UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ

Colegio de Ciencias e Ingenierías

Diseño y Configuración de red de sondas para monitoreo de censura en el acceso a Internet del Ecuador

Jonathan David Ocles Mina

Ingeniería en Sistemas

Trabajo de integración curricular presentado como requisito
para la obtención del título de:
Ingeniero en Sistemas

Quito, 3 de diciembre de 2019

UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ

COLEGIO DE CIENCIAS E INGENIERÍAS

HOJA DE CALIFICACIÓN
DE TRABAJO DE INTEGRACIÓN CURRICULAR

Diseño y Configuración de red de sondas para monitoreo de censura en el acceso a Internet del Ecuador

Jonathan David Ocles Mina

Calificación:	_____
Nombre del profesor, Título académico:	**Daniel Riofrío, PhD. in Computer Science**
Firma del profesor:	_____

Quito, 3 de diciembre de 2019

Derechos de Autor

Por medio del presente documento certifico que he leído todas las Políticas y Manuales de la Universidad San Francisco de Quito USFQ, incluyendo la Política de Propiedad Intelectual USFQ, y estoy de acuerdo con su contenido, por lo que los derechos de propiedad intelectual del presente trabajo quedan sujetos a lo dispuesto en esas Políticas.

Asimismo, autorizo a la USFQ para que realice la digitalización y publicación de este trabajo en el repositorio virtual, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Firma del estudiante: _____

Nombres y apellidos: Jonathan David Ocles Mina

Código: 00112226

Cédula de identidad: 1721345914

Lugar y fecha: Quito, 3 de diciembre de 2019

RESUMEN

A pesar de que el Internet ha influenciado de forma positiva en varias actividades de nuestra cotidianidad, como la comunicación, la salud, la educación, etc.; existe evidencia que grupos de poder aún tratan de reprimir la información existente en la gran red (Internet), basándose del uso de diferentes técnicas o metodologías para distorsionar la información o bloquear su acceso.

El presente documento describe el diseño de una red que permita monitorizar diferentes niveles de censura del Internet del Ecuador. Además, ofrece una discusión de cómo realizar la configuración de esta red de sondas (distribuidas que utilizan el proyecto OONI) y la implementación de un prototipo de esta red.

Palabras clave: derechos digitales, censura, Internet, OONI, Raspberry Pi, sonda

ABSTRACT

Although the Internet has positively influenced various activities of our daily lives, such as communication, health, education, etc.; there is evidence that groups in power try to repress exiting information in the Internet, based on the use of different techniques or methodologies to distort the information or block its access.

This document describes the design of a network that allows monitoring different levels of censorship in Ecuador's Internet space. Furthermore, this document discusses how to configure such network using OONI probes and shows how to implement a functional prototype of it.

Keywords: digital rights, censorship, Internet, OONI, Raspberry Pi, probe

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

Motivación

La evolución tecnológica ha influenciado en todos los ámbitos de la vida humana, desde la forma en la que realizamos los negocios hasta la forma en la que nos comunicamos, accedemos a la salud o a la educación (Rofrio et al., 2019); es decir, la tecnología hoy en día es un complemento importante para el desarrollo de varias actividades de nuestra cotidianidad, de tal forma que, para muchas personas, el Internet se ha convertido en sinónimo de libertad (Castells, 2003). Sin embargo, el control de la información ha sido un objetivo para muchos países y, con los avances tecnológicos que lo permiten, entidades como el Gran Cortafuegos de China no son las únicas amenazas a la libertad en el Internet (Ramesh, Leonid, & Roya, 2019).

Muchos estados han implementado prácticas de censura extensiva arguyendo para ello la necesidad de garantizar los derechos a la propiedad intelectual, la defensa a la seguridad nacional, la preservación de valores religiosos y normas culturales, el amparo de niños, niñas y adolescentes ante la explotación y la pornografía infantil. Las técnicas de las cuales hacen uso para restringir el acceso a la información van desde la manipulación del contenido para la difusión de información errónea hasta la inhabilitación parcial o total del servicio (Burnett & Feamster, 2013).

Debido a que el Internet por sí mismo es facilitador de derechos humanos, impulsador del desarrollo económico y social de las sociedades, es considerado por la Organización de Naciones Unidas, como derecho humano. Ergo, eventos como los casos de censura en Egipto, Libia y Siria durante la ‘primavera árabe’ (Fuertes, 2012), el bloqueo de Internet durante las manifestaciones de Irán en noviembre del 2019 (NetBlocks, 2019) o los bloqueos de servidores por el gobierno ruso en su intento de impedir el acceso a Telegram (Akbari &

Gabdulhakov, 2019) atentan contra el derecho a la libertad de expresión y opinión recogido en el artículo 19 de la Declaración Universal de Derechos Humanos (Delgado, 2014).

En consecuencia, el presente proyecto plantea como una alternativa desde la academia el transparentar la utilización de Internet y, promulgar y difundir los derechos digitales de la población del Ecuador, haciendo uso de una red conformada por dispositivos de placa Raspberry Pi, integrados con la herramienta de medición de censura del proyecto del Observatorio Abierto de Interferencia en la Red (OONI, por sus siglas en inglés), OONI Probe.

Objetivo Principal

Analizar las características del proyecto OONI para la medición de cesura en el acceso al Internet ecuatoriano.

Objetivos Específicos

- Examinar los tipos de pruebas que se pueden ejecutar contra sitios web y servidores en Internet haciendo uso de la herramienta para la medición de censura, OONI Probe.
- Diseñar un prototipo de red, que haga uso de la herramienta OONI Probe en Raspberry Pi, para monitorear potencial censura en el Internet ecuatoriano.
- Implementar un prototipo de red, que haga uso de la herramienta de OONI Probe en Raspberry Pi, para la medición de la censura en sitios web de interés.
- Implementar una herramienta web básica de visualización de resultados medidos por OONI.

DESARROLLO DEL TEMA

Proyecto OONI

El Observatorio Abierto de Interferencia de Red (OONI), conforma una red global de observación que tiene como objetivo la detección de presencia de dispositivos de interceptación de red aparentemente pasivos que realizan discriminación de tráfico y el entendimiento del contenido que está siendo objeto de discriminación. Es decir, OONI está diseñado con el objetivo de crear métodos y herramientas que permitan la comprensión de qué direcciones web se están bloqueando, las palabras clave que hacen uso para llevar a cabo el filtrado y los tipos de protocolos que se ven afectados durante estos procesos de censura. En consecuencia, el proyecto OONI ha desarrollado la herramienta OONI Probe, la misma que permite realizar mediciones de área local, ejecutándose en redes de borde (Filastò & Appelbaum, 2012).

Funcionamiento de OONI Probe

El proyecto de OONI está integrado por dos módulos principales (**Error! Reference source not found.**): OONIB, que es el componente de back-end responsable de la utilización de los ayudantes de prueba y de la colección de los informes de las pruebas; y, OONI Probe, módulo en el que reside la lógica de las pruebas y la generación de reportes (Filastò, s/f).

Los ayudantes de prueba son implementaciones de protocolos del lado del servidor que actúan como soporte para las pruebas realizadas por OONI Probe, estos pueden ser servidores HTTP (protocolo de transferencia de hipertexto, por sus siglas en inglés), servidores DNS (sistema de nombres de dominio, por sus siglas en inglés) o servidores Traceroute. El colector de reportes es el servicio ocupado por OONI para recibir y recolectar los resultados de las mediciones realizadas (Filastò & Appelbaum, 2012).

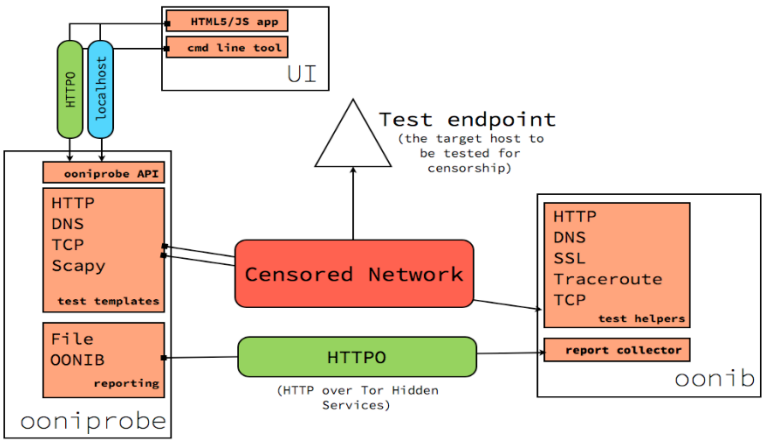


Figura 1. Diseño de arquitectura del proyecto OONI

Pruebas admitidas en OONI Probe

Las pruebas de medición de interferencia en la red, que se puede realizar en OONI Probe, están divididas por categorías, entre ellas: bloqueo de contenido, manipulación de tráfico y experimentales.

Pruebas de Bloqueo de Contenido.

El objetivo principal de estas pruebas es enumerar el tipo de contenido que está siendo bloqueado desde la perspectiva de la red en la que se están realizando las pruebas (OONI, 2013)

Bridge Reachability test.

Esta prueba examina la operatividad de los puentes Tor en la red. La prueba requiere que previamente se establezca una lista de puentes como entrada y, en caso de conectarse con éxito, se considerará que los puentes no se encuentran bloqueados en la red. Al contrario, si la prueba no puede enlazar ninguna conexión, se considera que los puentes de Tor se encuentran bloqueados o desconectados (OONI, s/f-h).

DNS Consistency test.

Esta prueba realiza comparación de las respuestas de un servidor DNS que se considera confiable con aquel servidor que está siendo probado. Si ambas direcciones IP (protocolo de internet, por sus siglas en inglés) del mismo sitio web consultado tienen resoluciones diferentes, se tiene un indicador de interferencia o bloqueo en la red. Si los ISP (proveedor de servicios de internet, por sus siglas en inglés) manipulan las respuestas de DNS los usuarios serán direccionados a otros portales web o no podrán conectarse (OONI, s/f-a). Hay que tomar en consideración que los servidores DNS proporcionan las direcciones IP más cercanas según su ubicación geográfica, razón por la cual de esta prueba pueden surgir falsos positivos.

Facebook Messenger test.

Esta prueba busca ver si existen bloqueos en la red hacia los servidores de Facebook. La metodología que utiliza OONI Probe inicia por intentar establecer una conexión TCP (protocolo de control de transmisión, por sus siglas en inglés) y realizar una búsqueda DNS en los dominios asociados a Facebook. Se reconoce un posible bloqueo en caso de que las conexiones TCP a los servidores de Facebook fallen o si las búsquedas DNS no se resuelven en las direcciones IP asignadas para Facebook (OONI, s/f-b).

HTTP Requests test.

Esta prueba realiza la comparación de solicitudes HTTP sobre la red de Tor y sobre la red del usuario, para determinar la censura. Para la detección de los casos de censura la prueba realiza solicitudes HTTP a determinados sitios web a través de ambas redes (Tor y la red del usuario), si ambos resultados coinciden se descarta una posible interferencia; sin embargo, si estos resultados difieren, el sitio web que se está probando probablemente esté censurado. Se reconoce una posible interferencia si la longitud del cuerpo o los encabezados HTTP no coinciden o si la solicitud HTTP a través de la red del usuario falla. Los creadores

de la prueba advierten que puede generarse un falso positivo cuando la conexión de control de Tor es discriminada por el servidor, lo que normalmente sucede con páginas donde aparecen controles CAPTCHA (OONI, s/f-f).

Meek fronted request test.

Meek es un tipo de puente Tor que utiliza dominios no bloqueados como google.com (Google), awsstati.com (Amazon) y ajax.aspnetcdn.com (Microsoft) para enviar a sus usuarios sobre Tor a sitios web bloqueados (Xynou, Filastò, Yusof, & Ming, 2016). Esta prueba realiza una conexión encriptada a dominios en la nube a través de HTTPS y examina si puede establecer una conexión.

Telegram test.

Esta prueba examina la accesibilidad de la aplicación y la versión web de, la metodología utilizada consiste en una solicitud HTTP POST y establecer una conexión TCP a los endpoints de Telegram, así como una solicitud HTTP GET al portal web de Telegram sobre la red del usuario. Según esta metodología si las conexiones TCP a todos los endpoints de Telegram probados fallan, o las solicitudes HTTP POST a los endpoints no envían una respuesta es probable que la aplicación de Telegram se encuentre bloqueada; mientras que para el portal web, si las solicitudes HTTP/HTTPS GET no envían una respuesta coherente, es probable que se encuentre bloqueada (OONI, s/f-g).

Vanilla Tor test.

Esta prueba intenta establecer una conexión con la red Tor, si la misma arranca con éxito dentro de una cantidad de segundos, definida previamente, se considera que Tor es accesible desde la red probada; pero, si la prueba no establece conexión es probable que la red Tor se encuentre bloqueada (OONI, s/f-i).

Web Connectivity test.

Esta prueba tiene la finalidad de identificar la accesibilidad de los sitios web. La prueba se basa en resolver la dirección DNS de una url, establecer una conexión TCP y realizar una solicitud HTTP/HTTPS GET, desde la red del usuario y a través de un servidor controlado (como Tor); si ambas respuestas proporcionan resultados coincidentes, no existen señales de interferencia de red; pero si los resultados difieren, el sitio web, al que se está haciendo la prueba, está probablemente siendo censurado (OONI, s/f-j).

WhatsApp test.

Esta prueba se encarga de examinar la accesibilidad de WhatsApp tanto en su versión web como en la plataforma de la aplicación. La prueba realiza una solicitud HTTP GET, establece una conexión TCP y resolución de DNS en los endpoints y al servicio de registro de WhatsApp, de acuerdo con esta metodología si las conexiones TCP a los a los endpoints o a los servicios de registro de WhatsApp fallan, las búsquedas de DNS se resuelven en IPs no asignadas a WhatsApp o las solicitudes HTTP al servicio de registro de WhatsApp no envían una respuesta, es probable que la aplicación de WhatsApp esté bloqueada. Mientras que, para la interfaz web probablemente se encuentre bloqueada si las conexiones TCP fallan, si en la resolución DNS se muestran diferentes IPs para web.whatsapp.com o si las solicitudes HTTP a web.whatsapp.com no envían ninguna respuesta coherente (OONI, s/f-k).

Pruebas de Manipulación de Tráfico.

Las pruebas de manipulación de tráfico están orientadas a la detección de la presencia de algún tipo de alteración o modificación del tráfico de Internet, entre la red desde la que se llevan a cabo las pruebas y un servidor externo (OONI, 2013).

HTTP Header Field Manipulation test.

Esta prueba busca detectar la presencia de mecanismos que puedan estar siendo usados para la censura o la manipulación del tráfico en la red, conocidos como cajas

intermedias (middle boxes, en inglés). La prueba emula una solicitud HTTP hacia un servidor, colocando en el encabezado variaciones de palabras escritas con letras que alternan las mayúsculas y minúsculas, es decir, encabezados válidos pero creados de una forma poco común; se hace comparación con los resultados recibidos, en caso de que los datos de respuesta no sean exactamente iguales a los enviados, la prueba asume que existe una caja intermedia que está vigilando o manipulando el tráfico de la red (OONI, s/f-c). Hay que tomar en cuenta que la presencia de una caja intermedia no es siempre un indicativo de manipulación de tráfico, ya que es de uso común en las infraestructuras de las redes para proporcionar garantías de seguridad y un buen rendimiento (Fayazbakhsh, Sekar, Yu, & Mogul, 2013).

HTTP Host test.

Esta prueba hace uso de procedimientos y técnicas utilizadas para evitar ser detectado por censores y luego utiliza una lista de dominios para enviar solicitudes HTTP a estos resultados y verificar la conexión. Los resultados obtenidos son en formato JSON (Notación de Objetos de Javascript, por sus siglas en inglés) y pueden incluir: la huella digital que determina la presencia de cajas intermedias, si se encuentran accesibles los dominios solicitados o información relevante para la identificación del tipo de infraestructura utilizada para implementar la censura (OONI, s/f-d).

HTTP Invalid Request Line test.

Esta prueba envía una solicitud HTTP no válida hacia un servicio *echo* que escucha en el puerto estándar HTTP. Ya que el servicio echo, devuelve una copia idéntica de los datos que recibió, en caso de que la red no esté siendo manipulada tendría que devolver la línea de solicitud HTTP no válida al usuario tal y cual la recibió. Sin embargo, si la red cuenta con algún dispositivo de manipulación, la solicitud inválida puede generar un error como respuesta. En algunas ocasiones estos errores pueden contener el nombre (o una forma de

rastrear la procedencia) del software o hardware que se está usando para la censura (OONI, s/f-e).

Pruebas Experimentales.

Son aquellas pruebas que aún no se consideran que alcanzaron la fase adecuada para que su resultado sea tomado como verás (OONI, 2013); en este tipo de pruebas OONI Probe da cabida a que el usuario cree y ejecute sus propias pruebas para la medición de censura en la red.

Diseño de una Red OONI Probe

Tomando en cuenta el porcentaje de participación de mercado de los principales proveedores de servicio de Internet en el Ecuador (Tabla 1Tabla 1) y el porcentaje de personas que han utilizado el Internet a nivel nacional por ubicación geográfica, según cifras de la última encuesta realizada por el Instituto Nacional de Estadísticas y Censos (Tabla 2**Error! Reference source not found.**); se propone instalar un nodo de medición de censura de Internet para cada uno de los cuatro principales proveedores de Internet en el país (CNT, Netlife, Claro y PuntoNet) en las diez provincias en las que el uso de Internet es mayor, es decir: Galápagos, Pichincha, Azuay, Guayas, El Oro, Santo Domingo de los Tsáchilas, Tungurahua, Imbabura, Loja y Santa Elena. Un servidor, el cual tendrá como principal función el almacenamiento de los resultados obtenidos por los nodos que idealmente estaría ubicado en las instalaciones de la Universidad San Francisco de Quito. Es decir, según lo propuesto, la red estará conformada por 40 nodos distribuidos en el territorio nacional y un

servidor central (ANEXO B).

PRESTADOR	NUMERO DE CUENTAS INTERNET FIJO	PARTICIPACIÓN DE MERCADO
CORPORACION NACIONAL DE TELECOMUNICACIONES CNT EP	933.906	46,3%
MEGADATOS S.A.	317.542	15,8%
SERVICIOS DE TELECOMUNICACIONES SETEL S.A.	230.519	11,4%
CONSORCIO ECUATORIANO DE TELECOMUNICACIONES S.A. CONECEL	201.533	10,0%
PUNTO NET S.A.	81.239	4,0%
ETAPA EP.	64.999	3,2%
TELCONET S.A.	19.070	0,9%
SOLUCIONES AVANZADAS INFORMATICAS Y TELECOMUNICACIONES SAITEL	18.400	0,9%
UNIVISA S.A.	8.752	0,4%
NECUSOFT CIA. LTDA.	7.878	0,4%
RESTO DE PRESTADORES	131.321	6,5%
TOTAL	**2.015.159**	**100%**

Tabla 1. Proveedores de Servicio de Internet Fijo en el Ecuador (ARCOTEL, 2019)

Provincia del Ecuador	Porcentaje de personas
Galápagos	81.3%
Pichincha	68.7%
Azuay	64.5%
Guayas	63.7%
El Oro	61.9%
Santo Domingo de los Tsáchilas	61.8%
Tungurahua	59.4%
Imbabura	56.8%
Loja	56.1%
Santa Elena	53.3%
Manabí	53.0%
Cotopaxi	50.3%

Amazonía (Napo, Pastaza, Sucumbíos, Orellana, Zamora Chinchipe y Morona Santiago)	50.2%
Cañar	48.6%
Carchi	48.2%
Los Ríos	48.1%
Esmeraldas	46.9%
Bolívar	45.5%
Chimborazo	45.1%

*Esta tabla contiene datos de encuestas realizadas en el 2017 por el Instituto Nacional de Estadísticas y Censos y representa la cantidad de usuarios de Internet correspondiente a cada provincia del Ecuador.

Tabla 2. Porcentaje de personas que utilizan Internet por provincias (INEC, 2017)

Configuración de un Nodo

Dado que OONI Project nos permite realizar pruebas que posibilitan determinar si el acceso al contenido en el Internet ha sido sujeto a algún tipo de discriminación y que, OONI Probe es el software/agente que permite realizar las pruebas sobre sitios web de interés y recolectar sus resultados; es de nuestro interés que cada nodo de la red de prueba pueda correr a OONI Probe de forma independiente.

Para ello, cada nodo correrá sobre un computador independiente de bajo costo como lo son las placas de computadora Raspberry Pi (Severance, 2013). Las Raspberry Pi son microcomputadoras, basadas en arquitectura de microprocesador ARM (usualmente utilizado en el desarrollo de dispositivos móviles inteligentes); al carecer de partes móviles, la Raspberry Pi es una computadora de una sola placa. Están integradas de un procesador gráfico, un microprocesador de 1 núcleo, puertos USB, puerto HDMI, y memoria SDRAM.

Su sistema operativo recomendado oficialmente y soportado por la fundación “Raspberry Pi” es Raspbian, una distribución GNU/Linux basada en Debian (Salcedo & Cendrós, 2016).

Para la configuración de cada nodo, se instaló la última versión disponible del sistema operativo Raspbian de su página oficial.

Instalación y configuración de OONI Probe.

1. Registrar el repositorio de OONI para poder hacer uso del administrador de paquetes:

gpg --keyserver keys.gnupg.net --recv

A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD 89

gpg --export A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89

sudo apt-key add echo 'deb http://deb.torproject.org/torproject.org buster main'

sudo tee /etc/apt/sources.list.d/ooniprobe.list

apt update; apt install ooniprobe

2. Clonar del repositorio GitHub el código del paquete de mediciones (Measurement kit):

git clone https://github.com/measurement-kit/measurement-kit.git

Previo al uso de OONI Probe, es necesario responder un cuestionario que asegura que se ha leído y aceptado la Política de Datos, y que se asumen los riesgos de ejecutar localmente OONI Probe, los cuales, se resumen en: que, cualquiera que esté realizando un monitoreo de la actividad de Internet (ISPs, gobierno, empleadores, etc.) serán capaces de ver que se está haciendo uso de OONI Probe; que, las pruebas de conectividad web realizan conexiones y descargas de datos de sitios que pueden ser considerados ilegales en algunos países (como sitios de pornografía); que, por defecto los datos recopilados por OONI Probe son enviados a OONI y publicados al público para aumentar la transparencia de la censura en Internet, fomentar el debate y apoyar a la investigación, lo que puede ser visto

desfavorablemente por algunos gobiernos y, algunos proveedores de servicio de Internet podrían intentar identificar usuarios a través de los datos públicos (OONI, s/f-l).

Debido a que en la realización del proyecto se ha creado un servidor propio para la recolección de los archivos, el cual se detalla más adelante, no se hace uso del módulo OONIB; por lo consiguiente, no enviamos los resultados al colector de OONI. Para este efecto, una vez realizado el cuestionario, ejecutamos los siguientes comandos en la terminal:

```
echo "collector: no" >> ~/.ooni/ooniprobe.conf
echo "collector: no" >> /etc/ooniprobe.conf
```

Con lo cual los resultados obtenidos de las pruebas realizadas se guardarán en el directorio local: ~/.ooni/measurements/.

Para listar las pruebas a realizarse en OONI Probe, es necesario tener un archivo YAML, que es un formato de serialización propuesto por Clark Evans en el 2001 e inspirado en lenguajes como XML, C, Python, Perl, cuyo objetivo es almacenar objetos de datos con estructura de árbol (Evans, Ingerson, & Ben-Kiki, 2001); en el cual se detallan los inputs y el nombre de la prueba a realizar, por la herramienta OONI Probe. Los archivos que contienen los inputs para las distintas pruebas (sean estos enlaces de páginas web o direcciones IP) se encuentran en el directorio ~/.ooni/data/input, que es el directorio por defecto en el cual OONI Probe espera encontrar los archivos de entradas para la ejecución de sus pruebas.

Configuraciones adicionales.

Considerando que los resultados de las pruebas deben ser enviados al servidor de archivos, se creó un script en Python para este fin, el cual toma todos los archivos que se encuentren en el directorio en el que se almacenan los resultados y los envía al servidor de archivos, haciendo uso del protocolo FTP (protocolo de transferencia de archivos, por sus siglas en inglés), para posteriormente eliminar el contenido del directorio (el funcionamiento está detallado en el diagrama de flujo de la Figura 2).

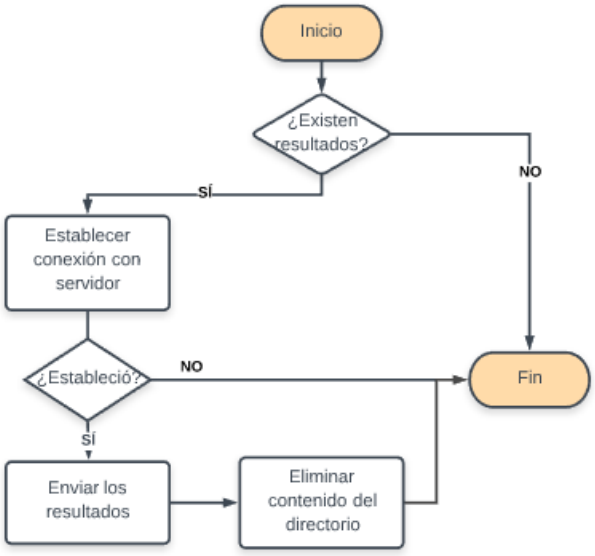


Figura 2. Diagrama de flujo de funcionamiento del script Python para el envío de datos al servidor de archivos FTP

Al prever cualquier eventualidad, se advirtió en la necesidad de implementar un método que nos permita acceder a los nodos de manera remota, creando así un script bash (Figura 3) que realiza la verificación de disponibilidad de los puertos asignados en un servidor para la conexión remota y, al encontrar uno dentro del rango, establece una conexión de túnel reverso o reverse SSH (reverse secure shell); y un script que permita la persistencia en la conexión (Figura 4). Ambos scripts fueron agregados al archivo de configuración del servicio cron (Figura 6).

```
#!/bin/bash
#echo 0>/home/pi/puerto
contador=20015
termina=20030
a=0
t=$(cat /home/pi/puerto)
sleep $t;
echo $a>/home/pi/puerto
while [ $termina -ge $contador ]; do
 s=$(/usr/bin/nmap -p $contador 51.79.70.105 | egrep 'closed | open')
 if [[ $s =~ 'closed' ]]; then
 # echo "entro cerrado, funciona el puerto $contador -> $s">>/home/pi/puerto
  a=$contador;
  break;
 else
  #echo "entró abierto, no funciona el puerto $contador -> $s">>/home/pi/puerto
  let contador=$contador+1;
 fi
done
echo $a>/home/pi/puerto
ssh -N -f -R $a:localhost:22 jocles@51.79.70.105
```

Figura** 3. **Script Bash para tunelaje reverso (reverse SSH)

```
#!/bin/bash
s=$(cat /home/pi/puerto)
/usr/bin/ssh -N -f -R $s:localhost:22 jocles@51.79.70.105
```

Figura** 4. **Script Bash de persistencia de reverse SSH

Además, se creó un script bash que permita la automatización de las pruebas (Figura 5), tanto la ejecución de la herramienta OONI Probe, como el envío de los resultados al servidor de archivos, este script también se lo agregó al servicio cron (Figura 6).

```
#!/bin/bash
ISP=$(curl -s https://www.whoismyisp.org | grep -oP -ml '(?<=isp">).*(?=</p)')
HORA=$(date +"%H:%M:%S")
tiempo_inicio=$(date +%s)
ooniprobe -i /home/pi/web-full.yaml
python subir_ftp.py
tiempo_final=$(date +%s)
DIA=$(date +"%Y%m%d")
IP=$(curl ifconfig.me)
echo "$ISP $IP $DIA $HORA $((tiempo_final - tiempo_inicio))">>registro.log
```

Figura** 5. **Script que llama a ejecución de la prueba, envío de archivos a ftp

```
# m h  dom mon dow   command
0 */2 * * * sudo sync && sudo sysctl -w vm.drop_caches=3
0 */4 * * * /home/pi/prueba.sh
@reboot sleep 15; /home/pi/init_script.sh
```

Figura** 6. **Archivo del servicio cron para la automatización de procesos

Configuración del Servidor de Archivos a través del protocolo FTP

Como se mencionó con anterioridad, al no hacer uso del módulo OONIB, los resultados son almacenados localmente, es decir, en cada nodo; por lo cual se configuró un servidor capaz de receptar los resultados generados por cada nodo haciendo uso del protocolo de transferencia FTP; el servidor tiene como sistema operativo Ubuntu.

La conexión FTP es usada para la transferencia entre equipos de forma relativamente segura y completa. Razón por la cual, una solución para el proceso de transferencia es el uso de VSFTPD, utilidad desarrollada como servidor FTP con licencia para sistemas UNIX, en la cual lo más destacable es su seguridad, estabilidad y rapidez (Bauer, 2004).

1. **Instalación de VSFTPD:**

1.1. El repositorio Ubuntu trae disponible por defecto VSFTPD, motivo por el cual la instalación hace uso del paquete de instalación por defecto en los sistemas Debian. Para la instalación, hacemos uso del siguiente comando en una terminal:

```
sudo apt install vsftpd
```

1.2. Una vez que se ha instalado, se activa el servicio y se lo habilita en el arranque del sistema operativo:

```
sudo systemctl start vsftpd
sudo systemctl enable vsftpd
```

2. ***Estructura del Directorio VSFTPD***

2.1. Se crea un usuario para el acceso a través de FTP:

```
sudo adduser vsftpd
```

2.2. Se crea el directorio que servirá para alojar los archivos recibidos y se asignan los permisos correspondientes:

```
sudo mkdir -p /home/vsftpd/ftp/test
sudo chown vsftpd:vsftpd /home/vsftpd/ftp/test
```

sudo chmod a-w /home/vsftpd/ftp

3. Configuración VSFTPD

3.1. Acceder al archivo de configuración, /etc/vsftpd.conf, haciendo uso de un editor y añadir al final del archivo las siguientes líneas de configuración:

```
listen=NO
listen_ipv6=YES
anonymous_enable=NO
local_enable=YES
write_enable=YES
local_umask=022
dirmessage_enable=YES
use_localtime=YES
xferlog_enable=YES
connect_from_port_20=YES
chroot_local_user=YES
secure_chroot_dir=/var/run/vsftpd/empty
pam_service_name=vsftpd
pasv_enable=Yes
pasv_min_port=10000
pasv_max_port=11000
user_sub_token=$USER
local_root=/home/$USER/ftp
userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
userlist_deny=NO
```

3.2. Reiniciamos el servicio VSFTPD con las nuevas configuraciones:

sudo systemctl restart vsftpd

3.3. Comprobamos que podamos acceder al servidor FTP ingresando a través de cualquier navegador:

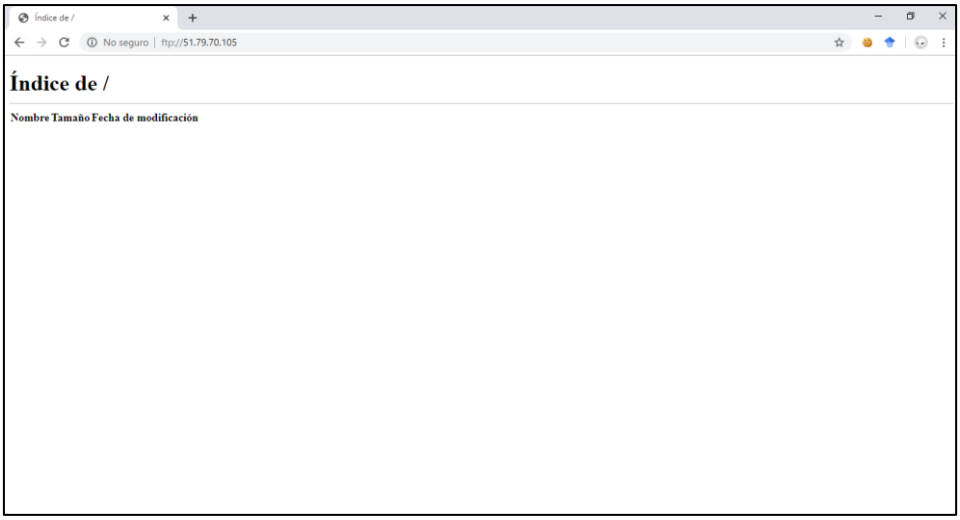


Figura 7. Servidor FTP visto desde navegor web

De esta forma tenemos ya en funcionamiento el servidor de archivos que nos servirá para la colección de los resultados obtenidos de las pruebas realizadas por nuestra red.

Pruebas y Prototipo

Para el diseño del prototipo se ha dispuesto de una red conformada por tres nodos y el servidor de archivos para la colección de los resultados. Cada nodo mantiene una conexión a Internet haciendo uso de los ISP's CNT, Claro y Netlife, respectivamente.

Para cada nodo se pensó en la ejecución de pruebas que nos permitan ver la existencia (o inexistencia) de cajas intermedias que estén manipulando el acceso normal del contenido de Internet, la disponibilidad de redes sociales y la disponibilidad de páginas web que creamos de interés para la prueba. De esta forma, las pruebas que se configuraron para la ejecución son:

- Web Connectivity test
- WhatsApp test
- HTTP Header Field Manipulation
- HTTP Invalid Request Line

Para las pruebas de Web Connectivity, en las cuales se requiere como entrada una lista de páginas web (ANEXO C), se ha utilizado una compilación de aquellas páginas que

fueron motivo de censura en el gobierno de Rafael Correa y de la lista de Citizen Lab's, de la Universidad de Toronto, que posee listas de páginas, a nivel mundial, más proclives a sufrir censura a causa de su contenido (Lab Citizen and Others, 2014).

La realización de las pruebas, haciendo uso del prototipo, se llevaron a cabo durante 3 semanas, tomando como fecha de inicio el 8 de octubre de 2019, semana en la cual distintos tipos de movimientos sociales daban continuidad a una manifestación, iniciada el 2 de octubre, hasta el 13 de octubre, tras el conocimiento público de medidas económicas, tomadas por el gobierno de Lenin Moreno, que afectarían el precio de la gasolina (El Universo, 2019).

Herramienta Web de Visualización de Resultados

Se implementó una plataforma web básica de visualización de alto nivel de los resultados obtenidos de las pruebas de mediciones. La página web consta de 3 pantallas principales:

Pantalla de Inicio

Presenta un calendario en el cual destacan los días de los cuales se ha recolectado datos, y al dar click en ellos, se los redirigirá a la pantalla de las pruebas recolectadas en el día especificado.

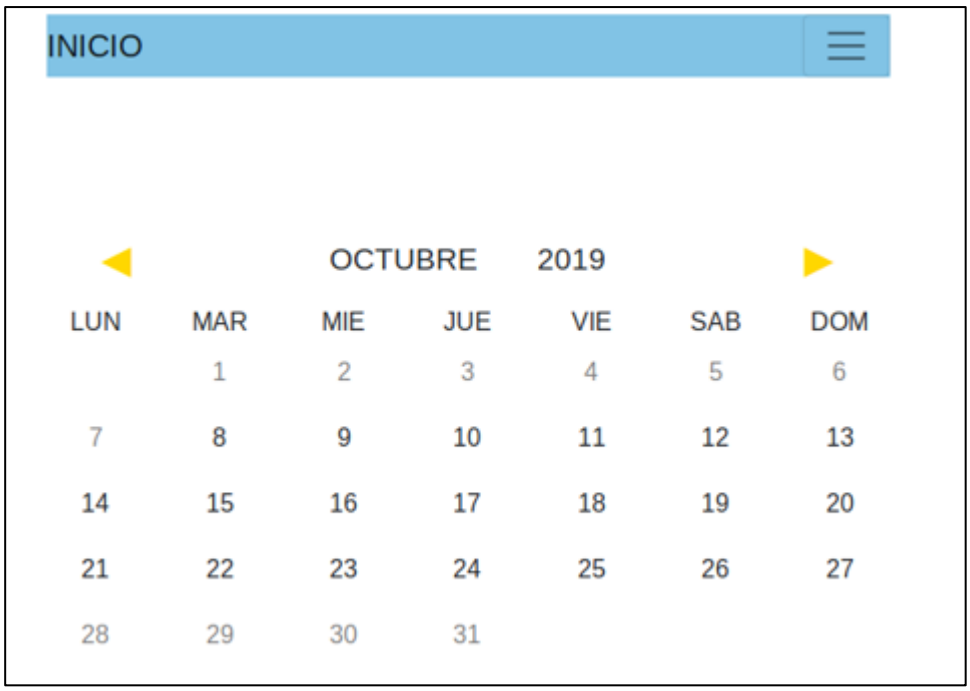


Figura 8. Página de Inicio del visor web

Pantalla de pruebas recolectadas

En la parte central se despliega, en forma de tabla, las pruebas recolectadas en el día accedido. Al lado izquierdo, presenta un formulario que permite realizar el filtrado de los datos de la tabla.

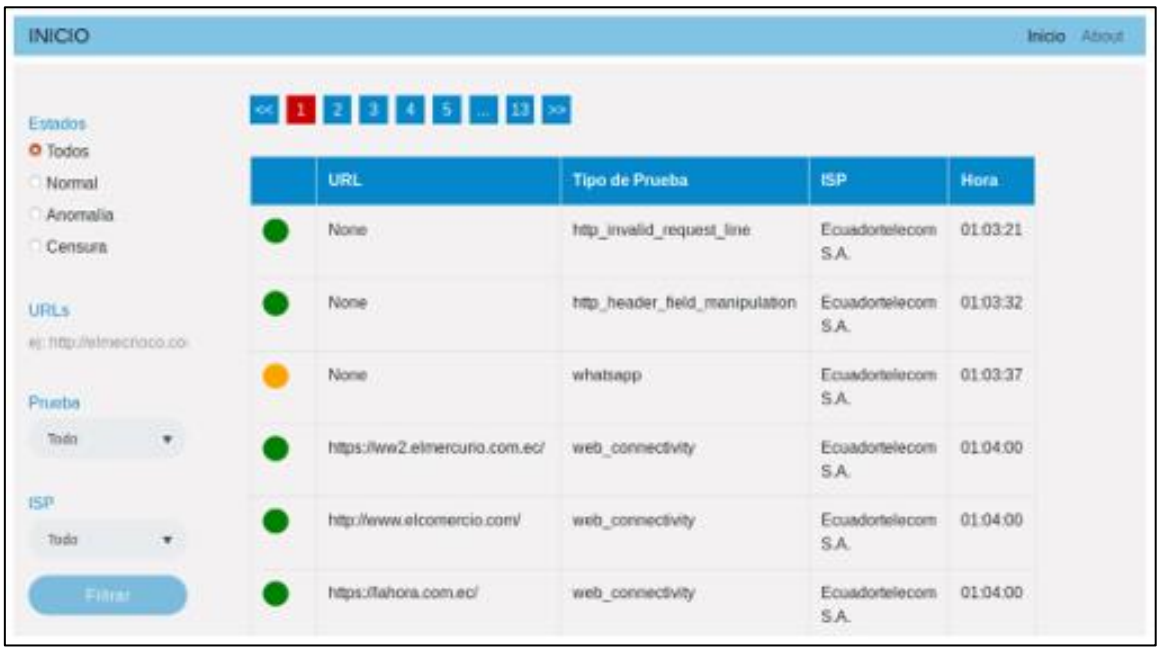


Figura 9. Página del visor web en la que se despliegan los resultados obtenidos

Pantalla de detalle de pruebas

Esta página nos da un conocimiento más a fondo de los detalles de la prueba, de los resultados obtenidos y permite realizar la descarga, en formato JSON, de los resultados obtenidos por las pruebas. Esta página provee de tres estados como indicadores de censura de una red, modificando el color de fondo de la cabecera. Los estados de las pruebas pueden ser:

Censura. Cuando los resultados obtenidos son concluyentes en la existencia de bloqueo o interferencia al acceso normal de Internet desde la red probada, se utiliza el color rojo como indicador de censura.

Anomalía. Cuando los resultados obtenidos indican un posible bloqueo o interferencia en el acceso normal; sin embargo, estos no pueden ser tomados como concluyentes debido a que podrían incurrir en la presencia de falsos positivos. En este caso se utiliza el color naranja como indicador de una anomalía en la red.

Normal. Cuando los resultados obtenidos niegan la existencia de algún bloqueo o interferencia en la red, se utiliza el color verde como indicador de ausencia de censura.

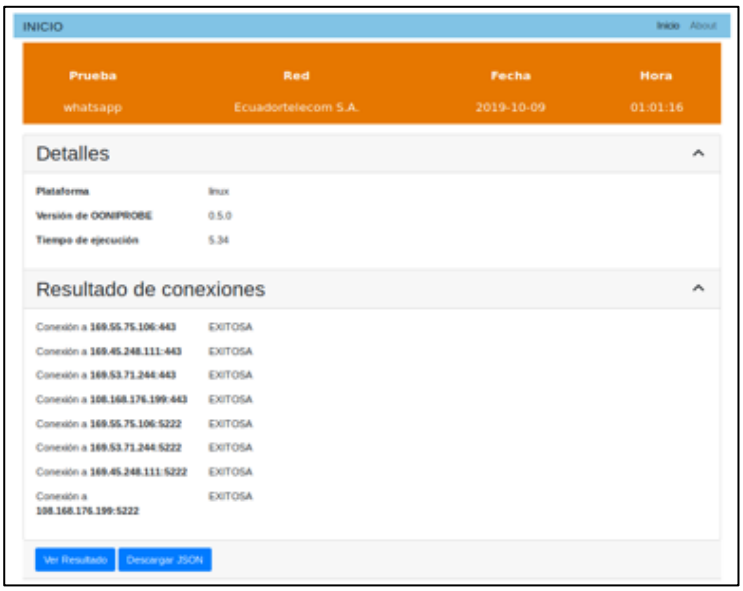


Figura 10. Página del visor web que presenta los detalles individuales de cada prueba

Resultados

Los resultados obtenidos durante las tres semanas de funcionamiento de la red tuvieron un volumen de aproximadamente 16 GB. Obteniendo un total de 167,805 pruebas, de las cuales el 2.27% presentaron algún tipo de anomalía, tal como se detalla en la Tabla 3. Cantidad de resultados obtenidos, clasificados por tipo y estado

Pruebas	**Estado de las Pruebas**		
	Normal	**Anomalía**	**Censura**
Web Connectivity (Ecuador)	4,232	6	0
Web Connectivity (Globales)	159,290	3,599	0
Whatsapp	0	215	0
HTTP Invalid Request Line	235	0	0
Http Header Field Manipulation	227	0	0

Tabla 3. Cantidad de resultados obtenidos, clasificados por tipo y estado

Debido a la coyuntura en la que se realizaron las pruebas, se tiene un mayor interés por los resultados nacionales, así que se separaron los resultados de las páginas web globales y nacionales de las pruebas de conectividad web. Los resultados que presentaron anomalía dentro de las pruebas de conectividad web de interés nacional, no fueron concluyentes para indicar la existencia de censura y se puede considerar la existencia de falsos positivos.

Fecha	**URL**	**Proveedor de Internet**
09 de octubre	https://wambra.ec/	Ecuadortelecom S.A (Claro)
09 de octubre	https://wambra.ec/	Corporación Nacional de Telecomunicaciones (CNT)
12 de octubre	https://wambra.ec/	Corporación Nacional de Telecomunicaciones (CNT)
18 de octubre	http://www.elcomercio.com/	Ecuadortelecom S.A (Claro)
22 de octubre	https://www.alainet.org/	Ecuadortelecom S.A (Claro)
26 de octubre	https://www.eluniverso.com/	Corporación Nacional de Telecomunicaciones (CNT)

Tabla 4. Resultados con anomalía de las páginas de interés nacional obtenidos durante las pruebas

Acerca de los resultados de la prueba de WhatsApp, acorde a lo mostrado en la Tabla 3, la totalidad de sus pruebas presentaron anomalías. La anomalía se percibió al momento de realizar las pruebas hacia su plataforma web, en la cual existía redireccionamiento de las solicitudes por incompatibilidad con el navegador utilizado por la herramienta de OONI Probe.

CONCLUSIONES Y TRABAJO FUTURO

Conclusiones

A pesar de que los datos obtenidos en las pruebas no generaron resultados concluyentes de existencia de censura, la implementación y funcionamiento exitoso de la red prototipo demuestran la viabilidad y la alta capacidad de escalabilidad para la implementación de la red de monitoreo de censura propuesta a nivel nacional, generando una alternativa viable para transparentar el uso de Internet; y propone, desde la academia, una manera de defender y promulgar los derechos digitales de los internautas del Ecuador.

Trabajo futuro

En primer lugar, la implementación de la red a nivel nacional y la realización permanente de pruebas en pro de transparentar el uso del Internet en el Ecuador supone la verdadera motivación de la realización del proyecto, por lo cual, la realización de trabajos futuros deben estar encaminados a la recolección de resultados durante un periodo mucho mayor, haciendo uso de una cantidad mayor de pruebas que permitan tener resultados más amplios y concluyentes sobre el estado de censura y la protección de los derechos digitales en el país.

Con la intención de optimizar el proceso de recolección de datos y la divulgación de los datos recolectados, sería interesante encontrar una manera de implementar el uso del módulo OONIB, modificándolo de tal forma que permita enviar datos al colector del proyecto OONI y realizar inserciones de los resultados a la base de datos de nuestro servidor central.

REFERENCIAS BIBLIOGRÁFICAS

Akbari, A., & Gabdulhakov, R. (2019). Platform surveillance and resistance in Iran and Russia: The case of Telegram. *Surveillance and Society*, *17*(1–2), 223–231. https://doi.org/10.24908/ss.v17i1/2.12928

ARCOTEL. (2019). Cuentas y Usuarios del Servicio de Acceso a Internet. Recuperado el 27 de septiembre de 2019, de http://www.arcotel.gob.ec/wp-content/uploads/2018/11/3.1.1-Cuentas-internet-fijos-y-moviles_Jul-2019.xlsx

Bauer, M. (2004). Paranoid Penguin—Secure Anonymous FTP with vsftpd. *LINUX®Journal*, *Jul*, *1*.

Burnett, S., & Feamster, N. (2013). Making sense of internet censorship. *ACM SIGCOMM Computer Communication Review*, *43*(3), 84–89. https://doi.org/10.1145/2500098.2500111

Castells, M. (2003). Internet , libertad y sociedad: Una perspectiva analítica. Polis revista de la Universidad Bolivariana. *Http://Journals.Openedition.Org/Polis*, (4). Recuperado de https://journals.openedition.org/polis/7145

Delgado, A. (2014). Nuevas (y viejas) formas de censura de la información en internet. *Cuadernos de periodistas: revista de la Asociación de la Prensa de Madrid*, (29), 110–118. Recuperado de http://www.cuadernosdeperiodistas.com/media/2015/05/110-118-ANTONIO-DELGADO.pdf%5Cnhttp://www.cuadernosdeperiodistas.com/nuevas-y-viejas-formas-de-censura-de-la-informacion-en-internet/

El Universo. (2019, noviembre 13). *Terminó el paro indígena en Ecuador: Nuevo decreto reemplazará al 883*. Recuperado de https://www.eluniverso.com/noticias/2019/10/13/nota/7558853/paro-ecuador-comenzo-dialogo-paz-gobierno-dirigencia-indigena

Evans, C., Ingerson, B., & Ben-Kiki, O. (2001). *YAML Ain't Markup Language*.

Filastò, A. (s/f). Architecture. Recuperado el 22 de noviembre de 2019, de https://ooni.readthedocs.io/en/latest/architecture.html

Filastò, A., & Appelbaum, J. (2012). OONI: Open Observatory of Network Interference. *Free and Open Communications on the Internet*.

Fuertes, J. A. (2012). Los regímenes árabes contra Internet durante la "primavera árabe": los casos de Egipto, Libia y Siria. En *Seguridad y conflictos: una perspectiva multidisciplinar* (pp. 367–404). Instituto Universitario General Gutiérrez Mellado.

INEC. (2017). Tecnologías de la Información y Comunicación. Recuperado el 27 de septiembre de 2019, de https://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/2017/Tics 2017_270718.pdf

Lab Citizen and Others. (2014). *URL testing lists intended for discovering website censorship*. Recuperado de https://github.com/citizenlab/test-lists

NetBlocks. (2019). Internet being restored in Iran after week-long shutdown. Recuperado el 25 de noviembre de 2019, de https://netblocks.org/reports/internet-restored-in-iran-after-protest-shutdown-dAmqddA9

OONI. (s/f-a). OONI - DNS consistency. Recuperado el 24 de septiembre de 2019, de https://ooni.torproject.org/nettest/dns-consistency/

OONI. (s/f-b). OONI - Facebook Messenger test. Recuperado el 24 de septiembre de 2019, de https://ooni.org/nettest/facebook-messenger/

OONI. (s/f-c). OONI - HTTP Header Field Manipulation. Recuperado el 24 de septiembre de 2019, de https://ooni.io/nettest/http-header-field-manipulation/

OONI. (s/f-d). OONI - HTTP Host. Recuperado el 24 de septiembre de 2019, de https://ooni.org/nettest/http-host/

OONI. (s/f-e). OONI - HTTP Invalid Request Line. Recuperado el 24 de septiembre de 2019, de https://ooni.torproject.org/nettest/http-invalid-request-line/

OONI. (s/f-f). OONI - HTTP Requests. Recuperado el 24 de septiembre de 2019, de https://ooni.torproject.org/nettest/http-requests/

OONI. (s/f-g). OONI - Telegram test. Recuperado el 24 de septiembre de 2019, de https://ooni.io/nettest/telegram/

OONI. (s/f-h). OONI - Tor Bridge Reachability. Recuperado el 24 de septiembre de 2019, de https://ooni.io/nettest/tor-bridge-reachability/

OONI. (s/f-i). OONI - Vanilla Tor. Recuperado el 24 de septiembre de 2019, de https://ooni.torproject.org/nettest/vanilla-tor/

OONI. (s/f-j). OONI - Web Connectivity. Recuperado el 24 de septiembre de 2019, de https://ooni.org/nettest/web-connectivity/

OONI. (s/f-k). OONI - WhatsApp test. Recuperado el 24 de septiembre de 2019, de https://ooni.org/nettest/whatsapp/

OONI. (s/f-l). Riesgos: Lo que debes saber antes de ejecutar OONI Probe. Recuperado el 22 de noviembre de 2019, de https://ooni.org/es/about/risks/

OONI. (2013). OONIPROBE Usage Manual. Recuperado el 24 de septiembre de 2019, de GitHub website: https://github.com/ooni/spec/wiki/ooniprobe-Usage-Manual

Ramesh, R., Leonid, E., & Roya, E. (2019). A Deep Dive Into Internet Censorship In Russia. Recuperado el 8 de noviembre de 2019, de https://censoredplanet.org/russia?fbclid=IwAR02hYbsv6ACtP_sxgmaa0RWGcUkz5MbtRvmP9N76dbCjjuENYL9DUQsfIk

Rofrio, D., Ruiz, A., Sosebee, E., Raza, Q., Bashir, A., Crandall, J., & Sandoval, R. (2019). Presidential Elections in Ecuador: Bot Presence in Twitter. *2019 Sixth International Conference on eDemocracy & eGovernment (ICEDEG)*, (2015), 218–223. https://doi.org/10.1109/ICEDEG.2019.8734426

Salcedo, M., & Cendrós, J. (2016). Uso del minicomputador de bajo costo “Raspberry Pi” en

estaciones meteorológicas. *Télématique: Revista Electrónica de Estudios Telemáticos*, *15*(1), 62–84.

Severance, C. (2013). Eben upton: Raspberry Pi. *Computer*, *46*(10), 14–16. https://doi.org/10.1109/MC.2013.349

Xynou, M., Filastò, A., Yusof, K., & Ming, T. S. (2016). OONI - The State of Internet Censorship in Malaysia. Recuperado el 24 de septiembre de 2019, de https://ooni.io/post/malaysia-report/

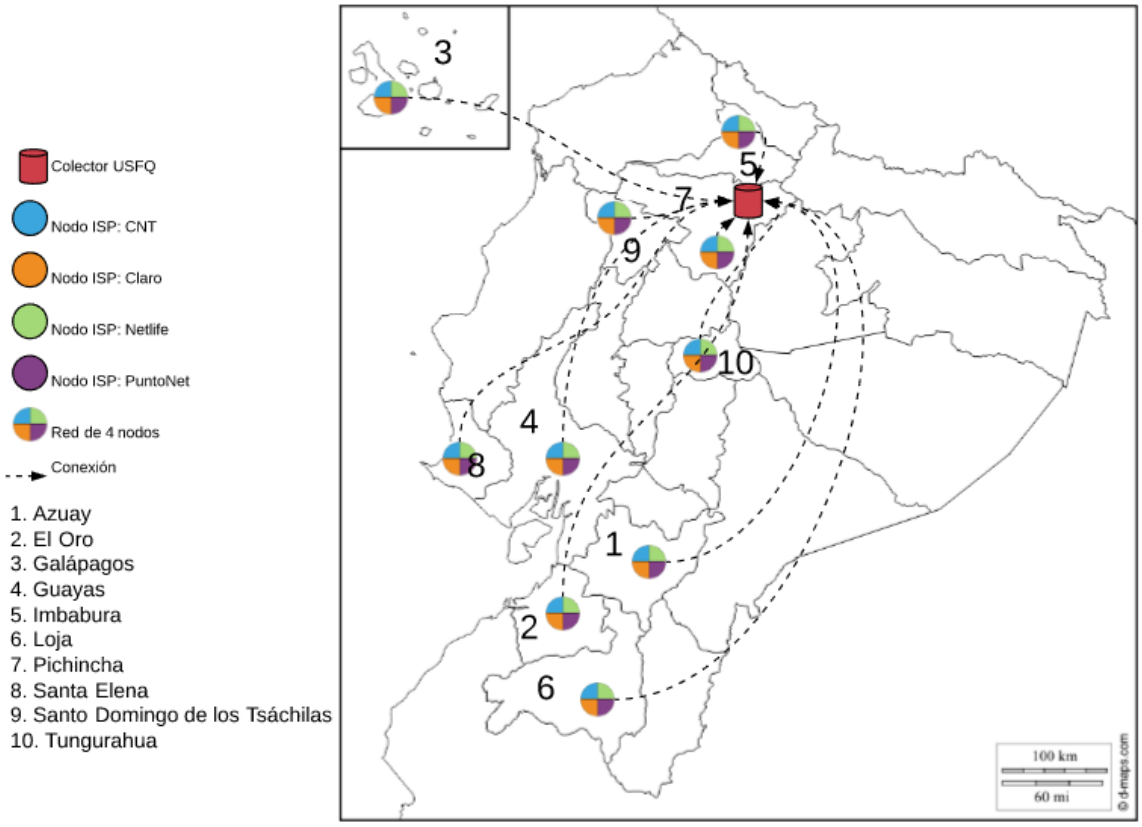
ANEXO A: HARDWARE Y SOFTWARE UTILIZADO

Listado de los dispositivos y software, con su respectiva versión, utilizado para la realización del proyecto:

SOFTWARE / DISPOSITIVO	VERSIÓN / MODELO
Flask	1.1.1
Jinja2	2.10.3
Measurament Kit	n/a
OONI Probe	2.0.0.1
PostgreSQL	11.6
Python (OONI Probe)	2.7.13
Python (Visor web)	3.6.8
Raspberry Pi	3 B+
Raspbian S.O.	4.19.66
Ubuntu Server S.O.	18.04.3 LTS
VSFTPD	3.0.3

ANEXO B: DISTRIBUCIÓN NACIONAL DE LA RED DISEÑADA

Distribución en el mapa del Ecuador del diseño de la red propuesta:



ANEXO C: LISTA DE PÁGINAS

Páginas de interés nacional

URL	DESCRIPCIÓN
http://www.elcomercio.com/	Medios de Comunicación
https://www.eluniverso.com/	Medios de Comunicación
https://ww2.elmercurio.com.ec/	Medios de Comunicación
https://lahora.com.ec/	Medios de Comunicación
http://www.elciudadano.gob.ec/	Medios de Comunicación
https://www.eltelegrafo.com.ec/	Medios de Comunicación
https://www.revistacrisis.com/	Crítica Política
http://www.milhojas.is/	Medios de Comunicación Crítica Política
http://ciespal.org/	Contenido vario
http://revistachasqui.org/	Cultura Medios de comunicación
http://elchuro.org/	Derechos Humanos Medios de Comunicación
https://wambra.ec/	Medios de comunicación
https://www.alainet.org/	Derechos Humanos Medios de Comunicación
http://labarraespaciadora.com/	Derechos Humanos Medios de Comunicación
http://4pelagatos.com/	Cultura Crítica Política
https://www.ecuadortransparente.com/	Medios de Comunicación
https://www.planv.com.ec/	Medios de Comunicación
https://es.wiktionary.org/	Cultura