Recursos técnicos y logísticos para garantizar la seguridad de la red

DIRECTV COLOMBIA

DIRECTV cuenta con mecanismos de seguridad tanto en la red de acceso del usuario final como para las interconexiones con redes de datos externas, tales como las salidas a Internet. Cumple con los aspectos básicos de seguridad establecidos en las normas **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**
Control de Acceso	En el Firewall se implementan reglas de control de acceso (ACLs), permitiendo puertos específicos para la integración con la red.
No repudio y protección de identidad	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	Para las conexiones con redes de datos externas como Internet, los Firewall cuentan con la funcionalidad IPS por sus siglas en inglés (Intrusion Prevention System), que permite la detección y protección basados en inspección profunda de paquetes (DPI, Deep Packet Inspection); además soportan las siguientes funcionalidades: análisis profundo del protocolo HTTP, paquetes fragmentados , análisis de aplicaciones en puertos no conocidos y detección de comportamiento anómalo de protocolos conocidos, detectando así: gusanos, troyanos, escaneo de puertos y spyware.
Disponibilidad	Para la interconexión con redes externas, los firewall cuentan con funcionalidades de defensa de ataques de denegación de servicio (DDoS); y también los firewall permiten protección ante ataques como SYN Flood, SYN-

	ACK Flood, FIN/RST Flood, UDP Flood, DNS query Flood, HTTP FLOOD e ICMP flood
Seguridad en la transmisión de datos en los dispositivos ACCESO	Nuestros sistemas admiten la aleatorización de números de secuencia para protocolos HTTPS y TCP, fortaleciendo la seguridad en la transmisión de datos.
Gestión de contraseñas de clave secreta en los dispositivos de ACCESO	Cumplimos con los requisitos de seguridad para las contraseñas clave. Las mismas no se mostrarán ni se enviarán en texto claro, y se prohíbe la codificación rígida de estas contraseñas.
Protección de datos personales en los dispositivos de ACCESO	Todos nuestros dispositivos están en conformidad con los requisitos de la regulación del RGPD de la UE, asegurando la protección de datos personales.

Así mismo, DIRECTV en sus interacciones con empresas aliadas para prestar el servicio de acceso a internet, se apoya en la recomendación ITU-T X.805 “Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo” para aplicar estas dimensiones de seguridad en las capas de infraestructura, servicios y aplicaciones.

Nota aclaratoria: de acuerdo con lo establecido en los artículos 5.1.2.3 y artículos 2.9.2.3 (Titulo II, Capitulo 9, Sección2) 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”