SOPORTE DE SEGURIDAD LOGICA (UIT-T X.800 / X.1121) - NETSLINK

Netslink S.A.S. - Documento Oficial de Seguridad y Normativa

1. MARCO DE REFERENCIA DE LA UNION INTERNACIONAL DE TELECOMUNICACIONES (UIT-T)

Netslink S.A.S. define sus mecanismos de seguridad de red con base en las recomendaciones de la Union Internacional de Telecomunicaciones (UIT). La arquitectura X.800 describe las pautas para establecer seguridad en redes de sistemas abiertos, estructurando los servicios de seguridad en cinco categorias clave: Autenticacion, Control de Acceso, Confidencialidad de Datos, Integridad de Datos y No Repudio.

Adicionalmente, se incorporan las recomendaciones de la norma UIT-T X.1121 para la proteccion contra amenazas en redes IP, garantizando un entorno confiable para nuestros abonados.

2. MECANISMOS DE SEGURIDAD LOGICA APLICADOS

Cifrado de datos en transito: Uso obligatorio de protocolos criptograficos fuertes. Para la administracion remota de equipos Core (OLTs y switches core), se inactiva el protocolo Telnet y se fuerza el uso de SSHv2 con llaves RSA de 4096 bits.

Seguridad en la Capa de Transporte: Todo el trafico hacia el portal de clientes y de administracion viaja encriptado mediante TLS 1.3/HTTPS, impidiendo ataques de interceptacion de datos (Man-in-the-Middle).

3. SEGURIDAD EN CORE Y ACCESO DE RED GPON

A nivel de Core: Implementacion de listas de control de acceso (ACLs) estrictas en los routers de borde BGP, bloqueando trafico de entrada no solicitado hacia puertos de gestion.

A nivel de Acceso (GPON): Aislamiento de puertos de capa 2 (Port Isolation) en las ONTs del usuario para evitar que un cliente pueda interceptar el trafico de otros usuarios en la misma red de fibra. Cifrado downstream AES de 128 bits activado en la OLT para asegurar la confidencialidad de los datos opticos.

4. PROTOCOLOS DE CONTROL Y GESTION (AAA)

Para la gestion de accesos de ingenieros y personal de soporte, se implementa un servidor de autenticacion centralizado AAA (Authentication, Authorization, and Accounting) que registra cada comando ejecutado en la red.

Auditoria logica periodica: Analisis de vulnerabilidades y escaneo de puertos trimestral para detectar posibles fallas en la configuracion de los firewalls perimetrales.