Recursos técnicos y logísticos para garantizar la seguridad de la red

DIRECTV cuenta con mecanismos de seguridad tanto en la red de acceso del usuario final (red 4G/LTE) como para las interconexiones con redes de datos externas, tales como las salidas a Internet.
Para la red de acceso 4G/LTE, los equipos de DIRECTV implementan la especificación técnica 3GPP 33.401 "Security architecture", que a su vez, cumple con los aspectos básicos de seguridad establecidos en las normal ITU-T X.800 "Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT" e ITU-T X.805 "Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo". Para la interconexión con redes externas, DIRECTV cuenta con equipos cortafuegos (firewall) de nueva generación, con una arquitectura distribuida carrier class de alta disponibilidad que proporcionan múltiples funciones para garantizar la protección de los datos y la seguridad de nuestros usuarios. Los recursos técnicos y logísticos para garantizar la seguridad de la red, se describen en la tabla siguiente:

Dimensión de seguridad [ITU-T X.805]	Descripción
Autenticación y control de acceso	Los equipos de acceso 4G/LTE cumplen con la especificación técnica 3GPP TS 33.102, cada transacción desde la interfaz de aire utiliza números de identificación de usuario que permiten tener trazabilidad. Al momento de la autenticación se utiliza el procedimiento EPS AKA (EPS Authentication and Key Agreement), definido en la especificación técnica 3GPP 33.401 "Security Architecture"
No repudio y protección de identidad	Para los equipos de acceso 4G/LTE, en los diferentes procedimientos de señalización, los números de identificación del usuario final, tales como: el IMSI (International Mobile Subscriber Identity), el IMEI (International Mobile Station Equipment Identity) y el IMEISV se protegen. Tanto el IMEI, el IMEISV como las llaves de usuario Ki, se almacenan de forma segura en una USIM alojada en el terminal de usuario (CPE, Customer Premises Equipment). Para la interconexión con redes externas, los firewall cuentan con perfiles de detección de anomalías y guardan logs con información representativa de las sesiones de datos
Integridad de los datos y seguridad de la comunicación	En la red de acceso 4G/LTE, se realiza protección del plano de control (CP, Control Plane) en la capa PDCP (Packet Data Control Protocol) [3GPP 36.323 "Packet Data Convergence Protocol (PDCP) specification"]. La 3GPP no define un mecanismo de integridad en plano de usuario (UP, User Plane) dado que tiene tolerancia a las pérdidas de paquetes y hay encabezados adiciones. El algoritmo de protección de integridad se configura mediante mensajes de señalización en capa RRC [3GPP 36.331 "Radio Resource Control (RRC) Protocol specification"], los nodos de acceso 4G/LTE soportan los siguientes algoritmos de cifrado: AES[1] y SNOW 3G. También se realiza protección de integridad de la señalización en capa RRC. Tanto los nodos de acceso, como los terminales de usuario (CPE, Customer Premises Equipment) soportan los algoritmos EEA0[2], 128-EEA1 y 128-EEA2 de acuerdo a la especificación técnica 3GPP TS 33.401 "Security Architecture". Para las conexiones con redes de datos externas como Internet, los Firewall cuentan con la funcionalidad prevención de intrusos (IPS, Intrusion Prevention System), que permite la detección y protección basados en inspección profunda de paquetes (DPI, Deep Packet Inspection), soporta análisis profundo de HTTP, paquetes fragmentados, análisis de aplicaciones en puerto no conocidos y detección de comportamiento anómalo de protocolos conocidos, detectando así: gusanos, troyanos, escaneo de puertos y spyware. Adicionalmente, los firewall cuentan con funcionalidad embebida de antivirus para bloquear archivos adjuntos maliciosos con malware y/o virus
Confidencialidad de datos	Se realiza cifrado en las capa PDCP (Packet Data Convergence Protocol) tanto para plano de control (CP, Control Plane) como para plano de usuario (UP, User Plane), se realiza protección de integridad en plano de control y luego se cifran tanto los datos del plano de control y de MAC-I. Para el plano de usuario se cifran las SDU (Service Data Unit) de capa PDCP
Disponibilidad	Para la red de acceso 4G/LTE, se cuenta con mecanismos de seguridad integrados: • ***Seguridad física:*** todos los equipos cuentan con puertas de seguridad y en la mayoría de los casos tienen cinturones de seguridad especiales. • ***Seguridad lógica:*** Los equipos de acceso 4G/LTE tienen una función de firewall integrada, que incluye : - *ACL (Access List Control):* Se filtran los paquetes para evitar ataques de denegación de servicio (DoS) - Interface Security Management: es una matriz de comunicación que desactiva los puertos de servicio y aprovisionamiento en caso de no cumplir los protocolos - *Seguridad de los accesos de operación y mantenimiento (OAM):* Los equipos cuentan con mecanismos de control de acceso, autenticación de usuarios, así como logs y alarmas de seguridad. Los canales de comunicaciones de OAM establecen un canal seguro entre los equipos de acceso y el sistema de gestión utilizando SSL Para la interconexión con redes externas, los firewall cuentan con funcionalidades de defensa de ataques de denegación de servicio (DDoS): El equipo permite protección ante ataques como SYN Flood, SYN-ACK Flood, FIN/RST Flood, UDP Flood, DNS query Flood, HTTP FLOOD e ICMP flood

[1] AES, Advance Encryption Standard
[2] EEA,EPS Encryption Algorithm

Nota aclaratoria: de acuerdo a lo establecido en el artículo 5.1.2.3 de la Resolución CRC 5050 de 2016 la responsabilidad a cargo de los proveedores de redes y servicios de telecomunicaciones que ofrezcan acceso a Internet no cubre los equipos del cliente, dado que los mismos son controlados directamente por el usuario del servicio, así como tampoco se cubren eventos propios proveedores de contenidos o de cualquier tipo de aplicación. Lo invitamos a seguir las recomendaciones establecidas en la sección “Recomendaciones sobre seguridad de la red”.