UNIVERSIDAD DON BOSCO

VICERRECTORÍA DE ESTUDIOS DE POSTGRADO

TRABAJO DE GRADUACIÓN

PROPUESTA DE DESARROLLO DE UN SITIO DE "EL SALVADOR-LEAKS", UTILIZANDO EL NAVEGADOR ANÓNIMO TOR Y LA TECNOLOGÍA "GLOBALLEAKS"

PARA OPTAR AL GRADO DE MAESTRO DE:

SEGURIDAD Y GESTIÓN DE RIESGOS INFORMÁTICOS

ASESOR:

Mg. ELMER ARTURO CARBALLO RUIZ

PRESENTADO POR:

LIC. JORGE ALBERTO RAMIREZ CORLETO

ING. NELSON ALEX BAIRES SALAZAR

ING. MELVIN GERARDO FLORES

.

Antiguo Cuscatlán, La Libertad, El Salvador, Centroamérica
Julio 2017

INDICE

LISTADO DE FIGURAS Y TABLAS

Pag.

INTRODUCCIÓN

A medida que pasan los años, la tecnología se está convirtiendo en un elemento indispensable para nuestra sociedad, debido a los avances y nuevas estrategias de diseño, las soluciones informáticas contribuyen notablemente en el desarrollo de actividades, facilitando el trabajo de los usuarios de la misma, optimizando los recursos y apoyando fuertemente el logro de los objetivos estratégicos, tanto a nivel personal como institucional. No obstante, por la cantidad de información que fluye a través de las estructuras de comunicación, existen cada vez más personas interesadas en vulnerar dichos canales, con el objetivo de obtener ventajas competitivas, provocar daños al emisor o receptor, acceder a información sensible, demostrar su capacidad para saltar barreras de seguridad o inclusive, simplemente por curiosear o pasar un momento de ocio.

Es por ello, que las soluciones tecnológicas presentes y futuras, deben ir acompañadas de un esquema de Seguridad robusto, que garantice los siguientes aspectos: 1) Disponibilidad de la información, a través de una Infraestructura con diferentes niveles de protección, 2) Confidencialidad de la información, de modo que sea consultada o revisada por las personas con autorización para hacerlo e, 3) Integridad de la Información, de tal manera que se garantice que intrusos no cambien su contenido o corrompan mensajes o documentos, otro elemento importante en la seguridad es el Anonimato si bien es cierto no es considerado como uno de los pilares de la seguridad de la información este elemento nos brinda la certeza de que la identidad de la fuente de información es desconocida, esto en casos como denuncias de diversos tipos, resulta esencial para evitar represarías contra las personas o entidades que envían la información.

En el entorno cambiante de nuestra sociedad, un aspecto que está tomando protagonismo es el tema de la Transparencia, donde se obliga a las diferentes instituciones, en especial aquellas que manejan fondos públicos, a rendir cuentas ante la sociedad, estableciendo mecanismos donde se ponga a disposición de la ciudadanía información de carácter pública y oficiosa, todo con el objeto de evitar actos de corrupción que pongan en riesgo a las empresas o inclusive generen un impacto en la reputación a nivel de todo el país.

Esto obliga a que la sociedad tome un papel más protagónico en la vigilancia de las instituciones y del Estado mismo, denunciando todos aquellos actos de corrupción de los cuales tiene conocimiento, sacando a la luz aspectos de enriquecimiento ilícito o abuso en el uso de los recursos por ejemplo, dejándolos al juicio y condena de la sociedad entera. Pero debido al temor de denunciar, por causa de las represalias o de quedar en evidencia, es necesario nuevamente crear mecanismos informáticos, que permitan ejercer libremente ese derecho, garantizando privacidad y el anonimato en las denuncias realizadas.

Debido a los problemas que pueden causar hacia los denunciantes, se utiliza la seguridad informática para proteger a las fuentes de información, generando el beneficio de ayuda a causas sociales y lograr derechos fundamentales que a través de plataformas como GlobalLeaks pueden ser logrados.

OBJETIVOS

Objetivo General

Construir un prototipo de sitio web, que sea una herramienta informática combinada con tecnología TOR y GlobalLeaks, para la denuncia ciudadana anónima y genere los recursos funcionales para su puesta en servicio.

Objetivos Específicos

- Identificar la red informática más apropiada, en base a las características establecidas en la norma ISO/IEC 9126.
- Diseñar un prototipo de sitio ElSalvadorLeaks basado en GlobalLeaks, haciendo uso de diagramas de red y UML.
- Sugerir una configuración (Hardening) adecuada en los servicios de la plataforma y el servidor a fin de garantizar la seguridad en la implementación.

ANALISIS DEL PROBLEMA

Con el fin de proveer un mecanismo informático que permita a la ciudadanía en general, presentar una denuncia sobre un acto de corrupción se basará el análisis correspondiente en tres aspectos importantes:

1) Confidencialidad del documento enviado

Un aspecto importante a considerar, es la confidencialidad de los documentos que respaldan una denuncia ciudadana. En ese sentido debe proveerse un mecanismo que permita cifrar el referido documento (texto, videos, imágenes, bases de datos) al momento que se esté enviando, a fin de que sea indescifrable para aquellos personas indeseables (intrusos) que se encuentren fisgoneando entre el denunciante y el equipo de resguardo (servidor), así como del equipo de resguardo (servidor) hasta el destinatario (periodista, comunicador, etc.) a quien deba llegar la denuncia.

Además de lo anterior existe el riesgo inherente que el denunciado (persona, institución, empresa, etc) quiera saber quién fue la persona que realizó una denuncia en su contra. Es por ello que debe existir un mecanismo que garantice la privacidad del denunciante de tal forma que no pueda conocerse la identidad ni la ubicación física de dicha persona.

2) Privacidad en el envío

Para garantizar la privacidad en la comunicación, se vuelve necesaria la creación de un sitio web que permita subir documentos haciendo uso de un lenguaje de programación web, que a su vez permita usar funciones de infraestructura de llave pública (SSL), para cifrar la comunicación entre el emisor y el receptor.

3) Anonimato

Es muy importante que el usuario que realiza la denuncia, tenga garantía de su identidad se mantendrá a salvo, a fin de evitar su relación con el acto ilícito publicado.

¿Por qué se vuelve importante proteger el contenido de los documentos producto de la denuncia y al emisor mismo? Porque al final del proceso existe la posibilidad de que intrusos puedan ver la información contenida e incluso modificar su contenido. Asimismo, estarán interesados en conocer al individuo que efectuó el envío correspondiente. Estos intrusos pueden ser el mismo proveedor de los servicios de internet, organismos gubernamentales de un “x” país, organizaciones internacionales, entre otros.

Para explicar mejor este problema se utiliza el método de la caja negra, considerando que existen entradas, un proceso interno (caja negra) y las salidas:

ENTRADAS	PROCESO	SALIDAS
Origen Conocido: **Una dirección IP real que puede ser detectada e identificado su origen geográfico, considerando que existe algún intruso que tenga control sobre el canal de comunicación. La dirección IP puede posteriormente ser vinculada a un servicio asociado a una persona natural o jurídica.**		Origen Anónimo: **Una dirección IP que no sea la IP real de origen, de tal forma que aunque un intruso tenga control sobre el canal de comunicación, no pueda identificar el origen real de esta, y por lo tanto no pueda vincular la comunicación a ninguna persona natural o jurídica.**
Documento normal: **Un documento que puede ser leído total o parcialmente usando el software de lectura multimedia o de lectura de texto.**		Documento cifrado: Un documento que no puede ser leído total ni parcialmente, sino solamente por el destinatario que posee autorización para ello.

ALCANCE DEL PROYECTO

Este proyecto está enfocado en el desarrollo de una plataforma web de denuncia ciudadana que asegure el anonimato de las personas que la realicen, permitiendo subir documentos, archivos, videos de evidencia con una llave pública (de la entidad receptora de la denuncia) de tal forma que sean almacenados cifrados en un contenedor temporal y solo puedan ser vistos por la persona o institución de destino.

ALCANCE:

Se hace uso del navegador TOR y su red de enrutado anónimo para evitar comprometer la identidad/seguridad de aquellas personas o instituciones que realicen la denuncia.

Se espera utilizar plataforma de código abierto de denuncia ciudadana de irregularidades con características como seguridad, anonimato y resistente a la censura.

LIMITANTES:

En este proyecto se desarrolla un prototipo funcional de una plataforma de denuncia ciudadana anónima, el cual se limita a mostrar como la plataforma es operada y configurada tanto del lado de los denunciantes como de los suscriptores los cuales reciben la información.

El proyecto no se basa en la implementación en una empresa o institución en específico. Sin embargo puede ser aplicado en instituciones relacionadas al periodismo objetivo, en instituciones educativas, instituciones de gobierno, etc. Esto se fundamenta ya que la plataforma GlobalLeaks permite la adaptación a diferentes casos de uso debido a su diseñado como framework (Rights, 2016).

Al ser implementado esta plataforma, la información que se recibe debe ser investigada y su validez como prueba se verá limitado a las leyes del país y como sus ejecutores la interpreten.

JUSTIFICACIÓN DEL PROYECTO

En la actualidad hay organizaciones con mucho poder que destinan importantes recursos económicos para mantener y manejar oculta información del conocimiento público. También existen negocios que proveen aspectos ilegales como venta de estupefacientes, venta de armas, pornográfica infantil, foros de delincuencia y otros contenidos ilegales e incluso de gobiernos con noticias de disidentes que buscan en el anonimato una salida a la represión, datos financieros y bases de datos con información clasificada. A la vez existen personas motivadas con conciencia y moral que están dispuestos a denunciar abusos de estas organizaciones, violaciones a los derechos humanos, corrupción, y situaciones injustas. Son personas que cuentan con bases de datos, notas, reportes, videos, audios, fotografías, entre otros que revelan estos secretos.(Assange J,2010)

Si este tipo de información sale a la luz pública puede contribuir a que hayan cambios positivos, pero existe un gran riesgo para los individuos involucrados: presiones políticas, demandas legales, pérdida de su trabajo, perdida de su reputación y hasta atentados a su integridad física y de sus familias en el peor de los casos. De ahí la importancia del anonimato en las denuncias ciudadanas. El presente proyecto tiene una gran importancia ya que trata sobre una de las formas más seguras de navegar anónimamente la cual es el navegador y la red Tor, y su uso para proteger el anonimato de las personas que realizan denuncias. Esta es una de las aplicaciones actuales de la criptografía: la protección de privacidad legítima.

La razón principal de porque se debe invertir tiempo y recursos en este proyecto radica en que se contaría con una plataforma segura y anónima para denunciar eventos de corrupción tanto en el ámbito de instituciones públicas como de empresas privadas, contando con la capacidad de subir, a dicha herramienta, la evidencia digital que sustente cada caso. En última instancia se contaría con una opción adicional para someter a la opinión pública información que afecte a todos los salvadoreños, esto puede traer el beneficio de consolidar instituciones públicas y empresas privadas más transparentes y conscientes de los derechos de los salvadoreños. Un ejemplo de éxito en este tipo de plataformas es el caso de Mexicoleaks, que cuenta con una alianza estratégica con algunos medios de comunicación y periodistas independientes, y permite a los ciudadanos mejicanos realizar sus denuncias anónimas.

CAPÍTULO I
MARCO TEÓRICO

1.1 Reseña de Red Tor

Históricamente la red TOR (TheOnionRouter) nace en 1995 como un proyecto de la NRL (Laboratorio de Investigación Naval de los Estados Unidos), (Molleapaza Calamani, 2014) esto con el objetivo de proteger los canales de comunicación militares de escuchas no autorizadas y análisis del tráfico, para conseguir una comunicación privada y anónima. En 1997 el proyecto es financiado por DARPA (agencia de defensa de investigación de proyectos avanzados de los Estados Unidos). En el año 2002 es lanzada la versión alpha y en 2004 es presentada la nueva versión de la herramienta, es en este mismo año cuando la NRL libera el código fuente de TOR bajo una licencia libre, y a partir de entonces la EFF (Electronic Frontier Foundation) continua con el financiamiento del proyecto.

La red Tor en la actualidad (The Onion Routing), una red abierta que le permite a los usuarios defenderse contra el análisis de tráfico que realizan algunas instancias gubernamentales sobre Internet, y que es una forma de vigilancia que amenaza la libertad personal, la privacidad, la confidencialidad en los negocios, así como las relaciones y la seguridad del Estado (Tor, 2014). (Amaro López, 2015)

La red funciona a partir de un conjunto de organizaciones e individuos que donan su ancho de banda y poder de procesamiento. Según información obtenida de los documentos de alto secreto filtrados por Edward Snowden en 2013, la Agencia de Seguridad Nacional de ESTADOS UNIDOS (NSA) habría, supuestamente, conseguido "romper" Tor y así descubrir las identidades de los usuarios que buscan el anonimato [2]. Actualmente la versión 6 de Tor liberada en 2016 cubre los bugs de seguridad identificados en las versiones anteriores.

1.2 Funcionamiento de la red Tor.

Es importante listar los elementos necesarios para el funcionamiento de la red TOR: Entidades, servicios de directorios, esquema de funcionamiento, punto de encuentro, servicios ocultos, células, claves de OR y algoritmos de cifrado (Es.wikipedia.org, 2016). Debido a que los datos están alojados exactamente en la misma red superficial o clara, la diferencia de que los caminos elegidos por esos datos no son predecibles y se cifran.

Por lo tanto la red TOR direcciona el tráfico de internet por distintos servidores que ocultan la información del usuario, cualquier actividad de monitoreo del usuario dentro de la red Tor es difícil de rastrear porque los datos se cifran varias veces y pasan a través de varios nodos repetidores Tor y de la red.

1.2.1 Entidades de red TOR

TOR está constituida por una serie de nodos que se comunican mediante el protocolo (Transport Layer Security (TLS)) [1]sobre protocolo (TCP/IP) manteniendo así secreta e íntegra, sin modificaciones externas, la información desde un nodo a otro. Hay dos tipos de entidades:

Entidad 1: **Nodos OR o simplemente OR (del inglés ''Onion Router''):** Funcionan como encaminadores y en algunos casos además como servidores de directorio (DNS) de una especie de servicio de mantenimiento. Los nodos OR mantienen una conexión TLS con cada uno de los otros OR. Las conexiones OR-OR no son nunca cerradas deliberadamente salvo cuando pasa cierto tiempo de inactividad. Cuando un OR comienza o recibe nueva información de directorio él intenta abrir nuevas conexiones a cualquier OR que no esté conectado.

Entidad 2: **Nodos OP o simplemente OP (del inglés ''Onion Proxy''):** Los usuarios finales ejecutan un software local que hace la función de nodo OP y que su función es obtener información del servicio de directorio, establecer circuitos aleatorios a través de la red y manejar conexiones de aplicaciones del usuario. Los OP aceptan flujos (Transmission Control Protocol(TCP)) de aplicaciones de usuarios y las multiplexa a través de la red OR's. Las conexiones OR-OP no son permanentes. Un OP debería cerrar una conexión a un OR si no hay circuitos ejecutándose sobre la conexión y ha vencido cierto temporizador.

1.2.2 Servicio de directorio

El servicio de directorio es en realidad un grupo de OR’s confiables, toda la información que entra a los directorios son protegidas criptográficamente con firmas digitales, esto quiere decir que solo las firmas registradas de OR’s confiables pueden proporcionar información a la base de datos del directorio. Es así como aparece un nuevo OR este debe ser registrado y firmado en los OR’s confiables para que pueda acceder a la base de datos del directorio.

Esto es un método para proteger de ataques agregando nodos OR’s que no son confiables a la red, si añadimos muchos nodos que no están registrados y no existiera este tipo de seguridad, la base de datos del directorio fallaría, sería un hueco de seguridad ya que puede ser que un OR no confiable este agregado en esa base de datos y este OR proporcione información a terceros y rompa el concepto de privacidad de la red Tor.

---

[1] Por sus siglas en inglés Transport Layer Security (Seguridad en la Capa de Transporte), un protocolo criptográfico empleado en redes.

1.2.3 Esquema de funcionamiento Interno red TOR

Tor sólo permite anonimizar tráfico TCP. Las aplicaciones acceden a la red TOR a través del interfaz SOCKS[2] lo cual significa que toda aplicación con soporte SOCKS puede usar TOR para realizar comunicaciones anónimas sin necesidad de modificaciones adicionales. El cliente Tor recibe tráfico SOCKS desde aplicaciones y luego, de forma transparente, se encarga de comunicarse con los routers de la red Tor para enviar las peticiones y posteriormente se devuelven los resultados.

SOCKS es un protocolo que facilita el enrutamiento de paquetes que se envían entre un cliente y un servidor a través de un servidor proxy. Según la pila de protocolos OSI[3]está en el nivel 5 (sesión). Según la pila de protocolos IP está en la capa de aplicación. En los primeros intentos de usar encaminamiento de cebolla se requería un proxy de aplicación para cada protocolo de aplicación soportado. Esto conllevaba mucho trabajo y provocaba que algunos proxys no fueran escritos nunca y por tanto algunas aplicaciones nunca fueron soportadas. Tor usa SOCKS para soportar la mayoría de programas basados en TCP sin hacer ninguna modificación.

Observar que cuando se navega por internet hacemos dos tipos de peticiones:

- Peticiones DNS para que el servidor de DNS que nos diga la dirección IP de una URL[4]
- Peticiones HTTP[5] a las direcciones IP del servidor web que aloja la información.

Si no se pasa por Tor las búsquedas con DNS que hacen los navegadores, pueden ser un problema de privacidad ya que si las peticiones se mandan directamente a través de la red regular un atacante podría deducir qué sitios se están visitando a través de Tor ya que antes de navegar por ellos se pregunta por DNS que IP tienen. Por tanto es necesario redirigir el tráfico de DNS por la red Tor.

Algunas aplicaciones convierten directamente el tráfico del protocolo la capa de aplicación en tráfico SOCKS. Por ejemplo Firefox permite convertir tanto el tráfico DNS como el HTTP a SOCKS y enviárselo al cliente Tor. Otras aplicaciones necesitan redirigir el tráfico del protocolo de la capa de aplicación hacia un proxy que realice la conversión al protocolo SOCKS.

---

[2] SOCKS es un protocolo de Internet que permite a las aplicaciones Cliente-servidor usar de manera transparente los servicios de un firewall de red. SOCKS es una abreviación de "SOCKetS".

[3] Fue desarrollado en 1980 por la ISO, una federación global de organizaciones que representa aproximadamente a 130 países. El núcleo de este estándar es el modelo de referencia OSI, una normativa formada por siete capas que define las diferentes fases por las que deben pasar los datos para viajar de un dispositivo a otro sobre una red de comunicaciones.

[4] URL (Uniform Resource Locators) o Localizadores de Recursos son direcciones únicas que sirven para localizar una página Web y sus contenidos en un servidor de la red.

[5] Hypertext Transfer Protocol o HTTP (en español protocolo de transferencia de hipertexto) es el protocolo de comunicación que permite las transferencias de información en la World Wide Web.

El esquema de funcionamiento interno que se desarrolla en figura 1 se describe a continuación:

- 1. A partir de la información obtenida de su configuración y del servicio de directorio el OP decide un circuito por el que van a circular los paquetes. Por defecto el circuito tiene 3 nodos OR.
- 2. El OP negocia, usando un enfoque telescópico[6], las claves de cifrado necesarias con cada OR del circuito para proteger sus datos en todo el camino antes de realizar transmisión alguna. La obtención de las claves simétricas (AES-128), una para cada sentido de comunicación (Kf<-forward key, Kb<-backward key), se realiza a partir del protocolo de establecimiento de claves Diffie-Hellman[7] para obtener una clave compartida y a partir de ella derivar las dos claves simétricas. El circuito es construido desde el punto de entrada (usuario) de la siguiente forma: 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 de cebolla del host que recibe el dato.
  3. A continuación cifra el paquete que contiene la clave para el último OR del circuito,
- 4. A continuación hace lo propio del penúltimo, hace lo mismo con todos los nodos hasta hacer lo propio con el paquete para el primer nodo.
- 5. Envía el paquete resultante al primer nodo del circuito. Observar que el paquete construido con este proceso se puede considerar como un paquete envuelto en varias capas de cifrado. Por eso se usa la metáfora de la cebolla para describir este tipo de método de encaminamiento (ver apartado 1.2.4 encaminamiento de cebolla).
- 6. El primer OR quita 'su' capa de la cebolla y envía el paquete al siguiente nodo
- 7. Según va llegando el paquete a cada OR éste pela la capa externa. De esta forma ningún OR puede hacerse con la imagen completa del circuito ya que sólo conoce los OR/OP anterior y posterior.

Como terminología se llama 'exit server' o 'exit node' al último servidor del circuito (y por tanto el único que se comunica con el destino), el primer OR se le llama 'entry node' (único que se comunica con el origen de la comunicación) y al resto de nodos se les llama middle-node.

Podemos observar que la forma en la que se establecen las claves y todas estas capas de cebolla que se construyen con ellas permiten que la información permanezca secreta mientras va circulando por el circuito de nodos OR. 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 (perfect forward secrecy).

---

[6] Tor y el enrutamiento cebolla realizan una construcción incremental e interactiva del circuito, a la que llaman enfoque telescópico

[7] Ver Glosario - Página 84

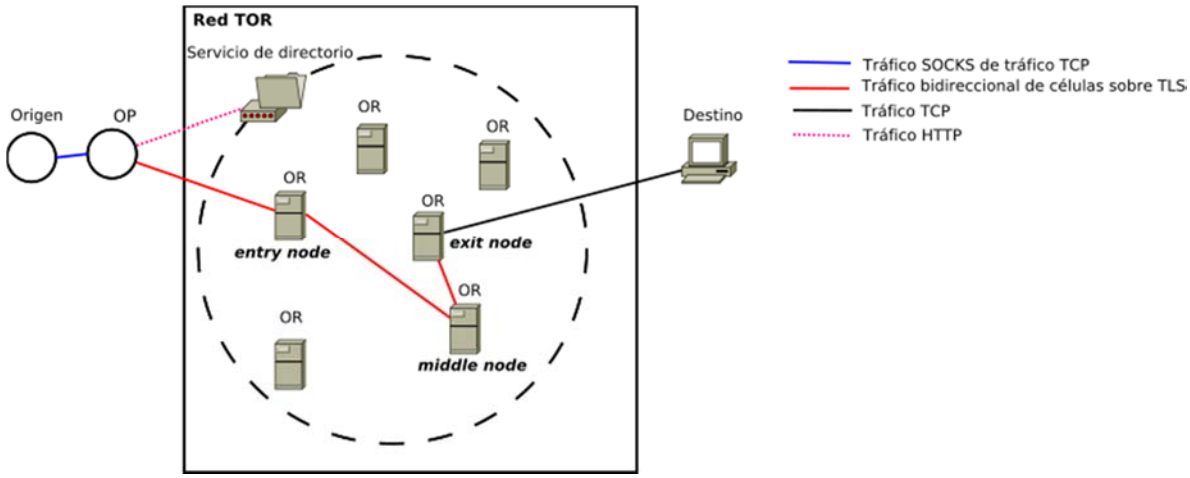


Figura 1 - Esquema de funcionamiento de interno Tor.

1.2.4 Esquema de funcionamiento de conexión a TOR

Tor ayuda a reducir los riesgos de análisis de tráfico simple y sofisticado mediante la distribución de sus transacciones en varios lugares en Internet, por lo que ningún punto único puede vincular a su destino. La idea es similar a usar una ruta tortuosa, difícil de seguir para deshacerse de alguien que te persigue - y luego borrar periódicamente tus huellas. En lugar de tomar una ruta directa desde la fuente hasta el destino, los paquetes de datos en la red Tor toman una ruta aleatoria a través de varios Nodos(reguladores o interruptores) que cubren sus pistas de modo que ningún observador en un solo punto puede decir de dónde vienen los datos o hacia dónde van.

Para crear una ruta de red privada con Tor, el software o cliente del usuario construye de forma incremental un circuito de conexiones cifradas a través de Nodos en la red. El circuito se extiende un salto a la vez, y cada relé a lo largo del camino sabe sólo qué relé le dio datos y a qué relé está dando datos. Ningún relé individual conoce la ruta completa que ha tomado un paquete de datos. El cliente negocia un conjunto separado de claves de cifrado para cada salto a lo largo del circuito para asegurar que cada salto no pueda rastrear estas conexiones a medida que pasan. Ver figura 2

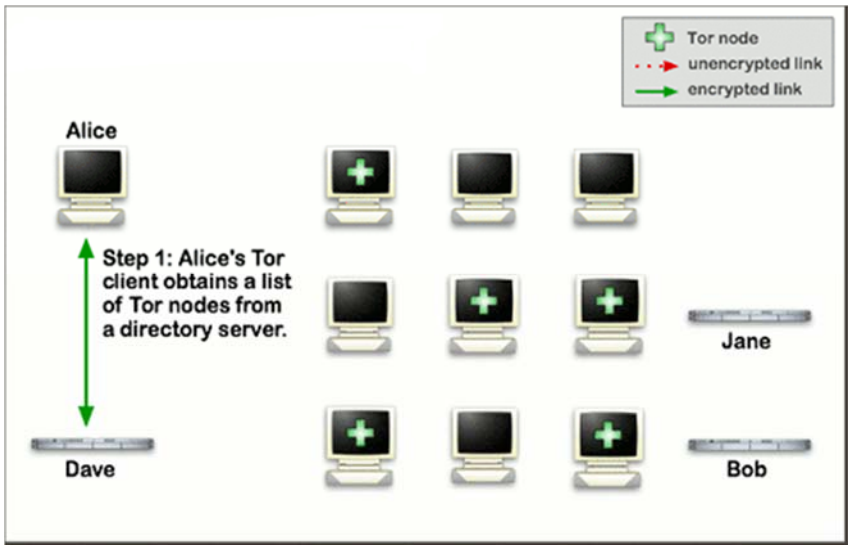


Figura 2 - Conexión a Red Tor, Listado de nodos activos de la red TOR

Una vez que se ha establecido un circuito, se pueden intercambiar muchos tipos de datos y se pueden desplegar varios tipos diferentes de aplicaciones de software a través de la red Tor. Debido a que cada relé no ve más de un salto en el circuito, ni un intruso ni un relé comprometido puede utilizar análisis de tráfico para vincular la fuente y el destino de la conexión. Tor sólo funciona para los flujos TCP y puede ser utilizado por cualquier aplicación con soporte SOCKS[8]. Ver figura 3

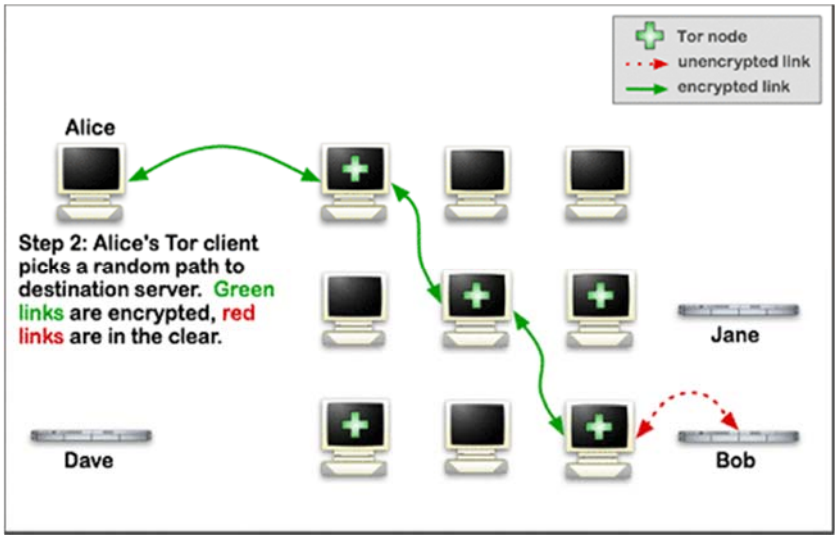


Figura 3 - Conexión a Red Tor, Establecimiento de un circuito en la red TOR.

[8] SOCKS es un protocolo de Internet que permite a las aplicaciones Cliente-servidor usar de manera transparente los servicios de un firewall de red. SOCKS es una abreviación de "SOCKetS". Ver funcionamiento interno de red TOR 1.2.3

Para mayor eficiencia, el software Tor utiliza el mismo circuito para conexiones que ocurren dentro de los mismos diez minutos aproximadamente. Las solicitudes posteriores reciben un nuevo circuito, para evitar que las personas vinculen sus acciones anteriores a las nuevas.

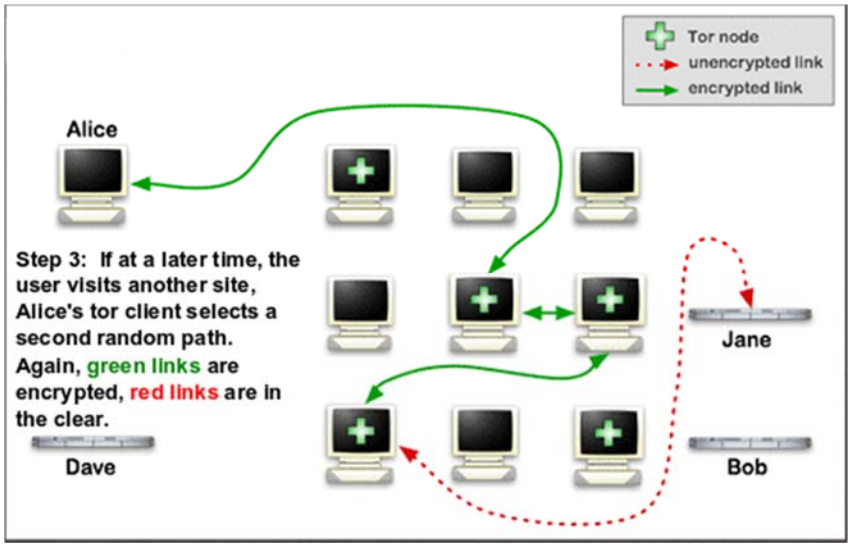


Figura 4 - Conexión a Red Tor, Selección de nuevas rutas

Es importante hacer énfasis que la Red Tor no puede resolver todos los problemas de anonimato. Se centra sólo en proteger el transporte de datos. Es necesario utilizar el software de soporte específico del protocolo si no desea que los sitios que visite identifiquen su información de identificación. Por ejemplo, puede utilizar el Navegador Tor mientras navega por la Web para retener cierta información sobre la configuración de su computadora.

Además, para proteger el anonimato, se recomienda. No proporcionar nombres u otra información reveladora en formularios web. Se debe tener en cuenta que, al igual que todas las redes de anonimato que son lo suficientemente rápidas para la navegación web, Tor no proporciona protección contra ataques de sincronización de extremo a extremo: Si el atacante puede ver el tráfico que sale de su computadora y también el tráfico que llega a su destino, puede utilizar el análisis estadístico para descubrir que son parte del mismo circuito.

1.2.5 Puntos de encuentro red TOR

La idea de los puntos de encuentro, denominados por las siglas RP (del inglés *Rendezvous Points*), es, en lugar de explícitamente enviar un paquete a un destino, establecer un punto de encuentro que actúe como nivel de indirección. De esta forma desacoplamos el acto de enviar del acto de recibir. Cada extremo de la comunicación envía sus mensajes a ese punto de encuentro y desde ahí son enviados a donde corresponda usando circuitos que esconden la localización del destino.

1.2.6 Servicios Ocultos red TOR

Los servicios que ocultan la localización (por ejemplo, la dirección IP) de quien provee el servicio (Ej. un servicio web accesible sólo desde la red de encaminamiento de cebolla) se les suele llamar servicios de localización oculta (en inglés location-hidden services) o simplemente servicios ocultos (en inglés hidden services).

Los servicios ocultos tratan de una de las características más interesantes que proporciona Tor para ofrecer servicios en máquinas de forma anónima. Estos pueden ser de cualquier tipo siempre y cuando se basen en protocolos: TCP: SSH, HTTP, IRC, SMB, FTP, etc. Es decir, para un cliente que accede a un servicio oculto realmente no accede a la propia máquina en sí (ya que se desconoce su dirección IP real), sino que accede únicamente al servicio publicado por la máquina.

Aunque los servicios ocultos hayan ganado popularidad por la existencia de actividades ilegales como el tráfico de drogas, existen servicios totalmente legítimos que buscan la libertad de expresión y evitar la censura.

Lógicamente los servicios ocultos solo están disponibles a través de Tor. Sin embargo, gracias al proyecto Tor2web[9], también están disponibles desde Internet sin necesidad de conectarse a la red Tor. No obstante, cabe destacar que el cliente pierde su anonimato al acceder a un servicio oculto de esta manera.

1.2.7 Células red TOR

En el funcionamiento de la red Tor es importante identificar las células de control y las células de transmisión una vez que se establece la conexión TLS, las entidades se envían paquetes de información estructurada llamadas células. Su formato es el siguiente:

- circID.- Es el identificador de circuito y especifica el circuito a el que se refiere la célula. Cada circuito tiene un CircId distinto para cada OR y OP del circuito.
- CMD.- Indica el comando que especifica el significado de la célula. Atendiendo al tipo de comando (valor de CMD) hay 2 tipos de células: Células de control y Células de transmisión.

Células de control: Las células de control (en inglés control cell) son siempre interpretadas por el nodo que las recibe y permiten controlar la comunicación. Comandos que tienen estas células:

- CREATE : para crear circuito
- CREATED : para indicar que se ha cerrado el circuito
- DESTROY : destruir circuito
- CREATE_FAST : para crear un circuito reaprovechando operaciones de clave pública existentes)
- CREATED_FAST : para indicar que se ha creado el circuito de una manera rápida

[9] Tor2web es el software detrás de la Red Tor2web, una red de proxis distribuida globalmente cuyo objetivo es crear un puente entre Internet y los servicios ocultos de Tor.

Células de transmisión: Las células de transmisión son usadas para la comunicación entre el OP y cualquiera de los OR del circuito, normalmente el exit node. En este tipo de células el formato tiene campos que forman parte de la carga útil (PAYLOAD):

- Relay command.- El el subcomando RELAY que indica el funcionamiento de la celda.
- Hay tres tipos de subcomandos relay:
  - forward: son enviados desde el OP origen del circuito.
  - backward: son enviados desde los OR del circuito al OP origen.
  - ambos: pueden funcionar como forward o como backward.

- RELAY_BEGIN: de tipo forward.
- RELAY_DATA: de tipo forward o backward.
- RELAY_END: de tipo forward o backward.
- RELAY_CONNECTED (código 4): de tipo backward.
- RELAY_SENDME: de tipo forward o backward. A veces se usa para funciones de control (streamID=0).
- RELAY_EXTEND: de tipo forward. Se usa para funciones de control (como veremos streamID=0).
- RELAY_EXTENDED: de tipo backward. Se usa para funciones de control (streamID=0).
- RELAY_TRUNCATE: de tipo forward. Se usa para funciones de control (streamID=0).
- RELAY_TRUNCATED: de tipo backward. Se usa para funciones de control (streamID=0).
- RELAY_DROP: de tipo forward o backward. Se usa para funciones de control (streamID=0).
- RELAY_RESOLVE: de tipo forward.
- RELAY_RESOLVED: de tipo backward.
- RELAY_BEGIN_DIR: de tipo forward.

Tabla 1: Posibles subcomandos que se usan en la célula de transmisión:

- **Recognized:** campo que junto con el campo digest permite identificar si la celda es para ser procesada localmente.
- **StreamID:** es el identificador de flujo. De esta forma se permite que varios flujos puedan ser multiplexados en un solo circuito. Este campo permite identificar el stream al que nos referimos entre los múltiples streams del circuito. Es seleccionado por el OP y permite al OP y al exit node distinguir entre múltiples streams en un circuito. Las células que afectan al circuito entero en lugar de a un streamID particular tienen este campo a 0 y se pueden considerar como de control.
- **Digest:** Permite el control de integridad extremo a extremo (end-to-end integrity checking). 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 originados desde este nodo del circuito (sólo conocidos por el origen y el destino ya que van cifrados.
- **Length:** Indica el número de bytes del campo DATA que contiene carga útil real. El resto del campo irá rellenado por bytes a NULL.

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. Observar que el campo Recognized permite, de una forma muy rápida, descartar ciertas células como candidatas a estar completamente descifradas.

La diferencia principal entre las células de control y las de transmisión es que las primeras pueden ser leídas por cualquiera mientras que las segundas solo por un nodo concreto. Por ejemplo: cuando se envía una célula destroy el OP la envía al primer OR este la recibe, cierra todos los flujos y la manda al siguiente. Así hasta llegar al final. Para células de transmisión el OP asigna el digest y después encripta la célula con cada una de las claves de los nodos OR. Como el digest está encriptado con distintos valores en cada paso solo el nodo objetivo podrá recibir el valor adecuado y por tanto hacer la función que le indique la célula. Cuando un nodo OR recibe una célula comprueba si al decifrar la célula con su clave da un código correcto de digest, sino es así comprueba el siguiente nodo, cambia el valor de CircID de la célula por el del siguiente nodo.

1.2.8 Claves de Onion Router (OR)

Cada OR[10] tiene asociados una serie de pares de claves pública/privada:

- Una clave larga de identidad (en inglés *Identity Key*) que sirve sólo para firmar información (Ej: descriptor de las capacidades del OR o información de directorio cuando actúa como servidor de directorio) y certificados, y es usado para permitir identificación. Para denotar la clave de identidad del nodo OR n usamos PKORn_ID
- Una clave mediana de enrutamiento de cebolla (en inglés Onion Key) que sirve para cifrar las peticiones de establecimiento de circuito (CREATE) para negociar las claves efímeras. Las claves viejas deben ser aceptadas durante al menos una semana después de que haya sido cambiada para dar tiempo a que todo haya sido actualizado. Para denotar la onion key del nodo OR n usamos PKORn_OK
- Una clave pequeña de conexión (en inglés Connection Key) usada en el handshake TLS. Esta clave 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[11] del TLS. El certificado de la clave identificación está firmado por la clave de

[10] Nodos OR o simplemente OR (del inglés Onion Router): Funcionan como encaminadores y en algunos casos además como servidores de directorio (DNS) de una especie de servicio de mantenimiento.

[11] Handshaking es una palabra inglesa cuyo significado es apretón de manos y que es utilizada en tecnologías informáticas, telecomunicaciones, y otras conexiones.

identificación. El certificado de la clave de identificación está autofirmado. Esta clave debería cambiarse frecuentemente, al menos una vez al día.

1.2.9 Esquema de funcionamiento red TOR

Se lista los diferentes algoritmos utilizados por 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
  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[12] 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[13]con claves de 1024 bytes y exponente fijo 65537. Usa como esquema de relleno OAEP-MGF1 (Optimal Asymmetric Encryption Padding) con SHA-1 usado como función resumen
- Como función resumen usa SHA-1
- Para establecimiento de claves usa DH (Diffie-Hellman)[14] con g=2 y para p usamos el primo seguro de 1024 bits obtenido de RFC 2409 con valor hexadecimal:

---

[12] Advanced Encryption Standard (AES), 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.

[13] River, Shamir, Adleman, (**RSA)** es un sistema criptográfico de clave pública desarrollado en 1977. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.

[14] 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).

1.2.10 Encaminamiento de la cebolla.

Es equivalente a una red de mixes, pero en el contexto de enrutamiento basado en circuitos. En vez de enrutar cada paquete separadamente, el primer mensaje lo que hace es abrir un circuito, etiquetando una ruta. Cada mensaje que tiene una etiqueta en particular se enruta por un camino predeterminado. Finalmente, un mensaje se envía para que cierre o clausure un camino. Con frecuencia se hace referencia a flujo anónimo como la información que viaja por estos circuitos.

Su objetivo es dificultar la tarea al análisis de tráfico, uno de los tipos de ataques más conocidos. Este sistema procura proteger la no relacionabilidad de dos participantes que se comunican a través de terceras partes, y procura proteger la identidad de las partes comunicantes. En vista de que las redes ISDN[15] son difíciles de implementar en Internet, lo que procuro OR es adaptar esta idea distribuyendo la red anónima y adaptándola para que se ejecute en el tope del modelo TCP/IP.

El primer mensaje enviado en la red se cifra en capas, que pueden ser descifradas en una cadena de enrutadores cebolla (onion routers) los cuales utilizan sus respectivas claves privadas. El primer mensaje tiene el material que debe ser compartido entre el emisor y los enrutadores, también las etiquetas y la información de direccionamiento del próximo nodo. Tal como sucede en los mixes de David Chaum,[16] de esconder la relación entre el origen y el destino de una información encapsulando los mensajes en capas de criptografía de clave pública. Obtiene su nombre por su composición en capas de cifrado superpuesta en la comunicación entre nodo y nodo, parecido a las capas de una cebolla.

Los datos que circulan por la red en un circuito establecido están cifrados con claves las simétricas[17] de los enrutadores. Las etiquetes se utilizan para indicar a cual circuito pertenece cada paquete. Se utilizan etiquetas diferentes para los distintos enlaces, asegurando así la no relacionabilidad, y además las etiquetas de los enlaces también se cifran utilizando una clave que se comparte entre los pares de enrutadores OR. Lo anterior previene los ataques de observadores pasivos que puedan determinar cuáles paquetes pertenecen al mismo flujo anónimo, pero no le oculta la información a un enrutador que pueda ser subversivo. OR es susceptible a un conjunto de ataques, tal como el ataque de tiempo. Esto se debe a que los patrones pudiesen ser analizados por un atacante en ausencia de un gran volumen de tráfico pesado.

---

[15] RDSI (Red Digital de Servicios Integrados, en ingles ISDN) como una evolución de las Redes actuales, que presta conexiones extremo a extremo a nivel digital y capaz de ofertar diferentes servicios.

[16] David Lee Chaum inventor muchos protocolos criptográficos y fundó la Asociación Internacional para la Investigación Criptográfica (CAII), que actualmente organiza conferencias académicas en la investigación de criptografía.

[17] Ver Glosario – Página 84

Tor es una red superpuesta sobre internet que está distribuida para desarrollo, formación y proporcionar un despliegue de una red anónima para las comunicaciones en baja latencia. Está diseñada para conseguir que el encaminamiento de los mensajes entre los hosts mantenga su privacidad y no se releve la información de los usuarios. Tor se basa en el establecimiento de un sistema virtual utilizando un circuito por capas, un circuito de enrutamiento de cebolla, de estudio del anonimato de una red de comunicaciones tipo TOR hecho, es conocido como la segunda generación de enrutamiento de cebolla. Antes de describir más profundamente el sistema TOR, enunciaremos los principios fundamentales del enrutamiento de cebolla para tener una comprensión de las bases de TOR. (Goldschlag, Reed, & Syverson, 1999)

A manera de ejemplo primero, el ordenador A, que quiere enviar el mensaje a B, calcula una ruta aleatoria al destino pasando por varios nodos intermedios. Después, consigue las claves públicas de todos los nodos utilizando un servicio de directorios.

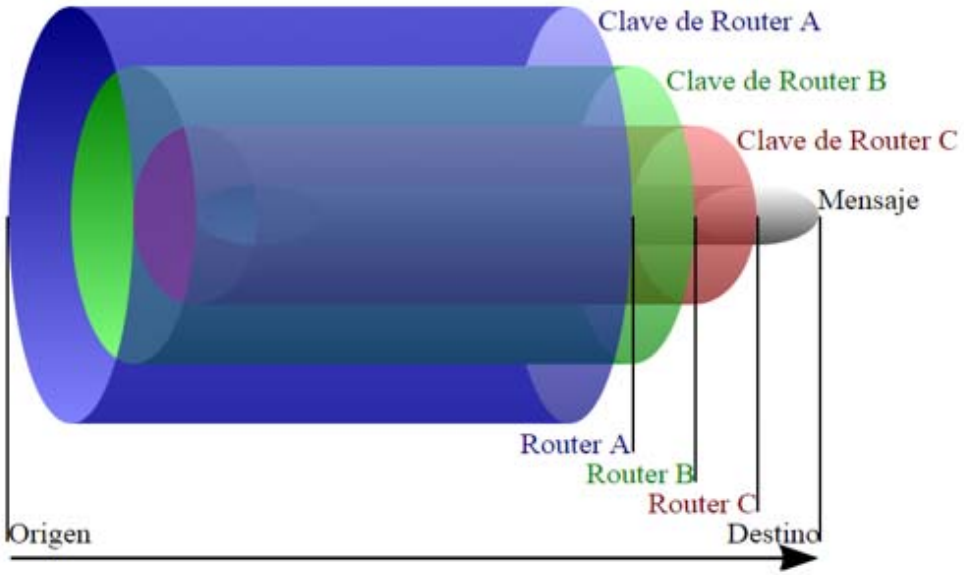


Figura 5 – Estructura de la transmisión de los datos con encaminamiento cebolla.

El mensaje se encuentra protegido por varias capas (cifrados) para cada uno de los nodos. El proceso se realiza con todos los nodos de la ruta, cuando este termina, el ordenador A conecta con el primer nodo de la ruta y envía el paquete. Este nodo lo descifra, y sigue las instrucciones que ha descifrado para enviar

el resto del paquete al nodo siguiente. Éste descifrará de nuevo y volverá a enviar al siguiente, y así sucesivamente. Los datos llegarán finalmente al nodo de salida, que enviará el mensaje a su destino.

1.3 GlobalLeaks.

GlobalLeaks es un software que permite a los individuos de denuncia de irregularidades para hablar de forma anónima sin importar cuál es su definición de "denuncia de irregularidades". La organización o individuos que ejecutan el software son capaces de personalizar la plataforma para que se adapte mejor a sus necesidades. GlobalLeaks está diseñado pensando en la flexibilidad y protege fuertemente la privacidad del usuario y presentaciones de forma predeterminada. Es de destacar que GlobalLeaks es compatible con la red Tor.

1.3.1 Principales características de GlobalLeaks.

GlobalLeaks está respaldado por Hermes Center for Transparency con la misión de apoyar la transparencia, libertad de expresión y apoyo al periodismo. Se busca la participación ciudadana en temas de interés público, y la participación de empleados en el correcto funcionamiento de las corporaciones e instituciones en las cuales laboran. GlobalLeaks cree que el público debe demandar que los gobiernos, corporaciones y organizaciones sean más responsables en sus acciones, y que dichas acciones benefician la promoción de la verdad y la toma de decisiones.

Algunos aspectos de interés relacionados GlobalLeaks son las siguientes:

- La denuncia anónima de irregularidades puede ser segura y fácil: GlobalLeaks permite la personalización del software por parte de los individuos u organizaciones de tal forma que se ajuste a sus necesidades, esta plataforma está pensada para considerar la flexibilidad y protege la privacidad de los usuarios y los envíos.
- Muchos casos de uso, un solo software Framework: GlobalLeaks considera muchos casos de uso y está diseñado como un framework. Desarrollado con la flexibilidad en mente ha sido adoptado por más de 40 proyectos: desde medios independientes a agencias públicas, desde corporaciones a activismo.
- Código abierto, documentación abierta: Este software de denuncia de irregularidades es gratis y es de código abierto bajo licencia AGPL, lo que permite una comunidad abierta de usuarios, voluntarios y contribuyentes para mejorar el software y la documentación.

¿Porque es importante la transparencia? La importancia radica en que cuando la información que afecta al público permanece oculta, la democracia y sus economías dejan de funcionar correctamente.

Que cosas no es GlobalLeaks:

- GlobalLeaks nos es un nuevo wikileaks: GlobalLeaks provee una plataforma de software mientras que ellos proveen un servicio, GlobalLeaks es una comunidad de código abierto mientras que wikileaks es un grupo cerrado, además GlobalLeaks no maneja documentos filtrados.

Otras consideraciones importantes:

- Los desarrolladores de GlobalLeaks no quieren tu información: La instalación de GlobalLeaks no implica ser parte de una red, sino que puede ser administrado como un nodo independiente. GlobalLeaks invita a registrar su sitio de denuncia de irregularidades en su directorio, pero eso realmente depende de cómo se configure.
- La seguridad de GlobalLeaks es limitada: GlobalLeaks hace su mejor esfuerzo por proveer de un software muy seguro, de cualquier forma GlobalLeaks es un software y como tal no puede proteger el anonimato fuera de su "Modelo de amenazas". Este software no protege de keylogger [18] es un malware o software malicioso que por medio del hardware captura contraseñas a través de pulsaciones del teclado, como el caso de algunos virus o cualquier otra amenaza que atente contra la seguridad de la computadora del usuario.

1.3.2 Globaleaks casos de USO alrededor del mundo

GlobaLeaks va dirigido a muchos casos de uso distintos, y por tanto ha sido diseñado a modo de marco estructural. Modelado pensando en la flexibilidad, a día de hoy GlobaLeaks ha sido adoptado por más de 60 proyectos por todo el mundo[19]. Nuestra gran gama de adoptantes incluye medios independientes, activistas, agencias públicas, corporaciones, y más entidades que han implementado GlobaLeaks

[18] Un keylogger: es un software o hardware que puede interceptar y guardar las pulsaciones realizadas en el teclado de un equipo que haya sido infectado. Este malware se sitúa entre el teclado y el sistema operativo para interceptar y registrar la información sin que el usuario lo note.

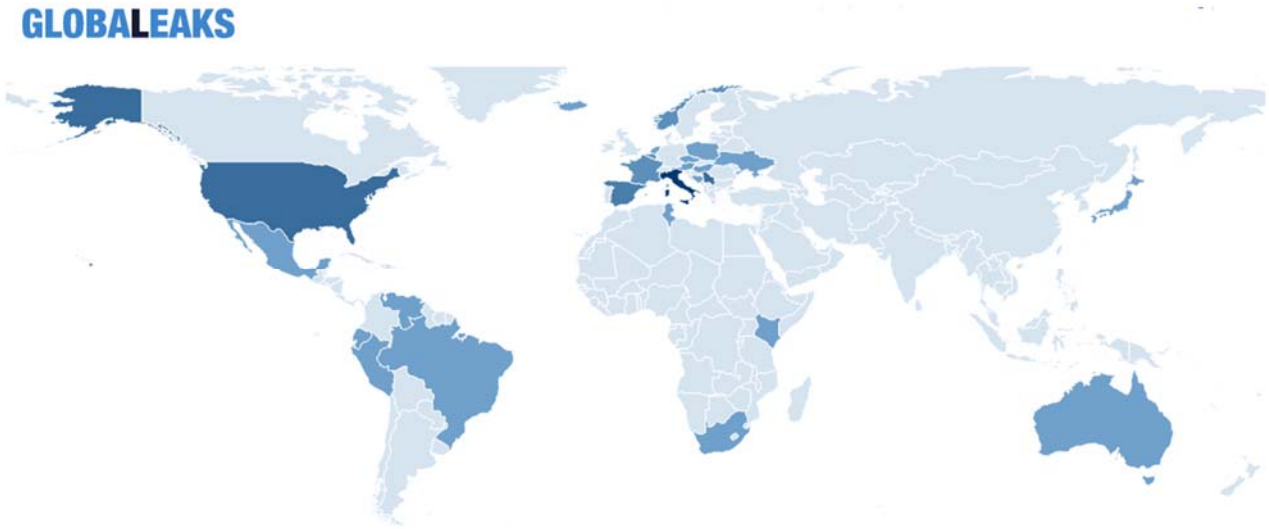
[19] https://www.globaleaks.org/who-uses-it/

Tabla 7 – Casos de uso alrededor del mundo.

Project Name	Year	Category	Tor URL	HTTPS URL	Country
Bústia Ètica	2016	Anticorruption		https://ajuntament.barcelona.cat/bustiaetica/es	Spain
Aotearoa Leaks	2016	Freedom of Information Activism	zjlzbo7y6nd2xbuz.onion		New Zealand
Curiamo La Corruzione	2016	Anticorruption	evz2fbu64s3lzhsi.onion	https://segnalazioni.curiamolacorruzione.it/#/	Italy
BrasiLeaks	2016	Activism	kzmw4yfm3viaojqt.onion	https://brasileaks.org	Brazil
Oko Press	2016	Investigative Journalism	p6vbgbn7ggutkt3i.onion		Poland
Edison Platform	2016	Corporate Whistleblowing	754hkfmiyumu5xlc.onion	https://segnalazioni.edison.it	Italy
Netpoleaks	2016	Activism	owmx2uvjkmdgsap2.onion		England
RegeniLeaks	2016	Journalism	diy7cyqbjh4p5apa.onion		Italy
ToristFR	2016	Literature and Arts	toristfgqiroaded.onion	https://mobile.twitter.com/TheToristFR	France
Oživení	2015	Anticorruption Activism	iopx5pchfdldldwp.onion	https://secure.bezkorupce.cz	Czech Republic
SecuriLeaks	2015	Investigative Journalism	ms5qd5es5qltiqsf.onion	https://www.securileaks.org	Norway
Nieuwsleaks	2015	Journalism	pb5icjbw6g5hnhl6.onion	https://nieuws.vtm.be/nieuwsleaks	Belgium
OCCRPLeaks	2015	Investigative Journalism	c4br2yayzdfcfkae.onion	https://occrp.org/occrpleaks	Bosnia
The Torist	2015	Literature and Arts	toristinkirir4xj.onion		Unknown
DataLeaks	2015	Freedom of Information Activims	x2tzc4z2kdi5io4j.onion	https://dataleaks.rs	Serbia

Project Name	Year	Category	Tor URL	HTTPS URL	Country
XnetLeaks	2015	Anticorruption Activism	ztjn5gcdsqeqzmw4.onion	https://xnet-x.net/en/xnetleaks	Spain
MexicoLeaks	2015	Journalism	pb5icjbw6g5hnhl6.onion	https://mexicoleaks.mx	Mexico
Xabardocs	2015	AntiCorruption Activism	rfftlkqzjdse5jvl.onion	http://www.xabardocs.org/start	Ukraine

Figura 10 – Mapa de casos de uso de GlobaLeaks



CAPÍTULO II
SITUACIÓN ACTUAL

2.1 Usos actuales de la herramienta Tor.

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

- Lo utilizan periodistas que trabajan en países donde la información es muy restringida y muy censurada.
- Lo utilizan políticos para entablar conversaciones privadas con otros colegas de otros países.
- Hackers para evitar ser identificados al realizar sus operaciones.
- Asuntos ilegales e inmorales en la DeepWeb (abuso del derecho a la privacidad)

Al centrarse en las denuncias ciudadanas anónimas, Tor ofrece una seguridad a nivel de confidencialidad en el sentido que sería muy difícil rastrear la fuente de la información original, lo que permite una mayor libertad para las personas o instituciones que haciendo el uso correcto de la libertad de expresión quieran denunciar hechos de corrupción, situaciones injustas relacionadas al abuso del poder, u otros hechos de interés para la ciudadanía.

2.2 Benchmarking Redes oscuras en Internet o Darknet[20]

Las redes oscuras o darknet son aquellas redes o subredes de Internet que, utilizando protocolos de encapsulado propios y esquemas complejos de comunicación entre pares, proveen a sus usuarios de anonimato y privacidad ante cualquier observador de la red.

Generalmente estas redes carecen de índices centrales a partir de los cuales extraer un listado de sitios, por lo que el acceso a los distintos sitios se consigue vía:

- Relaciones de confianza entre miembros que comparten enlaces
- Listados de sitios web recopilados y publicados por miembros
- Enlaces de un sitio web a otro

El uso de estas redes oscuras ha tomado auge en la última década por lo cual es común que los usuarios confíen la privacidad del contenido que comparten a este hecho, sin preocuparse de protegerlo mediante

[20] El término red oscura, del inglés Darknet, fue acuñado en noviembre de 2002 en el documento "The Darknet and the Future of Content Distribution" escrito por cuatro investigadores de Microsoft: Peter Biddle, Paul England, Marcus Peinado y Bryan Willman. Este documento se publicó en un entorno post-Napster y antes de que se implantara masivamente Gnutella. En él se definen las Darknets como 'una colección de redes y tecnologías usadas para compartir contenido digital. Las Darknet no son una red física separada sino una aplicación y una capa de protocolo montada sobre las redes existentes normalmente en Internet.

otro tipo de controles de acceso. Por tanto, si logramos un enlace de partida, es fácil que encontremos información comprometida.

En la investigación se ha considerado elaborar un benchmarking de las tres redes oscuras o darknet: TOR, FREENET y I2P. Donde se tomarán aspectos de anonimato, privacidad, navegación y soporte. Ver tabla 2.

Tabla 2- Benckmarking de Redes Anónimas en Internet		
Tor	**FreeNET**	**I2P**
Aspectos tomados en el Benckmarking: Anonimato, privacidad, navegación y soporte.		
- La Red TOR permite navegar de forma anónima, red compuesta por herramientas y software que te ayudan a usar Internet de manera anónima y sin dejar rastros. Tor esconde el origen y el destino de todo el tráfico que generas porque no revela la dirección IP y, además, mantiene la integridad y el secreto de la información que viaja por ella. Por este motivo se dice que esta tecnología pertenece a la Deep Web o Internet profunda, aquella que abarca el contenido en Internet que no forma parte de la superficie, es decir, sitios y contenidos que no son indexados por los motores de búsqueda tradicionales. (Pagnotta, 2014) - Si la privacidad, es una buena opción; no obstante, se observa que la navegación es más lenta porque el tráfico pasa por muchos proxies. Por otro lado, por más que haya anonimato, recuerda que las actividades delictivas siguen siendo ilícitas. Lo que hace Tor es volver más complejo el rastreo, pero la acción sigue estando fuera de la ley	-La RED FREENET es una plataforma peer-to-peer para la comunicación y la publicación resistente a la censura. -Se trata de herramientas con una finalidad bastante clara y con un nivel tecnológico alto, lo que ha permitido el surgimiento de las "darknets" en las que es posible encontrar personas que comparten información libremente sin ningún tipo de censura, no obstante, como ocurre con cualquier herramienta, pueden ser usadas de forma legítima para ayudar a personas que sufren abusos en zonas conflictivas o por ciberdelincuentes que se dedican a realizar actividades ilegales, valiéndose de los fuertes niveles de anonimato que aportan estas soluciones. En el presente documento encontrarás el funcionamiento de las principales herramientas para proteger tu privacidad y consolidar tu anonimato en entornos como Internet. (De La Luz, 2011)	- I2P es una red de capa anónima - una red dentro de una red. Está pensada para proteger la comunicación del seguimiento de las redes de vigilancia y la monitorización por terceras partes como los ISP`s (proveedores de Internet). -I2P es usado por muchas personas que se preocupan por su privacidad: activistas, poblaciones oprimidas, periodistas, denunciantes, así como por el ciudadano medio. -Para a anonimizar los mensajes enviados, cada aplicación cliente tiene su "ruter" I2P que crea unos cuantos túneles" de entrada y salida - una secuencia de pares que pasan el mensaje en una dirección (hacia y desde el cliente, respectivamente). (Geti2p.net, 2017)

Tor	**FreeNET**	**I2P**
- Para acceder a la red Tor es necesario usar un programa llamado Tor Browser que se puede descargar gratis desde su sitio oficial. Tor Browser es solo un archivo comprimido auto ejecutable que contiene en su interior dos aplicaciones: Vidalia que se ocupa de inicializar y monitorear la conexión con Tor. Una versión portable de Firefox, para navegar después de quedar establecida la conexión.	-La instalación recomienda usar un navegador en modo incógnito, o también llamado "Navegación Privada", también podéis usar un Mozilla Firefox Portable (que no necesita instalación). (De La Luz, 2011)	- Su navegador web necesita ser configurado para poder navegar en sitios y para utilizar los outproxies disponibles en I2P. Debajo tiene un paso a paso para configurar los navegadores más populares.
-Tor es una red que se ha vuelto muy popular precisamente porque es fácil de configurar, muy fácil de instalar y sobre todo porque permite salida a Internet utilizando los repetidores que se encuentran dentro de la red. Esto es una solución outproxy en donde los usuarios pueden salir hacia Internet utilizando la plataforma de anonimato, los repetidores que se encuentran disponibles en la red En soluciones como Tor si un servicio oculto lo levanto en mi ordenador, que es lo más habitual y posteriormente apago mi ordenador, ese servicio oculto deja de estar disponible. Entonces es lo que ocurre con muchas de las direcciones .onion que un día las vemos levantadas y el otro día ya no están, suele pasar debido a que son cosas, son servicios que no están 24/ 7.(Echeverri Montoya, 2016)	- En el caso de Freenet si se configura, ose monta servicio oculto en Freenet este servicio va a estar disponible aunque tu nodo ya no se encuentre levantado ¿por qué motivo? Porque otros usuarios, otros enrutadores dentro de la red, han consultado ese nodo, ese contenido y lo han cacheado dentro del propio datastore. Esto es una cosa que diferencia muchísimo a Freenet de otras soluciones de anonimato. -Es una redes inproxy, que solamente permiten la navegación dentro de la red. Es el concepto más puro de una VPN en donde todos los repetidores se pueden comunicar entre ellos pero no permiten salir afuera de esa VPN y este es el concepto clave para diferenciar entre una red como Tor y una red como Freenet.	- El equipo de desarrollo de I2P es un grupo abierto, todos los que estén interesados son bienvenidos a involucrarse en el proyecto, y todo el código es libre. El núcleo de I2P y la implementación del ruter están en java (actualmente trabajando con sun y kaffe, el soporte para gjc está planeado para más adelante), y hay un API simple para acceder a la red desde otros lenguajes (con una librería C disponible, y con Python y Perl en desarrollo). La red está en estos momentos en desarrollo activamente y aún no ha alcanzado la versión 1.0, pero la actual hoja de ruta describe nuestro programa. (Geti2p.net, 2017) -En soluciones como I2P si un servicio oculto lo levanto en mi ordenador, que es lo más habitual y posteriormente apago mi ordenador, ese servicio oculto deja de estar disponible. Son servicios que no están 24/7. (Echeverri Montoya, 2016)

2.2.1 Evaluación de las redes anónimas o darknet según características basado en ISO/IEC 9126[21] sobre la evaluación de la calidad del software.

Luego de revisar el benchmarking es importante fundamentar el uso de la Red Tor en la investigación. A continuación se presenta un cuadro resumen con las características y criterios de evaluación para definir cuál de las anteriores redes anónimas tiene mejor calificación.

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 herramientas representan 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

[21] ISO/IEC 9126; de la ISO (Organización Internacional de Normalización) y la IEC (Comisión Electrotécnica Internacional).

Según las características y sub-característica seleccionadas de calidad de software definidas en la ISO/IEC 9126 se formula la siguiente tabla 4:

				Redes Anónimas		
Características	**Pregunta Relacionada a la Característica**	**Sub-características**	**Pregunta Relacionada a la Sub Característica**	**Tor**	**FreeNet**	**I2P**
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 privacidad y anonimato?	3	3	3
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	2
Usabilidad	¿El Software es fácil de utilizar y aprender?	Aprendizaje (Criterio de evaluación 3)	¿Es fácil de utilizar en su navegador?	2	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	0	0
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, por ejemplo GlobalLeaks?	3	0	0
Portabilidad	¿Es instalable en ambientes multiplataforma	Facilidad de instalación (Criterio de Evaluación 3)	¿Es fácil instalar en ambientes multiplataforma?	2	2	2
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	3	3
			Total	16	12	12
			Puntuación Porcentual	76.19	57.14	57.14

Tabla 4– Evaluación según características y sub-características basado en ISO/IEC 9126[22] sobre la evaluación de la calidad del software.

De acuerdo a la evaluación anterior la red Tor obtiene un total de 16 puntos de 21 posibles siendo porcentualmente una puntuación de 76.19 superando a las redes anónimas FreeNet (57.14) y I2P (57.14).

2.2 Contexto legal de las denuncias ciudadanas anónimas

Comentario: Dentro del marco legal de las denuncias (correspondencia) anónimas (Lic. Álvarez Castaneda, 2016):

I. Constitución de la República de El Salvador:

Art. 24.- La correspondencia de toda clase es inviolable, interceptada no hará fe ni podrá figurar en ninguna actuación, salvo en los casos de concurso y quiebra. Se prohíbe la interferencia y la intervención de las comunicaciones telefónicas (Asamblea Constituyente, 1983).

Comentario: Respecto a la difusión de las denuncias ciudadanas anónimas también menciona:

Art. 6.- Toda persona puede expresar y difundir libremente sus pensamientos siempre que no subvierte el orden público, ni lesione la moral, el honor, ni la vida privada de los demás. El ejercicio de este derecho no estará sujeto a previo examen, censura ni caución; pero los que haciendo uso de él infrinjan las leyes, responderán por el delito que cometan (Asamblea Constituyente, 1983).

Comentario: Al ser redactado este artículo no estaba contemplado la publicación de información en sitios web, ni los problemas a los que se enfrentan aquellas personas que denuncian hechos de corrupción o similares que afecten a todos los ciudadanos, por lo que para preservar otros derechos fundamentales como el derecho a la vida y a la salud se vuelve indispensable el anonimato de los denunciantes.

II. Ley Especial Contra los Delitos Informáticos:

Comentario: De igual forma si alguien desea interceptar la comunicación entre los sistemas:

[22] ISO/IEC 9126; de la ISO (Organización Internacional de Normalización) y la IEC (Comisión Electrotécnica Internacional).

Art. 21.- La persona que sin justificación intercepte por medios tecnológicos cualquier transmisión hacía, desde o dentro de un sistema informático que no está disponible al público; o las emisiones electromagnéticas que están llevando datos de un sistema informático, será sancionada con prisión de siete a diez años (Asamblea Legislativa de El Salvador, 2016).

2.3 Modelo de amenazas y diseño de la seguridad de GlobalLeaks.

GlobalLeaks es un Framework que puede ser usado a través de distintos escenarios de tal forma que permita obtener flexibilidad y seguridad.

Matriz de Actores dentro del proceso:

- Delator (de actividades ilícitas): Es el usuario que envía un Aviso a través del Nodo de GlobalLeaks, es la persona que puede encontrarse en un contexto de entre un bajo a un alto riesgo, dependiendo del escenario de uso y del contenido de la información que envíe.
- Receptor: Es el usuario (persona u organización) que recibe el Aviso enviado por el Delator, la información puede ser recibida a través de una interface específica de GlobalLeaks denominado Tip (Aviso), o puede ser un software de terceras partes.
- Administrador de Nodo: El usuario (persona u organización) que está corriendo/ejecutando el nodo de GlobalLeaks, promocionado y gestionando la iniciativa de denuncia de irregularidades. El Administrador de nodo será considerado en todos los escenarios como una entidad confiable, en lo referente al intercambio de datos entre los actores. Por seguridad no será considerado una entidad confiable respecto a la identidad de los actores(es aquí donde se vuelve necesario el uso del navegador y la red Tor).(Pellerano, 2014)

Matriz de anonimato relacionado al medio:

Respecto al anonimato, GlobalLeaks maneja tres niveles:

- Anónimo: La identidad del actor (Delator) y su localización no puede ser descubierta.
- Confidencialidad: El receptor y el Administrador el nodo no pueden conocer la identidad del delator, pero una tercera parte (intruso con control sobre la red) puede identificar al actor (Delator).
- No anonimato: Los otros actores conocen la identidad del Delator, si este no ha tomado medidas para proteger su identidad.

La siguiente tabla muestra una matriz de cómo se aplican los niveles de anonimato de acuerdo a las diferentes arquitecturas utilizadas y a la implementación del Software de GlobalLeaks:

Matriz de Anonimato	Usando navegador Tor	Usando tecnología Tor2web	Usando Internet público (normal)
Receptor	Anónimo	Confidencial	No anonimato
Delator (de algún ilícito)	Anónimo	Confidencial	No anonimato
Administrador de Nodo	Anónimo	Anónimo	No anonimato

Tabla 5– Matriz de niveles de Anonimato

Diferentes escenarios requieren diferentes configuraciones las cuales pueden ser requeridas por el Administrador del Nodo.

Estos son algunos de los ejemplos del uso que puede ser dado a una implementación de GlobalLeaks, siempre en el escenario de los casos de uso:

- Medios de comunicación:
- Quejas dentro de una empresa.
- Denuncia de irregularidades respecto a pago de impuestos al gobierno.
- Activismo relacionado a derechos humanos.
- Iniciativa de comunicación ciudadana.
- Reporte sobre baches en las calles a la municipalidad (En este caso no es requerida la implementación de la protección de identidad).

Medidas de seguridad respecto al software de la aplicación:

- Seguridad de la aplicación Web: GlobalLeaks implementa las buenas prácticas de las medidas de seguridad "OWASP REST Security Cheat Sheet" en lo relativo a Autenticación, Autorización, Validación de entradas, Codificación de salidas, logeo seguro.
- Resistencia del servidor: Ya que el servidor puede ser sujeto a ataques de denegación de servicio, el servidor mitiga esta amenaza haciendo una clara separación de operaciones síncronas (peticiones) de operaciones asíncronas (manejo de data, cifrado de la data, manipulación de la data, envío de notificaciones). De esta forma el servidor no realizará operaciones intensivas relacionadas a peticiones HTTP.
- Seguridad de aplicación cliente: Entre otras cosas la aplicación cliente impide la inyección de código al servidor.

GlobalLeaks no protege contra:

- Factores del entorno: Por ejemplo, si se tiene alguna cámara que captura en video las operaciones que se realizan, o que deliberadamente alguno de los actores revele su actividad a amigos o conocidos.
- Negligencia humana: Por ejemplo si la información enviada por el Delator, hace referencia (nombre, apellido, identificación) a la persona que la envía.
- Data almacenada fuera de GlobalLeaks.
- Análisis avanzado de tráfico: En resumen es por esto que se sugiere el uso de Tor (Pellerano, 2014).

CAPÍTULO III
DISEÑO DE LA SOLUCIÓN

3.1 Análisis de requerimientos

Para garantizar la confidencialidad de la información, la privacidad en la comunicación y el anonimato del emisor y receptor, se ha hecho una revisión de los aspectos técnicos de la implementación de la plataforma GlobalLeaks[23] en la red TOR y una revisión técnica a nivel de hardware, software, dominio y direccionamiento que a continuación se presentan:

3.1.1 Requerimientos Técnicos:

Los requerimientos de hardware óptimos para el funcionamiento de la plataforma GlobalLeaks, en seguridad y disponibilidad de recursos, GlobaLeaks necesita un servidor dedicado. Para cumplimiento de la construcción de un prototipo de sitio web, que sea una herramienta informática combinada con tecnología TOR y GlobalLeaks.

Los requisitos técnicos para la implementación de GlobalLeasks en un servidor se listan en la siguiente tabla:

Modelo Servidor	Servidor HPE ProLiant ML10 Gen9
Microprocesador	Intel® Xeon® E3-1200 v5
RAM	16 GB. La cantidad de memoria RAM varía según la cantidad de usuarios Web.
Almacenamiento	2 HD SCSI 500 Gb Raid 1

Tabla 6: Requisitos Técnicos

Las especificaciones del servidor son exclusivamente para almacenar el sitio web en la plataforma GlobalLeaks, ahí mismo se almacenar el direccionamiento en la red Tor (xxxxxxxxxxxxxxxxx.onion) donde se enviar información anónima y hacer gestión de ella, es importante mencionar que el servidor también será el repositorio de los documentos relacionados con la denuncia ciudadana enviada para su evidencia.

[23] Requerimientos técnicos GlobalLeaks: https://github.com/globaleaks/GlobaLeaks/wiki/Technical-requirements

3.1.2 Requerimientos de dominio y direccionamiento:

- Se necesita adquirir un nombre de dominio. Para la implantación de GlobalLeaks se adquiere ElSalvadorLeak.online, será el nombre del sitio donde se desarrollara una plantilla que fácilmente y reconocible como un sitio de denuncias anónimo en internet ese sitio está basado en diseño al sitio https://mexicoleaks.mx/[24]
- Se debe realizar un hardening[25] de seguridad al servidor de implementación, para proteger de forma adecuada el acceso a los documentos de denuncias que se almacenen.

3.1.3 Requerimientos de Instalación de Framework GlobalLeaks

GlobaLeaks puede funcionar en muchos sistemas operativos diferentes, y Ubuntu Trusty Tahr 14.04 LTS es oficialmente compatible con la plataforma. Los requerimientos para la instalación del servidor PC de 32 bits (i386), que requiere librerías adicionales para preparar el entorno de implementación del framework GlobalLeaks son los siguientes:

- binutils
- cpp
- dpkg-dev
- fakeroot
- gcc
- g++

3.1.4 Requerimientos para su funcionamiento de Framework GlobalLeaks

Se debe realizar la instalación de sistema operativo Ubuntu 14.04.5 LTS (Trusty Tahr) dentro de un servidor PC de 32 bits (i386), que requiere las siguientes dependencias funcionales para la implementación del framework GlobalLeaks:

- AppArmor
- Zope

---

[24] Méxicoleaks.mx: una plataforma independiente de denuncia ciudadana y transparencia fundada en México.

[25] Hardening en términos de seguridad informática que es un conjunto de actividades que son llevadas a cabo por el administrador de un sistema operativo para reforzar al máximo posible la seguridad de su equipo. Su propósito, entorpecer la labor del atacante y ganar tiempo para poder minimizar las consecuencias de un inminente incidente de seguridad e incluso, en algunos casos, evitar que éste se concrete en su totalidad.

- Phyton versiones de la versión 2.7 y versión 3.0
- TorSOCKs
- Tor
- PyOpenSSL
- Python-Cryptography
- Python-GnuPG
- Py-scrypt
-

3.2 Funcionamiento del sistema

De forma general, el sitio web funcionará como cualquier otro sitio web normal con mucha información referente a las denuncias ciudadanas y una guía detallada de como instalar y utilizar el navegador Tor, y solo se diferenciará de otros sitios web en que este permitirá el envío de documentos/denuncias de forma cifrada con llave pública, será una operación invisible para el usuario.

3.2.1 Diagrama de Despliegue UML

Se presenta el diagrama de despliegue que es una de las clasificaciones de los diagramas UML, se desarrolla la definición y los componentes para su estructuración.

El diagrama de despliegue permite mostrar la arquitectura en tiempo de ejecución del uso de la plataforma GlobalLeaks funcionando en la red TOR con su navegador TOR respecto al hardware y software. El siguiente diagrama ha sido diseñado para la implementación sitio “ElSalvadorLeaks”, utilizando el “Navegador Tor” y la tecnología “GlobalLeaks”.

La explicación del diagrama es la siguiente: Desde el Nodo “Interacción de Usuario Denunciante” y desde los componentes “Computadora” y “Navegador Tor” se envía un “Documento Secreto” a traves de una relación de dependencia hacia el Nodo “Red Tor”, dicho nodo posee internamente un componente llamada “Enrutamiento Cebolla” que permite ocultar la direccion IP originante del “Documento Secreto” a través de un arreglo de servidores y una metodologia de envío y recepción de informacion entre ellos. El componente interno “Servidor GlobalLeaks” posee otro subcomponente “Framework GlobalLeaks” y dentro otro mas “Cifrado Open PGP” que contiene una “Llave publica del receptor”, dicha llave sirve para convertir el “Documento Secreto” en un “Documento Cifrado”. La relacion de dependencia llega del Nodo “Red Tor” hacia el Nodo “Interaccion de Usuario Receptor” quien posee los componentes “Computadora1” y “Navegador Tor1”, dentro de estos últimos se lleva a a cabo el descifrado del “Documento Cifrado” utilizando la “Llave privada del receptor”para tener acceso al “Documento Secreto” .

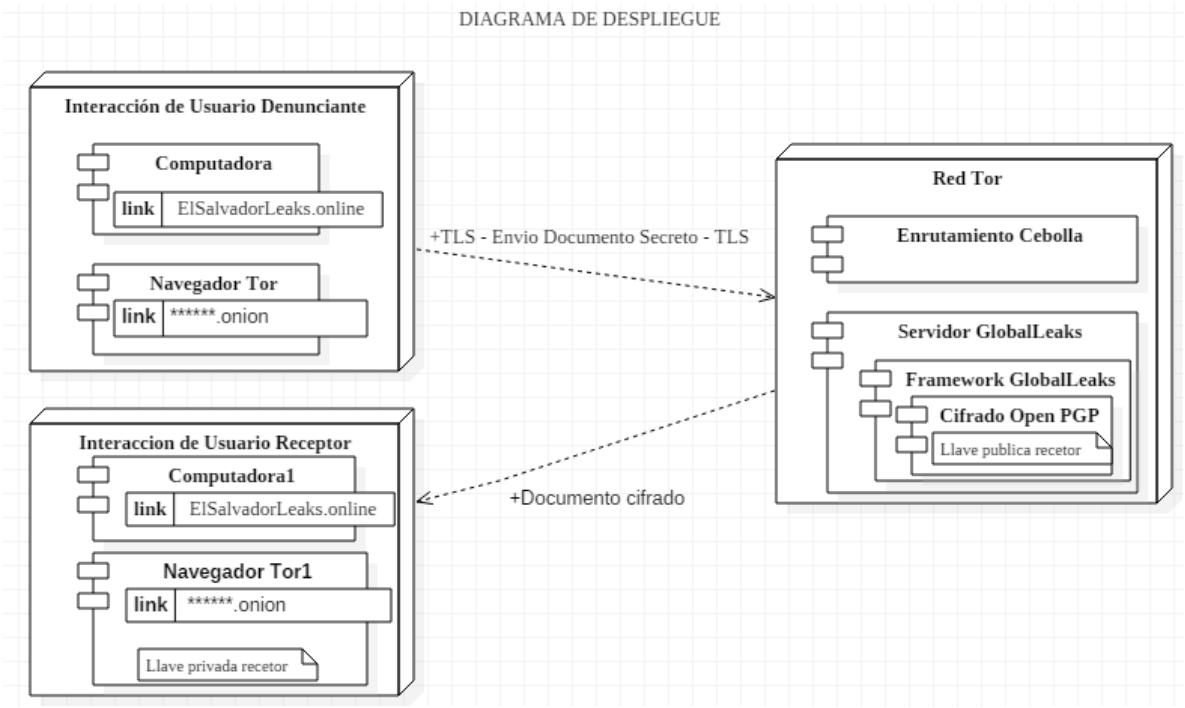


Figura 6. Diagrama de despliegue

3.2.2 Diagrama de componentes

El siguiente diagrama UML muestra los componentes principales de la solución propuesta y sus relaciones.

Siendo los componentes principales el “Client Host Origin”, “Client Host Destination” y la “Tor Network”, de forma tal que el primero contiene un sub componente “Tor Web Browser” para la navegacion anonima y el segundo tienen un “Web Browser”. La “Tor Network” posee internamente una “n” cantidad de “Server Node’s” que son subcomponentes por donde viaja la informacion desde el “Client Host Origin” hasta el “Client Host Destination”. Uno de dichos “Server Node’s” se diferencia de los otros porque es el Server Node “ElSalvadorLeaks Linux”, un componente servidor que contiene una instalacion de la plataforma “GlogalLeaks” con otros subcomponentes de Cifrado(“PGP Cipher”) y un Web Server(“Zope web server”), dicha instalacion aloja el sitio con extension “.onion” y se encuentra oculto a la navegacion normal:

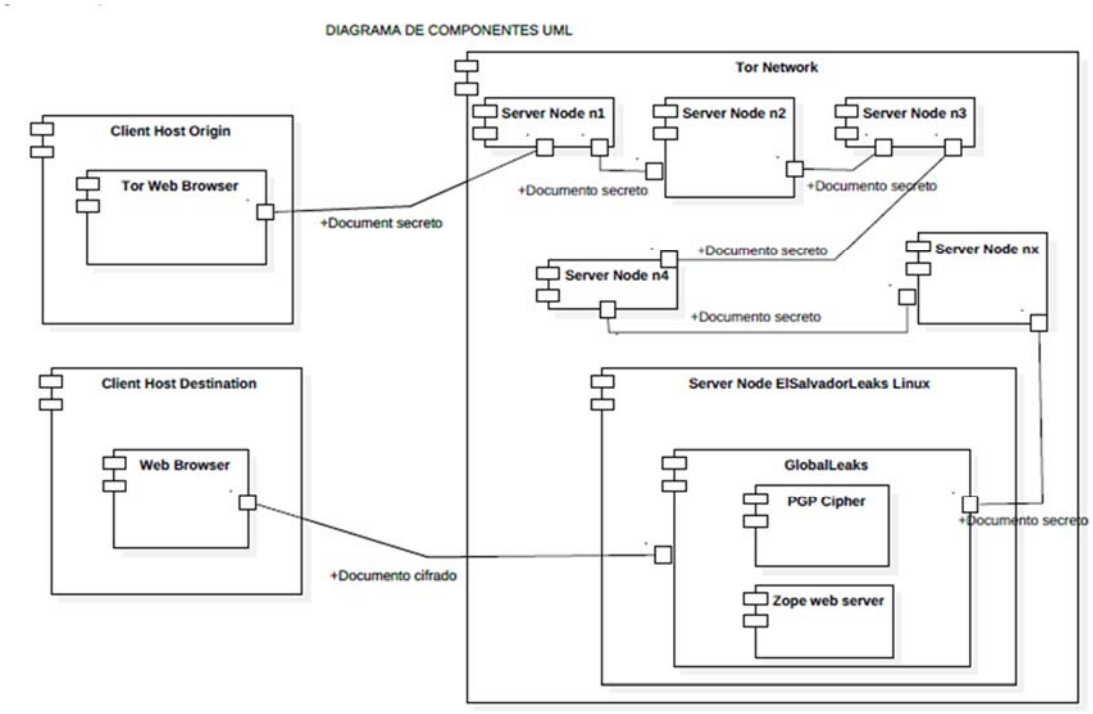


Figura 7. Diagrama de componentes

3.2.3 Diagrama de funcionamiento (diagrama de red), perspectiva del usuario.

Desde la perspectiva del usuario el envío de documentos será muy simple, una vez se haya instalado el "Navegador Tor" en la "Computadora Personal", el "Usuario Anónimo" podrá enviar un "Documento secreto" haciendo uso del "Navegador Tor", el usuario simplemente enviará la información y al otro extremo del canal estará un "Periodista"(o un usuario destinatario) que recibirá el "Documento secreto" a través de un "Servidor":

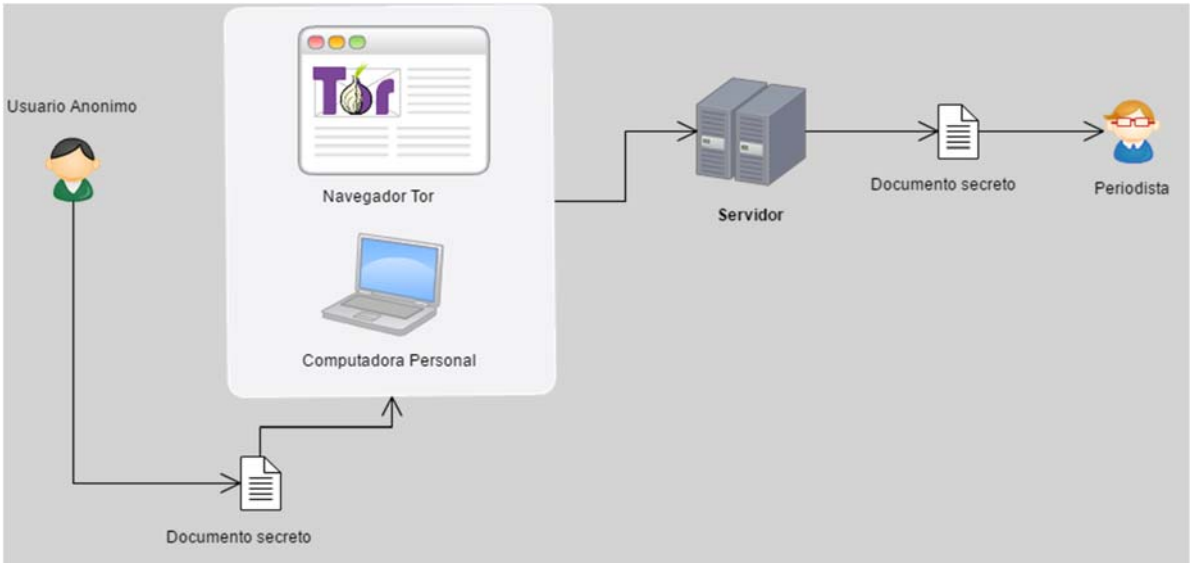


Figura 8: Diagrama de funcionamiento, perspectiva del usuario

3.2.4 Diagrama de funcionamiento (diagrama de red), aplicación de la criptografía para la seguridad

Desde la perspectiva de la seguridad, el diagrama anterior se vuelve más complejo al contemplar toda la lógica de la red Tor para proteger el anonimato y el cifrado del documento. Este nuevo diagrama contempla la posibilidad de intrusos en el paso final, estos pueden estar interesados en conocer el contenido de los documentos/denuncias enviadas, lo que deberá ser evitado con la adición de la criptografía de llave pública, en este caso usando GlobalLeaks.

La explicación de este diagrama es la siguiente: El “Usuario Anónimo” (Denunciante Anónimo) envía un “Documento secreto” a través del “Navegador Tor” que está instalado en su “Computadora personal”, dicho documento viaja usando el protocolo TLS dentro de la "Red Tor”, pasando por “n” nodos de tal forma que queda oculta la dirección IP original de donde se realizó el envío.

El documento llega a una instalación de la plataforma GlobalLeaks personalizada (ElSalvadorLeaks) que tiene configurado previamente al “Periodista” o entidad receptora del “Documento secreto”, con una llave pública de cifrado única. El “Documento secreto” se convierte en “Documento cifrado” y es almacenado temporalmente en el “Servidor” que contiene la misma instalación de GlobalLeaks.

Cuando el “Periodista” o entidad receptora desee acceder al “Documento cifrado” puede hacerlo desde su computadora personal, acceder a la plataforma GlobalLeaks personalizada (ElSalvadorLeaks) y descargar el Documento, luego de utilizar su llave privada de cifrado sobre el “Documento cifrado” puede finalmente acceder al “Documento secreto”. En este último paso pueden existir entidades (Proveedores de servicios de Internet, Entidades gubernamentales, etc) que tengan control del canal de

comunicación, pero no podrían acceder al “Documento secreto” ni conocer la dirección IP original del “Usuario Anónimo” (Denunciante Anónimo).

A continuación, el diagrama:

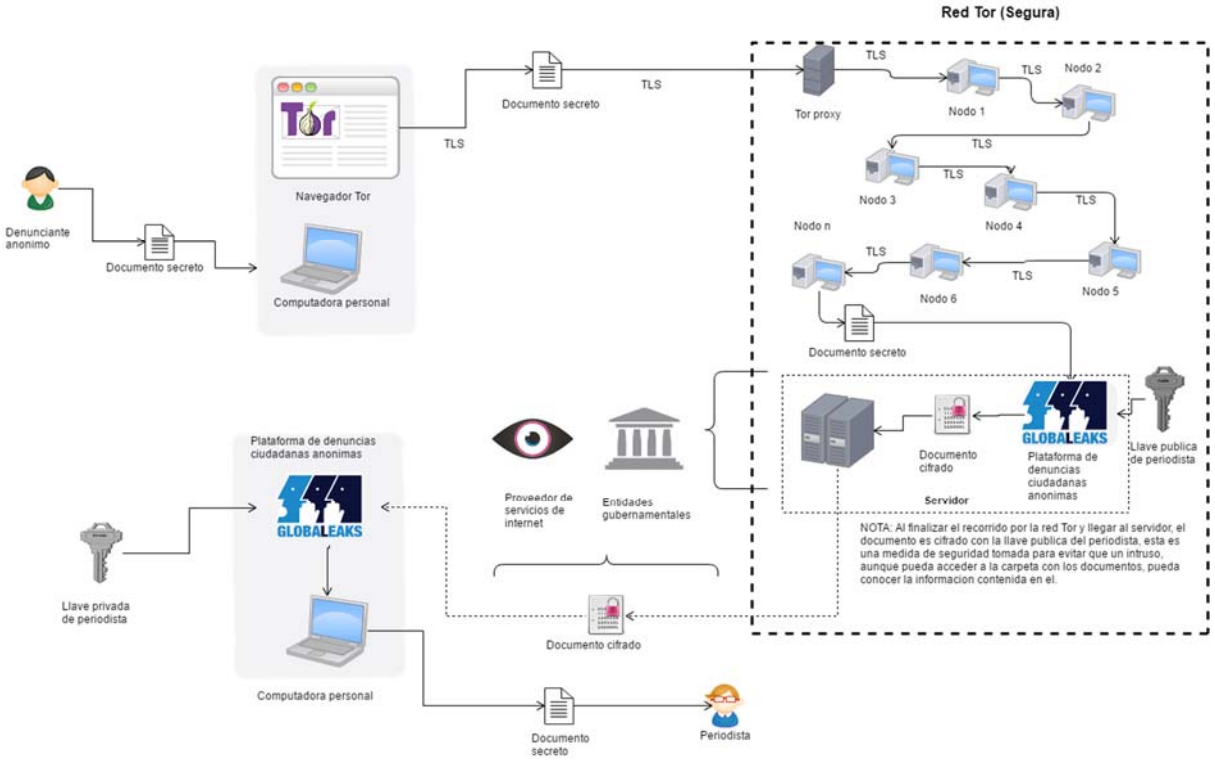


Figura 9: Diagrama de funcionamiento, aplicación de la criptografía para la seguridad.

CAPITULO IV

MANUAL DE INSTALACIÓN Y CONFIGURACIÓNES PARA PUESTA EN SERVICIO

DESARROLLO DE UN SITIO DE “EL SALVADOR-LEAKS”

Manual de Instalación

Versión: 0001

Primera versión del producto

HOJA DE CONTROL

Organismo	Maestría en Seguridad y Gestión de Riesgos Informáticos
Proyecto	DESARROLLO DE UN SITIO DE “EL SALVADOR-LEAKS”
Entregable	Manual de Instalación
Autor	Jorge Alberto Ramírez Corleto, Nelson Alex Baires Salazar, Melvin Gerardo Flores

REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Fecha del Cambio
0001	Versión inicial	Jorge Alberto Ramírez Corleto	01/03/2017

CONTROL DE DISTRIBUCIÓN

Nombre y Apellidos
Nelson Alex Baires Salazar

4.1 Manual De Instalación, Configuración y en servicio elsalvadorleak.com

Objeto

El propósito del presente manual es describir y guiar la forma en que debe ser instalada la plataforma GlobalLeaks en un servidor GNU Linux.

Alcance

Este manual no es un manual de usuario, es una guía de implementación dirigida a personal con conocimiento de infraestructura de tecnología de información, a nivel técnico o profesional.

Estructura de Manual:

- **4.1.1 Instalación y configuración del Sistema Operativo**
  Pantalla de configuración y descripción
- **4.1.2 Instalación y configuración de plataforma GlobalLeaks**
  Comandos necesarios para la instalación
  Pantallas de configuración y descripción
  Instalación del servidor Web
  Configuración y alojamiento en la red Tor
- **4.1.3 Sitio web Adaptación de contenido en la plataforma GlobalLeaks**
- **4.1.4 Hardening del servidor**

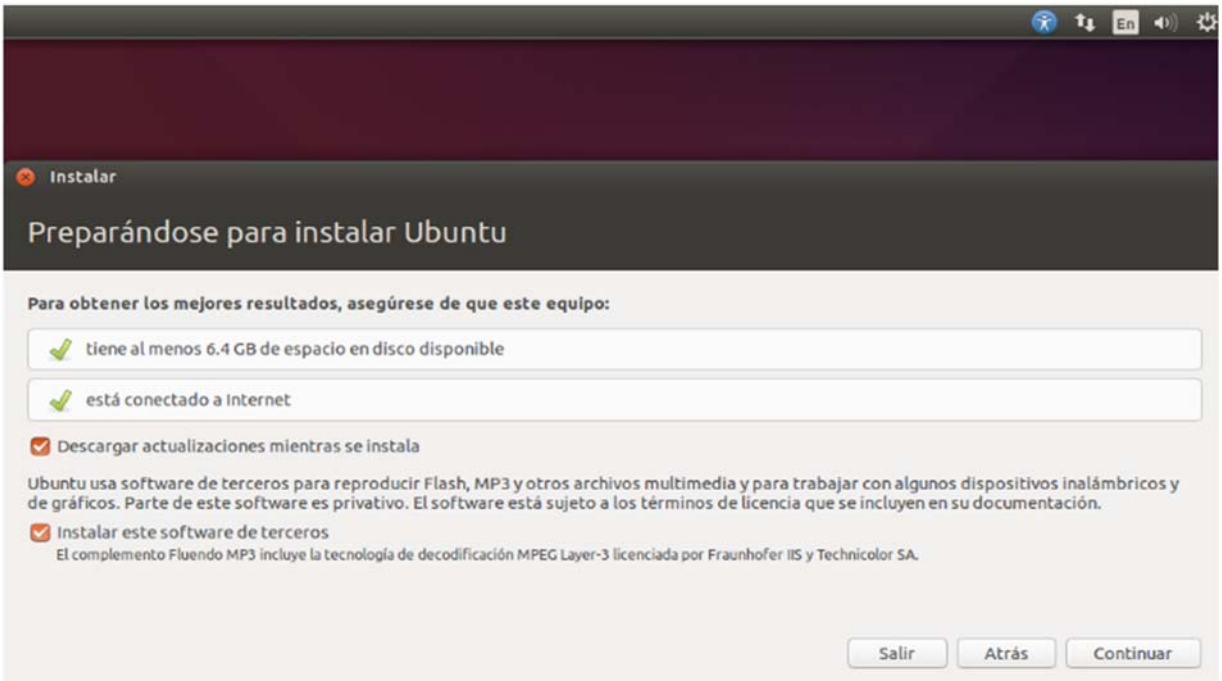
4.1.1 Instalación y configuración del SO Linux

Para el sistema operativo se utilizará Linux Ubuntu 14.04 LTS Trusty Tahr; la nueva versión estable de Canonical que recibirá soporte durante 5 años. A continuación se guiará la instalación paso a paso durante todo el procedimiento para realizarlo correctamente.

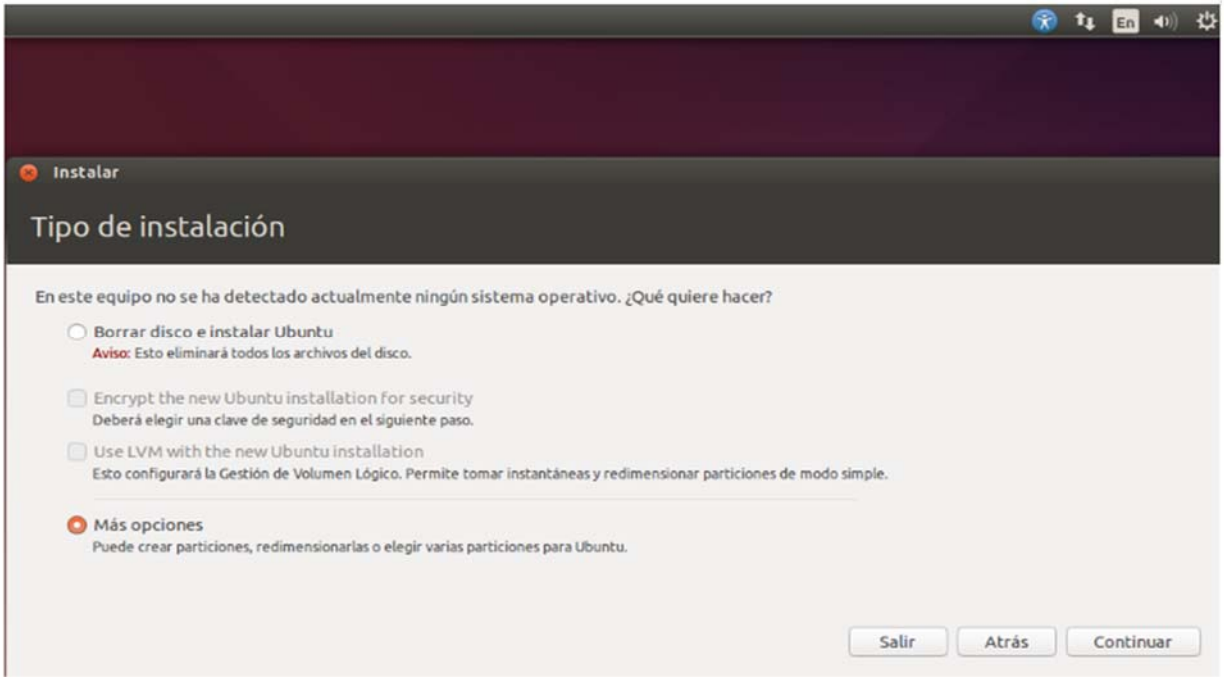
Lo primero que se debe realizar es la descarga de la ISO de Ubuntu 14.04 LTS Trusty Tahr y pasarla a un CD/DVD o una unidad USB; para quemar la imagen en un USB se recomienda utilizar UnetBootin. Se puede elegir entre descarga directa de 32 o 64 bits o torrent de 32 o 64 bits. Una vez hecho esto se procede con la instalación.

El primer paso en la instalación es la opción de elegir el idioma, en este caso se elige español y se selecciona “Instalar Ubuntu”, aunque si se desea puede probarse en sistema sin necesidad de instalación eligiendo la opción de probar Ubuntu.

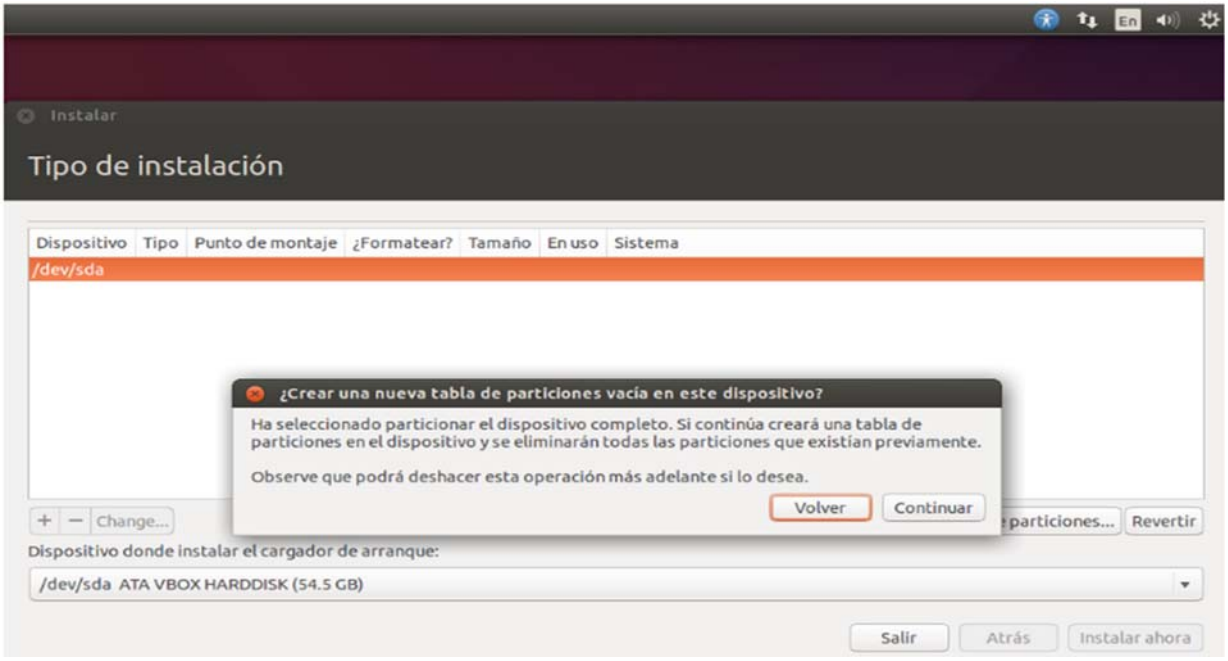
Segundo paso: se comprueba el espacio en el disco duro para poder instalar el sistema y la conexión a internet, se puede elegir “Descargar actualizaciones” mientras se instala; es opcional, pero es muy importante marcar la opción “Instalar este software de terceros”.



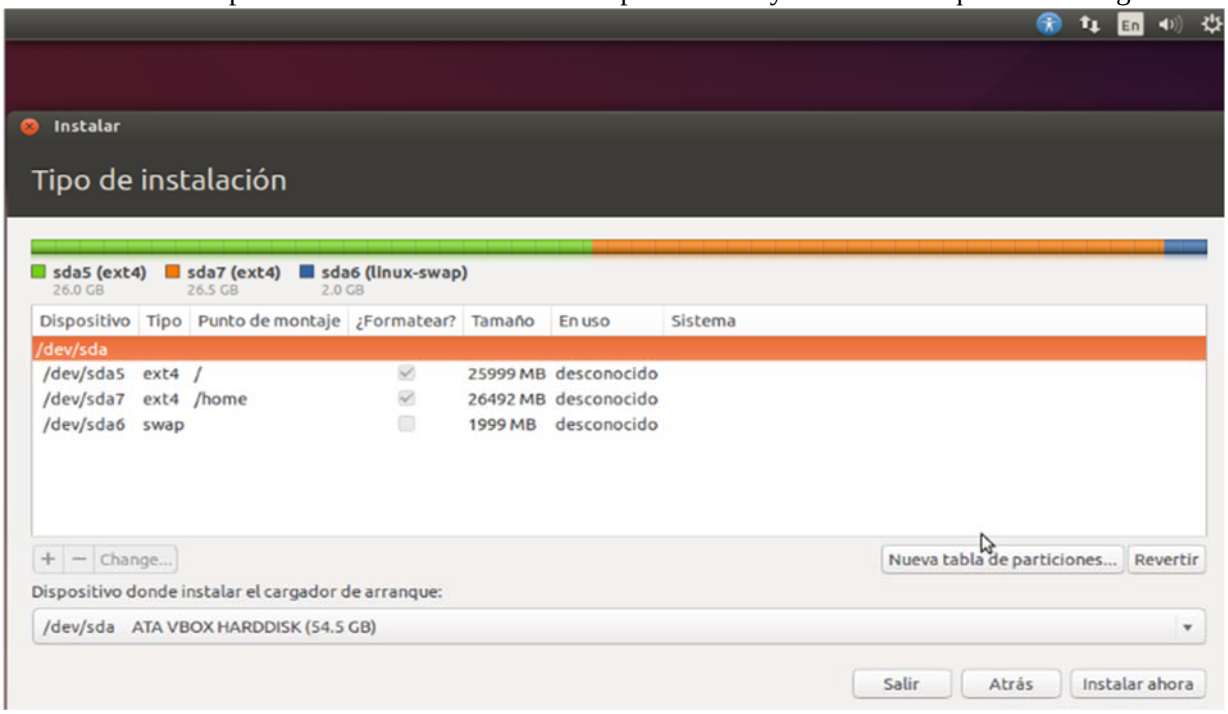
El tipo de instalación tiene varias opciones a elegir, si no se ha particionado el disco duro con anterioridad se recomienda elegir “Más opciones”.



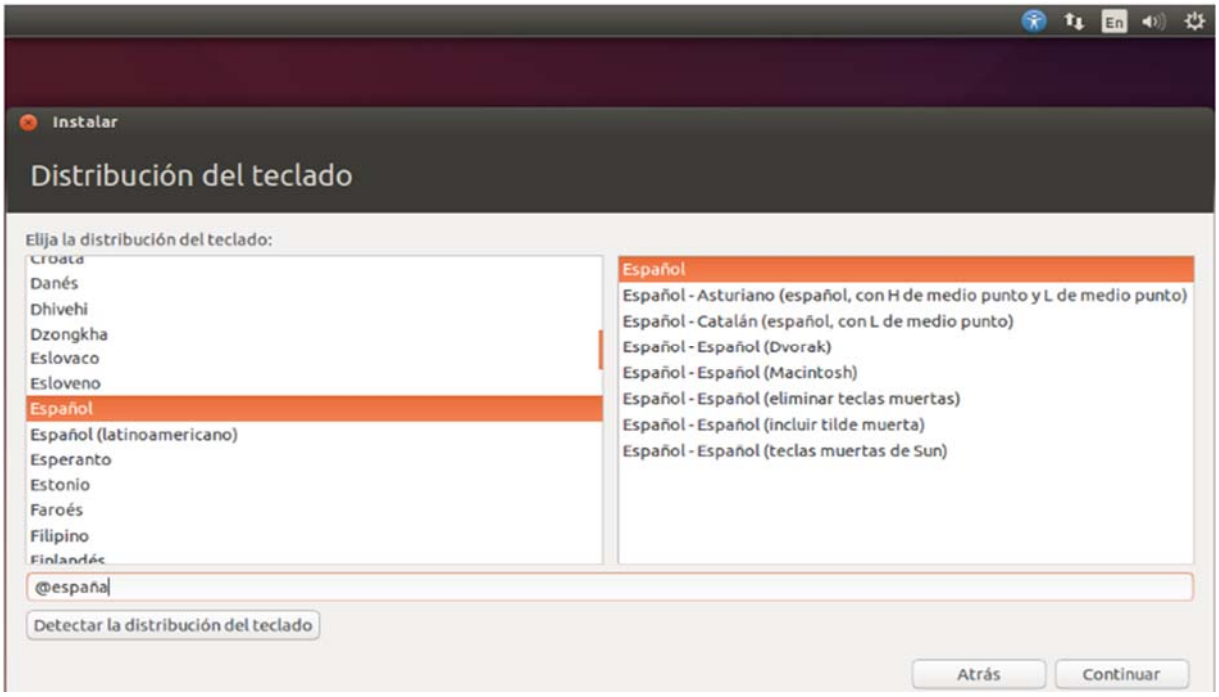
Al elegir más opciones se puede crear una nueva tabla de particiones, donde se selecciona el espacio necesario para la instalación, clickear opción de “Continuar”.



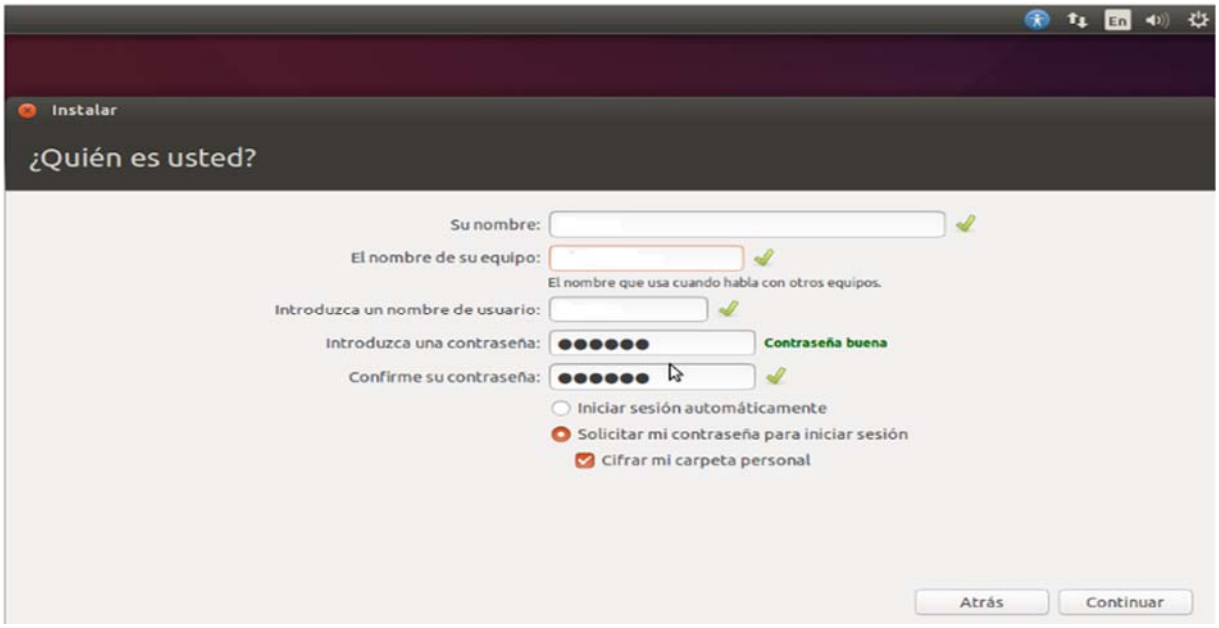
Ahora se crearán las particiones, para la “swap o área de intercambio” le daremos la mitad de la RAM y el resto de espacio se divide en dos para “/” y “/home” quedando algo así:



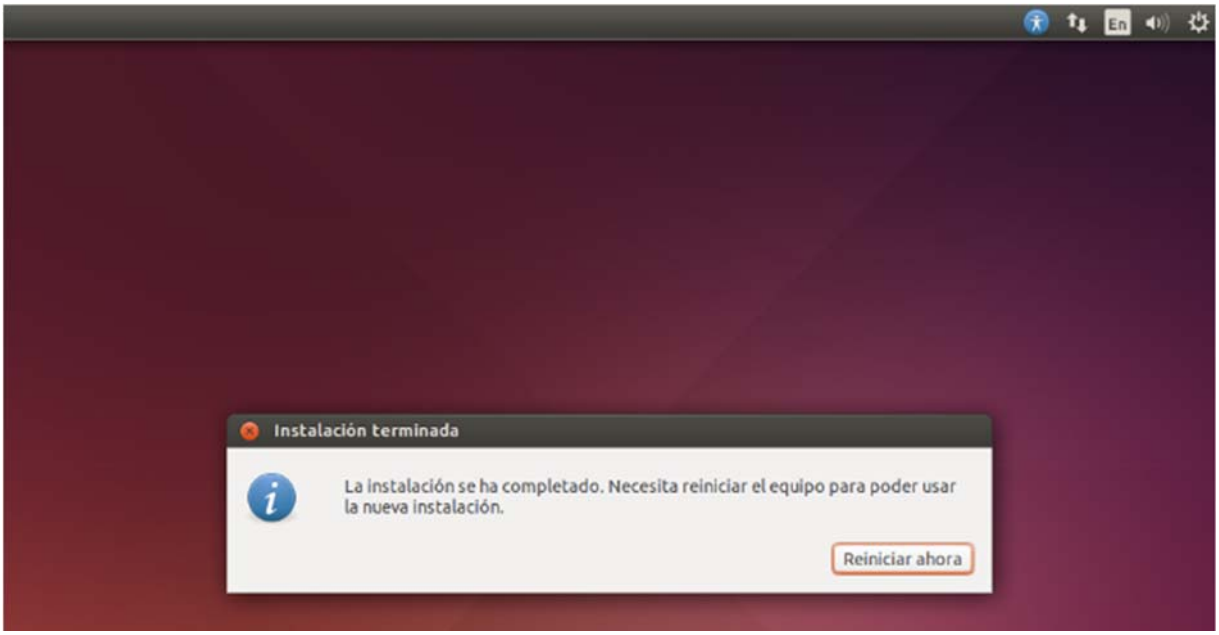
En la siguiente pantalla elegir el idioma del teclado, se puede escribir algo para comprobar que todo va correctamente.



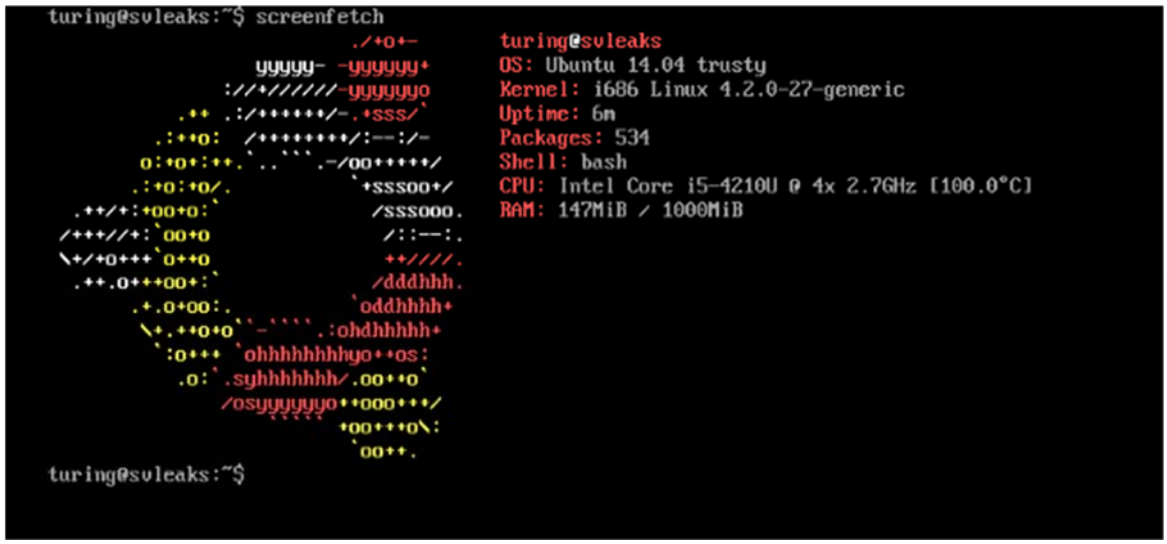
Luego se completa la configuración de nombre de usuario, el nombre del equipo y la contraseña, seleccionar “Solicitar contraseña para iniciar sesión” y “Cifrar carpeta personal” del perfil del sistema operativo que se está instalando.



En la siguiente pantalla se muestra la instalación final y luego se reinicia el sistema operativo



Información del sistema operativo instalado:


turing@svleaks:~$ screenfetch
turing@svleaks
OS: Ubuntu 14.04 trusty
Kernel: i686 Linux 4.2.0-27-generic
Uptime: 6m
Packages: 534
Shell: bash
CPU: Intel Core i5-4210U @ 4x 2.7GHz [100.0°C]
RAM: 147MiB / 1000MiB
turing@svleaks:~$

4.1.2 Instalación y configuración Básica de plataforma GlobalLeaks

En el siguiente apartado se muestran los comandos y pantallas utilizadas para la instalación y configuración de la plataforma Globalleaks. El comando de instalación que debe ser digitado en la terminal del servidor Ubuntu 14.04.5 LTS (Trusty Tahr):

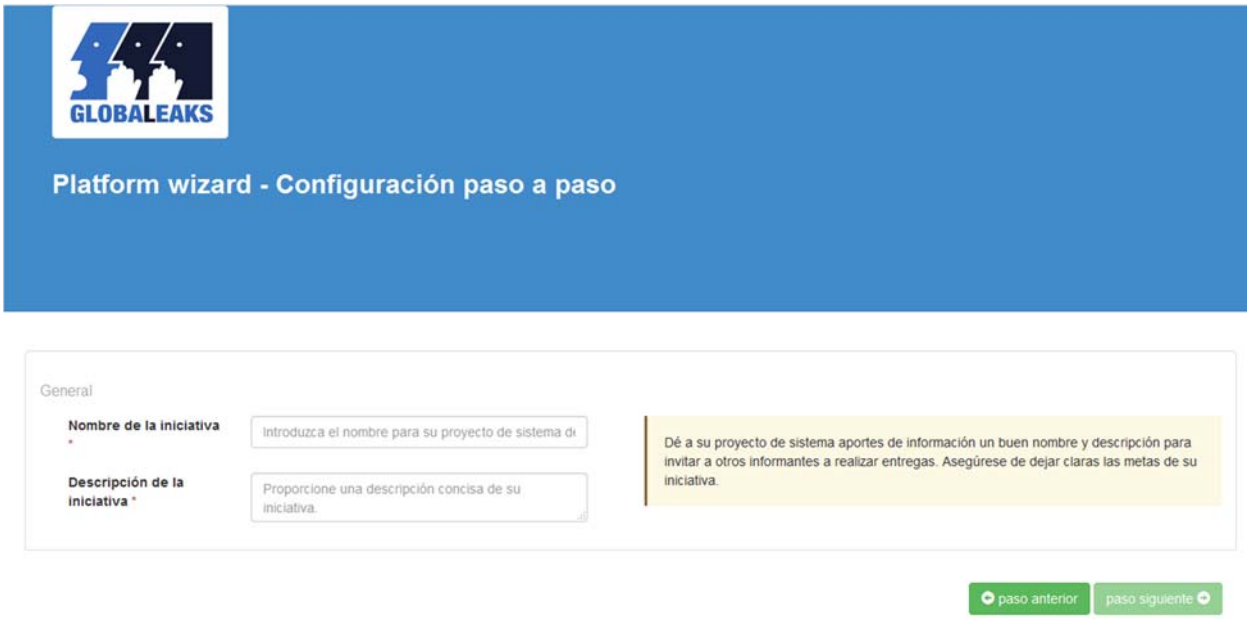
wget https://deb.globaleaks.org/install-globaleaks.sh chmod +x install-globaleaks.sh ./install-globaleaks.sh

A continuación se muestra la configuración básica de GlobalLeaks:

Pantalla Inicio - Configuración del idioma - Elegir el idioma principal del sitio. El valor predeterminado es el inglés, pero muchos otros están disponibles.

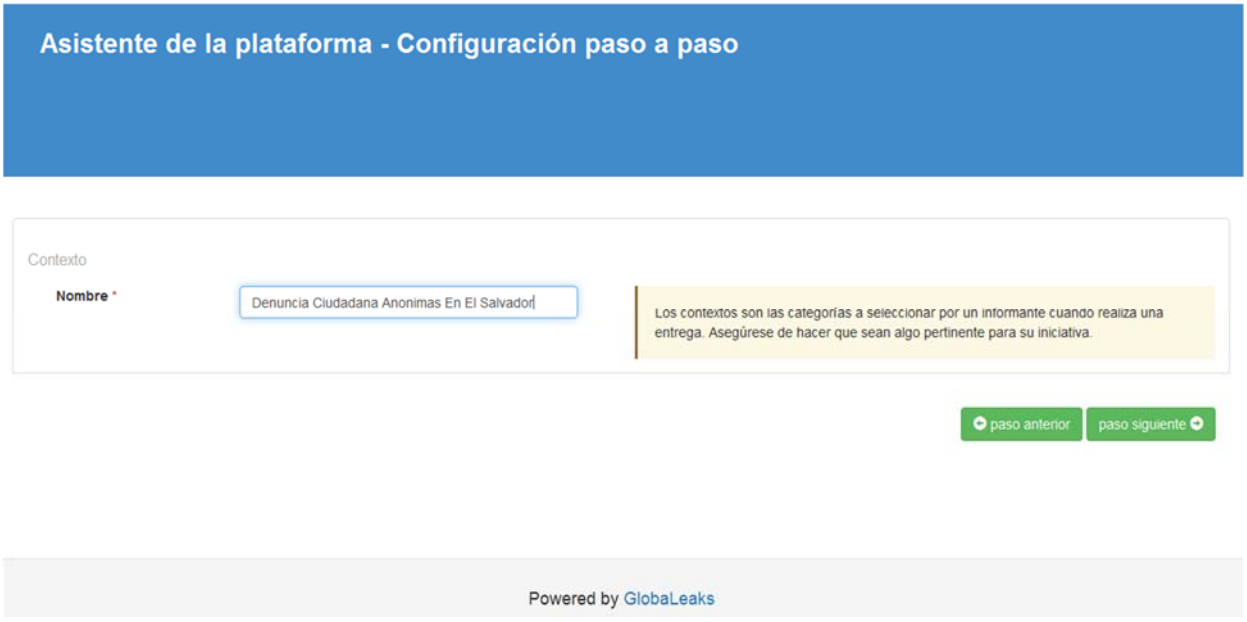
Pantalla de configuración general del proyecto. Los campos necesarios son, por sección:

Sección "General" se coloca el “Nombre del proyecto” y “Descripción del proyecto”.



Pantalla de Nombre del “Contexto” de la iniciativa de uso.

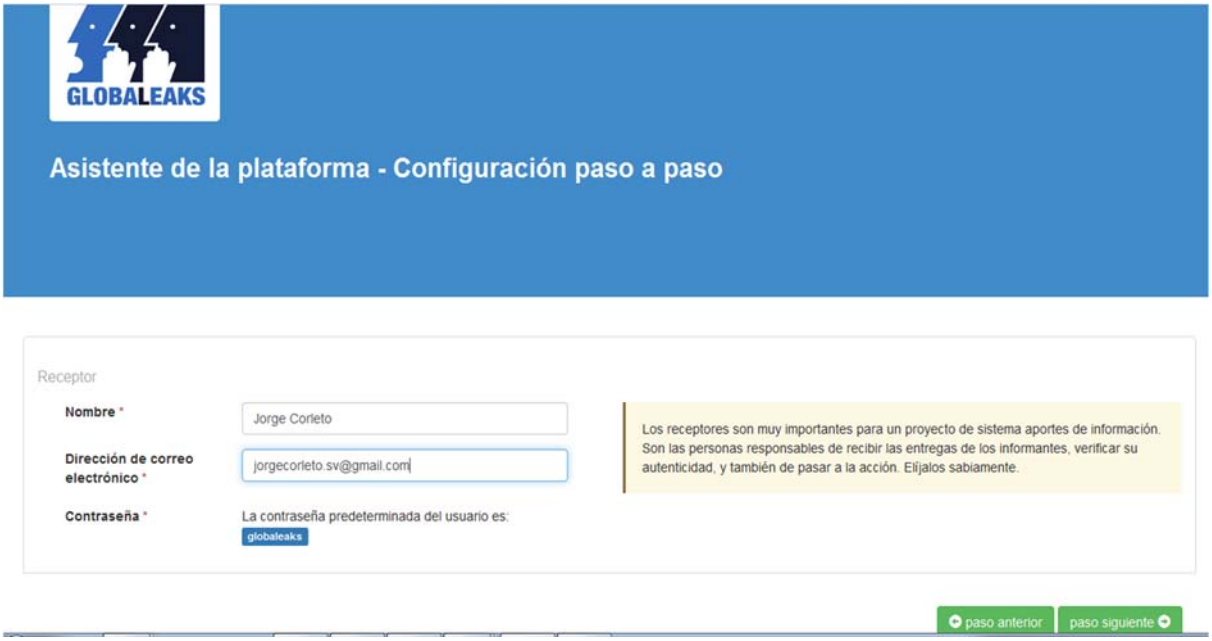
Sección "Contexto" - Nombre:



Pantalla de configuración de usuario de “Administrador” de la plataforma: Sección "Admin"

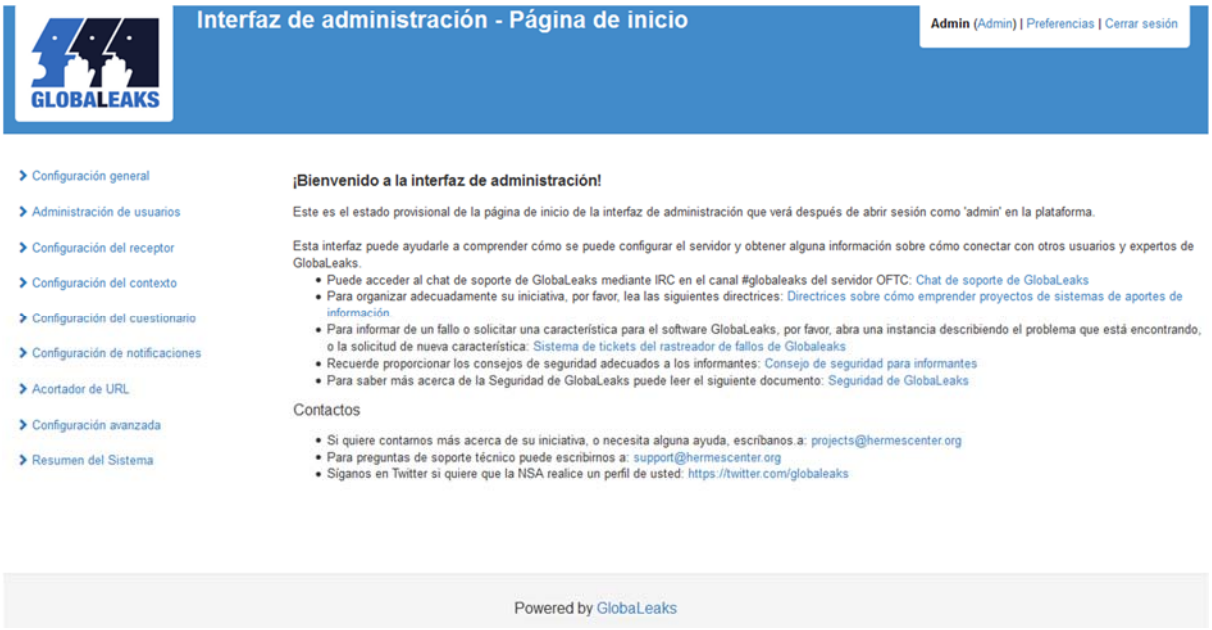
Se coloca la “Dirección de correo electrónico”, la “Contraseña” y la confirmación de la “Contraseña”.

Pantalla para validar los “Receptores” de la plataforma:



Pantalla de finalización de configuración básica de la plataforma:

Pantalla de bienvenida a la “Interfaz de administración” de la plataforma:



A continuación se personaliza la instalación, haciendo referencia a 8 pasos para recibir **anonymoussubmission que se envía a destinatarios configurados. (GitHub, 2016)**


De: GlobaLeaks - CHANGE EMAIL ACCOUNT USED FOR NOTIFICATION <notification@demo.globaleaks.org>
Fecha: 2 de diciembre de 2016, 19:14
Asunto: 20161203-1 Nueva entrega
Para: "jorgecorleto.sv@gmail.com" <jorgecorleto.sv@gmail.com>

Estimado Jorge Corleto,

Este es un correo para notificarle que un informante anónimo le ha seleccionado como un receptor valioso para su entrega.

Ellos desearían que prestase especial atención a la información y al material contenido ahí. Por favor, tenga en cuenta que los informantes a menudo se exponen a si mismos a elevados riesgos personales por el interés público. Por lo tanto, el material que proporcionan con estos reportes debe ser considerado de alta importancia.

La entrega es accesible:
vía Tor en: [CONFIGURED]
vía HTTPS en: [CONFIGURED]

Saludos cordiales,
ElSalvadorLeaks

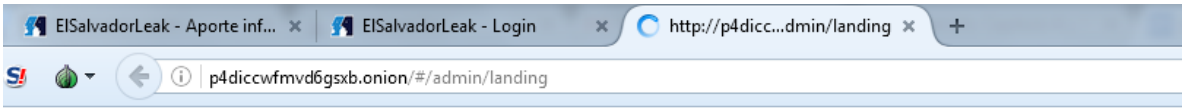
4.1.2.1 Configuraciones y personalización de GlobalLeaks

PASO 1 - Acceso a la interfaz de autenticación

La interfaz de autenticación es donde puede iniciar sesión. Tanto el administrador como los destinatarios pueden autenticarse con nombre de usuario y contraseña.

Puede acceder a la interfaz de autenticación con su navegador tor con el siguiente enrutamiento:

Desde tu nombre de host de Tor Hidden Service con Tor Browser. En el caso de esta instalación:

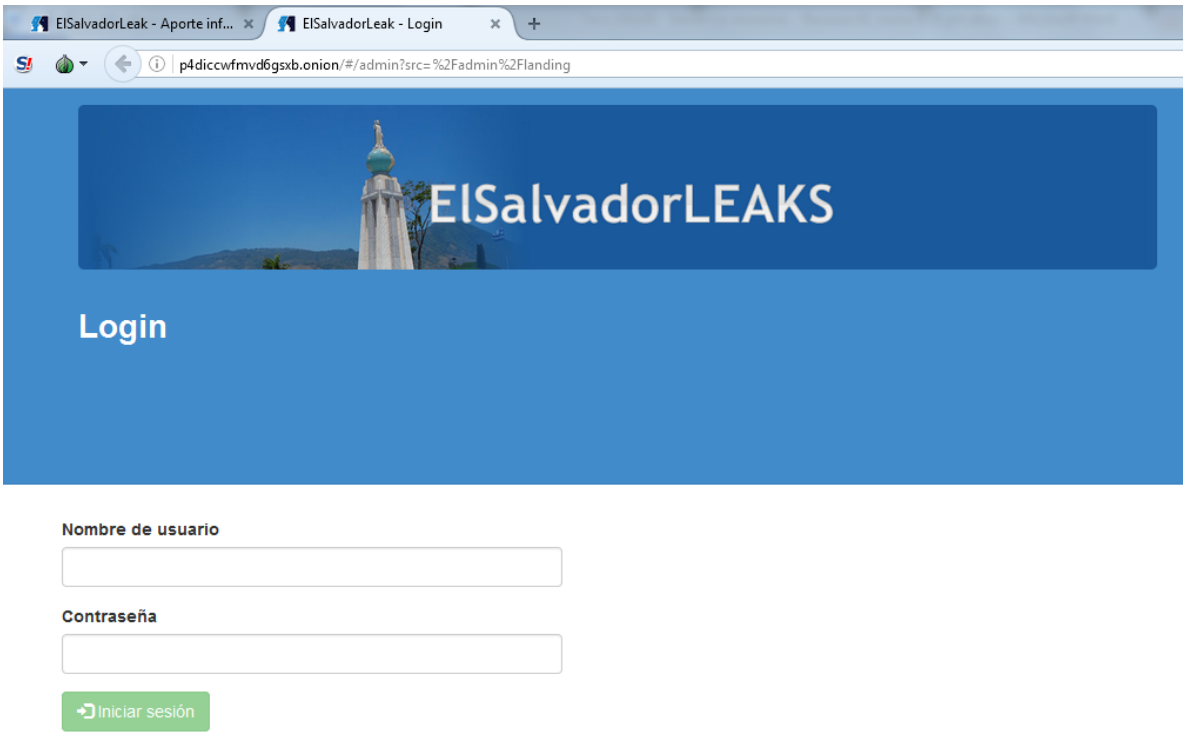


Direccionamiento a digitar el en browser de Tor **http://p4diccwfmvd6gsxb.onion/#/admin/landing**

Nota: La carga de la interfaz puede tardar un tiempo, debido a la alta latencia de Tor Hidden Service.

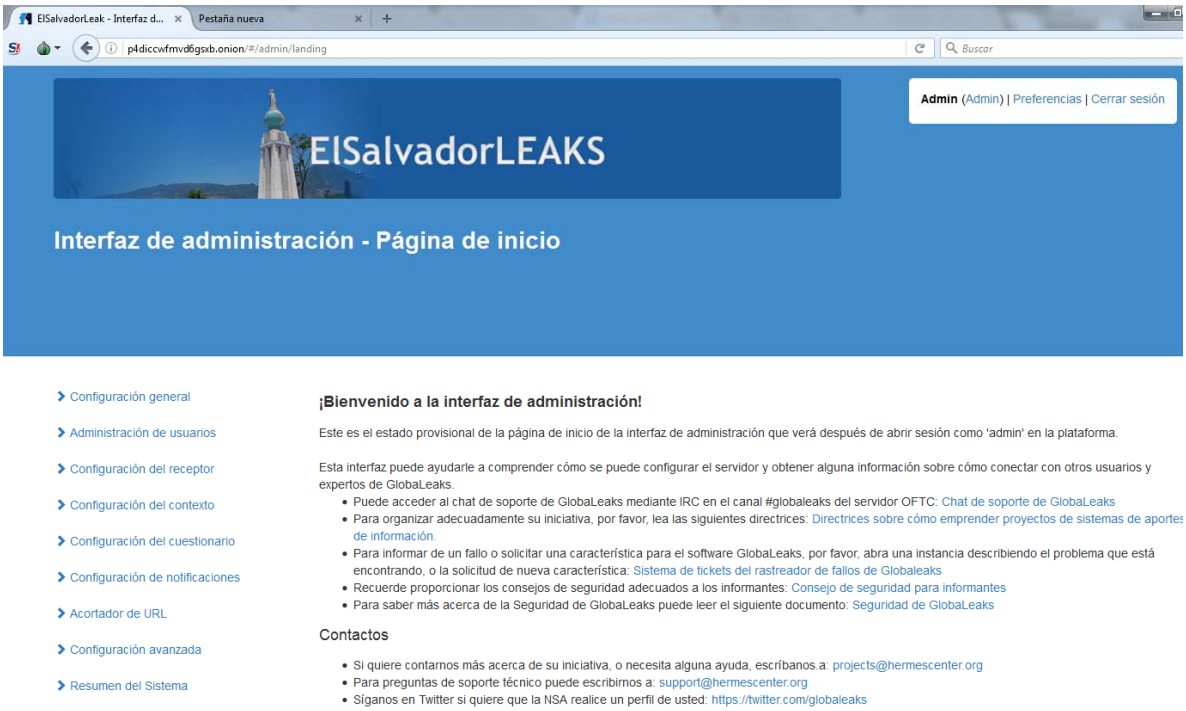
PASO 2 - Inicie sesión como administrador

Debe iniciar sesión en la interfaz de administración de su nodo GlobaLeaks.
http://p4diccwfmvd6gsxb.onion/#/admin/landing



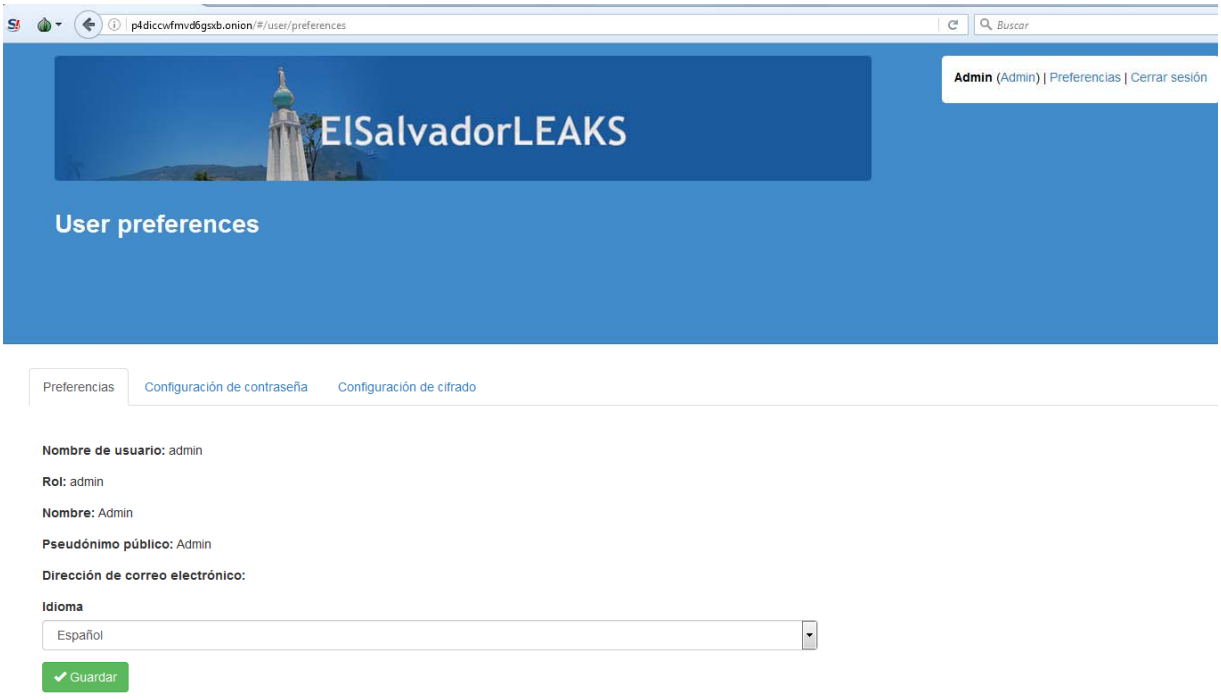
Iniciar sesión con las siguientes credenciales predeterminadas:

Usuario	**Contraseña**
admin	P31nandoLaGata123.

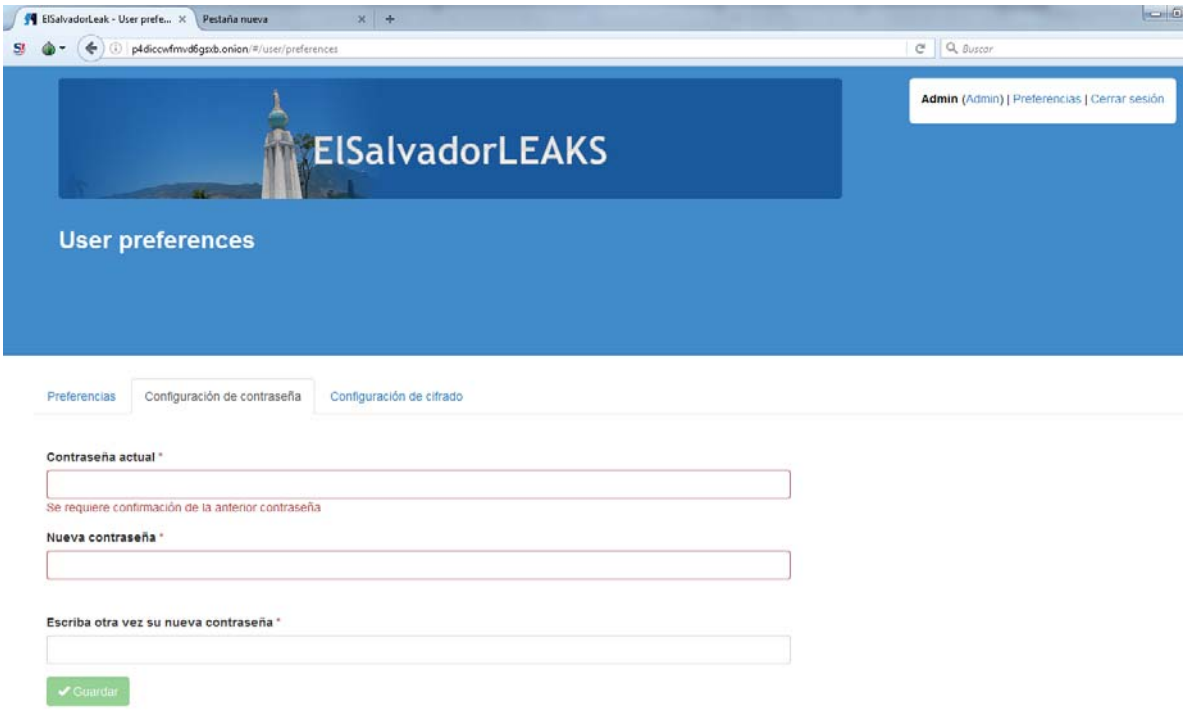


PASO 3 - Cambia tu contraseña de administrador

Haga clic en Admin Password. Como primer paso, debe cambiar la contraseña predeterminada de GlobaLeaks.



Cliquear la pestaña configuración de contraseña para cambia la ver la siguiente pantalla:



PASO 4 - Configure los datos básicos de GlobaLeaks

Haga clic en Configuración de contenido. Ha llegado el momento de configurar la información básica sobre la marca de su nodo.

Logo: Sube una imagen de 140x140 píxeles, en formato PNG

Seleccione Archivo

Haga clic en Cargar

Nombre del nodo: El nombre de su iniciativa (aparecerá en el encabezado)

Nodo Subtítulo: La recompensa que se mostrará con su nombre de nodo (aparecerá en el encabezado)

Descripción: Información sobre su iniciativa (aparecerá en el encabezado)

Correo electrónico: El correo electrónico al responsable de la iniciativa (Actualmente no utilizado por el software)

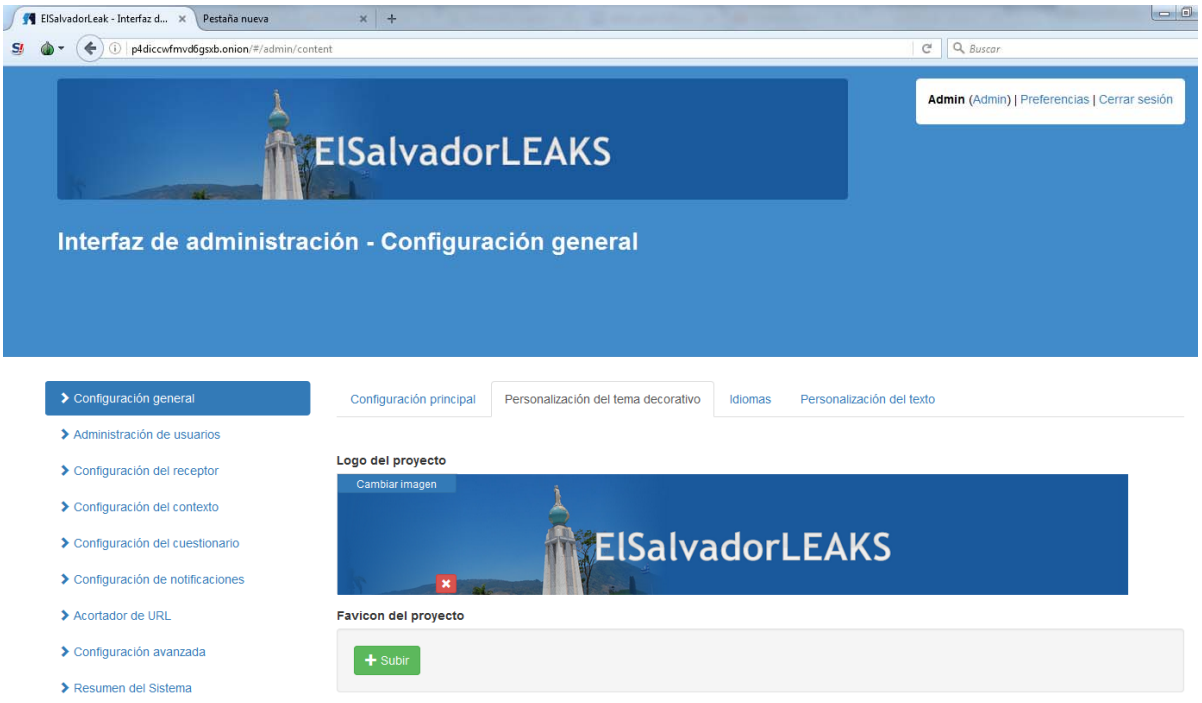
Presentación: El texto mostrado en la página de destino con el que se presentan los usuarios.

Pie de página: un pequeño texto mostrado en la parte inferior de cada página

Tor Hidden Service: Tu nombre de host Tor Hidden Service con HTTP: // (Usado en el correo electrónico de notificación)

Sitio Público de Tor2web: Su Sitio Público de Tor2web con HTTPS: // (Utilizado en el correo electrónico de notificación)


ElSalvadorLeak - Interfaz d...
Pestaña nueva
p4diccwfmvd6gsxb.onion/#/admin/content
Buscar
ElSalvadorLEAKS
Admin (Admin) | Preferencias | Cerrar sesión
Interfaz de administración - Configuración general
Configuración general
Administración de usuarios
Configuración del receptor
Configuración del contexto
Configuración del cuestionario
Configuración de notificaciones
Acortador de URL
Configuración avanzada
Resumen del Sistema
Configuración principal
Personalización del tema decorativo
Idiomas
Personalización del texto
Nombre de la iniciativa
ElSalvadorLeak
Título de la página principal
ElSalvadorLeak
Presentación
ElSalvadorLeak
Descripción
ElSalvadorLeak


ElSalvadorLeak - Interfaz d...
Pestaña nueva
p4diccwfmvd6gsxb.onion/#/admin/content
Buscar
ElSalvadorLEAKS
Admin (Admin) | Preferencias | Cerrar sesión
Interfaz de administración - Configuración general
Configuración general
Administración de usuarios
Configuración del receptor
Configuración del contexto
Configuración del cuestionario
Configuración de notificaciones
Acortador de URL
Configuración avanzada
Resumen del Sistema
Configuración principal
Personalización del tema decorativo
Idiomas
Personalización del texto
Logo del proyecto
Cambiar imagen
ElSalvadorLEAKS
Favicon del proyecto
Subir

PASO 5 - Configurar notificación por correo electrónico

Haga clic en Configuración de notificaciones. Configure la cuenta de correo electrónico y los parámetros del servidor relacionados, utilizados por GlobaLeaks para enviar notificaciones relacionadas con envíos a los destinatarios.

Le sugerimos que configure una cuenta de correo electrónico dedicada a enviar notificaciones de su iniciativa.

Introduzca los siguientes datos:

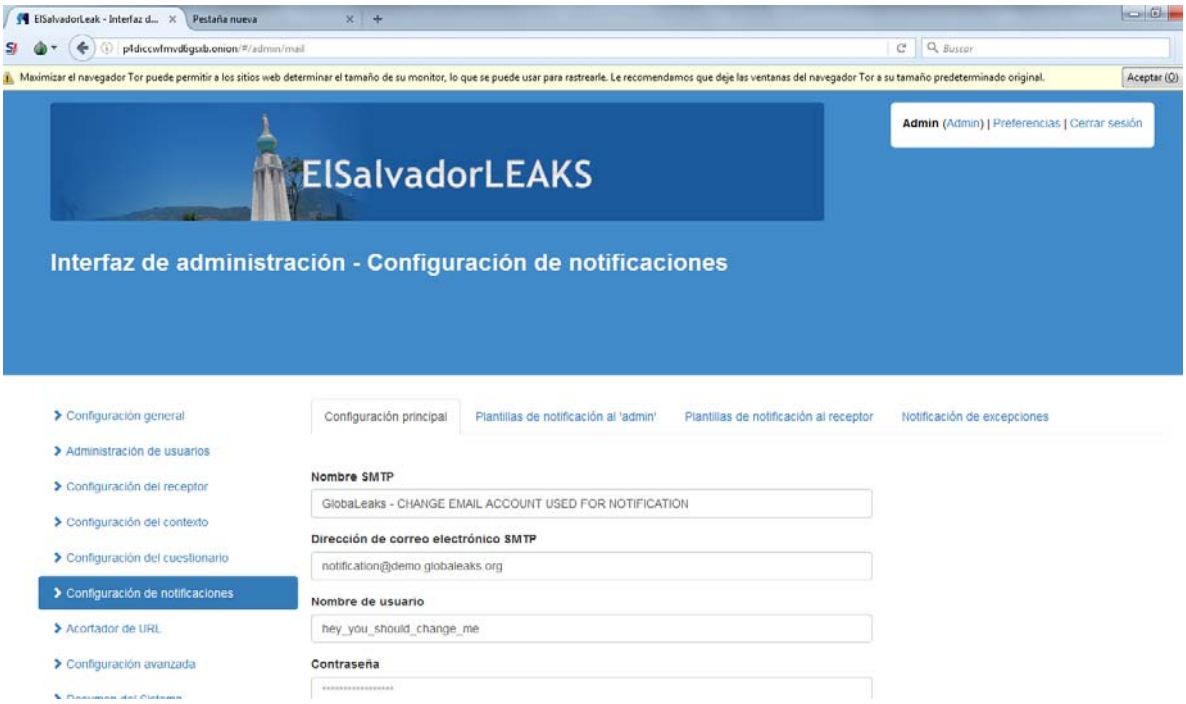
Nombre de usuario: Dirección de la cuenta de correo electrónico utilizada como nombre de usuario para enviar correo electrónico y autenticar con

Contraseña: Contraseña de la cuenta de correo electrónico

Servidor SMTP: Servidor saliente (SMTP) utilizado para enviar correos electrónicos desde esta cuenta

Puerto SMTP: Puerto utilizado para enviar correo electrónico saliente (puede ser 465 o 587 dependiendo de la configuración del servidor)

Seguridad de transporte: La seguridad de nivel de transporte de SMTP (SMTP con TLS está en el puerto TCP 587, pero SMTP con SSL está en 465)



PASO 6 - Agregar nuevos destinatarios

Haga clic en el destinatario. Ahora debe agregar a los destinatarios, personas que manejan las presentaciones de denunciantes.

Cada destinatario tiene que estar asociado con uno o más contextos, esto puede hacerse tanto desde la página "configuración del destinatario" como desde la página "configuración del contexto" después de crear el primer contexto.

Así que primero creemos al menos un destinatario.

Agregue el primer destinatario rellenando los datos siguientes y luego haga clic en Agregar.

Nombre: La dirección de su cuenta de correo electrónico. Se utiliza como nombre de usuario para enviar correo electrónico y autenticarse con

Correo electrónico: Contraseña de su cuenta de correo electrónico

Contraseña: La contraseña que utilizará el destinatario

Imagen: Cargue la imagen del destinatario (esto se mostrará en la interfaz de envío de denunciante)

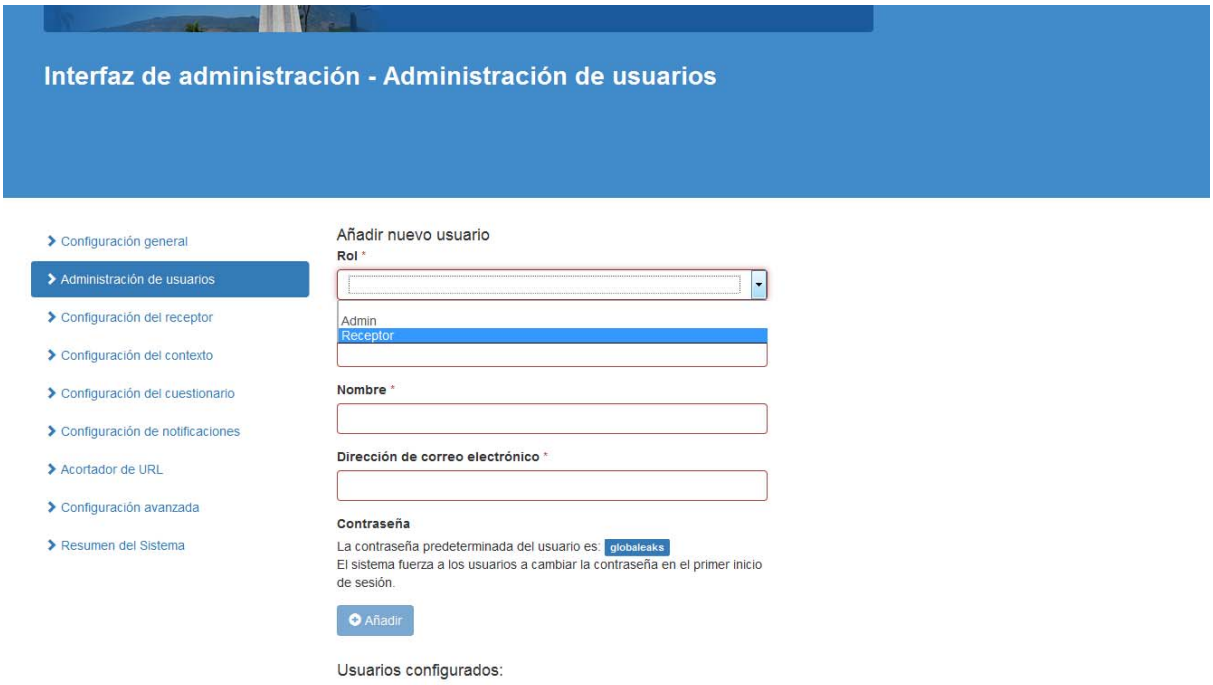
Descripción: Una breve descripción del destinatario

A continuación, debe agregar los destinatarios de la clave PGP haciendo clic en Configurar clave PGP. Cortar y pegar la versión ASCII (texto) de la clave pública PGP del destinatario.

Como último paso, puede otorgar al receptor una autoridad adicional:

Permitir que el destinatario aplace la fecha de vencimiento de las presentaciones

Almacene la cuenta del destinatario haciendo clic



PASO 7 - Crear nuevos campos contextuales y de presentación

Haga clic en Configuración de contexto.

El contexto representa el tema / categoría de su sitio de denuncia.

Puede ser una representación de un tema vertical (Corrupción, Abuso de Derechos Humanos, etc) o de un área geográfica para la que DEBE definir cuidadosamente:

Un conjunto de descripciones de contexto que se mostrarán al denunciante (como nombre y descripción)

Un conjunto de campos de presentación que representan las preguntas que usted desea hacer al denunciante

Un conjunto de destinatarios (personas que se ocupan de la presentación de ese tema específico)

Un conjunto de configuraciones avanzadas para personalizar varios criterios de seguridad / autorización y comportamientos de la interfaz de usuario.

En este paso editará:

Contexto: Representar los diferentes temas para los cuales su iniciativa GlobaLeaks acepta presentaciones

Destinatarios: Los destinatarios que forman parte de este contexto que reciben las presentaciones para ello.

Campos de presentación: Representa el contenido de la solicitud de formulario web y los datos que está solicitando al denunciante

Configuración de Contexto: Seguridad, Autorización y comportamiento de interfaz de usuarios específicos para ese contexto.

El procedimiento de configuración de Contexto es el siguiente:

Escriba el nombre de su contexto y luego haga clic en Agregar

Seleccione el destinatario que recibirá envíos para ese contexto específico

Añada una descripción sobre lo que es este contexto (qué tipo de información de presentación que desea recopilar)

Nota: Puede tener múltiples contextos para administrar varios temas y múltiples formularios de envío en una sola instalación.

Ahora puede administrar los campos de envío en la sección de campos del área de edición de contexto, haciendo clic en el campo Añadir.

Los campos de envió se pueden configurar para crear los formularios de envío con la siguiente información:

Nombre: una cadena corta que representa el campo (por ejemplo, mi título, no se mostrará)

Etiqueta: ¿Cuál es el título del campo?(se visualizará al remitente)

Sugerencia: lo que se muestra en mouseover para explicar el significado de este campo (se visualizará al remitente)

Requerido: Sí / No

Tipo: Botones de Radio, Menú Drop (Selección), Multi-Select, Casillas de verificación, Párrafo (s), Número, URL, Teléfono, Email

Los campos se mostrarán exactamente en el orden definido aquí. Sin embargo, es posible cambiar el orden arrastrando el contexto con el ratón y cayendo a la orden adecuada. También es posible cambiar el orden de los contextos a través de la interfaz de usuario con arrastrar y soltar.

Es muy importante marcar al menos un par de los campos más relevantes como "Preview". Éstos se mostrarán al destinatario en su interfaz de lista de envío, para proporcionar una mejor clasificación y comprensión de cada envío disponible en el sistema.

Por defecto hay dos Campos (que DEBEN ser modificados):

Titular

Descripción

Descripción del expediente

Nota: "Descripción del archivo" se convertirá en un campo dedicado asociado a cada archivo cargado con la implementación de https://github.com/globaleaks/GlobaLeaks/issues/719. Si desea ayudarnos a mejorar esta funcionalidad, considere hacer una donación en http://logioshermes.org/home/about-mission/support-us/.

En el contexto de ajustes avanzados es posible modificar todos los valores y comportamientos siguientes:

Requiere que se cargue al menos un archivo: ¿Es obligatorio cargar al menos un archivo para enviar una presentación en este contexto?

Seleccione todos los destinatarios de forma predeterminada: ¿Deberían seleccionarse todos los destinatarios de manera predeterminada para la presentación en este contexto? (El denunciante siempre puede desmarcarlos)

Mostrar tarjetas de pequeños destinatarios en la interfaz de envío: Si hay muchos destinatarios y desea mejorar la visualización, habilitar para mostrar las tarjetas del destinatario en líneas de 4.

Permitir a los destinatarios la posibilidad de posponer la fecha de vencimiento de las presentaciones: Decide si todos los destinatarios de este contexto pueden posponer la expiración de una presentación. (Para evitar la expiración de una presentación mientras se trata de un denunciante durante más días de lo permitido el tiempo de caducidad)

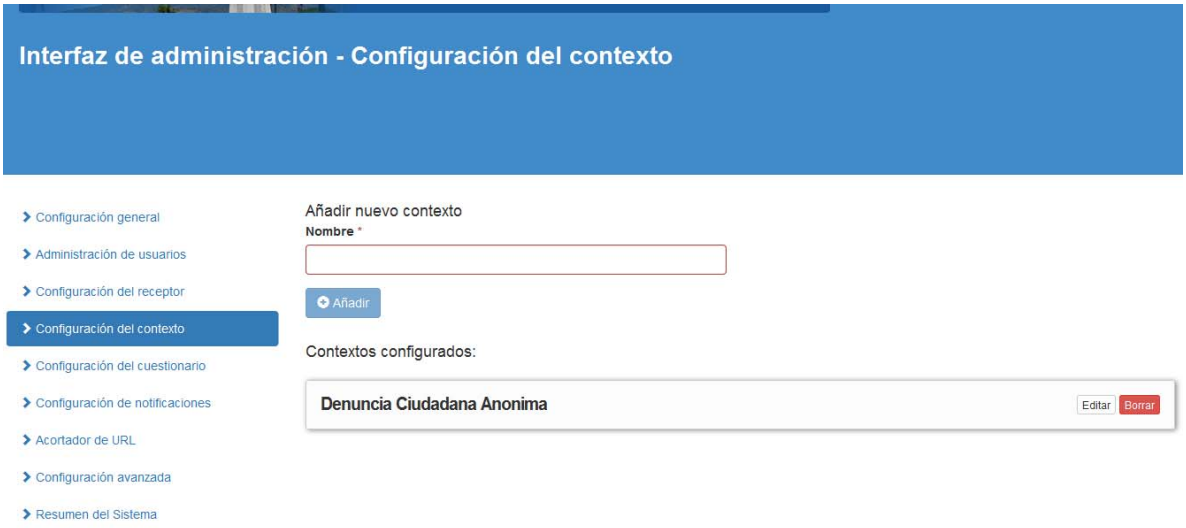
Permitir que los destinatarios eliminen envíos: ¿Pueden todos los destinatarios de este contexto eliminar las notificaciones?

Tiempo de expiración de las presentaciones incompletas (horas): Después de cuánto tiempo un envío incompleto debe ser auto-eliminado

Máximo de descargas de archivos: Cuántas veces un archivo puede ser descargado por los destinatarios

Tiempo de expiración de los envíos (días): Cuando el envío se borrará automáticamente (predeterminado 2 semanas)

Formato de recibo (expresión regular): ¿Qué formato es el recibo? (10 dígitos por defecto)



PASO 8 - Ajustar Ajustes Avanzados

El ajuste de los ajustes avanzados está sujeto a las necesidades fuera de lo ordinario de su iniciativa.

Los más interesantes son:

Tamaño máximo del archivo: establece un umbral en la cantidad de archivos que pueden cargarse (predeterminado 30 MB)

Política de retención de datos: El número de envíos de días se mantendrá antes de que se limpien y se eliminen automáticamente (predeterminado 15 días)

Informe de errores: dónde enviar informes de excepción si el software encuentra un error inesperado (por defecto info@globaleaks.org)

Configurar el acceso a la iniciativa a través de Tor2web:

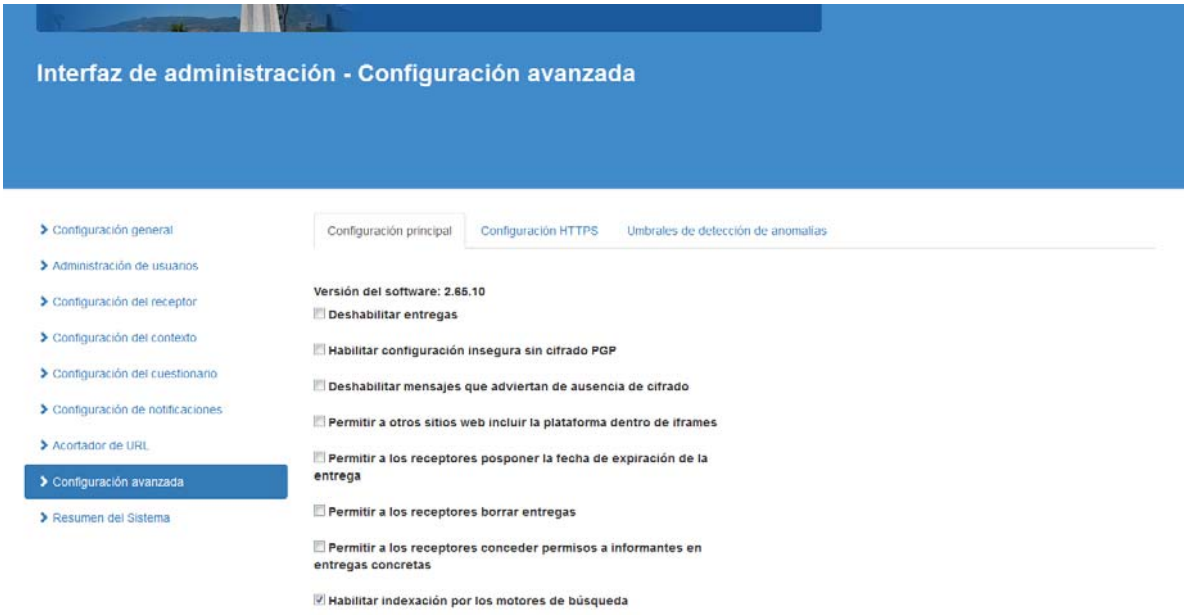
Permitir acceso de administrador a través de Tor2web

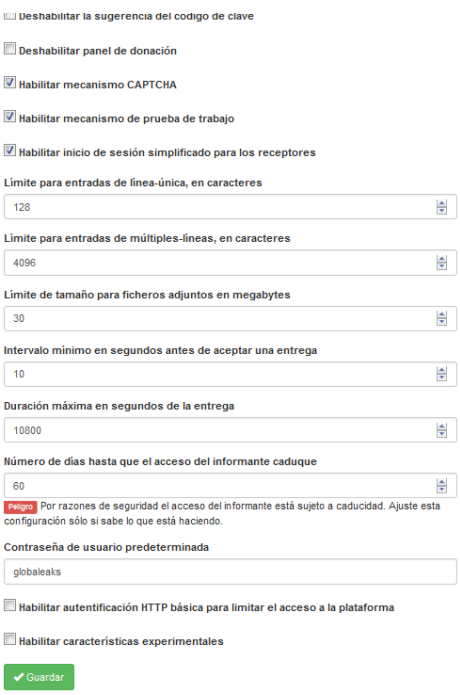
Permitir el acceso del destinatario a través de Tor2web

Permitir presentaciones de denunciantes a través de Tor2web

Permitir el acceso de los recursos públicos a través de Tor2web

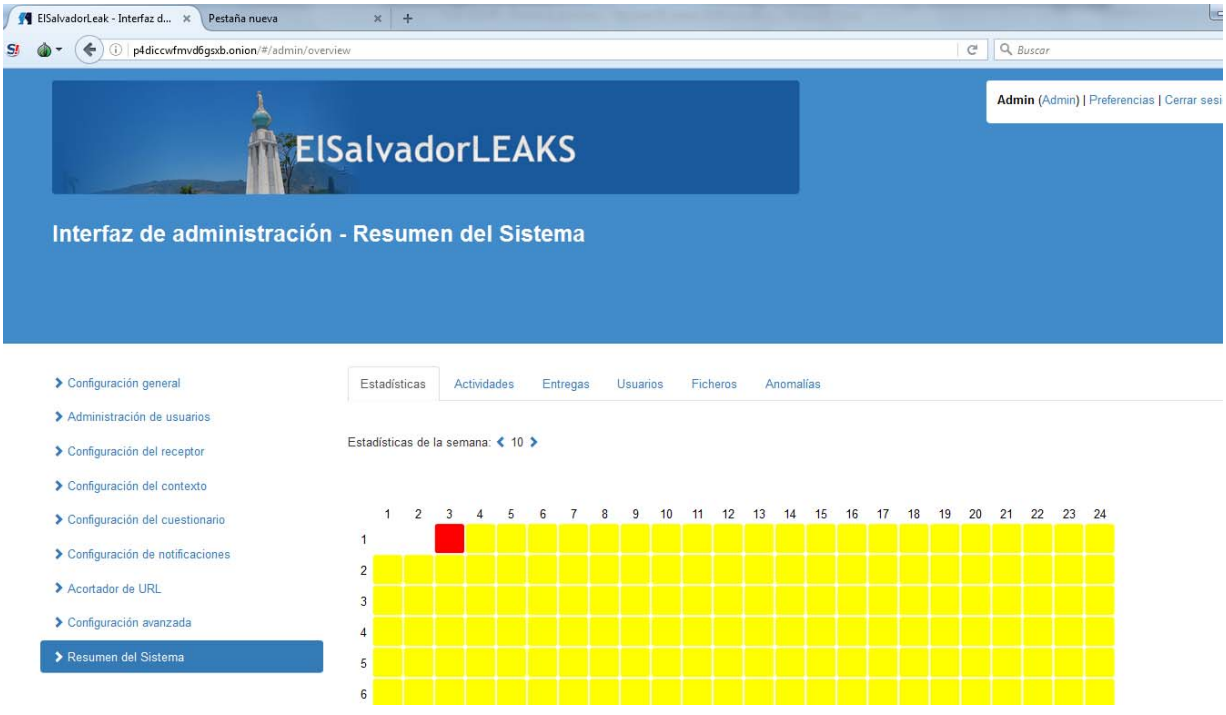
Lea Configuración avanzada para saber cómo cambiar esta configuración.





PASO 9 – Resumen de Sistema

En esta parte se presentan las estadísticas, actividad, entregas, usuarios, ficheros y anomalías.



4.1.2.2 Instalación del servidor Web

La instalación del servidor web Zope es realizado dentro del mismo comando de instalación de GlobalLeaks de tal forma que todo es ejecutado en el mismo paso (al cual se hace referencia en el apartado 4.1.2 de este mismo documento). Dentro del código de instalación del archivo "install-globaleaks.sh"(Deb.globaleaks.org, 2017) desde la línea 118 a la 126 se ve la instalación del software y lenguaje de programación Python, no es necesario realizar ningún cambio en el segmento de código, la funcionabilidad de las siguientes líneas de código es simplemente instalar el mencionado lenguaje de programación y las librerías (Zope incluida) que son posteriormente utilizadas por el Servidor de GlobalLeaks:

```
118 # on Ubuntu python-pip requires universe repository
119 if [ $DISTRO == "Ubuntu" ]; then
120   if [ $DISTRO_CODENAME == "precise" ]; then
121     echo "Installing python-software-properties"
122     DO "apt-get install python-software-properties -y"
123   else
124     echo "Installing software-properties-common"
125     DO "apt-get install software-properties-common -y"
126   fi
```

Al realizar la instalación de Python, se incluye la API de Zope (Pypi.python.org, 2017) el cual es el servidor web(Quintagroup.com, 2017) sobre el cual se ejecuta la plataforma GlobalLeaks.

4.1.2.3 Configuración y alojamiento en la red Tor

El alojamiento y configuración de la red Tor se realiza en código de instalación de GlobalLeaks (al cual se hace referencia en el apartado 4.1.2 de este mismo documento), dentro del archivo "install-globaleaks.sh". (Deb.globaleaks.org, 2017)

Para obtener la dirección ".onion" (dirección dentro de la red Tor) se debe ejecutar el comando "cat" dentro del directorio donde se encuentra compilado el servicio de Tor: cat /var/globaleaks/torhs/hostname

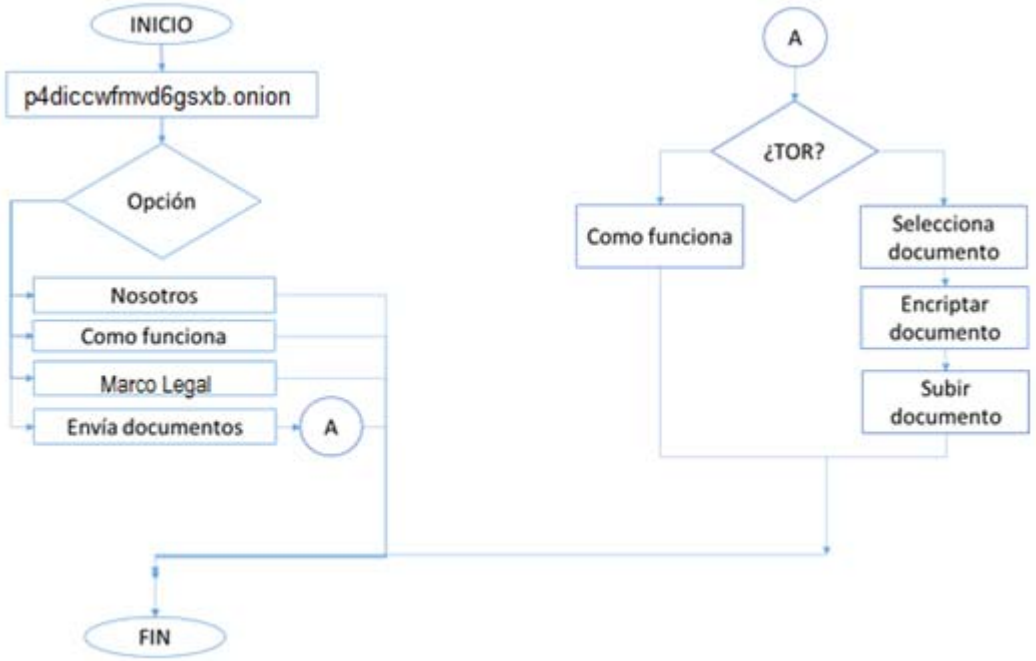
Ver dentro del código de instalación del archivo "install-globaleaks.sh"(Deb.globaleaks.org, 2017) desde la línea 151 a la 156:

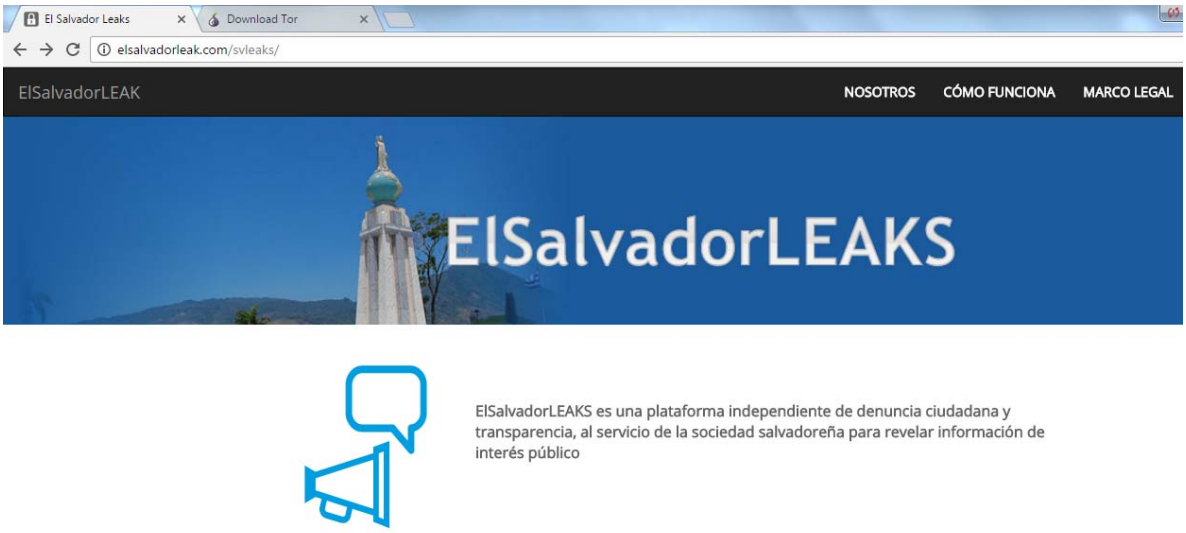
```
151 if [ -r /var/globaleaks/torhs/hostname ]; then
152   TORHS=`cat /var/globaleaks/torhs/hostname`
153   echo "To access your GlobaLeaks use the follc
154   echo "Use Tor Browser to access it, download
155   echo "If you need to access it directly on yc
156 fi
```

4.3 Sitio web Adaptación de contenido en la plataforma GlobalLeaks

El sitio web elsalvadorleak.com funcionará como como cualquier otro sitio web normal con información referente a las denuncias ciudadanas y una guía instalación del navegador Tor, y solo se diferenciará de otros sitios web en que este permitirá el envío de documentos y denuncias de a traves del navegador Tor para que sea desplegada la plataforma GlobalLeaks a traves de la direccion .onion p4diccwfmvd6gsxb.onion que debe ser colocada en el browser del navegador Tor.

El Siguiente diagrama muestra el funcionamiento del sitio web en internet y su funcionamiento con el navegador tor en la plataforma globalleaks.

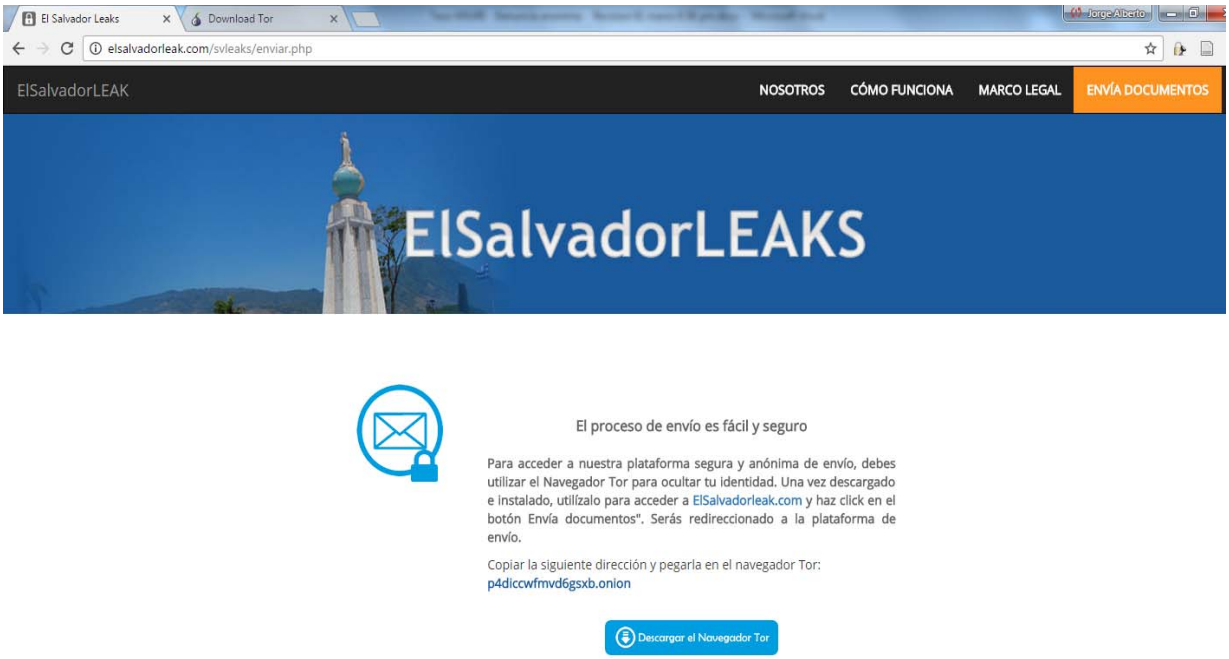




Pantalla de navegación pestaña NOSOTROS que describe el uso académico que se está realizando con la tecnología Tor y GlobalLeaks para denuncia ciudadana anónima.

Pantalla de navegación pestaña MARCO LEGAL que sustenta en El Salvador el uso del sitio.

Pantalla de navegación pestaña ENVIA DOCUMENTOS, describe el proceso de envío seguro del envío de la información



Una vez instalado el navegador Tor se copia y se pega la dirección .onion **p4diccwfmvd6gsxb.onion** en el browser para acceder a la plataforma GlobalLeaks que hace referencia a elsalvadorleak.com


Acerca de Tor
Buscar
Navegador Tor
6.0.8
Protegiendo a periodistas,
activistas e informantes desde 2006
Tor está en el corazón de la libertad en Internet
¡Done
ahora! »
Bienvenido al Navegador Tor
Ahora es libre de navegar por Internet anónimamente.
Probar las preferencias de red Tor
Busque de forma segura con Disconnect.me.
¿Qué sigue?
¡Tor NO es todo lo que necesita para navegar anónimamente! Puede necesitar cambiar alguno de sus hábitos de navegación para asegurar que su identidad permanezca segura.
¡Usted puede ayudar!
Hay muchas formas en que las puede ayudar a hacer la red Tor más rápida y fuerte.
Ejecutar un nodo de repetidor Tor »

4.4 Hardening del Servidor

Para realizar el hardening del servidor se procede a utilizar la herramienta Lynis(CISOfy, 2016), que permite identificar vulnerabilidades de seguridad en nuestro sistema Linux.

Previo a realizar todas los escaneos y configuraciones se debe ingresar al servidor Linux, con las credenciales del usuario “root”.

Servidor de la página web GlobalLeaks:

4.4.1 Instalación de la herramienta Lynis.

PASO Único: Para la instalación del paquete de la herramienta Lynis se procede a ejecutar el siguiente comando:

$ apt-get install lynis

4.4.2 Ejecución de la herramienta Lynis.

PASO 1: Se ejecuta el comando para auditar el servidor:

$ lynis audit system

PASO 2: Se analiza el resultado devuelto (Vista resumida):

NOTA: Se resume la visualización, por ser demasiado extensa para este documento.

```
################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2016, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################
[+] Initializing program
[+] System Tools
[+] Plugins (fase 1)
[+] Boot and services
```

[+] Kernel

[+] Memory and Processes

[+] Users, Groups and Authentication

[+] Shells

[+] File systems

[+] Storage

[+] NFS

[+] Name services

[+] Ports and packages

[+] Networking

[+] Printers and Spools

[+] Software: e-mail and messaging

[+] Software: firewalls

[+] Software: webserver

[+] SSH Support

[+] SNMP Support

[+] Databases

[+] LDAP Services

[+] PHP

[+] Squid Support

[+] Logging and files

[+] Insecure services

[+] Banners and identification

[+] Scheduled tasks

[+] Accounting

[+] Time and Synchronization

[+] Cryptography

[+] Virtualization

[+] Containers

[+] Security frameworks

[+] Software: file integrity

[+] Software: System tooling

[+] Software: Malware

[+] File Permissions

[+] Home directories

[+] Kernel Hardening

[+] Hardening

[+] Custom Tests

[+] Plugins (fase 2)

==

-[Lynis 2.4.0 Results]-

Warnings (4): …

Suggestions (46): …

==

Lynis security scan details:

Hardening index : 58 [###########]

Tests performed : 208

Plugins enabled : 0

Components:

- Firewall [V]

- Malware scanner [X]

Lynis Modules:

- Compliance Status [?]

- Security Audit [V]

- Vulnerability Scan [V]

Files:

…

4.4.3 Configuraciones para realizar hardening.

Con la revisión realizada en el apartado anterior se identifican las siguientes configuraciones que deben ser realizadas/mejoradas:

4.4.3.1 Apparmor:

Apparmor es una catarteristica incluida en el sistema operativo Ubuntu desde la versión 7.10, la funcion de esta carateristica es bloquear los procesos vulnerables.

PASO Unico: En este caso solo se validará que efectivamente este habilitado ejecutando el siguiente comando:

```
sudo apparmor_status
```

4.4.3.2 Configuración de Contraseña del Grub:

Por defecto las distribuciones más populares de Linux usan GRUB como su Bootloader. GRUB puede ser utilizado para seleccionar diversas imágenes de Kernel disponibles en la partición del sistema operativo, así como pasarle parámetros de booteo al Kernel. También nos permite bootear desde otra partición o dispositivo. GRUB puede ser utilizado para evadir cualquier medida de seguridad incluyendo la autenticación mediante el modo single User. Así que debemos proteger GRUB mediante un Password para mejorar la seguridad y que no puedan modificar los parámetros de booteo.

PASO 1: Lo anterior se logra con la ejecución del siguiente comando:

```
grub-mkpasswd-pbkdf2
```

PASO 2: Luego se ingresa la clave, y se generará la misma clave cifrada

4.4.3.3 Iptables:

En los servidores web uno de los ataques más frecuentes son aquellos en donde se usan direcciones IP enmascaradas o inválidas que intentan engañar al servidor para que entienda que los paquetes que recibe llegan desde la red interna o de una red confiable.

Otro de los eventos al que es expuesto es al escaneo de puertos de comunicación que tiene como objetivo ver que puertos de comunicación tiene abierto el equipo y así determinar los servicios que está corriendo y utilizar esa información como base a un posible ataque.

En el ANEXO 1 de este documento se.muestra un ejemplo de cómo puede restringirse/habilitarse características de seguridad atravez de las IP Tables.

El Script consiste en Reglas de Iptables para detener los paquetes inválidos y que llegan desde direcciones enmascaradas, intenta además detener el escaneo de puertos bloqueando por un tiempo determinado la dirección ip desde donde se origina. Otra de las mejores prácticas que se siguen aquí es la de Descartar las conexiones a todos los puertos de comunicación y solo crear reglas con los puertos que realmente vamos a necesitar.

El script permite las conexiones a los puertos HTTP (80), SSH (22), HTTPS (443), SMTP (25) y descarta cualquier otro.

4.4.3.4 Endurecimiento del servidor SSH

La configuración del servidor SSH permitirá proteger el acceso remoto:

4.4.3.4.1 Protocolo SSH versión 2

La versión 1 del protocolo SSH tiene un problema de vulnerabilidades de Seguridad. SSH-1 ya está obsoleto y se debe evitar. Para asegurar que se está corriendo la versión 2 se verifica el archivo sshd_config.

PASO 1: Ejecutar el siguiente comando.

vi /etc/ssh/sshd_config

PASO 2: Se verifica que esté la siguiente línea, si no está, será necesario agregarla.

Protocol 2

4.4.3.4.2. Limitar el acceso de usuarios vía SSH

Por Defecto todos los usuarios creados en un sistema linux pueden loguearse vía SSH usando sus contraseñas o llave pública. Al crear cuentas de usuarios para ftp, email u otro propósito, también se crea para estos usuarios también acceso a loguearse al sistema vía ssh lo que es una gran vulnerabilidad de seguridad. Estos usuarios tendrán acceso a herramientas del sistema y la capacidad de correr scripts ya sea para abrir puertos o hacer cualquier cosa. La mejor recomendación es limitar el acceso vía SSH.

PASO 1: Para esto se accede al archivo sshd_config

    # vi /etc/ssh/sshd_config

PASO 2: Si solo se quiere que se loguee vía ssh root, usuario1 y usuario2 modificamos lo siguiente en sshd_config

    AllowUsers root usuario1 usuario2

PASO: 3: Si solo se quiere bloquear los usuarios usuario3 y usuario4:

    DenyUsers usuario3 usuario4

4.4.3.4.3. Configure el LogOut por tiempo de inactividad

Es recomendable configurar esta directiva para evitar sesiones SSH desatendidas. Esto se configurar por igual en el archivo sshd_config.

PASO 1: Se accede al archivo sshd_config:

```
# vi /etc/ssh/sshd_config
```

PASO 2: Se modifica o agrega lo siguiente

```
ClientAliveInterval 300
```

Aquí se está indicando que pasado los 300 segundos sin entrada que desconecte el usuario.

4.4.3.4.5. Uso de contraseñas complejas

Es de vital importancia el uso de contraseñas complejas ya que los ataques de fuerza bruta utilizan claves basadas en diccionario.

4.4.3.4.6. Utilice Autenticación basada en llaves públicas

La autenticación mediante llaves públicas y privadas agrega una capa más de seguridad a las conexiones remotas y es un método de autenticación mucho más seguro. Una vez se confirma que la autenticación mediante las llaves se puede deshabilitar el acceso vía SSH a los servidores Linux usando contraseñas convencionales.

4.4.3.4.7. Deshabilitar la autenticación basada en Host

PASO 1: Para deshabilitar este método de autenticación, se accede al archivo en sshd_config.

```
# vi /etc/ssh/sshd_config
```

PASO 2: Se modifica la siguiente variable:

HostbasedAuthentication no

4.4.3.4.8. Filtrar las conexiones

Por defecto SSH permite conexiones desde cualquier dirección ip. Lo mejor es definir algunas reglas en Iptables para limitar las conexiones a una ip o segmento de red específico.

En este caso el puerto por defecto de SSH (22) o si se configura otro.

Para permitir la conexión SSH desde un segmento de red específico y bloquear las otras conexiones se hace lo siguiente como root:

PASO Unico: Ejecutar los siguientes comandos

iptables -A INPUT -p tcp -m tcp -s 192.168.3.0/24 –dport 22 -j ACCEPT

iptables -A INPUT -p tcp -m tcp -s 0.0.0.0 –dport 22 -j DROP

4.4.3.4.9. Port Knocking Para conexiones SSH

Port Knocking es una técnica utilizada para asegurar las conexiones o acceso a puertos a usuarios no deseados. Utilizando esta técnica se mantiene uno o varios puertos cerrados que previamente se configuran y estos solo serán abiertos usando una secuencia de solicitudes a una serie de puertos que también se configuran.

Para dar un ejemplo, se configura port Knocking para el acceso al puerto 50, pero este puerto solo se abrirá cuando se hagan las solicitudes de los puertos 1000,2500,3000 en ese mismo orden, al hacerlo así una vez completada la secuencia correctamente el firewall abrirá dicho puerto que previamente estaba cerrado.

Con esto se añade un filtro más de seguridad al servidor manteniendo los puertos sensibles cerrados y que solo serán abiertos con la secuencia de puertos que previamente se haya configurado.

Esta labor de Port Knocking se puede realizar usando Nmap, Telnet, o una herramienta para estos fines.

4.4.3.5. Incron

Incron es un demonio de Linux encargado del monitoreo de los directorios.

PASO 1: Lo primero es instalar Incron, desde la consola de Linux Ubuntu se ejecuta el siguiente comando:

sudo apt-get install incron

PASO 2: El siguiente paso consiste en añadir los directorios que se quieren monitorizar y las acciones a realizar:

incrontab -e

PASO 3: Para consultar las instrucciones que se han añadido se ejecuta el comando:

incrontab -l

4.4.3.6 Desinstalar compiladores

PASO 1: Ver la lista de paquetes instalados:

dpkg –list

PASO 2: Ver información del paquete especifico

dpkg –info nombredelpaquete

PASO 3: Para desinstalar el paquete se ejecuta el siguiente comando

apt-get remove nombredelpaquete

4.4.3.7. Hardening en el kernel

PASO Unico: Para el hardening del kernel se agregan las siguientes líneas al archivo “sysctl.conf”

```
$ sudo nano /etc/sysctl.conf

####### Agregar líneas #########

kernel.core_uses_pid = 1

kernel.kptr_restrict = 2

kernel.sysrq = 0

net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.all.log_martians = 1

net.ipv4.conf.all.send_redirects = 0

net.ipv4.conf.default.accept_redirects = 0

net.ipv4.conf.default.accept_source_route = 0

net.ipv4.conf.default.log_martians = 1

net.ipv4.tcp_timestamps = 0

net.ipv6.conf.all.accept_redirects = 0

net.ipv6.conf.default.accept_redirects =0
```

4.4.3.8 Cambiar puertos por defecto

En este caso se cambiará el puerto SSH. Por defecto SSH conecta desde todas las interfaces de Red y Direcciones ip del sistema. Se debe limitar las direcciones por donde conecta y cambiar el puerto por defecto de SSH (22). Por lo general los ataques de fuerza bruta intentan conectarse por el puerto 22.

PASO 1: Se accede al archivo sshd_config:

vi /etc/ssh/sshd_config

PASO 2: Se modifica lo siguiente:

port 2022

ListenAddress 192.168.3.1

ListenAddress 100.88.21.2

Aquí se esta indicando que solo permita conexiones por las direcciones 192.168.3.1, 100.88.21.2 y por el puerto 2022

Servidor de la página web ilustrativa:

NOTA IMPORTANTE: En este caso se decide alojar la página web ilustrativa en un Servidor Hosting, de tal forma que la seguridad en esta página ilustrativa sea administrada por el mismo proveedor.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

1) La integración de herramientas como Tor y GlobalLeaks ayudan a mejorar los niveles de seguridad de la información en las denuncias ciudadanas anónimas, cumpliendo con los siguientes puntos:

a) Confidencialidad: Se cumple la confidencialidad debido a que la información es enviada desde el origen de forma anónima utilizando Tor y llega al destino de forma cifrada utilizando GlobalLeaks, asegurando que únicamente el destinatario de la información pueda conocer el contenido de ella a través de su llave privada.
b) Disponibilidad: Se determina que el denunciante puede ingresar a la plataforma en el momento que decida realizar la denuncia y el destinatario puede tener acceso a la información cifrada en el momento que sea requerido. utilizando el navegador Tor conectándose a GlobalLeaks.
c) Integridad: La integridad de la información que viaja del origen al destino es respaldada por el protocolo TLS empleado en la red Tor y la integridad de la información almacenada en el servidor de la plataforma es respaldada por el hardening realizado al mismo.

2) La implementación de GlobaLeaks es muy amigable para personas que quieran iniciar un proyecto o actividad en iniciativas de sistemas anónimos para informantes. La plataforma está diseñada para realizar configuraciones asistidas que facilitara a los usuarios sin conocimientos técnicos la configuración personalizada según sus necesidades y protege por defecto la privacidad y las entregas de los usuarios.

3) En sociedades democráticas, una herramienta como GlobaLeaks pueden cumplir otro tipo de funciones. Concretamente, promover el papel de los whistleblowers (alertadores). Estas personas son las que denuncian situaciones irregulares, normalmente relacionadas con corrupción, en sus propias organizaciones.

5.2 Recomendaciónes

1) Es recomendable el uso de la tecnología GlobalLeaks y Tor para denuncias relacionadas al ámbito público o privado con el objetivo de que las personas, según el medio de implementación, puedan expresarse de forma anónima.

2) Es importante tener en cuenta que para garantizar la implementación y ciclo de vida sitios e iniciativas basadas en tecnología GlobaLeakas es fundamental el apoyo de asociaciones como Associated Whistleblowing Press (AWP)26, asimismo, la plataforma es impulsada por Globaleaks con apoyo del Centro Hermes de Transparencia y Derechos Humano Digitales.

3) La posibilidad de que la ciudadanía pueda denunciar y aportar pruebas de situaciones ilegales garantizando su anonimato por miedo a represalias, son actores principales en contexto de país donde se deben crear iniciativas de leyes que favorezcan la utilización de herramientas tecnológicas que faciliten la aportación de pruebas, más allá de la simple denuncia pública a través de redes sociales.

[26] Sitio Oficial de Associated Whistleblowing Press (AWP) https://awp.is/es/

GLOSARIO

Cifrado asimétrico: Es llamada también criptografía de llave pública es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado 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.

Criptografía simétrica: también llamada criptografía de clave secreta o criptografía de una clave.

Diffie-Hellman: 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).

DNS: (DNS, por sus siglas en inglés, Domain Name System) es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Este sistema asocia información variada con nombre de dominio asignado a cada uno de los participantes.

Keylogger: Es un software o hardware que puede interceptar y guardar las pulsaciones realizadas en el teclado de un equipo que haya sido infectado. Este malware se sitúa entre el teclado y el sistema operativo para interceptar y registrar la información sin que el usuario lo note.

Nodos OR: (OR, por si siglas en inglés Onion Router) Funcionan como encaminadores y en algunos casos además como servidores de directorio (DNS) de una especie de servicio de mantenimiento. Los nodos OR mantienen una conexión TLS con cada uno de los otros OR. Las conexiones OR-OR no son nunca cerradas deliberadamente salvo cuando pasa cierto tiempo de inactividad. Cuando un OR comienza o recibe nueva información de directorio él intenta abrir nuevas conexiones a cualquier OR que no esté conectado.

Nodos OP: (OP**,** por sus siglas en ingles Onion Proxy): Los usuarios finales ejecutan un software local que hace la función de nodo OP y que su función es obtener información del servicio de directorio, establecer circuitos aleatorios a través de la red y manejar conexiones de aplicaciones del usuario. Los OP aceptan flujos TCP de aplicaciones de usuarios y las multiplexa a través de la red OR's. Las conexiones OR-OP no son permanentes. Un OP debería cerrar una conexión a un OR si no hay circuitos ejecutándose sobre la conexión y ha vencido cierto temporizador

Protocolo TCP: (Protocolo de Control de Transmisión), uno de los principales protocolos de capa de transporte del modelo TCP, permite que se puedan administrar los datos al nivel más bajo del modelo, este protocolo se orienta a la conexión, es decir permite que dos máquinas través de comunicación controlen el estado de la transmisión.

RDSI: (Red Digital de Servicios Integrados, en ingles ISDN) como una evolución de las Redes actuales, que presta conexiones extremo a extremo a nivel digital y capaz de ofertar diferentes servicios.

TOR (The Onion Router): El más común, fue creado en el Laboratorio de Investigación Naval de EE.UU. como una forma segura de comunicación para militares. Tor está estructurado en nodos o capas, de forma que el usuario va saltando de capa en capa, protegido por una capa de cifrado que no permite que el servidor destino conozca su IP, contiene la una gran cantidad de servicios y a su propio navegador que facilita la búsqueda en el The Hidden Weeky; sin embargo al funcionar a través de un enrutado complejo, es muy fácil tener acceso a la Red TOR, es una buena opción para navegar de forma anónima y segura.

TLS: (TLS**,** por sus siglas en inglés Transport Layer Security(Seguridad en la Capa de Transporte), un protocolo criptográfico empleado en redes.

Hardening: (palabra en ingles que significa endurecimiento) en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios, etc. Innecesarios en el sistema así como cerrando puertos que tampoco estén en uso además de muchas otros métodos y técnicas que veremos durante este pequeño resumen introductorio al Hardening de sistemas.

Licencia AGLP: Licencia Pública General de Affero, es una licencia copyleft derivada de la Licencia Publica General de GNU diseñada específicamente para asegura la cooperación con la comunidad en caso de software que corran en servidores de red.

Software GlobalLeaks: Este software de denuncia de irregularidades es libre y de código abierto y utiliza la licencia AGPL. Está dotado de una comunidad abierta de usuarios, voluntarios y contribuyentes que trabajan juntos para mejorar constantemente el software y la documentación. Si usted ve un problema, crear un problema en nuestro sistema de tickets y ayúdanos a mejorar la transparencia en todo el mundo.

OAEP: En criptografía, Encapsulado de cifrado asimétrico óptimo (OAEP por sus siglas en inglés) es un esquema de encapsulado usado junto con el cifrado RSA. OAEP fue introducido por Mihir Bellare y subsecuentemente estandarizado en PKCS#1 v2 y RFC2437. Es una forma de las redes Feistel que usa un par de cajas negras (random Oracle) G y H para procesar texto plano en cifrado asimétrico.

REFERENCIAS BIBLIOGRÁFICAS

[1] Rights, H. (2016). *GlobaLeaks - Free Whistleblowing Software.* [online] GlobaLeaks. Disponible en: http://www.globaleaks.org [Accedido 24 Sep. 2016].

[2] Molleapaza Calamani, M. (2014). *¿Está roto el anonimato de Tor?*. [online] Revistasbolivianas.org.bo. Disponible en: http://www.revistasbolivianas.org.bo/scielo.php?script=sci_arttext&pid=S1997-40442014000100011&lng=es&nrm=iso [Accedido 20 Sep. 2016].

[3] Amaro López, J. A. A. (2015). El proyecto Tor. *Paakat: Revista de Tecnología y Sociedad*, *5*(9).Disponible en: http://www.suv.udg.mx/paakat/index.php/paakat/article/view/246/385 [Accedido 20 Sep. 2016].

[4] Es.wikipedia.org. (2016). *Tor (red de anonimato).* [online] Disponible en: https://es.wikipedia.org/w/index.php?title=Tor_(red_de_anonimato)&oldid=94603914 [Accedido 26 Oct. 2016].

[5] Goldschlag, D., Reed, M., & Syverson, P. (1999). *Onion routing. Communications of the ACM*, 42(2), 39-41.[Accedido 20-Nov-2016].

[6] Pagnotta, S. (2014). *Navegación anónima en Tor: ¿herramienta para cuidadosos o para cibercriminales?*. [online] WeLiveSecurity. Disponible en: http://www.welivesecurity.com/la-es/2014/07/02/navegacion-anonima-tor-herramienta-cuidadosos-o-cibercriminales/ [Accedido 2-Nov-2016].

[7] De La Luz, S. (2011). *Freenet : Instalación y Configuración de Freenet para saltarte la censura que hay en los programas P2P*. [online] Disponible en: http://www.redeszone.net/2011/02/19/freenet-instalacion-y-configuracion-de-freenet-para-saltarte-la-censura-que-hay-en-los-programas-p2p/ [Accedido 4-Nov-2016].

[8] Geti2p.net. (2017). *Introducción - I2P*. [online] Disponible en: https://geti2p.net/es/about/intro [Accedido 4-Nov-2016].

[9] Echeverri Montoya, D. (2016). *Deep Web: TOR, FreeNET & I2P - Privacidad y Anonimato*. Disponible en: http://0xword.com/es/libros/75-deep-web-tor-freenet-i2p-privacidad-y-anonimato.html [Accedido 3-Nov-2016].

[10] Lic. Alvarez Castaneda, R. (2016). *Entrevista con el Lic. Rafael Alvarez Castaneda, Abogado y Notario de la CSJ de El Salvador, sobre los aspectos legales de las denuncias ciudadanas anónimas.* [Entrevista realizada en 27-Nov-2016]

[11] Asamblea Constituyente (1983). *Constitución de la República de El Salvador. vol. 15, 1983*

[12] Asamblea Legislativa de El Salvador (2016). *«Ley Especial contra Delitos Informáticos y Conexos»*

[13] Asamblea Legislativa de El Salvador (2011). *«Ley de Acceso a la Información Pública»*

[14] Asamblea Legislativa de El Salvador (2011). *«Ley Especial para la Protección de Víctimas y Testigos»*

[15] Asamblea Legislativa de El Salvador (2011). *«Ley de Ética Gubernamental»*

[16] Pellerano, G. (2014). «GlobaLeaks Threat Model and Security Design» [Online]. Disponible es: https://docs.google.com/document/d/1niYFyEar1FUmStC03OidYAIfVJf18ErUFwSWCmWBhcA/pub [Accesido 10-Sep-2016].

[17] A. K. Hengartner y Greg Zaverucha (2007*). «Anonymity and Security in Delay Tolerant Networks»*, [En línea]. Disponible en: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.71.8314&rep=rep1&type=pdf. [Accedido 8-sep-2016].

[18] GitHub. (2016). *GlobalLeaks Configuration Guide*. [online] Disponible en: https://github.com/globaleaks/GlobaLeaks/wiki/Configuration-guide [Accedido 01 Ene 2017].

[19] CISOfy. (2016). *Lynis - Security auditing and hardening tool for Linux/Unix*. [online] Disponible en: https://cisofy.com/lynis/ [Accedido 03- Jan- 2017].

[20] Deb.globaleaks.org (2017). *"GlobaLeaks & Tor2web Package Repostory"*. [online] Disponible en: https://deb.globaleaks.org/install-globaleaks.sh [Accedido 5 Feb 2017].

[21] Pypi.python.org (2017). *zope.interface 4.3.3 : Python Package Index*. [online] Disponible en: https://pypi.python.org/pypi/zope.interface [Accedido 3 Feb 2017].

[22] Quintagroup.com (2017). *What is Zope?*. [online] Disponible en: http://quintagroup.com/cms/zope [Accedido 5 Feb. 2017].

[23] Assange,J (2010) *Why the world needs wikileaks* [online] Disponible en https://www.ted.com/talks/julian_assange_why_the_world_needs_wikileaks?language=es [Accedido 12 May. 2017].

ANEXO 1: EJEMPLO DE HARDENING CON IP TABLES

```
# Modify this file accordingly for your specific requirement.
# http://www.thegeekstuff.com
# 1. Delete all existing rules
iptables -F

# 2. Set default chain policies
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP

# 3. Block a specific ip-address
#BLOCK_THIS_IP="x.x.x.x"
#iptables -A INPUT -s "$BLOCK_THIS_IP" -j DROP

# 4. Allow ALL incoming SSH
#iptables -A INPUT -i eth0 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
#iptables -A OUTPUT -o eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT

# 5. Allow incoming SSH only from a sepcific network
#iptables -A INPUT -i eth0 -p tcp -s 192.168.200.0/24 --dport 22 -m state --state
NEW,ESTABLISHED -j ACCEPT
#iptables -A OUTPUT -o eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT

# 6. Allow incoming HTTP
#iptables -A INPUT -i eth0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
#iptables -A OUTPUT -o eth0 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT

# Allow incoming HTTPS
#iptables -A INPUT -i eth0 -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
#iptables -A OUTPUT -o eth0 -p tcp --sport 443 -m state --state ESTABLISHED -j ACCEPT

# 7. MultiPorts (Allow incoming SSH, HTTP, and HTTPS)
iptables -A INPUT -i eth0 -p tcp -m multiport --dports 22,80,443 -m state --state
NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -m multiport --sports 22,80,443 -m state --state ESTABLISHED -j
ACCEPT

# 8. Allow outgoing SSH
iptables -A OUTPUT -o eth0 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -i eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT

# 9. Allow outgoing SSH only to a specific network
#iptables -A OUTPUT -o eth0 -p tcp -d 192.168.101.0/24 --dport 22 -m state --state
NEW,ESTABLISHED -j ACCEPT
#iptables -A INPUT -i eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
```

```
# 10. Allow outgoing HTTPS
iptables -A OUTPUT -o eth0 -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -i eth0 -p tcp --sport 443 -m state --state ESTABLISHED -j ACCEPT

# 11. Load balance incoming HTTPS traffic
#iptables -A PREROUTING -i eth0 -p tcp --dport 443 -m state --state NEW -m nth --counter 0 --every
3 --packet 0 -j DNAT --to-destination 192.168.1.101:443
#iptables -A PREROUTING -i eth0 -p tcp --dport 443 -m state --state NEW -m nth --counter 0 --every
3 --packet 1 -j DNAT --to-destination 192.168.1.102:443
#iptables -A PREROUTING -i eth0 -p tcp --dport 443 -m state --state NEW -m nth --counter 0 --every
3 --packet 2 -j DNAT --to-destination 192.168.1.103:443

# 12. Ping from inside to outside
iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT

# 13. Ping from outside to inside
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT

# 14. Allow loopback access
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# 15. Allow packets from internal network to reach external network.
# if eth1 is connected to external network (internet)
# if eth0 is connected to internal network (192.168.1.x)
iptables -A FORWARD -i eth0 -o eth1 -j ACCEPT

# 16. Allow outbound DNS
#iptables -A OUTPUT -p udp -o eth0 --dport 53 -j ACCEPT
#iptables -A INPUT -p udp -i eth0 --sport 53 -j ACCEPT

# 17. Allow NIS Connections
# rpcinfo -p | grep ypbind ; This port is 853 and 850
#iptables -A INPUT -p tcp --dport 111 -j ACCEPT
#iptables -A INPUT -p udp --dport 111 -j ACCEPT
#iptables -A INPUT -p tcp --dport 853 -j ACCEPT
#iptables -A INPUT -p udp --dport 853 -j ACCEPT
#iptables -A INPUT -p tcp --dport 850 -j ACCEPT
#iptables -A INPUT -p udp --dport 850 -j ACCEPT

# 18. Allow rsync from a specific network
iptables -A INPUT -i eth0 -p tcp -s 192.168.101.0/24 --dport 873 -m state --state
NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 873 -m state --state ESTABLISHED -j ACCEPT

# 19. Allow MySQL connection only from a specific network
```

```
iptables -A INPUT -i eth0 -p tcp -s 192.168.200.0/24 --dport 3306 -m state --state
NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 3306 -m state --state ESTABLISHED -j ACCEPT

# 20. Allow Sendmail or Postfix
iptables -A INPUT -i eth0 -p tcp --dport 25 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 25 -m state --state ESTABLISHED -j ACCEPT

# 21. Allow IMAP and IMAPS
iptables -A INPUT -i eth0 -p tcp --dport 143 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 143 -m state --state ESTABLISHED -j ACCEPT

iptables -A INPUT -i eth0 -p tcp --dport 993 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 993 -m state --state ESTABLISHED -j ACCEPT

# 22. Allow POP3 and POP3S
iptables -A INPUT -i eth0 -p tcp --dport 110 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 110 -m state --state ESTABLISHED -j ACCEPT

iptables -A INPUT -i eth0 -p tcp --dport 995 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 995 -m state --state ESTABLISHED -j ACCEPT

# 23. Prevent DoS attack
iptables -A INPUT -p tcp --dport 80 -m limit --limit 25/minute --limit-burst 100 -j ACCEPT

# 24. Port forwarding 422 to 22
iptables -t nat -A PREROUTING -p tcp -d 192.168.102.37 --dport 422 -j DNAT --to
192.168.102.37:22
iptables -A INPUT -i eth0 -p tcp --dport 422 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 422 -m state --state ESTABLISHED -j ACCEPT

# 25. Log dropped packets
iptables -N LOGGING
iptables -A INPUT -j LOGGING
iptables -A LOGGING -m limit --limit 2/min -j LOG --log-prefix "IPTables Packet Dropped: " --log-
level 7
iptables -A LOGGING -j DROP
```