UNIVERSIDAD DON BOSCO

VICERRECTORÍA DE ESTUDIOS DE POSTGRADO

TRABAJO DE GRADUACIÓN

IMPLEMENTACIÓN DE UN PROTOTIPO DE SISTEMA DE DENUNCIA CIUDADANA UTILIZANDO REDES CIFRADAS BASADO EN LA PLATAFORMA SECUREDROP

PARA OPTAR AL GRADO DE MAESTRO DE:

SEGURIDAD Y GESTIÓN DE RIESGOS INFORMÁTICOS

ASESOR:

MG. FRANCISCO ROBLES

PRESENTADO POR:

ING. RICARDO PÁRRAGA ZALDÍVAR

ING. RONALD GONZÁLEZ RIVERA

Antiguo Cuscatlán, La Libertad, El Salvador, Centroamérica
Agosto 2018

INDICE

LISTADO DE TABLAS

LISTADO DE FIGURAS

INTRODUCCIÓN

La información es poder, la información es dinero, debemos garantizar la integridad, confidencialidad y la disponibilidad de la información que es fundamental para la transparencia y democracia en nuestra sociedad. Esto se ha visto opacado desde hace muchos años por el secretismo, manipulación de información, burocracia en instituciones públicas y privadas, y la tergiversación por parte de medios de comunicación.

Hoy en día contamos con nuevas soluciones tecnológicas accesibles en Internet e Instituciones Gubernamentales que regulan y dan la facilidad a la sociedad para solicitar información de nuestro Gobierno y el trabajo de los funcionarios públicos.

A través de estas tecnologías tenemos acceso a documentación como manuales, normativas, selección y contratación de personal, acceso a los funcionarios por medio de sus correos electrónicos, así mismo poder conocer su perfil académico y laboral como de sus asesores, informes legales, obras que estén en ejecución, estadísticas institucionales, presupuesto institucional, subsidios, recursos públicos, proveedores, licitaciones, remuneraciones, plazas vacantes, inventarios, viajes, estados financieros, contrataciones, adquisiciones, contratistas y rendición de cuentas entre otros.

Existe tecnología para que los ciudadanos puedan tomar un papel protagónico, y con información, sean vigilantes de la transparencia del país, pero esto no sucede de forma anónima y eso crea una barrera provocando el miedo. Debemos proporcionar a los ciudadanos una herramienta tecnológica, con seguridad y confidencialidad que preserve el anonimato para que pueda fluir más información y podamos acabar poco a poco con la corrupción y la polarización en nuestro país.

En los siguientes capítulos veremos la importancia de implementar esta herramienta, que a través de protocolos criptográficos fortalecen la seguridad e integridad en la comunicación de la información, la instalación de esta, y de qué manera se preservará el anonimato, así también como algunas recomendaciones y sugerencias.

En el capítulo 1 veremos cómo PGP[1] puede ayudar en proporcionar seguridad e integridad en las comunicaciones electrónicas cifrando mensajes que se envían por medio de correo electrónico y otros medios convencionales en donde no se provee de seguridad. PGP ha estado desde los inicios de Internet y es una de las herramientas más usadas para proteger las comunicaciones de usuarios que quieren enviar mensajes cifrados en canales públicos.

En el capítulo 2 exploramos el uso de SecureDrop y como este, integrado con PGP puede proporcionar una plataforma para las comunicaciones de manera segura y anónima para que los informantes puedan enviar sus denuncias sin miedo a que estas sean interceptadas. Analizaremos SecureDrop de manera comparativa con otra plataforma de envió de denuncias y veremos sus similitudes y diferencias.

Exploraremos el funcionamiento de la red TOR[2] en el capítulo 3 y como ayuda a que SecureDrop funcione proporcionando transporte en las comunicaciones sobre canales cifrados por medio de nodos en Internet agregando múltiples capas de cifrado de punta a punta.

En el capítulo 4 instalaremos SecureDrop siguiendo paso a paso la guía oficial de instalación y resaltando los aspectos más importantes a tener en cuenta como requisitos de hardware y software, configuraciones especiales, y otros para una instalación exitosa.

Finalizamos en el capítulo 5 con algunas recomendaciones y sugerencias acerca de este tipo de tecnologías y como estas pueden ayudarnos en nuestra sociedad.

---

[1] Pretty Good Privacy (PGP), es un programa desarrollado por Phil Zimmermann y cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.

[2] The Onion Router (TOR), es un proyecto cuyo objetivo principal es el desarrollo de una red de comunicaciones distribuida de baja latencia y superpuesta sobre internet, en la que el encaminamiento de los mensajes intercambiados entre los usuarios no revela su identidad

OBJETIVOS

Objetivo General

Implementar el prototipo de un sistema basado en la arquitectura de SecureDrop para que los periodistas y agencias de noticias puedan recibir información de sus informantes de manera confidencial y anónima; utilizando redes cifradas a través de Internet y de esta manera facilitar la denuncia ciudadana en nuestro país. Información que podría ser utilizada por los periodistas para su posterior investigación.

Objetivos Específicos

- Implementar todos los componentes de la arquitectura de SecureDrop en un ambiente controlado.
- Realizar un análisis documental comparativo entre SecureDrop y otras opciones públicamente disponibles en Internet.
- Realizar un análisis de las implicaciones sociales, éticas y legales del uso de este tipo de herramientas.
- Definir la arquitectura, requerimientos técnicos y los procedimientos necesarios para la implementación y uso de esta plataforma.

ANÁLISIS DEL PROBLEMA

Con el propósito de proporcionar una herramienta tecnológica que sirva a la ciudadanía de apoyo en la lucha contra la corrupción se basara el análisis del problema en tres aspectos fundamentales:

1. Confidencialidad del envío

La denuncia pudiese ser texto, documentos o imágenes. Esta denuncia tiene que estar cifrada con criptografía de llave pública entre el emisor y receptor durante el envío, para evitar manipulaciones por parte de terceros que quisieran alterarla y así mantener la integridad y confidencialidad de esta.

Si el denunciado (persona o entidad pública/privada) quisiera manipular la denuncia conociendo al denunciante para interferir en la misma la herramienta tecnológica debe proveer privacidad al denunciante evitando correlacionar denuncia con denunciante para evitar identificar al mismo.

2. Privacidad del envío

Para evitar que la denuncia sea manipulada en tránsito entre el emisor y receptor es importante cifrar la comunicación. Es necesario utilizar criptografía de llave pública entre el emisor y receptor para resguardar la denuncia, se reforzará la seguridad utilizando canales de comunicación cifrados.

3. Anonimato

Un aspecto fundamental para la denuncia es el anonimato del informante (persona, ciudadano, denunciante). Se debe utilizar algún método como un código o clave por denuncia para identificar la denuncia, pero sin revelar información que pudiese identificar informante.

ANTECEDENTES

En nuestro país existen métodos para la denuncia ciudadana a través de los cuales cualquier ciudadano puede realizar sus denuncias utilizando sistemas telefónicos como, por ejemplo, el de la Policía Nacional Civil y su Sistema 122[3] de denuncias telefónicas, en la cual se recibe información confidencial y de manera anónima sobre cualquier hecho delictivo, además cuentan también con un portal web dedicado a las denuncias ciudadanas[4].

El Tribunal de Ética Gubernamental[5] pone a disposición un formulario de denuncias en su sitio web para la denuncia ciudadana que hay que imprimir y firmar autenticando la firma del denunciante ante un notario para ser presentado en sus oficinas.

La alcaldía de Santa Tecla tiene a disposición "Tecla App", una aplicación para teléfonos móviles en la cual el ciudadano puede realizar sus denuncias directamente desde su teléfono móvil.

Muchas otras entidades públicas tienen diferentes métodos para la denuncia ciudadana similares a los casos anteriores en las cuales se ofrece realizar la denuncia por medios telefónicos, entregando en persona formularios y en línea por medio de sitios web o aplicaciones en teléfonos móviles las cuales no garantizan seguridad, privacidad y confidencialidad al denunciante ya que estos medios guardan en los servidores registro de las comunicaciones con las aplicaciones clientes exponiendo al denunciante.

---

[3] Policía Nacional Civil (2018). Denuncia al Sistema 122. Recuperado de: http://www.pnc.gob.sv/portal/page/portal/informativo/servicios/guia/servicios_al_ciudadano/sistema_122

[4] Crime Stoppers El Salvador (2018). Recuperado de: https://tupista.info

[5] Tribunal de Ética Gubernamental (2018). Denuncias. Recuperado de: http://www.teg.gob.sv/servicios/denuncias

LIMITANTES

El realizar una denuncia contra entidades públicas, privadas o contra cualquier servidor público puede traer consecuencias para el denunciante, al exponerse denunciando el hecho, lo que disminuye la cantidad de denuncias y credibilidad de las entidades que las reciben al desconocerse la manera de procesar la denuncia debido a que si esta afecta a grupos de intereses posiblemente quede en el olvido.

Es de tomar en cuenta también que el denunciar a una persona a través de una plataforma digital, publicar su nombre o su imagen acusándola de algún delito conlleva una responsabilidad civil y/o penal para el denunciante, como lo establece el Código Penal en su Art. 177 y 178.

La falta de acceso a las tecnologías de información, así como la falta de recursos económicos para tener acceso a las mismas, limita a personas de escasos recursos y con poco o nulo conocimiento en las mismas a realizar denuncias utilizando estos nuevos métodos.

En nuestra sociedad la falta de concientización de la población para realizar denuncias se ve afectada debido a la poca transparencia en la administración y resultados de las mismas.

JUSTIFICACIÓN

Durante muchos años los actos de corrupción en nuestro país, que han involucrado a entidades gubernamentales y entes privados han quedado impunes. Negocios ilegales de dichos entes como lavado de dinero, modificación de estados financieros, evasión de impuestos, malversación de fondos, alteración de documentos, extorsiones, trata de personas, hurto, amenazas, tráfico de drogas, posesión ilegal de armas de fuego, acoso y agresiones sexuales, expresiones de violencia contra la mujer, delitos contra menores de edad, estafa, falsedad material, fraude electrónico, suplantación de identidad, producción, posesión y distribución de pornografía infantil, mensajes con amenazas o extorsiones por medio de redes sociales como ciberbullying[6] entre muchos otros; muchas veces no son denunciados por miedo a que la identidad de las víctimas se vuelva pública y esté bajo riesgo, la Fiscalía General de la República no cuenta con suficientes pruebas para tener éxito en muchos de estos casos. En los últimos años, son pocos los casos que se han dado a conocer públicamente llegando a ser detenidos exfuncionarios de gobierno y figuras públicas.

Toda esa información podría obtenerse haciendo uso de la plataforma SecureDrop; lo cual sería de vital importancia para ayudar a las entidades fiscales y judiciales de nuestro país para crear y resolver casos; pero el miedo a no tener un canal seguro y anónimo, la falta de concienciación en la población, y la falta de recursos económicos y tecnológicos con el cuál cualquier persona que tenga acceso a información confidencial que tendría que estar a disposición de la sociedad y de las autoridades de justicia, la pueda revelar sin tener que dar a conocer su identidad.

Actualmente existen entes gubernamentales que fueron pensados para luchar a favor de la transparencia, entre ellos: la Secretaría de Participación Ciudadana, Transparencia y Anticorrupción de la Presidencia de la República, El Instituto de Acceso a la Información Pública, apoyándose con la Ley de Acceso a la Información Pública; pero este esfuerzo no es suficiente todavía, por lo cual la sociedad podría auxiliarse de un sistema electrónico que permita la administración y publicación de

[6] Ciberacoso, en inglés cyberbullying, también denominado acoso virtual o acoso cibernético, es el uso de medios de comunicación digitales para acosar a una persona o grupo de personas

información de forma segura y anónima, cuidando la privacidad del ciudadano que desee denunciar y que dicha información después de un proceso de análisis y revisión por las entidades correspondientes pueda llegar a ser utilizada para lograr la Transparencia necesaria para nuestro país.

CAPITULO 1

MARCO TEÓRICO

1.1 Criptografía de Llave Pública y PGP

1.1.1 Introducción

Pretty Good Privacy que por sus siglas en ingles se conoce como PGP, puede proteger el contenido de mensajes de correo electrónico, textos, y archivos de ser capturados o interceptados en Internet en tránsito a su destino. Cuando Edward Snowden dice "el cifrado funciona[7]", es de PGP y del software relacionado a este, del que está hablando. Desafortunadamente, PGP no es fácil de comprender, o utilizar. El cifrado de alta seguridad que utiliza PGP (cifrado de llave pública) es excelente, pero poco intuitivo.

PGP ha estado con nosotros desde 1991, lo que lo hace tan antiguo como las primeras versiones de Microsoft Windows, y su aspecto no ha cambiado mucho desde entonces. La buena noticia es que actualmente hay muchos programas disponibles que pueden ocultar el antiguo diseño de PGP y hacerlo un poco más fácil de usar, especialmente cuando se trata del cifrado y la autenticación del correo electrónico, que es la finalidad principal de PGP.

Antes de cifrar mensajes con PGP u otros programas que lo utilizan, vale la pena dedicar unos minutos al entendimiento de los conceptos básicos de cifrado de llave pública: lo que puede hacer, lo que no puede hacer, y cuando debería usarlo.

1.1.2 Historia de dos llaves

Cuando usamos cifrado para proporcionar confidencialidad, esto es lo que estamos tratando de hacer:

Tomamos un mensaje claramente legible como "Junta de Directores a las 8:00 pm" y lo ciframos en un mensaje codificado que es incomprensible para cualquiera que busque en él como, por ejemplo: “OesweW5ge+osh1aehah6”. Enviamos el mensaje cifrado a través de Internet, donde puede ser leído por muchas personas, pero no entendiendo el contenido por ninguno de ellos. Cuando

---

[7] TechCrunch (2013-2018). Encrypting Your Email Works, Says NSA Whistleblower Edward Snowden. Recuperado de: https://techcrunch.com/2013/06/17/encrypting-your-email-works-says-nsa-whistleblower-edward-snowden/

llega a su destino, el destinatario, y sólo el destinatario, tiene alguna forma de descifrar el mensaje original.

¿Cómo el destinatario sabe cómo decodificar el mensaje, cuando nadie más puede hacerlo? Es porque conoce algo de información extra que nadie más tiene. Llamaremos a esto la llave de descifrado, ya que desbloquea el mensaje dentro del código cifrado.

¿Cómo puede el destinatario conocer esta llave? Generalmente, es debido a que el emisor le ha comunicado previamente la llave, como ya sea "tomar cada letra y convertirla a la siguiente letra del alfabeto." Hay un problema con esta estrategia, sin embargo. Si le preocupa que su mensaje sea descifrado cuando usted envía su mensaje en llave, ¿cómo enviar al destinatario la llave sin que alguien intercepte esa conversación también? No tiene sentido enviar un mensaje ingeniosamente cifrado si el atacante ya sabe la llave para descifrarlo. Y si usted tiene un método secreto para enviar llaves de descifrado, ¿por qué no utilizarlo para todos sus mensajes secretos?

La criptografía de llave pública tiene una buena solución para esto. Cada persona en una conversación puede crear dos llaves. Una es la llave privada, que mantendrán para sí y nunca deberán permitir que nadie la conozca. La otra es la llave pública, que se entrega a cualquier persona con la que quiera comunicarse. No importa quién pueda ver la llave pública aun cuando la ponga en Internet en donde todo el mundo pueda verla.

Las "llaves" en sí son, en el fondo y en realidad, números muy grandes, con ciertas propiedades matemáticas. La llave pública y la llave privada se conectan. Si se cifra algo usando la llave pública, a continuación, otra persona puede descifrarlo con su llave privada correspondiente.

Veamos como esto podría funcionar en la figura 1. Se quiere enviar un mensaje secreto al destinatario que tiene una llave privada, pero al igual que un buen usuario de cifrado de llave pública, éste ha puesto su llave pública en su página web. Luego se descarga la llave pública, se cifra el mensaje con ella, y se le envía, él puede descifrarlo, porque él tiene la llave privada correspondiente, pero nadie más puede.

El cifrado de llave pública se deshace del problema del robo de la llave de descifrado de la persona a la que desea enviar un mensaje porque esa persona ya tiene la llave. Usted sólo debe tener la llave de cifrado pública correspondiente, que el destinatario ha repartido a todos/as en Internet, ya que es sólo útil para codificar un mensaje mientras es inútil para cualquier persona que intente descifrar el mismo mensaje.

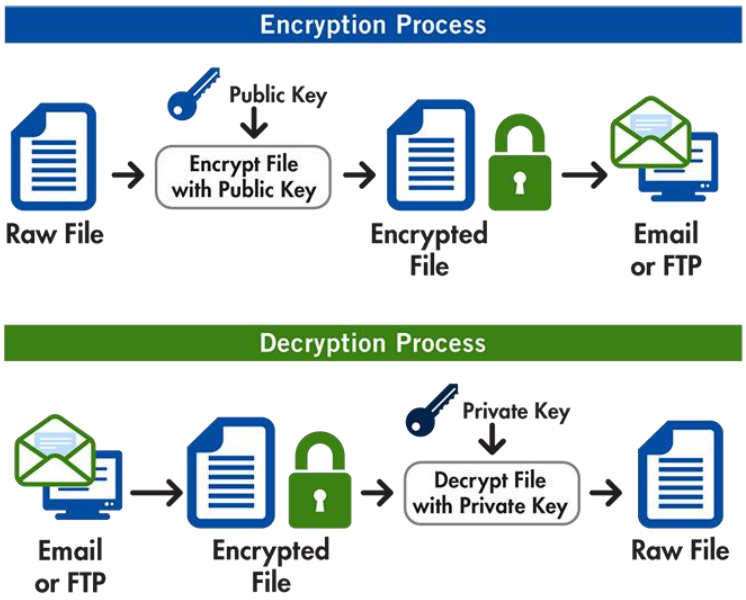

Figura 1: Criptografía de llaves públicas y privadas con PGP[8].

Pero, si se cifra un mensaje con una cierta llave pública, sólo puede ser descifrada por la llave privada correspondiente.

1.1.3 Métodos de Autenticación al usar PGP

¿Por qué sería útil utilizar PGP si todos los usuarios en Internet pueden ver la llave publica? A primera vista, no parece haber ninguna ventaja en crear un mensaje secreto con una llave privada que todo el mundo (o al menos, todo el que tiene la llave pública) puede descifrarlo. Pero se supone que al escribir un mensaje como: "Me comprometo a pagar $100" y luego se vuelve un mensaje secreto usando la llave privada. Cualquiera podía descifrar ese mensaje, pero sólo una persona podría

[8] GoAnywhere MFT (2018). OpenPGP Encryption Technology. Recuperado de: https://www.goanywhere.com/managed-file-transfer/encryption/open-pgp

haberlo escrito: la persona que tiene la llave privada. Si se ha hecho un buen trabajo manteniendo segura la llave privada, es decir, que solo un usuario la tenga, mediante el cifrado con la llave privada, se ha asegurado de que sólo podría haber venido de un remitente. En otras palabras, se ha hecho lo mismo con este mensaje digital como lo hacemos cuando firmamos un mensaje en el mundo real.

Firmar también hace que los mensajes sean a prueba de manipulaciones proporcionando integridad. Si alguien trata de cambiar "Me comprometo a pagar $100" por "Me comprometo a pagar a Juan $100", no sería capaz de volver a firmarlo utilizando la misma llave privada. Así que un mensaje firmado garantiza que procede de una fuente determinada, y no puede ser alterado en tránsito.

La criptografía de llave pública permite cifrar y enviar mensajes de forma segura a cualquier persona cuya llave pública se conoce. Si los demás conocen la llave pública, pueden enviar mensajes, que sólo el destinatario puede descifrar. Y si la gente conoce la llave pública, puede firmar los mensajes para que esas personas sepan que son del remitente realmente. Y si conoce la llave pública de otras personas, puede descifrar un mensaje firmado por ellos, y saber que sólo vino de ellos.

La criptografía de llave pública se vuelve más útil entre más personas conocen la llave pública. También debe ser evidente que se necesita mantener la llave privada muy segura. Si alguien recibe una copia de una llave privada, puede suplantar la identidad y firmar mensajes que simulen ser escritos por el remitente. PGP tiene una característica que permite "revocar" una llave privada, y advertir a la gente que ya no es confiable, pero no es una gran solución. La parte más importante del uso de un sistema de criptografía de llave pública es proteger la llave privada con mucho cuidado.

1.1.4 Funcionamiento de PGP

Pretty Good Privacy o PGP se ocupa principalmente de los pequeños detalles de creación y uso de llaves públicas y privadas. Puede crear un par de llaves pública/privada, proteger la llave privada con una contraseña y utilizarla junto a la llave pública para firmar y cifrar texto. También permitirá descargar las llaves públicas de otras personas y subir sus llaves públicas a "servidores de llaves públicas", que son los repositorios donde otras personas puedan encontrar la llave.

Si hay una cosa que hay que sacar de este panorama general es: se debe mantener la llave privada almacenada en un lugar seguro y protegido con una contraseña larga. Se puede compartir la llave pública a cualquier persona que desee comunicarse con el remitente, o que quiera confirmar si un mensaje realmente vino del remitente.

1.1.5 PGP Avanzado: La red de confianza

Es posible que se haya descubierto un defecto potencial en cómo funciona el cifrado de llave pública. Supongamos que se comienza a distribuir una llave pública que se dice pertenece a alguien más. Si la gente lo cree, podrían empezar a enviar mensajes secretos al remitente, cifradas con la llave. O se podría creer que nada firmado con esa llave es una declaración jurada del remitente. Esto es verdaderamente raro, y sin embargo actualmente les sucede a algunas personas en la vida real. No se sabe con seguridad si en realidad algunas de las personas que han hecho las llaves falsas realmente estaban capacitadas para interceptar los mensajes en tránsito y leer los mismos, o si esto es meramente un truco para hacer más difícil a las personas tener una conversación segura.

Otro atentado furtivo es que un atacante se ubique entre dos personas hablando en línea, espiando toda la conversación y ocasionalmente insertando mensajes engañosos en la conversación. Gracias al diseño de la Internet como un sistema que transporta los mensajes en varios equipos diferentes y particulares, este ataque es totalmente posible. En estas condiciones (llamados un ataque "Man In The Middle”), el intercambio de llaves sin acuerdo previo puede ser muy arriesgado. "Aquí está mi llave", anuncia una persona que suena como el remitente, y le envía un archivo de llave pública. ¿Pero quién dice que alguien no esperó hasta ese momento, interceptar la transmisión de la llave del remitente, y luego insertar su propia llave?

¿Cómo podemos demostrar que una determinada llave pertenece realmente a una persona determinada? Una forma es obtener la llave de ellos directamente, pero eso no es mucho mejor que obtener una llave secreta sin que alguien lo detecte. Aun así, la gente hace el intercambio de llaves públicas cuando se encuentran, en privado y en reuniones públicas.

PGP tiene una solución ligeramente mejor llamada la "red de confianza." En la red de confianza, si cree que una llave pertenece a una determinada persona, se puede firmar, y luego subir la llave (y la firma) a los servidores de llaves públicas. Estos servidores de llaves pasarán las llaves firmadas a cualquiera que pregunte por ellas.

En términos generales, cuantas más personas en quien se confía hayan firmado una llave, es más probable que se va a creer que la llave pertenece realmente a quien se dice que es. PGP permite firmar llaves de otras personas y también nos permite confiar en otros firmantes, de modo que, si ellos firman una llave, su software cree automáticamente que la llave es válida.

La web de confianza viene con sus propios retos, y organizaciones como EFF (Electronic Frontier Foundation) están investigando mejores soluciones. Pero por ahora, si se quiere una alternativa a entregar las llaves a otros en persona, usando la red de confianza y la red pública de los servidores de llaves es la mejor opción.

1.1.6 Lo que PGP no puede hacer

PGP trata de hacer que el contenido de un mensaje sea secreto, genuino e inalterable. Pero ese no es el único problema de privacidad que se puede tener. Como se ha señalado, la información acerca de los mensajes puede ser tan reveladora como su contenido. Si se está intercambiando mensajes PGP con un disidente conocido en un país, se puede estar en peligro por el simple hecho de comunicarte con él, aun sin decodificar dichos mensajes. De hecho, en algunos países puedes ser encarcelado simplemente por negarse a descifrar los mensajes cifrados.

PGP no hace nada para ocultar con quien se está hablando o que se está utilizando PGP para hacerlo. De hecho, si se sube una llave pública a los servidores de llaves o firmas las llaves de otras personas se está demostrando efectivamente al mundo que la llave es de esa persona y a quien se conoce.

No se tiene que hacer eso, se puede mantener la llave pública PGP discretamente y sólo darle a la gente con quien se siente seguro y pedirles que no lo suban a los servidores de llaves públicas. No es necesario atar un nombre a una llave.

Disfrazar que se está comunicando con una persona en particular es más difícil. Una forma de hacer esto es que ambos usuarios utilicen cuentas de correo electrónico anónimas, y acceder a ellas usando TOR. Si se hace esto, PGP seguirá siendo útil, tanto para mantener los mensajes de correo electrónico privados de otras personas, y demostrar a la otra persona que los mensajes no han sido alterados.

1.2 TOR (The Onion Router)

1.2.1 Historia de la red TOR

La red TOR abreviatura en ingles de The Onion Router, nace como un grupo de servidores que permite mejorar la privacidad y seguridad en Internet. En 1995 comienza el proyecto financiado por ONR (Oficina de Investigación Naval). En 1996 se analiza utilizar claves con el protocolo Diffie-Hellman. Se implementa un prototipo de PoC (Prueba de Concepto) en el sistema operativo Solaris 2.5.1. El documento inicial explica características que no se implementarán hasta la generación 2. El año 1997 además del financiamiento de ONR, el proyecto TOR es financiado por DARPA (Agencia de Proyectos de Investigación Avanzados de Defensa) bajo el programa de Redes de Alta Confianza.

En el año 2002 se anuncia una versión alfa del software libre con la red The Onion Routing en funcionamiento. Se creó en el 2003 como evolución del proyecto Onion Routing financiado por el Laboratorio de Investigación Naval de Estados Unidos, siendo la segunda versión de la red Onion Routing. La Electronic Frontier Foundation se convierte en patrocinador del proyecto a finales del año 2004. En la actualidad el proyecto TOR está en manos de The TOR Project, organización sin fines de lucro.

El objetivo principal de TOR es el desarrollo de comunicaciones distribuida de baja latencia y superpuesta sobre internet, sin revelar la identidad entre los usuarios durante el enrutamiento de intercambio de mensajes por medio de las direcciones IP.

En la red TOR por un lado se encuentran los usuarios de la red y por otro los enrutadores de tráfico, por lo cual no es una red entre iguales (peer to peer). Esconde el origen y el destino del tráfico que se genera sin mostrar la dirección IP manteniendo la integridad de la información.

Antes era complicado conectarse a la red TOR para usuarios sin mucha experiencia o conocimiento por la necesidad de instalar diversas aplicaciones que funcionaran como proxy, permitiendo el acceso a la red. Actualmente es más sencillo conectarse en esta red, The TOR Project lanzó el navegador web TOR Browser, el cual está listo para funcionar sin necesidad de ninguna configuración adicional que complique al usuario.

1.2.2 Funcionamiento de la red TOR

La red TOR permite enviar por medio de varios nodos intermedios los paquetes de información calculando primero una ruta pseudo-aleatoria hacia el punto de destino.

Los paquetes de información enviados se cifran progresivamente por cada capa, se cifra el mensaje, el destino y la ruta, y por cada nodo se envuelve este paquete con una nueva capa de cifrado por medio de las llaves públicas de cada nodo, en el último nodo, se descifra totalmente el paquete para enviarlo a su destino

Para el funcionamiento de la red TOR se necesitan los siguientes elementos: entidades, servicio de directorio, esquema básico, puntos de encuentro, servicios ocultos, células, claves de OR, algoritmo de cifrado.

1.2.3 Entidades Red TOR

Formado por una serie de nodos comunicándose mediante el protocolo TLS sobre TCP/IP para mantener secreta e íntegra la información de nodo a nodo. Existen dos tipos de entidades:

- Nodos OR (Onion Router): Son enrutadores y también pueden funcionar como servicio de directorio, estos mantienen conexión TLS con otros OR.
- Nodos OP (Onion Proxy): Obtienen información del servicio de directorio, establecen servicios aleatorios a través de la red y manejan conexiones de aplicaciones del usuario.

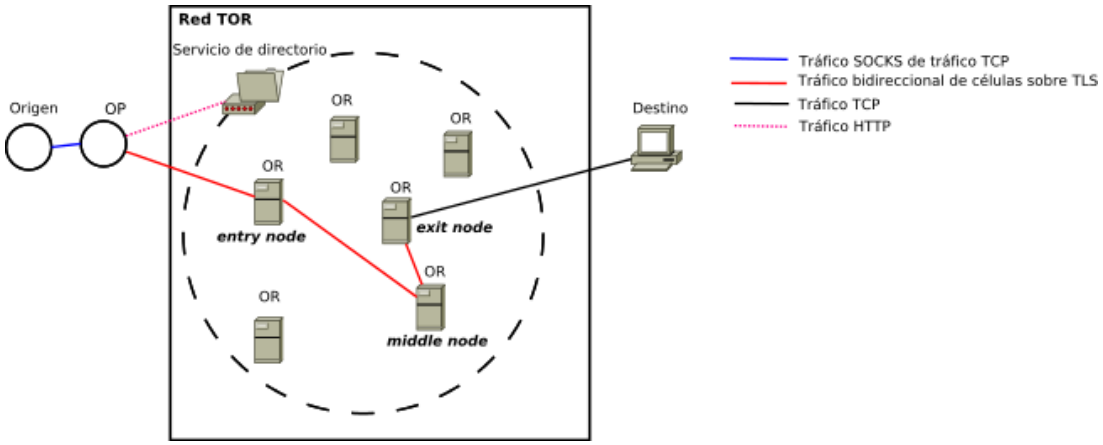

Figura 2. Entidades de la Red TOR[9].

En la figura 2 se muestran los nodos OR que enrutan el tráfico de las conexiones y aplicaciones del usuario u Origen y el nodo OP el cual su función es obtener información del servicio de directorio, establecer circuitos aleatorios a través de la red y manejar conexiones de aplicaciones del usuario.

1.2.4 Servicio de Directorio

Publica una base de datos que asocia a cada OR a información accesible a todos los OR y usuarios finales. Los OR que se usan como servicio de directorio mantienen duplicada su información enviándola de unos a otros para crear los respaldos. Por motivos de respaldo y de latencia los OR que dan el servicio de directorio mantienen duplicada la información pasándosela de unos a otros. Los servicios de directorios son un grupo de OR confiables.

---

[9] Wikipedia, la enciclopedia libre (2018). TOR (red de anonimato). Recuperado de: https://es.wikipedia.org/wiki/TOR_(red_de_anonimato)

Las entradas del servicio de directorio son protegidas criptográficamente con firmas, solo información de OR aprobados será publicada. Los nuevos OR tienen que ser aprobados para evitar ataques por otros nodos no confiables.

1.2.5 Esquema Básico

Con información obtenida de su configuración y servicio de directorio el OP elige un circuito donde van a circular los paquetes, el cual por defecto tiene 3 nodos como se muestra en la figura 3. OP negocia las claves de cifrado en cada OR del circuito antes de realizar transmisión alguna. Se obtienen las claves simétricas (AES-128) en cada sentido (Kf ← forward key, Kb ← backward key) con el protocolo Diffie-Hellman para obtener la clave compartida y generar las dos claves simétricas. El circuito es construido desde el punto de entrada así: Los mensajes para negociar las claves de la comunicación entre ORn y ORn+1 se realizan a petición del OP y retransmitiendo paquetes a través de los nodos OR1, … ORn. En cada paso los mensajes son cifrados con las claves de sesión negociadas, o cuando no lo están, con la clave pública del host que recibe el dato.

- Se cifra el paquete que contiene la clave para el último OR del circuito.
- Se cifra el paquete que contiene la clave para el penúltimo OR del circuito.
- Lo mismo con todos los nodos hasta hacer lo propio con el paquete para el primer nodo.
- Se envía el paquete resultante al primer nodo del circuito. Este paquete se puede considerar envuelto en varias capas de cifrado, es por eso la metáfora de la cebolla para describir este método de enrutamiento.
- El primer OR quita su capa enviando el paquete al siguiente nodo.
- Según llega el paquete a cada OR este remueve la capa externa. Ningún OR puede hacerse con la imagen completa del circuito, solo conoce el OR/OP anterior y posterior.

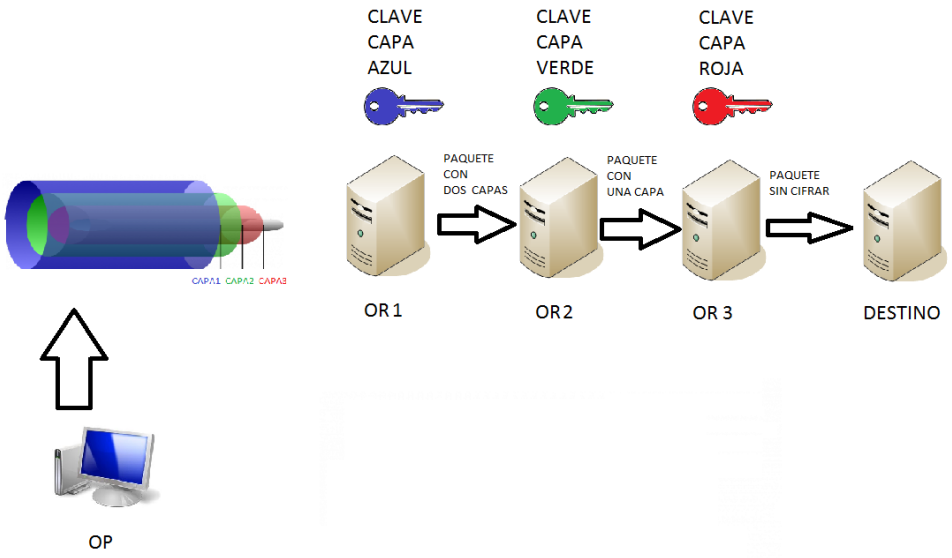

Figura 3. Esquema básico descifrado de capas por cada OR[10]

Se llama “exit server” o “exit node” al último servidor del circuito, el primer OR se llama “entry node”, los demás nodos se llaman “middle-node” como se muestra en la figura 4. Además, al estar el cifrado de las capas basado en claves de sesión, aunque un atacante recopilara todos los mensajes no podría descifrarlos una vez que estas claves de sesión son descartadas por el OR.

[10] Bytelearning (2015-2018). TOR: The Onion Router. Recuperado de: https://bytelearning.blogspot.com/2015/01/tor-onion-router.html

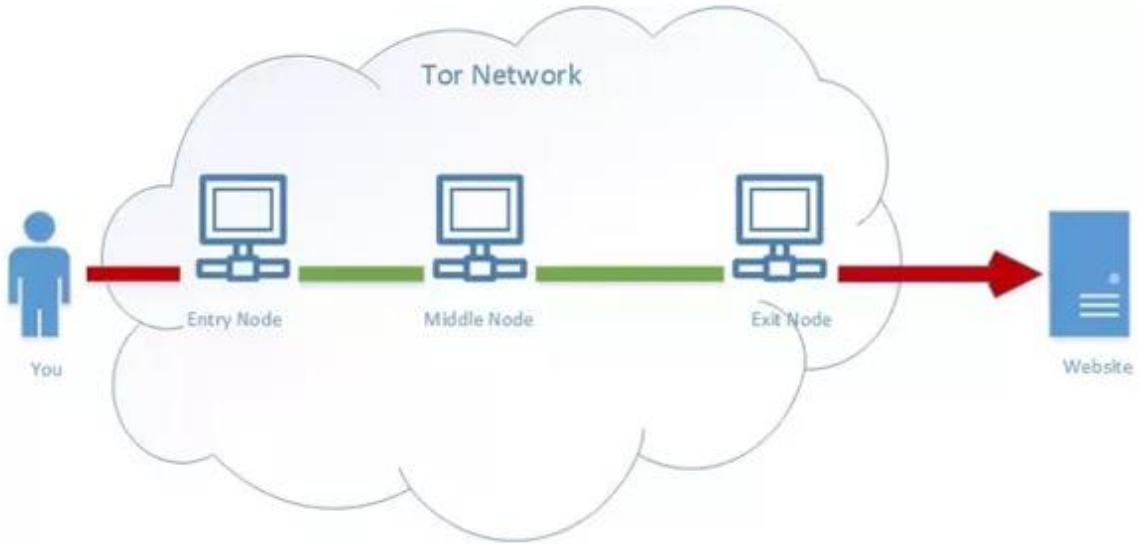

Figura 4. Entry Node, Middle Node, Exit Node[11].

1.2.6 Puntos de encuentro

Denominados por las sigas RP (Rendezvous Points), en lugar de enviar un paquete a un destino, establece un punto de encuentro que actúe como nivel de dirección. Los extremos de comunicación envían sus mensajes a este punto de encuentro y luego son enviados donde corresponda por medio de los circuitos escondiendo la localización de destino.

1.2.7 Servicios Ocultos

Ocultan la localización (dirección IP) de quien provee el servicio. (Un servicio web solo accesible desde la red de enrutamiento). Los proveedores de servicio generan una clave pública y privada para identificar su servicio, anuncian su servicio a distintos enrutadores haciendo peticiones firmadas con su clave pública que servirá como punto de contacto.

El proveedor de servicio asocia a su servicio una FQDN del pseudo-TLD.onion y la publica en un servidor de directorio. La FQDN tiene la forma <valorhash>.onion donde el valor hash es de 16 caracteres en Base32 y está generado usando una función hash sobre la clave pública del servicio.

---

[11] Quora (2017-2018). TOR Network. Recuperado de: https://www.quora.com/Is-it-true-that-the-government-has-control-of-TORs-servers-and-that-we-are-as-vulnerable-on-TOR-as-we-are-on-Chrome-Safari-or-Explorer

Un cliente se quiere conectar a cierta FQDN consulta un servicio de búsqueda (lookup service) y este le indica un punto de introducción (introduction point) y la clave pública del servicio. Para mantener el anonimato es necesario que la consulta del servicio de búsqueda se realice a través de TOR. El cliente se conecta con un punto de encuentro y se establece un identificador de esa conexión (rendezvous cookie).

1.2.8 Células

Establecida la conexión TLS, por OP-OR u OR-OR las entidades se envían paquetes de información estructurada llamadas células, las cuales tienen tamaño fijo de 512 bytes. Formadas por cabecera y una carga útil en este formato:

- **CircID**: Identificador del circuito y especifica el circuito al que se refiere la célula.
- **CMD**: Comando que especifica el significado de la célula, existiendo 2 tipos: Células de control y Células de transmisión.

1.2.8.1 Células de control

Siempre son interpretadas por el nodo que las recibe y permite controlar la comunicación. Los comandos de estas células son:

- PADDING: Actualmente no usadas porque los ataques existentes funcionan incluso con tráfico de relleno y porque el tráfico que provocan incrementa el ancho de banda necesario
- CREATE: Crear circuito
- CREATED: ACK de CREATE
- DESTROY: Destruir circuito.
- CREATE_FAST: Crear circuito reaprovechando operaciones de claves públicas existentes.
- CREATED_FAST: ACK de CREATE_FAST
- VERSIONS: Cuando se establecen las conexiones.
- NETINFO: Cuando se establecen las conexiones.

1.2.8.2 Células de Transmisión

Usadas para la comunicación entre el OP y cualquier OR del circuito, normalmente el exit node. Estas células se distinguen porque el valor del campo CMD siempre tiene el comando RELAY.

El formato tiene campos que forman parte de la carga útil (PAYLOAD):

Relay Comand: este subcomando indica el funcionamiento de la celda. Hay tres tipos de subcomandos Relay:

1. Forward: Enviados desde el OP origen del circuito.
2. Backward: Enviados desde el OR del circuito al OP origen.
3. Ambos: Funcionan como Forward y Backward.

Posibles subcomandos:

RELAY_BEGIN: Tipo forward.

RELAY_DATA: Tipo forward o backward.

RELAY_END: Tipo forward o backward. Permite indicar cierre de un stream TCP.

RELAY_CONNECTED: Tipo backward.

RELAY_SENDME: Tipo forward o backward. A veces se usa para funciones de control.

RELAY_EXTEND: Tipo forward. Se usa para funciones de control.

RELAY_EXTENDED: Tipo backward. Se usa para funciones de control.

RELAY_TRUNCATE: Tipo forward. Se usa para funciones de control.

RELAY_TRUNCATED: Tipo backward. Se usa para funciones de control.

RELAY_DROP: Tipo forward o backward. Se usa para funciones de control.

RELAY_RESOLVE: Tipo forward.

RELAY_RESOLVED: Tipo backward.

RELAY_BEGIN_DIR: Tipo forward.

Recognized: Junto con el campo digest permite identificar si la celda es para ser procesada localmente.

StreamID: Identificador de flujo, permite que varios flujos puedan ser multiplexados en un solo circuito además de identificar el stream al que nos referimos en múltiples streams del círculo.

Digest: Permite control de integridad de extremo a extremo. Contiene los primeros cuatro bytes de ejecutar SHA-1 sobre TODOS los bytes de células relay que han sido enviados a este nodo del circuito u originados desde este nodo del circuito usando las semillas Df o Db respectivamente e incluyendo la carga útil entera de esta célula RELAY cogiendo el campo digest a zero

Length: Indica el número de bytes del campo DATA que contiene carga útil real. El resto del campo irá rellenado por bytes a NUL.

Una célula se considera completamente descifrada si el campo Recognized está a ceros y el campo Digest es el primero de los 4 bytes resultado de ejecutar la función de digest de todos los bytes 'destinados a' o 'originados desde' este salto del circuito. Si una celda no está completamente descifrada se pasa al siguiente salto del circuito. Si la célula se ha comprobado que está completamente descifrada pero el comando de la célula no se entiende la célula será borrada e ignorada pero su contenido todavía cuenta respecto a los digests.

El contenido completo de la cabecera y de la carga útil es cifrado usando la clave AES-128 negociada en el establecimiento de circuito y haciendo un cifrado AES-128_en counter mode (AES-CTR).

1.2.9 Claves de OR

Cada OR tiene asociados una serie de pares de claves pública/privada:

Identity Key: Solo sirve para firmar información, certificados y es usado para permitir identificación. Para denotar la clave de identidad del nodo OR n usamos PKORn_ID.

Onion Key: Cifra las peticiones de establecimiento de circuito CREATE para negociar las claves efímeras. Para denotar la onion key del nodo OR n usamos PKORn_OK.

Key Connection: Usada en el handshake TLS, se mete en un certificado que se firma con la clave de identificación. Ambos certificados (certificado de la clave de conexión y certificado de la clave de identificación) se envían en el handshake del TLS.

1.2.10 Algoritmos de cifrado de la red TOR

Para establecer las conexiones TLS usa TLS/SSLv3. Todos los OR y OP tienen que soportar SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA y deberían tener disponible TLS_DHE_RSA_WITH_AES_128_CBC_SHA. Los OP para comunicarse con los OR pueden usar: TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA

Como algoritmo simétrico de cifrado se usa AES en counter mode (AES-CTR) con claves de 128 bits, con vector de inicialización con todos los bytes a 0.

Como algoritmo de clave pública usa RSA con claves de 1024 bytes y exponente fijo 65537. Usa como esquema de relleno OAEP-MGF1 con SHA-1 usado como función resumen.

Para establecimiento de claves usa DH (Diffie-Hellman) con g=2 y para p usamos el primo seguro de 1024 bits obtenido de RFC 2409 con valor hexadecimal:

FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E08
8A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B
302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9
A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE6
49286651ECE65381FFFFFFFFFFFFFFFF

1.3 SecureDrop

1.3.1 Reseña histórica de SecureDrop

SecureDrop es una plataforma de software de código abierto para la comunicación segura entre periodistas y fuentes de información. Originalmente fue diseñado y desarrollado por Aaron Swartz y Kevin Poulsen bajo el nombre DeadDrop.

Tras la muerte de Aaron Swartz, The New Yorker lanzó la primera versión de la plataforma el 15 de mayo de 2013 bajo el nombre de Strongbox. Posteriormente, la Freedom of the Press Foundation se hizo cargo del desarrollo de DeadDrop, bajo el nombre SecureDrop, y una versión adicional de la plataforma fue lanzada por la revista Forbes en octubre de 2013, bajo el nombre SafeSource.

1.3.2 Funcionamiento de SecureDrop

SecureDrop utiliza la red de anonimato TOR para facilitar la comunicación entre las fuentes de información, periodistas y organizaciones de noticias. Los sitios SecureDrop, por lo tanto, sólo son accesibles como servicios ocultos en la red TOR. Después de que un usuario visite un sitio web SecureDrop, se le asigna un nombre en clave generado aleatoriamente. Este nombre en clave se utiliza para enviar información a un determinado autor o editor a través de un servidor. Los periodistas de investigación pueden ponerse en contacto con la fuente de información a través del servicio de mensajería SecureDrop. Por lo tanto, el denunciante debe tomar nota de su código aleatorio.

El sistema utiliza servidores privados segregados que pertenecen a la organización de noticias. Los periodistas usan dos Memorias USB y dos ordenadores portátiles para acceder a los datos SecureDrop. El primer ordenador portátil accede a SecureDrop a través de la red TOR, el periodista utiliza la primera memoria para descargar los datos cifrados a través de Internet. El segundo ordenador portátil no se conecta a Internet, y es borrado durante cada reinicio del sistema. La segunda memoria USB contiene un código de descifrado. La primera y segunda memorias se insertan en el segundo ordenador portátil, y el material queda a disposición del periodista. El portátil se apaga después de cada uso.

La organización de noticias no registra ninguna información con respecto a la dirección del denunciante, es decir, ni la dirección IP, ni información sobre el equipo físico utilizado. El navegador no permite instalar cookies ni la incrustación de software de terceras partes. El anonimato no está garantizado, pero los creadores afirman que el sistema es más seguro que el correo electrónico[12].

[12] Periodismo.com (2017-2018). Los nuevos modos anónimos y seguros para que los lectores contacten a los medios. Recuperado de: https://www.periodismo.com/2017/01/20/los-nuevos-modos-anonimos-y-seguros-para-que-los-lectores-contacten-a-los-medios/

1.3.3 Casos de uso de SecureDrop

Con el fin de comprender el impacto en las agencias de noticias, analizaremos dos casos de uso que exitosamente han implementado y hacen uso de la plataforma SecureDrop.

1.3.3.1 The Washington Post

Para Barton Gellman, uno de los reporteros que investigó el caso de Edward Snowden y sus divulgaciones en The Washington Post, aprender a utilizar herramientas de cifrado solo probaron ser útil luego de esperar. "Publique mi primera llave PGP en el 2006", dijo Gellman. "Estaba utilizando herramientas de cifrado y TOR por siete años antes que Edward Snowden encontrara su camino a mi buzón de correo. Él no hubiera podido contactarme si no hubiera dejado afuera la alfombra de bienvenida". Gellman ahora administra su propia plataforma personal de SecureDrop en la Century Foundation, pero The Washington Post fue también uno de los primeros en implementarla, lanzando la plataforma en junio del 2014.

The Washington Post parece haber desarrollado un sistema eficiente para monitorear su plataforma SecureDrop. De acuerdo con Steven Rich, editor de investigaciones en The Washington Post, tienen un equipo de trabajo de tres periodistas que recaban, acceden, y distribuyen buenas prácticas a reporteros de noticias. Trevor Timm de Freedom of Press Foundation concuerda que The Washington Post tiene la "más coordinada" plataforma de SecureDrop entre todas las organizaciones que la utilizan.

"Invertimos una buena cantidad de tiempo tratando de averiguar que era y que debíamos de hacer", dijo Julie Tate, uno de los periodistas que monitorea SecureDrop en The Washington Post. Después de recibir piezas de información, Julie Tate y otros puntos de contacto responden a los informantes por medio de SecureDrop para hacerles saber que un reportero se encuentra investigando la información recibida. También dan expectativa al informante que tanto los estarán contactando si la información provista sigue en investigación.

"Si pongo en contacto a un reportero con el informante, usualmente ya no me involucro nuevamente. Un ciento por ciento de las veces ya no me involucro" dice Julie Tate. "Es más como, esto es lo que recibimos, esta persona se pondrá en contacto con el informante, ¿sabes a lo que me refiero? es como presentar a dos personas, y luego salirse de la conversación. Solo estoy facilitando la comunicación entre dos personas."

Cuando nos preguntan si SecureDrop ha sido exitoso en The Washington Post, Julie Tate responde, "Definitivamente, no puedo decir en que historias lo ha sido, pero hemos tenido éxito con la plataforma de SecureDrop, definitivamente".

Steven Rich dice que tienden a recibir piezas interesantes de información cada semana o dos en una etapa de pre-investigación antes de lanzar una investigación completa. "Uno no obtiene historias completas" dice Steven Rich. "Uno obtiene solo la punta del iceberg".

Steven Rich también dice que mucha gente en la agencia de noticias de The Washington Post están sabedores de la plataforma de SecureDrop, pero que la mayoría no lo utiliza. También dice que muchos reporteros piensan que no lo necesitan. "Mucha gente trabaja con más material sensible de lo que piensan" explica Steven Rich.

A pesar de que la mayoría de la agencia de noticias no utiliza la plataforma de SecureDrop, otros utilizan herramientas de cifrado como PGP. De acuerdo con Julie Tate, todos los reporteros internacionales de The Washington Post utilizan herramientas de cifrado de algún tipo. Información de los servidores de llaves de MIT revelan que la creación de llaves de reporteros de The Washington Post incrementó notablemente luego de que la información de Edward Snowden fue publicada, mientras que la instalación de SecureDrop tuvo poco efecto como se muestra en la figura 5.

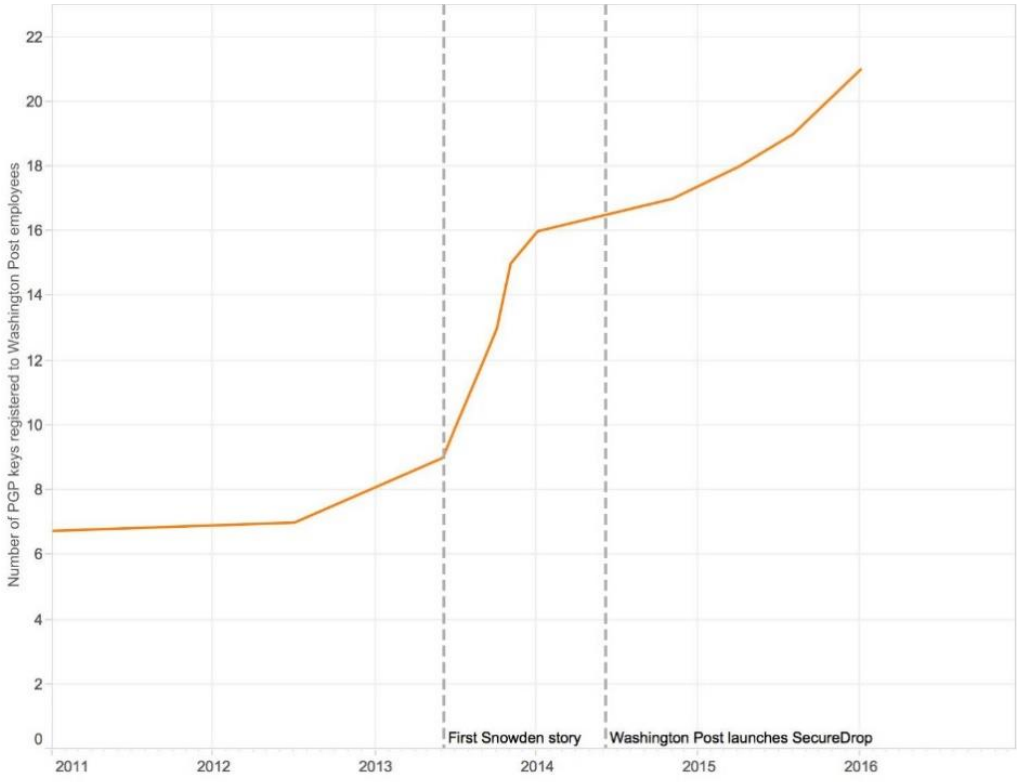

Figura 5: Numero de llaves publicas registradas por The Washington Post[13].

[13] The Washington Post (2018). Guide to SecureDrop. Recuperado de: https://towcenter.gitbooks.io/guide-to-securedrop/content/case_studies_news_organizations/the_washington_post.html

1.3.3.2 The Globe and Mail

En marzo del 2015, The Globe and Mail de TORonto instalo por primera vez SecureDrop en Canadá. En un artículo publicado anunciando el lanzamiento, el editor en jefe de The Globe and Mail, David Walmsley escribió, "SecureDrop es el equivalente al sobre de manila: Le proporciona un lugar anónimo para retransmitir material que crea que es de interés público y no tiene otra forma de divulgarlo públicamente.[14]"

El subdirector de producción Alasdair McKie, quien es el principal facilitador de SecureDrop para The Globe and Mail, dijo que el sistema rápidamente demostró ser útil, recibiendo información de un informante inmediatamente después de su lanzamiento. El uso de la plataforma de SecureDrop de The Globe and Mail está ligada al equipo investigativo. Un grupo de reporteros han sido capacitados en el uso de la plataforma SecureDrop y lo revisan por lo menos tres veces por semana en busca de algún material prometedor.

La cuenta de mensajes recibidos de Alasdair McKie en SecureDrop también sugiere que The Globe and Mail está más despreocupado por el spam que otras organizaciones de noticias. "La mayoría de información recibida, las llamaría noticias de informantes potenciales," y continúa diciendo:

Los informantes no están desperdiciando nuestro tiempo intencionalmente. No están enviándonos material que no es de valor periodístico. No están enviándonos basura con el propósito de llenarnos de contenido. Eso no es común y suele pasar. Pero no es algo que representa un problema para nosotros.

Como muchos otros medios informativos que utilizan SecureDrop, Alasdair McKie declino recalcar casos específicos en el cual documentos de SecureDrop terminaron publicados. Además, él dice que en The Globe and Mail establecieron una política explicita antes de lanzar SecureDrop, en

---

[14] The Globe and Mail (2015-2018). The Globe adopts encrypted technology in effort to protect whistle-blowers. Recuperado de: https://www.theglobeandmail.com/news/investigations/the-globe-adopts-encrypted-technology-in-effort-to-protect-whistle-blowers/article23302598/

el cual detalla que su organización, en ninguna circunstancia, revelaría la fuente de información que provenga por este medio.

Más que una herramienta de recibir información, Alasdair McKie recalco que tener SecureDrop refleja conciencia en nuestra sociedad sobre el presente dilema de vigilancia y respeto por el rol de la prensa en recalcar esa realidad:

El hecho que la gente que está dispuesta a contactarnos por medio de SecureDrop, que no están dispuestos a contactarnos por otro medio, subraya la importancia no solo de los líderes de la editorial, pero de la compañía en general, que la seguridad de la información es un hecho en la vida real. Y otras iniciativas, como que las personas utilicen llaves PGP es algo que será parte de nuestras vidas. Entre más rápido incorporemos eso en nuestra manera de hacer negocios, mejor será para las organizaciones, en particular porque somos el foco de atención en hacer políticas informativas en nuestra sociedad.

De acuerdo con los registros de los servidores de llaves de MIT, solo unos cuantos miembros de The Globe and Mail se registraron para utilizar llaves PGP antes que la organización implementara SecureDrop.

Alasdair McKie dice que muchos de los avances en capacitaciones de seguridad en su editorial se dieron en preparación para SecureDrop. Los registros también indican que la mayoría de las llaves PGP de The Globe and Mail fueron registradas meses después del lanzamiento de SecureDrop como se muestra en la figura 6. Durante el 2015, veintiocho más de los editores de prensa registraron llaves PGP, poniendo a The Globe and Mail en el top de las organizaciones que registraron llaves PGP adelante de The Wall Street Journal y bajo The Guardian.

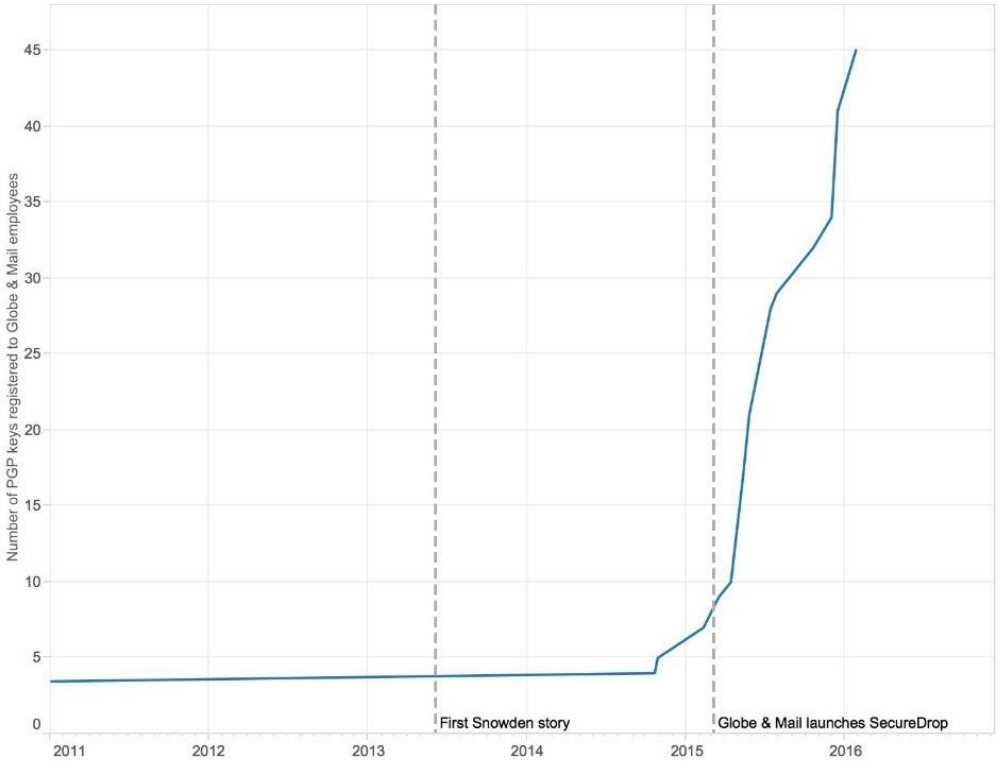

Figura 6: Numero de llaves publicas registradas por The Globe and Mail[15].

1.3.3.3 Otros casos de éxito en la implementación de SecureDrop

En el sitio oficial de SecureDrop se lista un directorio de entidades que han instalado SecureDrop en sus organizaciones como se muestra a continuación en la tabla 1:

Organización	Página web SecureDrop	TOR URL
Apache	https://www.apache.be/securedrop	zdf4nikyuswdzbt6.onion
Associated Press	https://www.ap.org/tips/	3expgpdnrrzezf7r.onion
Bloomberg News	https://www.bloomberg.com/tips/	m4hynbhhctdk27jr.onion
BuzzFeed	https://contact.buzzfeed.com	ftugftwajmgsmoau.onion
CBC	https://securedrop.cbc.ca	ad2ztmbv5vmbj7ic.onion
CPI	https://www.publicintegrity.org/securedrop	v2d6nf2nsvvbgaqe.onion
Dagbladet	https://securedrop.dagbladet.no	mz33367mcdrcdi7s.onion
Espen Andersen	https://espenandersen.no/contact	espenav2n45atpsj.onion
ExposeFacts	https://exposefacts.org	znig4bc5rlwyj4mz.onion

[15] The Globe and Mail (2018). Guide to SecureDrop. Recuperado de: https://towcenter.gitbooks.io/guide-to-securedrop/content/case_studies_news_organizations/the_globe_and_mail.html

FaithLeaks	https://faithleaks.org/	efeip5ekoqi4upkz.onion
Field of Vision	https://fieldofvision.org/securedrop	fovisionunz7mtxw.onion
Forbes	https://www.forbes.com/fdc/securedrop.html	t5pv5o4t6jyjilp6.onion
The Globe and Mail	https://sec.theglobeandmail.com/securedrop	sml5wmpuq7ifq2mh.onion
Greenpeace New Zealand	https://securedrop.greenpeace.org.nz	ll6edwtpfl3zdwoi.onion
The Guardian	https://securedrop.theguardian.com	33y6fjyhs3phzfjj.onion
HuffPost	https://img.huffingtonpost.com/securedrop	rbugf2rz5lmjbfun.onion
The Intercept	https://theintercept.com/source/#securedrop	intrcept32ncblef.onion
Lucy Parsons Labs	https://lucyparsonslabs.com/securedrop	qn4qfeeslglmwxgb.onion
Morgenbladet	https://morgenbladet.no/varsle	g4wmrmqxpj5bnvml.onion
MormonLeaks	https://mormonleaks.io/	efeip5ekoqi4upkz.onion
New Internationalist	https://digital.newint.com.au/securedrop	axcdo2zaeyrpdc6z.onion
The New York Times	https://www.nytimes.com/tips	nyttips4bmquxfzw.onion
NRK	https://www.nrk.no/varsle/	nrkvarslekidu2uz.onion
Project On Gov't Oversight (POGO)	https://securedrop.pogo.org	dqeasamlf3jld2kz.onion
Public Intelligence	https://publicintelligence.net/contribute/	arujlhu2zjjhc3bw.onion
Radio24syv	https://securedrop.radio24syv.dk	hpjw636qnt5avq62.onion
Radio-Canada	https://sourceanonyme.radio-canada.ca	w5jfqhep2jbypkek.onion
San Francisco Chronicle	https://newstips.sfchronicle.com/	nrwvazcz6figxpg5.onion
Stuff Limited	https://www.stuff.co.nz/securedrop	ki3emfb55ywtg5tm.onion
Barton Gellman	https://tcfmailvault.info	mqddpn6yt4f5uqei.onion
The Washington Post	https://www.washingtonpost.com/securedrop	jcw5q6uyjioupxcc.onion
USA TODAY	https://newstips.usatoday.com/securedrop.html	usatodayw7vu5egc.onion
VICE Media	https://news.vice.com/securedrop/	e3v3x57ykz25uvij.onion
Vox.com	https://apps.voxmedia.com/vox-tips/	2cq26ys7wjhryrzw.onion
The Verge	https://apps.voxmedia.com/verge-tips/	2xat73hlwcpwo2zy.onion

Wired's Kevin Poulsen	https://freedom.press/about/tech/kevin-poulsen	poulsensqiv6ocq4.onion

Tabla 1: Entidades que han implementado SecureDrop[16].

1.3.3.4 Caso de uso, cómo se podría aplicar SecureDrop en el Gobierno de El Salvador

En El Salvador, en el primer trimestre del año 2012 el Ministerio de Justicia y Seguridad Pública, junto con Policía Nacional Civil y Fiscalía General de la República iniciaron el programa Crime Stoppers a través del sitio web www.tupista.info para recibir denuncias anónimas sobre diversos delitos. La plataforma de este sitio web es un Sistema de Gestión de Contenido (CMS), WordPress, el cual no proporciona medidas de seguridad adecuadas en los protocolos de comunicación desde el denunciante hasta su destino, hardening, y otros, pudiendo comprometer la integridad, confidencialidad e integridad de la información. El uso de SecureDrop sería beneficioso para instituciones públicas como la Policía Nacional Civil, la seguridad y anonimato de esta plataforma puede mejora el programa de denunciantes y generando más confianza en la ciudadanía para hacer crecer el número de denuncias, con la información que ingrese por parte de los denunciantes se podría analizar con tecnología como Big Data e Inteligencia Artificial para poder plantear mejores planes de Seguridad Pública, planes de prevención, respuesta más efectiva e inmediata a casos iniciados por estas denuncias en Fiscalía General de la República.

Otra institución pública que se podría beneficiar al aplicar SecureDrop sería la Dirección General de Migración y Extranjería, con la información de las denuncias recibidas por esta plataforma se podrían mejorar planes de seguridad reforzando los controles fronterizos, se podría dar una mejor respuesta a delitos como tráfico de drogas, trata de personas entre otros.

La Secretaría de Participación Ciudadana, Transparencia y Anti Corrupción de la Presidencia se puede beneficiar con SecureDrop, al brindar de tecnología segura y anónima para el uso de la

[16] SecureDrop (2018). Directory. Recuperado de: https://securedrop.org/directory

ciudadanía, pudiendo recibir denuncias públicas y privadas de corrupción, fomentar iniciativas de ley o reformar las actuales.

SecureDrop podría ser de gran beneficio en la Superintendencia del Sistema Financiero, la seguridad y anonimato que brinda esta plataforma daría confianza a los usuarios y empleados de las entidades financieras para hacer denuncias de actos de corrupción de los cuales tengan conocimiento o información en sus instituciones, ayudando a hacer cumplir las leyes, reglamentos, normas técnicas y disposiciones legales del sistema financiero, controlar y monitorear preventivamente riesgos, proporcionar transparencia, vigilar de mejor manera que las instituciones supervisadas realicen sus operaciones de acuerdo a lo establecido.

La evasión de impuestos de entidades de la empresa privada podría ser denunciada por ciudadanos con información de estas o los mismos empleados de las entidades, desde el Ministerio de Hacienda podrían ser investigados por la Ley de Impuestos sobre la Renta, se pueden crear casos concretos beneficiando el incremento de las arcas públicas, y crear más obras en beneficio de la sociedad salvadoreña.

1.3.4 Análisis de las implicaciones sociales, éticas y legales del uso de SecureDrop

Al ser una sociedad con alto grado de corrupción que se puede observar con casos de ex funcionarios y empresarios que están siendo investigados bajo un proceso judicial, los niveles de violencia y criminalidad han hecho que la sociedad salvadoreña viva bajo el miedo de no denunciar cualquier acto que ponga en duda el funcionamiento del sistema gubernamental y la transparencia del país por temor a poner en riesgo su propia seguridad y la de su familia, además de no tener un medio que brinde la mayor seguridad y privacidad posible, ejemplo de esto es el sitio web www.tupista.info de Crime Stoppers, esta herramienta está específicamente diseñada para recibir denuncias anónimas y seguras, pero sus certificados digitales no funcionan adecuadamente al ingresar datos con información confidencial como muestra la figura 7, por tanto existe el riesgo de sufrir incidentes informáticos, además de tener un Administrador de Gestión de Contenido vulnerable al no ser

fortalecido adecuadamente, ejemplo de esto es el acceso fácil al página de autenticación de usuarios agregando '/wp-login.php' después de la dirección www.tupista.info como lo muestra la figura 8.

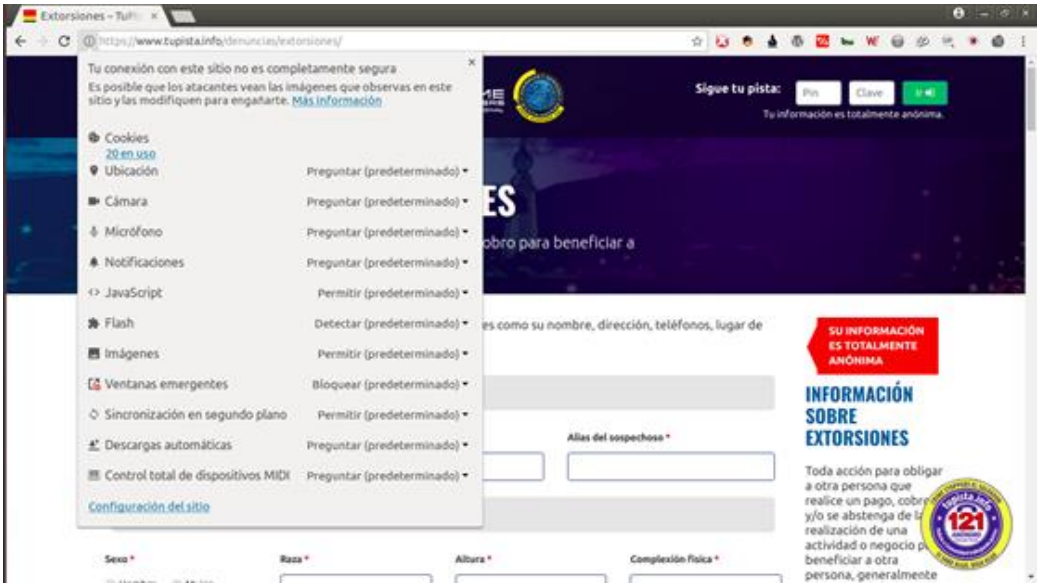

Figura 7: Sitio web www.tupista.info muestra que la conexión no es completamente segura[17].

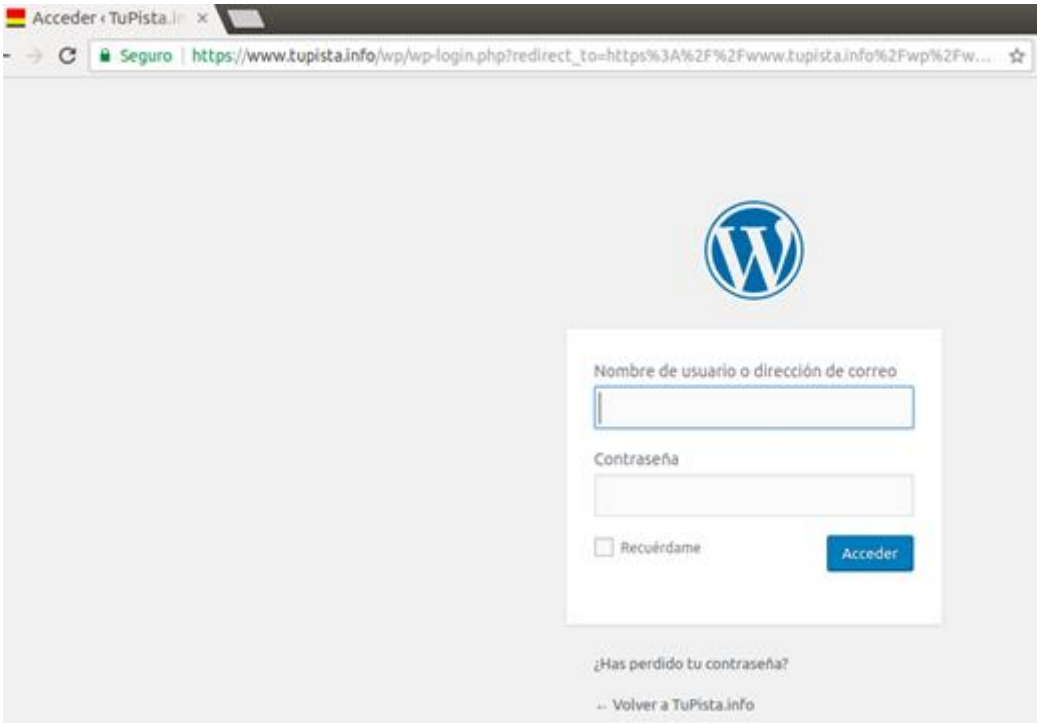

Figura 8: Página de acceso a usuarios para administración de contenido wp-login.php[18].

[17] Crime Stoppers El Salvador (2018). Recuperado de: https://www.tupista.info
[18] Crime Stoppers El Salvador (2018). Recuperado de: https://tupista.info/wp/wp-login.php

La seguridad, privacidad y anonimato que brinda SecureDrop para el ingreso de información confidencial generaría confianza en la sociedad salvadoreña. SecureDrop también implicaría la ética periodística por parte del medio de comunicación cuando reciba información confidencial y anónima para ser rechazada o investigada y no tergiversarla tratando de sacar provecho filtrando información.

A través de las investigaciones periodísticas que se realicen con la información que se ingrese por medio de SecureDrop, estos se pueden trasladar a Fiscalía General de la República y Policía Nacional Civil para iniciar un caso judicial. Se deberá enfatizar la ética a través del medio de comunicación para que los informantes no lleguen a utilizar deliberadamente técnicas de vulneración a sistemas informáticos para obtener información, como lo menciona el Artículo 9 "Violación de la Seguridad del Sistema" (Ley de Delitos Informáticos y Conexos de El Salvador) el cual dice "La persona que sin poseer la autorización correspondiente transgreda la seguridad de un sistema informático restringido o protegido con mecanismo de seguridad específico, será sancionado con prisión de tres a seis años"; con el Artículo 8 "Posesión de Equipo o Prestación de Servicios para la Vulneración de la Seguridad" (Ley de Delitos Informáticos y Conexos de El Salvador), el cual dice "El que utilizando las tecnologías de la Información y la Comunicación posea, produzca, facilite, venda equipos, dispositivos, programas informáticos, contraseñas o códigos de acceso; con el propósito de vulnerar, eliminar ilegítimamente la seguridad de cualquier sistema informático, ofrezca o preste servicios destinado a cumplir los mismos fines para cometer cualquiera de los delitos establecidos en la presente ley, será sancionado con prisión de tres a cinco años"; como se mencionó anteriormente la ética del medio informativo debe ser primordial, la información confidencial que se reciba a través de SecureDrop podría ser de carácter personal de ciudadanos, de no filtrar dicha información para publicarla como lo menciona el Artículo 26 "Revelación Indebida de Datos o Información de Carácter Personal" (Ley de Delitos Informáticos y Conexos de El Salvador), el cual dice "El que sin el consentimiento del titular de la información de carácter privado y personal revele, difunda o ceda en todo en parte, dicha información o datos a los que se refiere el presente artículo,

sean estos imágenes, video, texto, audio u otros, obtenidos por algunos de los medios indicados en los artículos precedentes, será sancionado con prisión de tres a cinco años."

Debemos aclarar que el uso de SecureDrop no violenta la Ley de Delitos Informáticos y Conexos de El Salvador en el Artículo 25 "El que deliberadamente obtenga y transfiera información de carácter confidencial y que mediante el uso de esa información vulnere un sistema o datos informáticos apoyándose en cualquier clase de las Tecnologías de la Información y la Comunicación, incluidas las emisiones electromagnéticas, será sancionado con prisión de cinco a ocho años", ya que ésta funcionara únicamente para la recepción de información confidencial y comunicación con el informante anónimo, esta información se tendrá que verificar para poderse publicar, no dando insumos que puedan ser perjudiciales para vulnerar un sistema o datos informáticos como menciona el artículo, al igual que lo hace el sitio web www.tupista.info.

1.3.5 Contexto legal de denuncias ciudadanas anónimas

1.3.5.1 Código Procesal Penal

Comentario: Si la información en las denuncias resulta útil, sería admisible como prueba.

Art. 177.- Será admisible la prueba que resulte útil para la averiguación de la verdad y pertinente por referirse directa o indirectamente a los hechos y circunstancias objeto del juicio, a la identidad y responsabilidad penal del imputado o a la credibilidad de los testigos o peritos.

Comentario: Respecto a qué partes de la documentación recibida por las denuncias serán admitidas como prueba.

Art. 178.- Las partes podrán acordar, total o parcialmente, la admisión y producción de la prueba pericial, documental y mediante objetos, en los términos establecidos en este Código.

1.3.5.2 Ley Especial de Delitos Informáticos y Conexos.

Comentario: Si una persona ofrece servicios de vulneración a un sistema informático para obtener información confidencial.

Art. 8.- El que utilizando las tecnologías de la Información y la Comunicación posea, produzca, facilite, venda equipos, dispositivos, programas informáticos, contraseñas o códigos de acceso; con el propósito de vulnerar, eliminar ilegítimamente la seguridad de cualquier sistema informático, ofrezca o preste servicios destinado a cumplir los mismos fines para cometer cualquiera de los delitos establecidos en la presente ley, será sancionado con prisión de tres a cinco años

Comentario: Si una persona revela o publica datos personales de otros.

Art. 26.- El que sin el consentimiento del titular de la información de carácter privado y personal revele, difunda o ceda en todo en parte, dicha información o datos a los que se refiere el presente artículo, sean estas imágenes, video, texto, audio u otros, obtenidos por algunos de los medios indicados en los artículos precedentes, será sancionado con prisión de tres a cinco años.

CAPITULO 2

SITUACIÓN ACTUAL

2.1 Usos actuales de la herramienta TOR

Los usos que actualmente se le dan a la herramienta TOR son los siguientes:

- Utilizado por periodistas que trabajan en países donde la información es muy censurada.
- Utilizado por políticos para entablar conversaciones privadas con otros países.
- Delincuentes para evitar ser identificados al realizar sus operaciones ilegales e inmorales en la DeepWeb.
- Hackers para hacer investigación de la red TOR y como mejorarla.
- Hackers e investigadores policiales persiguiendo delincuentes.

La red TOR ofrece un nivel de seguridad en el cual sería muy difícil rastrear a las fuentes de denuncias ciudadana, por lo cual permite tranquilidad en el anonimato para denunciar hechos de corrupción.

2.2 Usos actuales del sistema operativo TAILS

Los usos que actualmente se le dan al sistema operativo TAILS son los siguientes:

- Utilizado por periodistas que trabajan con SecureDrop como capa extra de seguridad criptográfica.
- Utilizado por informantes que quieran hacer una denuncia y mantener su anonimato.
- Utilizado por delincuentes que no quieran dejar rastro en un computador.
- Utilizado para borrar de forma segura cualquier información o archivos.

El sistema operativo TAILS ofrece un nivel extra de seguridad adicional al proporcionar fácil acceso a la red TOR, por ser un “Live CD” no ocupa espacio en el disco duro y tampoco deja rastro en el computador, consta de diversas herramientas que proveen mayor privacidad y capas de cifrado.

2.3 Benchmarking Análisis Comparativo entre SecureDrop y GlobalLeaks

Los denunciantes que pudieran estar en riesgo de aquellos a los que están denunciando ahora usan métodos de cifrado y software anónimo para compartir contenido y proteger su identidad. TOR, una red de anonimato altamente accesible, es una de las que utilizan con frecuencia los denunciantes de todo el mundo. TOR ha sido sometido a una serie de grandes actualizaciones de seguridad para proteger las identidades de potenciales denunciantes que pueden querer filtrar información anónimamente.

Recientemente se ha hecho software especializado en denuncias como SecureDrop y GlobaLeaks, siendo estos los únicos que se ejecutan sobre la red TOR para incentivar y simplificar su adopción para la denuncia segura de irregularidades. Podemos observar un cuadro comparativo entre estas dos tecnologías en la tabla 2.

Arquitectura	**SecureDrop**	**GlobalLeaks**
Arquitectura de un Servidor	No	Si
Multiservidor (envío vs recepción)	Si	No
Envío de documentos Anónimamente	Si	Si
Caso de uso definido	Si	Si
Interfaz de Usuario	HTML	JavaScript
Software		
Repositorio Debian	No	Si
Appliance de Máquina Virtual (Packer/Vangrant)	No	Si
Soporte Multilenguaje	Si	Si
Colaboración en traducción	Si	Si
Personalización de Interface	No	Si
Firmado de Código Fuente	Si	Si
Administración vía web	No	Si
Notificación a informantes de actualización de denuncias	No	Si
Selección de categorías de envío de denuncias	No	Si
Confirmación de recibido para que el denunciante contacte nuevamente	Si	Si
Seguridad		
Cifrado PGP de archivos	Si	Si
Cifrado de mensajes con PGP entre Informante y Receptor	Si	No
Secure Viewing Station	Si	Si
Retención de Datos	No	Si
Endurecimiento del Sistema Operativo	Si	No
AppArmor Sandboxing	Si	Si

Política de contraseña reforzada (Password Strength)	Si	Si
Auditorias de seguridad en el software	Si	Si
Almacenamiento de contraseñas con scrypt	Si	Si
Documentación		
Manual de Usuario	Si	Si
Manual de Desarrollador	Si	Si
Manual de Implementación	Si	Si

Tabla 2. Comparación de SecureDrop y GlobalLeaks.[19]

2.4 Evaluación entre las plataformas SecureDrop y GlobalLeaks según características basado en ISO/IEC 912621 sobre la evaluación de la calidad del software

El siguiente es un cuadro resumen con características y criterios de evaluación para de definir cuál de las siguientes plataformas tiene mejor clasificación.

Los valores de las métricas cuantitativas permitidos para la evaluación están en una escala del 0 a 3 indicando 0 el valor menor y 3 el valor máximo de favorabilidad del resultado.

# Criterios	Descripción de Criterios	Métrica
1	No cuenta con las especificaciones y funciones consultadas	0
2	El uso de las plataformas representa desafíos como lentitud, adaptación, etc.	1
3	Proporciona un navegador, instalación multiplataforma y soporte	2
4	Proporciona funcionabilidad con otras tecnologías que buscan proteger la privacidad, censura y anonimato	3

Tabla 3. Criterios de Evaluación de la calidad del software en base a ISO/IEC 912621.

				Plataforma	
Características	Pregunta Relacionada a la Característica	Subcaracterísticas	Pregunta Relacionada a la Sub Característica	SecureDrop	GlobalLeak
Funcionabilidad	¿Las funciones y propiedades satisfacen las necesidades de privacidad y anonimato?	Adecuación (Criterio de evaluación 4)	¿Tiene un conjunto de funciones apropiadas para las tareas de	3	3

[19] Libreationtech(2013-2018). GlobaLeaks - SecureDrop comparison & Security improvements. Recuperado de: https://mailman.stanford.edu/pipermail/liberationtech/2013-October/012029.html

			privacidad y anonimato?		
Confiabilidad	¿Puede mantener el nivel de rendimiento bajo ciertas condiciones y por cierto tiempo?	Entendimiento (Criterio de evaluación 3)	¿Es entendible para el usuario reconocer la estructura y la lógica de su aplicabilidad?	2	2
Usabilidad	¿El Software es fácil de utilizar y aprender?	Aprendizaje (Criterio de evaluación 3)	¿Es fácil de utilizar en su navegador?	2	2
Eficiencia	¿Es rápido en cuanto al uso de recursos, y bajo ciertas condiciones?	Comportamiento en el tiempo (Criterio de Evaluación 1 y 2)	¿Es lento el uso de sus navegadores en la red oscura?	1	1
Mantenibilidad	¿Es fácil de integrar y adaptar el software?	Adaptabilidad (Criterio de Evaluación 1 y 3)	¿Es fácil de adaptar a otros entornos u otras infraestructuras ?	2	2
Portabilidad	¿Es instalable en ambientes multiplataform a	Facilidad de instalación (Criterio de Evaluación 3)	¿Es fácil instalar en ambientes multiplataforma ?	2	0
Calidad de Uso	¿Muestra el usuario final aceptación y seguridad del software?	Eficacia (Criterio de Evaluación 4)	¿Es eficaz el software cuando el usuario final realiza los procesos?	3	2
			Total	15	12
			Puntuación Porcentual	71.42	57.14

Tabla 4. Métricas de Evaluación de la calidad del software en base a ISO/IEC 912621.

CAPITULO 3

DISEÑO DE LA SOLUCIÓN

3.1 Análisis de requerimientos

SecureDrop es una infraestructura de múltiples servidores y estaciones de trabajo. En este capítulo se ha hecho una revisión de los requerimientos y aspectos técnicos de SecureDrop en cuanto a hardware, software y otros componentes técnicos para la implementación de una infraestructura que proporcione confidencialidad y anonimato al denunciante y que a continuación se presentan:

3.1.1 Requerimientos de Hardware

Antes de iniciar la instalación de SecureDrop necesitaremos los siguientes requisitos mínimos de hardware en cada una de las computadoras basado en la recomendación del hardware Intel NUC[20]:

- 1.20 GHz de CPU Intel® Core™ i5
- 4 GB de memoria RAM
- 250 GB de Disco Duro

Utilizaremos 2 computadoras que actuarán como “Application Server” y “Monitor Server” para ejecutar la aplicación SecureDrop y 2 computadoras para las estaciones de trabajo “Secure Viewing Station” y “Admin/Journalist Workstation” y 1 computadora para el firewall pfSense.

El detalle de las funciones de cada una de las computadoras se muestra a continuación:

- 1 servidor de aplicación para la ejecución del Core de SecureDrop.
- 1 servidor de monitoreo que revisara la actividad del servidor de aplicación.
- 1 computadora dedicada para la estación “Secure Viewing Station”.
- 1 computadora dedicada para la estación “Admin/Journalist Workstation”.
- 1 firewall de red. Puede ser una computadora dedicada como firewall de red para los servidores de SecureDrop.

[20] SecureDrop (2018). Documentation. Recuperado de: https://docs.securedrop.org/en/release-0.8/hardware.html#intel-nuc

- 3 cables de red ethernet.
- 4 memorias USB:
    - 1 como USB “maestra” desde donde se crearán las USB con Tails para “Admin/Journalist Workstation” y “Secure Viewing Station”.
    - 1 para uso del Administrador en la “Admin/Journalist Workstation”.
    - 1 para la computadora “Secure Viewing Station”.
    - 1 para el dispositivo de transferencia.

3.1.2 Requerimientos de Software

El servidor de aplicación de SecureDrop (Application Server) y el servidor de monitoreo (Monitor Server) se ejecutan en Ubuntu-14.04.5 versión servidor. Para las estaciones de trabajo iniciaremos TAILS desde las memorias USB.

La instalación de los componentes de SecureDrop se descargarán directamente desde el repositorio de Freedom of the Press Foundation (https://apt.freedom.press/) desde donde se descargan componentes como:

- linux-image-4.4.*-grsec
- ossec-agent
- ossec-server
- securedrop-app-code
- securedrop-ossec-agent
- securedrop-ossec-server
- securedrop-grsec
- securedrop-keyring

3.2 Requerimientos previos a la instalación de SecureDrop

El instalar SecureDrop es un proceso manual y largo que requiere de preparación de varios componentes previos a la instalación como:

- Crear las memorias USB con TAILS.
- Configurar la estación de trabajo segura (Secure Viewing Station).
- Configurar la estación de trabajo del administrador (Admin Workstation).
- Preparar el dispositivo USB de transferencia.
- Generar la clave de envío de SecureDrop.
- Configurar el firewall de red.

3.3 Arquitectura de SecureDrop

Hay cuatro componentes principales en la arquitectura de SecureDrop como se muestra en la figura 9: los servidores, los administradores, los informantes y los periodistas.

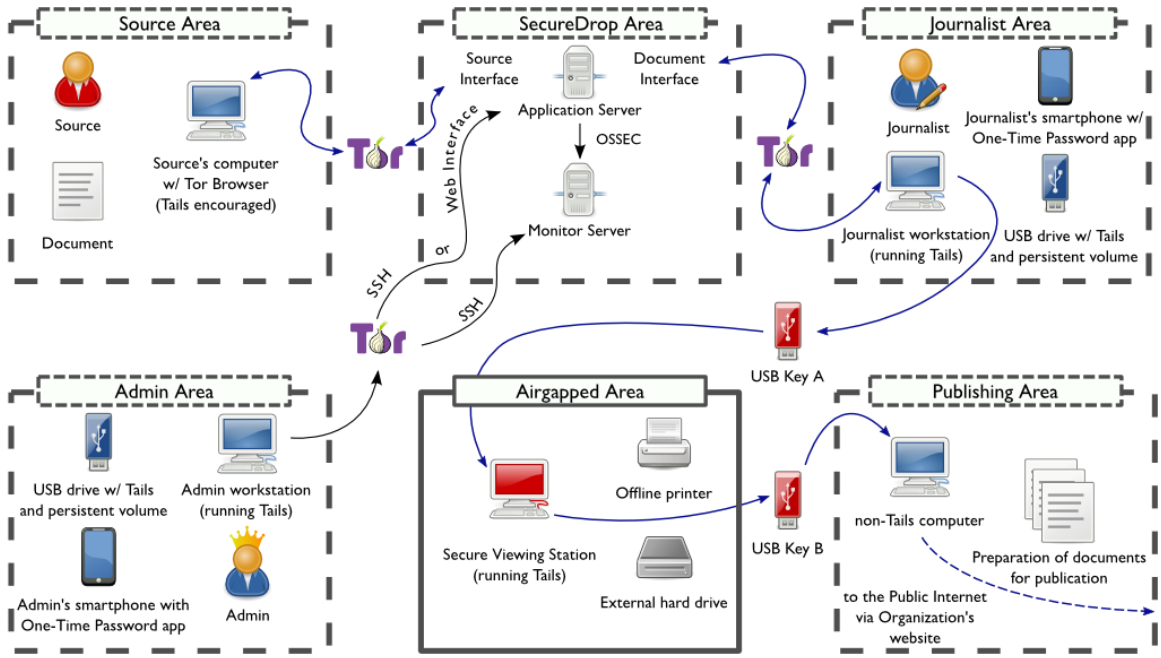

Figura 9: Componentes principales en la arquitectura de SecureDrop[21].

3.3.1 Los Servidores

En el centro de la arquitectura de SecureDrop se encuentran dos servidores: El servidor de Aplicación (*Application "App" Server*), que ejecuta el componente principal de software de

[21] SecureDrop (2018). Documentation. Recuperado de: https://docs.securedrop.org/en/stable/overview.html

SecureDrop, y el servidor de Monitoreo (*Monitor "Mon" Server*), que realiza un seguimiento del estado del servidor de aplicaciones (*Application Server*) y envía alertas cuando hay algún problema. Estos dos servidores se ejecutan en hardware dedicado y conectado a un Firewall dedicado.

3.3.2 Los Administradores

Los servidores de SecureDrop son operados por los administradores. Los administradores usan una estación de trabajo administrativa (*Admin Workstation*) ejecutando TAILS[22], una distribución de Linux basada en Debian centrada en la seguridad y dirigida a preservar la privacidad y el anonimato como sistema operativo, que se conecta a los servidores de aplicación y monitoreo (*Application and Monitor Servers*) de SecureDrop sobre TOR y administrados usando Ansible, un software de código abierto que automatiza el aprovisionamiento de software, la administración de configuraciones y la implementación de aplicaciones.

3.3.3 Los Informantes

Los informantes envían documentos y mensajes utilizando el navegador web de TOR (TOR Browser[23] o TAILS) para acceder a la interfaz de acceso (*Source Interface*) que es un servicio oculto publicado en TOR. Los envíos de denuncias se realizan cifrados en el momento de enviarlos en el servidor de aplicación (*Application Server*) cuando estos son cargados en la interfaz web.

3.3.4 Los Periodistas

Los periodistas trabajando en la sala de prensa usando dos estaciones de trabajo para interactuar con SecureDrop. Primero, ellos utilizan la estación de trabajo de Editores (*Journalist Workstation*) ejecutando TAILS para conectarse a la interfaz de los Editores (*Journalist Interface*), un servicio oculto y autenticado publicado en TOR. Los periodistas descargan los envíos cifrados con

---

[22] The Amnesic Incognito Live System conocido por sus siglas en inglés como TAILS es una distribución Linux diseñada para preservar la privacidad y el anonimato

[23] TOR Browser es un navegador web endurecido para acceder a la red TOR

PGP y los copian en un dispositivo de transferencia (*Transfer Device*) en USB. Esos envíos son conectados a la estación de trabajo de vista segura y fuera de línea (*Secure Viewing Station*) que tiene las llaves para descifrar. Los periodistas que usan la SVS (*Secure Viewing Station*) para leer, imprimir y preparar documentos para su publicación. A parte de esos documentos publicados, los documentos descifrados nunca son accedidos en una estación de trabajo conectada a Internet.

3.4 Diagrama de Flujo de Datos de SecureDrop

Los siguientes diagramas capturan el flujo de datos desde y hacia la zona segura de SecureDrop.

En la figura 10 podemos observar como las fuentes de información o denunciantes utilizando TOR Browser envían la información a SecureDrop por medio del portal de denunciantes. De igual manera la estación del administrador se conecta por medio del protocolo SSH[24] utilizando TOR a SecureDrop. Desde la estación de los editores o periodistas en la figura 6 se accede por medio de TOR Browser a la interfaz de los periodistas.

Desde SecureDrop podemos apreciar en la figura 5 salen las conexiones a servicios externos como: el servidor NTP[25], los repositorios de Ubuntu, los repositorios FPF[26], el repositorio de TOR, y el Relay SMTP[27].

---

[24] SSH (Secure SHell, en español: intérprete de órdenes seguro) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder servidores privados a través de una puerta trasera (también llamada backdoor).
[25] Network Time Protocol (NTP) es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable.
[26] Freedom of the Press Foundation por sus siglas en ingles FPF aloja paquetes de instalación y actualización de SecureDrop.
[27] Se entiende como open relay (‘relé abierto’ en inglés) un servidor SMTP configurado de tal manera que permite que cualquier usuario de Internet lo use para enviar correo electrónico a través de él, no solamente el correo destinado a, o procedente de usuarios conocidos

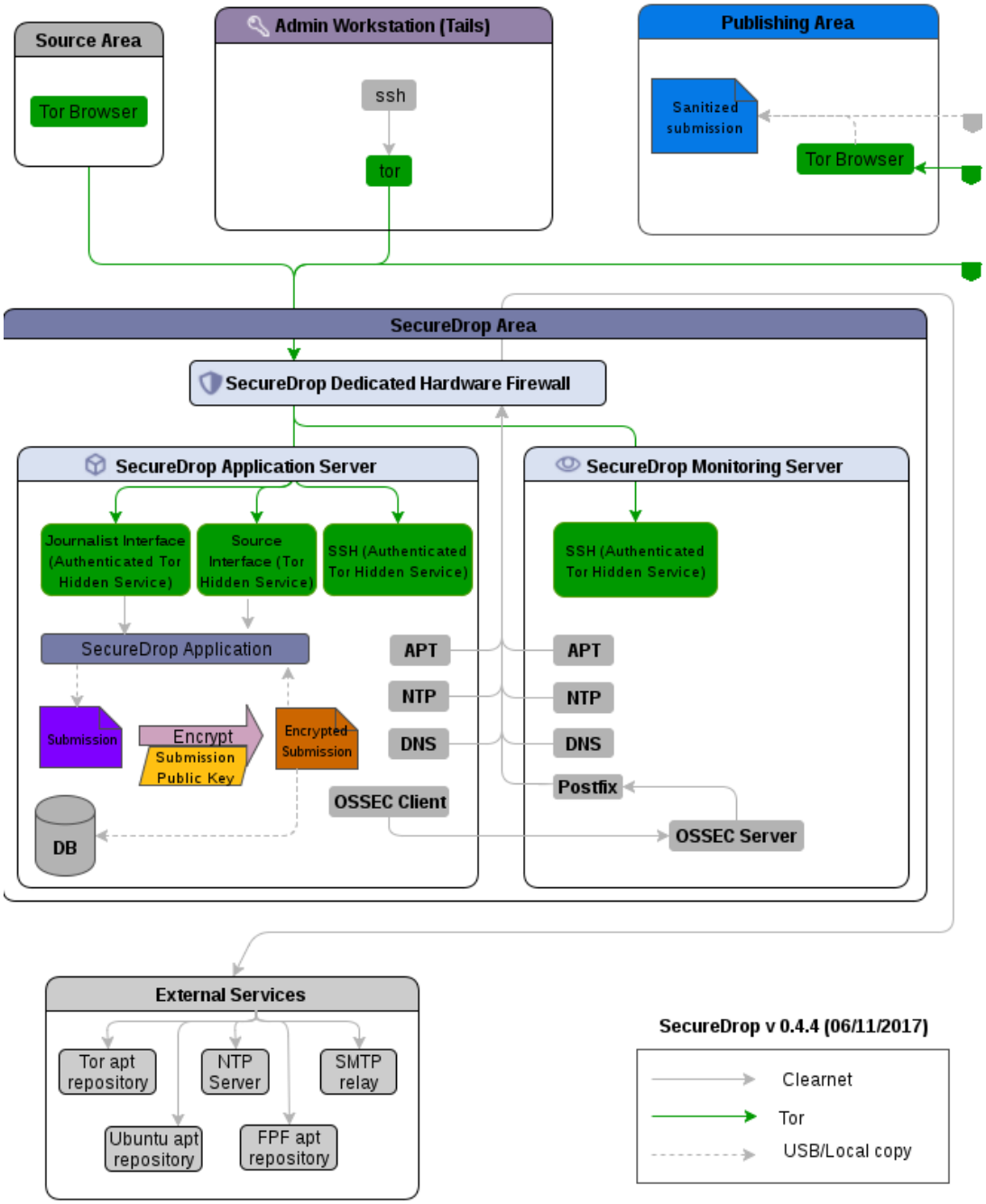

Figura 10: Diagrama de flujo de datos hacia SecureDrop[28] *y servicios externos.*

[28] SecureDrop Documentation (2018). Data Flow Diagram. Recuperado de: https://docs.securedrop.org/en/stable/threat_model/dataflow.html

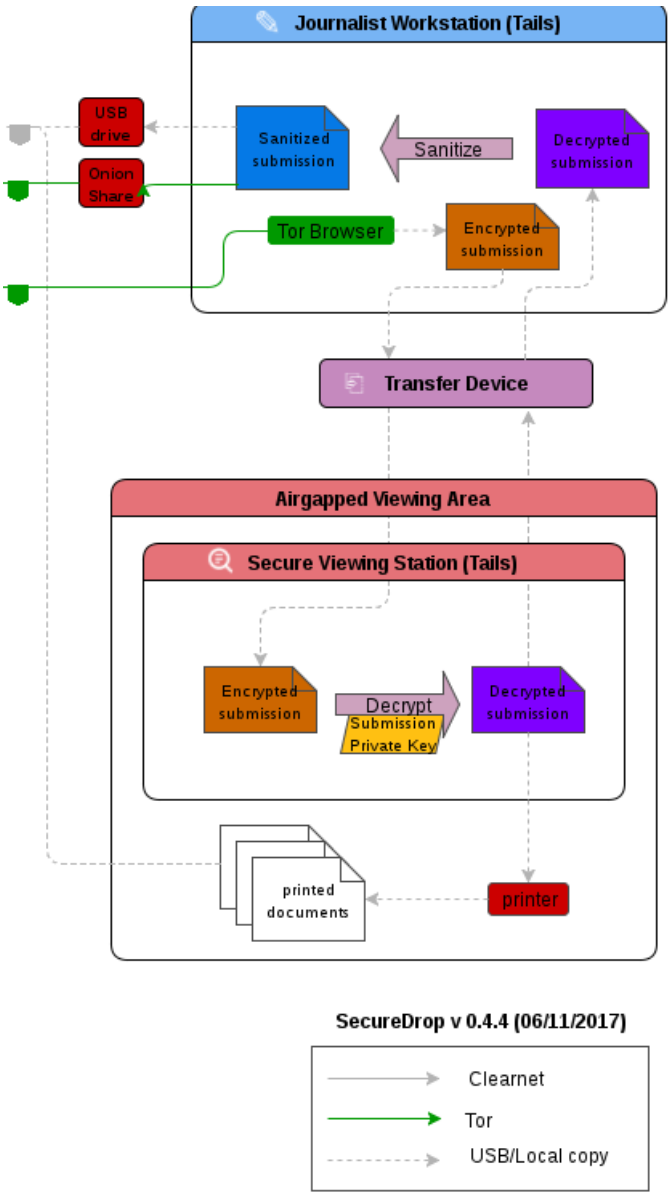

Figura 11: Diagrama de flujo de datos hacia SecureDrop[29] *y el área de publicación.*

En la figura 11 también podemos observar la estación de trabajo segura en la cual por medio de dispositivos removibles se puede cifrar o descifrar la información recibida para examinar la denuncia para su posterior publicación.

[29] SecureDrop Documentation (2018). Data Flow Diagram. Recuperado de: https://docs.securedrop.org/en/stable/threat_model/dataflow.html

3.5 Diagrama del funcionamiento, perspectiva del usuario y periodista

El usuario que envía la denuncia utilizara TAILS o el navegador web TOR Browser para conectarse a la interface de la fuente y enviar la información a SecureDrop como se muestra en la figura 12.

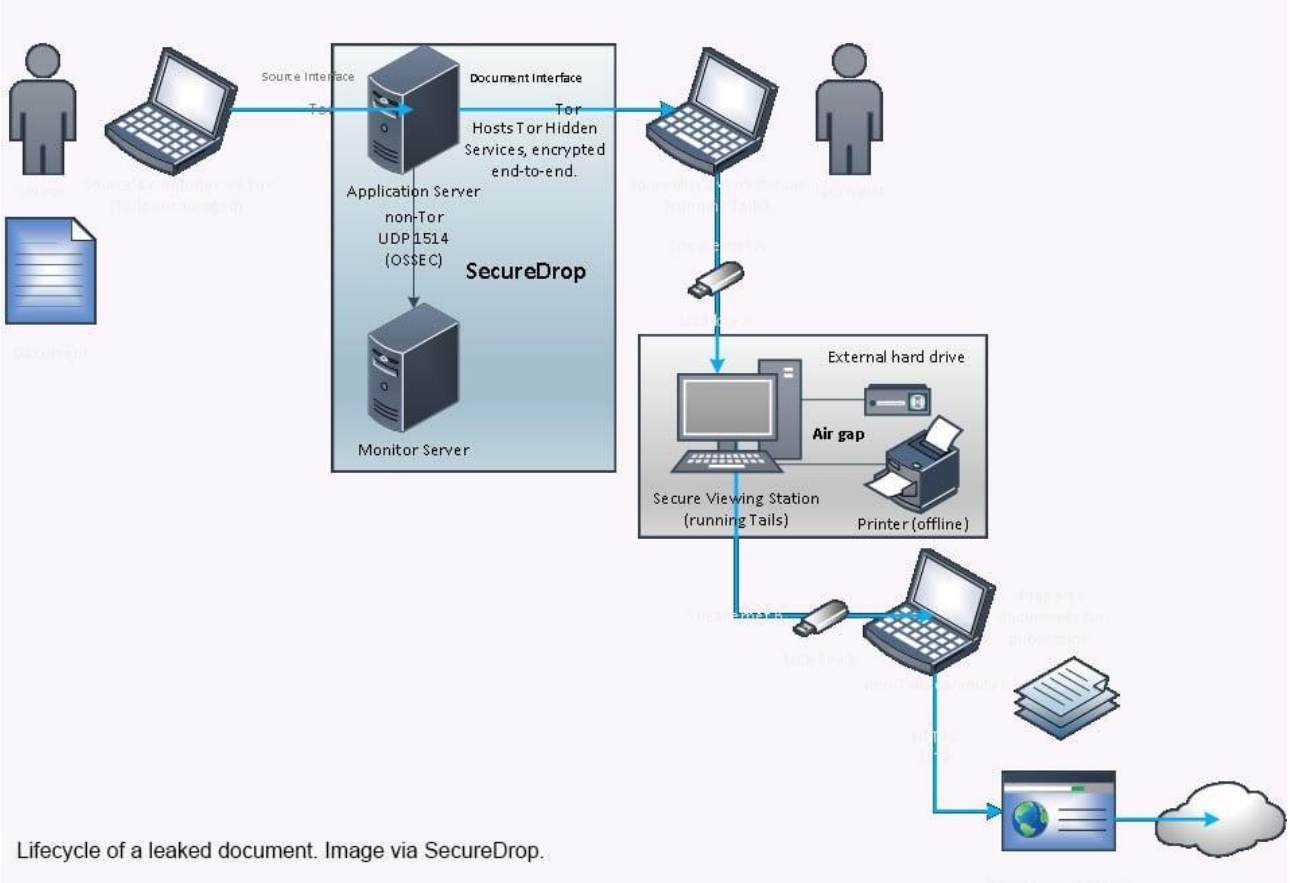

Figura 12: Perspectiva del usuario hacia SecureDrop[30] *y del periodista.*[31]

El periodista extra la información cifrada utilizando la interface del mismo para ser descifrada en la estación de trabajo segura (Secure Viewing Station) para su posterior publicación como se muestra en la figura 12.

[30] SecureDrop Documentation (2018). Data Flow Diagram. Recuperado de: https://docs.securedrop.org/en/stable/threat_model/dataflow.html
[31] Foliomag. (2018). As Journalists Seek Encryption, SecureDrop Proves a Challenge. Recuperado de: https://www.foliomag.com/journalists-seek-encryption-securedrop-proves-challenge/

CAPITULO 4

MANUAL DE INSTALACIÓN Y CONFIGURACIÓN

Implementación de un sistema de denuncia basado en SecureDrop

Manual de Instalación

Versión: 0001

Primera Versión del Producto

HOJA DE CONTROL

Organismo	Maestría en Seguridad y Gestión de Riesgos Informáticos		
Proyecto	Implementación de un sistema de denuncia basado en SecureDrop		
Entregable	Manual de Instalación		
Autor	Ing. Ronald González Rivera e Ing. Ricardo Párraga Zaldívar		
		N.º Total de Páginas	84

REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Fecha del Cambio
0001	Versión inicial	Ing. Ricardo Párraga Zaldívar	27/08/2018

CONTROL DE DISTRIBUCIÓN

Nombre y Apellidos
Ing. Ronald González Rivera

4.1 Manual de Instalación y Configuración de SecureDrop

Objeto

El propósito del presente manual de instalación es proporcionar una guía paso a paso sobre la instalación y configuración de la plataforma SecureDrop en servidores Ubuntu GNU Linux.

Alcance

El presente es un manual de instalación enfocado a personal con alto conocimiento técnico en infraestructuras basadas en GNU Linux, redes y conocimientos de seguridad de la información.

Estructura del Manual:

4.1.1 Pasos Previos a la Instalación de SecureDrop

4.1.2 Configuración del firewall de red con pfSense

4.1.3 Configuración de los servidores.

4.1.4 Instalación SecureDrop.

4.1.5 Configuración de la estación de trabajo del Administrador.

4.1.6 Creando la cuenta de administrador en la interfaz de los Periodistas.

4.1.1 Pasos Previos a la Instalación de SecureDrop

Para comenzar con la instalación creamos la memoria USB maestra con TAILS desde donde crearemos las memorias USB para “Admin Workstation” y “Secure Viewing Station”. Utilizaremos *Universal USB Installer* seleccionando en el paso 1 TAILS como sistema operativo, continuando con el paso 2 seleccionando la imagen ISO descargada y

en el paso 3 la unidad de destino que tomo la memoria USB en nuestro sistema operativo Windows como muestra la figura 13.

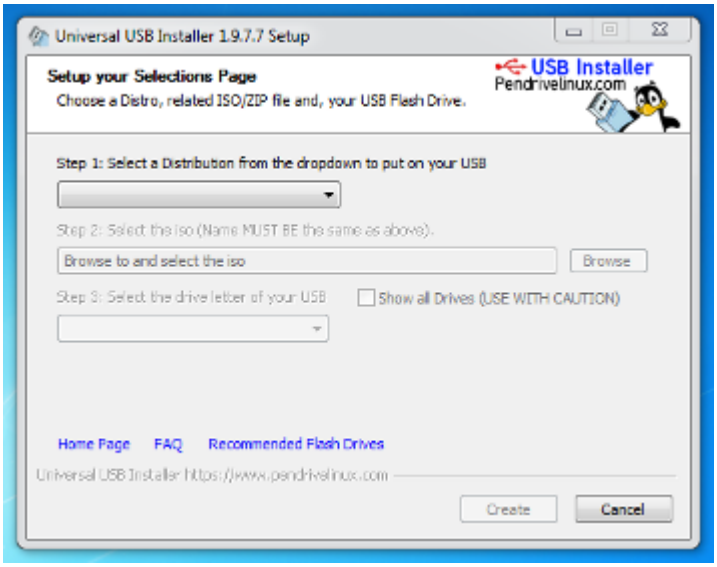

Figura 13: Interface Universal USB Installer[32].

Al reiniciar desde las memorias USB se inicia el sistema operativo TAILS. Al crear las memorias USB con TAILS es necesario habilitar persistencia para no perder la información después de un reinicio. Este paso se logra desde el sistema operativo TAILS en ejecución. seleccionamos en el menú Aplicaciones ▸ Tails ▸ Configurar volumen persistente, luego seleccionando una contraseña y presionando en el botón Crear.

Posteriormente se configura la estación “Secure Viewing Station” y se configura la memoria USB que servirá como dispositivo de transferencia. Generamos la llave

[32]Tails. Instalador Universal USB Installer. Recuperado de: https://tails.boum.org/uui/Universal-USB-Installer.exe

"SecureDrop Submission Key" como se muestra en la figura 14 y la copiamos al dispositivo de transferencia previo a la instalación de SecureDrop".

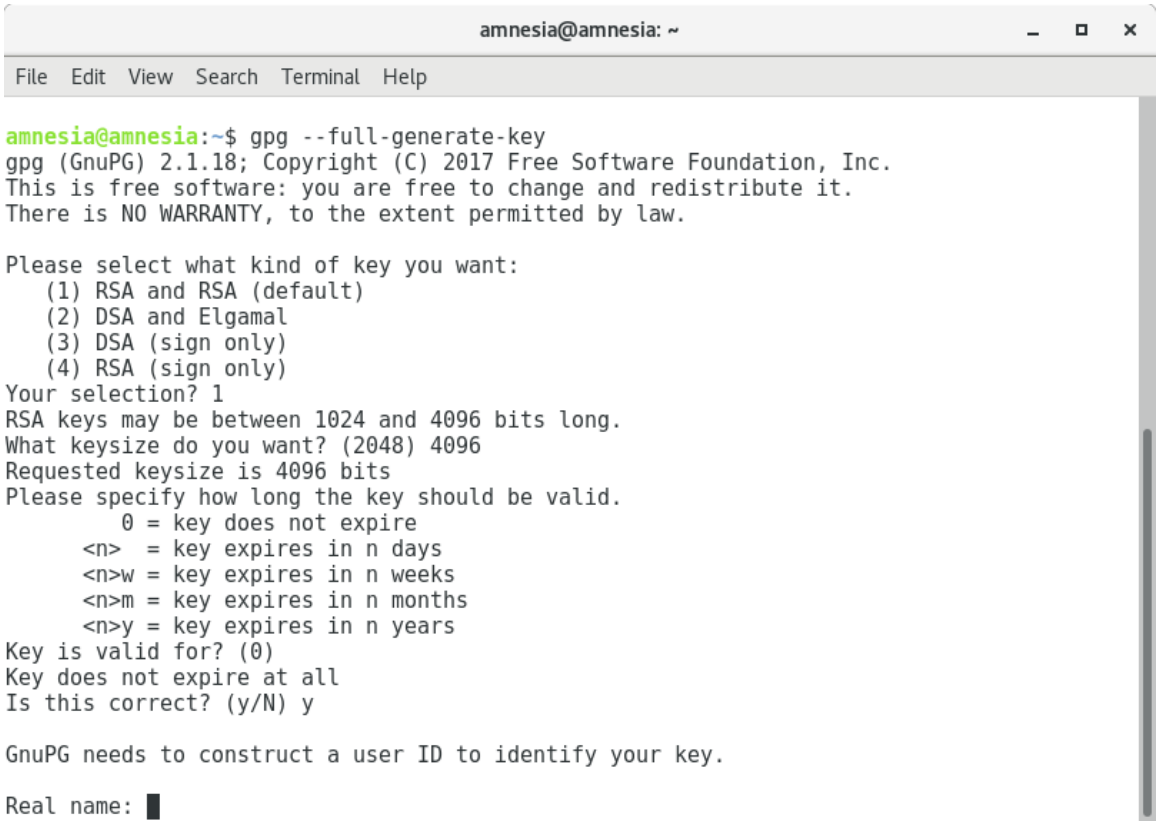

Figura 14: Generando la clave de envío (Submission Key) de SecureDrop.

4.1.2 Configuración del firewall de red con pfSense

Siguiendo las recomendaciones de la documentación de SecureDrop en cuanto a la instalación y configuración del firewall utilizaremos pfSense por la fácil explicación paso a paso de la configuración, pero se pudieran agregar las mismas configuraciones a cualquier otro firewall ya sea en hardware o software.

Para configurar el firewall pfSense utilizaremos la memoria USB de “Admin Workstation”. Accederemos a la IP del firewall por medio de la interfaz web y configuramos las reglas en base a las recomendaciones de SecureDrop[33] agregándolas paso a paso según hemos asignado las direcciones IP a nuestra topología.

SecureDrop sugiere diferentes segmentos de red como OPT1 para “Application Server” como lo muestra la figura 15, OPT2 para el “Monitor Server” como lo muestra la figura 16 y LAN para “Admin Workstation” como se muestra en la figura 17 a continuación:

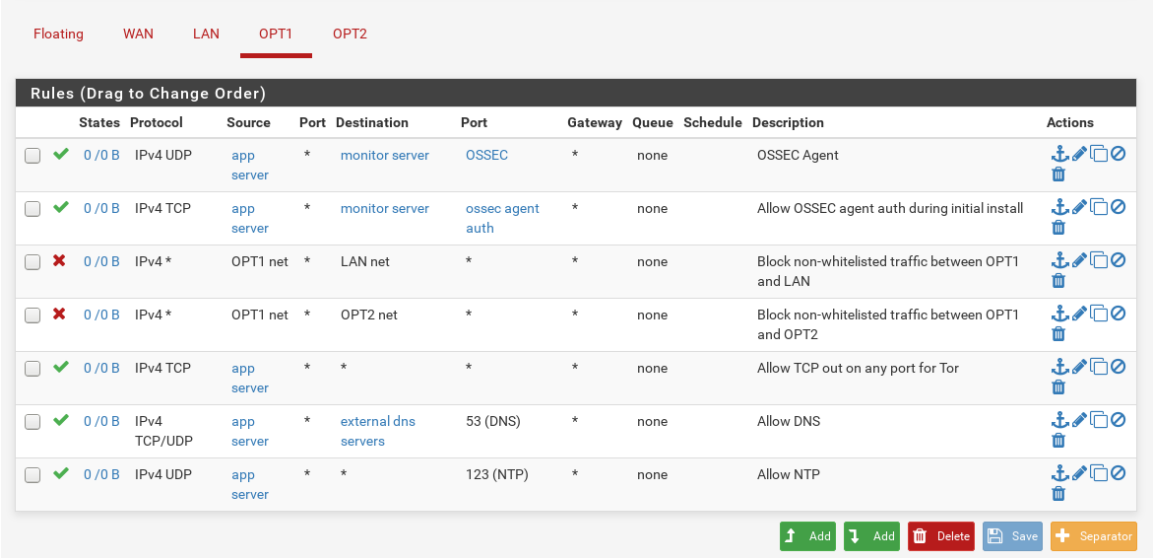

Figura 15: Reglas del firewall en la interfaz de red OPT1 de pfSense.

[33] SecureDrop Documentation (2018). Set up the Network Firewall. Recuperado de: https://docs.securedrop.org/en/release-0.6/network_firewall.html

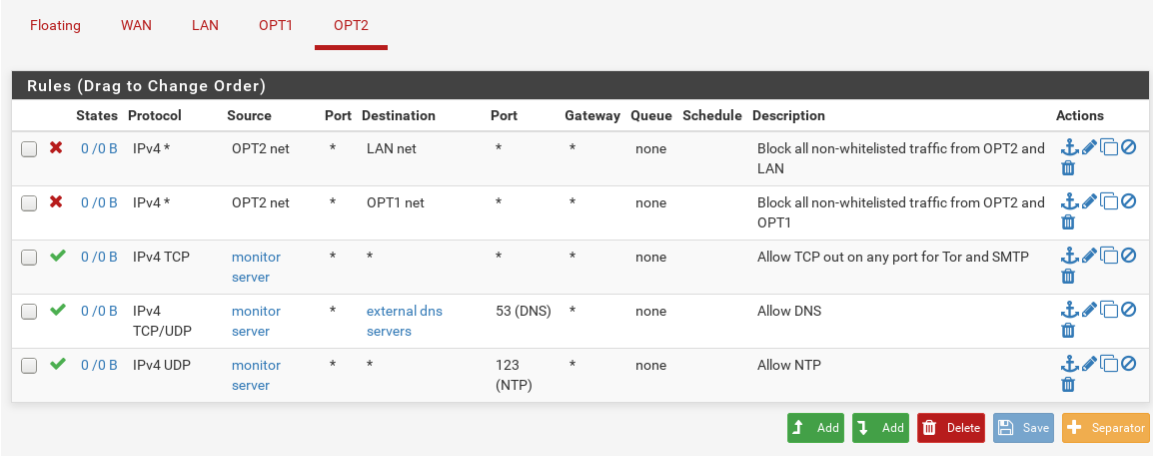

Figura 16: Reglas del firewall en la interfaz de red OPT2 de pfSense.

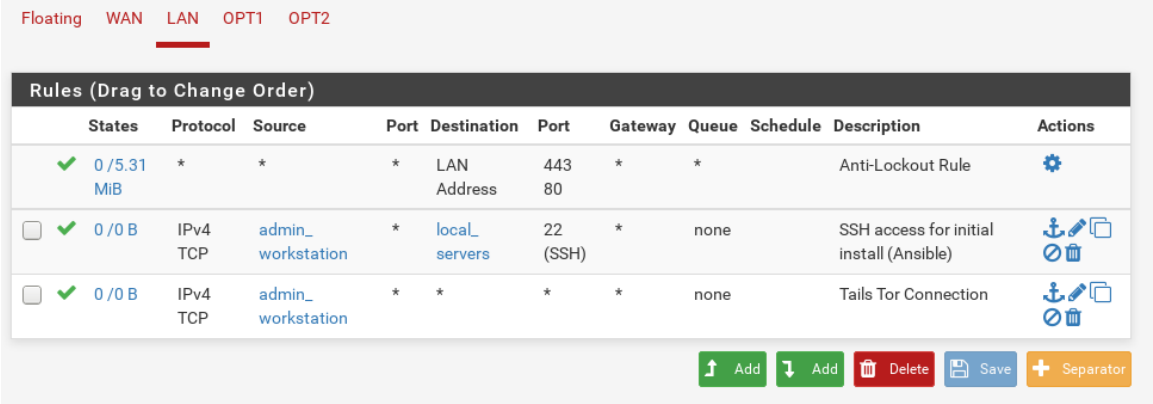

Figura 17: Reglas del firewall en la interfaz de red LAN de pfSense.

4.1.3 Configuración de los servidores

Una vez configuradas las reglas del firewall instalamos los servidores Ubuntu para "Monitor Server" y "Application Server" de la misma manera según la guía de instalación

de SecureDrop[34]. Es de notar que el proceso de instalación de SecureDrop configurará estos con todo lo necesario por lo que una instalación base idéntica para ambos servidores será suficiente. La versión sugerida por SecureDrop es ubuntu-14.04.5-server-amd64. Una vez instalado y configurados según la guía realizamos pruebas de conectividad para comprobar que las reglas del firewall funcionan accediendo por medio de SSH desde la "Admin Workstation". Si la conexión es exitosa crearemos las llaves publicas/privadas para acceder únicamente por medio de autenticación de llave pública en lugar de contraseñas.

4.1.4 Instalación SecureDrop.

SecureDrop tiene dependencias que previo a la instalación se tienen que cargar en la "Admin Workstation". Para cargar estas dependencias se ejecuta el script "*securedrop-admin setup".*

Iniciamos la configuración del "Playbook" que recogerá datos importantes previo a la instalación ejecutando el comando "*securedrop-admin sdconfig"*.

Una vez los pre-requisitos de instalación están completos iniciamos la instalación ejecutando el script "*securedrop-admin install"* que se muestra a continuación en la Figura 18 que modificara los servidores.

---

[34] SecureDrop Documentation (2018). Install SecureDrop. Recuperado de: https://docs.securedrop.org/en/release-0.6/install.html

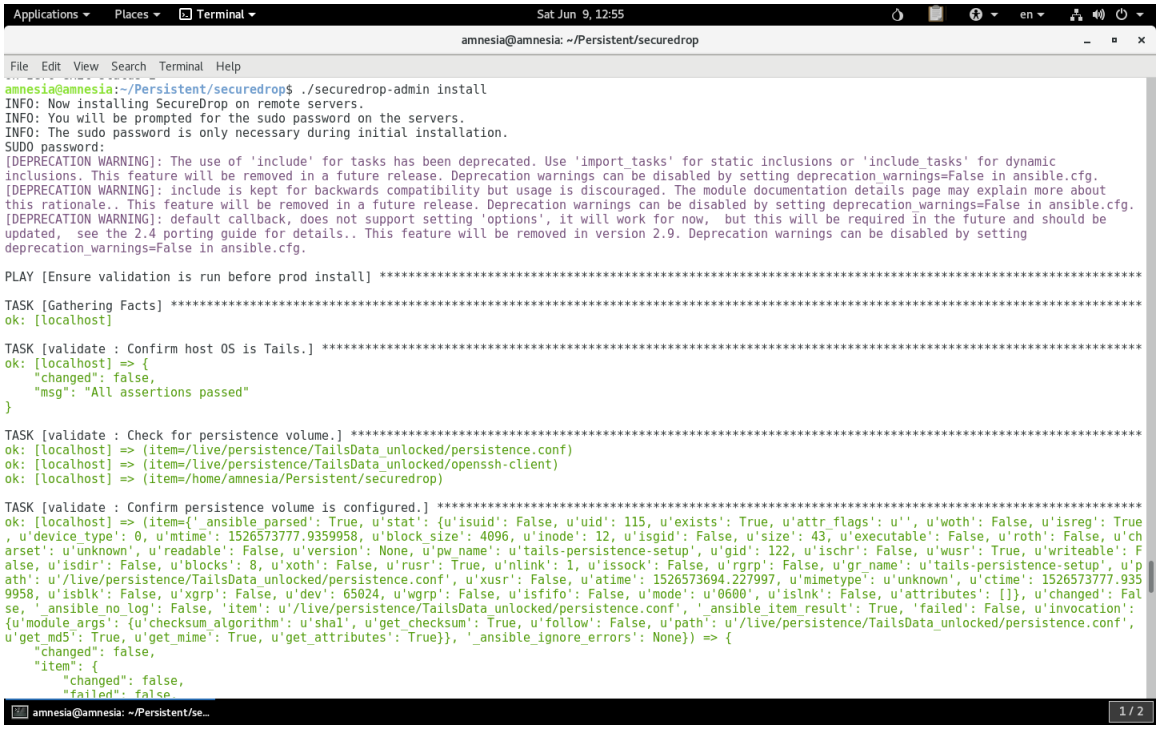

Figura 18. Ejecución del script de instalación de SecureDrop[35].

[35] SecureDrop Documentation (2018). Install SecureDrop. Recuperado de: https://docs.securedrop.org/en/release-0.6/install.html

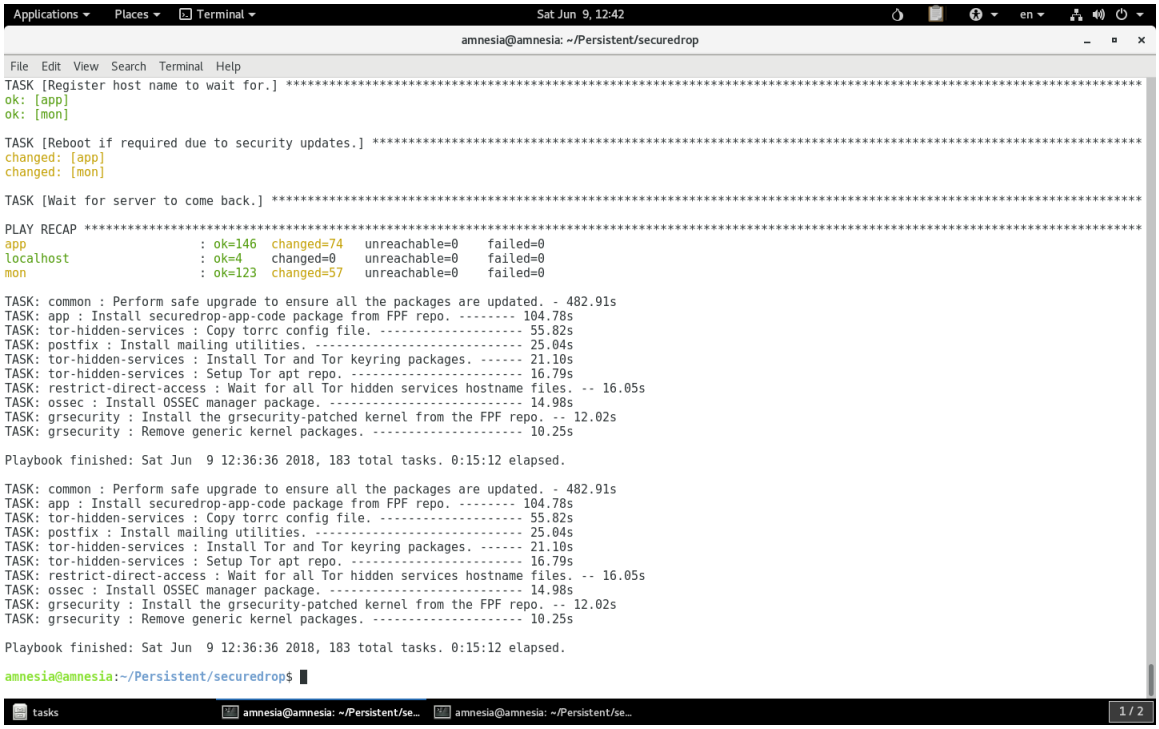

Figura 19. Finalización de la instalación de SecureDrop[36].

Una vez finalizado el script tendremos un resumen y cómo podemos ver en la figura 19 en la que se han ejecutado 146 cambios en el "Application Server" y 123 en el "Monitor Server" de SecureDrop.

4.1.5 Configuración de la estación de trabajo del Administrador

La instalacion de SecureDrop agrega diferentes capas de autenticación para proteger el sistema y los activos mas valiosos de SecureDrop bloqueando el acceso a los servicios SSH. Para acceder a estos como parte de la post-instalacion ejecutamos el

---

36 SecureDrop Documentation (2018). Install SecureDrop. Recuperado de: https://docs.securedrop.org/en/release-0.6/install.html

siguiente script con *securedrop-admin tailsconfig* como se muestra en la figura 20 para poder acceder a ellos.

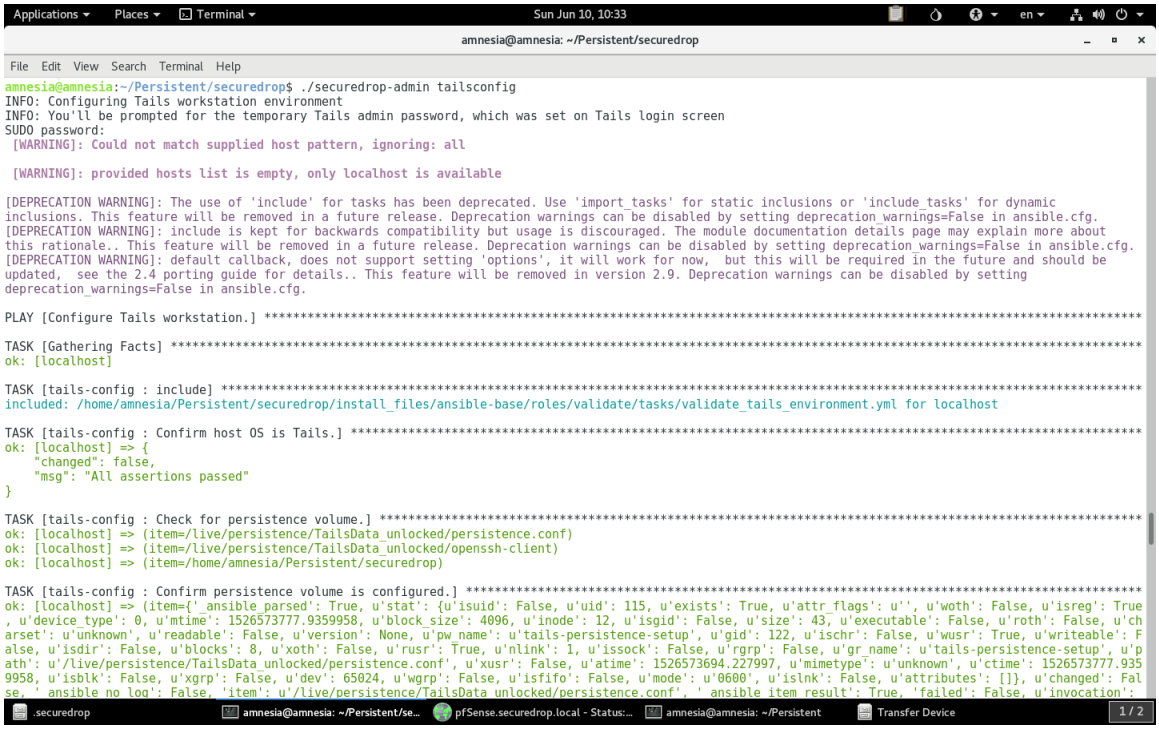

Figura 20. Configuración de Tails en "Admin Workstation"[37].

[37] SecureDrop Documentation (2018). Configure the Admin Workstation Post-Install. Recuperado de: https://docs.securedrop.org/en/release-0.6/configure_admin_workstation_post_install.html

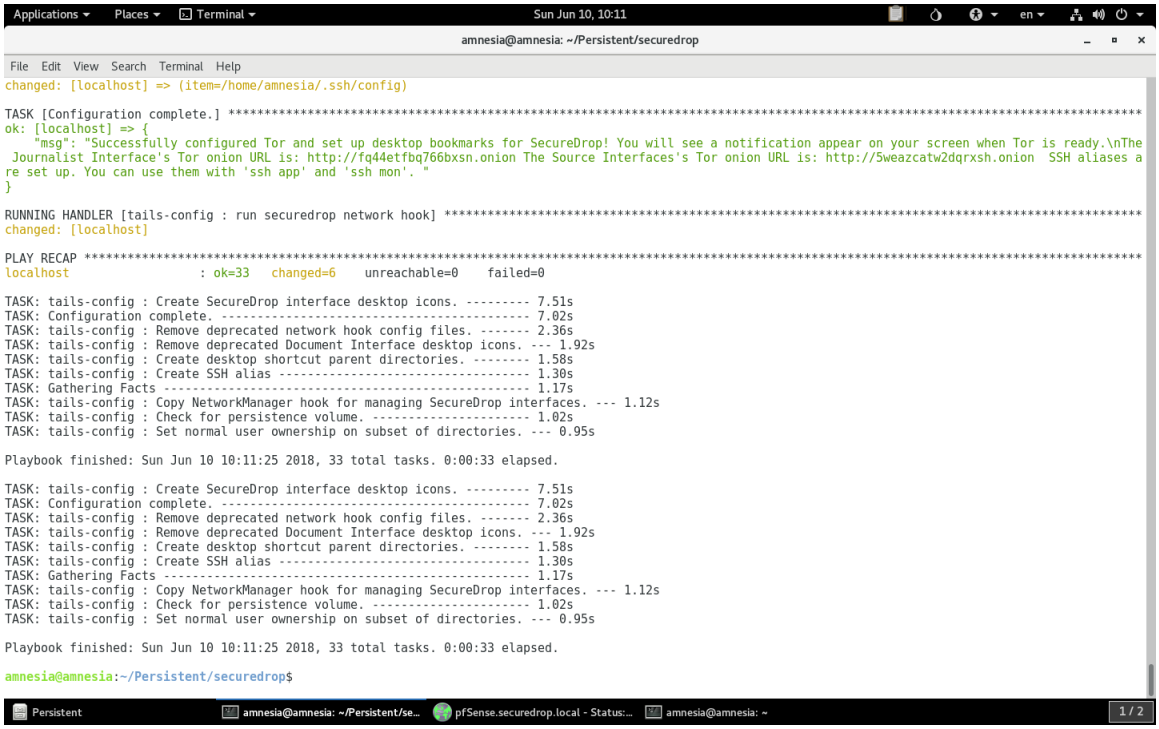

Figura 21. Finalización de la post-configuración[38].

El proceso realiza 33 cambios en el "Admin Workstation" incluyendo la generación de accesos directos a las interfaces de los informantes y de los periodistas como podemos ver en la figura 21.

Posteriormente verificamos la instalación accediendo a los sitios ocultos ATHS (Authenticated TOR Hidden Services) de nuestra instalación de SecureDrop como se muestra en la figura 22 y figura 23.

[38] SecureDrop Documentation (2018). Configure the Admin Workstation Post-Install. Recuperado de: https://docs.securedrop.org/en/release-0.6/configure_admin_workstation_post_install.html

Figura 22. Interfaz "Hidden Service" de SecureDrop para enviar denuncias.

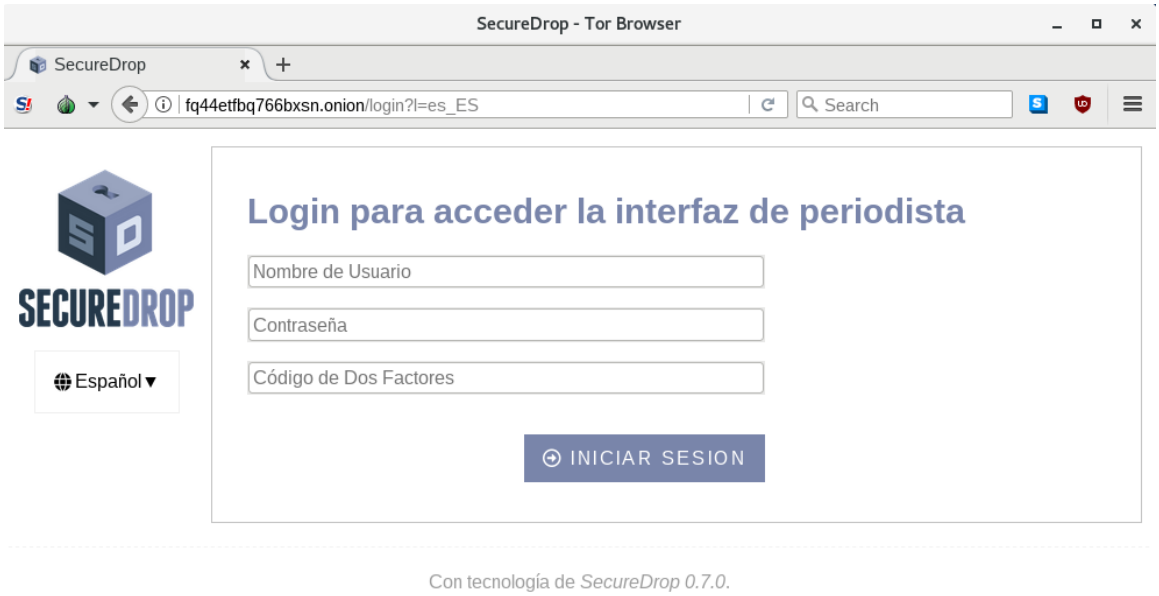

Figura 23. Interfaz de periodista como "Hidden Service" para ver denuncias.

4.1.6 Creando la cuenta de administrador en la interfaz de los Periodistas

En la “Journalist Interface” de SecureDrop se encuentran dos tipos de cuentas: cuenta de administrador y cuentas normales. Necesitamos crear una cuenta de administrador como primera cuenta de periodista, ya que esta puede agregar, borrar y cambiar las cuentas de los demás periodistas.

Realizaremos una conexión SSH al “Application Server” desde donde ejecutaremos el siguiente script que se muestra a continuación en la figura 24, para crear la cuenta de administrador.

Figura 24. Agregando a un Administrador/Periodista[39].

[39] SecureDrop Documentation (2018). Create an admin account on the Journalist Interface. Recuperado de: https://docs.securedrop.org/en/release-0.6/create_admin_account.html

El resultado será como se muestra en la Figura 18 El administrador/periodista tendrá que escanear el código QR[40] para agregarlo a su OTP[41] (Google en nuestro caso) y anotar la contraseña provista por el script.

Una vez en la interfaz de periodista, luego de habernos autenticado, veremos una ventana como en la figura 25 en donde se reciben las denuncias de los informantes.

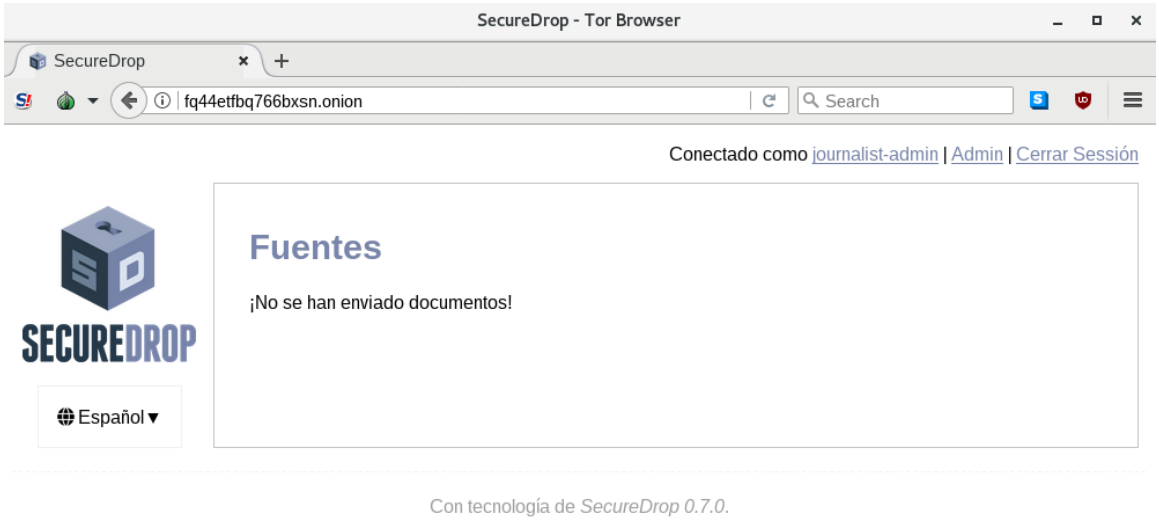

Figura 25. Interfaz de Administrador/Periodista autenticado en la consola de recepción de denuncias.

[40] Un código QR (del inglés Quick Response code, "código de respuesta rápida") es la evolución del código de barras. Es un módulo para almacenar información en una matriz de puntos o en un código de barras bidimensional.
[41] Una contraseña de un solo uso o OTP (del inglés One-Time Password) es una contraseña válida solo para una autenticación.

CAPITULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Hemos visto el uso de herramientas de seguridad como PGP y TOR y como estas han sido incorporadas en SecureDrop para proporcionar en conjunto una solución para facilitar el envío de denuncias por canales cifrados en Internet para su posterior investigación, dotando con los siguientes puntos al denunciante:

a) Integridad: Toda la información que se envía del emisor al receptor es transmitida a través del protocolo TLS de la red TOR, la integridad de la información es almacenada en el servidor de aplicación con hardening aplicado al mismo.

b) Confidencialidad: La información es enviada desde el emisor de forma anónima a través de la interfaz web utilizando el navegador TOR o preferentemente el sistema operativo TAILS desde una memoria USB, para iniciar este sistema operativo, llegando al receptor de forma cifrada, asegurando que solo el receptor podrá acceder por medio de su llave privada la información.

c) Disponibilidad: El emisor a través del navegador TOR o con una memoria USB con el sistema operativo TAILS y el navegador TOR puede acceder a cualquier computador con acceso a Internet a la plataforma y realizar una denuncia, de la misma manera el medio de comunicación tendrá disponibilidad de la información en el momento que desee accediendo a esta a través de una memoria USB con el sistema operativo TAILS y SecureDrop previamente configurados

SecureDrop, como toda herramienta de seguridad, no garantiza el 100% de seguridad y anonimato, pero ciertamente es un medio recomendado hoy en día para enviar

denuncias con la facilidad de su interfaz web, y un navegador con mayor seguridad, protegiendo también la privacidad.

Nuestro país necesita desarrollar una cultura de denuncia ciudadana por medio del uso de tecnologías que faciliten el medio seguro para garantizar la transparencia. Los ciudadanos pueden alertar situaciones irregulares de cualquier tipo, generalmente por corrupción en sus empresas o instituciones públicas.

5.2 Recomendaciones

Se recomienda que el uso de SecureDrop sea implementado en entidades que luchen por la corrupción como noticieros y periódicos en todo el país para aportar a la transparencia permitiendo que el ciudadano pudiese escoger la entidad donde enviar su denuncia sin miedo a represalias.

Se deben de crear iniciativas de ley o reformar la Ley de Especial de Delitos Informáticos y Conexos de manera que no pueda afectar el uso este tipo de tecnología, para poder dar la posibilidad a la sociedad salvadoreña de poder denunciar situaciones ilegales sin temor a represalias garantizando su anonimato a través del uso de nuevas tecnologías en El Salvador que faciliten el acceso de denuncia.

Para el funcionamiento óptimo de esta plataforma, que las denuncias recibidas y la comunicación entre el denunciante y el receptor sean anónimas, es recomendable capacitar a los medios de comunicación sobre la instalación, mantenimiento y uso de SecureDrop, TOR, TAILS y la infraestructura.

GLOSARIO

AES: Advanced Encryption Standard, también conocido como Rijndael (pronunciado "Rain Doll" en inglés), es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos.

Criptografía Asimétrica: También llamada criptografía de clave es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que recibirá el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Diffie-Hellman: El protocolo criptográfico Diffie-Hellman, debido a Whitfield Diffie y Martin Hellman (autores también del problema de Diffie-Hellman o DHP), es un protocolo de establecimiento de claves entre partes que no han tenido contacto previo, utilizando un canal inseguro y de manera anónima (no autentificada). Se emplea generalmente como medio para acordar claves simétricas que serán empleadas para el cifrado de una sesión (establecer clave de sesión). Siendo no autenticado, sin embargo, provee las bases para varios protocolos autenticados.

EFF: (EFF, por sus siglas en inglés, Electronic Frontier Foundation), es una organización sin ánimo de lucro con sede en San Francisco, Estados Unidos con el objetivo declarado de dedicar sus esfuerzos a conservar los derechos de libertad de expresión, como los protegidos por la Primera Enmienda a la Constitución de Estados Unidos, en el contexto de la era digital actual. Su objetivo principal declarado es educar a la prensa, los legisladores y el público sobre las cuestiones sobre libertades civiles que están relacionadas con la tecnología; y actuar para defender esas libertades.

FPF: (Freedom of The Press Foundation, por sus siglas en ingles FPF) aloja paquetes de instalación y actualización de SecureDrop.

FQDN: (FQDN, por sus siglas en inglés, Fully Qualified Domain Name) es un nombre que incluye el nombre de la computadora y el nombre de dominio asociado a ese equipo. Por ejemplo, dada la computadora llamada «serv1» y el nombre de dominio «bar.com.», el FQDN será «serv1.bar.com.»; a su vez, un FQDN asociado a serv1 podría ser «post.serv1.bar.com.».

GlobaLeaks: Es un software libre, de código abierto, orientado a habilitar iniciativas de plataformas para informantes. Ha sido desarrollado por el Hermes Center for Transparency and Digital Human Rights (Centro Hermes para la Transparencia y los Derechos Humanos Digitales), una ONG italiana que apoya la libertad de expresión en línea.

Man In The Middle: En criptografía, un ataque de intermediario es un ataque en el que se adquiere la capacidad de leer, insertar y modificar a voluntad. El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas y procurar que ninguna de las víctimas conozca que el enlace entre ellos ha sido violado. El ataque MITM es particularmente significativo en el protocolo original de intercambio de claves de Diffie-Hellman, cuando éste se emplea sin autenticación. Hay ciertas situaciones donde es bastante simple, por ejemplo, un atacante dentro del alcance de un punto de acceso inalámbrico sin cifrar, donde éste se puede insertar como intermediario.

Nodos OP: (Onion Proxy): Obtienen información del servicio de directorio, establecen servicios aleatorios a través de la red y manejan conexiones de aplicaciones del usuario.

Nodos OR: (Onion Router): Son enrutadores y también pueden funcionar como servicio de directorio, estos mantienen conexión TLS con otros OR.

NTP: (Network Time Protocol, por sus siglas en ingles NTP) es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable.

Open Relay: Es un servidor SMTP configurado de tal manera que permite que cualquier usuario de Internet lo use para enviar correo electrónico a través de él, no solamente el correo destinado a, o procedente de usuarios conocidos.

pfSense: Es una distribución personalizada de FreeBSD adaptado para su uso como Firewall y Router.

PGP: (Pretty Good Privacy, que por sus siglas en ingles se conoce como PGP) puede proteger el contenido de mensajes de correo electrónico, textos, y archivos de ser capturados o interceptados en Internet en tránsito a su destino.

SecureDrop: Es una plataforma de software de código abierto para la comunicación segura entre periodistas y fuentes. Originalmente fue diseñado y desarrollado por Aaron Swartz y Kevin Poulsen bajo el nombre DeadDrop. Tras la muerte de Aaron Swartz, The New Yorker lanzó la primera versión de la plataforma el 15 de mayo de 2013 bajo el nombre de Strongbox.3 Posteriormente, la Freedom of the Press Foundation se hizo cargo de desarrollo de DeadDrop bajo el nombre SecureDrop, y una versión adicional de la plataforma fue lanzada por la revista Forbes en octubre de 2013 bajo el nombre SafeSource.

SSH: (Secure Shell, en español: intérprete de órdenes seguro) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder servidores privados a través de una puerta trasera (también llamada backdoor). Por defecto se utiliza el puerto 22.

TAILS: (The Amnesic Incognito Live System, conocido en inglés como TAILS) es una distribución Linux diseñada para preservar la privacidad y el anonimato. Es la siguiente iteración de desarrollo de la distribución Incognito. Está basada en Debian GNU/Linux,

con todas las conexiones salientes forzadas a salir a través de TOR. El sistema está diseñado para ser iniciado como un Live CD o USB sin dejar ningún rastro en el almacenamiento local (por lo general, disco duro) a menos que se indique explícitamente.

TLS: TLS, por sus siglas en ingles Transport Layer Security es un protocolo criptográfico que proporciona comunicación segura por una red, comúnmente Internet.

TOR: TOR, por sus siglas en ingles The Onion Router (Enrutador de Cebolla). Es un proyecto cuyo objetivo principal es el desarrollo de una red de comunicaciones distribuida de baja latencia y superpuesta sobre internet, en la que el encaminamiento de los mensajes intercambiados entre los usuarios no revela su identidad, es decir, su dirección IP (anonimato a nivel de red) y que, además, mantiene la integridad y el secreto de la información que viaja por ella.

BIBLIOGRAFÍA

[1] ADSLZone., G. (2018). *Qué es la red TOR y cómo se usa.* Obtenido de https://www.adslzone.net/redes/privacidad/que-es-la-red-tor-y-como-se-usa/ [Accedido 12-Marzo-2018].

[2] Berret., C. (2018). *Guide to SecureDrop*. Obtenido de https://towcenter.gitbooks.io/guide-to-securedrop/content/ [Accedido 6-Enero-2018].

[3] Es.wikipedia.org. (2018). *SecureDrop*. Obtenido de https://es.wikipedia.org/wiki/SecureDrop [Accedido 3-Marzo-2018].

[4] Es.wikipedia.org. (2018). *Tor (red de anonimato)*. Obtenido de https://es.wikipedia.org/wiki/Tor_(red_de_anonimato) [Accedido 20-Enaro-2018].

[5] Foundation., E. F. (2018). *A Deep Dive on End-to-End Encryption: How Do Public Key Encryption Systems Work?* Obtenido de https://ssd.eff.org/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work [Accedido 5-Julio-2018].

[6] Foundation., F. o. (2018). *Welcome to SecureDrop's documentation!* Obtenido de https://docs.securedrop.org/en/release-0.6/index.html [Accedido 2-Diciembre-2017].

[7] Freeze., C. (2018). *The Globe adopts encrypted technology in effort to protect whistle-blowers.* Obtenido de https://www.theglobeandmail.com/news/investigations/the-globe-adopts-encrypted-technology-in-effort-to-protect-whistle-blowers/article23302598/ [Accedido 5-Marzo-2018].

[8] Pagnotta., S. (2018). *Navegación anónima en Tor: ¿herramienta para cuidadosos o para cibercriminales?* Obtenido de https://www.welivesecurity.com/la-es/2014/07/02/navegacion-anonima-tor-herramienta-cuidadosos-o-cibercriminales/ [Accedido 20-Abril-2018].

[9] Peterson., B. (2018). *As Journalists Seek Encryption, SecureDrop Proves a Challenge.* Obtenido de https://www.foliomag.com/journalists-seek-encryption-securedrop-proves-challenge/ [28-Agosto-2018].

[10] Project., T. T. (2018). *Tor: onion Service Protocol.* Obtenido de https://www.torproject.org/docs/onion-services.html.en [Accedido 4-Febrero-2018].

[11] Rights., H. C. (2018). *Welcome to GlobaLeaks's User Manual!* Obtenido de https://docs.globaleaks.org/en/latest/ [Accedido 4-Abril-2018].

[12] Salvador., A. L. (2018). *Ley Especial Contra los Delitos Iinformáticos y Conexos.* Obtenido de https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117_073646641_archivo_documento_legislativo.pdf [Accedido 20-Abril-2018].

[13] Syverson., P. (2018). *Onion Routing Brief Selected History*. Obtenido de https://www.onion-router.net/History.html [Accedido 17-Julio-2018].