DESCRIPCION TECNICA SERVICIO
DE INTERCEPTACION LEGAL
DE DATOS

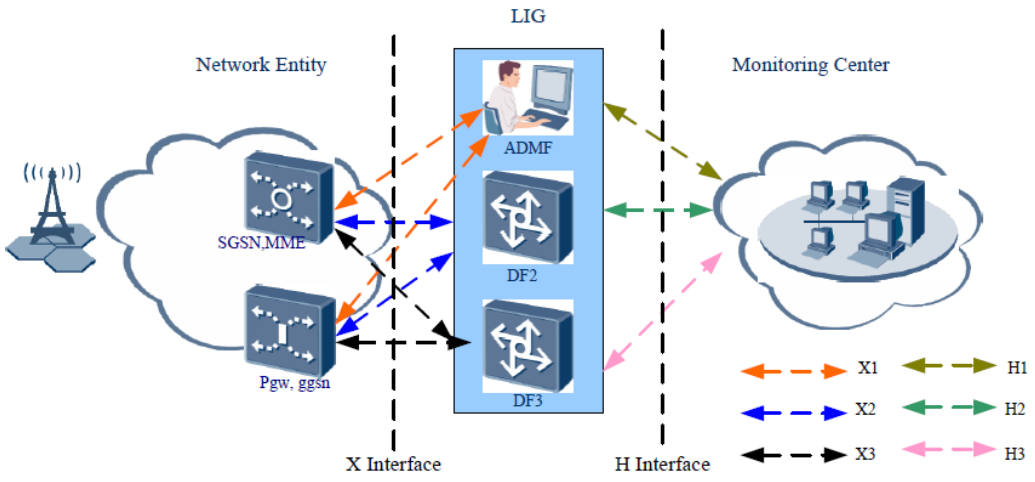
Gerencia de Ingeniería de Redes Móviles

2017

1 INTERCEPTACION DE DATOS MOVIL.

1.1 ESTÁNDAR

ETB sigue el estándar internacional ETSI para la arquitectura de implementación de la solución de interceptación legal de datos, de acuerdo con lo requerido por la fiscalía y con las normas: 3GPP TS 33 106, 3GPP TS 33 107, y 3GPP TS 33 108. La arquitectura que se sigue es:



En la arquitectura se ven tres (3) partes principales:

1. Network Entity (entidad de red) son los equipos del Core de paquetes (EPC) que soportan las interfaces con función de interceptación de datos legal como el SGSN, MME, GGSN y PGW.

2. LIG (Lawful Interception Gateway): este compuesto por tres partes: el ADMF (Administration Function) que desempeña la configuración de las funciones relacionadas con interceptación legal. El DF2 (Delivery Function) colecta y renvía la información de IRI (Intercept Related Information) y el DF3 (Delivery Function) colecta y renvía la información de media CC (Contents of Communication).

3. Centro de monitoreo: es el departamento o agencio del gobierno que ejecuta la orden para interceptación, acá se colecta la información de IRI (Intercept Related Information) y la información de media CC (Contents of Communication) desde las entidades de la red.

La interface X1: se utiliza entre el ADMF (Administration Function) y la entidad de red. Por medio de esta interface el ADMF genera gestión de las funciones de interceptación legal.
La interface X2: se utiliza entre el DF2 y la entidad de Red. El IRI (Intercept Related Information) es transferido dentro de esta interface.
La interface X3: se utiliza entre el DF3 y la entidad de red. La información de media CC (Contents of Communication) es transferida dentro de esta interface.

Los identificadores de los usuarios son el IMSI o el MSISDN para realizar el aprovisionamiento del objetivo.

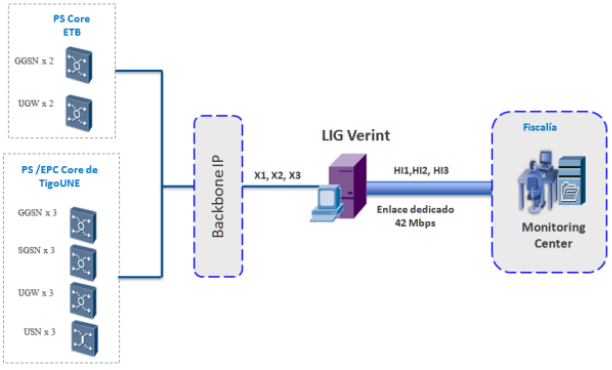
El uso de esta arquitectura permite que los elementos en la red de los operadores, NO identifiquen a cual usuario se está interceptando, ni se puede identificar o copiar la información de media o contenido de la comunicación que se está interceptando tanto en el sentido de entregan al LIG y del LIG al centro de monitoreo.

Adicionalmente una vez los equipos LIG + centro de monitoreo están operativos la interceptación queda exclusivamente a discreción del ente gubernamental competente.

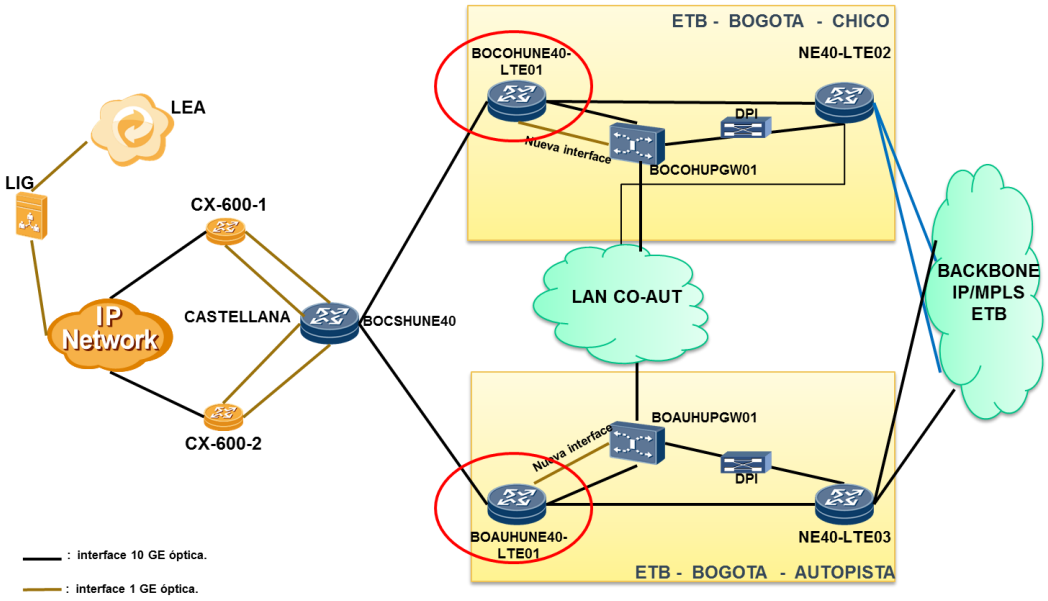
La parte administrativa y judicial de cómo se realiza la interceptación no la maneja ETB, sin embargo lo entendido con la Fiscalía en las reuniones de implementación de la solución es : la autoridad o agencia de investigación designada en un proceso, solicita a un juez de acuerdo a pruebas o por sospecha, la interceptación de determinado número, el juez emite el documento pertinente o mandato de interceptación, este documento es el soporte para que el centro de monitoreo habilite la interceptación del numero requerido, una vez que es interceptado, la copia del tráfico que entrega el LIG al centro de monitoreo, es entregada a la autoridad definida en el mandato del juez, por medio de contraseña de acceso a esa información. Como se explica en el siguiente esquema:

1.2 TOPOLOGIA IMPLEMENTADA

ETB posee dos (2) UGW9811 con funcionalidad GGSN/P-GW, la interface empleada para el aprovisionamiento del objetivo es la X1, que permite realizar interceptación legal a los usuarios de GSM, UTRAN y E-UTRAN, por medio de los SGSN/MME de TIGOUNE, siguiendo la especificación correspondiente es la 3GPP TS 33.107. El LIG es provisto por TIGOUNE marca VERINT y entrega las interface H1+H2+H3 al centro de monitoreo de la fiscalía.



ETB entrega el tráfico de la X3 al nodo castellana por medio de dos (2) subinterfaces exclusivas para este servicio y de allí se enruta al LIG. Los dos UGW están en Bogotá en dos (2) nodos diferentes.



Actualmente todas las interfaces X1, X2, X3, H1, H2 y H3 están arriba, se realizaron pruebas con aprovisionamientos manuales desde el monitoring center de la Fiscalía. A agosto se está esperando que la fiscalía automatice su monitoring center.

Abreviación	Significado
ADMF	Administration Function
CC	Contents of Communication
DF	Delivery Function
ETSI	European Telecommunications Standards Institute
EPC	Evolved Packet Core
HI	Handover Interface
IRI	Intercept Related Information
LEA	Law Enforcement Agencies
LIG	Lawful Interception Gateway
MC	Monitoring Center
IMSI	International Mobile Subscriber Identity
MSISDN	Mobile Station International Subscriber Directory Number