
Revista Logos Ciencia & Tecnología
ISSN: 2145-594X
ISSN: 2422-4200
Policía Nacional de Colombia

Vargas Montoya, Héctor Fernando; Vallejo Pinilla, Clay Schneider; Ruiz Patiño, Carlos Augusto
Fuga de información por ultrasonido: un delito sobre datos personales
Revista Logos Ciencia & Tecnología, vol. 14, núm. 3, 2022, Septiembre-Diciembre, pp. 102-116
Policía Nacional de Colombia

DOI: https://doi.org/10.22335/rlct.v14i3.1618

Disponible en: https://www.redalyc.org/articulo.oa?id=517775534008

Revista Logos Ciencia & Tecnología, 14(3): 102-116 | Septiembre-diciembre, 2022
https://revistalogos.policia.edu.co:8443/index.php/rlct

Estudio de caso

Revista Logos Ciencia & Tecnología
ISSN-L 2145-549X
ISSN 2422-4200 (en línea)

# Fuga de información por ultrasonido: un delito sobre datos personales

## Information leakage by ultrasound: a crime against personal data

## Vazamento de informações de ultrassom: crime contra dados pessoais

Héctor Fernando Vargas Montoya[*a] | Clay Schneider Vallejo Pinilla[b] | Carlos Augusto Ruiz Patiño[C]

[a] https://orcid.org/0000-0002-0861-2883 Instituto Tecnológico Metropolitano – ITM, Medellín, Colombia
[b] https://orcid.org/0000-0002-3244-2167 Instituto Tecnológico Metropolitano – ITM, Medellín, Colombia
[c] https://orcid.org/0000-0002-2421-4906 Instituto Tecnológico Metropolitano – ITM, Medellín, Colombia

- Fecha de recepción: 2022-05-26
- Fecha concepto de evaluación: 2022-09-20
- Fecha de aprobación: 2022-09-23

https://doi.org/10.22335/rlct.v14i3.1618

**Para citar este artículo/To reference this article/Para citar este artigo:** Vargas Montoya, H. F., Vallejo Pinilla, C. S., y Ruiz Patiño, C. A. (2022). Fuga de información por ultrasonido: un delito sobre datos personales. *Revista Logos Ciencia & Tecnología, 14*(3), 102-116. https://doi.org/10.22335/rlct.v14i3.1618

## RESUMEN

La utilización de mecanismos como la transmisión de datos por ondas ultrasónicas, puede permitir que malintencionados logren obtener datos personales de un sistema de cómputo, lo que podría constituir un delito informático. El objetivo de este artículo es demostrar cómo es posible filtrar información a través del ultrasonido, haciendo uso de los sistemas periféricos de estaciones de trabajo, con lo cual se podrían obtener datos personales generando un problema de confidencialidad y un posible delito. Para ello, el método utilizado fue realizar una caracterización de componentes informáticos, construir un software de apoyo para el envío y recepción de datos por ultrasonido (en una frecuencia por encima de los 18000 Hz), haciendo uso de los altavoces de un equipo computacional y la recepción datos fue desde otro equipo portátil, las pruebas fueron realizadas en un ambiente controlado con bajo ruido. Como resultado, se pudo transferir información a través de elementos computacionales básicos, aunque con alguna pérdida de paquetes, pero funcional para el cumplimiento del objetivo propuesto. Con lo cual, se concluye que es posible, a través de ultrasonido, filtrar datos y que alguna de esta información puede generar un delito informático a la luz de la Ley 1273 de 2009 en Colombia.

**Palabras clave**: crimen informático, derecho a la privacidad, medida de seguridad, protección de datos, sistema informático, ultrasonido.

## ABSTRACT

The use of mechanisms such as the transmission of data by ultrasonic waves can allow malicious personnel to obtain personal data from a computer system, which could constitute a computer crime. The objective of this article is to demonstrate how it is possible to filter information through ultrasound, using workstation peripheral systems, with which personal data could be obtained, which generates a confidentiality problem. For this, the method used was to perform a characterization of the computer components, a support software was built for sending and receiving ultrasound data (at a frequency greater than 18000 Hz), using the speakers of a computer equipment and the reception of data was from another laptop, the tests were performed in a controlled environment with low noise level. As a result, it was possible to transfer information through basic computational elements, although with some packet loss,





* Autor de correspondencia. Correo electrónico: hectorvargas@itm.edu.co

but functional for the fulfillment of the proposed objective, with which it is concluded that it is possible that part of this leaked information could generate a computer crime through the light of Law 1273 in Colombia.

**Keywords**: computer crime, computer system, data protection, right to privacy, security measure, ultrasound.



**RESUMO**

A utilização de mecanismos como a transmissão de dados por ondas ultrassônicas pode permitir que indivíduos mal-intencionados obtenham dados pessoais de um sistema informático, o que pode constituir um crime informático. O objetivo deste artigo é demonstrar como é possível filtrar informações por meio de ultrassom, utilizando sistemas periféricos de estações de trabalho, com os quais podem ser obtidos dados pessoais, o que cria um problema de confidencialidade. Para isso, foi realizada uma caracterização dos componentes do computador, foi construído um software de suporte para enviar e receber dados de ultrassom (na frequência superior a 18000 Hz), utilizando os alto-falantes de um equipamento computacional e foi realizada a recepção. Dados de outro laptop, os testes foram realizados em um ambiente controlado de baixo ruído. Consequentemente, a informação pode ser transferida através de elementos computacionais básicos, embora com alguma perda de pacotes, mas funcional para o cumprimento do objetivo proposto, com o qual é possível que parte desta informação filtrada possa gerar um crime informático de acordo com a Lei 1273 na Colômbia.

**Palavras-chave**: crime informático, direito à privacidade, medida de segurança, proteção de dados, sistema informático, ultrassom.

## Introducción

En consideración de la 4.ª revolución industrial y la potencialización de la tecnología para desarrollar y fortalecer los procesos empresariales, la seguridad de la información toma cada vez más fuerza y preocupación por los múltiples ciberataques que se presentan, y, en ese sentido, las personas y organizaciones vienen prestando más atención a la protección de los datos empresariales y personales.

Los avances tecnológicos en campos 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.

Las ondas acústicas poseen propiedades como la transmisión, absorción, reflexión, refracción, difracción o dispersión, y difusión que se ven afectadas por fenómenos físicos. Así, la propagación de la onda es menor en comparación con la afectación que se produce en la transmisión de las ondas electromagnéticas (Álvarez, 2018). Asimismo, dichas ondas acústicas, a diferencia de las electromagnéticas, son mecánicas, elásticas y requieren un medio para transportarse; además, son ondas longitudinales, no pueden ser polarizadas y su velocidad de propagación tiene una dependencia de las características del medio en el que se transmite, tales como la presión, temperatura, densidad y humedad (Chen *et al*., 2019).

Por otro lado, las comunicaciones inalámbricas (ondas electromagnéticas) como el estándar 802.11-WI-FI, *Near Field Communication*-NFC, *Bluetooth*, Infrarrojos, Redes 2g, 3g, 4g, 5g, entre otros (Waldmann-Selsama *et al.*, 2016), hacen posible la comunicación actual, aunque con algunas discusiones con respecto al daño ambiental que se puede generar, dada su operación en diferentes rangos de frecuencia; sin embargo, permite mayor cobertura y tasa de transmisión entre equipos computacionales.

Asimismo, una exfiltración de datos 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 o personas no autorizadas (Carpentier *et al.*, 2019). No obstante, dicha pérdida de confidencialidad debe estar asociada a un mecanismo de clasificación de información, que le indique a una organización o persona, qué tan crítica es la información que se pudo filtrar.

Este artículo presenta varios elementos que pueden desarrollarse de manera simple sin mucha tecnología, como prueba de una posible exfiltración de datos de un sistema informático mediante ultrasonido, haciendo uso de los elementos propios de cada equipo computacional, sin inversiones adicionales, y teniendo como objetivo lograr transportar datos desde un equipo a otro, considerando igualmente que esto puede constituir un delito informático en términos de la ley colombiana. Por consiguiente, se genera la pregunta ¿cómo se puede extraer datos que pueden ser sensibles por medios no convencionales, demostrando un posible delito informático?

## El ultrasonido y la pérdida de confidencialidad

El ultrasonido es una onda mecánica que está por encima de los 19500 Hz (20 Khz), dicha frecuencia es imperceptible para el odio humano, ya que éste es capaz de reconocer frecuencias acústicas por debajo de los 20 Khz (Ortega Seguel, 2004).

Los equipos de cómputo actuales (portátiles o equipos PC de escritorio), por su velocidad de funcionamiento (velocidad del disco duro y ventiladores, p. ej.), tienen la capacidad de generar este tipo de ondas en alta frecuencia (sin una intervención humana); sin embargo, los periféricos como parlantes y micrófonos, son elementos capaces de emitir y recepcionar ultrasonido, respectivamente, con la ayuda de algún software capaz de hacer mover las membranas físicas de que están compuestos (AlKilani *et al.*, 2019).

Poder enviar información por una red acústica como una tecnología de comunicación, sugiere un reto interesante a validar, ya que se puede usar como un canal encubierto para transportar datos, lo que permite una violación clara a la confidencialidad de la información si esto se logra, dado que no se tienen un control de acceso o mecanismos de autorización para ello.

En ese sentido, el ultrasonido se convierte en un canal de comunicación, permitiendo a través de un periférico enviar y recibir señales en altas frecuencias, y como resultado, el dispositivo origen se ve vulnerado al enviar datos no consentidos por medios no tradicionales, ejemplo de esto, es la forma como se ejecuta el ataque informático denominado *Dolphin Attack* o "comandos de voz inaudible" (Michael y Michael, 2014); A pesar de ello, como lo indica Leyden (2013), el hecho de no contar con documentación del ataque *DolphinAttack* que hace una explotación de la vulnerabilidad de manera recurrente, no significa que no se ejecuten ataques de tipo *malware* generando diferentes impactos en los equipos y que estos puedan ser transmitidos por diferentes medios.

## Periféricos en equipos de cómputo

Los equipos informáticos y de procesamiento podrían presentar exfiltración de datos a través de variados mecanismos, tal es el caso de pérdidas de datos e información a través de programas maliciosos, ya que estos una vez se implantan en los equipos, pueden ejecutar múltiples tareas maliciosas (caso de *spyware* y los *keylogger*), dichos ataques pueden amplificarse en consideración del uso de protocolos sin cifrar que circulan en Internet, que pueden ser fácilmente interceptados por atacantes (Pérez, 2013).

Por otro lado, los computadores presentan una exposición a posible pérdida de información (haciendo uso de ultrasonido) no solo por los elementos más visibles como los altavoces y los micrófonos, sino también a dispositivos como los ventiladores y discos duros, los cuales podrían generar frecuencias ultrasónicas, permitiendo así la exfiltración de la información (Solairaj *et al.*, 2016).

## Ataques informáticos

Las redes de computadores, las de telecomunicaciones y los sistemas de cómputo en general, vienen con una serie de vulnerabilidades que permiten a los atacantes obtener acceso o información de diferentes plataformas. Para el caso de los sistemas de cómputo, el *malware* ha crecido de manera importante en los últimos años, siendo el tipo *Ransomware* los de más impacto, dado que estos tienen la capacidad de ingresar a las redes y cifrar la información que encuentre (secuestro), con ello, los atacantes solicitan un rescate para su descifrado y entrega de información (Osorio *et al*., 2020).

Asimismo, de acuerdo con Roldán y Vargas (2020), los accesos a redes inalámbricas y en particular las redes de telecomunicaciones (como 3G y 4G), se puede sufrir diferentes ataques informáticos, desde interceptación de datos (ataque de hombre en el medio, o MiTM por sus siglas en inglés), *malware*, hasta negación de servicio por consumo exhaustivo de recursos, por ello la gestión de riesgos es fundamental a la hora de establecer las posibles amenazas y vulnerabilidades que éste tipo de redes puede contener y, con ello, proyectar posibles soluciones.

Por otro lado, los ataques informáticos se pueden presentar en diferentes tecnologías, como los sistemas industriales (SCADA, por sus siglas en inglés) capaces de controlar la producción, interactuando con dispositivos externos analógicos y con internos (redes de computadores), dichos ataques tienen la capacidad de generar indisponibilidad en la producción o un proceso como tal, con ataques como la inyección de código o modificación de datos (Quiroz Tascón *et al*., 2020).

En ese sentido, los ataques informáticos están presentes en cualquier plataforma y se ejecutan en la medida que las vulnerabilidades en los sistemas no se puedan cubrir adecuadamente, por lo cual, los atacantes vienen haciendo uso de canales, sistemas o plataformas tecnológicas no tradicionales para extraer información, modificarla o eliminarla según sea el caso, de ahí que los canales encubiertos (como el ultrasonido), puede verse como un sistema que permite obtener información sin que el usuario final o dueño de la información se percate de ello.

### Delito informático

Cada vez los ataques informáticos son más sofisticados, frecuentes y precisos, además, van ampliando su rango de acción con el uso mismo de la tecnología. Cuando se habla de delito informático, se establece esa línea delictiva que, haciendo uso de los dispositivos electrónicos e informáticos en general, tienen como fin vulnerar, robar o extraer, modificar o acceder a datos e información digital que, de alguna manera, está protegida (Peritos Informáticos [PI], 2021).

De igual forma, en Colombia, acorde al *World Legal Comporation* (junio, 2021), se define el delito informático como aquellos "accesos de manera ilícita o no autorizada a los datos e información que están resguardados en formatos digitales, estos actos están tipificados en la Ley 1273 del 2009", para lo cual, la mencionada ley estipula dentro sus artículos diferentes sanciones acordes a la categorización de lo que puede ser un delito.

En consecuencia, se tienen los siguientes articulados a considerar en este trabajo:

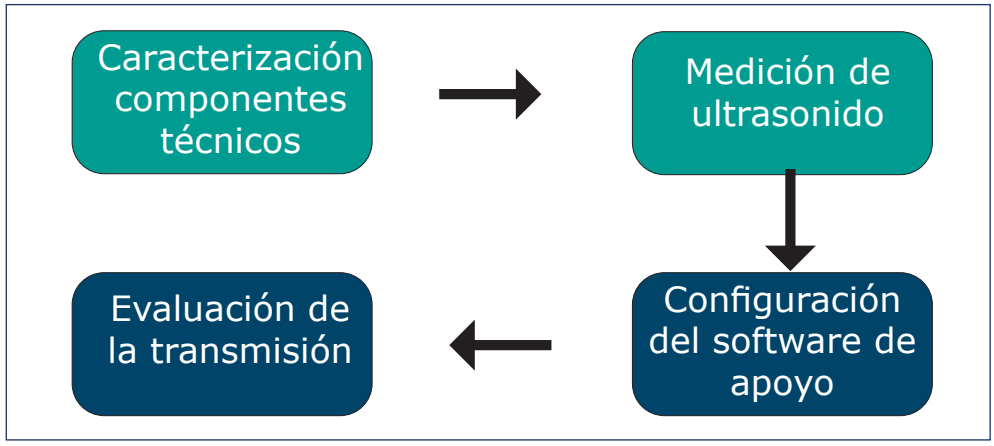
> Art. 269C: Interceptación de datos informáticos: El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.
>
> Art. 269F: Violación de datos personales: El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes (Congreso de la República, 2009).

## Método

Obtener resultados de envío y recepción de datos por ultrasonido haciendo uso de periféricos y logrando una clasificación base, supone establecer una serie de pasos que permitan la configuración de herramientas técnicas y funcionales, con las que se pueda llegar a un resultado óptimo, para lo cual se consideraron las siguientes fases (Figura 1) en la ejecución de las pruebas:

**Figura 1**

*Fases de la metodología para llevar a cabo las pruebas por ultrasonido*




*Nota.* Es una metodología básica de 4 fases que permitió obtener diferentes resultados.

A continuación, se hace una descripción de cada uno de los pasos desarrollados.

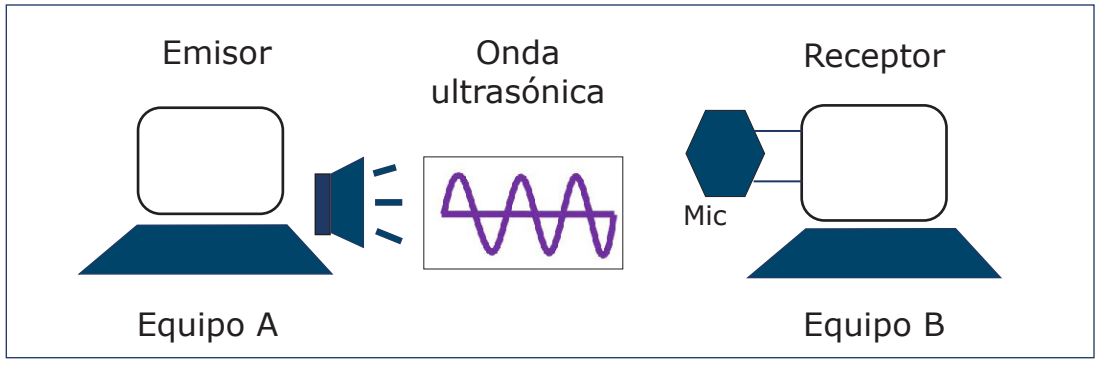
## Caracterización de componentes técnicos

Diferentes componentes técnicos pueden estar asociados a la transmisión y recepción de ondas ultrasónicas, como lo son los altavoces y micrófonos que vienen incorporados en los equipos portátiles o de mesa, con lo cual, cualquier persona tiene elementos necesarios para iniciar una transmisión.

Para la caracterización y posteriores pruebas de envío de datos, se consideraron equipos y periféricos con las siguientes condiciones técnicas y arquitectura (Figura 2). En dicha figura se representa el flujo de datos ante la transferencia y considera los elementos básicos ya instalados en los computadores (parlante y micrófono), el Equipo-A sirve de emisor (a través del parlante) y el B de receptor (a través del micrófono):

**Figura 2**

*Esquema para la transmisión y recepción de datos por ultrasonido*




*Nota.* El equipo A envía datos que son recibidos por el equipo B, haciendo uso de los elementos básicos de cualquier equipo.

Dado lo anterior, se contó con la siguiente configuración técnica en los dos equipos, el equipo A tiene un sistema operativo Windows 10 Pro (64 Bit), un procesador Intel(R) Core (TM) i7-6700HQ CPU CP 2.49Ghz 2.60 GHz, memoria RAM: 8,00 Gb y parlantes modelos Genelec 6010B.

El equipo B contó con un sistema Operativo Windows 10 Pro (64 bit), Procesador Intel(R) Core(TM) i7-5500U CPU CP 2.40Ghz 2.49 GHz, Memoria RAM de 12,00 Gb y micrófonos externos tlm103 neumann, Re20 Electrovoce, shure sm57, XYH-6 Stereo Mic, MSH-6 Stereo Mic.

## Medición de ultrasonido

Para evitar algunas interferencias o ruidos que pudiesen alterar las mediciones, se realizó el montaje de la arquitectura en un sitio con baja emisión de ruido, ubicado en uno de los centros de investigación y desarrollo del Instituto Tecnológico Metropolitano [ITM], en Medellín, bloque Parque-I, en el laboratorio de artes digitales (Figura 3). Dicha sala presta diferentes servicios como la grabación de videos, producción, diseño y ajustes de sonido, entre otros, dado que cuenta con adecuaciones acústicas aisladas y elementos de medición en temas de sonido.

**Figura 3**

*Disposición y distancia de los equipos de pruebas, ubicados en el laboratorio de artes digitales, parque-I del ITM*

*Nota*. Este laboratorio y el recinto como tal, es libre de ruido para mejorar los resultados.

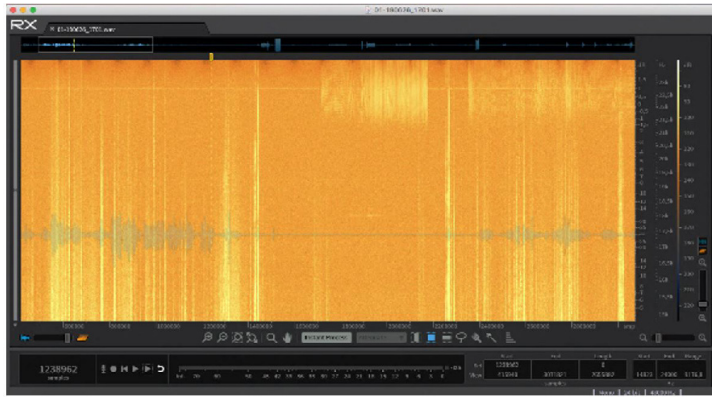
El sitio físico en donde se realizaron las pruebas, permitió la grabación de diferentes elementos asociados al sonido, entre ellos, el ultrasonido, dando la posibilidad de reducción de niveles de error a causa de interferencias, esto, considerando que la sala tiene una adecuación en paredes, pisos y techos que evita la reflexión y hace una adsorción de ruido.

Haciendo uso del laboratorio de artes digitales del ITM, la medición de algunas fuentes ultrasónicas fue realizada usando micrófonos externos del equipo receptor, los cuales se conectaron en los equipos de cómputo tipo *laptop*; con el uso de micrófonos externos, se comprobó que, a través de la integración de estos dispositivos, era posible obtener una captura de frecuencia al nivel deseado, de esta manera se integra al conjunto de dispositivos usados para la prueba respectiva.

Para el apoyo en la detección y el procesamiento de la señal, se usó el software iZotope RX 5 (figura 4), el cual tiene la capacidad de editar audio, mejorando la calidad, haciendo uso de características avanzadas para la reparación y pos-producción (iZotope, 2021).

**Figura 4**

*Frecuencia de onda ultrasónica detectada por el software de Medición iZotope Rx*



*Nota*. El software *iZotope* tiene la posibilidad de capturar diferentes frecuencias, entre ellas el ultrasonido.

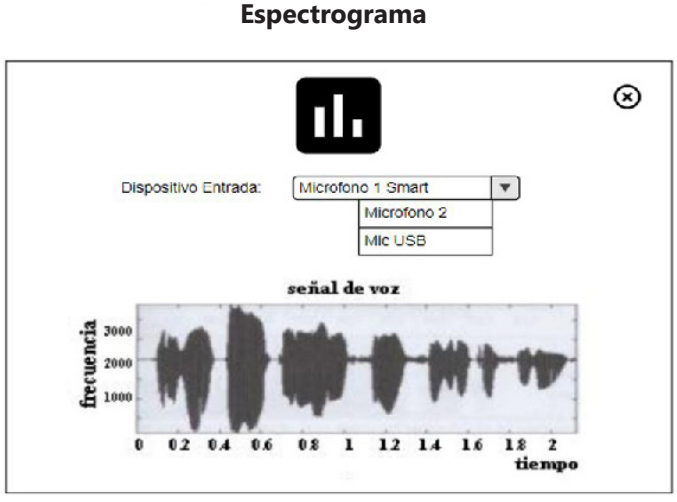
En ese sentido, la figura 4 muestra la detección de ultrasonido en las primeras pruebas, en la cual se observa el espectro de ondas y en el fondo (azul) la onda ultrasónica, dando la posibilidad de extraer de ella la respectiva portadora.

## Software de apoyo

Con el objetivo de tener mejores características y resultados a la hora de transmitir y recepcionar diferentes datos, se desarrolló una aplicación (Figura 5) que integra varias funcionalidades. Esta muestra la variación de los datos en una gráfica en el momento que se genera una onda ultrasónica en el equipo de cómputo, asimismo se configura un sistema básico para la clasificación de los datos e información que son capturados. El software contó con la integración de diferentes herramientas de uso libre y fue configurado en los dos equipos de las pruebas, activando la funcionalidad respectiva (emisión o recepción).

**Figura 5**

*Software propietario creado para la generación y recepción de ondas ultrasónicas*




*Nota.* El software permite una forma más simple de entender la recepción de tráfico, mostrando la onda en términos de frecuencia y tiempo.

El software fue usado para validaciones unitarias sobre la información enviada y recuperada en el destino. Asimismo, se desarrolló una aplicación que integra algunas funcionalidades de otros softwares bajo GNU, con el fin de poder enviar tramas de datos por ultrasonido (emisión) y captura de las mismas (recepción), como lo es GNU Radio, que es una aplicación utilizada como herramienta de desarrollo libre y abierta que provee bloques de procesamiento de señal para implementación de sistemas de radio definida por software. Puede utilizarse con hardware de bajo costo para crear radios definidas por software, o sin hardware en un ambiente de simulación (GNU Radio Project, 2022). Otro software de apoyo es *Quietnet – master*, el cual es un programa *open source* con funcionalidad de comunicación entre dispositivos a través de frecuencia ultrasónica tipo *chat* (Murphy, 2017). Y finalmente, se usó Qt5 que es un *framework* desarrollado y soportado por QT Group (2022) de licencia *open source*, que usa la gráfica y función sinusoidal para representar las señales acústicas cuando se estable las comunicaciones.

De igual manera, la nueva aplicación contó con la integración de librerías como *NumPy*, *Open Source*, la cual es usada como paquete de transformación de matrices multidimensionales de registros arbitrarios, y desarrollado y soportado por la empresa *NumPy Project* (2020) y *PyAudio*, *Open Source*, usado como biblioteca de flujo de entrada / salida de audio multiplataforma (PyAudio Project, 2020).

### Evaluación de la transmisión

Para la evaluación de la transmisión, se ejecutó una serie de pruebas de envío y recepción de datos, evaluando la efectividad y usabilidad del software, con lo cual, se ejecutó una prueba que simula el robo de información desde una máquina de cómputo a otra, usando un método que modula y de-modula la información que es transmitida por ondas ultrasónicas, tabulando la siguiente información: información transmitida, información capturada, frecuencia, distancia y resultado. Asimismo, se hace una evaluación de la información y cómo esta puede constituirse un delito informático en términos de la ley.

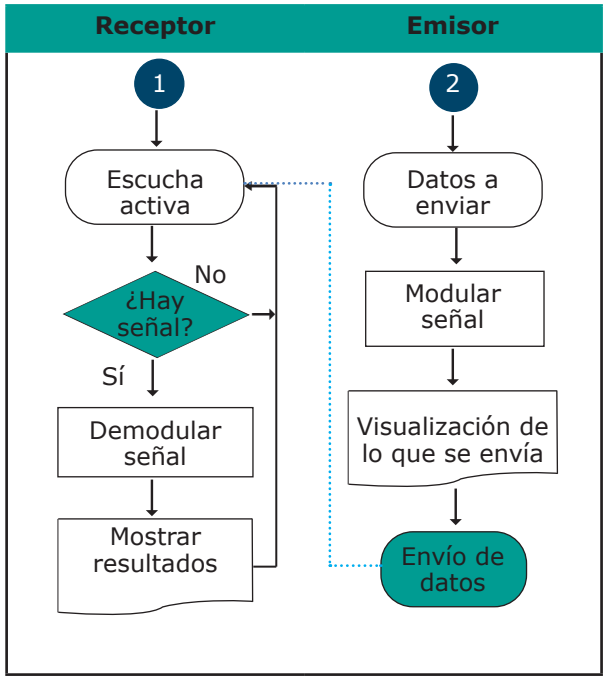
## Resultados

### Uso de equipos de cómputo

Para la implementación del proceso de transmisión, se definió un flujograma básico de funcionamiento (Figura 6). Lo primero realizado fue fijar el equipo receptor en modo escucha permanente y a una distancia de 1 metro (Figura 3), con ello, a través del micrófono conectado, se realiza la captura de las diferentes ondas ultrasónica emitidas; luego, desde el equipo emisor y con la ayuda del software construido, se envían datos usando el ultrasonido como onda envolvente, lo que genera una modulación ultrasónica que es enviada a través del parlante (Figura 2).

**Figura 6**

*Flujo de implementación de la prueba de concepto para transmisión y recepción de datos*




*Nota.* El flujo representa la forma como se enviaron los datos y los mismos fueron recibidos por el receptor, el cual, siempre está a la escucha de nuevos datos.

Una vez el equipo receptor hace la captura de las ondas, las de-modula y muestra los datos que logró capturar, y le da una clasificación básica de acuerdo con un registro previo de posibles palabras o frases, dicha clasificación puede ser secreta, confidencial, restringida, uso interno, público y sin clasificar, esta última se usa cuando un dato no encaja en las clasificaciones anteriores.

### Configuración del software desarrollado

Se configuraron las siguientes variables de entorno de la aplicación para la prueba ultrasónica:

(rate = 44100)(freq = 19500#)(channels = 1)(frame_length = 3)(chunk = 256)(datasize = chunk * frame_length).

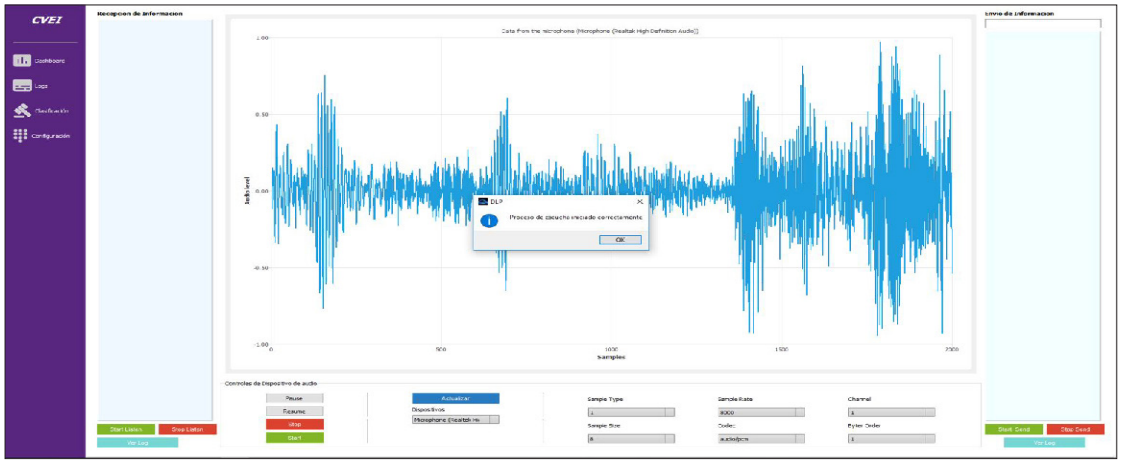
En donde la variable *rate* se refiere al número de muestras recolectadas por segundo, la variable *freq* corresponde al número de vibraciones por segundo que da origen al sonido analógico, *channels* define si la transmisión se realiza por un solo canal como lo es en este caso, ya que en las pruebas se captura con un solo micrófono, *frame length* es la información de amplitud (volumen) en ese momento en particular para producir sonido, *chunk* es el número de fotogramas en el búfer, y el *datasize* es una variable calculada del tamaño del dato entre el número de fotogramas asignadas por el volumen.

## Pruebas funcionales de transmisión

Con un diccionario de palabras de prueba, se realizó la respectiva transmisión y recepción de datos, ejecutando una comparación de lo que se muestra al envío y lo que se logra capturar. Para lo cual, se realizaron múltiples pruebas con diferentes ajustes a la parametrización de las propiedades de los dispositivos para garantizar un envío de paquetes exitoso, y, en ese sentido, se dejó con la configuración que en las pruebas otorgó la mejor tasa de transferencia, con ello, se pudo recolectar en el receptor (Figura 7 y 8) las diferentes ondas generadas desde el emisor.

**Figura 7**

*Software propietario construido para el envío y recepción de datos por ultrasonido*




*Nota*. La imagen muestra las diferentes ondas ultrasónicas enviadas desde el emisor con palabras en ellas.

**Figura 8**

*Software propietario, captura de una palabra transmitida*

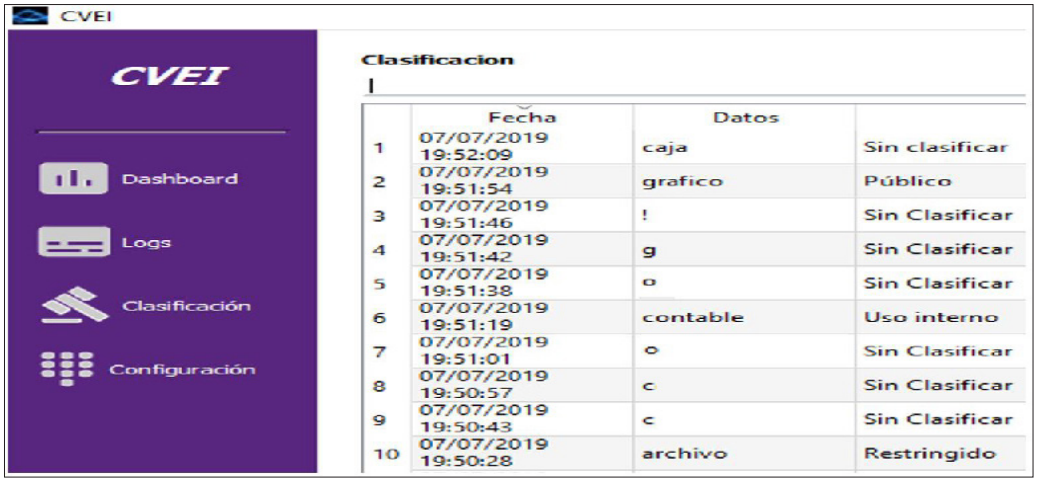

*Nota*. La captura de la onda da como resultado una posible palabra filtrada.

Se puede observar solo una fracción de una onda ultrasónica, lo que corresponde a una parte de las palabras enviadas desde el emisor. En consecuencia, las pruebas establecieron un porcentaje de pérdida en la transmisión.

Finalmente (Figura 9), se puede observar en los registros de log de la recepción, un informe de los datos detallados que lograron exfiltrarse, dándole una clasificación básica dependiendo de la palabra o frase recuperada.

**Figura 9**

*Log generado a partir de los datos por ultrasonido*




| | 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 |

*Nota*. Se tienen 4 campos básicos que se muestran para mejor comprensión.

La figura 9 establece una pequeña muestra de los datos recolectados, asimismo y de acuerdo con una categorización básica, se le dio una etiqueta de posible clasificación dependiendo de la naturaleza del dato, para lo cual, dicha clasificación puede variar dependiendo de las condiciones de cada organización.

Como se puede apreciar, de los datos transmitidos, la mayoría están en la categoría "sin clasificar", esto es debido a que fueron ingresadas pocas palabras a la lista de clasificación y solo para esta prueba de concepto.

Los resultados obtenidos (Tabla 1) muestran cómo la información transmitida por ultrasonido es capturada, asimismo el registro de la frecuencia, la distancia y el resultado final, para lo cual, se establece una prueba exitosa de paso de datos por ultrasonidos, considerando siempre la misma distancia (1 m) y enviando desde frases cortas hasta unas más extensas, con ello, se puede apreciar que cuando la frase es más larga, la pérdida de datos es mayor, también hubo una variación con respecto a la frecuencia, cuando la frecuenta está casi en el límite del ultrasonido, tiene mejores resultados.

**Tabla 1**

*Resumen de los datos transmitidos y recibidos en la prueba de concepto*

| Información transmitida | Información capturada | Frecuencia | Distancia | Resultado |
|---|---|---|---|---|
| Hola me llamo Carlos Augusto Ruiz Patiño | Llamo Carlos ugusto z paña | 20500 Hz | 1 m | Pérdida de datos |
| Hola me llamo Clay Vallejo estudio en el ITM | No capturada | 20500 Hz | 1 m | No captura |
| Hola comunidad ITM | Ola comunidad ITM | 19500 Hz | 1 m | Pérdida de la letra H |
| Buenos días | Buenos días | 19500 Hz | 1 m | Transmisión exitosa |
| Hola | Ola | 19500 Hz | 1 m | Pérdida de la letra H |

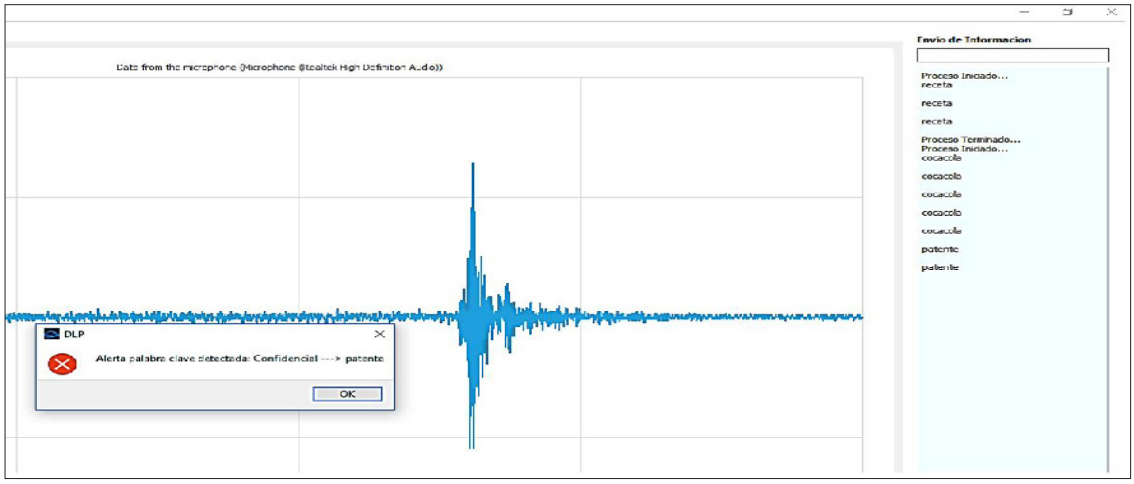
*Nota*. La mayoría de las palabras transmitidas fueron capturadas con un nivel bajo de error, permitiendo comprobar una posible fuga de información.

Los datos e información ejecutados en la tabla 1, hacen parte de palabras de común uso, esto, con el fin de validar qué tan efectiva es la transmisión-recepción de las mismas.

Ahora bien, para completar la simulación de datos e información que puede tener un alto nivel de importancia, se realizó una prueba haciendo un envío sistemático de palabras ya clasificadas (Figura 10 y Tabla 2) y realizando la respectiva medida desde el equipo de recepción.

**Figura 10**

*Recepción de la palabra "patente", clasificada como Confidencial*




*Nota*. La palabra "patente" fue transmitida y recibida en el equipo B, generando una clara violación a información de carácter confidencial de acuerdo a su clasificación.

**Tabla 2**

*Resultados en envío de datos que han sido previamente clasificados*

| Nivel de clasificación | Información detectada | Distancia entre equipos | Frecuencia | Resultado obtenido |
|---|---|---|---|---|
| **Secreto** | Pepsi | 1 m | 20000 Hz | Detección Exitosa |
| **Confidencial** | Patente | 1 m | 20000 Hz | Detección Exitosa |
| **Restringido** | Archivo | 1 m | 20000 Hz | Detección Exitosa |
| **Uso interno** | Contable | 1 m | 20000 Hz | Detección Exitosa |
| **Público** | Gráfico | 1 m | 20000 Hz | Detección Exitosa |
| **Sin clasificar** | Caja | 1 m | 20000 Hz | Detección Exitosa |

*Nota*. Diferentes palabras se enviaron, con un resultado del 100 % recepcionado.



Se puede apreciar, entonces, que si un sistema tiene una serie de información que fue clasificada por nivel de impacto (como números de tarjetas de crédito, saldos, fechas, etc.), esta puede ser filtrada de una manera simple, con lo cual, los datos e información perderían su propiedad de confidencial.

No obstante, si bien las pruebas se enfocaron en la posible pérdida de confidencialidad y

con ello validar acorde a la Ley 1273 de 2009 el posible delito en que se incurre, el hecho de poder tomar información y transmitirla por un medio encubierto, sugiere la posibilidad de modificarla antes de enviarla, dado que se tiene el control de la transmisión, por lo cual, el principio de integridad se vería igualmente afectado. Asimismo, las vibraciones que puedan generarse desde el ultrasonido hacia los discos duros (frecuencia de resonancia), podría colocar en riesgos la disponibilidad no solo de la información, sino del sistema como tal.

## Discusión

Teniendo en cuenta la probabilidad de poder transmitir datos por ultrasonido y tener la posibilidad de clasificarlos, la exfiltración de palabras, frases o archivos claves a una velocidad relativamente baja es un hecho; sin embargo, en consideración de las pérdidas potenciales, se puede dejar como un modo persistente, de manera que el software envíe datos de forma indefinida, con lo cual, del lado de la recepción se podría apreciar en el tiempo, posibles palabras o frases transmitidas de bajo tamaño.

Si se consideran los resultados de fallas y errores, así como el porcentaje de palabras que se transmitieron cortadas y las que transmitieron completas, se puede apreciar que este mecanismo, si bien no logró sostener la totalidad de las transmisiones, sí se puede seguir experimentando y afinando la recepción, de modo que la posibilidad de modular y de-modular exitosamente sea más alta.

Para las pruebas desarrolladas, las frases cortas fueron más exitosas que las largas, lo que podría sugerir eventualmente que, si se tiene una persistencia en el envío, podría ser más exitoso; por otro lado, se podría configurar la plataforma de envío para que no genere palabras completas (dejando un tiempo prudente entre palabras), así, cada letra se podría exfiltrar de manera independiente.

En consecuencia y revisando el problema de confidencialidad y fuga de información que se puede presentar a la luz de la ley del delito informático, se puede apreciar que, al hacer uso del ultrasonido para extraer información, se podría estar enviando datos por fuera del sistema sin el permiso requerido, lo que eventualmente constituye un delito informático en términos de la Ley 1273 de 2009 y, en particular, el art. 269C.

Asimismo, si los datos que se extraen están considerados como datos personales, tales como números de identificación, Nro. de tarjetas de crédito, teléfonos, entre otros, se estaría en frente del art. 269F "violación de datos personales", y como se pudo observar, la extracción de palabras cortas fue exitosa, lo que supone una facilidad de lograr obtener datos personales sin muchos recursos informáticos, en consecuencia, se estaría por fuera de la ley.

Por otro lado, y considerando las posibles afectaciones a la integridad de los datos y a la disponibilidad, se estaría frente a los art. 269B "Obstaculización ilegítima de sistema informático o red de telecomunicación" y 269D "daño informático", considerando la posible pérdida de integridad y daños que se puedan ocasionar por el uso mismo del ultrasonido.

En comparación con otros trabajos desarrollados, algunos se enfocaron en la exfiltración de datos haciendo uso de la captura de video, mediante motores de reconocimiento óptico de caracteres, reconstruyendo las tramas de los videos y extrayendo datos que pueden ser sensibles, lo que proporciona otro mecanismo de violación de la confidencialidad y privacidad de la información (Spiros y Braghin, 2019). En ese sentido, la exfiltración por ultrasonido se convierte en otro mecanismo no convencional para vulnerar la información.

Por otro lado, Liu *et ál*. (2019) hacen un sistema similar pero solo con altavoces, adecuando uno de ellos como el emisor y el otro como el receptor, ambos en una mismo sala o espacio físico; para el parlante receptor debieron realizar una adecuación adicional, que consiste en hacerlo reversible (por la funcionalidad propia de los altavoces), lo que implica cambiar de salida a entrega, pero dicha funcionalidad puede ser ajustada si un atacante logra ingresar un *malware* que lo pueda realizar; sin embargo, no se realiza un proceso de clasificación al final, por lo cual, no es claro que la información se pueda extraer y si tiene o no un nivel crítico.

Similarmente, se podría pensar en establecer un mecanismo contrario, en vez de sacar información de un equipo de cómputo, inyectar datos e información hacia los sistemas haciendo uso de ultrasonido, pudiendo pasar datos, y en ese sentido, se podría dejar un *malware* pequeño o de potencial daño como el 42.zip ejecutado por Stepen (2020) y Pérez (2020), un *malware* potencialmente peligroso que tiene un tamaño de solo 42 KB y que cuando se descomprime (proceso en cascada), puede llegar a 4.5 PB (PetaByte), con lo cual, se estaría frente a la violación del art. 269E "*Uso de software malicioso*", de la Ley 1273 de 2009.

Ahora bien, el hecho potencial que se pueda generar una negación de servicio en discos o sistemas, supone un problema mayor en términos de disponibilidad, y esto puede ser posible en la medida en que se conozca la velocidad de los discos duros tradicionales y su frecuencia de resonancia, con ello podría plantearse varias acciones malintencionadas, una de robar datos e información; y segundo, inhabilitar los discos para que no se conozca el proceso desarrollado (Shahrad *et al.*, 2018).

Finalmente, acorde con los resultados obtenidos en la prueba de concepto y de los autores relacionados, este artículo resalta otro mecanismo de evidencia y comprobación de la fragilidad que pueden ser los datos personales, los cuales son catalogados como confidenciales o reservados con base en la ley colombiana.

## Conclusiones

Para extraer datos que pueden ser sensibles por medios no convencionales, el ultrasonido es una de las opciones, dado que no requiere grandes recursos y los elementos computacionales (portátiles) vienen dotados de componentes capaces de generar las ondas portadoras para filtrar información.

La transmisión de datos por ultrasonido fue muy positiva y se lograron los objetivos planteados, esto gracias al software construido y las condiciones de sonido creadas en el laboratorio, con ello, se pudo obtener datos en el receptor; sin embargo, si bien diferentes palabras tuvieron problemas en su envío (las de mayor amplitud), muchas de ellas llegaron completas a través del canal encubierto, lo que supone poder afinar un poco más el software para que el porcentaje de error disminuya considerablemente.

Con los resultados obtenidos se ha demostrado que, de una manera simple, cualquier persona puede hacer un uso mal intencionado de datos en equipos de cómputo, y, en ese sentido, puede estar frente a un delito informático castigado con pena de prisión en Colombia bajo la Ley 1273 de 2009 y en especial los art. 269C, 269F, eventualmente el art. 269E puede aplicar en el caso que lo transmitido sea un *malware*.

En comparación con resultados de otros autores, las pruebas realizadas corroboran el potencial que tienen los atacantes al usar medios no convencionales para exfiltrar información, con lo cual, los administradores de seguridad se enfrentan a nuevos retos que no se tenían proyectados; sin embargo, la prueba realizada presenta algunas limitaciones, como lo es el uso de un software que module y envíe información, y del otro lado, un software que recolecte y de-module para conocer que se ha transmitido.

En futuros trabajos, se podría ejecutar la prueba contraria, con el fin de validar la posibilidad de inyectar datos e información (o algún programa de tipo *malware*), con ello establecer no solo el riesgo de fuga de información, sino demostrar la consolidación de otros tipos de delitos, así como los impactos a la integridad y a la disponibilidad de la información y las plataformas.

Asimismo, se propone ejecutar algunas pruebas en un ambiente no controlado, donde exista perturbaciones y se pueda probar la transferencia de la información a través de los elementos computacionales utilizados, con ello, establecer un ambiente más real (cotidiano).

Finalmente, se propone ampliar la base de palabras, frases y nombres de archivos que deban ser clasificados y, con la ayuda de un mecanismo de tipo DLP (*Data Loss Prevention*), lograr identificar y contrarrestar posibles fugas de información y, con ello, reducir la posible consolidación de algún delito informático.

## Referencias

AlKilani, H., Nasereddin, M., Hadi, A., y Tedmori, S. (2019). *Data Exfiltration Techniques and Data Loss Prevention System*. 2019 International Arab Conference on Information Technology (ACIT), 124-127. https://doi.org/10.1109/ACIT47987.2019.8991131

Álvarez Castelló, R. (2018). *Bases físicas de la luz, procedimientos Endoscópicos en Gastroenterología*. https://nanopdf.com/download/bases-fisicas-de-la-luz_pdf

Carpentier, E., Thomasset C., y Briffaut, J. (2019, 17-20 de noviembre). *Bridging The Gap: Data Exfiltration in Highly Secured Environments Using Bluetooth IoTs*. IEEE 37th International Conference on Computer Design (ICCD). https://doi.org/10.1109/ICCD46524.2019.00044

Chen, Q., Liu, F. W., Xiao, Z., Sharma, N., Cho, S. K. y Kim, K. (2019). Ultrasound Tracking of the Acoustically Actuated Microswimmer. *IEEE Transactions on Biomedical Engineering*, *66*(11), 3231-3237. https://doi.org/10.1109/TBME.2019.2902523

Congreso de la República. (2009). *Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones*. 5 de enero de 2009. Diario Oficial No. 47223.

GNU Radio project. (2022). *About GNU Radio*. https://www.gnuradio.org/about/

iZotope Corp. (2021). *The Complete Audio Repair Toolkit*. https://www.izotope.com/en/products/rx.html

Leyden, J. (2013, 5 de diciembre). *Hear that? It's the sound of BadBIOS wannabe chatting over air gaps, LANs-free prototype mimics notorious rootkit*. https://www.theregister.com/2013/12/05/airgap_chatting_malware/

Liu, X., Zhang, P., Wang, F., y Wu, X. (2019). *Design and Implementation of the Information Transmission System Based on Ultrasound*. IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), 1862-1865, https://doi.org/10.1109/ITAIC.2019.8785630

Murphy, K. (2017). *Quietnet*. https://github.com/Katee/quietnet/blob/master/Readme.md

NumPy Project. (2020). *NumPy software*. https://numpy.org/

Ortega, D., y Seguel, S. (2004). Historia del ultrasonido: el caso chileno. *Revista Chilena de Radiología*, *10*(2), 89-92. https://dx.doi.org/10.4067/S0717-93082004000200008

Osorio-Sierra, A., Mateus-Hernández, M. J., y Vargas-Montoya, H. F. (2020). Proceso para la identificación, clasificación y control del comportamiento de familias Ransomware. *Revista UIS Ingenierías*, *19*(3), 131-142. https://doi.org/10.18273/revuin.v19n3-2020013

Pérez, E. (2020). *El zip de la muerte: un "inocente" archivo comprimido capaz de explotar hasta colapsar tu PC con billones de datos*. https://www.xataka.com/aplicaciones/zip-muerte-inocente-archivo-comprimido-capaz-explotar-colapsar-pc-billones-datos.

Pérez, M. A. (2013). *Cómo actúa BadBIOS, el malware capaz de propagarse por el sonido*. https://blogthinkbig.com/badbios-malware-sonido-2

Peritos Informáticos. (2021, 18 de agosto). *Qué es un delito informático y qué tipos existen*. https://peritos-informaticos.com/que-es-un-delito-informatico-y-que-tipos-existen

PyAudio Project. (2020). *Python Bindings for PortAudio*. https://pypi.org/project/PyAudio/

Qt Group. (2022). *One framework. One codebase. Any platform*. https://www.qt.io/

Quiroz Tascón, S., Zapata Jiménez, J., y Vargas Montoya, H. F. (2020). Predicting Cyber-Attacks in Industrial SCADA Systems Through the Kalman Filter Implementation. *Revista TecnoLógicas*, *23*(48), 249-267. https://doi.org/10.22430/22565337.1586

Roldán Álvarez, M. A., y Vargas Montoya, H. F. (2020). Ciberseguridad en las redes móviles de telecomunicaciones y su gestión de riesgos. *Revista Científica Ingeniería y Desarrollo*, 38(2), 279-297. https://doi.org/10.14482/inde.38.2.006.31

Shahrad, M., Mosenia, A., Song, L., Chiang, M., Wentzlaff, D., y Mittal, P. (2018). *Acoustic Denial of Service Attacks on Hard Disk Drives. ASHES '18: Proceedings of the 2018 Workshop on Attacks and Solutions in Hardware Security*, 34-39. https://doi.org/10.1145/3266444.3266448

Solairaj, A., Prabanand, S. C., Mathalairaj, J., Prathap, C., y Vignesh, L. S. (2016). *Keyloggers software detection techniques*. 10th International Confe-

rence on Intelligent Systems and Control (ISCO), 1-6. https://doi.org/10.1109/ISCO.2016.7726880

Spiros, A., y Braghin, B. (2019). *4Kdump: Exfiltrating files via hexdump and video capture*. ICPS Proceedings, Proceedings of the Sixth Workshop on Cryptography and Security in Computing Systems. 1–6, https://doi.org/10.1145/3304080.3304081

Stepen, L. J. (2020). *El archivo de la muerte 42.zip – Como crear una Zip Bomba*. https://kodigo.info/el-archivo-de-la-muerte-42zip/