Revisión de la tecnología de redes Peer to Peer (P2P) seguras y sus posibles aplicaciones en entornos gubernamentales

FÉLIX LEONARDO ESCALANTE LEMUS

JUAN CARLOS PERTUZ OSPINA

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FÍSICO MECÁNICAS
ESCUELAS DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2011

Revisión de la tecnología de redes Peer to Peer (P2P) seguras y sus posibles aplicaciones en entornos gubernamentales

FÉLIX LEONARDO ESCALANTE LEMUS

JUAN CARLOS PERTUZ OSPINA

Monografía para optar el título de Especialista en Telecomunicaciones

Director

MIE. José Rugeles Uribe

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FÍSICO MECÁNICAS
ESCUELAS DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2011

AGRADECIMIENTOS

Todo éxito en la vida es producto de una serie de esfuerzos hechos por aquellos que llegan a gozar de las mieles del triunfo porque algún día se lo propusieron.

Agradecemos a Dios por ser el otorgante de vida, inteligencia y el espacio para nuestro estudio. A nuestras familias, soporte permanente de nuestras dichas y penas. A nuestros docentes por compartirnos su sabiduría y memorias. Finalmente a nuestros colegas compañeros de clases con quienes establecimos una entrañable amistad que se ha prolongado extra muros. Esto es un logro de todos.

CONTENIDO

Pag.

LISTA DE FIGURAS

Pag.

LISTA DE TABLAS

Pág.

GLOSARIO

TIC - Tecnologías de la Información y las Comunicaciones, agrupan un conjunto de elementos, técnicas, desarrollos y dispositivos utilizados en el tratamiento, almacenamiento, procesamiento y transmisión de la información.

Intranet - Es una red de equipos de cómputo pertenecientes a una organización privada, que utiliza Internet para compartir dentro de sus miembros, sistemas de información, bases de datos, documentos, entre otros sistemas operacionales.

Nodo - En informática, hace referencia a cualquier punto de conexión en una red, normalmente un nodo es cada una de los equipos de cómputo que la componen y que cumple una función específica para más de un usuario.

Teras - Un tera hace referencia a la unidad de almacenamiento de información terabyte, cuyo símbolo es TB y equivale a 10^{12} bytes.

Copyright - Derecho de autor. Conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores (los derechos de autor), por el solo hecho de la creación de una obra literaria, artística, científica o didáctica, esté publicada o inédita.
En el derecho anglosajón se utiliza la noción de copyright (traducido literalmente como "derecho de copia") que por lo general comprende la parte patrimonial de los derechos de autor (derechos patrimoniales).

Streaming - Es una tecnología que hace posible escuchar música y ver videos por Internet sin interrupción, permitiendo almacenar en un búfer la información recibida, sin necesidad de realizar una descarga previa. Consiste en la distribución de audio y video por Internet.

Hash - Hace referencia a una función o algoritmo que permite generar claves o llaves que identifiquen de manera única a un documento, archivo, registro, asegurando la integridad de su contenido.

Indexar - Corresponde al hecho de elaborar un índice en cuyo contenido se sostiene una información específica de manera ordenada y organizada, de tal manera que sea posible obtener resultados de una búsqueda de forma más rápida y eficiente.

Ping - Es una herramienta diagnóstica que permite verificar la conectividad en redes, comprueba el estado de la conexión y determina si es posible alcanzar a un host destino, por medio del envío de paquetes ICMP de solicitud y respuesta (Echo y Echo Reply).

Traceroute - Es una herramienta que permite la estimación de la distancia a la que se encuentran los extremos de una comunicación, de tal manera que permite conocer los saltos realizados para lograr la misma, mediante el envío de datagramas IP con bajos tiempos de vida.

Procedimientos - En la cadena de las políticas de seguridad los procedimientos corresponden a los pasos detallados que se deben seguir para realizar una tarea específica, proporcionando una guía detallada para la implementación de políticas, estándares y lineamientos previamente establecidos. Son considerados como guías para una buena práctica. Definición tomada de INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN [1]

Lineamientos - Hacen referencia a las metodologías implementadas para asegurar un sistema, no son de carácter obligatorio, y son referenciados como acciones recomendadas. Son usados para indicar la manera de hacer cumplir un estándar. Definición tomada de INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN [1]

Estándares – Especifican de forma uniforme el uso de tecnologías específicas. Su función corresponde a la generalización de las metodologías usadas en los controles de seguridad. Tienen un carácter obligatorio y deben implementarse

uniformemente en toda la organización. Definición tomada de INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN [1]

Confidencialidad – Principio que evita la divulgación intencional o accidental del contenido de cualquier información.Definición tomada de INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN [1]

Integridad – Principio que garantiza la exactitud de una información completa. Definición tomada de INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN [1]

Disponibilidad – Principio que asegura que usuarios autorizados en una red puedan tener acceso confiable y oportuno a la información en el momento que se requiera.Definición tomada de INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN [1]

Hosting -Servicio ofrecido a los usuarios con el fin de brindar la posibilidad de almacenar o alojar el contenido accesible vía web (sitio web, correo electrónico, archivos, imágenes, videos).

RESUMEN

TÍTULO:

REVISIÓN DE LA TECNOLOGÍA DE REDES PEER TO PEER (P2P) SEGURAS Y SUS POSIBLES APLICACIONES EN ENTORNOS GUBERNAMENTALES.[*]

AUTORES:

FÉLIX LEONARDO ESCALANTE LEMUS
JUAN CARLOS PERTUZ OSPINA[**]

PALABRAS CLAVES:

Redes, P2P, Peer to Peer, Seguridad, Enrutamiento, Protocolo, Conectividad, Gobierno.

DESCRIPCIÓN:

Las redes P2P iniciaron como un método para compartir recursos informáticos ya sea de almacenamiento, procesamiento o redundancia en equipos de investigadores o entusiastas de la red. Con el tiempo fue tomando un un tinte ilegal por su utilización, debido a que se usaba para compartir contenidos con derechos de autor. Una nueva tendencia nace buscando tornar las Peer to Peer en redes más seguras, estables y económicas. Al mismo tiempo los gobiernos de los países del mundo buscan alternativas electrónicas, que les permita establecer conexiones más estrechas con sus ciudadanos. Colombia no es la excepción y con su iniciativa de Gobierno en Línea está dando pasos muy acertados en materia de optimizar los procedimientos llevados a cabo por organismos estatales, buscando beneficiar y facilitar los trámites de los ciudadanos, todo esto bajo el uso y apropiación de las tecnologías de la información y las comunicaciones.

Con este documento se pretende dar a conocer el estado actual de las redes P2P seguras, su proyección y avance, así como las políticas adoptadas en materia de conectividad por parte del Gobierno Nacional, fundamentos que permitirán analizar la posibilidad de implementar esta tecnología en una entidad del gobierno atendiendo los riesgos y beneficios que esto conllevaría.

[*] Trabajo de Grado

[**] Facultad de Ingenierías Físico-Mecánicas. Escuela de Ingenierías Eléctrica, Electrónica, y de Telecomunicaciones. Director: Ing. José de Jesús Rugeles Uribe

SUMMARY

TITTLE

PEER-TO-PEER (P2P) TECHNOLOGICAL REVIEW AND ITS POSSIBLE APPLICATION IN GOVERMENT ENVIROMENTS*

AUTHORS

FÉLIX LEONARDO ESCALANTE LEMUS
JUAN CARLOS PERTUZ OSPINA **

KEY WORDS

Netowrks, P2P, Peer to Peer, Security, Routing, Protocol, Conectivity, Goverment.

DESCRIPTION

Peer-to-peer networks began as a method to share computer resources meaning storage, processing power o machine redundancy. This test were held by computer investigators or enthusiast over the world. With time an illegal shadow posed over the issue because it was used as a copyrighted material sharing tool. A new tendency recently has born seeking for secure, private, cheaper and stable P2P networks. Simultaneously, goverments around the globe are looking for electronical alternatives to help them keep a closer relationship with their citizens. Colombia is no exception and with its "Gobierno en Linea" iniciative is taking giant steps, looking a benefit and to ease the paperwork between users and the state. All this towards the correct use, ownership of the IT and Communications.

This document will show the state of the art of the actual secure P2P networks iniciatives, their objectives and actual achievements, also the Colombian Goverment's iniciatives towards citizens conectivity. This information will work as a basis to analyze the posibility of implementing this technology in a goverment office paying attention to its benefits and risks.

* Project of Degree

** Physical-mechanics Engineerings Faculty. Electricity, Electronics and Telecommunication Engineerings School. Manager: Eng. José de Jesús Rugeles Uribe.

INTRODUCCIÓN

En el mundo actual, es impensable concebir nuestras vidas sin el apoyo de las TIC[1]. La tecnología invade nuestras vidas y nuestros trabajos, y en el mundo empresarial se ha convertido en el socio estratégico, hecho que se ha visto reflejado en el aumento de producción. Hoy en día es muy común encontrar empresas cuya única fachada es una página web, unos correos electrónicos y algunos números de teléfono celular, sin ningún tipo de infraestructura que soporte sus actividades. Todo esto ha incrementado las posibilidades de establecer negociaciones, modelos, cotizaciones y servicios sin necesidad de existir contacto físico entre los miembros en el intercambio comercial.

La apropiación de estas tecnologías no sólo son adoptadas por las PyMEs[2], esta novedosa manera de llevar a cabo la gestión comercial también es aplicada en las grandes empresas. Dentro del ambiente gubernamental actual, es común encontrar entidades con portales donde los consumidores interactúan para gozar de los bienes y servicios ofrecidos por la empresa, además de contar con intranet donde se comparten recursos, archivos, datos y procesos internos, para los cuales se emplea una seguridad en diferentes niveles, dependiendo de la criticidad de la información. Vale la pena recordar que los entornos gubernamentales manejan información muy sensible para la comunidad como son los impuestos, registros de atención en salud, pasado judicial, central de riesgos, catastro, entre otros, lo que conlleva a tomar medidas más profundas de seguridad.

Las Redes P2P han evolucionado de su estatus de foco de piratería a convertirse en una plataforma que aprovecha los equipos de una red cualquiera para compartir recursos entre ellos y así hacer de esta una comunidad robusta para compartir archivos, procesamiento u otros recursos informáticos. Son una

[1]TIC Tecnologías de la Información y las Comunicaciones

[2]PyMEs Pequeñas y Medianas Empresas

alternativa económica ante el costo de los servidores robustos con altas prestaciones que pueden llegar a reemplazar.

En el entorno gubernamental si bien la intención es mejorar la conectividad electrónica entre el estado y los ciudadanos, los recursos para tal fin no parecieran ir en la misma dirección. Es por esto que se buscan alternativas económicas que permita la seguridad y que presten un servicio optimo y confiable entre instituciones y de cara al cliente final que es el ciudadano común.

En el presente documento se dará a conocer las redes P2P que han estado trabajando en formar un ambiente seguro y se tomará como objeto de análisis, una entidad del estado para proponer una solución basada en estas. Analizando los beneficios y perjuicios de estas redes, observaremos la factibilidad o no de estas topologías de red para prestar servicios en entornos seguros o gubernamentales.

1. ESTADO DEL ARTE DE LAS REDES P2P

1.1 RESEÑA DE LAS REDES P2P

Adam Hinkley desarrolló en 1996 un sistema conocido como ***Hotline Connect***, la primera aplicación P2P. Ésta buscaba permitirla distribución de archivos de Universidades y Empresas, pero tuvo un desvanecimiento de popularidad debido a que al poco tiempo de aparecer empezó a ser usada para intercambiar todo tipo de archivos, especialmente ilegales. El sistema no tardó en quedar obsoleto y además de funcionar sobre la plataforma minoritaria MAC OS no trascendió a la prensa, hecho que se vio superado por la aparición de un nuevo sistema conocido como ***Napster,*** al cual en 1999, se le atribuyó la invención del P2P. Este sistema no tardó en generalizarse como método de intercambio masivo de archivos en formato MP3, y a consecuencia de esto, varias discográficas demandaron a Napster, lo que paradójicamente sirvió para darle aún más publicidad al programa (de hecho, Napster llegó a 13,6 millones de usuarios). Luego de esta aparición, se estableció como líder P2P ***Audiogalaxy***, otra aplicación centralizada de intercambio de música, que acabó también por orden judicial. Por otra parte, la RIAA[3] tomó estas resoluciones judiciales como victorias importantes encaminadas a acabar con la llamada "piratería".

Terminar con las redes centralizadas era relativamente sencillo, pues bastaba con cerrar el servidor que almacena las listas de usuarios y archivos compartidos. Pero tras el cierre de cada servidor surgieron aplicaciones más modernas, y particularmente como gran logro fue la creación de redes descentralizadas, que no dependen de un servidor central, y por tanto no tienen constancia de los archivos intercambiados.

[3]Recording Industry Association of America, en español, Asociación de Industria Discográfica de Estados Unidos.

Clientes nuevos y la aparición de la red ***Gnutella***, fueron sustituyendo a Napster y Audiogalaxy, entre otros. Luego, en el año 2002, se dio un éxodo masivo de usuarios hacia las redes descentralizadas, y es así como aparecen redes como Kazaa, Grokster, Piolet y Morpheus. Dentro de éstas, también están Ares y Ares Lite, libres de spyware y que usan la red Ares Galaxy.

Luego apareció eDonkey 2000, aplicación que se mantuvo junto a Kazaa como líder del movimiento P2P. Más tarde, la aparición de otros clientes basados en el protocolo de eDonkey 2000, como Lphant, Shareaza, eMule y sus Mods, y otros menos conocidos como aMule y MLDonkey para Linux, causó el progresivo declive del programa original eDonkey 2000.

Otro paso importante lo marcó el protocolo BitTorrent, que pese a tener muchas similitudes con eDonkey 2000 proporciona, según los desarrolladores, una mayor velocidad de descarga, pero a costa de una menor variedad y longevidad de archivos en la red.

Con el tiempo se incremento la aparición de otros sistemas de distribución de archivos "no del tipo P2P", los cuales no están basados en la descentralización total (o en tender a la descentralización) sino en aumentar la tasa de transferencia de archivos mediante descargas de servidores.

De estos métodos, la mayor implantación la posee la descarga directa (comúnmente denotada por "DD") de servidores con una gran capacidad de almacenamiento y ancho de banda. Su popularización se debe a que son muy fáciles de usar y ofrecen unas tasas de transferencia de archivo muy elevadas, ya que basta con unos pocos clics para descargar un archivo.

Por último, otro de los sistemas que han aparecido recientemente como alternativa a los P2P es el comúnmente denominado peer to mail (P2M) basado en el envío de archivos troceados a un servidor POP3 o imap aprovechando la cantidad de espacio en disco y tasa de transferencia que ofrecen algunos servidores de

correo. No obstante, debido al desconocimiento de su existencia y la relativa complejidad de los clientes de descarga, éste método apenas ha logrado un mínimo de popularidad.

Debido a lo anterior, el panorama actual de descargas se encuentra definido fundamentalmente en la siguiente tabla de redes.

Redes P2P	
eMule	http://www.emule.com/
aMule	http://www.amule.org/
eDonkey 2000	http://www.edonkey2000.tk/ (demandado por la RIAA - Descarga no aprobada por los creadores)
Lphant	http://www.lphant.com/
Bittorrent	http://www.bittorrent.com
Azureus	http://azureus.sourceforge.net
BitComet	http://www.bitcomet.com/
BitTornado	http://www.bittornado.com/
BitSpirit	http://www.bitspirit.cc/en/
Utorrent	http://www.utorrent.com/intl/es/
Servidores Descarga Directa	
MegaUpload	http://www.megaupload.com/
RapidShare	https://www.rapidshare.com/
OxyShare	http://www.oxyshared.com/ (Dominio fuera de servicio) Buscador ww.searchshared.com/**oxyshare**.com/
YouSendIt	https://www.yousendit.com/
turbouploa d	http://www.turbouploa d.com/
GigaSize	http://www.gigasize.com/

Tabla 1. Redes más empleadas para descargas.

1.2 REDES P2P

El nombre de las redes P2P proviene de la frase en ingles "Peer to Peer", cuya traducción más cercana es "red punto a punto" puesto que la traducción literal seria "red puerto a puerto".

Una red P2P comprende una topología de red donde los miembros son vistos como iguales. En otras palabras, en una red P2P cada nodo es cliente y servidor al mismo tiempo. Este tipo de configuración es propicia para el intercambio de información entre los nodos que la componen.

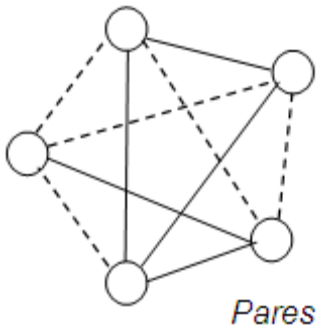


Figura 1. Topología lógica de una red P2P**.**

Las redes P2P se destacan por su aprovechamiento de ancho de banda debido a la replicación de la información. Normalmente, un archivo en particular es contenido por más de un nodo, dicho esto, cuando otro nodo requiere adquirir el archivo, la información es dividida por partes (en redes tipo *Gnutella*[2]) y enviadas simultáneamente por diferentes nodos al nodo solicitante. Lo anterior se convierte en práctico, toda vez que se cuente con mayor cantidad de nodos oferentes y la multiplicidad de los archivos; esto permite tener múltiples opciones de adquirir/compartir la información reduciendo al mínimo los cuellos de botella presentados enel modelo Cliente/Servidor convencional, donde al estar centralizada la información, es muy fácil copar el ancho de banda, reduciendo la capacidad de acceso.

1.2.1 Empleo de las redes P2P

La versatilidad de las redes P2P permite que sean empleadas para múltiples funciones.

1.2.1.1 VoIP

Voz sobre IP es un sistema de comunicación muy empleado actualmente. De éste hacen parte un grupo de recursos que permiten transmitir voz y video a través de internet empleado el protocolo IP. Esto quiere decir que tanto la voz o el video es digitalizado y empaquetado para poder viajar a través de la red.

Figura 2. Skype: Sistema de VoIP sobre P2P más usado del mundo.

Fuente: Imagen tomada de http://www.skype.com/

La VoIP usa la topología P2P de una manera híbrida, a saber, las listas de usuarios están centralizadas normalmente en un servidor, el cual tiene la descripción y la forma de acceder al usuario. Posee una puerta de enlace que enruta la llamada, pero una vez la comunicación es establecida, estos dos agentes dejan de aparecer en la ecuación dejando enlazados los dos clientes que son las personas que desean comunicarse. De ahí en adelante la comunicación es de nodo a nodo.

Este estándar ha disminuido costos en las telecomunicaciones, permitiendo realizar llamadas transcontinentales a solo centavos de dólar aprovechando la tecnología existente. Estas llamadas usualmente usan el protocolo **H.323**[4] para la compresión de voz y video y servidores **SIP**[5] para la conexión y tasación de las llamadas. La principal ventaja de este tipo de servicios es que evita los cargos altos de telefonía (principalmente de larga distancia) que son usuales de las compañías de la Red Pública Telefónica Conmutada (PSTN). Algunos ahorros en el costo son debido a la utilización de una misma red para llevar voz y datos, al mismo tiempo sin coste adicional. Sin embargo, una desventaja importante es la calidad de la transmisión, la cual se ve disminuida, ya que los datos viajan en forma de paquetes, lo que se expone a pérdidas de información y demora en la transmisión. Otra desventaja es la latencia, que se percibe en la pausa de transmisión debido al uso del canal.

1.2.1.2 Cómputo Distribuido

Las redes P2P son ideales para compartir poder de procesamiento entre muchas máquinas para lograr cálculos que, si se tratara de una sola CPU, tardaría décadas.

Figura 3. Logo de SETI@Home

Fuente: Imagen tomada de http://setiathome.berkeley.edu/

[4]**H.**323, es una recomendación del ITU-T(International Telecommunication Union), que define los protocolos para proveer sesiones de comunicación audiovisual sobre paquetes de red.

[5]**SIP** (Session Initiation Protocol) Protocolo de Inicio de Sesiones, desarrollado por la IETF (Internet Engineering Task Force), contiene los lineamientos para el inicio, transcurso y finalización de sesiones interactivas, de los cuales hacen parte elementos multimedia.

Esta técnica se lleva a cabo desde hace más o menos una década donde entidades científicas y de investigación piden a usuarios del común que descarguen un aplicativo para usar los ciclos de CPU que no estén usando en favor de la ciencia. SETI@Home [3] (Search for ExtraTerrestrial Intelligence por su sigla en inglés), es un ente organizado por los estudiantes de la Universidad de Berkeley en Estados Unidos, cuyo propósito es recolectar teras de información de lecturas de ruido espacial en múltiples frecuencias a través de los radio telescopios que usan para captarlas. Este "Ruido Cósmico" es distribuido en paquetes a los más de 3 millones de usuarios que colaboran con el proyecto. Cada máquina analiza por medio de algoritmos, sonidos o señales que tengan un sentido lógico o estructura para separarlo y luego ser analizado por máquinas más expertas, con el objeto de tratar de encontrar transmisiones o señales no hechas por humanos. Proyectos similares a este se emplean con otros fines: el genoma humano, búsqueda de tratamientos para el cáncer, operaciones matemáticas distribuidas, entre otros, los cuales se basan en las bondades de las redes P2P.

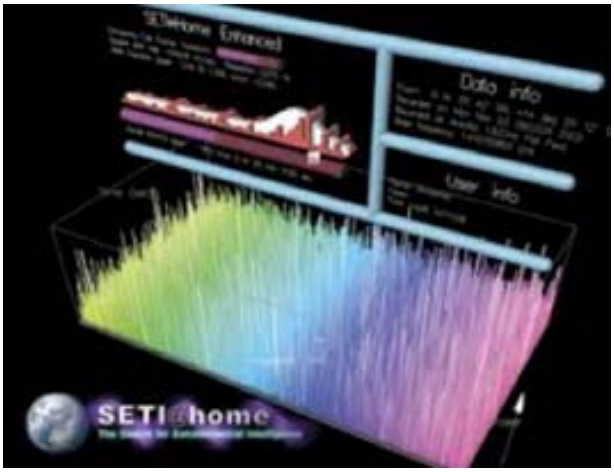


Figura 4. Captura de pantalla del cliente SETI@Home en acción.

Fuente: Imagen tomada de http://setiathome.berkeley.edu/

1.2.1.3 Transferencia de archivos

Quizá ésta es la tarea más empleada por las redes P2P. Debido a ella recibe el mal ganado estigma de ilegalidad, ya que muchas personas emplean esta técnica para intercambiar contenidos con derechos de autor o copyright.

Varias herramientas se han venido desarrollando para compartir ficheros a través de redes P2P. El inicial y más sonado fue *Napster*[4], que por su modelo de operación, fue demandado por el gobierno de los Estados Unidos y obligo a cambiar su modelo de negocio a una empresa de distribución de música. Luego con el advenimiento de la competencia, cambio a ser un sistema de streaming por red pago. A partir de este desarrollo, redes como *Kazaa*[5], *Ares*[6] usaron el sistema *GNUTella* para lograr compartir la información. Estos sistemas por ser de sistema distribuido, hacen más difícil su detección e individualización, puesto que no hay un nodo líder, sino que todos los nodos son clientes y servidores a la vez, siendo puros a la definición de una red P2P.

Figura 5. Ares y uTorrent. Clientes más usados para compartir archivos.

Fuente: Imagen tomada de http://www.ares.com.es y http://www.utorrent.com

Otras redes como las *BitTorrent*[7] se basan en P2P para compartir grandes archivos compartidos por muchos nodos. El secreto de todo este poder se encuentra en el HASH. Cada archivo genera su propio HASH el cual es

identificado por los nodos para individualizar cada archivo y evitar transferencias erróneas por archivos homónimos o del mismo tamaño. Al separar el archivo por su hash se hace virtualmente imposible confundirlo con otro, permitiendo así su identificación.

1.2.2 Ventajas de las Redes P2P

Teniendo en consideración su estructura y topología de red, en contraste con el modelo Cliente-Servidor, se establecen ciertas ventajas diferenciadoras.

1.2.2.1 Escalabilidad

La naturaleza de distribución intrínseca en las redes P2P permite que pueda cambiar su tamaño de manera constante. Claro está, entre más nodos, existe mayor garantía de encontrar lo que se busca, pero también esto permite que en caso que clientes se desconecten, o salgan del sistema no hagan que la estructura colapse. Dicho esto el concepto de P2P está hecho para ser escalable de manera constante e indefinida.

1.2.2.2 Robustez

La escalabilidad y la naturaleza distribuida de las redes P2P permite que esta tenga un carácter estable y robusto. Como su concepto es distribuir recursos, ya sea procesamiento o almacenamiento, nos permite una redundancia de datos y recursos que de otra forma no se tendría. En el caso de procesamiento: si entidades como SETI@Home detecta que un cliente no retorna los resultados del segmento de información que se le dio a procesar, el sistema es capaz mediante un TTL[6], de reenviar ese dato a otro cliente para su análisis. En los archivos, tenemos que la información esta replicada y otorga la capacidad ante el fallo de uno de los nodos encontrarla en otro sin perder la descarga.

[6]TTL*: Time To Live* o tiempo de vida de un dato o paquete.

1.2.2.3 Descentralización

Todos los nodos son iguales. No existen nodos con funciones especiales, y por tanto ningún nodo es imprescindible para el funcionamiento de la red. En realidad, algunas redes comúnmente llamadas P2P no cumplen esta característica, como Napster, eDonkey [8] o BitTorrent.

1.2.2.4 Costos

Al ser distribuida, los costos de funcionamiento y de sostenimiento son repartidos entre los usuarios. Entidades científicas que requieren procesamiento obsequian el programa a cambio del procesamiento de los clientes. Se comparten o donan recursos y según sea la aplicación de la red, los recursos pueden ser archivos, ancho de banda, ciclos de proceso o almacenamiento de disco.

1.2.2.5 Anonimato

Esta es la base para algunas aplicaciones ilegales en las redes P2P. El sistema funciona de manera tal que es muy difícil identificar el origen inicial de un archivo o quienes están compartiendo un dato en un momento determinado. Gobiernos y empresas desarrollan técnicas para poder identificar más confiablemente los usuarios. Esto esta aun en desarrollo.

1.2.2.6 Seguridad.

Se encuentra aun en desarrollo. El anonimato que genera las estructuras de las redes P2P actuales, hace más difícil considerarlas como redes seguras. Nuevas propuestas surgen y se desarrollan para lograr un manejo de las redes P2P más confiable entre los nodos, evitando ataques, falsos archivos, protección de los derechos de autor, entre otras. Los mecanismos más prometedores son: cifrado multiclave, cajas de arena (Sandboxing), gestión de derechos de autor (ya sea por restricción o por autorización), reputación (permitir acceso sólo a los conocidos), comunicaciones seguras, comentarios sobre los ficheros, entre otros.

1.2.3 Tipos de Redes P2P

Si bien en las redes P2P su centro y su fin son sus nodos, existen arreglos de estas redes, que tienen por tanto diferentes funciones. Tenemos entonces algunos tipos básicos de redes P2P.

1.2.3.1 Redes P2P Centralizadas

Son regidas bajo un único servidor que gestiona, conecta y transfiere datos entre los nodos. Su gran problema es la escalabilidad, puesto que si la cantidad de nodos sobrepasa la capacidad del servidor, se obtiene un cuello de botella. Así mismo, la seguridad se ve afectada, puesto que un ataque al servidor por un cliente malintencionado generaría la falla del mismo provocando un colapso en el sistema. Como ventaja se observa que al estar toda la información indexada en un servidor central, los tiempos de búsqueda se reducen ya que la consulta se limita a un solo equipo que cuenta con toda la información. En estos tipos de redes, el servidor define como se distribuye la información que tiene poca rotación dentro de la red, pero que de alguna forma, es necesario tener disponible. Prueba de esta técnica es el programa *Napster*.

1.2.3.2 Redes P2P Puras

Son el tipo de redes que el concepto P2P busca, total descentralización. En este concepto no se cuenta con un servidor central, carece de enrutamiento centralizado. Los clientes se convierten entonces en servidores al mismo tiempo. Las consultas se hacen a todos los nodos. En ciertas plataformas los nodos ayudan a enlazarse entre si y generan pequeñas tablas para ayudar con la indexación y búsqueda de contenidos. Este tipo de redes trabaja igual con direcciones IP públicas o cubiertas bajo NAT. Soportan una cantidad indefinida de usuarios, garantizan mayor disponibilidad, pero usualmente son anónimas y esto le resta seguridad al modelo. Redes como estas pueden destacarse *ARES*, *Gnutella* entre otras.

1.2.3.3 Redes P2P Híbridas

Como su nombre lo indica, son una combinación de las dos redes mencionadas anteriormente. Un servidor central enruta los contenidos, los gestiona, concentra y tabula la información, pero desconoce la identidad de los clientes quienes comparten los archivos o procesamiento. Ejemplos de estas redes son*BitTorrent*, *eDonkey*, entre otros.

1.2.3.4 Redes P2P No Estructuradas

En este tipo de redes, el anonimato juega un papel clave. Los usuarios que desean conectarse a la red necesitan largas consultas a todos los nodos para encontrar el contenido deseado. Este tipo de redes no son óptimas para el usuario que busca un contenido con poca demanda, puesto que no lo tendrán tantos nodos como quisiese, limitando su disponibilidad. Esta constante búsqueda por toda la red genera cargas de la misma que, dependiendo del ancho de banda del nodo, puede causar problemas de sobrecarga en la red. *Gnutella*, *KaZaA* son ejemplos de este comportamiento.

1.2.3.5 Redes P2P Estructuradas

Estas redes evolucionaron a través de los errores de las redes no estructuradas. Mantienen una tabla de hash distribuida (HDT), compartiendo el contenido a través de los usuarios de la red haciéndolos responsables de éste. También agregan métodos de redundancia y distribución, de tal manera que en caso de falla de un nodo, otro nodo en la red cuente con la informacióny esté en la capacidad de distribuir los contenidos. Redes como *Chord*[9] son redes distribuidas donde se manejan todas estas variables.

1.3 REDES P2P SEGURAS

El advenimiento de programas P2P, como *Napster*, *Gnutella* y el más reciente *Ares Galaxy*, generó una explosión desinterés en el diseño de redes P2P, tanto entre los investigadores, los profesionales y compañías de medios. Las redes P2P han aumentado en popularidad en parte, a la facilidad y economía de su implementación, ya que pueden ser instaladas sobre una variada colección de hardware y software. La infraestructura de red también tiende a ser altamente tolerante a fallos, por la forma como aborda la entrada y salida de sus nodos. El ancho de banda y otros recursos computacionales, se comportan de manera equilibrada entre los nodos involucrados, lo que beneficia aun más el concepto de robustez en el que se tiene a estas redes.

Sin embargo, las redes P2P que cuentan con mayor popularidad en la red poseen una falencia, que poco se estudia: el anonimato. Redes como *Ares Galaxy*, *Gnutella* benefician a las personas que comparten ilegalmente contenido con copyright debido a la estructura altamente pura y no estructurada. Lo anterior permite que un nodo desconozca la fuente de la información de descarga, además de los archivos buscados y la dirección IP con la que se enlaza, esta última fácilmente puede ser alterada mediante ***ip-spoofing***[7], haciendo muy difícil tener una relación de confianza entre los nodos.

Un diseño de red robusta requiere que los nodos en una red P2P se consideren de confianza, para asegurarla integridad y confidencialidad de los datos compartidos. En los últimos años se han adelantado investigaciones para la aplicación de técnicas de seguridad para lograr que todo el sistema en las redes P2P sea confiable y seguro de extremo a extremo. Con esto se logra que los nodos dentro

[7] En las redes de computadores, la falsificación de direcciones IP o IP spoofing es un término que se refiere a la creación del Protocolo de Internet (IP) con una dirección IP de origen falsos, llamada spoofing, con el propósito de ocultar la identidad del remitente o hacerse pasar por otro sistema de computación.

de una red sean de confianza, que la información no se altere, y si se hace, se conozca que nodo altero el fichero, así como garantizar integridad y confidencialidad, sin dejar de lado la economía y versatilidad que brindan este tipo de redes.

Las redes P2P proporcionan la infraestructura para soportar las diversas aplicaciones de la tecnología tales como gestión de datos, colaboración en línea, y toma de decisiones. Se cuenta también con aplicaciones en ambientes distribuidos, el comercio electrónico, cómputo distribuido, entre otros, lo que permite que las redes P2P puedan ser utilizadas como base para el soporte de aplicaciones en entornos de confianza.

Las redes P2P se han desarrollado como un medio para balancear los costos de la computación a través de la red y máquinas más económicas. En contraste con las redes tradicionales donde todo se reduce a servidores y clientes, las P2P hacen que todos actúen como iguales, siendo clientes y servidores a la vez, permitiendo con ello que los servicios sean ofrecidos por un alto número de servidores en vez de unos pocos como en el modelo tradicional.

Desde el punto de vista de seguridad, las redes P2P son inherentemente robustas, difícilmente igualable por el modelo tradicional. La redundancia evitaría problemas tales como la negación de servicio, puesto que una máquina que cae al ser atacada, tiene el respaldo de las otras que seguirían ofreciendo el servicio demandado.

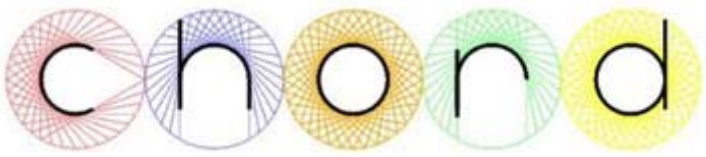


Figura 6. Logo de las Redes CHORD

Fuente: Imagen tomada de http://pdos.csail.mit.edu/chord/

Sin embargo, en la práctica las técnicas de las redes P2P seguras siguen siendo vulnerables a los ataques de negación de servicio, por la forma de enrutamiento del protocolo mismo. Las redes P2P tipo *Chord*, una de las más seguras por su manera de distribuir y redundar la información entre sus pares, tiene como falencia que el protocolo de enrutamiento para enviar la información entre los equipos y los dos puntos que desean comunicarse, están obligados a confiar en los demás nodos en la red. Estos pares son escogidos determinísticamente según estándares establecidos por el nodo principal de la red, ya sea por carga de red, cantidad de información, o por simple imposición. Lo normal es que sean asignados aleatoriamente por el mismo protocolo (en caso de no existir intervención en las reglas), pero en una red *Chord*, al afectar una máquina y dejarla fuera de línea, también afecta las que por enrutamiento pasen por ella, exponiendo a los nodos a un tiempo de desconexión, hasta que el mismo protocolo note el problema y reorganice la red. En otras palabras, el ataque no desconecta la red pero si deja los equipos influenciados por la máquina atacada, incapaz de comunicarse entre sí. Protocolos como PASTRY [10] y CAN [11] sufren falencias similares pero las consecuencias varían en cada caso.

Las redes P2P se ven influenciadas también por el problema de la suplantación, afectando la integridad de la información. Esto se debe a la capacidad de los nodos en la red de "mentirle" a sus iguales, sobre los archivos que sirven a sus semejantes. Dicho esto, es posible diseminar ***malware***[8]en la red publicando los archivos como material inofensivo o como el original que debería estar en su lugar. Esto es visible en redes empleadas actualmente como *Ares* o *Limewire* [12], las

[8] **Malware** (del inglés ***mal****icious soft****ware***), también llamado **badware**, **software malicioso** o **software malintencionado** es un tipo de software que tiene como objetivo infiltrarse o dañar un computador sin el consentimiento de su propietario.

cuales ofrecen canciones para descargar, usualmente de moda y al descargar son links a páginas para ***phishing***[9]o diseminar malware.

La confidencialidad es normalmente una carta a favor de las redes P2P. Esta puede ser vista desde dos frentes:

- Políticas de Confidencialidad: Por medio de permisos se impide el acceso a archivos clasificados a personal no deseado o sin las credenciales adecuadas.

- Anonimato del Usuario: Políticas previamente establecidas que impiden la divulgación de la información privada del usuario, tales como archivos descargados, credenciales de acceso (así sea solo usuario), historial de cargas y descargas o listas de nodos con los que ha interactuado.

Los programas P2P conocidos por el público carecen de estas políticas debido a que su propósito es compartir libremente la información. El anonimato tampoco es implementado ya que al compartir libremente se necesita divulgar los archivos descargados para nuevamente compartirlos.

Teniendo en cuenta las falencias se han buscado maneras de evitar los peligros inherentes de las redes P2P en lo que a confidencialidad e integridad se refiere. A continuación se mencionara varias de las propuestas tratadas en la actualidad.

1.3.1 Propuestas de Seguridad de Redes P2P

Teniendo en cuenta las falencias en seguridad se han buscado maneras de evitar los peligros inherentes de las redes P2P en lo que a confidencialidad e integridad

[9]Tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

se refiere. A continuación se mencionara varias de las propuestas tratadas en la actualidad.

1.3.1.1 Relación de confianza basada en la Reputación

Este modelo emergió como una idea que prometía resolver la mayoría de los problemas intrínsecos de las redes P2P, sin afectar las ventajas de balanceo de carga que la tecnología ofrecía. El sistema operaba manejando un membrete de confianza para cada agente en la red. Cuando la red comienza a operar con el nivel de reputación de confianza, se tienen en cuenta las opiniones, archivos, aportes, descargas y cargas (según el caso) de los nodos que tengan identificación de agente. De otra manera, solo los agentes con identificación serían tenidos en cuenta mientras que los aportes de agentes con menor privilegio serian obviados u observados en segunda instancia.

Más que una forma de valorar los nodos, el sistema basado en la Reputación busca es reconocer los nodos que activamente son menos propensos a transmitir malware o vulnerabilidades. Esto facilita a los miembros de la red a identificarse entre ellos y descartar aquellos que no posean las credenciales adecuadas.

Investigaciones efectuadas en la universidad de Texas en Dallas muestran como esta tecnología de manejo de Relaciones de Confianza es una gran ayuda para mantener la integridad de los datos en las redes P2P. A un objeto se le asigna un membrete de integridad global, el cual debe tenerlo todas sus replicas a lo largo de la red. Todo objeto similar que la carezca es simplemente descartado o ignorado por el agente que desee descargarlo. De todas maneras queda a criterio del nodo que solicite la información, descartarlo o aceptarlo a pesar de carecer de esta cualidad. Luego de descargar el fichero solicitado el nodo puede emitir un reporte de confianza del fichero a sus nodos anexos y de este modo ratificar o refutar el membrete que porta el documento.

Este tipo de solución es de fácil implementación y de alto impacto para prevenir falsificación y suplantación de archivos en las redes P2P. Básicamente, cuando un nodo detecta que un archivo es sospechoso o dañino, le baja la reputación e inmediatamente difunde su cambio a la red, permitiendo a los demás nodos detectar la suplantación y así descartar o ignorar el archivo en el momento de necesitarlo. El equipo que detecte el archivo malicioso automáticamente subirá su reputación dando más confianza a sus pares, siempre y cuando estos validen la veracidad de la sentencia que lanzo a la red.

Este sistema nos permite confiar en los archivos y las máquinas que trabajan en nuestra red. Es importante tener en cuenta que solo protege un aspecto de la red y están supeditados los records de reputación de los archivos en las tablas.

1.3.1.2 Enrutamiento Seguro

La posibilidad de marcar con calificación de confianza a un archivo o un nodo, es una herramienta muy conveniente, pero es más práctico aún, poder evitar colocar en las tablas de enrutamiento de los nodos, aquellos pares que su reputación sea tan baja como para confiar en ellos. Esto nos obliga a mantener los records de la reputación actualizados y así poder tomar este tipo de decisiones.

Lo anterior no es una tarea fácil, de hecho es considerado muy complicado y sigue siendo un problema aún en desarrollo. Pero se ha detectado propuestas promisorias en el tema, proponiendo que el sistema de gestión de confianza sea implementado sobre un protocolo de enrutamiento seguro.

Es importante tener en consideración los ataques significativos a la estructura de enrutamiento de una red P2P, los cuales se presentan en diversas formas:

- Agentes maliciosos con capacidad de silenciar o eliminar mensajes que deben ser enviados.

- Agentes maliciosos que pueden interferir en el enrutamiento con el objeto de retrasar o impedir la entrega de los mensajes.

- Un agente malicioso puede mentir acerca de su ubicación en la topología, ocasionando que la información de las tablas de enrutamiento de otros agentes se corrompan, al mismo tiempo, se causa que los demás nodos de la red se redirijan hacia los agentes maliciosos.

- Un ataque **Sybil**[10], corresponde a un agente malicioso que adopta la identidad de diferentes agentes, en el esfuerzo por controlar un gran porcentaje del especio de identificación de las tablas de enrutamiento [13].

En muchas topologías de redes P2P existen múltiples posibilidades de enrutamiento de un par a otro, aunque se implemente un protocolo de enrutamiento determinístico, éste siempre tendrá en cuenta la misma ruta para cualquier par dado de nodos; lo que conlleva a una susceptibilidad ante los ataques de agentes maliciosos.

Una defensa prometedora contra estos ataques, combina la identificación mediante un auto-certificado con tablas de rutas contrastadas por parte de cada nodo que pertenezca a la red. Una posición de un par dentro de una red P2P es determinada por un único identificador asignado, que usualmente proviene de aplicar una función hash segura a la dirección IP del par. La identificación de los pares por medio de auto-certificados, se logra verificando los bits de una clave pública contenida en una clave asimétrica propia de cada par. Esto permite que un par provea a sus vecinos una identificación dada para asignar sus respuestas con la clave privada del par. Una vez que un par pueda verificar las identidades de los pares con quien desea comunicarse, podrá contrastar su tabla de rutas y así redirigir los mensajes a sus destinos. El par recibe el mensaje solo si la ruta es

[10] Ataque Sybil, nombre asignado por Microsoft Research, con el cual se hace alusión al tema del libro Sybil de la autoría de Flora Rheta Schreiber, que trata del estudio de caso de una mujer con trastorno de personalidad múltiple.

identificada y contrastada por el par, de este modo, se limita el grado con el cual los pares maliciosos pueden corromper los mensajes, ya que al ser detectado como malicioso, con esta técnica el mensaje será rechazado, además que el nodo será identificado con una dudosa reputación.

Otra forma de contrarrestar los ataques se asemeja a un rompecabezas encriptado. En esta defensa un nodo malicioso recién llegado a la red P2P está requiriendo resolver un algoritmo matemático generado aleatoriamente, para obtener la identificación de la red. El algoritmo es elegido de tal manera que no sea resuelto por un equipo de cómputo normal, lo que lo convierte en un tarea muy difícil para el agente malicioso. Sin embargo este tipo de soluciones son muy costosas, por lo que para una red común se convierte en una solución inalcanzable.

Una buena alternativa es capturar los históricos de los eventos que han ocurrido en la red, tomando en consideración cuáles pares inducen a otros a su red. Un ataque típico, por ejemplo el Sybil, empieza con un nodo malicioso convenciendo a otro inocente a convertirse en un miembro de su red. Una vez éste lo logra, el nodo malicioso se aprovecha de los vecinos inocentes del nodo embaucado, logrando incrementar la colección. Sin embargo, esta colección de nodos maliciosos auto-inducidos, puede ser detectada observando la larga colección de pares con baja reputación, e identificar aquel par que ha venido induciendo al resto de pares, con esto se logra establecer una catalogación de nodos maliciosos, reduciendo así su potencial de ataque.

1.3.1.3 Niveles de Verdad para Control de Acceso

La confianza de un sistema de gestión basado en la reputación, implementado sobre un protocolo de enrutamiento seguro, se puede incrementar aplicando fuertes políticas de integridad a los datos en un entorno distribuido.

Los sistemas de gestión confiables basados en la reputación mantienen un nivel de integridad global para cada objeto en el sistema. Esto se puede extender fácilmente a un vector de niveles o etiquetas basadas en diferentes criterios, por ejemplo, las etiquetas de la integridad y confidencialidad. La combinación de las etiquetas de confianza global de los pares, permite gestionar las políticas de control de acceso de los pares que están sujetos a la red. Por ejemplo, antes de realizar una solicitud de descarga, un par puede consultar los niveles de seguridad global para el objeto solicitado y la etiqueta de la confianza global del par con el que desea establecer conexión. Si la etiqueta de integridad del objeto es demasiado baja, o la etiqueta de confidencialidad del objeto solicitado es demasiado alta en relación a la etiqueta de confianza del solicitante, entonces el par se niega a la solicitud. Lo anterior previene la divulgación de datos de baja integridad, así como también previene que pares de baja confianza obtengan datos de alta confidencialidad.

Sin embargo, mientras que la estrategia anterior es suficiente para hacer cumplir las políticas de acceso de lectura basadas en la integridad de datos, se pierde una sutileza importante relacionada con la aplicación de las políticas de confidencialidad. Para que un sistema de gestión de confianza pueda hacer cumplir una política de seguridad, las violaciones de estas últimas tendrán que ser reportadas con reputación de violador, con el objetivo de prevenir futuras intervenciones que atenten contra la seguridad. Aunque existan muchos escenarios en donde se reportan violaciones de integridad (por ejemplo, un par no malicioso descarga un archivo y descubre que su contenido no era el que había requerido), no está claro cómo violaciones de confidencialidad no se denuncian. Las típicas violaciones de confidencialidad, suelen incluir un par malicioso que divulga datos confidenciales a otro par malicioso, en cuyo caso ninguno de los pares se atreve a denunciar la violación.

La aplicación de políticas de confidencialidad, sigue siendo un problema difícil en las redes P2P. Plataformas confiables de computación podrían ser la única

solución en la actualidad, ya que tanto las políticas globales de seguridad como las de control de acceso obligatorio se gestionan de forma remota. Una red P2P basada en esta plataforma, podría estar en la capacidad de verificar que cada par esté ejecutando el hardware y software de confianza, antes de ser admitido en la red. El hardware y software de confianza estarían obligados a obedecer el protocolo de la red P2P y de suministrar los datos de acuerdo con las políticas de control de acceso. Si bien esta estrategia puede ser viable como arquitectura confiable de computación y seguir ampliando su disponibilidad, continúa siendo inadecuada para algunas configuraciones de P2P donde los usuarios desean un mayor control sobre sus sistemas de clientes.

1.3.1.4 Una herramienta en desarrollo: Computación de confianza.

Este tipo de trabajo en equipo, permite que políticas de seguridad sean manejadas remotamente (conocidas como control de acceso). Este sistema es ideal para redes corporativas puesto que el administrador de la red maneja los permisos y libertades desde su estación de trabajo. Por el contrario las redes P2P abiertas al público no son muy aceptadas puesto que cada nodo tiene su propietario y como usuario final no estarían de acuerdo con el hecho que un agente externo administre la seguridad en su nodo.

Visto de esta forma, en redes que estén a lo largo de internet vía VPN[11]pueden interactuar con redes P2P puesto que la VPN impide el acceso de agentes externos a los equipos involucrados. Esta es una alternativa razonable, pero la idea es proporcionar una opción donde los nodos trabajen directamente sobre internet sin necesidad de sobreponerse a otra plataforma de red. Esto último, con el fin de reducir costos y procesamiento.

Una de los sistemas distribuidos usados para redes P2P son las redes ***CHORD***[14]***.*** Estas redes son útiles en entornos LAN o VPN donde las máquinas

[11]VPN: Red Privada Virtual (Virtual Private Network), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

son administrables por un área de sistemas, además de estar distribuidas geográficamente, y a su vez basan su funcionamiento de la administración proporcionada por un equipo central que distribuye la información.

La red CHORD es otro modelo de auto-organización estructurada del sistema P2P. Este algoritmo proporciona una implementación de las políticasbásicas de CHORD para el modelado de las redes peer-to-peer, con el fin de realizar la búsqueda de tales topologías. Acorde ofrece una solución flexible, de alto rendimiento de la búsqueda básica en la que la funcionalidad en la ubicación eficiente de los datos, el anonimato de búsqueda, selección de servidor, autenticación, entre otros, pueden ser distribuidas por capas.

CHORD utiliza hashing para asignar los nodos en un espacio de identificación de anillo. Cuando un nuevo nodo N se añade, los atributos de los nodos adyacentes a N en el anillo se utilizan para agregar información de los demás nodos distribuidos en el espacio. Cada nodo también realiza un seguimiento de su nodo antecesor y sucesor. Esto proporciona una ventaja significativa sobre hashing estándar, el cual requiere que cada nodo realice un seguimiento a casi todos los demás nodos.

1.3.1.4.1 Búsqueda en una Red CHORD

La eficiencia en una búsqueda descentralizada es un problema fundamental en las redes P2P. Un servicio de búsqueda eficaz, que sólo utiliza la información local es esencial para su capacidad de ampliación y, en última instancia, su éxito. Se sugiere que exista una fuerte relación entre la topología de la red y los algoritmos de búsqueda.

Las redes CHORD proporcionan un método eficiente de localizar los documentos, mientras que maneja algunas restricciones en la aplicación que lo utilice o la jerarquía del equipo que genere la consulta. Dado que cada nodo mantiene información acerca de sólo un subconjunto de los nodos en estructura, la

búsqueda se aproxima cada vez más a la identificación del sucesor con cada paso.

El propósito de la búsqueda, es encontrar un nodo dado a partir de un nodo inicial. El algoritmo de búsqueda entrega un resultado mostrando los costos involucrados en la realización de la búsqueda. Con costo de búsqueda se hace referencia al número de mensajes que se pasan en el sistema para encontrar el nodo de destino. Una estructura tipo CHORD consiste en un anillo virtual en el que cada nodo sabe cómo llegar a su antecesor y sucesor de k nodos en las tabla de identificación. Para buscar el nodo de destino, se pasa al sucesor de un nodo que está más cerca del nodo de destino en el anillo. El mensaje se propaga de manera progresiva hasta que el nodo de destino es encontrado.

El modelo CHORD es ventajoso para la construcción de sistemas donde la colocación controlada de recursos es de alta prioridad, tales como almacenamiento de archivos distribuidos. CHORD ofrece mecanismos de búsqueda no-lineal o sub-lineal.

1.3.1.4.2 Redes PASTRY

Una red PASTRY [15]no es una red en todo el sentido. Es un algoritmo de enrutamiento implementado para tablas hash distribuidas, en un entorno similar al de las redes CHORD.

El protocolo es soportado bajo el suministro de la dirección IP de un nodo que se encuentre en la red, ya partir de esto la tabla de enrutamiento es dinámicamente construida y modificada. Debido a su carácter redundante y descentralizado no hay ningún punto único de fallo y cualquier nodo puede desconectarse de la red en cualquier momento sin previo aviso y con poca o ninguna posibilidad de pérdida de datos. El protocolo también es capaz de usar una métrica de enrutamiento proporcionada por un programa externo, tales como ping o

traceroute, para determinar las mejores rutas para almacenar en su tabla de enrutamiento.

Aunque la cualidad de la Tabla de Hash distribuida (DHT) en PASTRY es casi idéntica a las DHT de otros modelos de red, el factor diferencial es el modelo de enrutamiento superpuesto al concepto de DHT. Esto permite a PASTRY notar la tolerancia, la escalabilidad y los fallos de la red, al tiempo que reduce el coste global de enrutamiento de un paquete de un nodo a otro, evitando la necesidad de paquetes de inundación o flood. Debido a que la métrica de enrutamiento es suministrada por un programa externo basado en la dirección IP del nodo de destino, la métrica se puede cambiar fácilmente contando a partir del salto más cercano, menor latencia, mayor ancho de banda, o incluso una combinación general de las métricas.

La lista de claves de la tabla de hash es circular, como el espacio de claves en CHORD, y los ID de nodo son de 128 bits, esto representa la posición del nodo en la red de anillo. El ID de nodo es elegido al azar y uniformemente, de manera que los ID nodos vecinos a un cliente particular, están geográficamente dispersos. La tabla de enrutamiento superpuesta a la tabla de hash en cada nodo permite descubrir sus adyacentes, recibir e intercambiar información de estado que consiste en una lista de los nodos vecinos, y una tabla de enrutamiento.

La lista de nodos está formada por la distancia media de los nodos más cercanos en cada dirección alrededor del anillo. Además los nodos vecinos también están en una lista de vecindad. Esto representa los M pares más cercanos en términos de la métrica de enrutamiento. A pesar de que no se utiliza directamente en el algoritmo de enrutamiento, la lista de vecindad se utiliza para el mantenimiento de los nodos principales en la tabla de enrutamiento.

Por último, está la tabla de enrutamiento en sí. Contiene una entrada por cada bloque de direcciones asignado. Para formar los bloques de direcciones, la clave de 128 bits se divide en cifras con cada bits b dígitos ser largo, produciendo un

sistema de numeración con base 2b. Este sistema parte las direcciones en distintos niveles. Desde la perspectiva del cliente, el nivel 0 representa un prefijo común de digito cero entre dos direcciones, el nivel 1 un prefijo de un uno común, y así sucesivamente. La tabla de enrutamiento contiene la dirección de los nodos conocidos más cercanos para cada dígito común en cada nivel, excepto de los dígitos que identifica al propio nodo en el nivel de red.

1.3.1.5 Enrutamiento basado en ID de vecindad

Un paquete puede ser enrutado a cualquier dirección en la tabla de claves, aún si existe un compañero de ID de vecindad o no. El paquete es encaminado hacia su propio lugar en vecindad interior y el nodo cuyo ID sea más cercano al destino deseado. Cada vez que un nodo recibe un paquete para enrutar o enviar, primero se examina el conjunto de las tablas y rutas directamente al nodo correcto. Si esto falla, el par siguiente consulta su tabla de enrutamiento con el objetivo de encontrar la dirección de un nodo que ha compartido por más tiempo, el prefijo común de la dirección de destino. Si el compañero no tiene contactos con un prefijo más cercano o más relacionado, entonces tomará un par de su lista de contactos con el prefijo de la misma longitud cuyo ID de nodo es numéricamente más cercano al de destino, y enviará el paquete a los que sean visibles. Dado que el número de dígitos correctos en la dirección de siempre aumenta o se mantiene igual y si se mantiene la misma distancia entre el paquete y su destino o se hace más pequeña, esto hace que el protocolo de enrutamiento sea efectivo.

1.3.1.5.1 PAST

Corresponde a un sistema de archivos distribuido en capas montado sobre PASTRY. Un archivo se almacena en el sistema calculando el valor hash de su nombre. A continuación, PASTRY enruta el contenido del archivo al nodo cuyo hash corresponda al obtenido del nombre del archivo. Este nodo enviará copias de los archivos a los nodos más cercanos según su clave particular, buscando aquellos que se aproximen al nivel del emisor por ID y así garantizar la entrega del

archivo. La recuperación de datos se realiza mediante la obtención de un nuevo hash según el nombre del archivo y buscar en cualquiera de los nodos que contengan estas mismas características. Esto logra la redundancia de datos y balanceo de carga. Dado que los nodos adyacentes en la tabla de claves se encuentran geográficamente dispersos las posibilidades de que todos estén fuera de línea simultáneamente son muy pequeñas. Además, ya que el protocolo de enrutamiento PASTRY busca minimizar la distancia recorrida, el nodo más cercano a la máquina que hizo la solicitud (de acuerdo con la métrica) es probable que sea la que responde con los datos.

1.3.1.5.2 SCRIBE

Es un sistema descentralizado de publicación/suscripción que utiliza PASTRY para gestión de rutas adyacentes y la búsqueda de nodos. Los usuarios pueden crear temas para que otros usuarios puedan suscribirse. Una vez que el tema ha sido creado, el dueño del tema puede publicar nuevas entradas en el tema que se distribuirá en un árbol multicast a todos los nodos que se han suscrito con el tema. El sistema funciona mediante el cálculo del valor hash del nombre del tema concatenado con el nombre del usuario que posee este último. Este hash se utiliza como una clave PASTRY, y el nodo editor de la información enruta los paquetes al nodo más cercano usando el algoritmo PASTRY de enrutamiento para crear los vínculos hacia el nodo raíz del tema. Los usuarios se suscriben a este mediante el cálculo de la clave hash del tema y el nombre del editor y luego se implementa PASTRY para encaminar un mensaje hacia el nodo raíz. Cuando el nodo raíz recibe el mensaje de suscripción de otro nodo se añade el identificador de nodo a la lista y comienza a actuar como un promotor del tema.

La descentralización se logra a través de tener todos los nodos de la red espiando mensajes que pasan por ellos en su camino hacia el nodo raíz del tema. Si el tema es uno en que el nodo desea suscribirse, dejará de enviar el paquete hacia el nodo raíz y agrega el nodo tratando de inscribirse como uno de sus hijos. De esta

forma una estructura en árbol se forma con el nodo raíz en la parte superior, luego los nodos que se inscribieron primero y luego cada uno de estos nodos reenvía los mensajes a sus hijos, y así sucesivamente. Como los paquetes de los nodos saltan al azar en la red PASTRY a menudo terminan viajando a lo largo del mismo camino ya recorrido, y terminan vinculados a cualquier parte del árbol más cercano a ellos en la red PASTRY. Dado que cada salto a lo largo de una ruta representa la mejor ruta a nivel local de acuerdo con la métrica de enrutamiento en uso, el mensaje de suscripción busca la distancia más cercana dentro del árbol de clientes y se anexa ahí.

Finalmente la tolerancia a fallos entre los miembros del árbol de la distribución se realiza mediante el uso de los tiempos de espera y conexiones abiertas con las transmisiones de datos reales, como duplicar conexiones abiertas para minimizar el tráfico. Si un nodo hijo no escucha a su padre por un tiempo, las rutas de un nuevo mensaje de suscripción hacia el nodo raíz del árbol, se reactiva buscando cualquier nodo con el árbol de ese tema. Si un padre no escucha a un nodo hijo por un período de tiempo de espera, suprime al nodo de la lista de los hijos. (Si esta acción hace que su lista de elementos secundarios sea nula, el padre deja de actuar como tal y deja de reenviarle contenidos).

1.3.2 Redes IPsec[12]

Una alternativa para la consecución de la seguridad en el transporte de los datos sobre una red P2P segura, corresponde a la implementación de la tecnología IPsec, que adopta una variante de la opción de Red-a-Red, en donde cada nodo actuaría como una red y así mantener cifrada la información que corre entre ellos.

[12] **IPsec** (abreviatura de **Internet Protocol Security**) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

IPsec es la tecnología de seguridad recomendada por la **IETF** (Internet Engineering Task Force) para la protección de las comunicaciones sobre redes IP a través del uso de servicios de seguridad criptográficos.

Como el IP intrínsecamente carece de capacidad de seguridad alguna, IPsec se introdujo para proporcionar servicios de seguridad tales como:

- Cifrar el tráfico (para evitar su lectura por nodos que no estén adscritos a la red o que carezcan de las llaves para descifrarlo).
- Validación de integridad (permitir garantizar que el contenido enviado o recibido no haya sido alterado).
- Autenticar a los extremos (asegurar que el tráfico proviene de un extremo de confianza).
- Anti-repetición (proteger contra la repetición de la sesión segura).

Teniendo en cuenta lo anterior, IPsec se proyectó para proporcionar seguridad en modo transporte (nodo a nodo) del tráfico de paquetes, en el que los ordenadores de los extremos finales realizan el procesado de seguridad, o en modo túnel donde la seguridad del tráfico de paquetes es proporcionada a varias máquinas (incluso a toda la red de área local) por un único nodo.

1.3.2.1 Propiedades de seguridad de IPsec

La seguridad de comunicaciones extremo a extremo a escala Internet se ha desarrollado muy lentamente. En parte se debe a que no ha surgido infraestructura de clave pública universal o universalmente de confianza (DNSSEC fue originalmente previsto para esto); por otra parte, muchos usuarios no comprenden lo suficientemente bien sus necesidades en seguridad, ni las opciones disponibles como para promover su inclusión en los productos disponibles en el mercado actual.

Las redes públicas y privadas actualmente son susceptibles a monitoreos y accesos no autorizados. Los ataques internos pueden ser un resultado de la carencia o inexistencia de seguridad ante riesgos originados de las conexiones a Internet y redes externas. Los controles de acceso a usuarios basados en password, por sí solos, no protegen la transmisión de datos a través de una red.

IPsec fue diseñado para brindar una solución de seguridad al tráfico basado en IP. Los protocolos de IPsec actúan en la capa de red, la capa 3 del modelo OSI. Otros protocolos de seguridad para Internet mayormente empleados, tales como SSL, TLS y SSH operan de la capa de transporte (capas 4 a 7) hacia arriba. Esto permite a IPsec mayor flexibilidad, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo TCP y UDP. Una ventaja importante de IPsec frente a SSL y otros métodos que operan en capas superiores, es que para que una aplicación pueda usar IPsec no hay que hacer ningún cambio, mientras que para usar SSL y otros protocolos de niveles superiores, las aplicaciones tienen que modificar su código.

1.3.2.2 Protección basada en burlas contra intrusos

IPsec protege a los paquetes IP, mediante la implementación de estrategias de burla contra intrusos. Los paquetes IP utilizan una suma de comprobación de tal forma que el nodo que recibe pueda verificar el cambio de los bits, detectando de esta manera si ha ocurrido algún error durante la transmisión o enlace. Sin embargo, la suma de comprobación no provee integridad o seguridad para el paquete IP. Por consiguiente, un nodo IP intermedio puede recibir un paquete IP, alterar su contenido, actualizar la suma de comprobación y reenviar el paquete a su destino. Lo anterior es debido a que el cálculo de la suma de comprobación no provee integridad, el host destino no puede determinar si el paquete fue modificado en el tránsito. IPsec usa una suma de comprobación encriptada, que incorpora una clave secreta conocida únicamente por los dos pares que hacen

parte de la comunicación. Cualquier intento de modificar el contenido de los paquetes, o de burlar las direcciones es fallido, debido a que el atacante no puede calcular fácilmente la suma de comprobación encriptada.

1.3.2.2.1 Utilidad de la criptografía

Sin un servicio criptográfico adoptado en un intercambio de información, un par perteneciente a una comunicación, puede capturar los paquetes enviados por el par opuesto, y de esta manera analizar la composición del paquete, y determinar los datos que han sido cambiados. En el caso particular que un cliente desee realizar una conexión con un servidor de archivos, para obtener información de datos confidenciales, se encuentra con una primera barrera, la lista de control de acceso en el servidor; ésta determina cuales usuarios pueden acceder a determinados archivos y lo que ellos tienen permitido hacer. Sin embargo, una vez que un usuario sea validado, se genera una conexión al servidor de archivos confidenciales, permitiendo copiar los archivos de un lado a otro de la red. Un atacante ubicado entre el servidor de archivos y el cliente, pude capturar el grupo de paquetes y reconstruir el contenido del archivo sin necesidad de conocer las credenciales que implementa el cliente para conectarse al servidor de archivos. Con la adopción de un servicio criptográfico, el mismo atacante puede capturar los paquetes, pero no puede interpretar y reconstruir el contenido tan fácilmente.

1.3.2.2.2 Autenticación del Par

Los nodos IP requieren de la autenticación de cada una de las credenciales de sus vecinos, antes de establecer cualquier comunicación con ellos. Sin embargo, IP no incorpora autenticación de pares; los host IP pueden iniciar comunicaciones con otros pares sin haber probado que ellos hacen parte de una verdadera estructura de seguridad. Con IPsec, se establece una verdadera autenticación de credenciales entre pares, antes de iniciar cualquier intercambio de información. Lo anterior reduce el número de equipos de los cuales se pueden originar ataques a la red.

1.3.2.3 Protección del tráfico IP mediante IPsec

La figura muestra un paquete IP conteniendo un segmento TCP sin protección con IPsec.

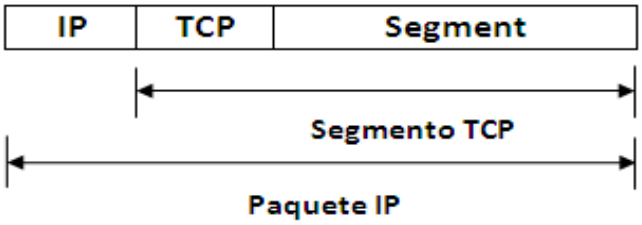


Figura 7. Paquete IP sin protección IPsec

Considerando lo anterior, existe una suma de comprobación en la cabecera de IP que permite la detección de errores (basados en nivel de bits), además de una suma de comprobación en la cabecera TCP que detecta los errores en el segmento TCP entero. Sin embargo, ninguna de esas sumas de comprobaciones fue concebida para proveer una protección segura, dejando al paquete IP susceptible a varios tipos de ataques en la red como suplantación de identidades (spoofing), modificación y determinación de datos.

Con el objeto de adicionar una protección de seguridad a los paquetes IP, IPsec añade dos protocolos de estructura, a saber:

Una extensión de la cabecera localizada entre la cabecera IP y el segmento TCP, conocida como Encabezado de Autenticación (**AH**, en inglés, Authentication Header).

De igual forma, una extensión de la cabecera y la cola del paquete IP conocida como Contenido de Seguridad Encapsulado (**ESP**, Encapsulating Security Payload).

1.3.2.3.1 Encabezado de Autenticación (AH)

La figura muestra un paquete IP que ha sido protegido con AH.

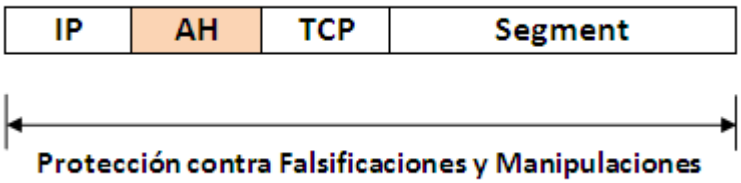


Figura 8. Paquete IP con protección AH

AH provee protección contra falsificaciones y manipulaciones de todo el paquete IP, excepto los campos específicos en la cabecera IP que pueden cambiar el tránsito. El AH incluye una suma de comprobación encriptada conocido como un código de autenticación de mensajes hash (**HMAC**, en inglés, Hash Message Authentication Code), cuyo cálculo incorpora una clave secreta compartida. En ambientes Windows, IPsec soporta el uso de los algoritmos **SHA1** (HMAC-Secure Hash Algorithm 1), el cual autentica con una clave secreta compartida de 160 bits y **MD5** (HMAC-Message Digest 5), cuya clave es de 128 bits.

AH proporciona entonces autenticación e integridad del paquete IP entre la comunicación de dos pares, sin permitir confidencialidad.

1.3.2.3.2 Contenido de Seguridad Encapsulado (ESP)

La figura muestra un paquete IP que ha sido protegido con ESP.

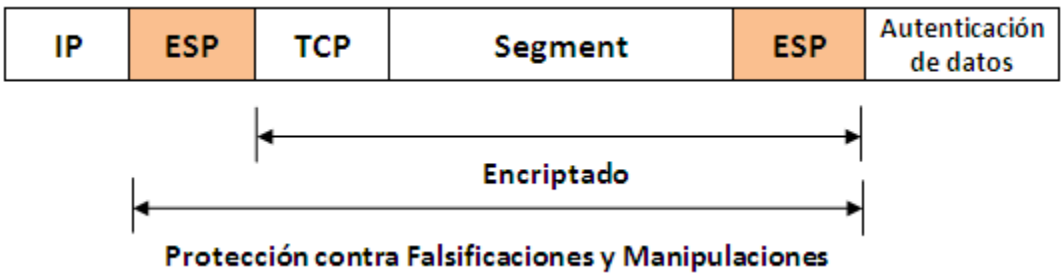


Figura 9. Paquete IP con ESP y Servicio de Seguridad Criptográfico

El conjunto de ESP y el servicio de seguridad criptográfico proveen una protección contra falsificaciones y manipulaciones. El campo de autenticación de datos en la cola del ESP incluye el resultado del cálculo de los algoritmos HMAC-SHA1 o HMAC-MD5.

ESP proporciona confidencialidad, autenticación e integridad, mediante la encriptación del paquete IP, esta última oculta los datos y las identidades de origen y de destino. Lo anterior se logra implementado algoritmos como DES (Data Encryption Standard) o 3DES (Triple Data Encryption Standard), el cual ofrece un mejor encriptamiento que el DES correspondiente a 56 bits.

El servicio de seguridad Criptográfico o encriptación, así como la autenticación son opcionales en ESP, es necesario seleccionar una de las dos como mínimo. A diferencia del AH, el ESP no provee protección para la cabecera IP. Sin embargo, el cálculo de la suma de comprobación en la cabecera TCP incluye los valores de las direcciones IP fuente y destino de la cabecera IP. Debido a que el campo de suma de comprobación en la cabecera TCP está protegido de manipulación, un atacante no pude cambiar la dirección IP en la cabecera IP, por tanto no se hace necesario la protección para la cabecera IP.

1.3.2.4 Estructura de IPsec

La implementación de IPSec se basa sobre un conjunto de protocolos criptográficos para:

Asegurar el flujo de paquetes.

Garantizar la autenticación mutua.

Establecer parámetros criptográficos.

La arquitectura de seguridad IP utiliza el concepto de asociación de seguridad (SA) como base para construir funciones de seguridad en IP. Una asociación de seguridad, en pocas palabras, consiste en el paquete de algoritmos y parámetros

(tales como las claves) que se usan para cifrar y autenticar un flujo particular en una dirección. Por lo tanto, en el tráfico normal bidireccional, los flujos son asegurados por un par de asociaciones de seguridad. La decisión final de los algoritmos de cifrado y autenticación (de una lista definida) le corresponde al administrador de IPsec.

La decisión de protección a proporcionar a un paquete saliente, IPsec emplea el índice de parámetro de seguridad (SPI), un índice a la base de datos de asociaciones de seguridad (SADB), junto con la dirección de destino de la cabecera del paquete, que juntos identifican de forma única una asociación de seguridad para dicho paquete. Para un paquete entrante es similar el procedimiento; en este caso IPsec toma las claves de verificación y descifrado de la base de datos de asociaciones de seguridad.

En el caso de multicast, se proporciona una asociación de seguridad al grupo, y se duplica para todos los receptores autorizados del grupo. Puede haber más de una asociación de seguridad para un grupo, utilizando diferentes SPI, y por ello permitiendo múltiples niveles y conjuntos de seguridad dentro de un grupo. En ese orden de ideas, cada remitente puede tener múltiples asociaciones de seguridad, permitiendo autenticación, ya que un receptor sólo puede saber que alguien que conoce las claves ha enviado los datos. Hay que observar que el estándar pertinente no describe cómo se elige y duplica la asociación a través del grupo. Esto se debe a que el emisor decide sobre qué seguridad manejar. En algunos casos el usuario es quien la elige, en otros, es la configuración misma de la red la que toma la decisión. Esta dualidad está en manos del administrador de la red.

Retomando los modelos principales de IPSec, en modo transporte, sólo la carga útil (los datos que realmente se quieren enviar, no el encabezado) del paquete IP es cifrada o autenticada. El enrutamiento permanece intacto, ya que no se modifica ni se cifra la cabecera IP; sin embargo, cuando se utiliza la cabecera de autenticación (AH), las direcciones IP no pueden ser traducidas, ya que eso

invalidaría el hash. Las capas de transporte y aplicación están siempre aseguradas por un hash, de forma que no pueden ser modificadas de ninguna manera (por ejemplo traduciendo los números de puerto TCP y UDP). El modo transporte se utiliza para comunicaciones ordenador a ordenador.

IPsec basa su estructura en una serie de algoritmos, representados en la siguiente figura.

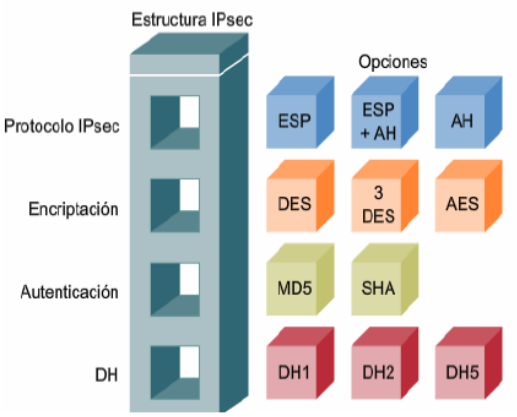


Figura 10. Estructura IPsec

Fuente: Tomada de Material Cisco “Servicios a Trabajadores a Distancia”, proporcionado por el Ingeniero Raúl Bareño Gutiérrez.

ALGORITMO	DESCRIPCIÓN	APLICACIÓN
DES	Encripta y descifra los datos.	Algoritmo de Encriptación
3DES	Mejora el encriptamiento de los datos que el DES, a 56 bits.	Algoritmo de Encriptación
AES	Alto rendimiento y encriptamiento más fuerte y rápido, según clave utilizada.	Algoritmo de Encriptación
MD5	Autentica con una clave secreta compartida de 128 bits.	Autenticación para proporcionar integridad
SHA-1	Autentica con una clave secreta compartida de 160 bits.	Autenticación para proporcionar integridad
DH	Dos partes establecen una clave secreta mediante la encriptación y los hash, como DES y MD5, sobre un canal no seguro.	Los pares comparten información de clave. DH1 ó DH2

Tabla 2 Síntesis de Algoritmos que conforman la estructura de IPsec.

Fuente: Adoptado del Material Cisco “Servicios a Trabajadores a Distancia”, proporcionado por el Ingeniero Raúl Bareño Gutiérrez.

IPsec impone un nivel de autenticación a los equipos que conforman una red, permitiendo negociar y proteger el tráfico de datos entre pares IPsec. Un host desconocido puede enviar paquetes a un host compatible con IPsec. Si este último requiere que todos los datos entrantes sean protegidos, éste descartará los paquetes provenientes del host desconocido. Sólo después de garantizar la autenticación IPsec y asegurar la negociación de las herramientas de seguridad, el host compatible con IPsec aceptará los paquetes entrantes que se determinen como protegidos.

Los paquetes protegidos por IPsec son examinados de fin a fin. El servicio de seguridad criptográfico adicional, hace difícil el acceso a los host maliciosos, detectando intrusiones, intentos de manipulaciones y falsificaciones. Un host malicioso puede ser capaz de falsificar la MAC y la dirección IP de un host IPsec, pero no pueden calcular fácilmente la suma de comprobación encriptada correcta, de esta manera no puede determinar el contenido de los paquetes capturados.

Sin embargo IPsec cuenta con varias limitaciones, como por ejemplo, en la transmisión de paquetes pequeños, el proceso de encriptación así como el de IPsec, genera un gran un gasto de recursos, lo que disminuye el desempeño de la red. Este gran número de características y opciones que ofrece IPsec, la convierten en una opción de seguridad muy compleja, lo que incrementa la probabilidad de presencia de puntos débiles, tal es el caso que IPsec es débil ante ataques de repetición.

2. REDES GUBERNAMENTALES

Los gobiernos actuales enfrentan el desafío doble de las crecientes amenazas para la seguridad de su tecnología y las reducciones frecuentes de sus presupuestos.

Conforme la tecnología avanza, son más las personas con conocimientos en redes y con capacidades para atacar servidores y portales estatales. Es por esto que el gobierno debe incrementar los esfuerzos para robustecer su seguridad en la red, así como las bases de datos cuya información afecta a todos sus ciudadanos.

Desafortunadamente el concepto de seguridad para muchos países como Colombia, se traduce en fuerza pública, policía, ejército y acompañamiento al ciudadano, olvidado que nuestro patrimonio digital, aunque intangible, es igual o más importante, y por tal motivo requiere de protección. Sin embargo es destacable el interés del gobierno Colombiano ante la problemática de la seguridad electrónica, estableciendo iniciativas en las que se proponen muchas alternativas para actualizar sistemas y equipos con el fin de ofrecer mejores servicios al ciudadano. Es así como se busca controlar las amenazas originadas cada día con el uso de las tecnologías de la información, el acceso a internet, comercio electrónico y el amplio acceso a la infraestructura tecnológica, mediante la creación e implementación de procedimientos, lineamientos y estándares, que contribuyan al mejoramiento de las políticas de seguridad de la información.

2.1 MODELO ACTUAL DE SEGURIDAD DE LA INFORMACIÓN GUBERNAMENTAL

Con el propósito de brindar una contribución al Estado Colombiano, respecto a la eficiencia, transparencia y niveles de participación ciudadana, se ha venido adoptando por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, MINTIC, el programa de ***Gobierno en Línea*** que busca la prestación de mejores servicios involucrando la participación de la sociedad mediante el uso y apropiación de las TIC, hecho que conlleva a impulsar la competitividad y mejoramiento de la calidad de vida de los colombianos.

Figura 11. Sala de espera oficinas Gobierno en Línea, previo a entrevista con la Ing. Yaciris Cantillo. Ed. Murillo Toro Piso 6.

Gobierno en línea está constituido por una serie de aspectos normativos, sociales, culturales, que implican un cambio organizacional para un Estado centrado en las necesidades del ciudadano, siendo este último, cliente de la Administración Pública y al cual se debe prestar un buen servicio. Desde este punto de vista, actualmente existen dos objetivos trazados por parte del gobierno nacional, los cuales corresponden a la protección de la información del individuo y la credibilidad y confianza en el Gobierno en Línea, para lo cual se deben establecer

mecanismos basados en estándares internacionales en seguridad de la información, así como estudios tecnológicos de mejores prácticas.

Figura 12. Escarapela entregada para lograr acceso a las oficinas de Gobierno en Linea

Tal es el hecho que organizaciones pertenecientes a diferentes sectores económicos del país, entidades gubernamentales, instituciones y profesionales dedicados a la normalización, se han ceñido a estándares y guías de normas internacionales con el objetivo que tanto los Servicios de Gobierno en Línea[13]como la Intranet Gubernamental[14] [16] cumplan con los principios básicos

[13]Servicios de Gobierno en Línea: "La aplicación de tecnología optimiza la prestación de trámites y servicios ofrecidos por las entidades públicas, lo cual impulsa un modelo de gestión pública orientado a una mayor satisfacción de la ciudadanía, como eje central de los procesos administrativos y consumidores de los servicios del Estado", tomado de http://programa.gobiernoenlinea.gov.co

[14] Intranet Gubernamental: "Es la estructura tecnológica a través de la cual se interconectan e integran las entidades para compartir recursos, intercambiar información, realizar procesos y actividades conjuntas, desarrollar trámites y servicios en línea, y facilitar el acceso de todos los ciudadanos a su información y servicios. Está compuesta por una Plataforma de Interoperabilidad y una Infraestructura Tecnológica", tomado de http://programa.gobiernoenlinea.gov.co

de la Seguridad de la Información (CIA[15]), a saber: confidencialidad, integridad, y disponibilidad de la información y los servicios.

En Colombia, actualmente las normas internacionales en seguridad de la información, has sido adoptadas, por el Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, de igual manera se han generado normativas de control interno como el MECI 1000, y de calidad como la NTCGP 1000, apoyado por estándares internacionales como COSO[16], ISO9001[17].

2.1.1 Estándares de Seguridad de la Información.

A continuación se presentan los principales estándares y mejores prácticas para la seguridad de la información y su relación con las normativa NTCGP 1000:2004 y el Modelo MECI, adoptados de la distribución realizada por el anterior Ministerio de Comunicaciones, en Octubre de 2008, en el documento "DIAGNÓSTICO DE LA SITUACIÓN ACTUAL -MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA ESTRATEGIA DE GOBIERNO EN LÍNEA" [17], con el cual se pretende dar en conocimiento, la base documental que se tiene en esta materia con relación a la seguridad de la información en el país.

[15] CIA, por sus siglas en inglés Confidentiality, Integrity, Availability, correspondiente a los Principios Básicos de la Seguridad de la Información.

[16]COSO: Committee of Sponsoring Organizations of the Treadway Commission. Comité de Organizaciones Patrocinadoras de la Comisión Treadway. Se centra en el control interno, especialmente el financiero. En Colombia este estándar fue utilizado para realizar el estándar de control interno MECI. Tomado de DIAGNÓSTICO DE LA SITUACIÓN ACTUAL -MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA ESTRATEGIA DE GOBIERNO EN LÍNEA, Ministerio de Comunicaciones, Octubre 2008.

[17] ISO 9001: Normas de gestión y garantía de calidad definidas por la ISO, Organización Internacional de Normalización.

2.1.1.1 Normas de gestión de seguridad

- ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems - Requirements. La norma equivalente en Colombia es la NTCISO/IEC 27001 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI) Requisitos.
- ISM3 v2.00 Information Security Management Maturity Model. Fue desarrollada por el ISM3 Consortium.

2.1.1.2 Mejores prácticas para Seguridad de Información

- ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management. La norma equivalente en Colombia es la NTC-ISO/IEC 17799 Tecnología de la Información. Técnicas de Seguridad. Código de Práctica para la gestión de la Seguridad de la Información, la cual corresponde a una traducción idéntica de la ISO/IEC 17799:2005.
- The Standard of Good Practice for Information Security 2007. Ha sido desarrollada por el Information Security Forum, ISF. La versión disponible actualmente corresponde al año 2007.
- NIST SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems. Esta guía fue desarrollada por el National Institute of Standards and Technology, NIST y la fecha de su publicación corresponde a septiembre de 2006.

2.1.1.3 Mejores prácticas de Gobierno y Control en Tecnología de Información

- Cobit 4.1 Control Objectives for Information and related Technology.
- IT Control Objectives for Sarbanes Oxley

- CONCT- Control Objectives for Net Centric Technologies.
- NIST SP 800 – 53 Recommended Security Controls for Federal Information Systems

2.1.1.4 Mejores prácticas para la prestación de servicios de TI

- Service Management - ITIL Version 3. Conjunto de mejores prácticas para la prestación del servicio de TI. Desarrollado por La Oficina de Gobierno de Comercio del Reino Unido.
- ISO/IEC 20000-1:2005 Information technology - Service management - Part 1:Specification
- ISO/IEC 20000-2:2005 Information technology - Service management - Part 2: Code ofpractice.

2.1.1.5 Normas de Administración de Riesgos

• AS/NZ 4360:2004 Risk Management, Standards Australia/Standards New Zealand

• ISO/IEC 27005:2008 Information technology - Security techniques - Information securityrisk management

• NIST SP 800-30 Risk Management Guide for Information Technology Systems.

2.1.1.6 Metodologías de Administración de Riesgos

• MAGERIT

• Octave

• General Security Risk Assessment Guidelines, ASIS International.

2.1.1.7 Normas para planeación de continuidad del negocio

• BS 25999-1:2006 Gestión de Continuidad de Negocio. Parte 1: Códigos de Práctica.

• BS 25999-2:2007 Especificaciones para la continuidad del negocio.

•NFPA 1600:2007 Standard on Disaster/Emergency Management and Business Continuity Programs.

De lo anterior y luego de realizar un análisis de los requerimientos de Gobierno en Línea, se seleccionaron los estándares cuyo propósito y principios, se interrelacionan con la estrategia de Gobierno en Línea de manera general:

- NTC ISO/IEC 27001:2005
- ISM3 v 2.00
- The Standard of Good Practice for Information Security - ISF-SOGP
- COBIT 4.1
- ITIL v 3
- AS/NZ 4360 Risk Management.

Las organizaciones, entidades gubernamentales, sectores de la industria y comunidad en general, se han concientizado de la importancia de brindar niveles de seguridad a la información que se maneja, para ello se está haciendo un uso efectivo de mejores prácticas y seguimiento de estándares, con el propósito de optimizar el uso de los recursos de las Tecnologías de la Información y reducir la presencia errores que puedan generar fallas en los proyectos, sistemas críticos, servicios proveídos, así como pérdida de inversiones y profundas brechas de seguridad que al final redunden en pérdidas económicas.

2.1.2 Iniciativas Nacionales en materia de Seguridad Informática

El actual desarrollo de Internet ha llevado a las entidades del país ha enfocar parte de sus recursos económicos y humanos, al estudio e implementación de medidas que contribuyan a preservar la seguridad de su información. El uso de redes públicas y el incremento de agentes maliciosos que enfocan sus ataques sobre infraestructuras computacionales, son una de las mayores preocupaciones de organizaciones privadas, públicas y académicas que últimamente han impulsado

la creación de entes o grupos enfocados a la atención de emergencias de seguridad informática, dirigiendo sus esfuerzos a las transacciones en línea del país.

A partir de esta necesidad el Estado Colombiano en conjunto con otras organizaciones, establecen un equipo de especialistas en seguridad informática bajo el Sistema Administrativo Nacional de Seguridad de la Información (SANSI), conocido como CSIRT[18]Colombia [18], cuyo fin es brindar respuestas a los incidentes relacionados con la seguridad, minimizando los riesgos ante vulnerabilidades de software, hardware o comunicaciones.

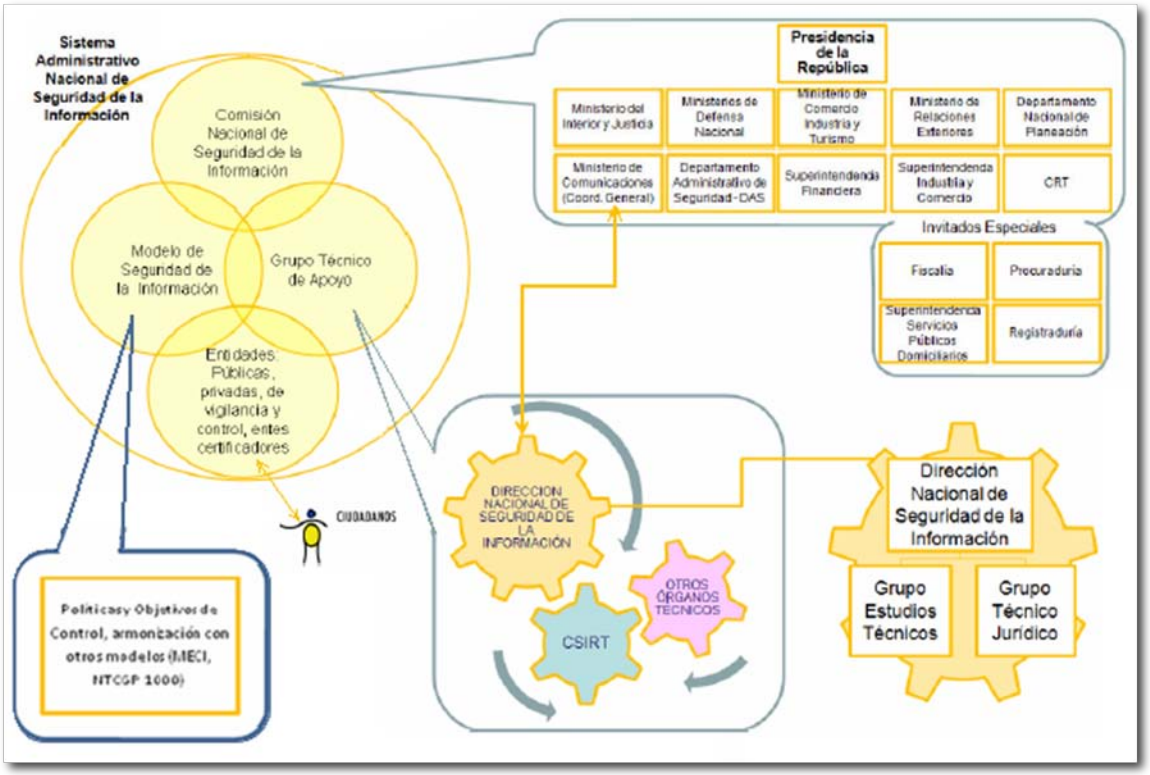


Figura 13. Modelo Detallado del Sistema Administrativo Nacional de Seguridad de la Información.

Fuente: Adoptado de DISEÑO DE UN CSIRT DE COLOMBIA PARA LA ESTRATEGIA GOBIERNO EN LÍNEA, Ministerio de Comunicaciones, 2008 [19].

[18]CSIRT (Computer Security Incident Response Team / Equipo de Respuesta a Incidentes de Seguridad Informática).

De esta manera, el SANSI desarrollará actividades de coordinación relacionadas con ejecución, seguimiento y, mantenimiento de políticas y lineamientos necesarios para robustecer la gestión de la seguridad informática en la nación. Actualmente este modelo de gestión se aplica a los siguientes servicios y productos:

Servicios de Gobierno en Línea

- Información y servicios.
- Portales de acceso.
- Trámites en línea.
- Sistemas sectoriales.
- Compras públicas.
- Sistemas transversales.

Intranet Gubernamental

- Plataforma de inter-operabilidad.
- Infraestructura tecnológica de comunicaciones.
- Infraestructura tecnológica de computación (Centro de Datos).
- Infraestructura tecnológica de contacto (Centro Interacción Multimedia).

2.2 INTRANET GUBERNAMENTAL

La Intranet Gubernamental [20] es una iniciativa actual del Estado Colombiano, que hace parte de la estrategia de Gobierno en línea y se define como la estructura tecnológica a través de la cual se integran dos componentes fundamentales, el primero la Infraestructura Tecnológica conformada por la Red de Alta Velocidad, el Centro de Datos y el Centro de Contacto Ciudadano y el segundo, la Plataforma de Interoperabilidad seccionada en Lenguaje para el Intercambio de Información y el Tramitador en Línea, todo esto con el propósito de

compartir recursos, información, realizar procesos y actividades conjuntas, llevar a cabo trámites y servicios en línea, además de fomentar el comercio electrónico y facilitar el acceso de todos los ciudadanos a su información.

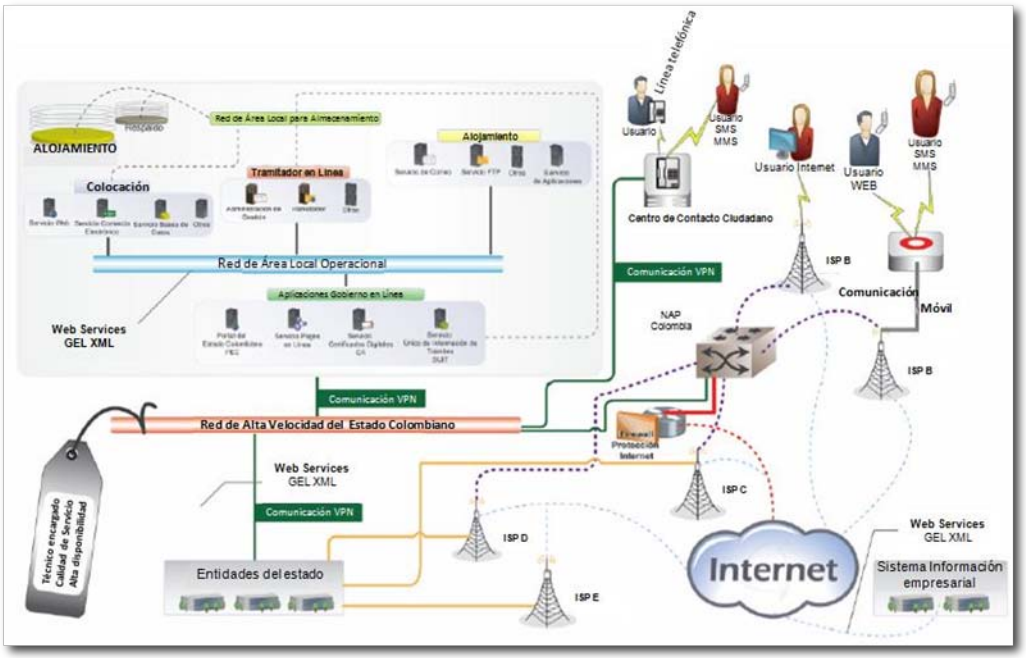


Figura 14. Modelo de Intranet Gubernamental

Fuente: Adoptado de http://www.intranet.gov.co

Dentro de los propósitos de la Intranet Gubernamental, se encuentran:

- Proporcionar a las entidades del Estado, una red privada de última tecnología, que permita la interconexión de las entidades públicas a altas velocidades, con lo que se pretende intercambiar información, llevar a cabo procesos y actividades conjuntas, todo esto con los más altos niveles de disponibilidad y seguridad. Esta posibilidad de ofrecer servicios convergentes y en ambiente, colaborativo trae como beneficio la comunicación transparente y eficiente de información entre organizaciones gubernamentales, lo que redunda en una optimización de los servicios entregados a los ciudadanos.
- Suministrar un centro de datos basado en un modelo de computación por demanda, que permita a las entidades gubernamentales conocer en un periodo de tiempo, la cantidad de recursos consumidos, así también las capas

funcionales utilizadas y el costo por consumo de recursos, todo ello con los más altos niveles de disponibilidad, oportunidad, crecimiento y seguridad.

- Desarrollar una Plataforma de Interoperabilidad para el intercambio de información, en donde sea posible llevar a cabo trámites, transacciones y servicios utilizando las entidades gubernamentales como mediador. Lo anterior bajo la adopción de un lenguaje basado en XML[19] para el intercambio de información, y una solución de software conocido como tramitador en línea.
- Implementar un punto integrado de contactos para usuarios, en donde se brinde atención, respuestas inmediatas y seguimiento a solicitudes, quejas y reclamos de los ciudadanos, ofrecido a través de distintos canales de comunicación.

Actualmente esta iniciativa se encuentra en estado terminado anormalmente [21], en cuya licitación se pretendía la selección de un oferente que garantizara la operación completa y eficiente de las soluciones de Gobierno en Línea, así mismo que estableciera la integración de las entidades estatales y la infraestructura y servicios incorporados a la Intranet Gubernamental. Este proceso viene siendo liderado por un convenio entre el Ministerio TIC y el Fondo de Proyectos de Desarrollo (FONADE), con el propósito fundamental de "lograr que los servicios del Estado sean más eficientes y que las entidades estatales colombianas se acerquen a los ciudadanos a través de la tecnología. Se busca, además,

[19]XML, por sus siglas en inglés e**X**tensible **M**arkup **L**anguage (Lenguaje de Marcas Extensible), corresponde a un lenguaje desarrollado para el intercambio de información estructurada entre diferentes plataformas. Permite que diferentes sistemas de información se entiendan e intercambien información de manera adecuada, sin tener que desechar los sistemas ya existentes.

garantizar los más altos estándares de seguridad en el manejo de la información".[20]

De lo anterior es importante resaltar que en la actualidad, el país no cuenta con una tecnología que ofrezca comunicación eficaz y segura entre las entidades gubernamentales, sólo se cuenta con desarrollos puntuales entre organizaciones en algunas ciudades del país, adelantos aislados que no involucran información con el resto del territorio Colombiano, lo que en materia de telecomunicaciones despierta la atención de realizar estudios de tecnologías aplicables a brindar una solución a esta necesidad, tal como las redes P2P, objeto de estudio del presente documento.

[20]Declaración del actual Ministro TIC, Diego Molano Vega, en la apertura de la licitación LP001- de 2011 correspondiente a la Intranet Gubernamental para Gobierno en línea. Bogotá, D.C. Enero 21 de 2011.

3. PROPUESTA TECNOLOGÍA P2P PARA LA SECRETARÍA DE SALUD DISTRITAL DE SANTA MARTA

El propósito de conocer las actividades que ha venido desarrollando el Gobierno Nacional en materia de TIC, posibilita el ofrecimiento de soluciones al implementar nuevas tecnologías que contribuyan a la comunicación entre organizaciones gubernamentales, pudiendo de este modo compartir recursos, transferir información y demás actividades inherentes de manera rápida, eficaz y segura. Partiendo de lo anterior y considerando los temas tratados a lo largo de este documento, se establece la revisión del estado informático de la Secretaría de Salud Distrital de Santa Marta, con el fin de establecer la viabilidad de implementar una red P2P segura en sus procesos de comunicación.

El conocimiento de las funciones de la entidad pública, así como el contenido de la información manipulada, se convierte en un factor fundamental que determina el tipo de red de datos necesaria para llevar a cabalidad sus labores con la calidad requerida. De este modo se evalúan distintos parámetros que conllevan a valorar positiva o negativamente la tecnología propuesta.

3.1 SECRETARÍA DE SALUD DISTRITAL DE SANTA MARTA

Figura 15. Secretaría de Salud del Distrito de Santa Marta

Los distritos son entidades territoriales que tienen una o varias características que las destaca o diferencia de los municipios circundantes, tales diferencias redundan en su importancia política, comercial, histórica, turística, cultural, industrial, ambiental, portuaria, universitaria o fronteriza.

El Distrito Turístico, Cultural e Histórico de Santa Marta nace como una iniciativa de sus gobernantes y a la Constitución de 1991, la cual decretó a los Distritos portuarios de las Ciudades de Barranquilla, Santa Marta y Cartagena[21]. Luego este estado fue reiterado en los años de 1993[22]y 2009[23].

Si bien, El distrito de Santa Marta no posee el nivel considerable a un departamento como el Distrito Especial de Bogotá, si posee un régimen de transferencias y de manejo independiente del Departamento del Magdalena, del cual, aún es capital.

Como todo municipio, posee sus entidades descentralizadas. Entre estas, se encuentra la Secretaria de Salud Distrital.

Figura 16. Ubicación Geográfica de la Secretaría de Salud del Distrito de Santa Marta.
Fuente: Google Maps.

[21]Artículo 356 de la Constitución de Colombia de 1991.

[22]Artículo 2º del acto legislativo número 1 de agosto 18 de 1993.

[23]Corte Constitucional, Sentencia C-033 de 2009.

La secretaría de Salud del Distrito de Santa Marta tiene como misión dirigir, coordinar, evaluar y controlar el Sistema General de Seguridad Social de Salud en el Distrito, para garantizar de manera efectiva el derecho de los habitantes a la seguridad social e impulsar la obtención de un mejor nivel de bienestar y progreso integral a la población del Distrito de Santa Marta.

3.1.1 Estado tecnológico de la secretaría de salud distrital de Santa Marta[24]

Dentro de las funciones de la secretaría de salud distrital, se desataca la de "Adoptar, administrar e implementar el sistema integral de información en salud, así como generar y reportar la información requerida por el Sistema" (Ver Anexo 1. Funciones de la secretaría de salud distrital de Santa Marta), que junto con actividades de promoción y prevención, son llevadas a cabo por otra entidad descentralizada, adscrita pero no dependiente de la secretaria de salud misma. Dicha entidad es la encargada de manejar la atención de primer nivel, así como gran parte de la estadística del organismo público, lo que conlleva a un desentendimiento con las demás entidades gubernamentales relacionadas con el sector salud.

A nivel de infraestructura tecnológica, la Secretaria de Salud Distrital se encuentra en un estado de retraso, debido a los problemas económicos que padece el Distrito de Santa Marta. Es mínimo el recurso destinado a las TIC y en la mayoría de los casos se destina al mantenimiento o cambio de equipos que por su uso y deterioro requieren reemplazo. En periodos administrativos anteriores, se contaba con página web propia, en la cual se ofrecían servicios a entidades para validar su información y registro ante este organismo, iniciativa que terminó con el cambio de mandato, hecho que dejó de lado esta propuesta tecnológica.

[24]Información recopilada de visita sostenida con Adrian Diazgranados, Ingeniero de Sistemas de la Secretaría de Salud Distrital de Santa Marta.

Actualmente la entidad cuenta con los siguientes equipos relacionados.

EQUIPO	CANTIDAD
Equipos de Cómputo Desktop	32
Servidores	3
Equipo de Cómputo Laptop	10
Modem ADSL	1
Switch 24 Puertos	3
Switch 8 Puertos	2
Router Cisco 2500 series	1
Router WiFi	1

Tabla 3. Inventario de Equipos de Comunicaciones de la Secretaria de Salud Distrital de Santa Marta

Las observaciones realizadas por el ingeniero jefe del área de sistemas, indican que los servidores han venido cambiando sus funciones conforme las administraciones lo requieran. En el periodo en que la página web se encontraba en funcionamiento, uno de los equipos actuaba como servidor de base de datos de la información ingresada en el portal web, éste era manejado por un hosting. Al finalizar el contrato, este aun mantiene la base de datos adquirida, sin embargo actualmente posee un servidor local que cumple la función de recepción de documentos de usuarios, los cuales son ingresados localmente por la red LAN. Un segundo servidor tenía la función de actuar como Firewall de la conexión a Internet para proteger la base de datos, actualmente se tiene como un elemento más del inventario. Un tercer servidor actuaba como servidor de directorio activo, puesto que la dependencia contaba con un sistema de dominio basado en Windows NT (Windows 2003 Server Standard). Actualmente esta plataforma se

dejo de usar y solo se usa como servidor de almacenamiento donde se almacena la información importante para mantenerla centralizada.

La Secretaria de Salud se conecta a Internet a través de una conexión de par de cobre, mediante un Modem ADSL, el cual maneja un ancho de banda de 4 Mb, causando cuellos de botella en horas pico. Además la entidad carece de sistemas de control de ancho de banda, y proxy para la optimización del canal a Internet.

Según información suministrada, la interacción de la secretaría con demás entidades centrales (Alcaldía, MinProtección), se lleva por medio de correo electrónico o físico. Esto se debe que al terminar el contrato de hosting se perdió el dominio y por tanto el servicio de correo electrónico. Actualmente, la mayoría de los casos, los funcionarios usan sus correos electrónicos personales para distribuir información institucional con los problemas de seguridad que esto puede acarrear.

3.2 PROPUESTA DE RED P2P

Tal como se describió en el estado del arte de la Secretaría de Salud del Distrito Turístico, Cultural e Histórico (DTCeH) de Santa Marta, la entidad atraviesa un atraso en el área de las TIC, con pocas opciones de solucionar esta problemática a corto o mediano plazo.

Atendiendo a la descripción de los equipos, redes y conexiones, las redes P2P seguras surgen como una alternativa para tener en cuenta en este caso de acuerdo con los siguientes lineamientos:

EQUIPOS: Se cuenta con una cantidad de equipos de escritorio con una limitada capacidad de procesamiento debido a su tiempo de vida, además de la ausencia de equipos servidores. Las redes P2P no requieren máquinas potentes, solo

requiere equipos con gran capacidad de almacenamiento, acceso a la red y unos cuantos ciclos de procesamiento que no afectan el desempeño general del equipo y que generan poco impacto a la UI[25]o a la experiencia del usuario.

REDES: La única salida a Internet es un canal por par de cobre con una conexión ADSL[26] con 4Mb de descarga y unos 900kbps de subida. Como la mayoría de la información será manejada localmente, la red LAN de la secretaría de salud, con sus 100Mbps de velocidad son ideales para compartir la información. La información para otras entidades puede ser enviada a través del canal de ADSL, teniendo en cuenta que la gran cantidad de los datos son documentos de texto y hojas de cálculo, la tasa de transferencia sigue siendo aceptable teniendo en cuenta lo que se envía.

PERSONAL REQUERIDO: Una vez se decide la infraestructura y se deja programado el software requerido para instalarse en los nodos, el mantenimiento es sencillo, casi nulo, y de acuerdo al grado de redundancia de la información que se proporcione, el soporte es mínimo y solo se aplicaría en caso de falla catastrófica del nodo.

Para esta aplicación se cuenta con tres servidores, de los cuales dos están sub utilizados, se propone implementar una red P2P híbrida de tipo CHORD con manejo de jerarquías por reputación y validación de usuarios.

Vale la pena recordar que en las redes P2P tipo CHORD, la única función del servidor es la de organizar la distribución de la información de acuerdo a las

[25]**UI:** User interface o Interfaz de Usuario, es el entorno que el usuario de un sistema informático recibe de la máquina y con el cual interactúa.

[26]**ADSL** son las siglas de Asymmetric Digital Subscriber Line ("Línea de Abonado Digital Asimétrica"). Consiste en una transmisión analógica de datos digitales apoyada en el par simétrico de cobre que lleva la línea telefónica convencional o línea de abonado, siempre y cuando la longitud de línea no supere los 5,5 km medidos desde la Central Telefónica, o no haya otros servicios por el mismo cable que puedan interferir.

necesidades y niveles de demanda de las mismas. Esto quiere decir, que documentos con alta rotación y demanda, deben ser replicados para un acceso más fácil. A los archivos de bajo uso, se reducirá su nivel de redundancia y se mantendrán solo con fines de reserva de información. Atendiendo que la mayoría de los equipos tienen 2 años de antigüedad, sus discos duros oscilan entre los 80 y 250 Gb de capacidad. Realizando un cálculo sencillo, teniendo en cuenta la cantidad de equipos estáticos (aproximadamente 32), se obtiene alrededor de 5 Terabytes de capacidad; cantidad suficiente para almacenar la información[27] de la entidad.

Con el objeto de respetar la integridad de la información, la red debe contar con un sistema de jerarquías que permita establecer permisos de lectura y edición de documentos según el cargo del funcionario a cargo de los mismos. Una vez que el servidor valide la identidad del funcionario, éste puede brindar acceso al archivo ya sea para solo lectura o edición. Una vez termine la lectura o edición del documento, éste debe actualizar su base de datos y en momentos de baja demanda debe reemplazar las replicas del archivo por la versión actualizada. Así mismo, el sistema debe mantener una base de datos con el registro de las ediciones hechas y por quienes fueron hechas. Es posible implementar una base de datos para tal fin o en los metadatos del documento guardar este registro.

La UI del sistema debe ser muy similar a un sistema de consulta bibliográfica, donde se pueda apreciar los documentos recientes manejados por el funcionario y permitirle efectuar búsquedas por título o por áreas de desempeño de la entidad; por ejemplo: Promoción y prevención, contabilidad, personal, políticas públicas, proveedores, EPS, IPS, entre otras.

[27] No se tiene en cuenta la capacidad de los servidores que es aun mayor puesto que uno mantendrá la base de datos de entidades y otro actuaria como índice de la plataforma CHORD.

Manteniendo la premisa de no obligar a la entidad a adquirir nuevos servicios y recordando que carecen de portal web para atención al público, no se permitirá acceso a usuarios anónimos o al público en general al sistema.

La conectividad entre equipos se maneja a nivel de IP permitiendo que los nodos sean capaces de comunicarse entre redes independiente si están bajo un NAT, (ya sea por relevo o por cualquier otra técnica para superarlo), de otra manera, si poseen una IP pública. Este funcionamiento es el similar a los programas P2P que se conocen para el intercambio de música, nos permite superar los módems y equipos que pueden afectar la conectividad. Esta propiedad se torna más importante teniendo en cuenta que los equipos en la secretaría de salud se encuentran tras un modem ADSL que maneja la traducción de direcciones para lograr, con una sola IP pública brindar servicio a las más de 30 máquinas trabajando en el lugar. Sumado a esto, debemos contemplar las máquinas que tendrán acceso a la información desde fuera de las instalaciones de la secretaría. Equipos en la Alcaldía, Ministerio de Protección Social o en cualquier otra dependencia que el administrador de la red considere que es necesario conectar.

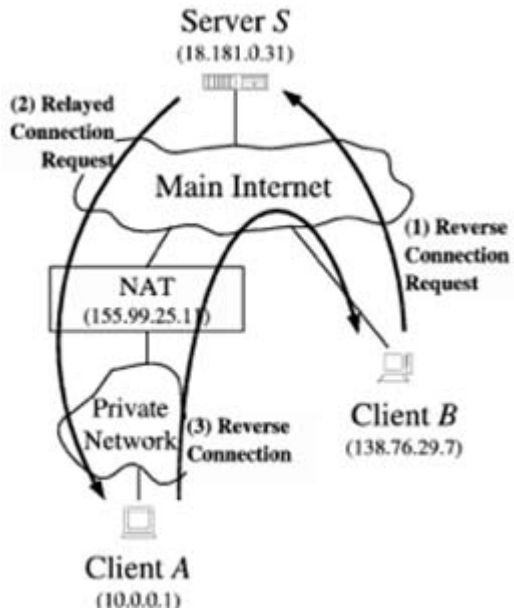


Figura 17. Ejemplo de una red P2P atravesando NAT usando el método de conexión inversa. Fuente: Adoptado de http://www.brynosaurus.com

Es necesario recordar que el sistema debe contar con una plataforma de validación de usuarios el cual correrá en el servidor CHORD, este último a su vez es quien maneja el índice de los archivos y decide la distribución y redundancia de los mismos.

Al estar el sistema expuesto a Internet, salen a flote los problemas intrínsecos de las redes P2P actuales: entradas no autorizadas, imposibilidad de controlar quienes acceden y modifican los archivos, y el posible anonimato al acceder a contenidos restringidos.

Los contenidos compartidos en esta red son altamente sensibles, al manejar información sobre estadísticas de atención, proveedores de servicios, seguimiento a políticas en salud pública y subsidiada así como tarifas y costos de servicios y prestaciones hacia el estado. Todo esto en manos inadecuadas puede alterar fácilmente el comportamiento de la salud pública en el área de influencia de la secretaría. La opción más viable (sin salir de los limites de las capacidades de las redes P2P) es considerar una simbiosis entre manejo de reputación en los nodos, manejo de usuarios con contraseña y control de cambios en los archivos. En el medio no es común encontrar una red P2P bajo el GNU (libre) que cuente con los tres principios de seguridad y funcione correctamente. Lo anterior genera dudas en la factibilidad de la propuesta ya que, con la criticidad de los datos traficados en la red, se requiere el máximo de seguridad posible.

Tomando en consideración la información recopilada a través del presente documento, las redes P2P que se destacan por su seguridad, basan su funcionamiento básicamente en dos métodos: el sistema de jerarquías y enrutamiento seguro basado en esas jerarquías. Cuando un equipo transmite información dudosa o alterada, los otros nodos notan su error y reducen la jerarquía dentro de la red. Al bajar su reputación, los otros nodos omitirán acudir al equipo involucrado, y con el sistema de enrutamiento seguro, al reducir también su

jerarquía los servidores cambian las reglas de enrutamiento para evitar accederlo y arriesgar la integridad de la información en los nodos anexos.

Dos situaciones salen a flote, a saber, primero la manera de garantizar la integridad de los archivos, una vez se evite acceder a un nodo comprometido con la seguridad y en segundo lugar, la forma de validar los usuarios que acceden a los archivos, toda vez que las máquinas involucradas en la interconexión se encuentren validadas.

Una solución viable corresponde a la implementación de una VPN[28] en la cual los nodos incluidos en la solución P2P se encuentren dentro de la misma red. Esto permitiría validar el nodo antes de ingresar y una vez adentro podría trabajar libremente sin riesgos. Nuevamente surge otro interrogante: cómo manejar los niveles de acceso a los diferentes tipos de usuarios?. Se debe implementar una plataforma similar a la de una base de datos donde de acuerdo con el usuario, le sea permitido el acceso a diferentes carpetas o procesos del sistema. En P2P este tipo de seguridad no es fácil de implementar debido a lo versátil, anónima y variable de la red misma.

Si bien no hay red 100% segura, las redes P2P no son la excepción, estas son vulnerables a ser alteradas o suplantadas. Sin embargo las características que hacen considerar las redes P2P como una opción fácil de implementación para compartir contenidos restringidos, son las mismas que hacen difícil su posibilidad de ser aplicadas en redes donde la seguridad sea la clave del éxito.

La seguridad en las redes y en los sistemas informáticos se basa en tres aspectos y/o principios fundamentales:

[28] Red privada virtual, RPV, o **VPN** de las siglas en inglés de **Virtual Private Network**, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

Figura 18. Pirámide de seguridad en informática.

De acuerdo con lo expuesto en el presente análisis, las redes P2P garantizan por sobre todo la disponibilidad. Las redes P2P seguras permiten, hasta cierto punto contar con confidencialidad, pero actualmente se están buscando alternativas que garanticen la integridad de la información. El sistema CHORD, el usado en redes universitarias para el manejo de datos en redes P2P, solo puede discriminar los equipos que atentan alterar la información sin previa autorización. Pero la red misma no es capaz de determinar con un alto grado de seguridad el equipo que inició el ataque o el usuario que altero la información en primer lugar. Teniendo en cuenta la criticidad de la información manejada en una entidad como una Secretaría de Salud, al carecer de garantías de la integridad de la información, se torna inviable la factibilidad de una solución como estas para un entorno gubernamental.

Los casos de éxito de las redes P2P seguras se encuentran en entornos controlados como redes universitarias o redes corporativas donde el acceso desde Internet está restringido. Los equipos involucrados son de granjas de equipos usado por empleados o estudiantes dentro de ambientes seguros y en los que la

información está disponible a todos. Esto sucede porque la información es altamente segura o clasificada y hace necesario medidas adicionales para evitar la filtración de esta. Estas restricciones se convierten en un paso muy limitante si se quiere aprovechar las capacidades de estas redes en entornos abiertos como Internet.

La intención de esta propuesta corresponde a garantizar los tres pilares de la seguridad en red en una plataforma libre, económica y versátil. Si bien las redes P2P son una opción viable en estos ambientes controlados, no son aplicables a nuestro caso particular.

Es necesario recordar que no hay infraestructura de red 100% segura, pero un servidor con una base de datos el cual está dentro de una zona protegida con firewall y con un sistema de validación mediante usuario, contraseña y privilegios de acceso, resulta más viable que una red P2P segura, de acuerdo con las investigaciones actuales y el estado del arte de este sistema.

No se debe desconocer los avances notorios que han tenido las redes P2P en lo que a seguridad y confiabilidad se refiere. Pero actualmente los avances que han tenido las redes P2P, no alcanzan con la capacidad de permitir un nivel de seguridad suficiente para satisfacer las demandas de los entornos donde se exigen niveles altos de seguridad e integridad, por ende se puede decir que aún no está lista.

	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD
BASE DE DATOS	Según la capacidad del servidor, la capacidad está supeditada a la capacidad del equipo y el canal que posea.	El control de acceso a usuarios y privilegio controla los cambios y quien los hizo. Se debe hacer constante backup en caso de necesitar volver a una versión anterior.	El motor de base de datos garantiza la privacidad de la información mediante usuario y contraseña y/o otras medidas biométricas de ser necesario o estar disponible.
REDES P2P	Alta disponibilidad. Las redes P2P permiten alta redundancia y alta tolerancia a fallos.	Muy Baja, por su característica de anonimidad es poco fácil garantizar quien modifico y desde que equipo.	Las redes CHORD mediante manejo de reputación y tablas de enrutamiento según calificación permite evitar accesos indeseados hasta cierto nivel.

Tabla 4. Comparación entre las Redes P2P seguras y un sistema de base de datos, teniendo en cuenta los factores principales de la seguridad en la red.

CONCLUSIONES

Las redes P2P están sufriendo una transición de ser un sistema del mundo de la piratería y violación de derechos de autor a ser una alternativa de conectividad y de respaldo viable para el mundo corporativo. Diariamente se avanza en nuevas técnicas que permitan convertir las redes peer to peer en sistemas robustos para entidades que requieran de una solución económica para el almacenamiento, acceso y distribución de la información.

Modelos de red como las redes CHORD y PASTRY demuestran la factibilidad de construir una red basada en equipos económicos los cuales permiten crear una infraestructura redundante y rápida para el almacenamiento e intercambio de información. Métodos tales como el sistema de jerarquías y los modelos de enrutamiento basados en la reputación del nodo permiten un grado de seguridad que identifica al perpetrador y lo aísla, evitando la diseminación de documentos falsos o alterados en la red. Diariamente se observan avances en las otras áreas de seguridad como son la integridad y la confidencialidad, ya que la disponibilidad esta mas que cubierta.

Los Gobiernos de países en desarrollo, en especial Colombia, apenas comienzan a valorar las capacidades de las redes en la prestación de sus servicios a sus ciudadanos. Nuestro país actualmente desarrolla dos grandes proyectos: Gobierno en Línea y la Intranet Gubernamental. Con estas iniciativas, el estado Colombiano pretende acercarse al ciudadano de una manera que evite traumatismos, la manipulación desgastante de documentos y congestión en oficinas, evitar el desplazamiento a las grandes urbes y el consumo de recursos innecesarios. Desafortunadamente, por problemas económicos y por la estructura misma del estado, estas propuestas solo serán efectivas en entidades directamente influenciadas por el gobierno central. Organizaciones descentralizadas como secretarías municipales o departamentales están a la merced de sus entes territoriales.

La secretaría de Salud del Distrito de Santa Marta no es ajena al precario estado de las TIC en entidades del Estado. Un municipio declarado en insolvencia económica (Ley 550), malos movimientos políticos, poco cuidado a el estado de las redes y subvaloración a la importancia de las TIC la han convertido en una entidad carente de una plataforma tecnológica que facilite su operación. A juzgar por la situación actual del municipio el panorama no promete mejorar en el mediano plazo.

En vista del estado de la Secretaría de Salud del Distrito de Santa Marta, se propuso una red P2P con los avances actuales en seguridad para usarlo como alternativa de conectividad y de almacenamiento masivo usando la infraestructura existente en la Secretaria de Salud del Distrito de Santa Marta. Al analizar las variables involucradas y el estado del arte de las redes P2P seguras, la posible implementación enfrenta grandes retos para superar problemas importantes en las áreas de Integridad y Confiabilidad de la información depositada en la red. Siendo una entidad estatal, manejando información sensible para la ciudadanía, esta propuesta resulta inviable de acuerdo con los avances de las redes P2P a hoy día.

Hasta hace unos años, se consideraba risible pensar que una red usada para compartir información con derechos de autor, fuese considerada como una alternativa de almacenamiento y acceso a información. Casos de éxitos en universidades como la de Washington demuestra que la propuesta es viable a futuro. Se reconoce que los avances en el tema de las redes P2P muy pronto permitirán superar estos impases, pero actualmente estas falencias generan más problemas que los que soluciona. Consideramos que una vez solventados, las redes P2P seguras podrán convertirse en el sistema de almacenamiento y consulta rápido, económico y seguro que se espera ser.

BIBLIOGRAFÍA

[1] Medina V, Jorge A, “INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN”, Segunda Edición, Especialización en Telecomunicaciones, UIS, Abril 2011.

[2] Gnutella, http://www.gnutella.com

[3] SETI@HOME , http://setiathome.berkeley.edu/

[4] Napster, http://www.napster.com.

[5] Kazaa, http://www.kazaa.com

[6] Ares, http://aresgalaxy.sourceforge.net/

[7] BitTorrent, http://www.bittorrent.com

[8] eDonkey, FALTA

[9] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, “Chord: A scalable peer-to-peer lookup service for internet applications,” in Proc. ACM Conf. on Applications, Technologies, Architectures, and Protocols for Comp. Comm. (SIGCOMM’01), San Diego, California, August 2001, pp. 149–160.

[10] A. Rowstron and P. Druschel, “Pastry: Scalable, decentralized object location and routing for large-scale peer-to-peer systems,” in Proc. IFIP/ACM Int. Conf. on Distributed Sys. Platforms (Middleware ’01), Heidelberg, Germany, November 2001, pp. 329–350.

[11] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Schenker, “A scalable, content-addressable network,” in Proc. ACM Conf. on Applications,

Technologies, Architectures, and Protocols for Comp. Comm. (SIGCOMM' 01), San Diego, California, August 2001, pp. 161–172.

[12] A. Kalafut, A. Acharya, and M. Gupta, "A study of malware in peer to peer networks," in Proc. 6th ACM SIGCOMM Internet Measurement Conf. (IMC'06), Rio de Janeiro, Brazil, October 2006, pp. 327–332.

[13] J. R. Douceur, "The Sybil attack," in Proc. 1st Int. Workshop on Peer to peer Sys. (IPTPS'02), Cambridge, MA, March 2002, pp. 251–260.

[14]Kevin W. Hamlen and Bhavani Thuraisingham - Secure Peer-to-peer Networks for Trusted Collaboration - Computer Science Department – MS EC31 University of Texas at Dallas

[15] Rupert Gatti, Stephen Lewis, Andy Ozment, Thierry Rayna, and Andrei Serjantov- Sufficiently Secure Peer-to-Peer Networks - Faculty of Economics and Politics, University of Cambridge.

[16] http://programa.gobiernoenlinea.gov.co

[17] DIAGNÓSTICO DE LA SITUACIÓN ACTUAL -MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LA ESTRATEGIA DE GOBIERNO EN LÍNEA, Ministerio de Comunicaciones, Octubre 2008.

[18] http://www.cert.org.co/

[19] DISEÑO DE UN CSIRT DE COLOMBIA PARA LA ESTRATEGIA GOBIERNO EN LÍNEA, Ministerio de Comunicaciones, Octubre 2008

[20] http://www.intranet.gov.co

[21] http://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=11-1-63306

[22] Peter Danielis, Dirk Timmermann - Use of Peer-To-Peer Technology in Internet Access Networks and its Impacts (IPDPS 2010 PhD Forum) - The Institute of Applied Microelectronics and Computer Engineering at University of Rostock - 18051 Rostock, Germany

[23] Voichita Iancu, Iosif Ignat - A self-adapting peer-to-peer logical infrastructure, to increase storage reliability on top of the physical infrastructure - University Politehnica of Bucharest, Technical University of Cluj-Napoca - voichita.iancu@cs.pub.ro

[24] Hailong Sun, Jinpeng Huai - Combining Reliability and Economic Incentives in Peer-to-Peer Grids - School of Computer Science and Engineering, Beihang University, Beijing, China - {sunhl, huaijp }@buaa.edu.cn

[25] Simon Rieche, Klaus Wehrle, Olaf Landsiedel, Stefan Götz, Leo Petrak - Reliability of Data in Structured Peer-to-Peer Systems - Protocol Engineering and Distributed Systems Group University of T¨ubingen, Germany.

[26] Lee Garber - Proponents Try to Rehabilitate Peer-to-Peer Technology - IEEE Computer Magazine - Edición abril 2008, Paginas 16 - 19. - l.garber@computer.org

[27] Tim Schattkowsky, Christoph Loeser, Wolfgang Mu□ller - Peer-To-Peer Technology for Interconnecting Web Services in Heterogeneous Networks - Paderborn University, Germany, C-LAB, Germany - timschat@uni-paderborn.de

[28] KATO Tomoya, YOKOI Shigeki - Application of P2P (Peer-to-Peer) Technology to Marketing - Graduate School of Human Informatics, Nagoya University - tkatoh@info.human.nagoya-u.ac.jp, yokoi@info.human.nagoya-u.ac.jp

[29] http://iv.slis.indiana.edu/sw/chord-model.html

[30] https://gnunet.org/es

[31] http://setiathome.berkeley.edu/

[32] Camarillo, G., "Peer-to-Peer (P2P) Architecture: Definition, Taxonomies, Examples, and Applicability", RFC 5694, November 2009.

[33] Milojicic, D., Kalogeraki, V., Lukose, R., Nagaraja, K., Pruyne, J., Richard, B., Rollins, S., and Z. Xu, "Peer-to-Peer Computing", Technical Report HP, March 2002.

[34] Schollmeier, R., "A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications", In Proceedings of the First International Conference on Peer-to-Peer Computing P2P ’01, 2001.

[35] Roussopoulus, M., Baker, M., Rosenthal, D., Guili, T., Maniatis, P., and J. Mogul, "2 P2P or Not 2 P2P", Workshop on Peer-to-Peer Systems, February 2004.

[36] Friedman, Allan, Camp, L. Jean – Peer to Peer Security – Harvard Security

[37] Millán Tejedor, Ramón Jesús, “Domine las redes P2P: “Peer to Peer” orígenes, funcionamiento y legislación P2P, selección y configuración del acceso de banda ancha a internet”, Creaciones Alfaomega, Copyright, 2007.

[38] González, Abel Santín, “Peer 2 Peer, Sistemas Operativos Distribuidos”, 2007.

[39] Huang, H., Wu, H., Wang G., “Study of Distributed P2P Information Sharing System”, Third International Symposium on Intelligent Information Technology Application, 2009.

[40] Schulzrinne, H., Marocco, E., Ivov, E., “Security Issues and Solutions in Peer-to-Peer Systems for Realtime Communications”, RFC 5765, February 2010.

[41] Marc Sánchez-Artigas, Dept. of Computer Engineering and Maths, Universitat Rovira i Virgili, Spain, “Distributed Access Enforcement in P2P Networks: When Privacy Comes Into Play”, IEEE P2P 2010 proceedings, 2010.

[42] Lehrieder, F., Oechsner, S., Hobfeld, T., Despotovic, Z., Kellerer, W,Michel, M., “Can P2P-Users Benefit from Locality-Awareness?”, IEEE P2P 2010 proceedings, 2010.

[43] Bauwens, M., “P2P and Human Evolution: Peer to Peer as the premise of a new mode of civilization”, Foundation for P2P Alternative, Draft 1.1, March 2005.

[44] http://www.mintic.gov.co/

[45] Bareño G. Raul., “Servicios a Trabajadores a Distancia”, Material de Curso Cisco, 2011.

[46] Al-Amodi A., “Authentication study and Implementation using IPsec and IEEE 802.1X technology”, University Technology Malasia, April 2009.

[47] http://technet.microsoft.com/en-us/library/bb727017.aspx

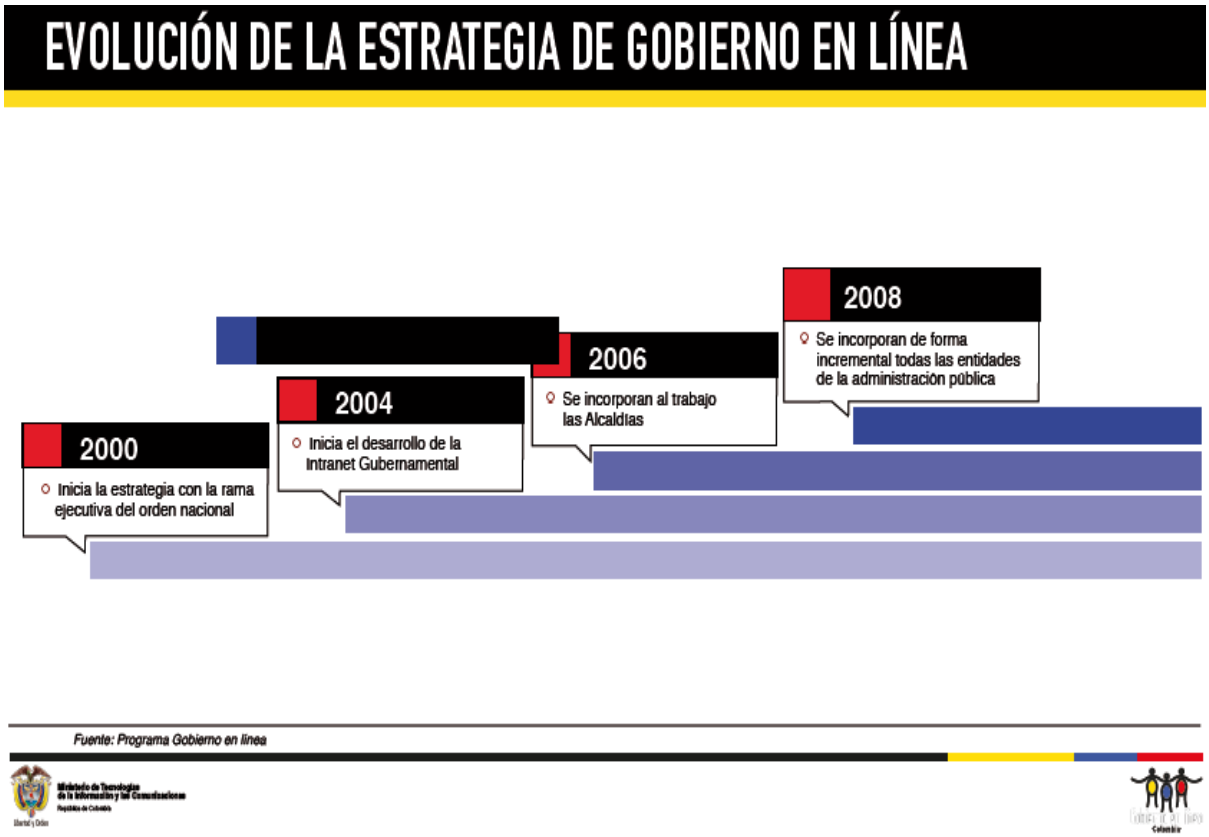
[48] Kent S., Seo K., “Security Architecture for the Internet Protocol”, Request for Comments, RFC 4301, December 2005.

ANEXOS

ANEXO 1.

EVOLUCIÓN DEL GOBIERNO EN LÍNEA 2011-2019.

Tomado de Ponencia del Doctor Francisco Camargo Salas, Gerente Programa Gobierno en Línea. Diciembre 2010.

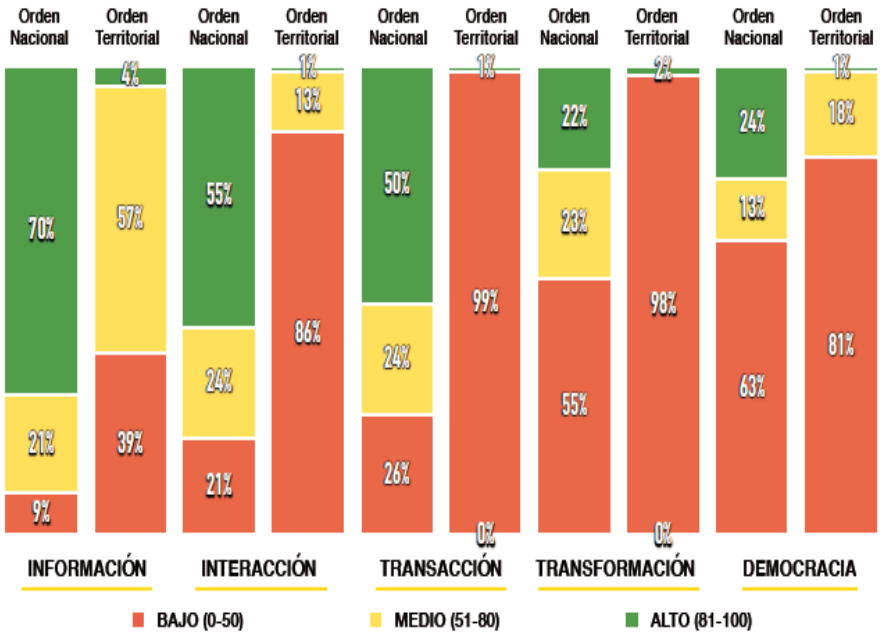


FACTORES CLAVE DE ÉXITO

	Descripción	Aspectos a Destacar
ENFOQUE INTEGRAL Y AUNAR ESFUERZOS	○ Todas las instituciones estatales son responsables	○ 1er país de la región con el **100% de alcaldías** en línea ○ De 73 a **542** trámites y servicios en línea en 2 ½ años
ACOMPAÑAMIENTO	○ Diagnósticos y planes de acción	○ **+108%** en índice consolidado de Gobierno en línea del orden nacional en 2 años
APROPIACIÓN	○ Difusión y acompañamiento a servidores y ciudadanía	○ De 31% a **62%** en el uso de los servicios en línea ○ **114.000** servidores públicos capacitados en 2 ½ años
SOLUCIONES TRANSVERSALES	○ Soluciones basadas en estándares para la colaboración entre entidades	○ Intranet Gubernamental ○ Abordaje por el modelo de cadenas de trámites (11) ○ Marco de interoperabilidad definido para el Estado
MONITOREO Y EVALUACIÓN	○ Enfoque sistémico para evaluar el avance, uso, calidad e impacto	○ El monitoreo se realiza tanto del avance en el Estado como de la percepción de los usuarios

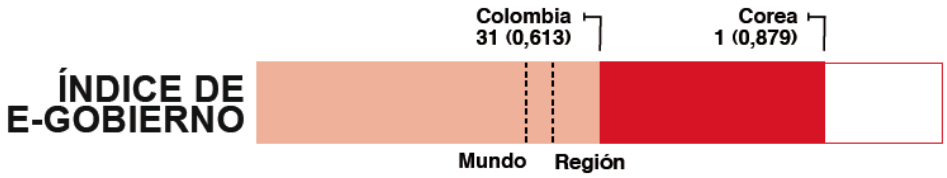
Fuente: Programa Gobierno en línea

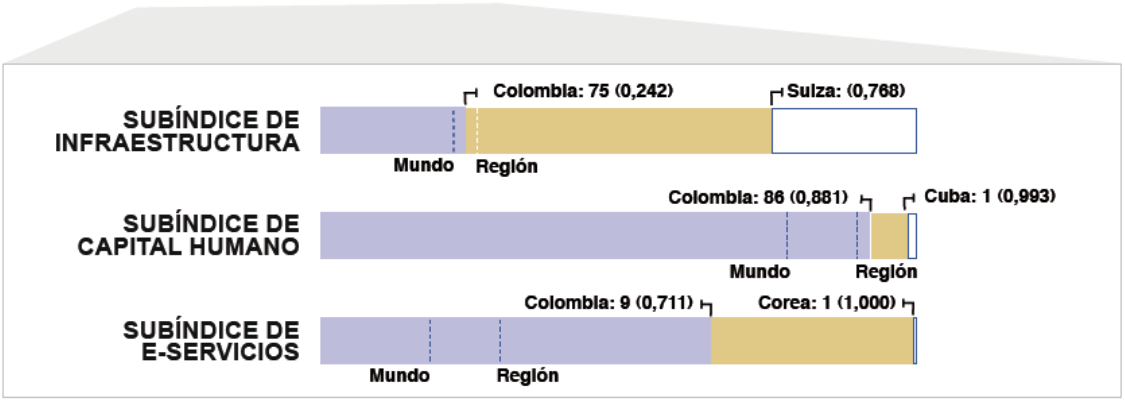
ESTADO ACTUAL

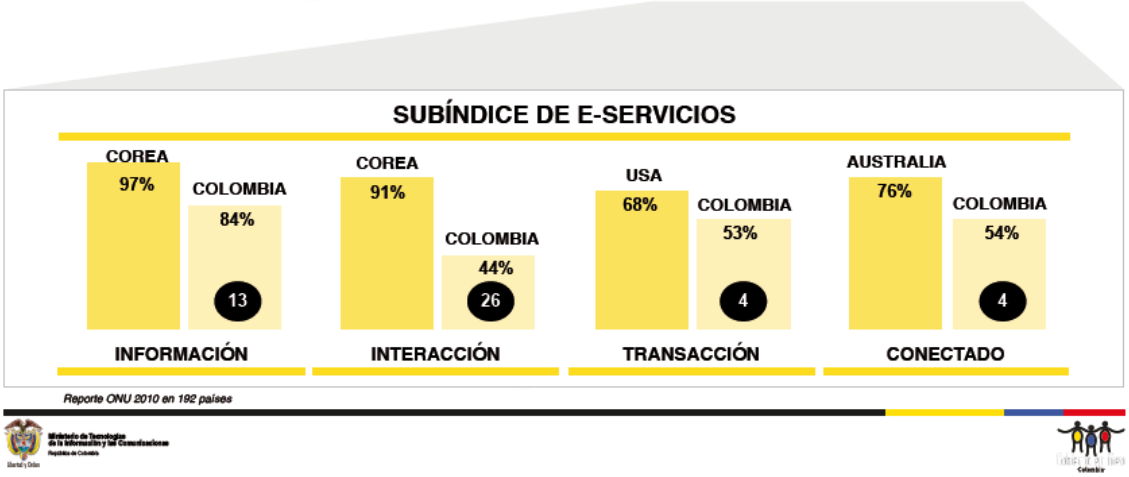


Fuente: Programa Gobierno en línea

COLOMBIA EN EL ÍNDICE MUNDIAL DE GOBIERNO ELECTRÓNICO







Reporte ONU 2010 en 192 países

ANÁLISIS DE GRUPOS DE INTERÉS

Fuente: Investigaciones de monitoreo y evaluación, Programa Gobierno en línea, 2007-201

Más allá de la oferta de Información y Trámites en Línea por parte del Estado

APERTURA

- **Apertura de datos:** Implica la oferta por parte del Estado de conjuntos de datos abiertos y reutilizables
- **Apertura de servicios:** Implica que no sólo el Estado genera servicios de valor agregado

COLABORACIÓN

- **Colaboración en políticas públicas,** toma de decisiones y resolución de problemas: implica que el Estado aprovecha la inteligencia colectiva mediante el "crowdsourcing".
- **Colaboración en servicios:** implica que terceros aprovechan los datos abiertos para producir servicios

Fuente: Investigación en visión y prospectiva, Programa Gobierno en línea y CINTEL, 2010

Un Estado construido por y para la prosperidad de los colombianos, mediante el aprovechamiento de las TIC

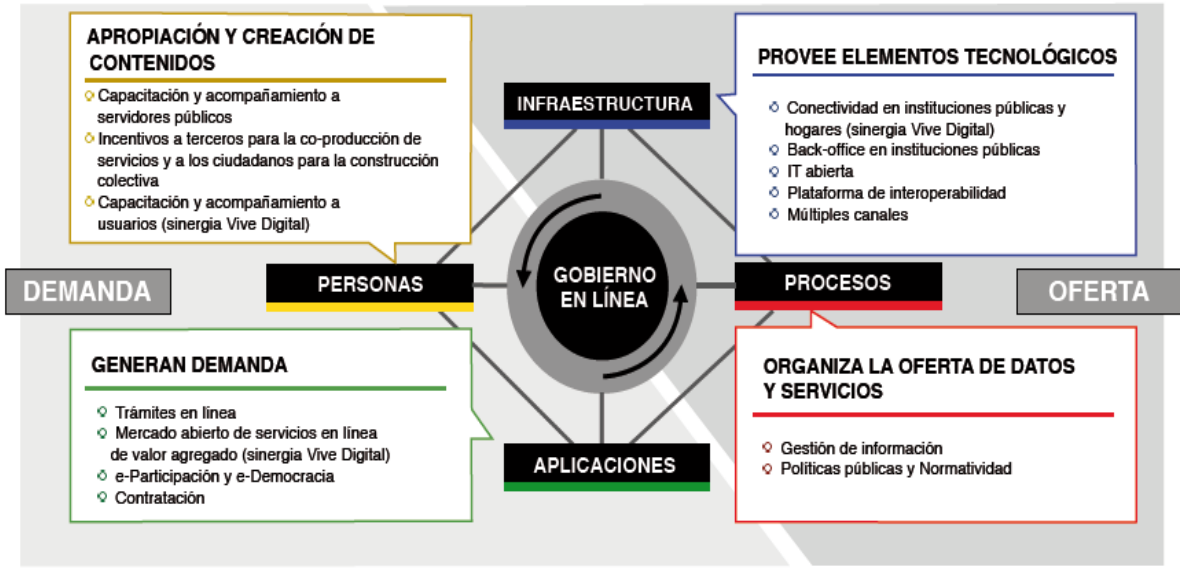
OBJETIVO GENERAL

La **Estrategia** de Gobierno en línea contribuye con la construcción de un Estado más **eficiente**, más **transparente** y **participativo** y que presta mejores servicios con la **colaboración** de toda la sociedad, mediante el aprovechamiento de las TIC. Lo anterior, con el fin de impulsar la **competitividad** y el mejoramiento de la **calidad de vida** para la **prosperidad** de todos los colombianos.

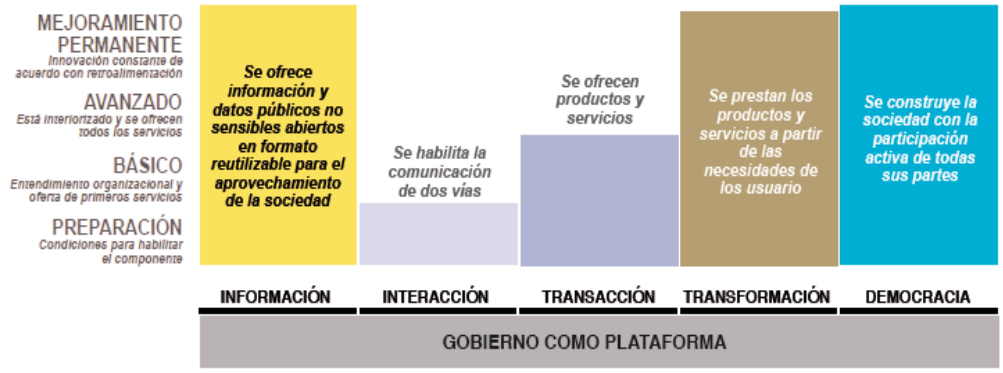
OBJETIVOS ESPECIFICOS

- Facilitar la **eficiencia** y **colaboración** en y entre las entidades del Estado, así como con la sociedad en su conjunto
- Contribuir al incremento de la **transparencia** en la gestión pública
- Promover la **participación ciudadana** haciendo uso de los medios electrónicos
- Fortalecer las condiciones para el incremento de la **competitividad** y el mejoramiento de la **calidad de vida**

ECOSISTEMA DE GOBIERNO EN LÍNEA



MODELO DE MADUREZ



ANEXO 2.

Tomado de ESTRATEGIA GOBIERNO EN LÍNEA. NIVEL NACIONAL. MINTIC

Ministerio de Tecnologías de la Información y las Comunicaciones
República de Colombia
Libertad y Orden

Gobierno en línea
Colombia

Estado actual – Nivel Nacional

Alto (81-100)
Medio (51-80)
Bajo (0-50)

Rótulos de fila	Índice 2010-2	Información	Interacción	Transacción	Transformación	Democracia
Educación Nacional	0,958	100%	100%	99%	92%	100%
Estadística	0,938	100%	100%	98%	96%	79%
Protección Social	0,921	98%	97%	94%	83%	97%
Economía Solidaria	0,898	100%	100%	100%	66%	100%
Minas y Energía	0,891	100%	97%	95%	87%	74%
Hacienda y Crédito Público	0,890	96%	93%	93%	83%	87%
Tecnologías de la Información y las Comunicaciones	0,889	96%	95%	91%	81%	89%
Agricultura y Desarrollo Rural	0,882	97%	99%	99%	74%	83%
Ciencia, Tecnología e Innovación	0,869	93%	61%	87%	89%	100%
Planeación	0,844	94%	73%	89%	81%	88%
Función Pública	0,840	94%	87%	93%	68%	90%
Seguridad	0,813	89%	100%	93%	87%	40%
Relaciones Exteriores	0,799	98%	94%	73%	79%	70%
Defensa	0,792	96%	93%	87%	64%	73%
Transporte	0,714	96%	78%	82%	60%	58%
Organismos de Control	0,693	80%	69%	81%	68%	53%
Comercio, Industria y Turismo	0,693	94%	93%	89%	74%	76%
Ambiente, Vivienda y Desarrollo Territorial	0,673	83%	75%	85%	44%	66%
Interior y Justicia	0,635	96%	71%	65%	60%	44%
Presidencia	0,607	92%	83%	79%	67%	100%
Organismos Independientes	0,574	78%	59%	81%	52%	25%
Rama Judicial	0,569	68%	68%	72%	45%	41%
Corporaciones Autónomas Regionales	0,553	90%	83%	68%	38%	27%
Organización Electoral	0,422	64%	44%	30%	43%	45%
Cultura	0,400	88%	72%	57%	35%	35%
Universidades e Institutos	0,326	51%	41%	37%	33%	12%
Rama Legislativa	0,319	58%	49%	56%	10%	10%

Fuente: Programa Gobierno en línea – Corte 31-Ene-11. Diagnóstico de 195 entidades de 27 ramas/sectores/organismos

Estado actual de apropiación de Gobierno en Línea en algunas de las entidades del Estado:

Ministerio de Tecnologías de la Información y las Comunicaciones
República de Colombia
Libertad y Orden

Gobierno en línea
Colombia

Educación
Diciembre 2010

Entidad	Fase Información	Fase Interacción	Fase Transacción	Fase Transformación	Fase Democracia
Ministerio de Educación Nacional	100%	100%	100%	91%	100%
Instituto Colombiano para la Evaluación de la Educación	100%	100%	97%	86%	100%
Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior	100%	100%	100%	82%	100%
Instituto Nacional para Ciegos	99%	100%	98%	93%	100%
Instituto Nacional para Sordos	100%	100%	100%	83%	100%

Ministerio de Tecnologías de la Información y las Comunicaciones
República de Colombia
Libertad y Orden

Gobierno en línea
Colombia

Estadística
Diciembre 2010

Entidad	Fase Información	Fase Interacción	Fase Transacción	Fase Transformación	Fase Democracia
Instituto Geográfico Agustín Codazzi	100%	100%	95%	91%	95%
Departamento Administrativo Nacional de Estadística	100%	100%	100%	100%	63%

Ministerio de Tecnologías de la Información y las Comunicaciones
República de Colombia
Libertad y Orden

Gobierno en línea
Colombia

Protección Social
Diciembre 2010

Entidad	Fase Información	Fase Interacción	Fase Transacción	Fase Transformación	Fase Democracia
Ministerio de la Protección Social	100%	94%	95%	92%	100%
Instituto Colombiano de Bienestar Familiar	98%	100%	100%	81%	80%
Instituto Nacional de Salud	100%	100%	89%	74%	79%
Instituto Nacional de Vigilancia de Medicamentos y Alimentos	100%	100%	100%	92%	100%
Servicio Nacional de Aprendizaje	98%	93%	92%	74%	90%
Superintendencia del Subsidio Familiar	100%	100%	96%	90%	100%
Superintendencia Nacional de Salud	100%	100%	100%	90%	100%
Instituto Nacional de Cancerología	92%	85%	83%	84%	100%
Caja de Previsión Social de Comunicaciones - Caprecom	100%	100%	100%	92%	100%
Fondo de Pasivo Social de Ferrocarriles Nacionales de Colombia	85%	95%	80%	57%	100%
Fondo de Previsión Social del Congreso	100%	100%	100%	80%	100%
Fondo Nacional de Estupefacientes	100%	93%	97%	76%	100%
Sanatorio de Contratación E.S.E.	99%	100%	97%	79%	100%
Sanatorio Agua de Dios E.S.E.	100%	100%	100%	90%	100%
Centro Dermatológico Federico Lleras Acosta	98%	100%	86%	90%	100%

Ministerio de Tecnologías de la Información y las Comunicaciones
República de Colombia
Libertad y Orden

Gobierno en línea
Colombia

Economía Solidaria
Diciembre 2010

Entidad	Fase Información	Fase Interacción	Fase Transacción	Fase Transformación	Fase Democracia
Departamento Administrativo Nacional de Economía Solidaria	100%	100%	100%	66%	100%

Ministerio de Tecnologías de la Información y las Comunicaciones
República de Colombia
Libertad y Orden

Gobierno en línea
Colombia

Minas y Energía
Diciembre 2010

Entidad	Fase Información	Fase Interacción	Fase Transacción	Fase Transformación	Fase Democracia
Agencia Nacional de Hidrocarburos	100%	94%	100%	84%	79%
Ecopetrol	98%	100%	88%	100%	89%
Comisión de Regulación de Energía y Gas	100%	100%	100%	100%	100%
Instituto de Geología y Mineria	100%	93%	70%	89%	65%
Instituto de Planificación y Promoción de Soluciones Energéticas	100%	100%	100%	82%	65%
Financiera Energética Nacional S.A.	100%	87%	100%	70%	56%
Ministerio de Minas y Energía	100%	100%	100%	91%	50%
Unidad de Planeación Minero Energética - UPME	100%	100%	100%	83%	84%

Ministerio de Tecnologías de la Información y las Comunicaciones
República de Colombia
Libertad y Orden

Gobierno en línea
Colombia

Hacienda y Crédito Público
Diciembre 2010

Entidad	Fase Información	Fase Interacción	Fase Transacción	Fase Transformación	Fase Democracia
Ministerio de Hacienda y Crédito Público	100%	100%	98%	91%	70%
Contaduría General de la Nación	100%	100%	100%	100%	100%
Dirección de Impuesto y Aduanas Nacionales	100%	100%	83%	100%	100%
Superintendencia Financiera	98%	100%	100%	100%	100%
Fondo de Garantías de Entidades Cooperativas - FOGACOOP	100%	100%	100%	100%	89%
Superintendencia de Economía Solidaria	95%	84%	46%	51%	50%
Unidad de Información y Análisis Financiero - UIAF	83%	88%	100%	49%	60%
Central de Inversiones S.A. - CISA	100%	80%	97%	48%	100%
Sociedad Financiera de Desarrollo Territorial S.A. - FINDETER	100%	100%	100%	92%	100%
Fondo de Garantías de Instituciones Financieras - FOGAFIN	100%	100%	100%	84%	100%
La Previsora S.A. Compañía de Seguros	84%	71%	91%	94%	78%
Fiduciaria La Previsora S.A.	92%	100%	100%	91%	100%
Positiva S.A	100%	88%	100%	73%	78%

Ministerio de Tecnologías de la Información y las Comunicaciones
República de Colombia
Libertad y Orden

Gobierno en línea
Colombia

Tecnologías de la Información y las Comunicaciones
Diciembre 2010

Entidad	Fase Información	Fase Interacción	Fase Transacción	Fase Transformación	Fase Democracia
Ministerio de Tecnologías de Información y Comunicaciones	94%	85%	81%	74%	100%
Comisión de Regulación de Comunicaciones	100%	100%	100%	100%	100%
Radio Televisión de Colombia	95%	91%	96%	53%	100%
Servicios Postales Nacionales	93%	100%	79%	100%	65%
Agencia Nacional del Espectro	99%	100%	100%	80%	80%

Ministerio de Tecnologías de la Información y las Comunicaciones
República de Colombia
Libertad y Orden

Gobierno en línea
Colombia

Agricultura y Desarrollo Rural
Diciembre 2010

Entidad	Fase Información	Fase Interacción	Fase Transacción	Fase Transformación	Fase Democracia
Ministerio de Agricultura y Desarrollo Rural	100%	100%	96%	64%	10%
Banco Agrario de Colombia	100%	100%	100%	92%	100%
Corporación Colombiana de Investigación Agropecuaria	92%	100%	100%	44%	50%
Fondo para el Financiamiento del Sector Agropecuario	98%	100%	100%	89%	100%
Instituto Colombiano Agropecuario	98%	100%	96%	59%	85%
Instituto Colombiano de Desarrollo Rural	99%	94%	100%	58%	100%
Almacenes Generales de Depósito	98%	100%	100%	100%	100%
Empresa Colombiana de Productos Veterinarios	99%	100%	100%	79%	100%
Fiduagraria	92%	100%	100%	82%	100%

Ministerio de Tecnologías de la Información y las Comunicaciones
República de Colombia
Libertad y Orden

Gobierno en línea
Colombia

Ciencia, Tecnología e Innovación
Diciembre 2010

Entidad	Fase Información	Fase Interacción	Fase Transacción	Fase Transformación	Fase Democracia
Departamento Administrativo de Ciencia, Tecnología e Innovación - Colciencias	93%	61%	87%	89%	100%

Ministerio de Tecnologías de la Información y las Comunicaciones
República de Colombia

Gobierno en línea
Colombia

Defensa
Diciembre 2010

Entidad	Fase Información	Fase Interacción	Fase Transacción	Fase Transformación	Fase Democracia
Superintendencia de Vigilancia y Seguridad Privada	86%	85%	44%	37%	50%
Caja de Retiro de las Fuerzas Militares	98%	91%	100%	73%	100%
Agencia Logística de las Fuerzas Militares	100%	100%	100%	76%	100%
Caja de Sueldos de Retiro de la Policía Nacional	100%	83%	96%	80%	89%
Defensa Civil Colombiana	99%	85%	88%	76%	70%
Instituto de Casas Fiscales del Ejército	100%	100%	100%	49%	78%
Servicio Aéreo a Territorios Nacionales	98%	90%	92%	55%	100%
Caja Promotora de Vivienda Militar y de Policía	97%	94%	86%	78%	14%
Fondo Nacional para la Defensa de la Libertad Personal	86%	94%	14%	21%	26%
Hospital Militar Central	99%	82%	73%	41%	5%
Club Militar	99%	100%	84%	73%	100%
Fondo Rotatorio de la Policía Nacional	97%	90%	38%	66%	100%
Industria Militar	100%	100%	100%	94%	100%
Ministerio de Defensa Nacional	100%	100%	96%	59%	30%
Comando General de las Fuerzas Militares	94%	81%	92%	75%	100%
Ejército Nacional	93%	100%	95%	22%	50%
Fuerza Aérea Colombiana	100%	100%	100%	74%	100%
Armada Nacional	98%	91%	87%	49%	100%
Policía Nacional	98%	100%	95%	91%	89%
Corporación de la Industria Aeronáutica Colombiana	100%	100%	100%	71%	100%
Dirección General Marítima	100%	100%	100%	91%	56%
Sociedad Hotel Tequendama	77%	72%	87%	63%	50%
Dirección General de Sanidad Militar	100%	100%	100%	43%	28%
Universidad Militar Nueva Granada	98%	100%	96%	83%	84%

Ministerio de Tecnologías de la Información y las Comunicaciones
República de Colombia

Gobierno en línea
Colombia

Interior y Justicia
Diciembre 2010

Entidad	Fase Información	Fase Interacción	Fase Transacción	Fase Transformación	Fase Democracia
Ministerio del Interior y de Justicia	99%	67%	38%	39%	25%
Dirección Nacional de Derecho de Autor	99%	74%	80%	42%	95%
Dirección Nacional de Estupefacientes	96%	67%	28%	81%	55%
Instituto Nacional Penitenciario y Carcelario	100%	100%	64%	76%	50%
Superintendencia de Notariado y Registro	95%	91%	89%	89%	58%
Imprenta Nacional de Colombia	91%	45%	83%	32%	5%
Corporación Nasa Kiwe	89%	56%	75%	63%	21%

Ministerio de Tecnologías de la Información y las Comunicaciones
República de Colombia

Gobierno en línea
Colombia

Presidencia
Diciembre 2010

Entidad	Fase Información	Fase Interacción	Fase Transacción	Fase Transformación	Fase Democracia
Accion social	85%	73%	100%	52%	100%
Departamento Administrativo de la Presidencia	76%	53%	53%	35%	10%

Ministerio de Tecnologías de la Información y las Comunicaciones
República de Colombia
Libertad y Orden

Gobierno en línea
Colombia

Universidades e Institutos
Diciembre 2010

Entidad	Fase Información	Fase Interacción	Fase Transacción	Fase Transformación	Fase Democracia
Fondo de Desarrollo para la Educación Superior - FODESEP	68%	48%	76%	45%	10%
Instituto Técnico Central	55%	30%	24%	35%	10%
Instituto Técnico Nacional de Comercio Simón Rodríguez INTENALCO	51%	30%	42%	37%	10%
Colegio Mayor de Bolívar	44%	16%	9%	26%	0%
Instituto Tolimense de Formación Técnica	56%	31%	11%	26%	60%
Instituto de Educación Técnica Profesional de Roldanillo	86%	45%	31%	42%	0%
Instituto Nacional de Formación Técnica Profesional de San Andrés y Providencia	0%	0%	12%	26%	0%
Instituto Nacional de Formación Técnica Profesional de San Juan del Cesar	0%	0%	12%	26%	0%
Instituto Tecnológico de Soledad Atlántico ITSA	47%	24%	29%	26%	0%
Universidad de Caldas	59%	29%	17%	26%	50%
Universidad de Córdoba	65%	30%	60%	26%	0%
Universidad de la Amazonía	52%	50%	54%	33%	0%
Universidad de los Llanos	56%	50%	57%	35%	0%
Universidad de Pamplona	19%	50%	28%	33%	0%
Universidad del Pacífico	39%	50%	27%	42%	0%
Universidad Nacional Abierta y a Distancia UNAD	72%	90%	61%	52%	60%
Universidad Pedagógica Nacional	91%	90%	52%	37%	0%
Universidad Surcolombiana	53%	72%	39%	32%	30%
Universidad Tecnológica de Pereira	55%	71%	55%	27%	0%
Universidad Tecnológica del Chocó Diego Luis Córdoba	44%	14%	48%	21%	0%

Ministerio de Tecnologías de la Información y las Comunicaciones
República de Colombia
Libertad y Orden

Gobierno en línea
Colombia

Rama Legislativa
Diciembre 2010

Entidad	Fase Información	Fase Interacción	Fase Transacción	Fase Transformación	Fase Democracia
Senado de la República	73%	78%	67%	16%	20%
Cámara de Representantes	42%	21%	44%	3%	0%