vuelto cada vez más móvil y la posibilidad del acceso a Internet de alta velocidad, los dispositivos móviles inteligentes y el almacenamiento portátil significa que "la oficina" puede estar en cualquier lugar. Como consecuencia, se ha vuelto más difícil que nunca para las organizaciones evitar la pérdida de datos confidenciales. Por lo tanto, las organizaciones buscan cada vez más las soluciones de prevención de pérdida de datos (DLP) para proteger sus datos confidenciales. Un sistema DLP típico puede incluir un analizador de protocolo de datos, un extractor de contenido textual, un motor de coincidencia de contenido y un motor de cumplimiento de reglas. Los datos analizados por un sistema DLP pueden ser procesados por cada uno de estos motores para determinar si debe ocurrir una acción de cumplimiento, como bloquear la transmisión de un archivo, poner en cuarentena un

archivo o crear una violación de seguridad. Los dos estados de más alto gasto a nivel computacional en DLP pueden ser la extracción de contenido y la coincidencia de contenido. Estas etapas de DLP pueden gravar numerosos recursos, lo que ocasiona tiempos altos de espera de aplicaciones, mayor carga en los procesadores de red y picos de unidades de procesamiento central en los sistemas locales. Debido al costo de la extracción y el emparejamiento del contenido, un DLP eficiente y completo puede no ser posible utilizando los sistemas DLP tradicionales en algunas situaciones [19].

Para realizar la detección de información ante una posible fuga de información, en la actualidad existe un método implementado por computadora para normalizar la información de categorización de prevención de pérdida de datos, al menos una parte del método que está siendo ejecutado por un sistema informático que comprende al menos un procesador, puede identificar un objeto de datos por primera vez. El método puede aplicar una primera versión de un conjunto de reglas de prevención de pérdida de datos al objeto de datos para determinar un conjunto de categorizaciones de datos del objeto de datos. El método puede aplicar, según el conjunto de categorizaciones, una primera política de prevención de pérdida de datos al objeto de datos. El método puede identificar el objeto de datos por segunda vez y aplicar, según el conjunto de categorizaciones basadas en contenido, una segunda política de prevención de pérdida de datos al objeto de datos. También se describen otros métodos, sistemas y medios legibles por computadora [19].

Para entender la funcionalidad, se describen los pasos a tener en cuenta:

- Identificar un objeto de datos a la vez
- Aplicar un conjunto de reglas de prevención de pérdida de datos al objeto de datos para determinar un conjunto de categorizaciones del objeto de datos
- Aplique, en función del conjunto de categorizaciones, una primera política de prevención de pérdida de datos para el objeto de datos.
- Identificar el objeto de datos por segunda vez.
- Aplicar, basado en el conjunto de categorizaciones basadas en contenido, una segunda política de prevención de pérdida de datos.

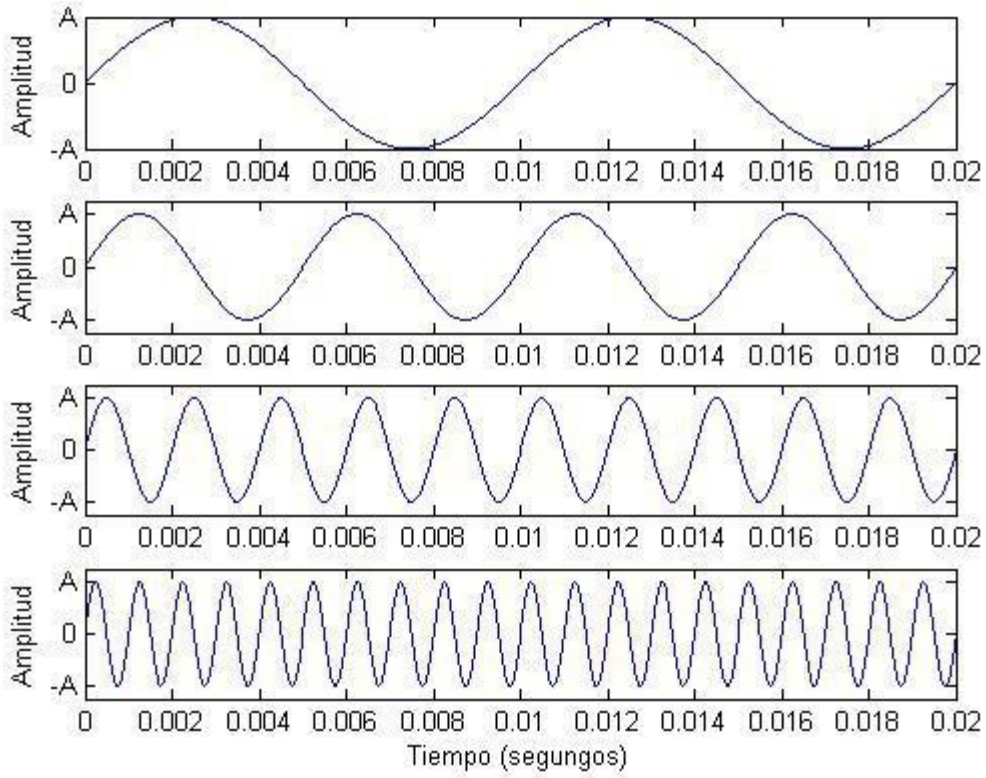
Una vez el método se encuentre desarrollado se realizó una implementación de software que se instaló en los dispositivos adquiridos donde se realizó la evaluación del comportamiento del método tanto en un ambiente controlado versus un ambiente real y se concluyó el porcentaje de cumplimiento por el software.

Para el de desarrollo de software se usó el lenguaje de programación (versión 3.7.3 libre) Python, un lenguaje de programación dinámico típico, usado cada vez más en muchos dominios de aplicaciones. Las características dinámicas en Python permiten a los desarrolladores cambiar el código en tiempo de ejecución. Algunas funciones dinámicas, como la comprobación dinámica de tipos, desempeñan un papel activo en las actividades de mantenimiento, por lo que el código dinámico de las características a menudo se cambia para adaptarse a la evolución del software. Aunque los programadores a menudo han mencionado las potentes funciones dinámicas de los lenguajes de programación como construcciones extremadamente útiles, los usos de las funciones dinámicas pueden modificarse durante la evolución del software. Por un lado, los usos de las características dinámicas desempeñan un papel activo en actividades de mantenimiento especiales,

por ejemplo, añadiendo la verificación dinámica de tipos para corregir errores de tipo. Como resultado, el código de función dinámico a menudo se cambia para atender las actividades de mantenimiento [20] .

En la siguiente figura se aprecia el tipo de señal sinusoides aumentando la frecuencia para apreciar el periodo cuando disminuye[13].

Figura 3: Frecuencias de 100hz, 200hz, 500hz y 1Khz [13]**.**



5.2 Estado del arte

En 1981, se realizaron varios estudios y experimentos que perfeccionan los métodos de comunicación a través de emisión de ondas ultrasónicas en submarinos. Las cuales, durante años anteriores, se han utilizado en la industria de la comunicación en el mar, basado en la modulación FSK (Frecuencia de modulación por desplazamiento). Estos requisitos limitan sistemas anteriores a muy bajas velocidades de datos, realizaron un módem acústico capaz de ordenar a mayor magnitud, el aumento en las tasas de datos. Esta mejora de módem acústico logra datos de mayores tarifas por la transmisión simultánea de múltiples tonos utilizando la modulación FSK [21].

En 2005 en la universidad de Oslo, Noruega. Se desarrolló un aplicativo capaz de transmitir información por medio de ondas de ultrasonido, apoyados en instrumentos electrónicos como: micrófonos, computadoras y otros complementos [22]. En un sistema de comunicaciones, -60 dB es un valor tan pequeño y conservador que se puede utilizar en el diseño de la comunicación ultrasónica. Los valores típicos son 50 - 300 ms. Los valores más grandes deben ser utilizados para las comunicaciones, como ejemplo: un largo pasillo con paredes de concreto, piso y techo. Esta asegura que la gama estará limitada por el ruido de fondo y no por las reverberaciones. Éste es identificado e interpretado por el aplicativo, después de tener datos concretos de las mediciones de estos sonidos, hallaron que las frecuencias emitidas eran interrumpidas y dispersadas por el entorno en que la que se encontraban los dispositivos en la habitación de pruebas, por tal detalle los datos transmitidos eran capturados de forma incompleta [22] .

En 2006, Lemay y Tan [23] demostraron experimentalmente que las emanaciones acústicas pueden ser manipuladas para transmitir datos arbitrarios entre dispositivos, adicional crearon un tipo de malware de recolección de datos de los periféricos (keylogger) de tipo acústico, demostrando cómo se puede utilizar dicho malware para enviar datos a través de ondas acústicas [23]. En octubre del año 2009, se logró perfeccionar la recepción y emisión de sonidos ultrasónicos de forma confiable, utilizando un compuesto orgánico llamado polimerización en los dispositivos; dichos compuestos fueron diseñados para ampliar el rango de cobertura hasta 2 MHz [24].

En Alemania en el año 2010 se realizaron experimentos basados en transmisión de datos con los que se logró un ataque por medio de ondas ultrasónicas, además de desarrollar un dispositivo capaz de capturar el 70% de información, en dicho ataque se logró demostrar, cómo texto impreso pudo ser reconstruido partiendo de una grabación capturada de una impresora de puntos, la técnica usada fue desarrollada realizando las comparaciones y fuerza del sonido cuando las cabezas de la impresora golpeaban el papel, de acuerdo a lo fuerte o leve del sonido , se mapeaba la letra impresa con el sonido [25].

En noviembre del año 2013 se informó sobre un laboratorio que fue atacado por un virus que se instalaba en la BIOS de las computadoras y como característica adicional que se esparcía a través de ondas en ultrasonido por los periféricos como micrófonos y altavoces, a raíz de esto se realizaron varias investigaciones en laboratorios. En 2014 en Alemania demuestran que se puede utilizar este medio de comunicación como un canal secreto, para modular la frecuencia de la señal

y desmodular, si es posible, la transferencia de información sin que el sistema y el usuario sean percatados [6], [26].

En 2014 investigadores basados en los estudios realizados en Alemania en 2013, lograron perfeccionar los métodos de recepción y envío de información con desarrollos de software que llamaron QuitChat y DogWhisper respectivamente, reduciendo la tasa de pérdida de información por paquete enviado entre dos computadoras y logrando que sea posible la comunicación entre dispositivos con más del 80% de efectividad en el envío de información [27].

Son variados los mecanismos que pretenden tomar el control del equipo a partir de códigos maliciosos, y forzarlo a ejecutar la encriptación y transmisión de la información a través de canales secretos, que pueden pasar desapercibidos para los usuarios de los dispositivos y los instrumentos de control de flujo de la información. Encontramos que estudios llevados a cabo por estudiantes de doctorado de la Universidad Ben-Gurionen en Israel, demostraron que es posible el intercambio encubierto de datos, entre dos ordenadores en una proximidad cercana, por medio del control de las emisiones de calor; uno de los computadores se encargaría de encriptar la información y generar las emisiones de acuerdo a un código malicioso, y el otro de recibirlas a través del sensor de calor, descifrarlas y filtrar los datos [28].

Así mismo, Mordejai Guri investigador de la misma universidad israelí, ha estudiado acerca de las fugas de información y presentado varios avances en la materia. Guri generó una técnica para la filtración de datos de un ordenador asilado a un teléfono móvil, a través de ondas de radio; y con

un equipo de investigación desarrolló un canal secreto para la transmisión de información a través de señales ultrasónicas generadas por el disco duro del computador[29].

Por otro lado, en Estados Unidos Luke Deshotels [30] trabajó en la transferencia de datos entre dispositivos móviles mediante dos mecanismos, el primero son las señales ultrasónicas y el segundo unas vibraciones sutiles con información encriptada; ambos canales pueden pasar encubiertos y generar pérdidas de información [30].

En las últimas investigaciones realizadas, se encuentra que se están potencializando los canales encubiertos de ondas acústicas, para que la información y / o software malicioso que viaja a través de estos canales sea cada vez más difícil de ser percibida por los usuarios o el software que tiene como fin detectar los ataques [31].

En el año 2013 investigadores revelan que existe vulnerabilidades que amenazan la seguridad de nuestra información, mediante medios de comunicación acústico encubierto en el aire, esto pudo eludir las políticas de seguridad de los componentes de un sistema informático, dado esto, se despertó gran interés por un grupo de investigadores que lograron publicar el concepto y la implementación de una red de malla acústica encubierta en el aire, identificando qué canales encubiertos pueden utilizarse para eludir las directivas del sistema y de la red, esto, mediante comunicaciones que no fueron considerados en el diseño del sistema informático origen, además demostraron que el concepto de una red de malla acústica encubierta tiene muchos conceptos de seguridad convencionales inútiles (ruido, datos basura, etc.), finalmente en este trabajo discuten

las contramedidas contra las redes de malla acústica encubiertas, incluyendo el uso de filtros de paso bajo en los sistemas de computación y un sistema de detección de intrusiones (IDS por sus siglas en inglés Intrusion detection system) basado en host para el análisis de entrada y salida de audio, con el fin de detectar cualquier irregularidad. A lo anterior, proponen para futuros trabajos implementar un IDS de audio dentro de un componente del sistema operativo para la detección de ultrasonido [9].

En [32] se demuestra que a través de computadoras que emiten un ruido agudo que emiten un ruido agudo durante su funcionamiento, y debido a su vibración en algunos de sus componentes eléctricos las señales acústicas pueden transmitir información de acuerdo al software en que se ejecute y también es particular a la información que se pueda exfiltrar en términos relacionados con la seguridad . También describen un nuevo ataque de extracción de clave de criptoanálisis acústico, aplicable a la actual implementación de RSA por GnuPG. El ataque puede extraer las claves de cifrado RSA de 4096 bits completas de computadoras portátiles (de varios modelos), en una hora, utilizando el sonido generado por el ordenador durante el cifrado de algunos textos cifrados elegidos, a esto demostraron experimentalmente que tales ataques se pueden realizar, usando un teléfono móvil colocando al lado del ordenador, o un micrófono más sensible colocado a 4 metros de distancia [32].

Luego de un análisis, investigadores revelan que un malware futuro podría utilizar comunicaciones acústicas encubiertas, siendo capaz de extraer información de computadoras que no tienen ningún tipo de conexión alguna en redes Ethernet, Wifi o WLAN, entre otras [9].

Un análisis de algunos investigadores encontraron que una red encubierta podría ser oculta al ejecutar el sistema de comunicación como un proceso de fondo en el sistema informático, lográndose implementar mecanismos de ocultación avanzados [33]. Basado en esto se podría decir que una red encubierta podría estar operando en un estado sigiloso, enviando datos importantes como contraseñas y claves de cifrado, así la red encubierta podría estar oculta en términos de prevenir la detección humana a altos niveles de volumen utilizando únicamente el rango de frecuencia ultrasónica [6]. Pero para entablar una Buena comunicación a través de ultrasonido fue necesario que investigadores diseñaran herramientas que mejoraran el alcance , la precisión y la no detección de los canales acústicos encubiertos, logrando explotar cuatro implementaciones existentes para transmitir señales a través de ultrasonido, a partir de esto diseñaron un nuevo sistema que consigue un mejor rango de trabajo y mejor precisión, también implementan un sistema capaz de extender la no detección a dispositivos de escucha menos limitados [27].

En el año 2014 investigadores implementaron un IDS de audio adaptativo. El cual tiene como funcionalidad extraer y analizar un segmento de tiempo de una señal pregrabada, también extrae diferentes características de señal en señal para un análisis posterior. Por medio del IDS de audio automático, logran caracterizar las señales, que luego son almacenadas como una firma de una señal conocida. Luego al tener las firmas almacenadas, durante el funcionamiento del IDS de audio, los datos de la señal en tiempo real, se comparan con las firmas almacenadas. Como resultado lograron identificar coincidencias, generando a su vez una advertencia de intrusión con respecto a la detección de una señal de audio conocida [6].

Investigadores en el año 2017, logran desarrollar un sistema ultrasónico que interactúa con los sistemas de reconocimiento de voz más populares, como el software Siri, Google Now, Samsung S Voice, Huawei HiVoice, Cortana y Alexa, Al inyectar una secuencia de comandos de voz inaudibles presentan algunos ataques que logra activar Siri y le dan la instrucción de realizar una llamada FaceTime en Iphone o activar el modo avión el dispositivo en Google Now. A su vez propusieron soluciones de defensa tanto en hardware como en software, la posibilidad de clasificar los audios utilizados en la máquina, y sugieren rediseñar los controladores de voz para que sean resistentes a los ataques inaudibles de comandos de voz, a través de comunicación ultrasónica [34], sin embargo, no hay una solución clara a la vista de cómo detectar posible información que sale a través de ultrasonido (controlar éste) y que es generado desde componentes informáticos.

Finalmente, investigadores lograron comprobar que por medio de dispositivos como auriculares o audífonos de forma encubierta pueden intercambiar datos a través de ondas ultrasónicas. No se requieren micrófonos. El método se basa en la capacidad de un software malicioso para explotar una característica chip de audio específico con el fin de revertir los altavoces conectados de dispositivos de salida en los dispositivos de entrada - discretamente ellos representan los micrófonos. Se demuestra que, aunque los altavoces / auriculares / cascos invertidos no fueron diseñados originalmente para funcionar como micrófonos, todavía responden bien a la gama por ultrasonidos (18 kHz a 24 kHz). Evaluaron el canal de comunicación con diferentes equipos y en diferentes distancias y velocidades de transmisión, y obtuvieron algunas consideraciones prácticas s tener en cuenta. Los resultados muestran que la comunicación por medio de Altavoces puede ser utilizado para transmitir de forma encubierta datos entre dos ordenadores a una distancia máxima

de nueve metros de distancia el uno del otro. Lo anterior permite que de 'auriculares a auriculares' se puede establecer una comunicación secreta [35].

6. Metodología

La investigación es de tipo cuantitativo y está soportada por el método inductivo, según el cual se logrará llegar a premisas generales, partiendo de variables específicas; además se hará una descripción del fenómeno.

En cuanto a la recolección de datos se utilizará un sensor ultrasónico para identificar las fuentes de emanación de ondas ultrasónicas, y se identificará, caracterizará y procesará la información obtenida en diferentes ambientes, basado en las estadísticas de muestras que se obtengan de los estudios de las fuentes de dichas ondas sonoras en ambientes controlados, áreas de trabajo y lugares domésticos, para identificar el comportamiento y lograr la detección de la información ex filtrada. En este estudio se medirán de forma independiente las variables recolectadas en el muestreo de los diferentes ambientes de prueba, para la caracterización y almacenamiento de la información.

Con el crecimiento de los dispositivos portátiles que contienen una unidad de procesamiento central en este trabajo se seleccionaron los notebook o portátiles como unidades de prueba, debido a la versatilidad que manejan precisamente por su diseño compacto y portable, permiten realizar pruebas con los mismos componentes en diferentes sitios, además los dispositivos lanzados al mercado después del año 2015 cuentan con integración en hardware en los micrófonos y altavoces necesarios para llevar a cabo la muestra del proyecto, en algunos dispositivos de escritorio estos periféricos se tienen que conseguir externamente y la intención del proyecto fue realizarlo con hardware incorporado e integrado directamente de fábrica.

De acuerdo con los criterios: de uso y propósito de los equipos de cómputo en este caso oficina y hogar, se incluye un ambiente de laboratorio para evaluar comparar y acondicionar propiedades ideales en las que es más efectiva una comunicación entre dispositivos sin interferencia de ruidos o material externo que afectase la comunicación estos se detallan más adelante.

Basados en las estadísticas de los computadores portátiles más comercializados y de mayor demanda para el año 2016 y 2017, se recolectara información de 2 máquinas en las cuales se analizara los componentes de hardware que, basados en análisis experimentales propuestos en la literatura, puedan y sean emisores y receptores de ondas acústicas con capacidad ultrasónica en dos tipos de entorno: Ambiente libre de ruido (Instalaciones del Instituto Tecnológico Metropolitano parque I, sede fraternidad, laboratorio de artes digitales) y Tipo oficina (Simulando el entorno empresarial que posean varios equipos de cómputo en un mismo sitio). Una vez identificado cada uno de los dispositivos se evaluará los rangos de inicio y de límite de onda ultrasónica, para delimitar el umbral con el que se trabajará en los dispositivos.

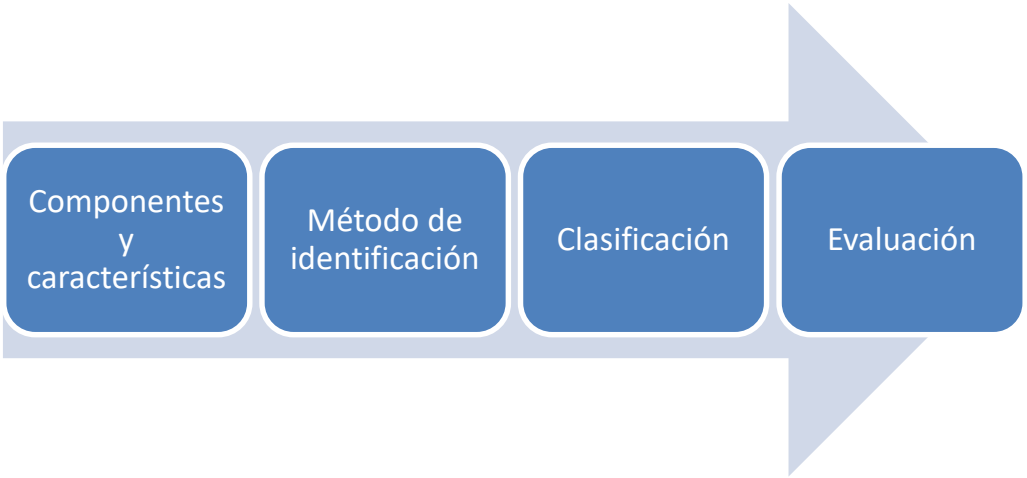
Una vez realizado el estudio lógico y físico de las posibles fuentes de recepción y emanación de ondas se procederá a evaluar el comportamiento de las frecuencias que estén en el umbral ultrasónico y acústico que permitan desarrollar el modelo estadístico de identificación de un patrón que garantice que se está transmitiendo información, en un entorno no controlado las fuentes de emanación acústica pueden surgir de otros dispositivos, por ende para garantizar que los eventos son producidos por el mismo dispositivo, se realizará un estudio del comportamiento de los

dispositivos para clasificar el comportamiento bajo experimentación cuando se produce un envió de información modulado y demodulado a diferentes frecuencias.

Para el desarrollo de las pruebas el primer caso de estudio fue demostrar que los equipos soportaban él envió y la recepción de ondas ultrasónicas en los 2 ambientes, en las pruebas de comunicación aún no se enviaba información, se enviaba una señal sonora en frecuencia ultrasónica esto con el fin de tomar la muestra de la capacidad receptiva y emisora de los equipos, después vendría como tal las pruebas de envío de información en cadenas de texto, ya que el objetivo de este trabajo no fue en centrarse en la infección de los dispositivos y el modo de recolección de información dentro de una máquina ,se centró como tal en enviar información del tipo cadenas de texto codificadas en frecuencia ultrasónica para el establecimiento del canal de comunicación entre los dispositivos. Como prueba adicional se realizan pruebas en dispositivos móviles de su capacidad, también de envío y de recepción de ondas ultrasónicas, pero no se profundiza en el envío y recepción de información dado que no hace parte del alcance de proyecto.

A continuación, se describe la metodología empleada para el desarrollo del proyecto:

Figura 4: Fases de la metodología. Fuente propia.



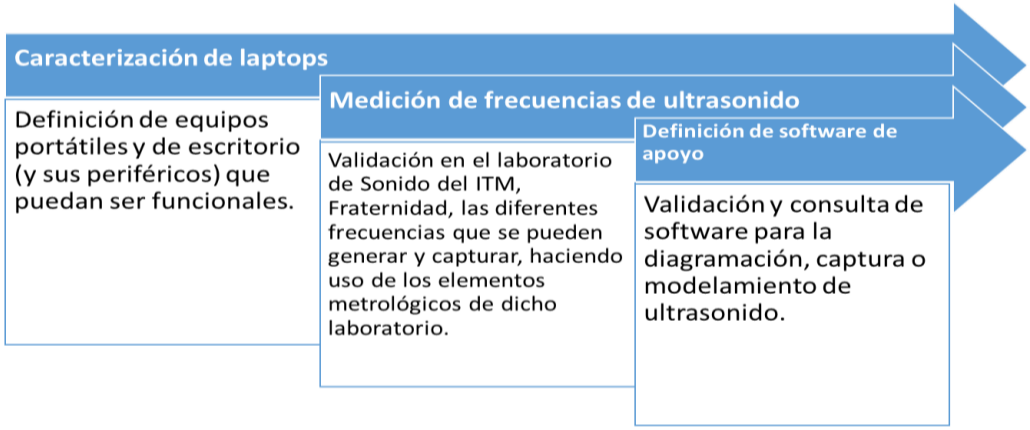
6.1 Fase 1: Componentes y características

Definir un conjunto de componentes y características en hardware de computadores tipo portátil y de escritorio que permitan transmisión ultrasónica susceptible de permitir exfiltración de información.

En esta fase se determinaron los equipos de cómputo capaces de generar ondas acústicas en frecuencia ultrasónica (por encima de los 20 Ghz), adicionalmente se analizó la capacidad de frecuencia que emite y recibe los dispositivos integrados en los equipos de cómputo tipo laptop y el software necesario para la transferencia y recepción de ultrasonido.

En la siguiente figura se muestra el procedimiento ejecutado para identificar las condiciones técnicas de los equipos:

Figura 5: Proceso de caracterización y medición de ultrasonido. Fuente Propia.

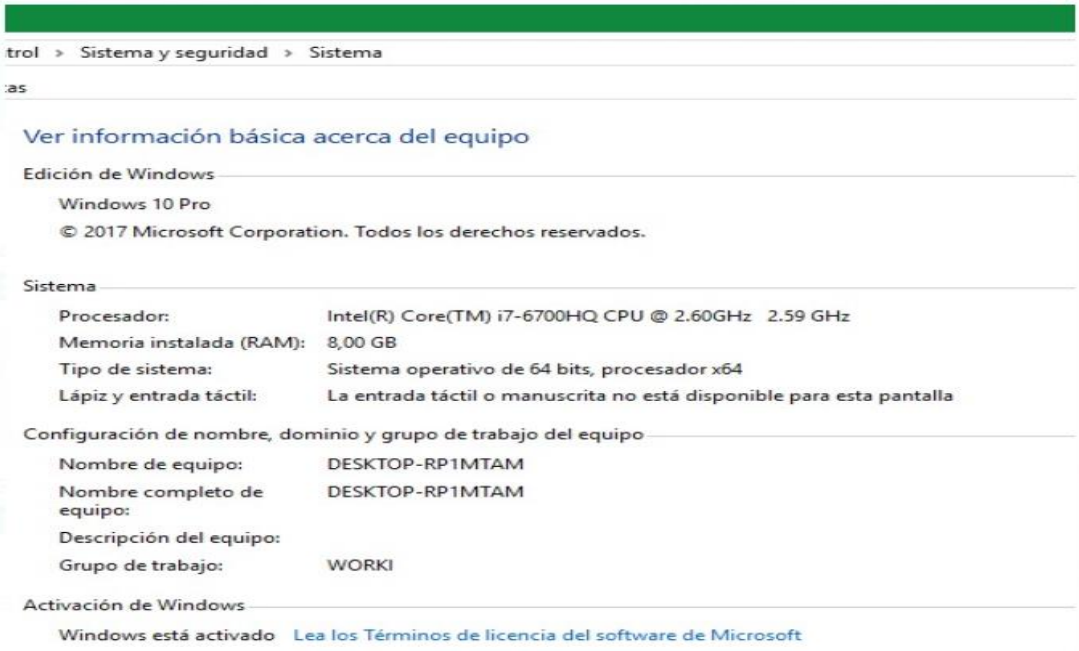


I. Caracterización de Laptops.

Utilizaremos dos equipos de cómputo tipo laptop marca ASUS. A continuación, se relaciona las características de cada equipo.

a) Equipo 1: Asus GL555VW - año de fabricación 2016.

Figura 6: Especificaciones técnicas equipo de cómputo. Fuente propia.



b) Equipo 2: Asus A555L – año de fabricación 2016.

Figura 7: Especificaciones técnicas equipo de cómputo. Fuente propia.

II. Medición de frecuencias de ultrasonido:

Para la definición del conjunto de componentes, se realizó primero diferentes pruebas de laboratorio con micrófonos de alta gama, con el fin de identificar los rangos de frecuencia en que se puede detectar el ultrasonido. Las pruebas iniciales se realizaron en los laboratorios digitales del parque I del ITM, en Fraternidad (en la figura 4 se encuentran las características del laboratorio) y se usaron los siguientes micrófonos de alta gama:

Tabla 1: Micrófonos empleados para las pruebas. Fuente obtenida en la página web del fabricante.

Modelo Micrófono	**Descripción Técnica**	**Respuesta en frecuencia**
tlm103 Neumann	El TLM 103 también ha establecido nuevos estándares para el desempeño técnico. Con un ruido propio increíblemente bajo de solo 7 dB-A, se encuentra entre los micrófonos más silenciosos disponibles. Y su alta sensibilidad de 23 mV / Pa garantiza un ruido ultra bajo incluso con preamplificadores de bajo presupuesto e interfaces de audio o equipos de tubo vintage. Al mismo tiempo, el TLM 103 puede manejar enormes niveles de presión de sonido de hasta 138 dB sin la necesidad de preatenuación. Su vasto rango dinámico de 131 dB hace que el TLM 103 sea un micrófono de estudio muy fácil de usar, ya que	45 Hz - 18,000 Hz

	capturará cualquier cosa, desde un susurro suave hasta un atronador tambor sin añadir ruido ni distorsión. https://en-de.neumann.com/tlm-103	
Re20 Electrovoce	El micrófono cardioide dinámico RE20 es verdaderamente un estándar de la industria, uno de los favoritos de los difusores e ingenieros de sonido de todo el mundo. Su popularidad también se extiende a la producción musical como un micrófono de instrumento de calidad superior. Su diseño Variable-D ™ y su filtro pop interno de alto rendimiento son excelentes para trabajos de voz cercanos, mientras que un elemento interno de montaje contra golpes reduce el ruido inducido por vibraciones. https://www.electrovoice.com/product.php?id=91	45 Hz - 18,000 Hz
shure sm57	Micrófono dinámico de instrumento de directividad cardioide que ofrece una reproducción limpia de los instrumentos amplificados y acústicos. Dispone de una respuesta en frecuencia modelada para conseguir una reproducción vocal de gran riqueza, reducción del ruido de fondo y sistema antigolpes neumático. https://www.shure.es/productos/microfonos/sm57	40 a 15.000 Hz
XYH-6 Stereo Mic	La cápsula XYH-6 emplea dos micros unidireccionales de alta calidad colocados en ángulo que son sensibles a señales	40 a 17.000 Hz

	provenientes de la parte frontal pero menos a las señales provenientes de los laterales y parte posterior. La grabación X/Y es óptima cuando quiere cubrir una amplia área y aun así capturar una fuerte imagen central. https://www.zoom-na.com/es/products/accesorios/zoom-xyh-6-xy-c-psula-de-micr-fono-est-reo	
MSH-6 Stereo Mic	Nivel de precisión en su capacidad para dar forma al sonido. La MS Capsule contiene elementos de micro duales: un micrófono orientado hacia adelante, unidireccional (el "Mid") y un micrófono orientado hacia el lado, bidireccional (el "lado"). Junto con el decodificador MS a bordo proporcionado por el H5 y el H6. https://www.google.com/search?ei=1zMhXayhE8W05gLol4bABw&q=MSH-6+Stereo+Mic&oq=MSH-6+Stereo+Mic&gs_l=psy-ab.3..0i22i30.1362.1362..2512...0.0..0.156.156.0j1.....0....2j1..gws-wiz.X3XRBJjAUz4	40 a 17.000 Hz

Con los micrófonos que se mencionan anteriormente, se recrearon diferentes pruebas desde los equipos de cómputo, con el objetivo de obtener un nivel más óptimo de capturar de frecuencia de ondas ultrasónicas emitidas desde otros dispositivos, logrando así identificar que otros componentes externos le pueden dar más rendimiento a la captura de este tipo de ondas desde los equipos de cómputo, realizando la respectiva captura y toma de datos finales.

Describiendo todo lo anterior, para las pruebas se tendrán los siguientes componentes los cuales ayudaran a determinar cuál es el medio más óptimo para realizar capturas y emisión de ondas ultrasónicas; se utilizara los equipos de cómputo mencionados anteriormente los cuales tienen integrados su propio micrófono, auricular y driver, también, se utilizara los micrófonos externos provenientes del laboratorio del ITM , además se usarán periféricos como diademas que integran altavoz y micrófono los cuales serán conectados a los equipos de cómputo.

Se definieron los siguientes escenarios para las pruebas:

- **Lugar:** Instalaciones del Instituto Tecnológico Metropolitano parque I, sede fraternidad, se relacionan las especificaciones del laboratorio de artes digitales, que se ilustran en la Figura 08.

Figura 8: Especificaciones Laboratorio Artes Digitales. Fuente Instituto Tecnológico Metropolitano.

Institución Universitaria	FICHA TECNICA DE LABORATORIO	Código	FGL 006
		Versión	01
		Fecha	2011-05-03

I. Información Administrativa			
Laboratorio	ARTES DIGITALES	Fecha Actualización	08/06/2017
Responsable		Formación	
Jorge Mario Valencia Upegui		Ing. Electrónico – Master of Arts in Music Technology	
II. Información Física			
Ubicación	Sede Parque i, Nivel 3	Área Física	133.28m²
Instalaciones Especiales		Dotación Seguridad Industrial	
Estudio de grabación de audio. Estudio de producción audiovisual con sinfín.		N/A	
III. Información Técnica y Tecnológica			
Puestos de Trabajo	Dotación		
Puesto de docente – Jorge Mario Valencia Upegui	Computador iMAC - Escritorio		
Puesto de docente – David Sánchez	Computador iMAC - Escritorio		
Puesto de Estudiante investigador	Computador PC - Escritorio		
Estación Investigadores	Computador PC - Escritorio		
Estación Audio 7.1	Interfaz MOTU – Sistema 7.1 KRK Rokit		
Estudio de Grabación de Audio	MAC PRO – Consola Yamaha 02R – Controlador MIDI M-Audio – Interfaz Apogee – Channel Strip Avalon – Batería Electrónica Roland – TV Samsung Smart TV – Sistema 5.1 Genelec – Monitores Dynaudio.		
Software utilizado		Herramientas y accesorios en general	
Avid Protools 10 y 12 – NI Komplete – East West EWQLO – Celemony Melodyne – Steinberg Wavelab – Bocaligne - Adobe CS – Office 2011 – Unity – Izotope Ozone – Wwise		Micrófonos: AKG C414 (2), Neumann TML 103 (2), Neumann KM184 (2), EV RE20 (2), Shure SM57 (2), RODE videomic Pro. Audífonos Sony MDR 7506 (5) Cámaras: Canon 5D Mark II, Canon 6D (2), Go Pro Hero 3. Amplificador de audífonos. Juego de cromas, Kit de Luces. Importadora de video Matrox. Tarjeta de sonido M-Audio Fastrack Pro. Grabadora de campo TASCAM. Sensor de reconocimiento de movimiento (2). Multímetro (2). Proyectores: Panasonic PT-EX12KU con lente, Panasonic PT-VW440.	
IV. Estadísticas Generales			
Programa		Asignaturas que sirve	
- Tecnología en Informática Musical - Artes de la grabación y producción musical - Artes Visuales - Cine - Maestría en innovación de la educación		- Semillero de creación de productos audiovisuales VISUS - Semillero Técnicas de Grabación de Audio TECNIGRAU - Semillero de modelamiento matemático	

- **Escenario 1, tipo oficina:** El escenario recrea todas las condiciones de la vida cotidiana de una oficina, donde se encuentran elementos, equipos de cómputo, impresoras y ruido del ambiente incluyendo las voces de las personas.
- **Escenario 2:** Ambiente cerrado libre del ruido. Para replicar en condiciones ideales cual sería la mejor condición del ambiente para lograr una mejor comunicación entre los dispositivos.

En cada uno de los escenarios, se probó el siguiente software/hardware:

- **Portátil tipo laptop:** Asus GL555VW, Asus A555L.

- **Micrófonos Externos:** tlm103 neumann, Re20 Electrovoce, shure sm57, XYH-6 Stereo Mic, MSH-6 Stereo Mic.
- **Software:** Smaart V8, Praat, Ultrasound, Quinet, GnuRadio, Audacity,Izotope.

III. Software de apoyo para generar frecuencia y analizador de espectro.

Para realizar las pruebas se utilizó el software de apoyo que se encuentra en el mercado, cuya utilidad es generar frecuencia y analizar el espectro de frecuencia emitidos o trasmitidos desde un dispositivo móvil o equipo de compto tipo laptop, los cuales fueron instalados y probados, con el objetivo de demostrar que existe una variedad de aplicaciones enfocadas a utilizar ondas ultrasónicas para muchos fines en común, y para nuestro el de demostrar que nuestros dispositivos son susceptibles a este tipo de señales. Todas las aplicaciones que se listan a continuación, cumplieron con todas las características necesarias para capturar o emitir ondas ultrasónicas, dado que las aplicaciones evaluadas ofrecen la parametrización de rangos para generar y capturar frecuencias de hasta unos 22.000 hz.

- **Smaart V8:** En su esencia, Smaart es una plataforma FFT de doble canal basado en computadora que utilizado en el campo de la ingeniera de audio para ver el contenido de frecuencia de las señales o medir la respuesta de nuestros sistemas eléctricos y electroacústicas. Demo gratuito con vigencia de 30 días. Para mayor comprensión utilizar enlace de la página oficial https://www.rationalacoustics.com/smaart/smaart-v8/

- **Praat:** Praat es capaz grabar la voz en varios tipos de archivos de audio y mostrar los espectrogramas. Además, permite el análisis de la entonación, la intensidad o volumen, los formantes, cocleagrama, etc. Praat también puede ser automatizado para análisis más complejos, lo que ha resultado útil para investigadores de alto nivel. Por lo que se pueden calcular valores de jitter, shimmer, entre otros, y utilizarlos para la clínica de análisis acústico. Demo gratuito con vigencia de 30 días. Para mayor comprensión utilizar enlace de la página oficial https://praat.softonic.com/

- **UltraSound Detector for Android:** UltraSound Detector es la aplicación que le permite detectar señales acústicas de ultrasonido (ultrasónicas) por encima de la frecuencia definida por el usuario (por encima de 18 KHz por defecto). Para detectar la presencia de la tecnología de seguimiento ultrasónico de dispositivos cruzados en algunos lugares públicos. La tecnología incorpora tonos de alta frecuencia que son inaudibles para los humanos en anuncios, páginas web e incluso ubicaciones físicas como tiendas minoristas. Demo gratuito con vigencia de 30 días. Para mayor comprensión utilizar enlace de la página oficial. https://download.cnet.com/UltraSound-Detector/3000-2141_4-77575119.html

- **Audacity:** Es una aplicación informática multiplataforma libre, que se puede usar para grabación y edición de audio, distribuido bajo la licencia GPLv2+. Es el editor de audio y sonido más difundido en los sistemas del planeta GNU/Linux. Demo gratuito con vigencia de 30 días. Para mayor comprensión utilizar enlace de la página oficial https://www.audacityteam.org/

- **iZotope V5.01.184:** iZotope es una herramienta muy poderosa para editar y optimizar archivos de audio. Con este software, puede importar sus archivos de audio que no son de buena calidad al software y con herramientas. Optimice los distintos tipos de archivos. Este software también tiene la capacidad de editar archivos, que puede aplicar y guardar efectos en el archivo de audio además de crear sus propios archivos. El formato de audio es compatible para que pueda importar sus archivos de audio sin cambiar el formato con el comando Arrastrar y soltar. También puede guardar sus archivos en diferentes formatos al guardar. El Editor de audio avanzado iZotope RX se puede usar para eliminar el ruido o el sonido que distrae de una herramienta analítica. Se puede instalar en diferentes Windows 10 e instalar en Cuenta con sistemas de 32 bits y 64 bits. Demo gratuito con vigencia de 30 días. Para mayor comprensión utilizar enlace de la página oficial https://appdb.winehq.org/objectManager.php?sClass=version&iId=34745

Adicional, se utilizaron las siguientes referencias de dispositivos móviles y software generador y emisor de frecuencias ultrasónicas.

- **Motorola G5, SO Android**.
    - Utilizamos Software Generador de frecuencia.
    - Para capturar información, usamos el software ultrasound detector

- **IPhone 6.**
    - Para generar frecuencia utilizamos el software generador de frecuencia.

Analizador de espectro.

IV. Software de apoyo para transmitir información de un equipo a otro.

Las dos aplicaciones que se mencionan a continuación, fueron para el caso del proyecto interpretados como el Malware, los cuales tienen la funcionalidad de enviar información de un equipo de cómputo a otro.

- **Quietnet - master:** Programa de chat utilizando frecuencias sonoras y ultrasónicas. Funciona sin wifi o Bluetooth y no se mostrará en un pcap. Software libre - gratuito. Para mayor comprensión utilizar enlace de la página oficial https://github.com/Katee/quietnet/blob/master/Readme.md

- **GnuRadio:** Es una herramienta de desarrollo libre y abierta que provee bloques de procesamiento de señal para implementar sistemas de radio definida por software. Puede utilizarse con hardware de RF de bajo costo para crear radios definidas por software, o sin hardware en un ambiente de simulación. Es utilizada extensivamente por ambientes académicos, aficionados y comerciales para dar soporte a la investigación en comunicaciones inalámbricas y en sistemas de radio en el mundo real. Software libre - gratuito. Para mayor comprensión utilizar enlace de la página oficial https://www.gnuradio.org/

V. Framework de apoyo para interpretar las ondas ultrasónicas a través de un gráfico.

Se seleccionó la librería de audio Qt5, para integrarlo al software que se desarrolló para este proyecto, con el fin de demostrar la variación en una gráfica en el momento que se genera una onda ultrasónica en el equipo de cómputo.

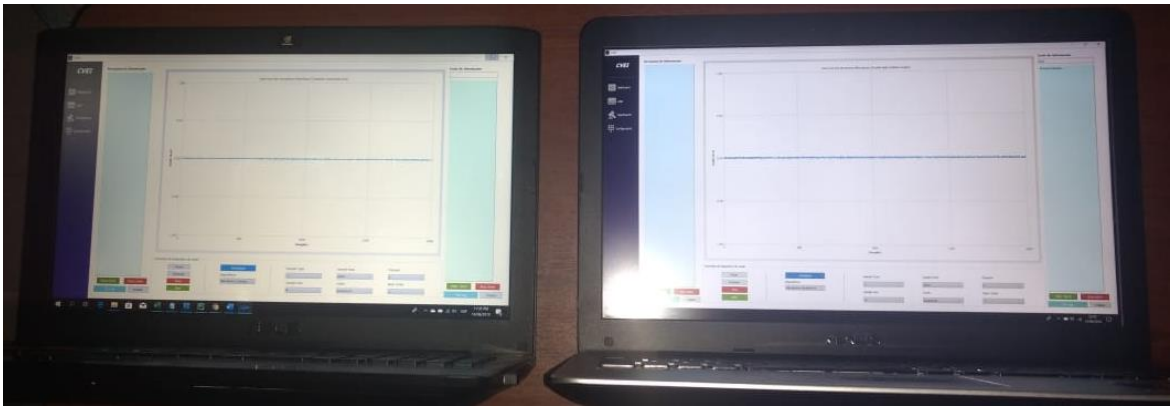
- **Framework librería de audio Qt5:** Framework Qt5 de licencia open source que usa la gráfica y función senoidal. Software libre - gratuito. Para mayor comprensión utilizar enlace de la página oficial https://doc.qt.io/qt-5/qtcharts-audio-example.html.

6.2 Fase 2: Método de identificación

Desarrollar un método para la detección de eventos de transmisión de datos a través de fuentes ultrasónicas en un ordenador portátil y de escritorio.

Escenario de pruebas.

Figura 9. Escenario en el laboratorio Artes Digitales. Fuente Propia.



En fase se realizaron varias pruebas con software: quinet y gnuradio, con cada uno de ellos generaron diferentes transmisiones y se midieron los resultados de recepción, y se concluye que el quinet cuenta con procesos más óptimos en la tasa más alta de transmisión de paquetes sin pérdida de información para realizar la modulación y la demodulación y adicional no depende del protocolo tcp, puertos como lo requiere la aplicación Gnuradio.

En fase se desarrolló un método basado en software que permite la identificación de ondas ultrasónicas, con ello, la posible detección de datos en dichas ondas.

Igualmente se definieron los siguientes parámetros de medición con el fin de obtener unos resultados de captura en transferencia de datos más eficientes:

Medida: Dado que las ondas mecánicas generadas a través de ultrasonido son susceptibles a tener interrupciones en el momento de viajar de un destino a otro cuando la distancia es demasiado prolongada (por ende se pierden muchos paquetes de información), basados en la literatura de investigación se define la distancia en la que se utilizara en cada una de las pruebas entre un equipo de cómputo y el otro, Se ilustran en la Tabla 2.

Tabla 2: Definición de medida pruebas de un equipo al otro. Fuente Propia.

Medida/Distancia
5 cm
10 cm
30 cm
1 mtrs

1.2 mtrs

A continuación, se relacionan el set de pruebas desarrolladas:

Laboratorio de acústica ITM Parque I: Se probó en un ambiente cerrado libre del ruido.

Escenario 1: Ambiente cerrado libre de ruido.

Prueba 1:

- Se inició el (los) programa para captura de ultrasonido y se verifico que hay en el ambiente, documentar.
- Se encendido los portátiles y se captura por medio de los dispositivos móviles si se generó ultrasonido a una distancia de 5cm, 10 cm, 30 cm, 1 mtrs, 1.2 mtrs.
- Se activó en el portátil una aplicación que genera Ultrasonido por los parlantes y capturar por medio de los dispositivos móviles.

Prueba 2:

- Con el medidor de espectro, se capturo la señal de un micrófono y diferentes ondas sonoras.
- Se conectó un micrófono como receptor y con el generador de Onda hacia un parlante capturando por medio del micrófono externo.
- Se verifico como se gráfica la Onda recibida, aumentando la frecuencia en el generador y se verifico si el micrófono es capaz de detectarlo.

- Se aumentó hasta que se verifico el nivel más alto de recepción del micrófono.
- Se buscó una aplicación compatible con equipos de cómputo tipo laptop que grafique las Ondas, se procedió a descargar y se emulo con el MIC interno.

Ya entendido como se ve en el analizador de espectro, se precedió a lo siguiente:

- Se Ejecutó la prueba 1 pero con el analizador de espectro.

Prueba 3: Se Incluyó ondas de sonido en ultrasonido.

- Se Capturó ondas ultrasónicas modulando y demodulando.
- Se enviaron otros tipos de datos por ultrasonido y se procedió a realizar los pasos 2 y 3.

Escenario 2: Tipo Oficina.

Pruebas 1: Emisión.

En el laboratorio acústico se utilizó una cámara sonoamortiguadora, uno de los computadores laptop se le instalado el software de medición para capturar los niveles de sonido que se produce en un ambiente. A continuación, se enuncian los pasos que se realizaron en la prueba 1.

Se obtuvieron los datos de la prueba 1 y se procedió a realizar lo que se describe a continuación:

Primero se normalizó los datos que se enviaron en este ambiente y se tomó la muestra de las ondas que se generan antes y después de encender los dispositivos, sin ejecutar ningún software que genere o detecte ultrasonido, en este caso los computadores laptops y los dispositivos móviles.

Una vez obtenido los datos provenientes del ambiente insonoro, se utilizó uno de los dispositivos móviles con el software generador de frecuencia, con el cual se realizó una muestra global pasando

desde tonos audibles hasta alcanzar un tono ultrasónico y se obtuvo la muestra de lo que el equipo de cómputo capturo en su momento, para la prueba se cambiaron entre muestra y muestra la distancia de dichos dispositivos y se analizó entre el rango la señal más intensa o dispersa dependiendo el caso.

Se realizó la prueba cambiando el emisor de ondas, siendo este el computador y el detector de sonido el cual fue interpretado por el dispositivo móvil, la intensión de esta prueba fue que se lograra medir que capacidad que tienen los altavoces que posee el computador portátil instalados predeterminadamente y se logró calcular acorde a la distancia entre los dispositivos y el tono generado y así se identifica los umbrales de ondas que se pueden transmitir desde el dispositivo.

Se ejecutó en uno de los equipos de cómputo un software que permitió la manipulación de algunos de sus componentes como los ventiladores y discos duros logrando así obtener ondas ultrasónicas.

Se manipularon cada uno de estos elementos y se transcribieron los resultados de dichas pruebas, se concluyó que los dispositivos que trabajan independiente o conjuntamente tienen efectividad para producir ultrasonido.

Se realizó una prueba añadiéndole al computador portátil un dispositivo externo en este caso unos diferentes micrófonos. Se tomó la muestra y la medida respectiva sobre los rangos que son capaces de emanar este dispositivo conectados al computador.

Se realizó una prueba añadiéndole al computador portátil dispositivos externos en este caso una diadema que contiene un micrófono y unos parlantes. Se tomó la muestra y la medida respectiva sobre los rangos que son capaces de emanar este dispositivo conectados al computador.

6.3 Fase 3: Clasificación

Desarrollar un procedimiento de clasificación que permita establecer si los datos que se está transmitiendo son información relevante.

Basada en la recopilación y reestructuración propuesta por los autores en la literatura se proporciona una nueva definición de la clasificación que se agrupa en 6 categorías de restricción de acceso a la información en la cual se toma las mejores prácticas de las normas: COBIT, NIST, ISO, ISA, RFC, NERC, y se definen los patrones que partiendo de una definición macro se pueda ajustar a la normativa singular según la forma de trabajo en las diferentes organizaciones privadas o gubernamentales. Con lo anterior se logró una mayor atención enriqueciendo la clasificación de seguridad de información interdisciplinaria en la dialéctica de seguridad informática de una manera actualizada a la nueva gestión de la información.

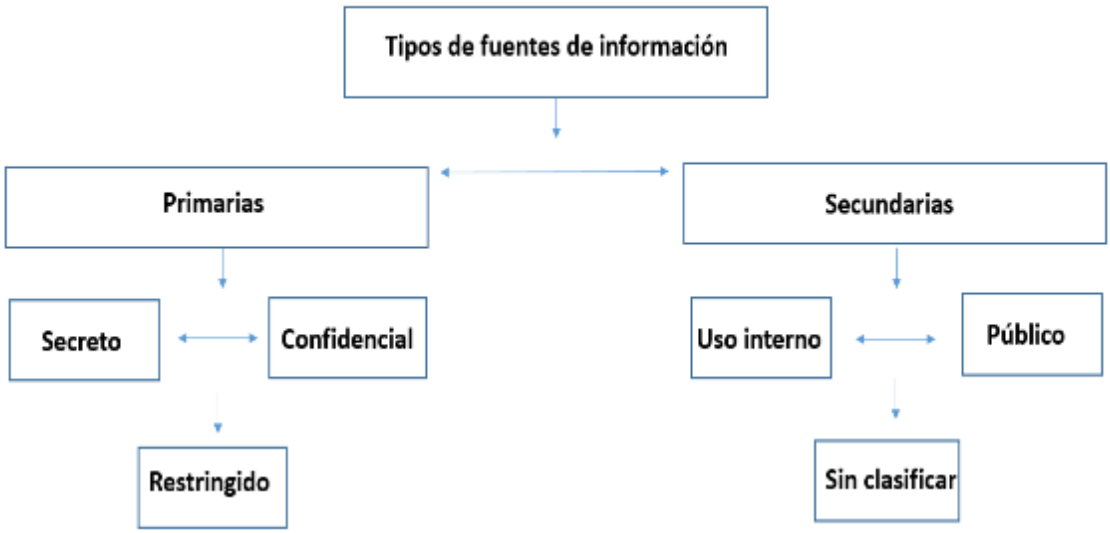
Los 6 nuevos niveles para realizar una clasificación de información efectiva son:

1) Noción de: protección, la sensibilidad, la criticidad, valor, ciclo de vida, contextualización, uso, disponibilidad, integridad, evaluación de riesgos, el riesgo del propietario, y el riesgo de almacenamiento de información legal que es el tema predominante en la definición del NIST.
2) Noción de: Información, Protección, Riesgo Legal, sensibilidad, ciclo de vida, Contextualización, uso, Disponibilidad, La integridad, la evaluación de riesgos, el riesgo del propietario, y el riesgo de Almacenamiento de Información.

3) Noción de: Protección, del ciclo de vida, contextualización, uso, disponibilidad, integridad, evaluación de riesgos, el riesgo del propietario, y el riesgo de Almacenamiento de Información.
4) Noción de: Contextualización, uso, evaluación de riesgos, el riesgo del propietario, y el riesgo de Almacenamiento de Información.
5) Noción de: Sensibilidad, criticidad, Ciclo vital, Contextualización, Riesgo Legal, uso, disponibilidad, integridad, evaluación de riesgos, el riesgo del propietario, y el riesgo de Almacenamiento de Información.
6) Noción de: Protección, criticidad, del valor, del ciclo de vida, contextualización, uso, disponibilidad, integridad, evaluación de riesgos, el riesgo del propietario, y el riesgo de Almacenamiento de Información [18].

Se desarrolló una aplicación de software de detección de información, la cual se le denominó CVEI - Clasificador y visualizador de exfiltracion de información, ésta cuenta con los niveles de clasificación ya definidos, describiendo por cada nivel la complejidad o importancia de la información, este se pasa por un filtro de clasificación y como resultado entregó la respectiva detección de la información que se encuentra en los niveles de clasificación.

Figura 10: Niveles de clasificación de información. Fuente Propia.



Para el proceso de la clasificación de la información se utiliza la funcionalidad de un sistema prevención de perdida de datos, la cual se relaciona con los grupos de clasificación de la información ya definidas en el marco teórico del presente trabajo. Los propietarios de la información tienen la capacidad de definir si un archivo dentro de sus propiedades de nombramiento, dato en particular (como el número de una tarjeta de crédito) debe ser analizado y, en su caso, bloqueado si es transmitido por una onda ultrasónica.

Estas herramientas pueden ser configuradas según la clasificación propuesta: Secreto, Confidencial, Restringido, Uso interno, Público, Sin clasificar. Dentro de las funcionalidades: monitoreo y bloqueo se encuentran cualquier intento de transferencia no autorizada de los datos en resguardo. Esto funciona con la semejanza en tecnología a un firewall, que detiene un patrón de ataque, pero en este caso se evita que la información clasificada se transmita si no posee autorización[18].

Para la clasificación de la información, se creó un diccionario de palabras claves, éste listado es comparado con la recepción de los datos por ultrasonido, y si coinciden, el dato se lleva al campo respectivo dentro del aplicativo CVEI. En consideración que se trata de un ejercicio académico, se definieron las siguientes palabras de acuerdo al nivel de clasificación:

Grupo 1: Secreto: Pepsi, receta

Grupo 2: Confidencial: patente, nomina

Grupo 3: Restringido: archivo, claves

Grupo 4: Uso interno: contable, correos

Grupo 5: Público: grafico, balances

Grupo 6: Sin clasificar: Cualquier dato no incluido en lo anterior, debe ser revisado por una persona.

6.4 Fase 4: Evaluación

La evaluación del proceso consiste en realizar las pruebas de envió de información por ultrasonido desde un PC, recepcionar dicha información y aplicar, a través del software construido, una clasificación para validar los datos recolectados que nivel de criticidad tienen.

En el desarrollo del software - CVEI se tuvieron en cuenta 4 componentes para realizar efectivamente la muestra de:

1) Envió de información en ultrasonido.

2) Recepción de información en ultrasonido.

3) Detección y registro de información transmitida en ultrasonido.

4) Configuración y parametrización del envió de información.

Para la verificación de que el software construido cuenta con la fiabilidad en la recepción de datos, se enviaron los mismos datos enviados por Quietnet (figura 43), éstos se capturaron en CVEI para efectos de validar coherencia y que si se tuviera un ambiente homólogo en la recepción (comprobación que los datos de entrada corresponden a los datos de salida en el software propietario).

Figura 11: Homologación y verificación de funcionalidad al integrar QuietNet al software CVEI.

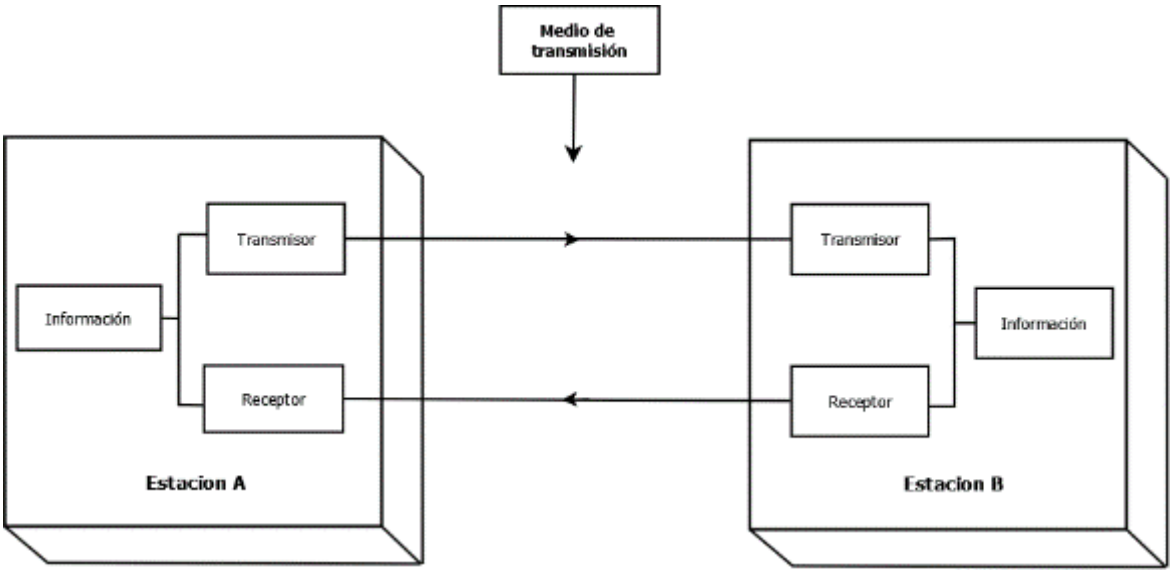
Ya que el objetivo de este trabajo no fue en centrarse en la infección de los dispositivos y el modo de recolección de información dentro de una máquina, se centró como tal en enviar información del tipo cadenas de texto codificadas en frecuencia ultrasónica para el establecimiento del canal de comunicación entre los dispositivos y además lograr su detección y clasificar la información de la manera que funciona un sistema de prevención de perdida de datos. El envío de la información se realiza de forma manual.

Evaluar el método diseñado para la detección de exfiltración de información.

En ésta fase, se desglosaron las siguientes actividades:

1) Diagrama general del método diseñado.

Figura 12: Diagrama de comunicación. Fuente propia.



En la figura 10 se ilustra dos dispositivos que portan características iguales en cuanto a componentes, aunque pueden tener referencias distintas al detalle en nivel de hardware. En la estación A y B se tienen información almacenada en un storage y a su vez ambos dispositivos cuentan con periféricos de emisión y recepción de sonido con capacidad ultrasónica. El medio de transmisión es el aire ya que este tipo de onda es mecánica. La estación A funciono como víctima y tuvo el proceso de filtrado y clasificación de la información la cual sale por medio de ultrasonido, esto es, el equipo PC al cual se le exfiltro información, y la estación B, es el PC (atacante) al cual llego la información.

Anexo 1: Detalles Diagrama general del método.

2) Construcción del software de ultrasonido.

a) Flujograma

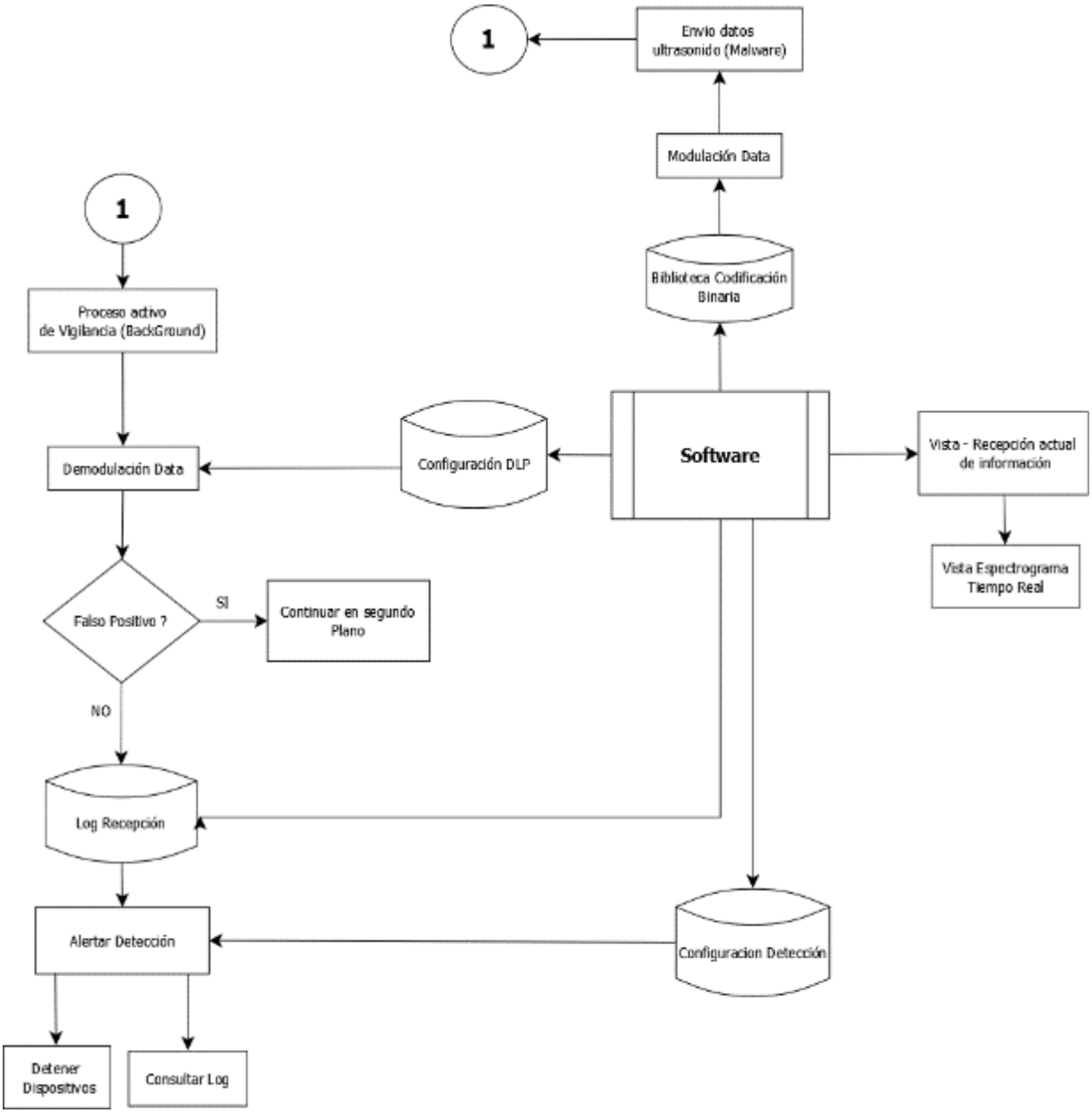
Se partió del software como un componente modular, este constó de 4 fuentes de datos: El primero fue la biblioteca de codificación que se encargó de almacenar en equivalencia binaria los datos del teclado QWERTY del dispositivo. La segunda fue la configuración del DLP la cual tuvo la asociación entre los niveles de clasificación parametrizados y los datos de importancia para el usuario. La tercera es el log de recepción en el que se alojaron todos los movimientos detectados por el algoritmo de monitoreo del dispositivo. Y la cuarta es la configuración de la detección en la cual el usuario ajusta la acción que tomara el algoritmo al detectar una exfiltración.

Con las 4 fuentes de datos funcionando como almacenamiento y consulta se logró partir al módulo de envió de información, que se desempeña en este caso, como el malware en el cual consulta la información que es almacenada en la biblioteca de forma codificada y enviada a través de los altavoces del dispositivo. A su vez el software tiene en su proceso de segundo plano, una rutina que es la encargada de receptar toda la información modulada, en el proceso de detección se tiene una rutina para clasificar si un movimiento detectado se cataloga como un falso positivo o un dato clasificado de información relevante para que el usuario según la configuración que realizo en el módulo de almacenamiento de información sea alertado y pueda realizar una acción.

Dentro del proceso de detección se tuvo una rutina para clasificar si un movimiento detectado se cataloga como un falso positivo o un dato clasificado de información relevante para que el usuario según la configuración realice una acción.

Además, se logró integrar el **Framework librería de audio Qt5**, consulta visual con la ayuda de un espectrograma el movimiento de los dispositivos receptores de ondas sonoras (micrófonos).

Figura 13: Diagrama de flujo clasificador y visualizador de exfiltracion de información.



Fuente Propia.

Anexo 2: Detalles diagrama de flujo.

Diagrama de clases.

Las entidades generadas en este modelo contienen las propiedades y las funciones que ejecutan el software para realizar el proceso completo que comprende el envío la detección el registro y la acción a ejecutar frente a una exfiltración por ultrasonido.

TipoClasificación: Tabla de parametrización, esta tiene según los tipos de clasificación a nivel de gobierno de la información los grupos de clasificación que usuario desea manejar.

ConfiguraciónDLP: Tabla de almacenamiento y consulta. Esta entidad asocia según el tipo de clasificación la referencia de un dato a que tipo pertenece, además ejecuta la función de registrar la clasificación de la información que sea importante para el usuario.

Configuración: Tabla de parametrización en la que se realiza el ajuste de ejecutar la transmisión por ultrasonido. Debido a que los dispositivos a nivel de hardware tienen características diferentes en esta entidad se configuro la velocidad, la frecuencia el canal, el tamaño del dato y la cantidad. Además, tiene la función de parar los dispositivos en caso de que el usuario lo configure.

ModulaciónDemodulaciónBackground: Entidad que por propiedad recibe la cadena de información y como funciones tiene la escucha activa del dispositivo, Registro de los movimientos detectados, alerta de detección de exfiltración y el comparativo de datos configurado en el DLP contra lo que en tiempo real está detectando el software.

LogRecepción: Entidad que tiene como propiedades identificador único, fecha de captura de la información, dato capturado y el tipo de clasificación, como función tiene la posibilidad de Consulta la información registrada.

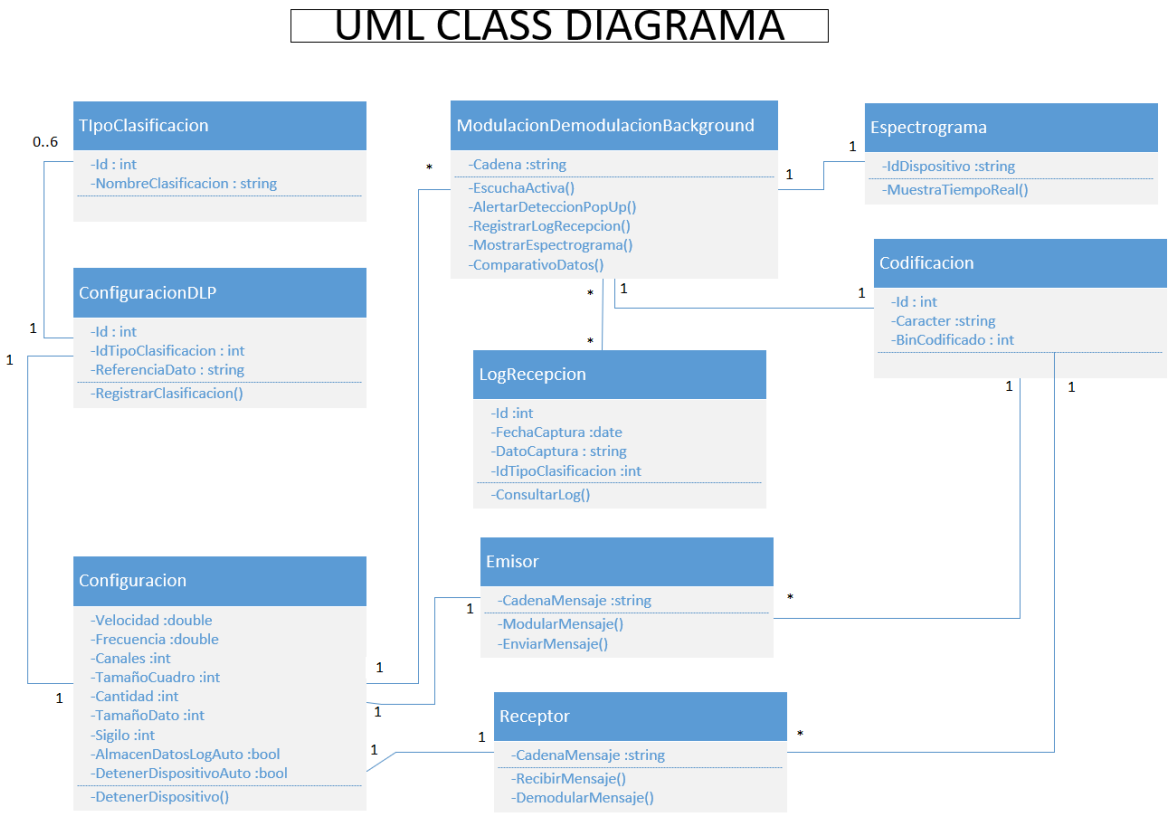
Emisor: Entidad que contiene la cadena de información, como función este modula la información en ultrasonido y envía la cadena de datos.

Receptor: Entidad que contiene la cadena de información, como función esta demodula la información en ultrasonido y recibe la cadena de datos.

Espectrograma: Entidad que contiene el identificador del dispositivo de recepción (micrófono), como función puede enseñar en tiempo real la actividad del dispositivo.

Codificación: Entidad que contiene las propiedades de identificador único, carácter, y equivalencia binaria. Funciona como la biblioteca de codificación.

Figura 14: Diagrama de clases - clasificador y visualizador de exfiltracion de información.



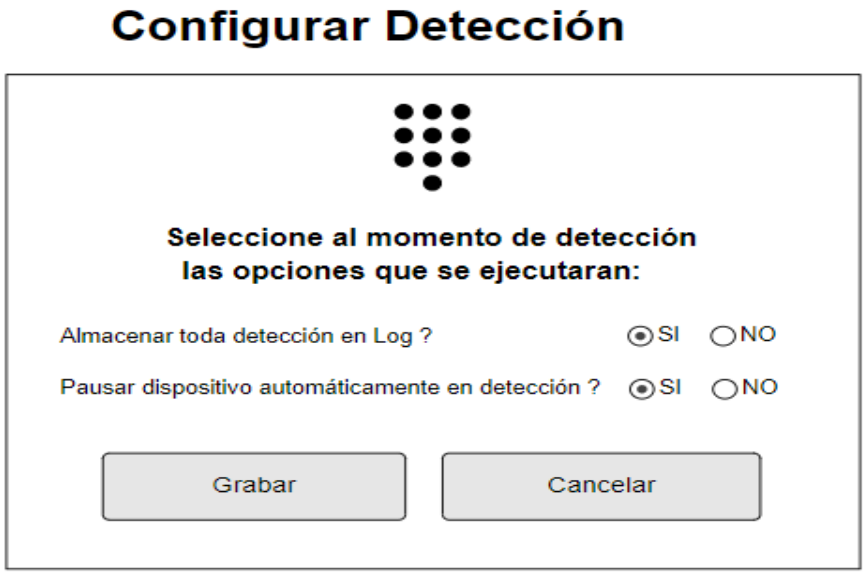
Fuente Propia.

Anexo 3: Detalles diagrama de clases.

b) Diseño de los módulos del software.

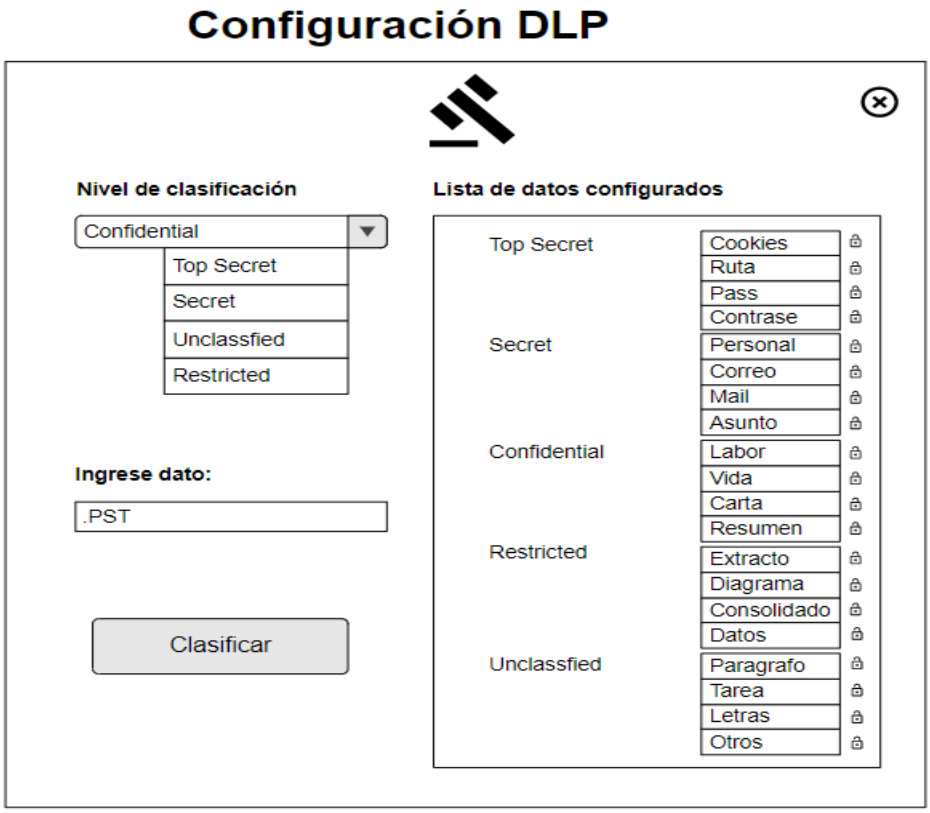
Pantalla configuración detención: Permite parametrizar el almacenamiento del log y pausar la gráfica cuando se capture un dato que se encuentre en los niveles de clasificación.

Figura 15: Diseño Modulo de Configuración. Fuente Propia.



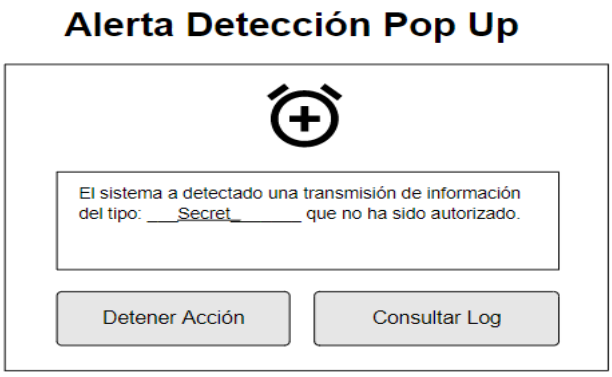
Pantalla configuración detención: Permite ingresar la información basado en el nivel de clasificación.

Figura 16: Diseño Modulo Configuración DLP. Fuente Propia.



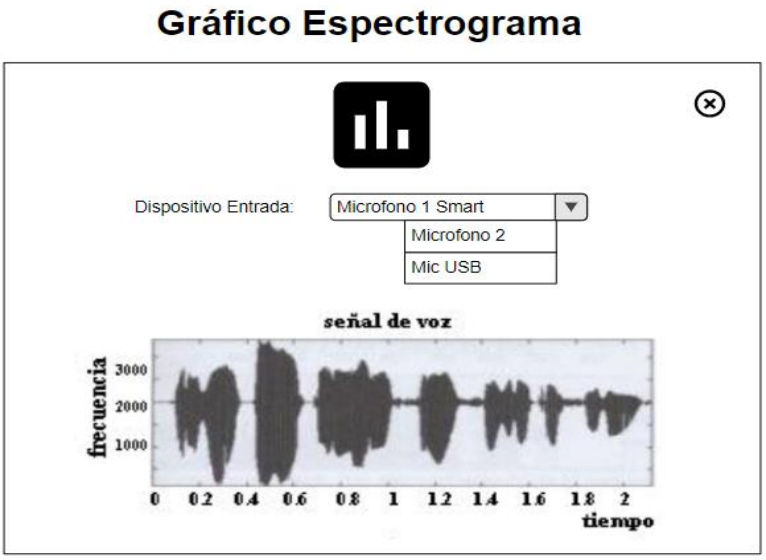
Alerta de detención Pop Up: identifica que alguno de los datos que están almacenados en el nivel de clasificación este siendo vulnerado, el sistema detecta la acción y avisa al usuario que a cuál le están intentado robar su información notificando por medio de un mensaje de advertencia.

Figura 17: Notificación de Detección. Fuente Propia.



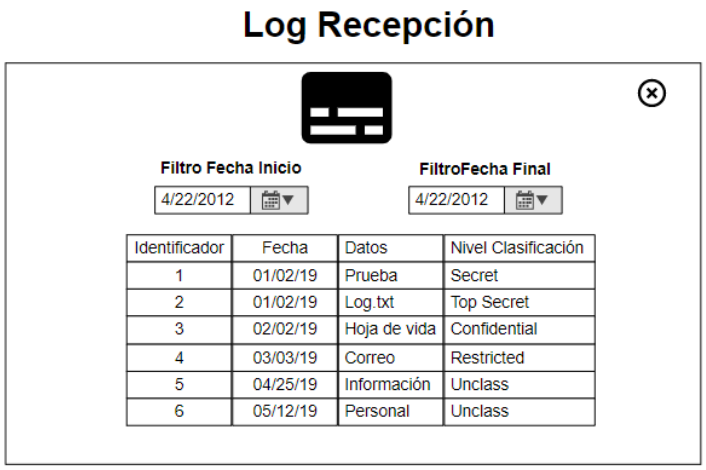
Pantalla grafico espectrograma: En esta pantalla se listan los dispositivos internos y externos tipo hardware de sonido, y adicional muestra el espectrograma con la medición de la señal que se está emitiendo. Se integró al CVEI el **Framework librería de audio Qt5.**

Figura 18: Diseño Modulo Grafico Espectrograma. Fuente Propia.



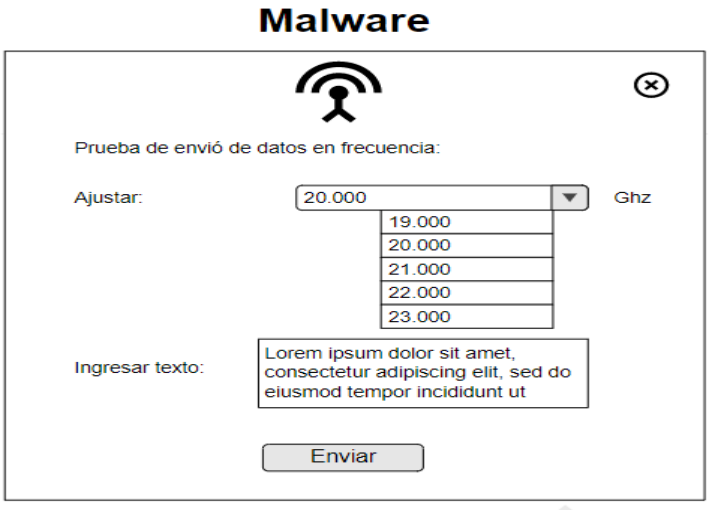
Pantalla Recepción: Se integró el Quietnet, en este proyecto lo llamamos Recepción, es el encargado de recibir la información en el equipo del atacante, recibiendo la información que se encuentra almacenada en los niveles de clasificación del equipo atacado, esta funcionalidad estará integrada nativamente la aplicación CVEI.

Figura 19: Diseño Log transaccional. Fuente Propia.



Pantalla Malware: Se integró el Quietnet, en este proyecto lo llamamos Malware, es el encargado de realizar la fuga de información que se encuentra almacenada en los niveles de clasificación, esta funcionalidad está integrada nativamente en la aplicación CVEI.

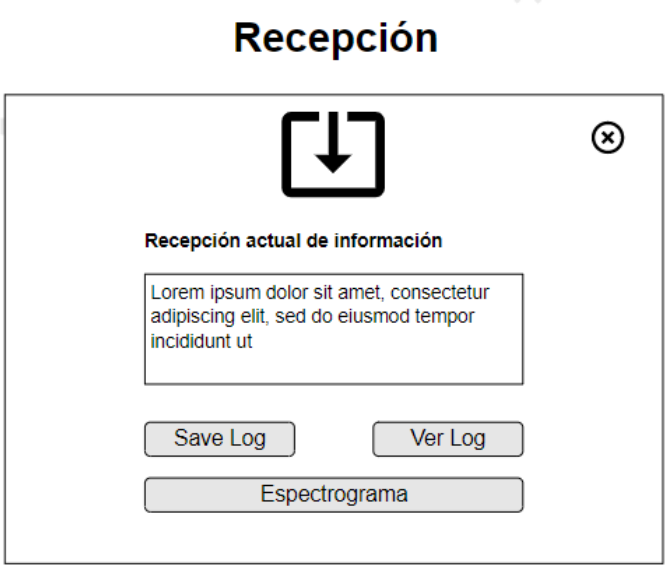
Figura 20: Diseño Modulo Malware. Fuente Propia.



Pantalla Recepción: Se integró el Quietnet, en este proyecto lo llamamos Recepción, es el encargado de recibir la información en el equipo del atacante, recibiendo la información que se

encuentra almacenada en los niveles de clasificación del equipo atacado, esta funcionalidad estará integrada nativamente la aplicación CVEI.

Figura 21: Diseño Modulo Recepción. Fuente Propia.



Anexo 4: Detalles diseño del software.

c) Diseño pruebas funcionales.

Se usó los equipos de cómputo tipo laptop marca Asus 555L y Asus GL555VW con sus características propias de hardware y software, cada equipo de cómputo representa un actor en las pruebas:

- Asus 555L equipo víctima.
- Asus GL555VW equipo atacante.

Inicialmente se instaló el software desarrollado CVEI en cada uno de los equipos de cómputo. Luego se realizó la configuración de la aplicación CVEI de la siguiente forma:

En el equipo Asus 555L equipo víctima, solo se activó las funcionalidades del DLP, y el envío de información a través del Malware y el gráfico espectrograma, en el módulo de configuración del DLP se ingresó información en cada uno de los niveles de clasificación (Secreto, Confidencial, Restringido, Uso interno, Público y Sin clasificar).

El equipo Asus GL555VW equipo atacante, solo se le activo las funcionalidades de Malware receptor y el grafico espectrograma.

Para ambos equipos se configuró, el envío y recepción da frecuencia de 21.000 Ghz (ultrasonido).

Ya con los equipos de cómputo configurados, se realizaron las pruebas funcionales en los siguientes escenarios:

Escenario 1, ambiente libre de ruido: Se ejecutaron los siguientes pasos para las pruebas funcionales en el ambiente.

- Se ubicaron los equipos Asus 555L equipo víctima y Asus GL555VW equipo atacante a una distancia de 1 mtrs, en una posición opuesta.
- Se ejecutó el software desarrollado CVEI en cada uno de los equipos con los parámetros establecidos.
- El equipo victima Asus 555L, digito en la pantalla llamada **malware de envío**, información (cadena de texto) que se almacenó en la base de datos de cada uno de los niveles de clasificación.
    - **Secreto:** receta
    - **Confidencial:** nomina
    - **Restringido:** claves
    - **Uso interno:** correos

- **Público:** balance
- **Sin clasificar:** hola

- En el sistema de clasificación se habilita un grupo nombrado sin clasificar el cual conglomera todas aquellas cadenas de información que no pertenece a los grupos de: Secreto, Confidencial, Restringido, Uso interno, Público, Sin clasificar. Lo anterior permite al usuario tomar la decisión sobre una acción del evento que se ejecuta en el momento de transmitir algún tipo de información.
- Se capturó pantallazos de todo lo ejecutado en el proceso.
- Se creó una tabla con los resultados obtenidos en cada fase del proceso.
- Se dígito información que no se encuentra en la base de datos del nivel de clasificación, esta información se recibió de forma exitosa por el atacante. Se hizo captura de pantalla a la actividad, al igual se creó una tabla con los resultados que demuestran la medida de frecuencia capturada, distancia, palabra capturada y estado de la captura.

Escenario 2, tipo oficina: Se ejecutaron los siguientes pasos para las pruebas funcionales en el ambiente.

- Se ubicaron los equipos Asus 555L equipo víctima y Asus GL555VW equipo atacante a una distancia de 1 mtrs, en una posición frontal.
- Se ejecutó el software desarrollado CVEI en cada uno de los equipos con los parámetros establecidos.

- El equipo victima Asus 555L, digito en la pantalla llamada **malware de envío**, información (cadena de texto) que se almacenó en la base de datos de cada uno de los niveles de clasificación.
    - **Secreto:** pepsi
    - **Confidencial:** patente
    - **Restringido:** archivo
    - **Uso interno:** contable
    - **Público:** grafico
    - **Sin clasificar:** caja

- En el sistema de clasificación se habilita un grupo nombrado sin clasificar el cual conglomera todas aquellas cadenas de información que no pertenece a los grupos de: Secreto, Confidencial, Restringido, Uso interno, Público, Sin clasificar. Lo anterior permite al usuario tomar la decisión sobre una acción del evento que se ejecuta en el momento de transmitir algún tipo de información.
- Se capturó pantallazos de todo lo ejecutado en el proceso.
- Se creó una tabla con los resultados obtenidos en cada fase del proceso.
- Se dígito información que no se encuentra en la base de datos del nivel de clasificación, esta información se recibió de forma exitosa por el atacante. Se hizo captura de pantalla a la actividad, al igual se creó una tabla con los resultados que demuestran la medida de frecuencia capturada, distancia, palabra capturada y estado de la captura.

7. Resultados

Basados en la literatura científica y las metodologías aplicadas en anteriores proyectos que transmiten información a través de paquetes modulados en ondas ultrasónicas, se realizó una integración de una solución aplicativa basada en un nuevo procedimiento de identificación, caracterización, almacenamiento y procesamiento de la información, para generar una solución que permita control sobre las transmisiones de información que vulneren la confidencialidad de los datos dentro de un sistema computacional personal.

A continuación, se presentan los resultados obtenidos de los 4 objetivos específicos del trabajo de grado presentado:

- **Caracterización de los elementos:** Para la caracterización se definió un conjunto de componentes y características en hardware de computadores tipo portátil y de escritorio que permiten la transmisión ultrasónica susceptible de permitir exfiltración de información.
- **Identificación:** Se desarrolló un método para la detección de eventos de transmisión de datos a través de fuentes ultrasónicas en un ordenador portátil y de escritorio.
- **Clasificación de información:** Se desarrolló un procedimiento de clasificación que permita establecer si los datos que se está transmitiendo son información relevante, tuvo

una tasa de falsos negativos de menos del 10.0% y una falsa tasa de descubrimiento de menos del 5.0% en todas nuestras pruebas.

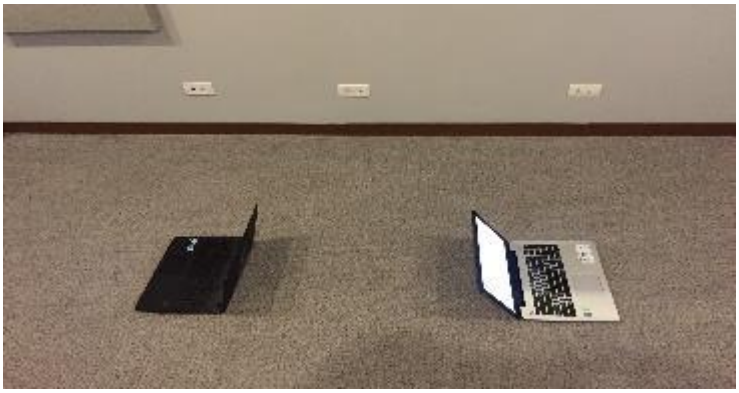
7.1 Evaluación del modelo.

- **Equipos de cómputo seleccionados**: Se comprueba que los equipos de cómputo tipo laptop cuentan con las características idóneas para nuestro trabajo, entre ellos el hardware de sonido integrado y adicional su fácil desplazamiento, haciendo así que sea un dispositivo con altas probabilidades de ser vulnerada. Se descartó el uso de equipos de cómputo tipo escritorio, dado que no cuentan con el hardware de sonido integrado y necesita de hardware externo para cumplir con los requisitos, adicional estos tipos de equipos generan mucho más sonidos o ruidos propios del hardware, lo cual se dificulto la captura de frecuencia ultrasónica que se requiere.

Equipos de cómputo tipo laptop

- Asus GL555VW - año de fabricación 2016
- Asus A555L – año de fabricación 2015
- Micrófonos y altavoces integrados de los equipos de cómputo.

Figura 22: Equipos de cómputo seleccionados. Fuente Propia.



- **Lugar seleccionado para recrear los escenarios requeridos:** El laboratorio musical ITM, fue seleccionado para realizar las pruebas y toma de resultados, dado que posee las condiciones requeridas y adicionales se cuenta con software y hardware que complementaron la investigación y pruebas. En el laboratorio musical ITM se recreó los ambientes Tipo Oficina y libre de sonido.

Acondicionamiento del laboratorio musical ITM:

Figura 23: Laboratorio seleccionado para las pruebas. Fuente Propia.

- Espacio libre de sonido, este ambiente no cuento con ningún objeto o ruidos en el entorno.
- Ambiente tipo oficina, el cual cuenta con objetos y ruidos generados por defecto por los dispositivos, el medio ambiente y las personas.
- Altavoces y micrófonos profesionales para captura de sonido.
- Identificación de elementos de medición: Micrófonos
    - Micrófono tlm103 neumann.
    - Micrófono Re20 Electrovoce: Dinámico.
    - Micrófono shure sm57: Dinámico.

Figura 24: Micrófonos seleccionados para las pruebas. Fuente Propia.



- **Mediciones:** Se utilizó los micrófonos externos los cuales se conectaron en los equipos de cómputo tipo laptop, se comprobó que a través de la integración de estos dispositivos fue posible obtener una captura de frecuencia con un nivel más alto y eficiente a comparación del hardware de sonido integrado en los equipos de cómputo, de esta manera se integra al conjunto de dispositivos usados en este proyecto. El objetivo del uso de esta clase de dispositivos es encontrar otras alternativas de captura de ondas ultrasónicas a través de los equipos de cómputo. Los resultados obtenidos fueron documentados, dejando registro como insumo de futuras investigaciones.

7.2 Identificación.

Con las condiciones de ambiente y dispositivos caracterizados en el punto 7.1, se realizaron las pruebas y se obtuvo los siguientes resultados:

Escenario 1: Ambiente libre de ruido.

Prueba 1: Esta prueba tuvo como objetivo demostrar que los equipos de cómputo tipo laptop seleccionados, cuentan con todas las características tipo hardware y software de sonido para capturar y generar frecuencias por encima del umbral humano. Se logró identificar las capacidades de captura de cada uno de los equipos de cómputo seleccionados, logrando identificar que el equipo de cómputo Asus cuentan con mayores capacidades para capturar frecuencias generadas en ondas ultrasónicas. A continuación, se describe los pasos utilizados en esta prueba:

- En una distancia de 1.2 mts se ubicaron los equipos de cómputo.
- Se inició un programa generador de frecuencias en un equipo y en el otro equipo un programa para capturar la frecuencia.
- Se obtuvo el resultado de captura de cada uno de los equipos de cómputo.

Resultados obtenidos con los equipos de cómputo: Los equipos de cómputo Asus GL555VW y Asus A555L, se utilizaron con las características propias de hardware de sonido y software externo instalado, y se logró evaluar la efectividad y precisión de cada software evaluado, así

como el comportamiento en cada uno de los equipos de cómputo. Se generó frecuencia desde 18 – 20 kHz.

Figura 25: Equipos de cómputo tipo laptop en ambiente libre de ruido. Fuente Propia.

Tabla 3: Resultados usando software iZotope V5.01.184. Fuente Propia.

Equipo	Distancia	Frecuencia capturada	Software	Escenario
Asus A555L	1.2 metro	18kHz	iZotope V5.01.184	Emisor Receptor
Asus GL555VW	1.2 metro	20 kHz	iZotope V5.01.184	Receptor Emisor

Se logró demostrar que los equipos de cómputo laptop, cuentan con las capacidades para generar y capturar frecuencias ultrasónicas. En la tabla anterior se puede identificar que el equipo Asus A555L, solo alcanzo a generar y capturar 18 kHz y el equipo Asus GL555VW respondió con más eficiencia logrando generar y capturar 20 kHz, que es considerado ultrasónico.

Escenario 2: Tipo Oficina pruebas de emisión.

- En el laboratorio acústico se utilizó una cámara sonoamortiguadora, uno de los computadores que poseen instalado el software de medición para tomar los niveles de sonido que se produce en un ambiente.

- Primero se normalizo los datos que se realizaron en este ambiente se tomó la muestra de las ondas se generan antes y después de encender los dispositivos sin correr ningún software, en este caso los computadores.

  Adicional se realizaron los siguientes pasos:

- Se obtuvo los datos provenientes del ambiente insonoro se utilizó uno de los dispositivos móviles con el software generador de frecuencia, el cual se realizó una muestra global que paso desde tonos audibles hasta que alcanzo un tono ultrasónico y se obtuvo la muestra de lo que el equipo capturo en ese momento, para esta prueba se cambiaron entre muestra y muestra la distancia de dichos dispositivos para analizar entre qué rango la señal es más intensa o dispersa según sea el caso.

- Ahora se realizará la prueba cambiando el emisor de ondas siendo este el computador y el detector de sonido será interpretado por el dispositivo móvil, la intención de realizar esta prueba es lograr medir qué capacidad tienen los altavoces que posee el computador portátil instalados predeterminadamente y así se logró calcular acorde a la distancia entre los dispositivos y el tono generado el umbral de ondas que se pudo transmitir desde el dispositivo móvil.

- Se ejecutó en el computador un software que permitió manipular algunos de sus componentes como los ventiladores y discos duros logrando alcanzar una rotación que permito generar un umbral ultrasónico.

- Se manipulo cada uno de estos elementos se transcriben los resultados de dichas pruebas concluyendo cuál de estos dispositivos trabajando independiente o conjuntamente lograron obtener mejor efectividad para producir ultrasonido.

Prueba 2: El objetivo de esta prueba, fue demostrar que utilizando dispositivos externos a los equipos de cómputo, fue posible capturar frecuencias ultrasónicas con mayor eficiencia, dado que los micrófonos seleccionados cuentan con condiciones especiales. Se realizó las pruebas en los dos equipos de cómputo con 3 diferentes micrófonos, a continuación se describe los resultados obtenidos a partir de los 3 micrófonos.

Figura 26: Equipos generadores y medidores acústicos. Fuente Propia.

- Se conectó los micrófonos como receptores y con el generador de onda hacia un parlante el cual fue capturado por el micrófono.

- Se verifico la gráfica de la Onda recibida, también se le aumentó la frecuencia en el generador y se verifico si el micrófono es capaz de detectar las ondas ultrasónicas.

- Se aumentó hasta que se verifico el nivel más alto de recepción del micrófono.

- Se instaló software en el equipo de cómputo con el que se graficó las ondas capturadas, lo anterior se emulo con el MIC interno del equipo de cómputo.

Resultado 1: Se obtuvieron los siguientes resultados utilizando el micrófono tlm103 neumann (Condensador) en los equipos de cómputo Asus A555L y Asus GL555VW. Se generó frecuencia desde 22 – 25 kHz.

Figura 27: Micrófono Modelo tlm103 Neumann. Fuente Propia.

Tabla 4: Resultados usando software iZotope V5.01.184. Fuente Propia.

Equipo	Distancia	Frecuencias capturadas	Software	**Imágenes y audios**
Asus A555L	30 cm	22, 23 Khz	iZotope V5.01.184	Anexo 5: Captura Asus A555L frecuencia 30 cm.

Asus GL555VW	30 cm	22,23,24,25,25.3,25.5 Khz	iZotope V5.01.184	Anexo 6: Captura Asus GL555VW frecuencia 30 cm.

En los datos descritos en la tabla 4, se puede observar que a una distancia de 30 cm del micrófono tlm103 neumann, fue posible capturar una medida de frecuencia mucho más alta que la capturada por el hardware propio de las maquinas. También se identifica que con dicho micrófono se obtuvo una captura muy similar en ambos equipos que está en el rango de 22 – 25.5 kHz, en los anexos se aprecia la captura del valor Khz indicado en la tabla. También se observa que el equipo Asus GL555VW obtuvo mejor resultado en la captura.

Resultado 2: Se obtuvieron los siguientes resultados utilizando el micrófono Re20 Electrovoce en los equipos de cómputo Asus A555L y Asus GL555VW, se generó frecuencia desde 22 – 25 kHz.

Figura 28: Micrófono Modelo Re20 Electrovoce. Fuente Propia.

Tabla 5: Resultados usando software iZotope V5.01.184. Fuente Propia.

Equipo	Distancia	Frecuencias capturadas	Software	**Imágenes y audios**
Asus A555L	1 mts	No captura	iZotope V5.01.184	Anexo 7: Captura Asus A555L frecuencia 1 mts.
Asus GL555VW	1 mts	22,23 khz	iZotope V5.01.184	Anexo 8: Captura Asus GL555VW frecuencia 1 mts.
Asus GL555VW	30 cm	23,24,25, khz	iZotope V5.01.184	Anexo 9: Captura Asus GL555VW frecuencia 30 mts.

Asus A555L	30 cm	No captura	iZotope V5.01.184	Anexo 10: Captura Asus GL555VW frecuencia 30 mts.

En los datos descritos en la tabla 5, se puede observar que a una distancia de 30 cm y 1 mts del micrófono Re20 Electrovoce, fue posible capturar una medida de frecuencia mucho más alta que la capturada por el hardware propio de las maquinas. Se identifica que con dicho micrófono se obtuvo una captura positiva por el equipo Asus GL555VW en ambas distancias, mientras que el equipo Asus A555L no registró actividad, en los anexos se aprecia la captura del valor Khz indicado en la tabla. También se observa que el equipo Asus GL555VW obtuvo mejor resultado en la captura.

Resultado 3: Se obtuvo los siguientes resultados utilizando el micrófono shure sm57 en los equipos de cómputo Asus A555L y Asus GL555VW. Se generó frecuencia desde 22 – 25 kHz.

Figura 29: Micrófono shure sm57. Fuente Propia.

Tabla 6: Resultados usando software iZotope V5.01.184. Fuente Propia.

Equipo	Distancia	Frecuencias capturadas	Software	**Imágenes y audios**
Asus A555L	1 mts	No captura	iZotope V5.01.184	Anexo 11: Captura Asus A555L frecuencia 1 mts.

Asus GL555VW	1 mts	22 Khz	iZotope V5.01.184	Anexo 12: Captura Asus GL555VW frecuencia 1 mts.

En los datos descritos en la tabla 6, se puede observar que a una distancia de 1 mts del micrófono shure sm57, fue posible capturar una medida de frecuencia mucho más alta que la capturada por el hardware propio de las maquinas. Se identifica que con dicho micrófono se obtuvo una captura positiva por el equipo Asus GL555VW, mientras que el equipo Asus A555L no registró actividad, en los anexos se aprecia la captura del valor Khz indicado en la tabla. También se observa que el equipo Asus GL555VW obtuvo mejor resultado en la captura.

Adicional a los micrófonos descritos anteriormente, se utilizó otra clase de dispositivos como diademas con micrófono y parlantes externos, los cuales son muy convencionales o de uso común entre las personas.

Resultado 4: Se obtuvo los siguientes resultados utilizando la diadema MDR-7506, Dinámico. Se generó frecuencia desde 22 – 25 kHz.

Figura 30: Diadema modelo MDR-7506. Fuente Propia.

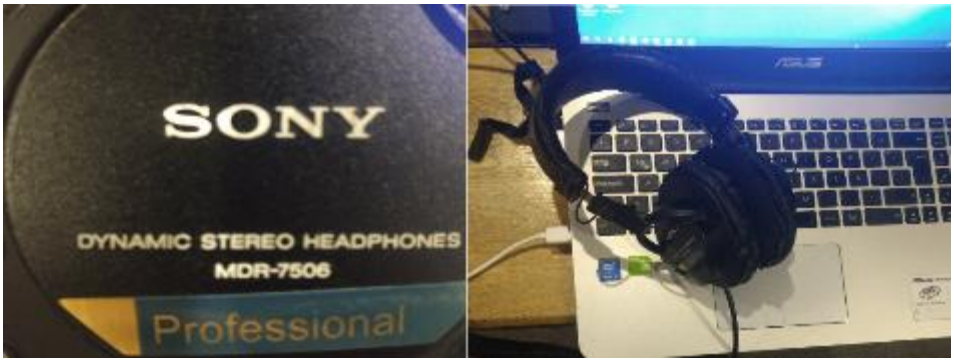


Tabla 7: Frecuencia capturada usando la Diadema. Fuente Propia.

Equipo	Distancia	Frecuencias capturadas	Software
Asus A555L	1 mts	22,5 khz	iZotope V5.01.184
Asus GL555VW	1 mts	22,23 khz	iZotope V5.01.184

En los datos descritos en la tabla 7, se puede observar que a una distancia de 1 mts del micrófono shure sm57, fue posible capturar una medida de frecuencia mucho más alta que la capturada por el hardware propio de las maquinas. Se identifica que con dicho micrófono se obtuvo por ambos

equipos, en los anexos se aprecia la captura del valor Khz indicado en la tabla. También se observa que en este caso el equipo Asus A555L obtuvo mejor resultado por un margen de medida muy corto.

Resultado 5: Se obtuvieron los siguientes resultados utilizando parlantes Genelect 6010B. Se generó frecuencia desde 22 – 25 kHz.

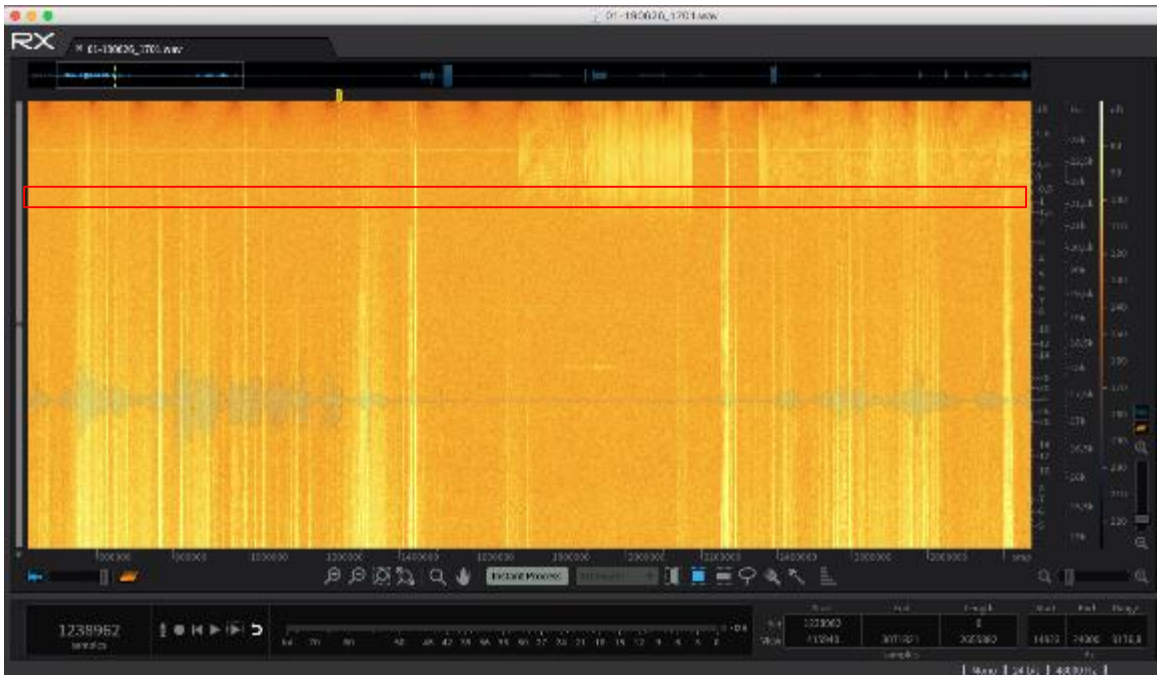
Figura 31: Parlantes modelo Genelec 6010B. Fuente Propia.

Tabla 8: Frecuencia capturada usando parlantes. Fuente Propia.

Equipo	Distancia	Frecuencias capturadas	Software
Asus A555L	1 mts	22,5 khz	iZotope V5.01.184
Asus GL555VW	1 mts	22,23 khz	iZotope V5.01.184

Con esta prueba se quiso demostrar que utilizando parlantes externos es posible generar frecuencia de forma eficiente, se identificó que los paquetes de sonido emitido desde los parlantes se capturan del otro lado de una forma más clara.

Figura 32: Captura utilizando los parlantes y Diadema. Fuente propia.



Prueba 3: Comportamiento de sonidos emitidos por defecto por los equipos de cómputo Asus A555L y Asus GL555VW.

Utilizando el hardware de sonido interno de los equipos, se identificó que no es posible que un laptop escuche frecuencias ultrasónicas emitidas por defecto de los equipos de cómputo. Es por esto que se realizó la prueba con micrófonos externos diferentes a los utilizados en la prueba 2. Y se logró identificar que con dichos micrófonos es posible capturar las frecuencias ultrasónicas emitidas por el equipo de cómputo por defecto.

Para este caso, se realizó las pruebas en un ambiente libre de ruidos (interconexión de equipos de cómputo en un espacio físico reducido y con bajo nivel de ruidos laboratorio musical ITM.

Se utilizó una grabadora externa (Modelo H6 Handy Recorder 200M), con la que se capturo la frecuencia emitida por los equipos de cómputo.

Figura 33: Grabadora Modelo H6 Handy Recorder 200M. Fuente Propia.

La grabadora H6 Handy Recorder 200M, cuenta con dos micrófonos que se integraron a la grabadora: Modelo XYH-6 Stereo Mic y Modelo MSH-6 Stereo Mic.

Se utilizó la grabadora y el Micrófono XYH-6 Stereo Mic, para capturar las frecuencias ultrasónicas que por defecto género el equipo computo Asus A555L.

Figura 34: Micrófono XYH-6 Stereo Mic. Fuente Propia.

Tabla 9: Resultados usando hardware y software de la grabadora. Fuente Propia.

Caso de prueba	Distancia	Frecuencia capturada	Imágenes y audios
Apagar equipo	**5 cm**	**24 khz**	Anexo 13: Captura imagen Asus A555L frecuencia 5 cm. Anexo 14: Captura audio generado Asus A555L frecuencia 5 cm.
Encendido equipo de computo	**10 cm**	**25 khz**	Anexo 15: Captura imagen Asus A555L frecuencia 10 cm. Anexo 16: Captura audio generado Asus A555L frecuencia 10 cm.
Apagar equipo	**10 cm**	**24 khz**	Anexo 17: Captura imagen Asus A555L frecuencia 10 cm. Anexo 18: Captura audio generado Asus A555L frecuencia 10 cm.
Equipo encendido, sin ejecutar	**10 cm**	**24.5 khz**	Anexo 19: Captura imagen Asus A555L frecuencia 10 cm.

programas			Anexo 20: Captura audio generado Asus A555L frecuencia 10 cm.
Equipo encendido, ejecutando programa (Arduino)	**10 cm**	**24.5 khz**	Anexo 21: Captura imagen Asus A555L frecuencia 10 cm. Anexo 22: Captura audio generado Asus A555L frecuencia 10 cm.
Transferencia de datos a una unidad de almacenamiento extraíble	**10 cm**	**28.5 khz**	Anexo 23: Captura imagen Asus A555L frecuencia 10 cm. Anexo 24: Captura audio generado Asus A555L frecuencia 10 cm.
Disco duro	**5 cm**	**28.5 khz**	Anexo 25: Captura imagen Asus A555L frecuencia 5 cm. Anexo 26: Captura audio generado Asus A555L frecuencia 5 cm.
Equipo encendido, ejecutando programa (Word)	**10 cm**	**28.6 khz**	Anexo 27: Captura imagen Asus A555L frecuencia 10 cm. Anexo 28**:** Captura audio generado Asus A555L frecuencia 10 cm.

Equipo reiniciando	**10 cm**	**24.3 khz**	Anexo 29: Captura imagen Asus A555L frecuencia 10 cm. Anexo 30: Captura audio generado Asus A555L frecuencia 10 cm.
Escuchar entorno del Cuarto solo	**Posición, centro del cuarto.**	**2000 hz**	Anexo 31: Captura imagen frecuencia de ambiente cuarto solo. Anexo 32: Captura audio frecuencia de ambiente cuarto solo.

Del resultado anterior que se visualiza en la tabla 10, se puede evidenciar que en una distancia de 5 – 10 cm, se logró capturar de diferentes comportamientos del equipo de cómputo, frecuencias ultrasónicas, que van desde un rango de 2000 hz a 28 Khz. En los anexos se encuentra el soporte del audio y la imagen de dicha captura.

También se utilizó la grabadora y el Micrófono MSH-6 Stereo Mic, para capturar las frecuencias ultrasónicas que por defecto género el equipo computo Asus A555L.

Figura 35: Micrófono MSH-6 Stereo Mic. Fuente Propia.

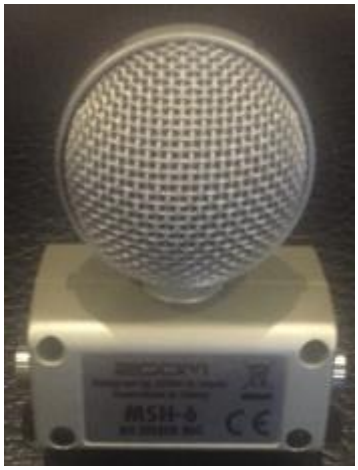


Tabla 10: Resultados usando hardware y software de la grabadora. Fuente Propia.

Caso de prueba	**Distancia**	**Frecuencia capturada**	**Imágenes y audios**
Apagar equipo	**5 cm**	**24.3 khz**	Anexo 33: Captura imagen Asus A555L frecuencia 5 cm. Anexo 34: Captura audio generado Asus A555L frecuencia 5 cm.
Encendido equipo de	**5 cm**	**24.5 khz**	Anexo 35: Captura imagen Asus A555L frecuencia 5 cm.

computo			Anexo 36: Captura audio generado Asus A555L frecuencia 5 cm.
Apagar equipo	**10 cm**	**24.2 khz**	Anexo 37: Captura imagen Asus A555L frecuencia 10 cm. Anexo 38: Captura audio generado Asus A555L frecuencia 10 cm.
Equipo encendido, sin ejecutar programas	**10 cm**	**24.5 khz**	Anexo 39: Captura imagen Asus A555L frecuencia 10 cm. Anexo 40: Captura audio generado Asus A555L frecuencia 10 cm.
Equipo encendido, ejecutando programa (Arduino)	**10 cm**	**24.7 khz**	Anexo 41: Captura imagen Asus A555L frecuencia 10 cm. Anexo 42: Captura audio generado Asus A555L frecuencia 10 cm.
Transferencia de datos a una	**10 cm**	**16 khz**	Anexo 43: Captura imagen Asus A555L frecuencia 10 cm.

unidad de almacenamiento extraíble			Anexo 44: Captura audio generado Asus A555L frecuencia 10 cm.
Disco duro	**5 cm**	**16.5 khz**	Anexo 45: Captura imagen Asus A555L frecuencia 10 cm. Anexo 46**:** Captura audio generado Asus A555L frecuencia 10 cm.
Equipo encendido, ejecutando programa (Word)	**10 cm**	**28.6 khz**	Anexo 47: Captura imagen Asus A555L frecuencia 10 cm. Anexo 48: Captura audio generado Asus A555L frecuencia 10 cm.
Equipo reiniciando	**10 cm**	**24.5 khz**	Anexo 49: Captura imagen Asus A555L frecuencia 10 cm. Anexo 50: Captura audio generado Asus A555L frecuencia 10 cm.
Sonido por defecto del	**Posición**	**2500 hz**	Anexo 51: Captura imagen frecuencia de ambiente cuarto solo.

entorno del Cuarto solo	**centro del cuarto**		Anexo 52: Captura audio frecuencia de ambiente cuarto solo.

Del resultado anterior que se visualiza en la tabla 11, se puede evidenciar que en una distancia de 5 – 10 cm, se logró capturar de diferentes comportamientos del equipo de cómputo, frecuencias ultrasónicas, que van desde un rango de 2500 hz a 28 Khz.

A continuación, se muestran algunas capturas de frecuencia ultrasónica que van desde de la figura 34 a la 40, se puede observar que existe una escala de medidas y en color amarillo encerrado en un cuadro rojo en posición horizontal, se evidencia el comportamiento que tuvo el sonido capturado de los resultados de la tabla 11. En los anexos se encuentra el soporte del audio y la imagen del resto de las capturas. La importancia de tomar la captura, es evidenciar que, con las pruebas y resultados arrojados, se identifique que si hubo captura de frecuencias ultrasónicas en todos los escenarios descritos.

Figura 36: Medida Espectrograma encendido equipo de cómputo. Fuente Propia.

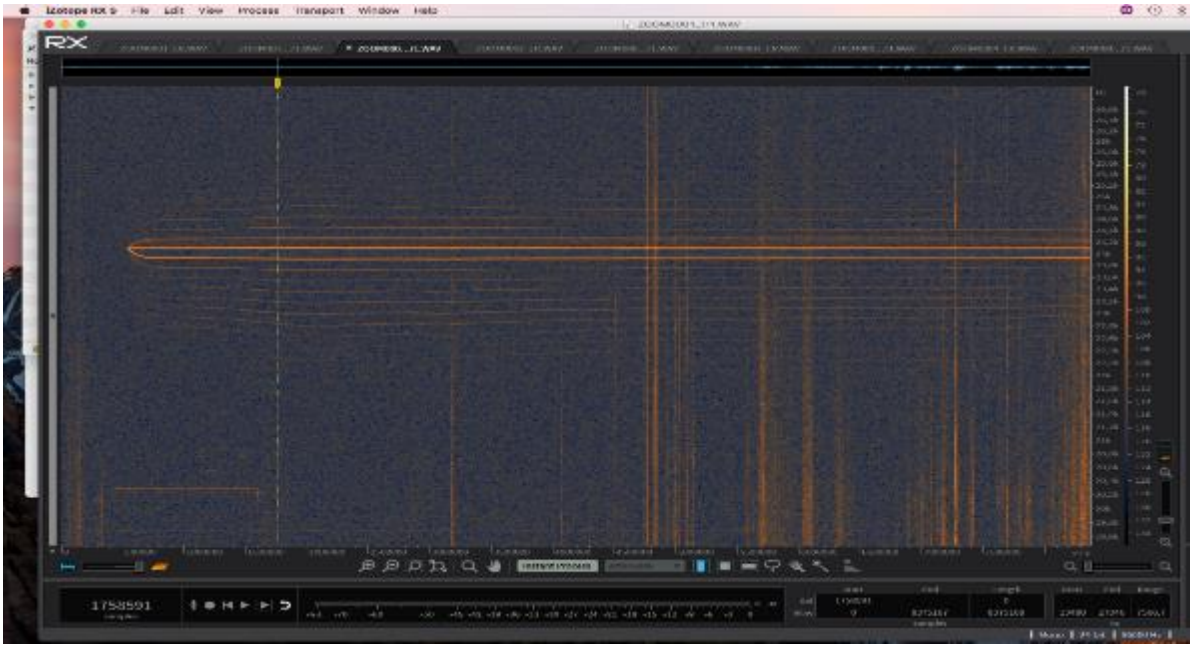


Figura 37: Medida Espectrograma Apagar Equipo 5 cm. Fuente Propia.

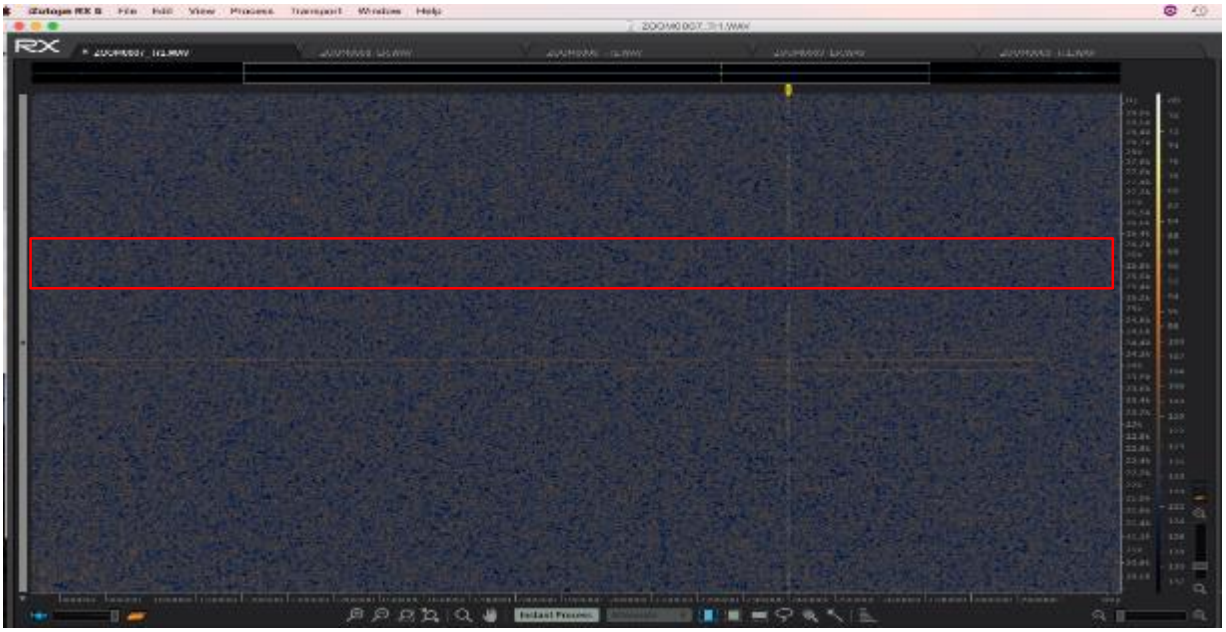


Figura 38: Medida Espectrograma Apagar equipo 10 cm. Fuente Propia.

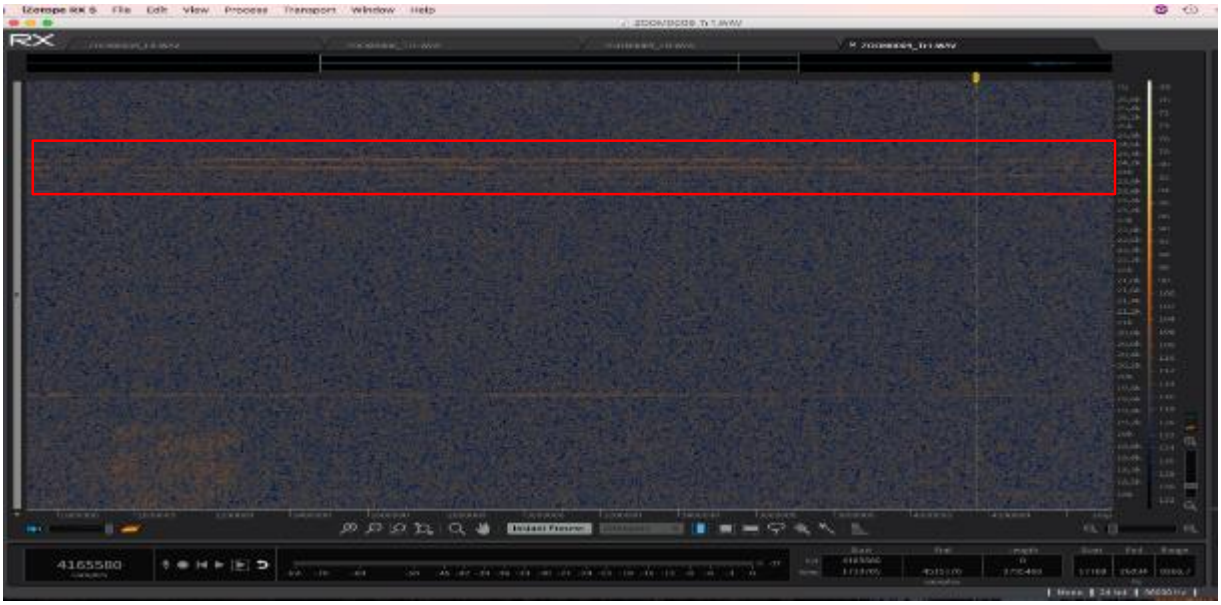


Figura 39: Medida Espectrograma Equipo encendido sin ejecutar programas. Fuente Propia.

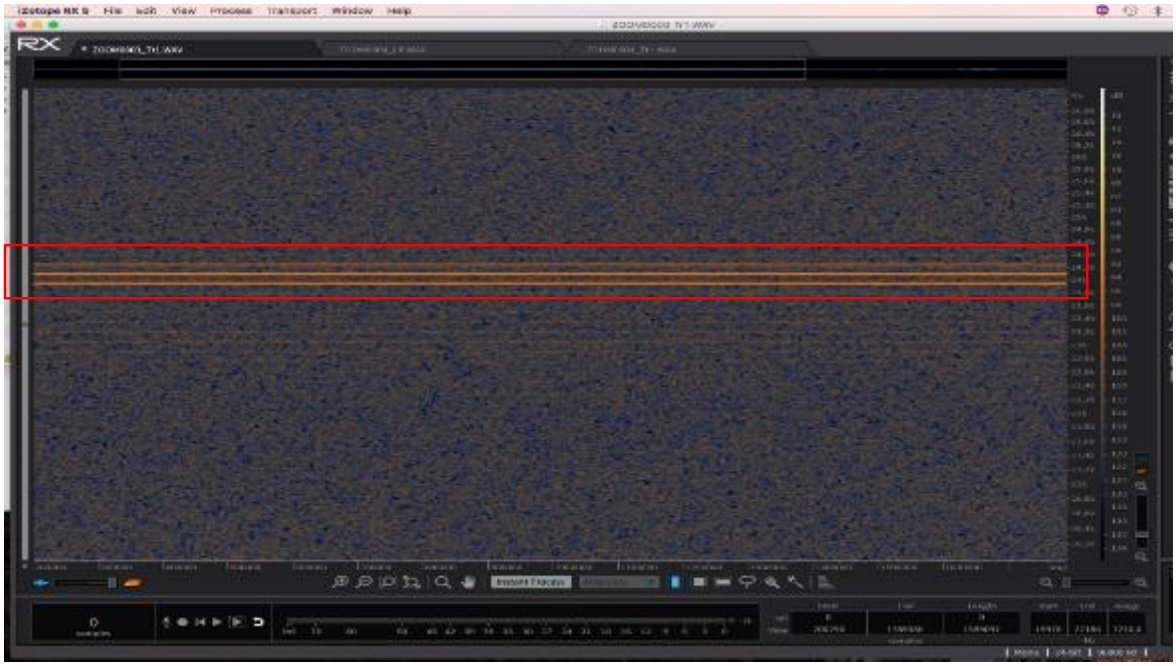


Figura 40: Medida Espectrograma equipo encendido programa Arduino. Fuente Propia.

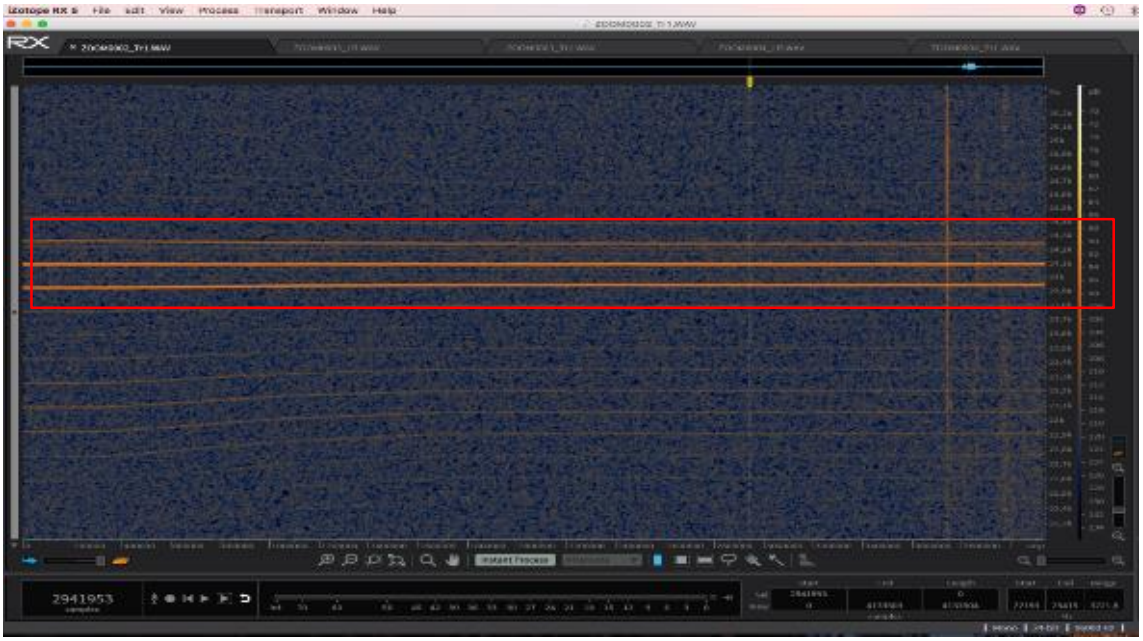


Figura 41: Medida Espectrograma Transferencia de datos a una unidad de almacenamiento extraíble. Fuente Propia.

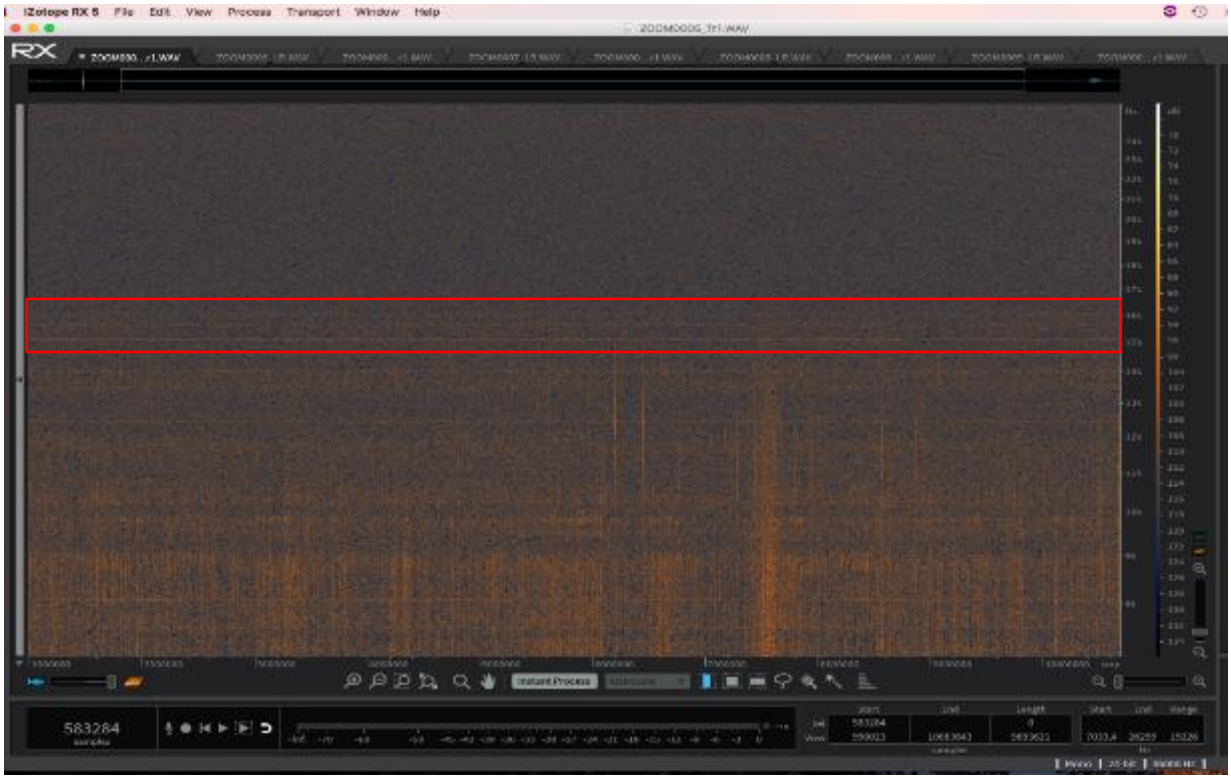
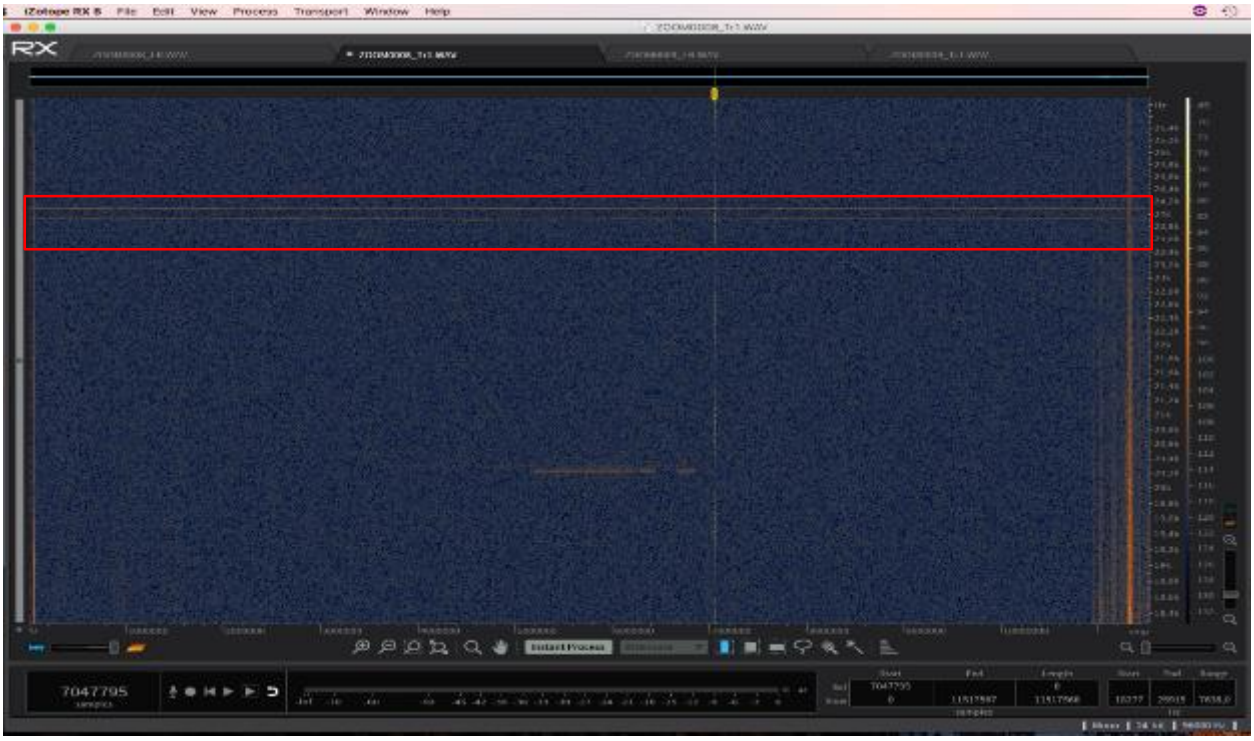


Figura 42: Medida Espectrograma Reiniciar Equipo. Fuente Propia.



El mismo ejercicio se realizó con el equipo de cómputo Asus GL555VW, usando el micrófono - XYH-6 Stereo Mic.

Tabla 11: Resultados usando hardware y software de grabadora. Fuente Propia.

Caso de prueba	Distancia	Frecuencia capturada	Imágenes y audios

Encendido equipo de computo	**30 cm**	**19.7 khz**	Anexo 53: Ver Carpeta Anexos.
Apagar equipo	**5 cm**	**24 khz**	Anexo 53: Ver Carpeta Anexos.
Apagar equipo	**10 cm**	**24 khz**	Anexo 53: Ver Carpeta Anexos.
Encendido equipo de computo	**10 cm**	**24 khz**	Anexo 53: Ver Carpeta Anexos.
Equipo encendido, sin ejecutar programas	**10 cm**	**24.5 khz**	Anexo 53: Ver Carpeta Anexos.
Equipo encendido, ejecutando programa (Visual Studio)	**30 cm**	**19.7 khz** **23.9 khz**	Anexo 53: Ver Carpeta Anexos.
Transferencia de datos a una unidad de almacenamiento extraíble	**10 cm**	**28.5 khz**	Anexo 53: Ver Carpeta Anexos.

Disco duro	**5 cm**	**28.5 khz**	Anexo 53: Ver Carpeta Anexos.
Equipo encendido, ejecutando programa (Word)	**10 cm**	**19.7 khz** **23.9 khz**	Anexo 53: Ver Carpeta Anexos.
Equipo reiniciando	**10 cm**	**19.7 khz** **23.9 khz**	Anexo 53: Ver Carpeta Anexos.
Escuchar entorno del Cuarto solo	**Posición centro del cuarto**	**2000 hz**	Anexo 53: Ver Carpeta Anexos.

Del resultado anterior que se visualiza en la tabla 12, se puede evidenciar que en una distancia de 5 – 10 cm, se logró capturar de diferentes comportamientos del equipo de cómputo, frecuencias ultrasónicas, que van desde un rango de 2000 hz a 28 Khz. En los anexos se encuentra el soporte del audio y la imagen de las capturas.

Resultados obtenidos con el Micrófono MSH-6 Stereo Mic.

Tabla 12: Resultados usando hardware y software de grabadora. Fuente Propia.

Caso de prueba	**Distancia**	**Frecuencia capturada**	**Ruta Anexos**
Encendido equipo de computo	**10 cm**	**24.5 khz**	Anexo 53: Ver Carpeta Anexos.
Apagar equipo	**5 cm**	**24.3 khz**	Anexo 53: Ver Carpeta Anexos.
Apagar equipo	**10 cm**	**24.2 khz**	Anexo 53: Ver Carpeta Anexos.
Encendido equipo de computo	**10 cm**	**24.5 khz**	Anexo 53: Ver Carpeta Anexos.
Equipo encendido, sin ejecutar programas	**10 cm**	**24.5 khz**	Anexo 53: Ver Carpeta Anexos.
Equipo encendido, ejecutando programa (Arduino)	**10 cm**	**24.7 khz**	Anexo 53: Ver Carpeta Anexos.

Transferencia de datos a una unidad de almacenamiento extraíble	**10 cm**	**16 khz**	Anexo 53: Ver Carpeta Anexos.
Disco duro	**5 cm**	**16.5 khz**	Anexo 53: Ver Carpeta Anexos.
Equipo encendido, ejecutando programa (Word)	**10 cm**	**28.6 khz**	Anexo 53: Ver Carpeta Anexos.
Equipo reiniciando	**10 cm**	**24.5 khz**	Anexo 53: Ver Carpeta Anexos.
Escuchar entorno del Cuarto solo	**Posición centro del cuarto**	**2500 hz**	Anexo 53: Ver Carpeta Anexos.

Del resultado anterior (tabla 12), se puede evidenciar que en una distancia de 5 – 10 cm, se logró capturar de diferentes comportamientos del equipo de cómputo, frecuencias ultrasónicas, que van desde un rango de 2500 hz a 28 Khz. En los anexos se encuentra el soporte del audio y la imagen de las capturas

Adicional a lo anterior, se utilizó un software instalado en los equipos de cómputo y con su propio hardware de sonido se realizó el mismo ejercicio de la prueba 3.

Pruebas de recepción:

Se realizaron las pruebas en un ambiente real (interconexión de equipos de cómputo en un ambiente de oficina), se relaciona el software y equipos utilizados:

Figura 43: Ambiente Tipo Oficina. Fuente Propia.

Software Audacity utilizado para la recepción de ondas sonoras ultrasónica en los dos equipos de cómputo.

Tabla 13: Resultados usando software Audacity. Fuente Propia.

Caso de prueba	Distancia	Frecuencia capturada	Software
Equipo encendido sin ejecutar programas	10 cm	Capturó por debajo de los 16 khz	Audacity
Transferencia de datos a disco extraible	10 cm	Capturó por debajo de los 15 khz	Audacity
Apagar equipo	10 cm	Capturó por debajo de los 15 khz	Audacity
Encender equipo	10 cm	Capturó por debajo de los 15 khz	Audacity
Ejecución de software	5 cm	Capturó por debajo de los 16 khz	Audacity

Se concluye que el software (Audacity) obtenido con licencia gratuita, instalados en la máquina de cómputo, no permiten realizar la captura necesaria para validar la identificación de ondas ultrasónicas, en este tipo de ambientes (no se capturo imágenes). Con lo anterior también se concluye que no todo el software que existe para capturar frecuencias ultrasónicas cuenta con condiciones óptimas para realizar el objetivo que se tiene previsto, por eso la importancia de haber probado por varios medios. También debido a que la frecuencia ultrasónica está en el rango de los 20 Khz hacia arriba y en este caso no cumple la condición.

Prueba 4: Mediante esta prueba se logró evaluar la efectividad y usabilidad del software que se encuentra disponible para simular el robo de información desde una máquina de cómputo a otra usando un método que modula y desmodula la información que es transmitida por ondas ultrasónicas.

a. El primer software que se evaluó fue quietnet- master desarrollado por Python de distribución libre por Github, para sistema operativo Windows en ambiente tipo oficina, donde se logró enviar información de un equipo de cómputo a otro. Y se identificó también la flexibilidad de uso que posee la aplicación.

Se identifica que el Quienet utiliza una base de datos almacenado que se encuentra almacenado en su librería , en esta base de datos se encuentra el abecedario, números y caracteres especiales los cuales son representados en números binarios, con el objetivo de traducir cada letra, carácter o número, logrando así modular la información que se envió. En la siguiente imagen se puede apreciar el almacenamiento y la traducción en binarios.

Figura 44: Diccionario de datos Quietnet. Fuente Software Quietnet.

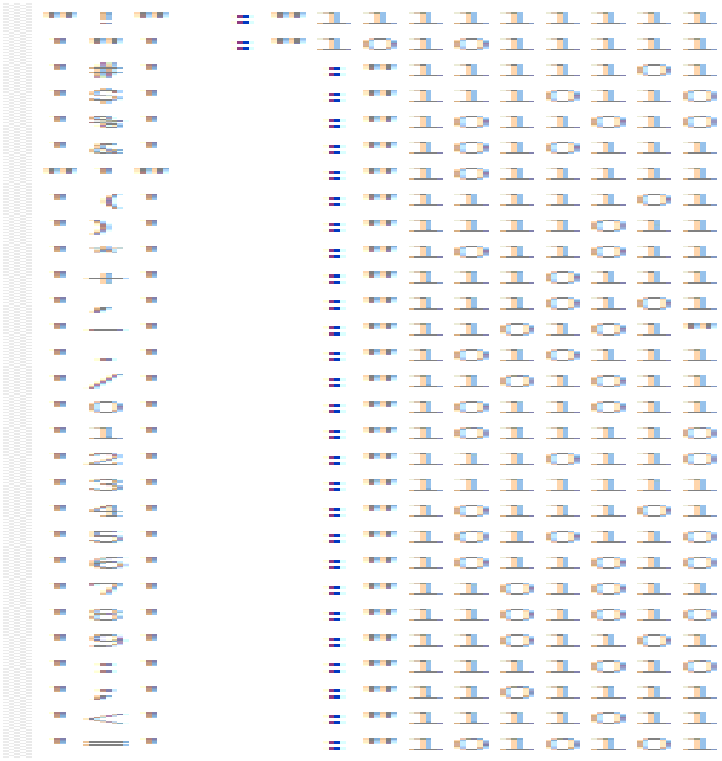


Figura 45: Captura información Quienet. Fuente Propia.

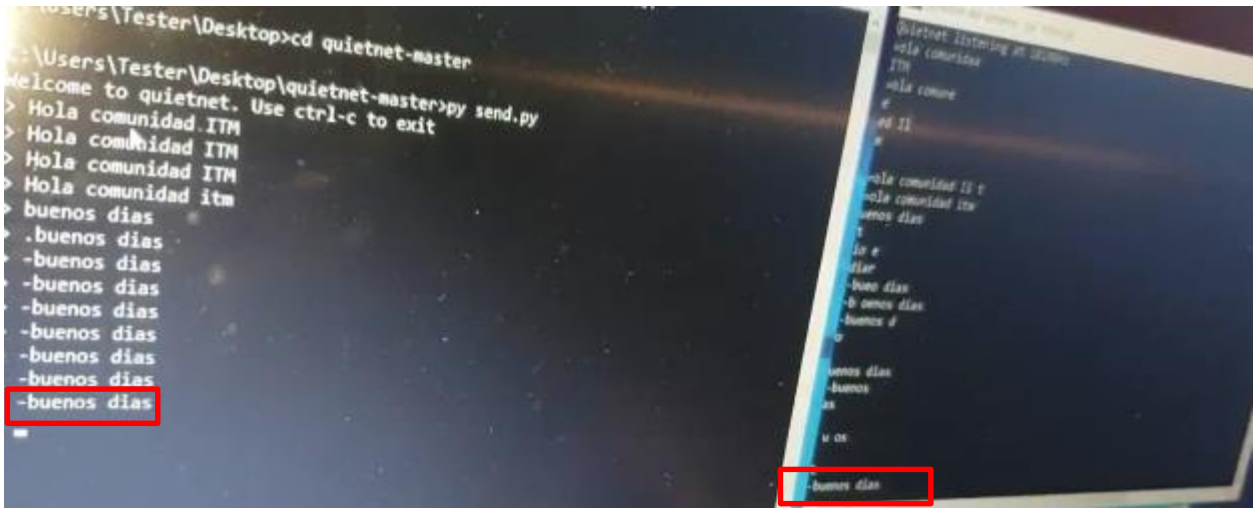


Tabla 14: Resultados captura de información Quienet. Fuente Propia.

Información transmitida	**Información capturada**	**Frecuencia**	**Distancia**	**Resultado**
Hola comunidad ITM	ola comunidad ITM	19500 HZ	1 mts	Perdida de la letra H
Buenos días	Buenos días	19500 HZ	1 mts	Transmisión exitosa

Tabla 15: Captura QUIETNET- MASTER información ambiente libre de ruido. Fuente Propia.

Información transmitida	**Información capturada**	**Frecuencia**	**Distancia**	**Resultado**
Hola	ola	19500 HZ	1 mts	Perdida de la letra H
prueba2	prueba2	19500 HZ	1 mts	Transmisión exitosa

En la imagen 52, se puede apreciar cómo fue posible transportar de un punto X a un punto Y por medio de ondas ultrasónicas. Adicional podemos observar en los resultados de la tabla 14 y 15, que a una distancia de 1 mts de un equipo del otro se logró enviar y recibir con éxito la información enviada.

El segundo software evaluado fue el gnuradio para el sistema operativo Windows en ambiente en ambiente libre de ruido, donde se logró enviar información de un punto a otro, pero la experiencia, usabilidad y estructura no es tan buena como la del Quienet.

Se logró modular y de modular la información que fue capturada y enviada a través de la aplicación Gnuradio, en la figura 54 se puede apreciar lo que se envió, (se usó el puerto 1234 para transportar la información) y en la pantalla 1 lo que capturo (Se abrió el puerto 9989 donde se recibió la información), en el fondo de la figura se aprecia la distribución del sonido capturado en el momento de enviar la información. La frecuencia que se utilizo fue 19500 hz.

Figura 46: Resultados obtenidos modulando y demodulando con Gnuradio.

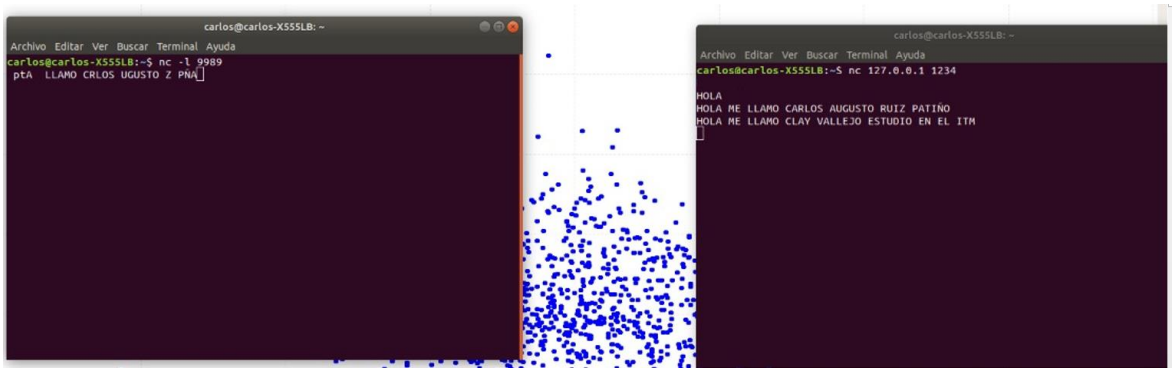


Tabla 16: Resultados obtenidos captura de información Gnuradio. Fuente Propia.

Información transmitida	**Información capturada**	**Frecuencia**	**Distancia**	**Resultado**
HOLA ME LLAMO CARLOS AUGUSTO RUIZ PATIÑO	LLAMO CARLOS UGUSTO Z PAÑA	19500 HZ	1 mts	Perdida de datos
HOLA ME LLAMO CLAY VALLEJO ESTUDIO EN EL ITM	NO CAPTURADA	19500 HZ	1 mts	No captura

Tabla 17: Captura Gnuradio información ambiente libre de ruido. Fuente Propia.

Información transmitida	**Información capturada**	**Frecuencia**	**Distancia**	**Resultado**
Hola	ola	19500 HZ	1 mts	Perdida de la letra H
prueba3	prueba3	19500 HZ	1 mts	Transmisión exitosa

Se identifica que en los resultados de la tablas 15 y 16, en algunos casos llego incompleta la información y en algunos casos no fue posible capturarla.

7.3 Clasificación de información.

Definidos los grupos de clasificación, se realizó un nombramiento basado en la norma ISO 27001, en el cual corresponde un identificador que conglomere la mayoría de los atributos que califican los grupos. De tal manera a consideración se realizó el siguiente nombramiento:

Grupo 1: Secreto: Nivel más alto de clasificación de material en un nivel nacional o gubernamental.

Grupo 2: Confidencial: Nivel de confidencialidad de la información se incremente.

Grupo 3: Restringido: Para niveles medios de confidencialidad.

Grupo 4: Uso interno: Información con un nivel bajo de confidencialidad.

Grupo 5: Público: Todas las personas pueden ver la información.

Grupo 6: Sin clasificar: Captación de información que no está en ninguno de los 5 grupos clasificatorios, y que debe ser intervenido por una persona.

La categoría de seguridad ayuda a proteger la información de eventos que podrían impactar involuntariamente al propietario de esta información: este aspecto explica por qué necesitamos para etiquetar información con una categoría de seguridad.

7.4 Evaluación del modelo.

Código fuente y librería, ejecutable y algunas pantallas de configuración del software CVEI.

Anexo 54: Código fuente CVEI. Fuente Propia.

Con el diccionario de palabras clave listado se comparó con la recepción de datos por ultrasonido. En las pruebas coincidieron las palabras enviadas con el clasificador de grupos a nivel de seguridad.

Realizando múltiples pruebas en los ambientes de tipo oficina y ambiente libre de ruido se realizó los ajustes a la parametrización de las propiedades de los dispositivos para garantizar un envió de paquetes exitoso, se dejó con la configuración que en pruebas otorgo la mejor tasa de transferencia.

En el siguiente anexo se encuentra la librería y el ejecutable de la aplicación CVEI.

Anexo 55: Librería y ejecutable software CVEI.

A continuación, se describe algunas funcionalidades del software las cuales son ilustradas en las figuras 55 hasta la 57, donde se puede apreciar los campos y funcionalidades necesarias para ingresar y clasificar la información:

En la figura 45, se ilustra el formulario que administra el almacenamiento de la información por cada nivel de clasificación.

Figura 47: Pantalla almacenamiento de información clasificada por niveles. Fuente Propia.

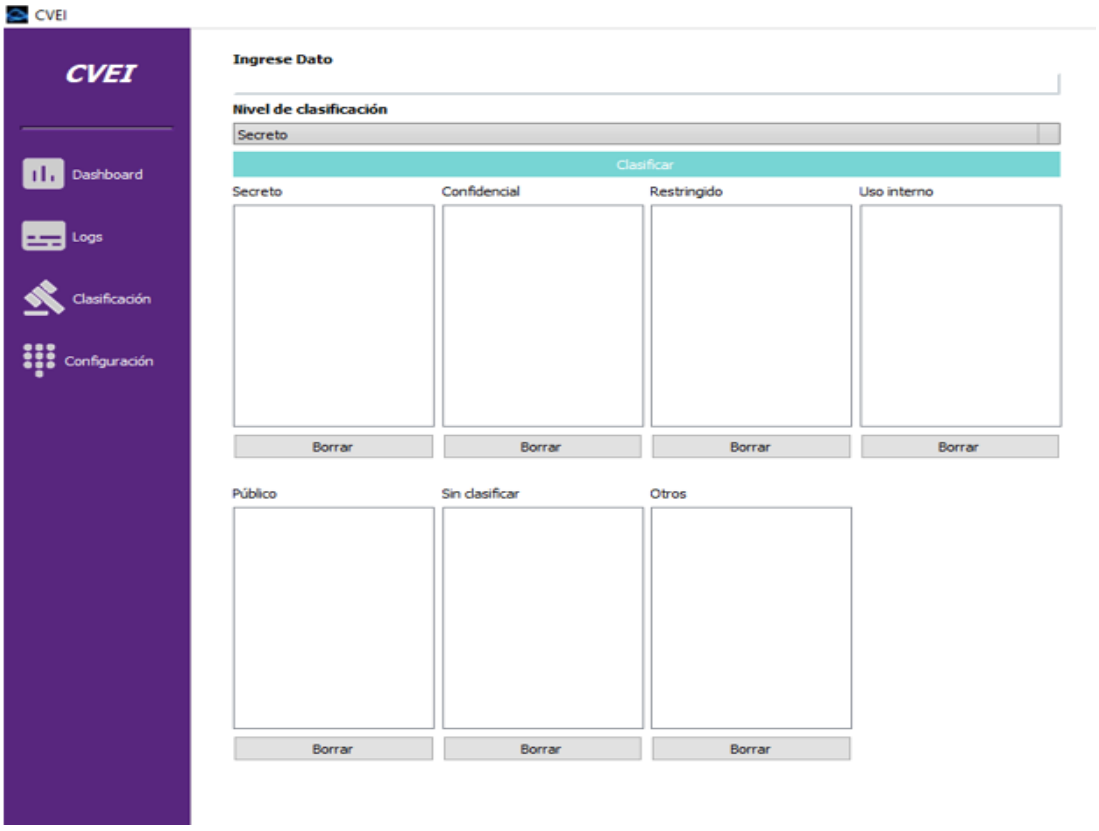
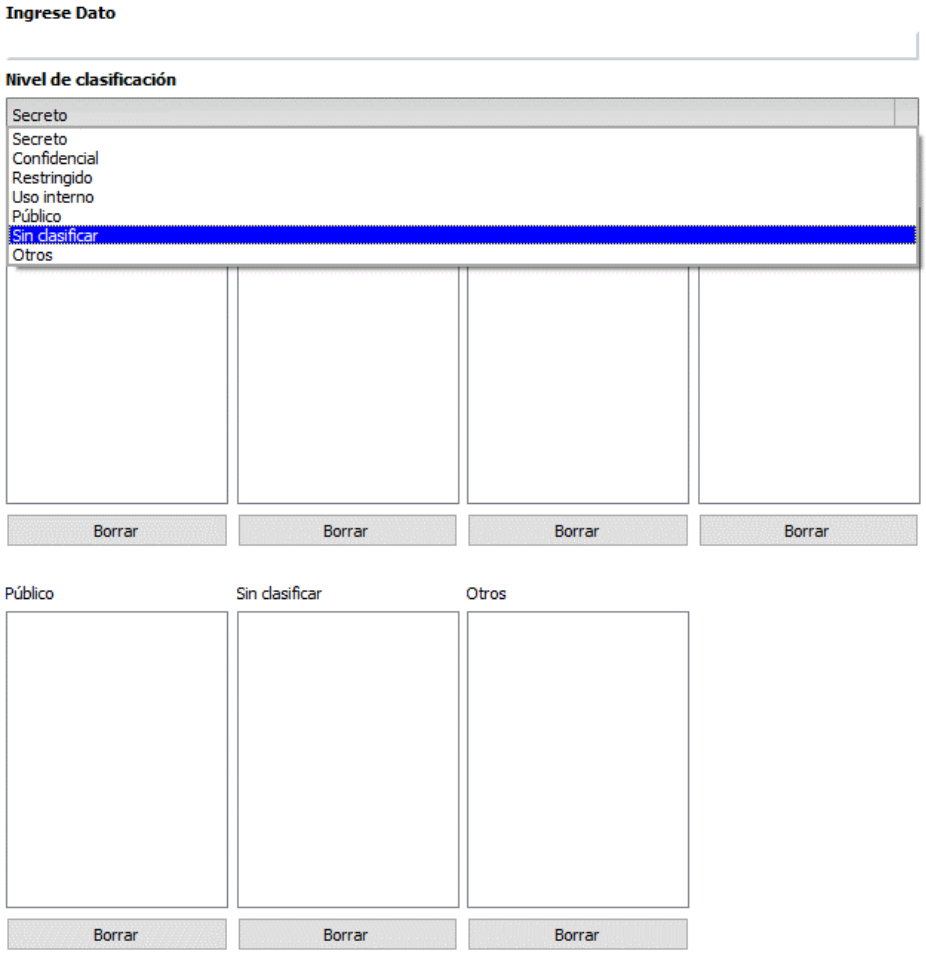


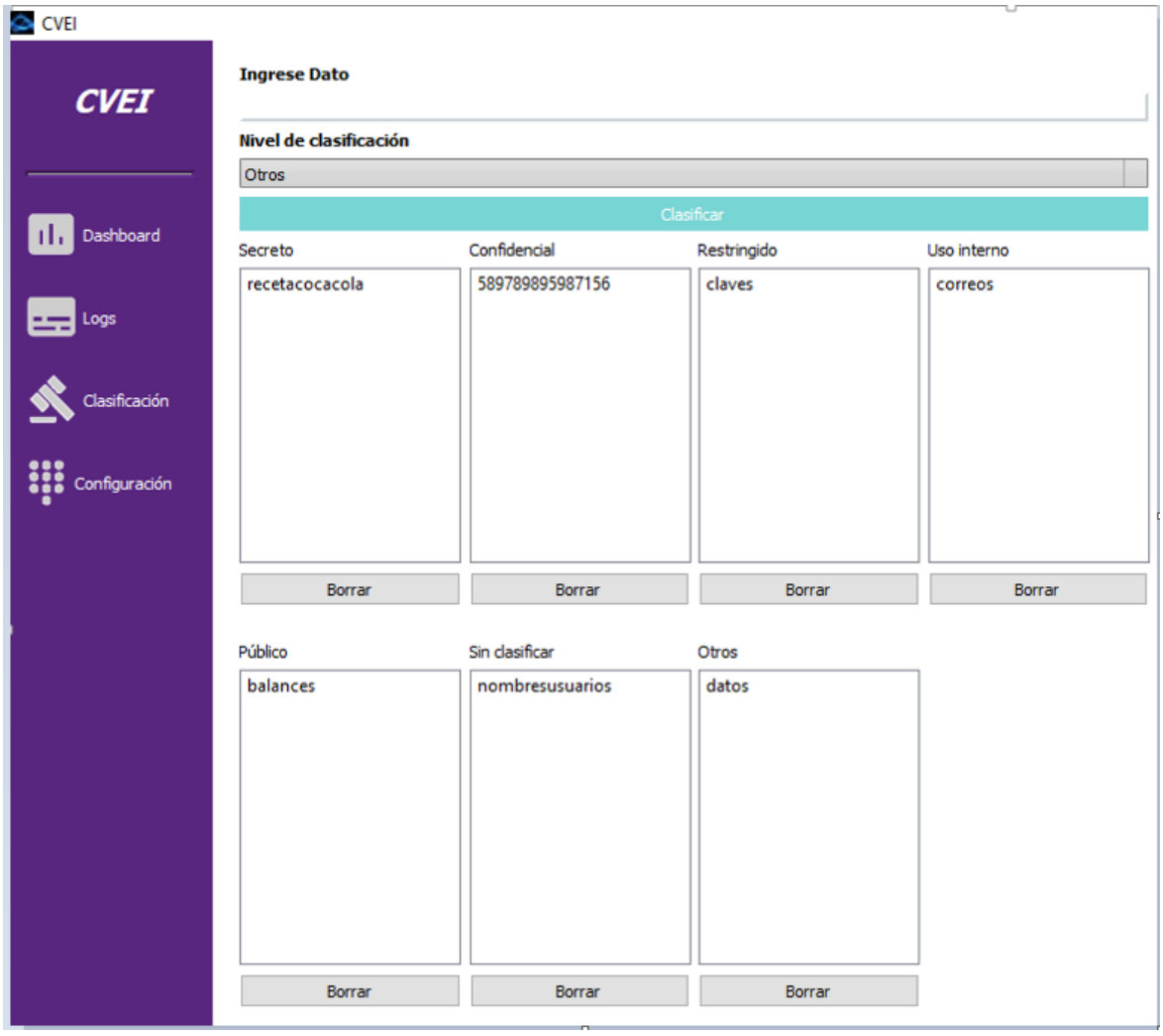
Figura 48: Lista de niveles de clasificación. Fuente Propia.

Ejemplo de datos de clasificación.



En la figura 47, se ilustra como ejemplo la información que fue ingresada y almacenada por cada una de las categorías.

Figura 49: Información almacenada por categorías. Fuente Propia.



Evaluación del software en los dos ambientes seleccionados.

Resultados escenario 1, ambiente libre de ruido: Se obtuvo los siguientes resultados colocando los equipos de cómputo en una posición opuesta (en reversos).

- Se ubicaron los equipos Asus 555L equipo víctima y Asus GL555VW equipo atacante a una distancia de 1 mtrs, en una posición opuesta.

Figura 50: Resultados ambiente libre de ruido. Fuente Propia.

- Se ejecutó el software desarrollado CVEI en cada uno de los equipos con los parámetros establecidos, que son la frecuencia y la información almacenada en los niveles de clasificación.

Asus GL555VW equipo atacante. En la figura 49 se ilustra que la aplicación se activó de forma correcta para el envío de información.

Figura 51: Activación software CVEI equipo atacante en ambiente libre de ruido. Fuente Propia.

Asus 555L equipo víctima. En la figura 50, se ilustra que la aplicación se activó de forma correcta para escuchar la información que es trasmitida por el canal.

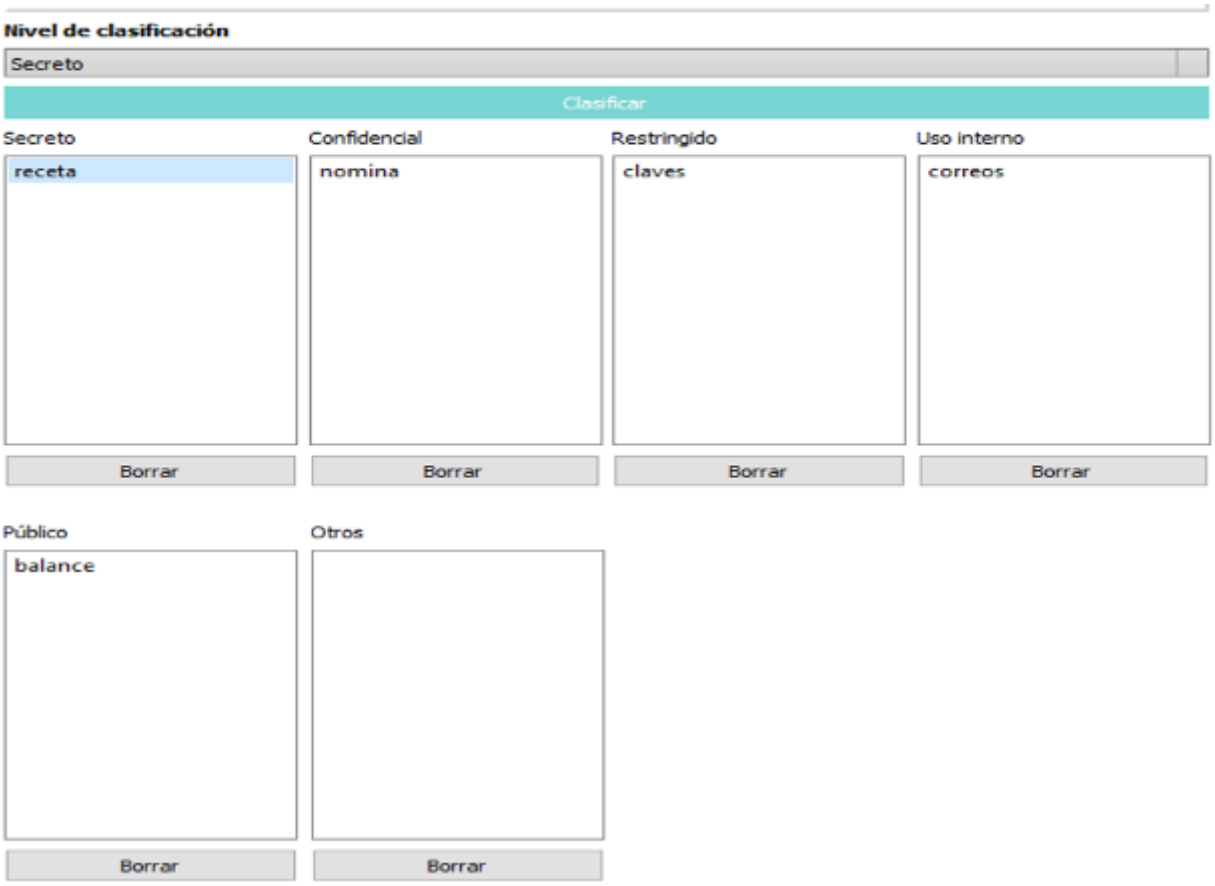
Figura 52: Activación software CVEI equipo victima en ambiente libre de ruido. Fuente

Propia

El equipo victima Asus 555L, el usuario dígito en la pantalla llamada **malware de envío**, información (1 palabra) de cada uno de los niveles de clasificación.

En la figura 51, se ilustra la información que fue almacenada para cada nivel de clasificación, la cual fue utilizada para comprobar el buen funcionamiento de la aplicación desarrollada CVEI .

Figura 53: Información almacenada para probar con el ambiente libre de ruido. Fuente



Propia.

En el ambiente libre de ruido del laboratorio artes digitales del ITM **(El software se comportó de una manera más adaptable dado a las condiciones del ambiente)**, en el momento que se activa el software CVEI se puede ver cómo se obtiene información circulante de lo que se capta en ambiente entregando información aleatoria del abecedario como (**a, b, a, o, n, a, e6 y e** entre otros, esta información se almaceno en el log en el nivel de clasificación **Sin Clasificar**), además se obtuvo por cada nivel de clasificación utilizando el software propio CVEI los resultados que se aprecian en las figuras (61, 62, 63, 64,65 y 66) se observa que el atacante trata de vulnerar a una distancia de 1 m la palabra **receta, nomina, claves, correos, balance y hola** de los niveles de

clasificación **Secreto**, **Confidencial, Restringido, Uso interno, Publico y Sin Clasificar,** pero no fue exitoso el ataque de fuga de información, dado que el Sofware CVEI logro detectar, notificar y almacenar el log de dicha fuga de información. El eje x que va de -1 a 1 representa una función senoidal una función senoidal muestra claramente en el momento que fue enviada la señal ultrasónica de 22000 hz, en el periodo de tiempo el eje Y represento el número de muestra que se tomó por la trama que entrego el audio capturado, entonces el samples rate, lo que hizo fue discretizar la señal convirtiéndola de forma análoga a digital.

En la figura 52, se ilustra la detención de la palabra receta, la cual se encuentra en el nivel de clasificación Secreto. Se visualiza en dicha imagen un mensaje alertando la acción y adicional se aprecia la variación de la gráfica en el momento que se trató de exfiltrar la información en una frecuencia considerada ultrasonica de 22000 Hz.

- **Secreto:** receta

Figura 54: Detención información nivel de clasificación secreto. Fuente propia.

En la figura 53, se ilustra la detención de la palabra nomina, la cual se encuentra en el nivel de clasificación Confidencial. Se visualiza en dicha imagen un mensaje alertando la acción y adicional se aprecia la variación de la gráfica en el momento que se trató de exfiltrar la información en una frecuencia considerada ultrasónica de 22000 Hz.

Confidencial: nomina

Figura 55: Detención información nivel de clasificación confidencial. Fuente propia.

En la figura 54, se ilustra la detención de la palabra claves, la cual se encuentra en el nivel de clasificación Restringido. Se visualiza en dicha imagen un mensaje alertando la acción y adicional se aprecia la variación de la gráfica en el momento que se trató de exfiltrar la información en una frecuencia considerada ultrasónica de 22000 Hz.

Restringido: claves

Figura 56: Detención información nivel de clasificación restringido. Fuente propia.

En la figura 55, se ilustra la detención de la palabra correos, la cual se encuentra en el nivel de clasificación Uso Interno. Se visualiza en dicha imagen un mensaje alertando la acción y adicional se aprecia la variación de la gráfica en el momento que se trató de exfiltrar la información en una frecuencia considerada ultrasónica de 22000 Hz.

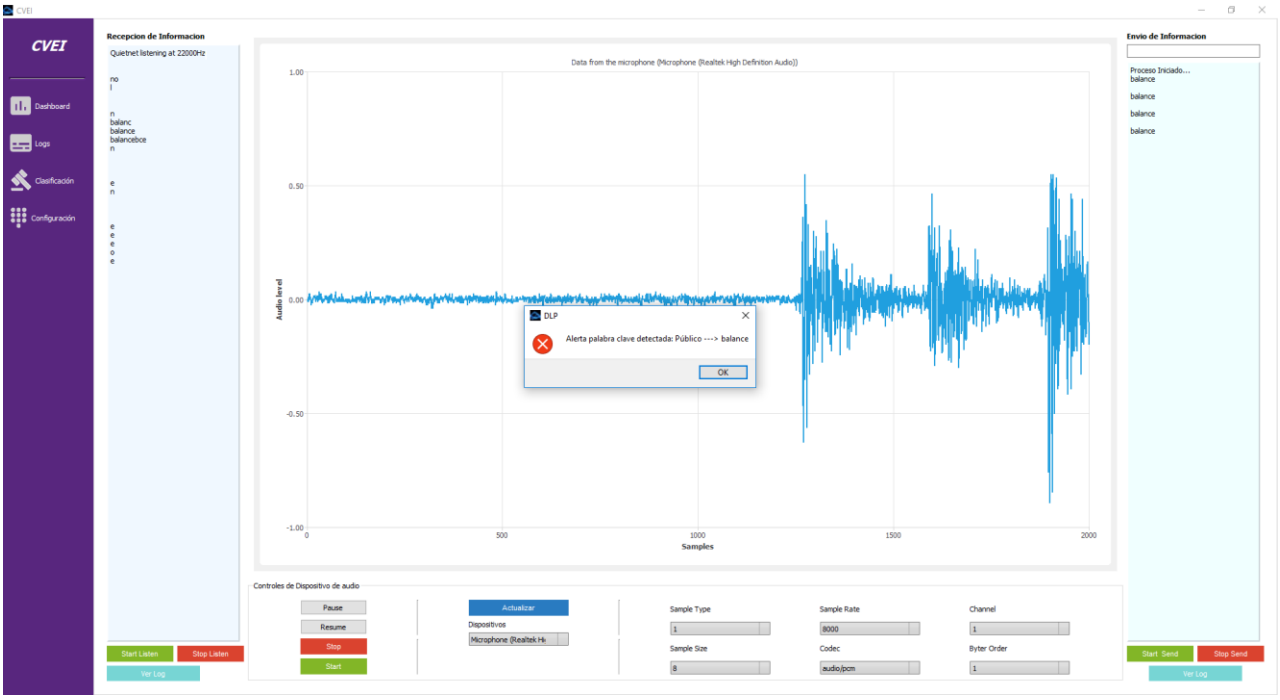
Uso interno: correos

Figura 57: Detención información nivel de clasificación uso interno. Fuente propia.

En la figura 56, se ilustra la detención de la palabra balance, la cual se encuentra en el nivel de clasificación Público. Se visualiza en dicha imagen un mensaje alertando la acción y adicional se aprecia la variación de la gráfica en el momento que se trató de exfiltrar la información en una frecuencia considerada ultrasónica de 22000 Hz.

Público: balance

Figura 58: Detención información nivel de clasificación público. Fuente propia.



En la figura 57, se ilustra la detención de la palabra hola, la cual se encuentra en el nivel de clasificación Sin Clasificar. Se visualiza en dicha imagen un mensaje alertando la acción y adicional se aprecia la variación de la gráfica en el momento que se trató de exfiltrar la información

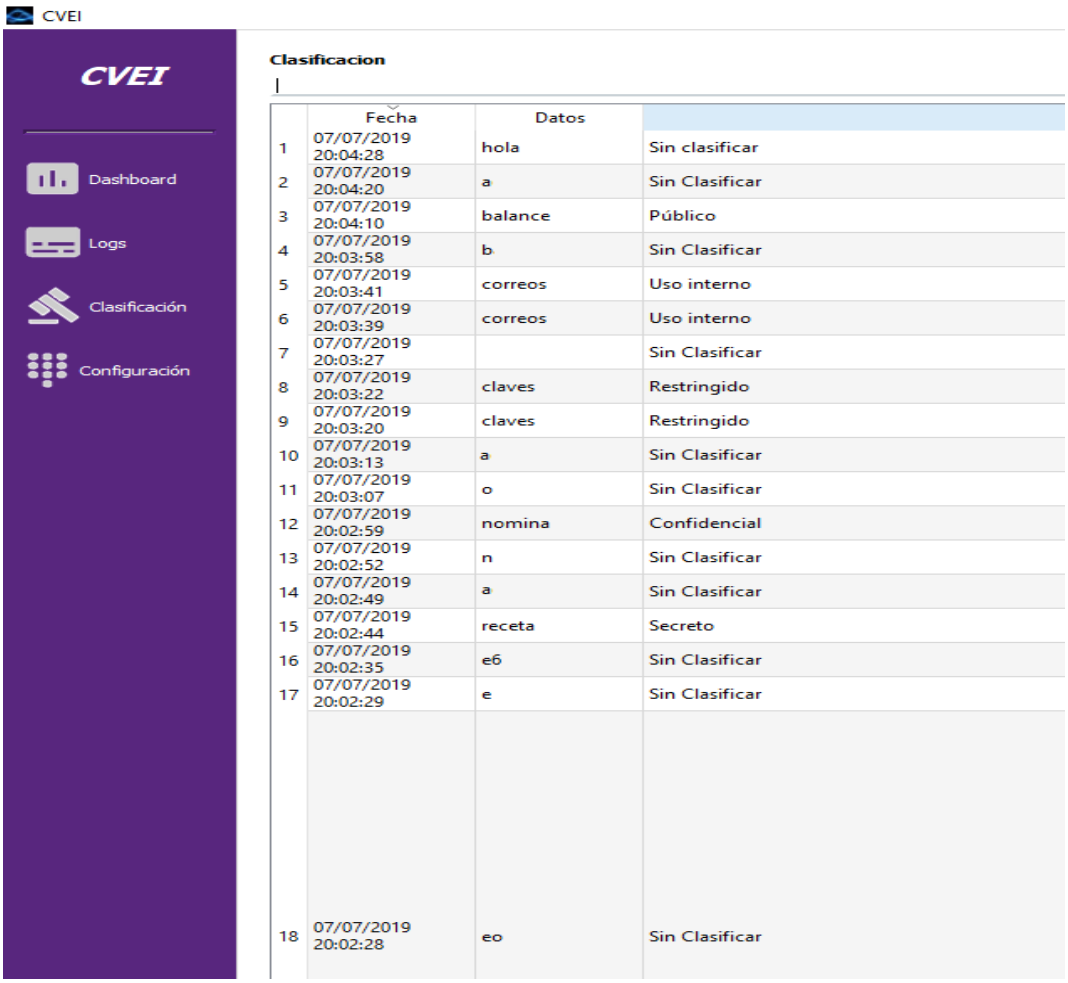
Sin clasificar: hola

Figura 59: Detención información nivel de clasificación sin clasificar. Fuente propia.

De la interacción que se ilustran en figuras 52 hasta la 57, se almacena en el log transaccional, toda la información que se detectó, entregado en el informe datos detallados como la fecha día/mes/año,

hora – minutos – segundos, la información que se trataron de exfiltrar y el nivel de clasificación al que pertenece. En la figura 58, se ilustra el orden como fue detectada la exfiltración de información.

Figura 60: Log de detección basado en nivel de clasificación. Fuente Propia.



	Fecha	Datos	
1	07/07/2019 20:04:28	hola	Sin clasificar
2	07/07/2019 20:04:20	a	Sin Clasificar
3	07/07/2019 20:04:10	balance	Público
4	07/07/2019 20:03:58	b	Sin Clasificar
5	07/07/2019 20:03:41	correos	Uso interno
6	07/07/2019 20:03:39	correos	Uso interno
7	07/07/2019 20:03:27		Sin Clasificar
8	07/07/2019 20:03:22	claves	Restringido
9	07/07/2019 20:03:20	claves	Restringido
10	07/07/2019 20:03:13	a	Sin Clasificar
11	07/07/2019 20:03:07	o	Sin Clasificar
12	07/07/2019 20:02:59	nomina	Confidencial
13	07/07/2019 20:02:52	n	Sin Clasificar
14	07/07/2019 20:02:49	a	Sin Clasificar
15	07/07/2019 20:02:44	receta	Secreto
16	07/07/2019 20:02:35	e6	Sin Clasificar
17	07/07/2019 20:02:29	e	Sin Clasificar
18	07/07/2019 20:02:28	eo	Sin Clasificar

Tabla 18: Resultados detección de información clasificada en ambiente libre de ruido. Fuente Propia.

Nivel de clasificación	**Información detectada**	**Distancia entre equipos**	**Frecuencia**	**Resultado obtenido**
Secreto	receta	1 mtrs	22000 Hz	Detección Exitosa
Confidencial	nomina	1 mtrs	22000 Hz	Detección Exitosa
Restringido	claves	1 mtrs	22000 Hz	Detección Exitosa
Uso interno	correos	1 mtrs	22000 Hz	Detección Exitosa
Público	balances	1 mtrs	2000 Hz	Detección Exitosa
Sin clasificar	hola	1 mtrs	22000 Hz	Detección Exitosa

De los resultados obtenidos en este escenario se puede determinar que, en un ambiente libre de ruido, se puede llevar con éxito el envío y la detención de información en frecuencias ultrasónicas hasta los 22000 Hz, a una distancia de 1 mts entre los equipos participantes, es de anotar que en el ambiente intervenido también se puede hacer uso de frecuencias audibles al ser

humano en cualquiera de sus rangos. Adicional se concluye que la información almacenada en los niveles de clasificación se encuentra seguros mediante el uso del software desarrollado CVEI.

Resultados escenario 2, tipo oficina: Se ejecutaron los siguientes pasos para las pruebas funcionales en el ambiente.

- Se ubicaron los equipos Asus 555L equipo víctima y Asus GL555VW equipo atacante a una distancia de 1 mtrs, en una posición frontal.

Figura 61: Ambiente tipo oficina. Fuente Propia.

- Se ejecutó el software desarrollado CVEI en cada uno de los equipos con los parámetros establecidos, que son la frecuencia y la información almacenada en los niveles de clasificación.

Asus GL555VW equipo atacante. En la figura 60, se ilustra que la aplicación se activó de forma correcta para el envío de información.

Figura 62: Activación software CVEI equipo victima en ambiente tipo oficina. Fuente Propia.

Asus 555L equipo víctima. En la figura 61, se ilustra que la aplicación se activó de forma correcta para escuchar la información que es trasmitida por el canal.

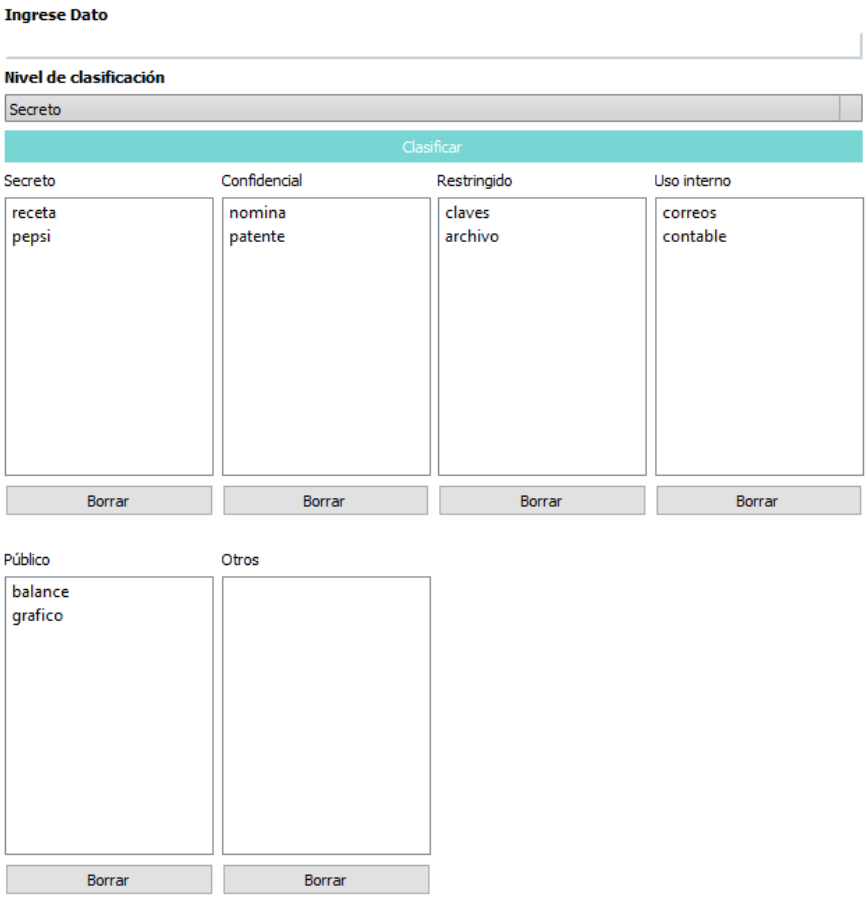
Figura 63: Activación software CVEI equipo victima en ambiente tipo oficina.

Fuente Propia.

El equipo victima Asus 555L, el usuario dígito en la pantalla llamada **malware de envío**, información (1 palabra) de cada uno de los niveles de clasificación.

En la figura 62, se ilustra la información que fue almacenada para cada nivel de clasificación, la cual fue utilizada para comprobar el buen funcionamiento de la aplicación desarrollada CVEI.

Figura 64: Información almacenada para probar con el ambiente tipo oficina.



Fuente Propia.

En el ambiente Tipo Oficina del laboratorio artes digitales del ITM **(El software se comportó de una manera menos adaptable dado a las condiciones del ambiente)**, en el momento que se activa el software CVEI se observó cómo se obtiene información circulante de lo que se capta en ambiente, entregando información aleatoria del abecedario y caracteres especiales como : **!, g, o, c, o, e y p** entre otros, esta información se almaceno en el log en el nivel de clasificación **Sin Clasificar**, además se obtuvo por cada nivel de clasificación utilizando el software propio CVEI los resultados que se aprecian en las figuras (71,72,73,74,75 y 76) se observa que el atacante trata de vulnerar a una distancia de 1 mt la palabra **pepsi, patente ,archivo, contable, grafico y caja** de los niveles de clasificación **Secreto**, **Confidencial, Restringido, Uso interno, Publico y Sin Clasificar,** pero no fue exitoso el ataque de fuga de información, dado que el Software CVEI logro detectar, notificar y almacenar el log de dicha fuga de información. . El eje x que va de -1 a 1 representa una función senoidal que muestra claramente en el momento que fue enviada la señal ultrasónica de 22000 hz, en el periodo de tiempo el eje Y represento el número de muestra que se tomó por la trama que entrego el audio capturado, entonces el samples rate, lo que hizo fue discretizar la señal convirtiéndola de forma análoga a digital.

En la figura 63, se ilustra la detención de la palabra pepsi, la cual se encuentra en el nivel de clasificación Secreto. Se visualiza en dicha imagen un mensaje alertando la acción y adicional se aprecia la variación de la gráfica en el momento que se trató de exfiltrar la información en una frecuencia considerada ultrasónica de 20000 Hz.

- **Secreto:** Pepsi

Figura 65: Detención información nivel de clasificación secreto. Fuente propia.

En la figura 64, se ilustra la detención de la palabra patente, la cual se encuentra en el nivel de clasificación Confidencial. Se visualiza en dicha imagen un mensaje alertando la acción y adicional se aprecia la variación de la gráfica en el momento que se trató de exfiltrar la información en una frecuencia considerada ultrasónica de 20000 Hz.

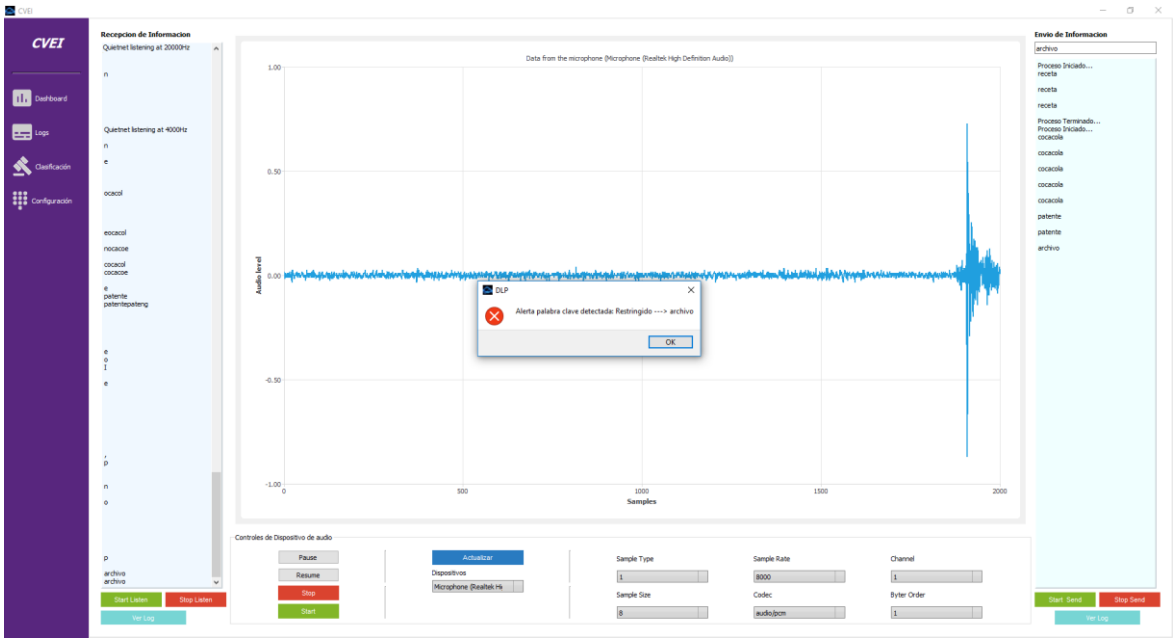
- **Confidencial:** patente

Figura 66: Detención información nivel de clasificación confidencial. Fuente propia.

En la figura 65, se ilustra la detención de la palabra archivo, la cual se encuentra en el nivel de clasificación Restringido. Se visualiza en dicha imagen un mensaje alertando la acción y adicional se aprecia la variación de la gráfica en el momento que se trató de exfiltrar la información en una frecuencia considerada ultrasónica de 20000 Hz.

- **Restringido:** archivo

Figura 67: Detención información nivel de clasificación restringido. Fuente propia.



En la figura 66, se ilustra la detención de la palabra contable, la cual se encuentra en el nivel de clasificación Uso interno. Se visualiza en dicha imagen un mensaje alertando la acción y adicional se aprecia la variación de la gráfica en el momento que se trató de exfiltrar

- **Uso interno:** contable

Figura 68: Detención información nivel de clasificación uso interno. Fuente propia.

En la figura 67, se ilustra la detención de la palabra gráfico, la cual se encuentra en el nivel de clasificación Público. Se visualiza en dicha imagen un mensaje alertando la acción y adicional se aprecia la variación de la gráfica en el momento que se trató de exfiltrar.

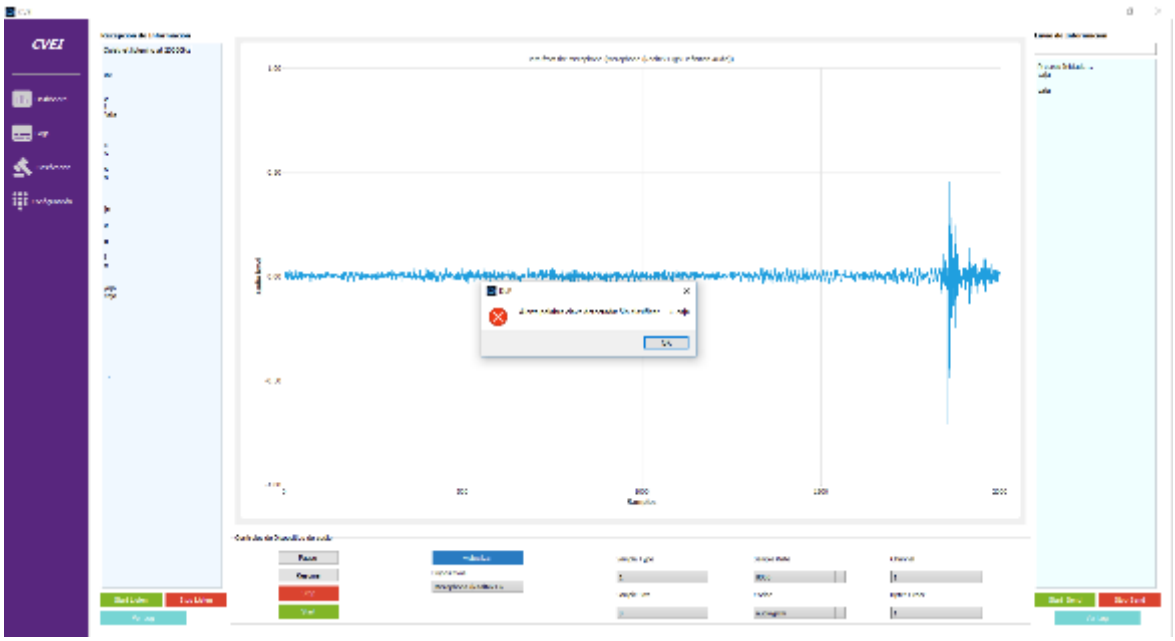
- **Público:** grafico

Figura 69: Detención información nivel de clasificación público. Fuente propia.

En la figura 68, se ilustra la detención de la palabra caja, la cual se encuentra en el nivel de clasificación Sin Clasificar. Se visualiza en dicha imagen un mensaje alertando la acción y adicional se aprecia la variación de la gráfica en el momento que se trató de exfiltrar.

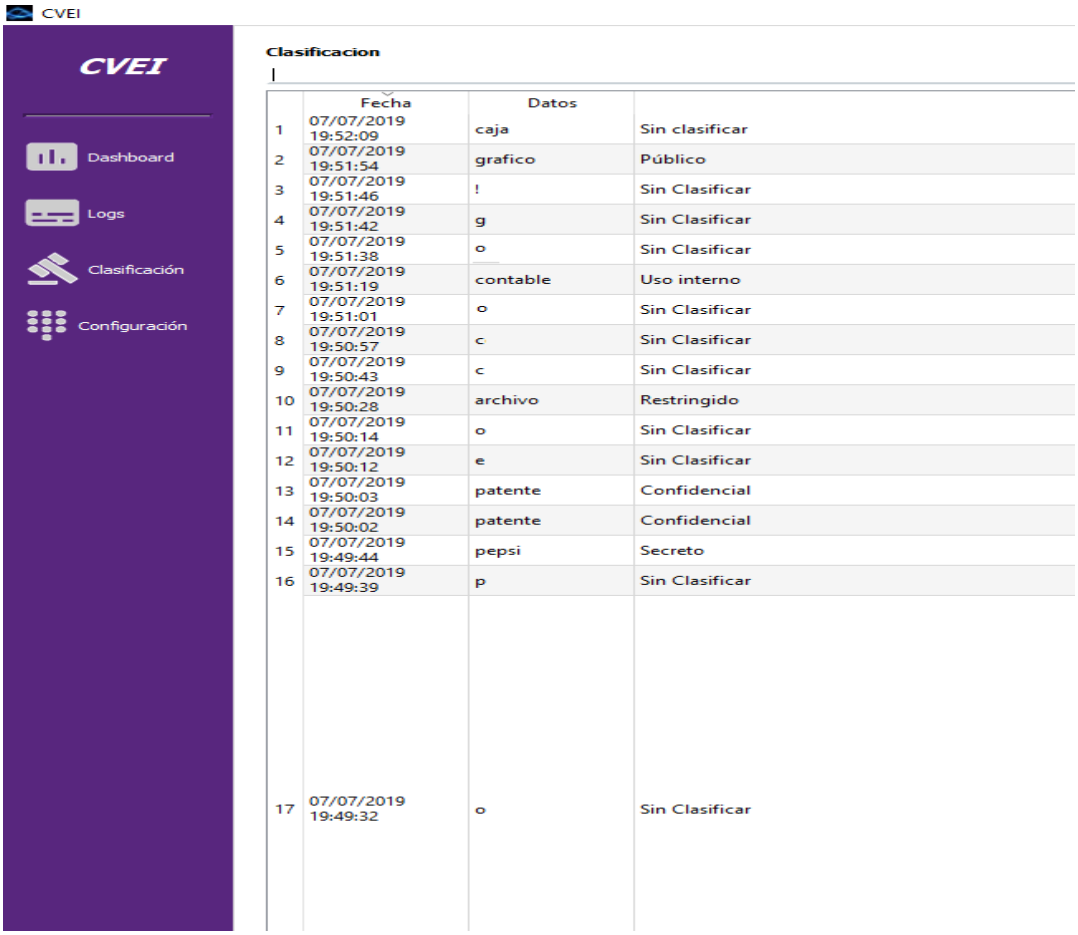
- **Sin clasificar:** caja

Figura 70: Detención información nivel de clasificación sin clasificar. Fuente propia.



De la interacción que se ilustran en figuras 63 hasta la 68, se almacena en el log transaccional, toda la información que se detectó, entregado en el informe datos detallados como la fecha día/mes/año, hora – minutos – segundos, la información que se trataron de exfiltrar y el nivel de clasificación al que pertenece. En la figura 69, se ilustra el orden como fue detectada la exfiltración de información.

Figura 71: Log de detección basado en nivel de clasificación. Fuente Propia.



	Fecha	Datos	
1	07/07/2019 19:52:09	caja	Sin clasificar
2	07/07/2019 19:51:54	grafico	Público
3	07/07/2019 19:51:46	!	Sin Clasificar
4	07/07/2019 19:51:42	g	Sin Clasificar
5	07/07/2019 19:51:38	o	Sin Clasificar
6	07/07/2019 19:51:19	contable	Uso interno
7	07/07/2019 19:51:01	o	Sin Clasificar
8	07/07/2019 19:50:57	c	Sin Clasificar
9	07/07/2019 19:50:43	c	Sin Clasificar
10	07/07/2019 19:50:28	archivo	Restringido
11	07/07/2019 19:50:14	o	Sin Clasificar
12	07/07/2019 19:50:12	e	Sin Clasificar
13	07/07/2019 19:50:03	patente	Confidencial
14	07/07/2019 19:50:02	patente	Confidencial
15	07/07/2019 19:49:44	pepsi	Secreto
16	07/07/2019 19:49:39	p	Sin Clasificar
17	07/07/2019 19:49:32	o	Sin Clasificar

Tabla 19: Resultados detección de información clasificada en ambiente tipo oficina. Fuente Propia.

Nivel de clasificación	**Información detectada**	**Distancia entre equipos**	**Frecuencia**	**Resultado obtenido**
Secreto	pepsi	1 mtrs	20000 Hz	Detección Exitosa
Confidencial	patente	1 mtrs	20000 Hz	Detección Exitosa
Restringido	archivo	1 mtrs	20000 Hz	Detección Exitosa
Uso interno	contable	1 mtrs	20000 Hz	Detección Exitosa
Público	grafico	1 mtrs	20000 Hz	Detección Exitosa
Sin clasificar	caja	1 mtrs	20000 Hz	Detección Exitosa

De los resultados obtenidos en este escenario se puede determinar que, en un ambiente libre de ruido, se puede llevar con éxito el envío y la detención de información en frecuencias ultrasónicas hasta los 20000 Hz, a una distancia de 1 mts entre los equipos participantes, es de anotar que en el ambiente intervenido también se puede hacer uso de frecuencias audibles al ser humano en

cualquiera de sus rangos. Adicional se concluye que la información almacenada en los niveles de clasificación se encuentra seguros mediante el uso del software desarrollado CVEI.

8. Conclusiones y recomendaciones

8.1 Conclusiones

Con el desarrollo tecnológico y el avance a nivel de hardware los componentes periféricos de los equipos informáticos poseen mayores características físicas para generar una mejor calidad en cuanto a audio y recepción de sonido. Esto permite a su vez que los problemas a nivel físico que afectan la transmisión de las ondas ultrasónicas se reduzcan y habilite la posibilidad de que los paquetes de información que son enviados y recibidos, sean más fiables. Es posible entonces desarrollar un sistema que permita el envío de archivos de mayor volumen de información como fotos, videos, bases de datos, música, datos de registros.

Los dispositivos computacionales de vanguardia ofrecen mejor calidad en la emisión y recepción de sonido gracias a la alta competencia en hardware para destacar de otras productoras en tecnología lo que ha llevado a que los antiguos problemas de emisión y recepción en un canal de aire pueda considerarse hoy día no como un problema si no como alternativas de comunicación factible en los dispositivos, por ende para reducir las vulnerabilidades, los sistemas de cómputo como (IDS, Antivirus, SIEM) deberían incluir dentro de sus módulos una opción de monitoreo.

Presentamos un método para la detección de exfiltración de información que, basado en datos transmitidos por ultrasonido, logra identificarla y clasificarla. Esto permite reconocer si un dispositivo es susceptible de fugas de información.

Las pruebas en el ambiente de laboratorio que posee condiciones de no ruido y no generadores de ondas ultrasónicas externas, corroboran que, si un equipo de cómputo posee un disco duro mecánico, dentro de los procesos de arranque del sistema operativo sin manipulación por otro tipo de software, no es posible emitir ondas que puedan ser detectada por nuestro equipo. Podemos conjeturar que esto ocurre porque el componente está físicamente dentro de la carcasa del equipo.

Lo anterior podría generar una interrupción a la señal generada y evita enviar de forma exitosa un paquete de información. No se encontraron más componentes con la capacidad de desarrollar un sonido ultrasónico que fuera detectable, por ende, los componentes principalmente involucrados en este tipo de comunicación resultan ser los altavoces que en las máquinas de pruebas muestran tener la capacidad de generar una frecuencia hasta de 23000 Hz y los micrófonos receptar ondas ultrasónicas en el rango de los 20000 Hz y 22000 Hz.

En una implementación real el clasificador puede identificar más del 90% de las fugas de información al tiempo que aumenta como máximo 1 falsa alarma cada 100 ª vez.

El resultado de las pruebas de clasificación de texto para diferenciar el nivel de seguridad y relevancia de los datos puestos como: Secreto, Confidencial, Restringido, Uso interno, Público, Sin clasificar logró su propósito gracias a la inclusión de una estrategia de, complemento y ajuste, para crear un clasificador que tiene una tasa de descubrimiento de falsos baja, incluso cuando se presentan información no relacionados con los grupos de clasificación. Evaluamos nuestro algoritmo en varios cuerpos que recopilamos a partir de información con variabilidad en el tamaño de caracteres y bajo las diferentes condiciones ambientales (hogar, trabajo y empresa). Nuestro clasificador tuvo una tasa de falsos negativos de menos del 10.0% y una falsa tasa de descubrimiento de menos del 5.0% en todas nuestras pruebas.

El método propuesto cumple con su función de clasificación y prevención de perdida de datos, manteniendo siempre el canal vigilado y con una reducción de falsos positivos logrado a través de la regulación del rango de la producción de la onda y su recepción entre 20 Khz y 23 Khz permite que el dispositivo se encuentre bajo vigilancia permanente y en caso de presentarse algún evento de fuga, también se encuentra en capacidad de alertar e informar según los niveles de clasificación

que información y con qué clasificación se encuentra comprometida en un evento, con una tasa de probabilidad del 90% bajo las pruebas generadas en los dos ambientes (Tipo oficina y cerrado libre de ruido).

La implementación de un sistema de detección de intrusión de audio adaptativo ha sido evaluada con éxito, logro demostrar que la detección automática de acústica en las comunicaciones son factibles comparando las características de las emanaciones en diferentes ambientes: Tipo oficina y cerrado libre de ruido

8.2 Recomendaciones

Acorde a las políticas empresariales, es común encontrar procedimientos de clasificación basados en teorías antiguas, por ende el método tradicional de clasificación puede verse afectado bajo el nuevo panorama que ofrece los aspectos en seguridad informática, se recomienda utilizar un nuevo modelo que se encuentra disponible en donde se habilitan 6 grupos con diferentes propiedades y características donde permite un libre nombramiento respetando las características de agrupación. Para nuestro propósito los nombramos como: Secreto, Confidencial, Restringido, Uso interno, Público, Sin clasificar.

Los dispositivos móviles tipo: smartphone, tabletas, laptops, smartwatch, entre otros también pueden ser objetivos de ataques debido a que al agregar funcionalidades de accesibilidad para la interacción del usuario con el dispositivo en la actualidad se utilizan los comandos de voz para ejecutar acciones remotas en los equipos, a su vez estos dispositivos tienen dentro de sus procesos de segundo plano tienen activos los micrófonos para recibir los comandos en cualquier momento y es posible según una investigación conocida como Dolphinattack utilizar frecuencias en

ultrasonido para ejecutar comandos sin necesidad de que sean que sea el dueño audiblemente reconocido. Por ende, es necesario extender esta protección a los nuevos dispositivos móviles.

A. Anexos:

Bibliografía

[1] E. Santos De La Cruz, N. Cancino Vera, J. Yenque Dedios, D. Ramírez Morales, and M. Palomino Pérez, "El Ultrasonido Y Su Aplicación," *Ind. Data*, vol. 8, no. 1, p. 025, 2014.

[2] A. Balmori, "Posibles efectos de las ondas electromagnéticas utilizadas en la telefonía inalámbrica sobre los seres vivos," *Ardeola*, vol. 51, no. 2, pp. 477–490, 2004.

[3] Romero Luis, "Seguridad Informática Bibliografía Contenidos Definiciones," *Univ. Salamanca.*, vol. 1, pp. 1–36, 1997.

[4] I. S. Castillo, R. J. Caldera, F. Losavio, and A. Matteo, "Caracterización de Sistemas Fiables basada en (Characterization of Dependable Systems based on a standard quality model)."

[5] A. Chavez, "Seguridad Informática," p. 218, 2009.

[6] M. Hanspach and M. Goetz, "Recent Developments in Covert Acoustical Communications.," *Sicherheit*, pp. 243–254, 2014.

[7] I. N. D. T. D. L. C. (Inteco), "Guía gestión de fuga de información," pp. 1–23, 2012.

[8] "Baca Urbina, Gabriel (2016)." .

[9] M. Hanspach and M. Goetz, "On covert acoustical mesh networks in air," *J. Commun.*, vol. 8, no. 11, pp. 758–767, 2013.

[10] "Gooding, D (2013)." .

[11] D. Arp, E. Quiring, C. Wressnegger, and K. Rieck, "Privacy Threats through Ultrasonic Side Channels on Mobile Devices," *Proc. - 2nd IEEE Eur. Symp. Secur. Privacy, EuroS P 2017*, pp. 35–47, 2017.

[12] F. Pacheco, *Fuga de información : ¿ una amenaza pasajera ?*, vol. 54, no. 11. 2011.

[13] J. Medina, “Teoría básica (I): frecuencia y amplitud | Hispasonic,” no. I, 2013.

[14] P. E. Services, “Ultrasonic Data,” *Prod. data*, p. 2, 2016.

[15] A. Giani, V. H. Berk, and G. V. Cybenko, “Data exfiltration and covert channels,” *Sensors, Command. Control. Commun. Intell. Technol. Homel. Secur. Homel. Def. V*, pp. 620103-620103–11, 2006.

[16] A. Sala Cola, “Revista General,” *Rev. Gen. Mar.*, pp. 313–349, 2013.

[17] “Mitre Corp.” .

[18] G. Collard, S. Ducroquet, E. Disson, and G. Talens, “A definition of Information Security Classification in cybersecurity context,” *Proc. - Int. Conf. Res. Challenges Inf. Sci.*, pp. 77–82, 2017.

[19] R. Dandliker *et al.*, “(12) United States Patent,” vol. 1, no. 12, 2011.

[20] Z. Chen, W. Ma, W. Lin, L. Chen, and B. Xu, “Tracking down dynamic feature code changes against python software evolution,” *Proc. - 2016 3rd Int. Conf. Trust. Syst. Their Appl. TSA 2016*, pp. 54–63, 2016.

[21] D. Wax, “MFSK--The Basis for Robust Acoustical Communications,” *Ocean. 81*, pp. 61–66, 1981.

[22] S. Holm, O. B. Hovind, S. Rostad, and R. Holm, “Indoors Data Communications Using Airborne Ultrasound,” *IEEE Int. Conf. Acoust., Speech, Sign. Proc*, pp. 4–7, 2005.

[23] M. LeMay and J. Tan, “Acoustic Surveillance of Physically Unmodified PCs.,” *Secur. Manag.*, pp. 328–334, 2006.

[24] C. Li, D. A. Hutchins, and R. J. Green, “Short-range ultrasonic communications in air using quadrature modulation,” *IEEE Trans. Ultrason. Ferroelectr. Freq. Control*, vol. 56, no. 10, pp. 2060–2072, 2009.

[25] M. Backes, M. Dürmuth, S. Gerling, M. Pinkal, and C. Sporleder, "Acoustic Side-channel Attacks on Printers," *Proc. 19th USENIX Conf. Secur.*, p. 20, 2010.

[26] R. Callan, A. Zajic, and M. Prvulovic, "A Practical Methodology for Measuring the Side-Channel Signal Available to the Attacker for Instruction-Level Events," *Proc. Annu. Int. Symp. Microarchitecture, MICRO*, vol. 2015-Janua, no. January, pp. 242–254, 2015.

[27] L. Evan, L. Yihua, and Z. Wei, "Covert Acoustic Channels Improving Range, Accuracy, and Undetectability," 2014.

[28] M. Guri, Y. Solewicz, A. Daidakulov, and Y. Elovici, "DiskFiltration: Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard Drive Noise," p. 28, 2016.

[29] M. Guri, G. Kedma, A. Kachlon, and Y. Elovici, "Air hopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies," *2014 9th Int. Conf. Malicious Unwanted Softw. Am.*, no. Malcon, pp. 58–67, 2014.

[30] L. Deshotels, "Inaudible Sound as a Covert Channel in Mobile Devices," *Proc. 8th USENIX Work. Offensive Technol. - WOOT '14*, p. 16, 2014.

[31] W. Mazurczyk and L. Caviglione, "Information Hiding as a Challenge for Malware Detection," *IEEE Secur. Priv.*, vol. 13, no. 2, pp. 89–93, 2015.

[32] D. Genkin, A. Shamir, and E. Tromer, "RSA key extraction via low-bandwidth acoustic cryptanalysis," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8616 LNCS, no. PART 1, pp. 444–461, 2014.

[33] G. Erdélyi, "Hide & Seek? Anatomy of Stealth Malware," *Virus Bull. Conf. 2003*, no. c, pp. 1–21, 2004.

[34] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, and W. Xu, "DolphinAtack: Inaudible Voice

Commands," 2017.

[35] I. Comunicación, M. Guri, Y. Solwicz, A. Daidakulov, Y. Elovici, and U. B. Negev, "MOSQUITO : Las transmisiones encubiertas de ultrasonidos entre dos Aire Gapped Los ordenadores que utilizan."