UNIVERSIDAD NACIONAL DE CHIMBORAZO
FACULTAD DE INGENIERÍA
CARRERA DE TELECOMUNICACIONES

Análisis de seguridad de contenidos a través del estudio de vulnerabilidades, riesgos y mecanismos de protección para la transmisión de contenidos en sistemas de TDT, IPTV y OTT

Trabajo de Titulación para optar al título de Ingeniero/a en Telecomunicaciones

Autor:
Pazmiño Ortiz, Gabriel Alejandro.

Tutor:
Phd. Ciro Diego Radicelli García.

Riobamba, Ecuador. 2026

DECLARATORIA DE AUTORÍA

Yo, Gabriel Alejandro Pazmiño Ortiz, con cédula de ciudadanía 0604875245, autor del trabajo de investigación titulado: Análisis de seguridad de contenidos a través del estudio de vulnerabilidades, riesgos y mecanismos de protección para la transmisión de contenidos en sistemas de TDT, IPTV y OTT, certifico que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de mí exclusiva responsabilidad.

Asimismo, cedo a la Universidad Nacional de Chimborazo, en forma no exclusiva, los derechos para su uso, comunicación pública, distribución, divulgación y/o reproducción total o parcial, por medio físico o digital; en esta cesión se entiende que el cesionario no podrá obtener beneficios económicos. La posible reclamación de terceros respecto de los derechos de autor (a) de la obra referida, será de mi entera responsabilidad; librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

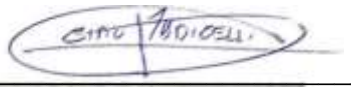
En Riobamba, 5 de Enero del 2026.

Gabriel Alejandro Pazmiño Ortiz
C.I: 0604875245

DICTAMEN FAVORABLE DEL PROFESOR TUTOR

Quien suscribe, Ciro Diego Radicelli García catedrático adscrito a la Facultad de Ingeniería, por medio del presente documento certifico haber asesorado y revisado el desarrollo del trabajo de investigación Análisis de seguridad de contenidos a través del estudio de vulnerabilidades, riesgos y mecanismos de protección para la transmisión de contenidos en sistemas de TDT, IPTV y OTT, bajo la autoría de Gabriel Alejandro Pazmiño Ortiz; por lo que se autoriza ejecutar los trámites legales para su sustentación.

Es todo cuanto informar en honor a la verdad; en Riobamba, a los cuatro días del mes de Diciembre de 2025.



PhD. Ciro Diego Radicelli García
C.I: 1713535225

CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL

Quienes suscribimos, catedráticos designados Miembros del Tribunal de Grado para la evaluación del trabajo de investigación Análisis de seguridad de contenidos a través del estudio de vulnerabilidades, riesgos y mecanismos de protección para la transmisión de contenidos en sistemas de TDT, IPTV y OTT, presentado por Gabriel Alejandro Pazmiño Ortiz, con cédula de identidad número 0604875245, bajo la tutoría de PhD. Ciro Diego Radicelli García; certificamos que recomendamos la APROBACIÓN de este con fines de titulación. Previamente se ha evaluado el trabajo de investigación y escuchada la sustentación por parte de su autor; no teniendo más nada que observar.

De conformidad a la normativa aplicable firmamos, en Riobamba 5 de Enero del 2026.

PhD. Daniel Antonio Santillan Haro.
PRESIDENTE DEL TRIBUNAL DE GRADO _____

Mgs. Alejandra del Pilar Pozo Jara.
MIEMBRO DEL TRIBUNAL DE GRADO _____

PhD. Luis Patricio Tello Oquendo.
MIEMBRO DEL TRIBUNAL DE GRADO _____

CERTIFICACIÓN

Que, **PAZMIÑO ORTIZ GABRIEL ALEJANDRO** con CC: **060487524-5**, estudiante de la Carrera de **TELECOMUNICACIONES** , Facultad de **INGENIERÍA**; ha trabajado bajo mi tutoría el trabajo de investigación titulado "**ANÁLISIS DE SEGURIDAD DE CONTENIDOS A TRAVÉS DEL ESTUDIO DE VULNERABILIDADES, RIESGOS Y MECANISMOS DE PROTECCIÓN PARA LA TRANSMISIÓN DE CONTENIDOS EN SISTEMAS DE TDT, IPTV Y OTT**", cumple con el 7% de acuerdo al reporte del sistema Anti plagio **COMPILATIO**, porcentaje aceptado de acuerdo a la reglamentación institucional, por consiguiente autorizo continuar con el proceso.

Riobamba, 15 de diciembre de 2025.

Firmado electrónicamente por:
CIRO DIEGO
RADICELLI GARCIA
Validar únicamente con FirmaEC

PhD. Ciro Diego Radicelli García
TUTOR

DEDICATORIA

Dedico este trabajo a mi familia, cuyo apoyo constante y confianza en mis capacidades han sido fundamentales para culminar este proyecto. A mis padres, por su esfuerzo incondicional y por enseñarme el valor de la perseverancia; a mis hermanos, por su compañía, respaldo y aliento en cada etapa de mi formación. Extiendo también esta dedicatoria a mis amigos más cercanos, quienes me acompañaron con su apoyo sincero en los momentos de mayor desafío y crecimiento personal. A todos ustedes, gracias por ser parte esencial de este logro académico.

AGRADECIMIENTO

Expreso mi agradecimiento a la Universidad Nacional de Chimborazo y a la Facultad de Ingeniería por brindarme la formación académica necesaria para el desarrollo de este trabajo de titulación. Mi sincero reconocimiento al tutor de tesis, cuya guía, observaciones y acompañamiento académico fueron fundamentales para orientar correctamente el proceso investigativo.

Agradezco profundamente a mi familia por su apoyo incondicional, su confianza y por ser el pilar que me ha sostenido durante toda mi formación profesional. A mis hermanos, por su compañía y aliento constante, y a mis amigos más cercanos, quienes me acompañaron con paciencia y motivación a lo largo de este camino. A todas las personas que, de una u otra manera, aportaron con sus conocimientos, sugerencias o palabras de ánimo, les extiendo mi gratitud por formar parte de la culminación de este logro académico.

ÍNDICE GENERA.

DECLARATORIA DE AUTORÍA
DICTAMEN FAVORABLE DEL PROFESOR TUTOR
CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL
CERTIFICADO ANTIPLAGIO
DEDICATORIA
AGRADECIMIENTO
ÍNDICE GENERAL.
ÍNDICE DE TABLAS.
ÍNDICE DE FIGURAS
RESUMEN
ABSTRACT
ÍNDICE GENERAL
ÍNDICE DE TABLAS
ÍNDICE DE FIGURAS
RESUMEN
ABSTRACT
CAPÍTULO I. INTRODUCCION. 15
1.1 Antecedentes. 15
1.2 Planteamiento del problema 16
1.2.1 Situación 16
1.2.2 Formulación del problema 17
1.3 Justificación 18
1.3.1 Justificación teórica 18
1.3.2 Justificación práctica. 18
1.3.3 Justificación metodológica. 19
1.4 Objetivos 19
1.4.1 Objetivo general 19
1.4.2 Objetivos específicos 19
1.5 Hipótesis 19
1.5.1 Hipótesis general. 19
1.5.2 Hipótesis especificas 20
CAPÍTULO II. MARCO TEÓRICO. 21
2.1 Estado del Arte. 21
2.2 Introducción a las tecnologías TDT, IPTV y OTT. 22
2.2.1 Televisión digital terrestre (TDT). 22
2.2.2 Televisión por protocolos de internet (IPTV) 23
2.2.3 Over the top (OTT) 24

2.3 Fundamentos técnicos de la seguridad en TDT, IPTV y OTT. 25
2.4 Marco normativo nacional e internacional 26
2.5 Comparativa entra cada tecnología 26
2.6 Análisis de brechas y problemáticas. 28
CAPÍTULO III. METODOLOGIA. 29
3.1 Enfoque de la investigación 29
3.2 Tipo y diseño de investigación. 29
3.3 Técnicas de recolección de datos. 29
3.4 Población y muestra. 30
3.5 Hipótesis 31
3.5.1 Hipótesis general 31
3.5.2 Hipótesis especificas 31
3.6 Variables y Operacionalización 31
3.7 Métodos de análisis y procesamiento de datos. 32
3.7.1 Métodos de análisis 32
3.7.2 Procesamiento de datos 32
3.8 Fases del Proyecto. 33
CAPÍTULO IV. RESULTADOS Y DISCUSIÓN 35
4.1 Resultados. 35
4.1.1 Análisis técnico de implementación de mecanismos de seguridad 35
4.1.2 Evaluación normativa frente a estándares internacionales. 41
4.1.3 Análisis de brechas de riesgos en la protección de contenidos. 47
4.1.4 Comparación transversal del cumplimiento entre TDT, IPTV y OTT 51
4.2 Discusión 52
4.2.1 Capacidad operativa y solidez tecnológica de TDT, IPTV y OTT. 52
4.2.2 Coherencia regulatoria y alineación con estándares internacionales. 53
4.2.3 Brechas estructurales y riesgos asociados a la protección de contenidos. 53
4.2.4 Relación entre factores técnicos, regulatorios y brechas de seguridad. 54
4.2.5 Síntesis interpretativa sobre el comportamiento comparado de las tres tecnologías 54
4.3 Evaluación de hipótesis 55
4.3.1 Evaluación de la hipótesis general 55
4.3.2 Evaluación de las hipótesis específicas. 55
CAPÍTULO V. CONCLUSIONES y RECOMENDACIONES 57
5.1 Conclusiones. 57
5.2 Recomendaciones 58

BIBLIOGRÁFIA 59

ÍNDICE DE TABLAS.

Tabla 1: Cuadro comparativo de características: TDT vs IPTV vs OTT..... 27
Tabla 2: Técnicas de recolección de datos. 30
Tabla 3:Operacionalización de variables 31
Tabla 4: Existencia de mecanismos de seguridad en TDT..... 35
Tabla 5: Existencia de mecanismos de seguridad en IPTV 37
Tabla 6: Existencia de mecanismos de seguridad en OTT..... 39
Tabla 7: Brechas normativas en TDT 41
Tabla 8: Brechas normativas en IPTV 43
Tabla 9: Brecha normativa de OTT 44
Tabla 10: Comparación de las brechas normativas de TDT, IPTV y OTT..... 46
Tabla 11: Nivel de cumplimiento final de mecanismos de seguridad en TDT 47
Tabla 12: Nivel de cumplimiento final de mecanismos de seguridad en IPTV 48
Tabla 13: Nivel de cumplimiento final de mecanismos de seguridad en OTT 50

ÍNDICE DE FIGURAS

Figura 1: Cadena de entrega de TDT, OTT e IPTV [24]. 23
Figura 2: Esquema de red y entrega de contenidos IPTV/VoD [27]. 24
Figura 3: Esquema de distribución de OTT [30]. 25
Figura 4: fases del trabajo de titulación 34
Figura 5: Distribución del nivel de cumplimiento de mecanismos de seguridad en TDT. 37
Figura 6: Distribución del nivel de cumplimiento de mecanismos de seguridad en IPTV. 39
Figura 7: Distribución del nivel de cumplimiento de mecanismos de seguridad en plataformas OTT. 40
Figura 8: Nivel de cumplimiento de mecanismos de seguridad en TDT 42
Figura 9: Nivel de cumplimiento de mecanismos de seguridad en IPTV 44
Figura 10: Nivel de cumplimiento de mecanismos de seguridad en OTT 45
Figura 11: Distribución proporcional de brechas en TDT, IPTV y OTT 46
Figura 12: Nivel de cumplimiento final de los mecanismos de seguridad en TDT 48
Figura 13: Nivel de cumplimiento final de los mecanismos de seguridad en IPTV 49
Figura 14: Nivel de cumplimiento final de los mecanismos de seguridad en plataformas OTT 51

RESUMEN

Palabras claves: Seguridad digital; TDT; IPTV; OTT; Protección de contenidos; DRM; Normativa tecnológica; Ciberseguridad.

El presente trabajo analiza la seguridad de contenidos en los sistemas de Televisión Digital Terrestre (TDT), Televisión por Protocolo de Internet (IPTV) y plataformas Over-The-Top (OTT) en Ecuador, mediante una investigación de enfoque documental y no experimental. El estudio se desarrolla a través de un análisis comparativo de mecanismos técnicos de protección, estándares internacionales y normativa nacional vigente, con el propósito de identificar vulnerabilidades, brechas y niveles de cumplimiento regulatorio. Para ello, se construyeron matrices de evaluación basadas en seis mecanismos esenciales de seguridad y ocho instrumentos normativos nacionales e internacionales, lo que permitió determinar el grado de alineación de cada tecnología.

Los resultados evidencian diferencias marcadas entre las tres plataformas: TDT presenta el menor nivel de seguridad debido a la ausencia de mecanismos avanzados como DRM, MFA e IDS/IPS; IPTV muestra un nivel intermedio con implementación parcial de mecanismos como CAS y cifrado; mientras que OTT registra el mayor nivel de cumplimiento gracias a la adopción directa de estándares globales de seguridad digital. Asimismo, el análisis revela brechas regulatorias significativas en Ecuador, particularmente en TDT e IPTV, asociadas a la falta de normativas específicas y procesos de fiscalización técnica.

Se concluye que la protección de contenidos en el país depende tanto de la arquitectura tecnológica como del marco regulatorio aplicable, siendo necesario fortalecer las políticas nacionales de seguridad digital para garantizar la integridad y protección de los contenidos audiovisuales.

ABSTRACT

This research analyzes the security of audiovisual content on Digital Terrestrial Television (TDT), Internet Protocol Television (IPTV), and Over-The-Top (OTT) platforms in Ecuador using a documentary, non-experimental methodological approach. The study conducts a comparative examination of essential technical protection mechanisms, international security standards, and the national regulatory framework to identify vulnerabilities, protection gaps, and levels of normative compliance. To achieve this, evaluation matrices were developed using six core security mechanisms and eight national and international regulatory instruments, allowing the assessment of security alignment across the three technologies.

The findings reveal substantial differences in the implementation of security. TDT exhibits the lowest level of protection due to the absence of advanced mechanisms such as DRM, multifactor authentication, and IDS/IPS. IPTV shows an intermediate level of adoption, with partial implementation of mechanisms such as conditional access systems and basic encryption. In contrast, OTT platforms demonstrate the highest level of compliance, resulting from direct adoption of global digital security standards. The analysis also identifies significant regulatory gaps in Ecuador, particularly affecting TDT and IPTV, which stem from the lack of specific security requirements and insufficient technical oversight.

In conclusion, the protection of audiovisual content in Ecuador is strongly influenced by both the technological architecture and the regulatory framework associated with each service. Strengthening national digital security policies is essential to guarantee the integrity and protection of transmitted content.

Keywords: Digital security; TDT; IPTV; OTT platforms; Content protection; DRM; Cybersecurity; Regulatory frameworks.

Reviewed by:

Mgs. Sofia Freire Carrillo

ENGLISH PROFESSOR

C.C. 0604257881

CAPÍTULO I. INTRODUCCION.

La convergencia tecnológica, resultado de la integración entre los sistemas analógicos y digitales conocida también como simulcast, ha redefinido de forma sustancial los procesos de producción, distribución y consumo de contenidos audiovisuales constituyéndose como un eje central para la evolución de las telecomunicaciones y medios digitales.

La combinación de la televisión digital terrestre (TDT), la televisión por protocolo de internet (IPTV) y los servicios Over-The-Top (OTT) ha generado un ecosistema en el que confluyen redes de radiodifusión, protocolos IP, y plataformas basadas en la nube que, aunque potencian la accesibilidad y diversidad de servicios, también incrementan los desafíos de seguridad y protección de contenidos, debido a la exposición simultánea de sistemas con arquitectura y normativas distintas [1], [2].

El desarrollo de tecnologías 5G, NFV (Network Function Virtualization) y computación en la nube han mejorado la eficiencia de transmisión y distribución de contenidos, pero al mismo tiempo han ampliado la superficie de ataque, aumentando los riesgos de piratería digital, robo de credenciales y accesos no autorizados [3], [4].

Organismos internacionales como la Unión Internacional de Telecomunicaciones (UIT) y el Instituto Europeo de Normas de Telecomunicaciones (ETSI) recomiendan la adopción de sistemas de gestión de derechos digitales (DRM), cifrado extremo a extremo (E2EE) y sistema de acceso condicional (CAS) para garantizar de esta manera la integridad y confidencialidad de la información [5], [6].

En Ecuador se implementan el estándar ISDB-Tb para TDT y la expansión de los servicios de IPTV y OTT evidencian la necesidad de una infraestructura de contenidos robusta, que asegure la protección de la información y de los derechos de autor.

De acuerdo al Boletín de cierre de la ARCOTEL (2023), existe un aproximado de 467.075 suscriptores a servicios audiovisuales, con una penetración del 9.75%, mientras que los servicios de OTT presentan un crecimiento sostenido impulsado por la conectividad de banda ancha [7].

Sin embargo, persisten vacíos normativos y técnicos en la implementación de medidas de seguridad, especialmente en lo relacionado con DRM, cifrado y cumplimiento regulatorio [8].

El presente trabajo tiene como finalidad analizar teóricamente las medidas de seguridad y protección de contenidos en los sistemas TDT, IPTV y OTT en el Ecuador, a partir de una revisión bibliográfica y comparativa de normas, mecanismos técnicos y regulaciones vigentes.

1.1 Antecedentes.

La televisión digital y las plataformas basadas en Internet representan la transmisión hacia un entorno comunicativo , donde los sistemas tradicionales de radiodifusión coexisten con infraestructuras IP [1].

En IPTV estudios recientes destacan la integración de inteligencia artificial para la gestión de tráfico y detección de anomalías de seguridad [9]. Sin embargo, la dependencia de protocolos abiertos como Real time Transport Protocol (RTP) o Real-time Streaming

Protocol (RTSP) expone la transmisión a ataques de denegación de servicios (DDoS) y manipulación de middleware [3].
Los servicios de OTT al operar sobre Internet público, carecen de control de red por parte del proveedor, lo que incrementa los riesgos de interceptación y vulneración de derechos digitales. Para contrarrestarlo, se utilizan protocolos de cifrado (TLS 1.3, HTTPS), autenticación (OAuth 2.0) y DRM (Widevine, PlayReady, Fair Play) [6]. No obstante, los desafíos persisten siendo de los más comunes la piratería, account sharing y exposición de claves Digital Rights Management / Gestión de Derechos Digitales (DRM) [10].
La TDT por su parte, aplica mecanismos de CAS y cifrado de transporte, basándose en las recomendaciones del estándar ISDB-Tb [11]. Sin embargo, la implementación no es uniforme en el Ecuador, lo que genera brechas en la protección del contenido transmitido.

1.2 Planteamiento del problema

1.2.1 Situación

EL crecimiento exponencial del consumo de contenidos digitales ha impulsado la expansión de plataformas digitales como es TDT, IPTV y OTT. Estas tecnologías, aunque amplían el acceso a la información, generan nuevos retos de seguridad en la transmisión, almacenamiento y distribución de los contenidos [1], [2].
En el ámbito internacional, organismos como la UIT y el Instituto Europea de Normas de Telecomunicaciones (ETSI) han desarrollado marcos técnicos y normativos orientados a garantizar la protección de los derechos de autor, la integridad de las señales y la seguridad de los datos. La recomendación UIT-T H.701 establece procedimientos de DRM y CAS como elemento esencial para la protección de los servicios de TDT e IPTV [12], mientras que la norma ETSI TS 103 829 (2020) define arquitecturas de seguridad para los servicios de difusión de nueva generación [6].
Sin embargo, la aplicación efectiva de estos estándares depende de las condiciones de cada país. En Ecuador, la Ley Orgánica de Telecomunicaciones (2015) reconoce el deber de los prestadores de servicios de telecomunicaciones de garantizar la seguridad de la información y la protección de los derechos de los usuarios [9].
A pesar de esta disposición, el país enfrenta limitaciones estructurales y técnicas para aplicar mecanismos de seguridad integral en la transmisión de contenidos. En base al Boletín estadístico de ARCOTEL (2023), el Ecuador registra un aproximado de 467.075 suscriptores a servicios de televisión por suscripción, con una penetración el 9.75%, mientras que los servicios de OTT presentan un crecimiento sostenido, impulsado por el incremento de acceso a internet de banda ancha [7].
Las cifras demuestran la magnitud del desafío, más del 50% de visitas a portales de video en el país se dirige a sitios ilegales, ubicando al Ecuador entre los tres primeros de América Latina en consumo de contenidos no autorizados [13]. Esta realidad disminuye los ingresos de la industria audiovisual, incentiva la piratería y expone a los usuarios a amenazas como el robo de credenciales, la interceptación de datos y la difusión de software malicioso [14]. Paralelamente, aunque la ley orgánica de telecomunicaciones impulsa la reforma del sector y promueve el uso eficiente del espectro radioeléctrico, persisten brechas en la implementación de mecanismos robustos de cifrado, DRM y

MFA, indispensable para alinearse con los estándares internacionales sobre derechos de autor y ciber seguridad [9].

1.2.2 Formulación del problema

El desarrollo tecnológico asociado a la TDT, IPTV y OTT ha generado una convergencia entre servicios tradicionales de radiodifusión y plataformas digitales lo que lo conocemos como un proceso de simulcast, lo que requiere alinear la normativa nacional con los estándares internacionales de seguridad.

No obstante, en el Ecuador persiste un desfase entre la regulación existentes y la implementación técnica de mecanismos de protección de contenidos, generando riesgos de vulneración de derechos de autor, pérdidas de integridad de las señales y exposición de información sensible de los usuarios [7], [9].

A nivel técnico, la falta de adopción de protocolos unificados de seguridad (como cifrado integral, MFA y gestión de claves DRM) limita la capacidad de los proveedores locales para garantizar la confidencialidad y disponibilidad de los contenidos audiovisuales.

A nivel normativo, legislación ecuatoriana no establece procedimientos específicos para la supervisión de plataformas OTT internacionales, lo cual crea una brecha jurídica respecto a los operadores nacionales regulados por ARCOTEL y MINTEL.

Esta falta de coordinación provoca inconsistencias en la aplicación de políticas de seguridad y control de acceso, especialmente en entornos de distribución de contenidos en la nube.

Como resultado, los sistemas de difusión del país en especial las plataformas de OTT emergentes presentan debilidades en la gestión de DRM, baja adopción de cifrado y limitada aplicación de políticas de autenticación. Esto vulnera la confianza del consumidor y afecta la competitividad de los servicios audiovisuales frente a los modelos internacionales.

1.2.2.1 Problema general

La ausencia de mecanismos integrales de protección de contenidos y la limitada aplicación de normativas de seguridad en los sistemas TDT, IPTV y OTT en Ecuador generan vulnerabilidades técnicas y vacíos regulatorios que comprometen la integridad, confidencialidad y disponibilidad de los contenidos audiovisuales.

1.2.2.2 Problemas específicos

- Las plataformas de transmisión audiovisuales presentan vulnerabilidades técnicas que facilitan accesos no autorizados y la piratería digital
- Los mecanismos de seguridad implementados no garantizan el cumplimiento total de las normativas internacionales sobre derechos digitales y protección de contenidos
- Las brechas regulatorias y la falta de fiscalización impiden la implementación efectiva de seguridad en los sistemas de TDT, IPTV y OTT.

1.3 Justificación

1.3.1 Justificación teórica

El presente trabajo se fundamenta en un enfoque teórico y documental, orientado a analizar de manera conceptual y comparativa la seguridad de contenidos digitales en los sistemas de TDT, IPTV y OTT.

La constante evolución tecnológica de estas plataformas exige estudios que integren perspectivas técnicas, normativas y de gestión de riesgos, sin requerir experimentación empírica, sino mediante el análisis crítico de información existente.

En el contexto ecuatoriano, la literatura académica sobre seguridad de contenidos en sistemas de transmisión audiovisual es aún limitada. Los trabajos revisados evidencian que la mayoría de estudios abordan la TDT desde su implementación técnica, dejando de lado aspectos relacionados con la protección de los contenidos y los derechos digitales.

Por tanto, esta investigación contribuye a fortalecer el marco conceptual sobre vulnerabilidades, riesgos y mecanismos de protección en entornos convergentes, articulando los aportes de autores contemporáneos y organismos especializados como la UIT y la ETSI [1], [2].

La revisión bibliográfica abarca estándares internacionales como las recomendaciones ITU-T H.701 y ETSI TS 103 829 que establecen modelos de seguridad y DRM aplicables a la IPTV y a los servicios de difusión digital [6], [15].

De igual manera, se incluyen normativas nacionales como la Ley Orgánica de Telecomunicaciones (2015) y el Plan Nacional de Telecomunicaciones y Sociedad de la Información 2020–2025, que orientan la protección de la información en Ecuador [9], [16].

En consecuencia, la justificación teórica radica en la generación de conocimiento sistemático, sustentado en la recopilación, clasificación y análisis de fuentes académicas, técnicas y normativas, que permiten comprender los fundamentos de la seguridad de contenidos digitales sin recurrir a experimentación directa.

1.3.2 Justificación práctica.

La relevancia práctica de esta investigación no reside en la implementación de pruebas o prototipos, sino en su utilidad analítica y referencial para instituciones, operadores y organismos reguladores del sector de telecomunicaciones.

El estudio ofrece un marco de referencia teórico y comparativo, a partir del cual se pueden identificar brechas tecnológicas, normativas y de gestión en la seguridad de los contenidos transmitidos por TDT, IPTV y OTT.

Al ser un trabajo de carácter documental, la información recopilada y analizada permite generar una visión integral sobre el estado actual de la seguridad audiovisual en Ecuador, basada en informes técnicos (ARCOTEL, UIT, ETSI) y estudios académicos actualizados.

De acuerdo con el Boletín de ARCOTEL (2023), el aumento sostenido del consumo de servicios OTT e IPTV demanda políticas más robustas de protección digital y control de piratería [7].

Asimismo, informes del Centro de Estudios de Telecomunicaciones de América Latina (CETLA) subrayan la necesidad de implementar mecanismos de seguridad estandarizados para reducir las pérdidas por distribución ilegal de contenidos [14].
Por tanto, la utilidad práctica de este estudio se centra en proporcionar fundamentos teóricos aplicables, que puedan servir como insumo técnico para la formulación de políticas públicas, estrategias regulatorias y futuras investigaciones empíricas, fortaleciendo la gestión de la seguridad en el ecosistema digital ecuatoriano.

1.3.3 Justificación metodológica.

Metodológicamente, la investigación se enmarca en un diseño no experimental, descriptivo y documental, sustentado en la revisión bibliográfica sistemática de fuentes secundarias.
No se recopilan datos de campo ni se ejecutan pruebas experimentales, sino que se realiza un análisis comparativo y crítico de la información proveniente de artículos científicos, documentos normativos y reportes técnicos de organismos especializados.
El proceso metodológico contempla:

1. Recolección de información a partir de bases de datos académicas (IEEE Xplore, Scopus, SSRN) y fuentes institucionales (UIT, ETSI, ARCOTEL, MINTEL).
2. Clasificación temática de la información en torno a vulnerabilidades, riesgos, mecanismos de protección y normativa aplicable.
3. Síntesis teórica y analítica, con el fin de construir un marco conceptual que relacione los aspectos técnicos y regulatorios de la seguridad de contenidos.

De esta manera, la metodología documental garantiza la coherencia entre los objetivos, la hipótesis y el desarrollo teórico del trabajo, consolidando un estudio de carácter explicativo y analítico, propio de las investigaciones de enfoque teórico.

1.4 Objetivos

1.4.1 Objetivo general

Analizar las medidas de seguridad y protección de contenidos en los sistemas de televisión digital terrestre (TDT), televisión por protocolo de internet (IPTV) y Over-The-Top (OTT) en el Ecuador.

1.4.2 Objetivos específicos.

- Analizar las vulnerabilidades y riesgos que afectan la seguridad de la transmisión de contenidos en sistema TDT, IPTV y OTT en el Ecuador.
- Analizar si los mecanismos de protección de contenidos existen en Ecuador cumplen con las normativas y estándares internacionales en materia de derechos de autor y seguridad digital.
- Analizar las regulaciones existentes en el país y como estas influyen en la seguridad de los contenidos transmitidas a través de tecnologías TDT, IPTV y OTT.

1.5 Hipótesis.

1.5.1 Hipótesis general.

Si los sistemas TDT, IPTV y OTT en Ecuador implementan mecanismos de seguridad integrales como E2EE, DRM, CAS y MFA alineados con los estándares internacionales

de seguridad digital, se reduciría significativamente el riesgo de vulnerabilidades técnicas, accesos no autorizados y pérdida de integridad de los contenidos audiovisuales.

1.5.2 Hipótesis especificas

- H1: Las vulnerabilidades presentes en los sistemas TDT, IPTV y OTT en Ecuador se deben a la limitada implementación de mecanismos técnicos de protección, como el cifrado integral y MFA.
- H2: El cumplimiento parcial de los estándares internacionales de seguridad digital y derechos de autor incide en la eficacia de los mecanismos de protección de contenidos aplicados en Ecuador.
- H3: Las brechas regulatorias y la falta de fiscalización en la aplicación de políticas de seguridad limitan la protección integral de los contenidos audiovisuales transmitidos por TDT, IPTV y OTT.

CAPÍTULO II. MARCO TEÓRICO.

2.1 Estado del Arte.

Diversos estudios han abordado los desafíos de la seguridad en plataformas digitales de transmisión de contenidos, lo que demuestra la importancia del tema en la era digital. Fernández Manzano y Gonzáles Vasco analizan cómo los modelos de negocio basados en big data y plataformas de OTT pueden comprometer la privacidad de los usuarios si no se aplica medidas regulatorias sólidas, alertando así sobre el riesgo de la recopilación excesiva de datos sin consentimiento explicito [17].

En contexto latinoamericano, un estudio realizado por CETLA evidencia que más del 60% de visualizaciones de contenido de plataformas digitales en el Ecuador se realiza a través de sitios ilegales. Esto no posiciona como país en uno de los más afectados por la piratería digital en la región, revelando así una alta exposición a riesgos como la distribución de contenidos no autorizada, pérdidas económicas para los proveedores y posibles amenazas de ciberseguridad para los usuarios [14].

Por su parte, la investigación realizada por Zeadally profundiza en las arquitecturas de IPTV y sus vulnerabilidades asociadas, identifica problemas como la ausencia de mecanismos robustos de autenticación, deficiencias en el cifrado de la señal y limitaciones en la gestión de DRM. En este estudio se destaca la necesidad de implementar soluciones de seguridad que garanticen la autenticidad y privacidad de los servicios IPTV [18].

Diversas investigaciones sobre TDT han señado que, aunque esta tecnología ofrece ventajas significativas como es el uso eficiente del espectro radioeléctrico y una alta calidad de imagen, enfrenta desafíos importantes con respecto a la cobertura, compatibilidad entre dispositivos y seguridad de la señal. De acuerdo con el Ministerio de Telecomunicaciones del Ecuador, la implementación del estándar ISDB-Tb ha sido positiva en zonas urbanas; sin embargo, persisten obstáculos técnicos y económicos para su adopción plena en sectores rurales [19].

El estudio de Martin con especto a las plataformas OTT, analiza su impacto en el mercado audiovisual español por medio del cual concluye que estas plataformas han transformado de manera radical la estructura tradicional tanto de la producción y distribución de contenidos. Así mismo presentan un desafío para regulación de derechos de autor y la fiscalización de contenidos digitales. Esta problemática agravada por la naturaleza transnacional de estas plataformas, dificulta la aplicación de normativas locales [20].

Otras investigaciones como la de Kim, Nam y Ryu abordan la disyuntiva que enfrentan los proveedores tradicionales de telecomunicaciones al tener que adaptar su infraestructura para competir con servicios emergentes OTT que utilizan el ancho de banda sin contribuir directamente a su mantenimiento. Esto plantea un conflicto tanto tecnológico como económico [15].

En el campo normativo, Copara Morocho y León Salinas proponen modelos de negocios para TDT basados en software libre, destacando la falta de integración entre el desarrollo tecnológico nacional y las exigencias internacionales en términos de protección de contenidos y derechos de autor [21].

Finalmente, la UIT han elaborado varios documentos técnicos y normativos buscando así la estandarización las prácticas de seguridad en servicios de IPTV y OTT. Entre su recomendaciones más importantes, promueven el uso de herramientas como cifrado de extremo a extremo (E2EE), la autenticación multifactor, y control de acceso basado en roles (RBAC), como se resume en el suplemento de la serie H del ITU-T [15]. En el contexto ecuatoriano, el Ministerio de Telecomunicaciones evaluó la implementación del estándar ISDB-Tb para la Televisión Digital Terrestre (TDT), destacando la importancia de reforzar los sistemas de acceso condicional y los diferentes mecanismos de cifrado, con el fin de garantizar la seguridad y protección de contenidos [19].

2.2 Introducción a las tecnologías TDT, IPTV y OTT.

2.2.1 Televisión digital terrestre (TDT).

La TDT es la evolución de la televisión analógica por lo cual esta nos ofrece mejoras en la calidad de sonido e imagen en comparación con su predecesora.

Esta permite servicios de alta definición (HD) subtítulos, múltiples pistas de audio y acceso a guías de la programación (EPG) [22]. Mediante este sistema se optimiza el uso del espectro radioeléctrico por medio de técnicas avanzadas de compresión y modulación que nos permiten las señales digitales, como son Moving Picture Experts Group 4 (MPEG-4) y Digital Video Broadcasting Terrestrial (DVD-T); estas nos permiten la transmisión de varios canales por medio de una sola frecuencia [23].

La figura 1 muestra un esquema panorámico de la cadena de distribución de contenidos audiovisuales, desde la producción hasta el consumo final en el hogar del usuario. En el gráfico se distinguen claramente las diferentes topologías de red asociadas a los sistemas de TDT, IPTV y OTT. La TDT se basa en una topología de radiodifusión punto multipunto, utilizando el espectro UHF para la difusión masiva de contenidos lineales. En contraste, IPTV y OTT emplean topologías cliente-servidor sobre redes IP de banda ancha fija, permitiendo comunicación bidireccional, interactividad y personalización del servicio. Finalmente, en el entorno doméstico, la distribución se realiza a través de redes locales en topología estrella, donde múltiples dispositivos acceden de forma simultánea a contenidos provenientes de diferentes plataformas de entrega.

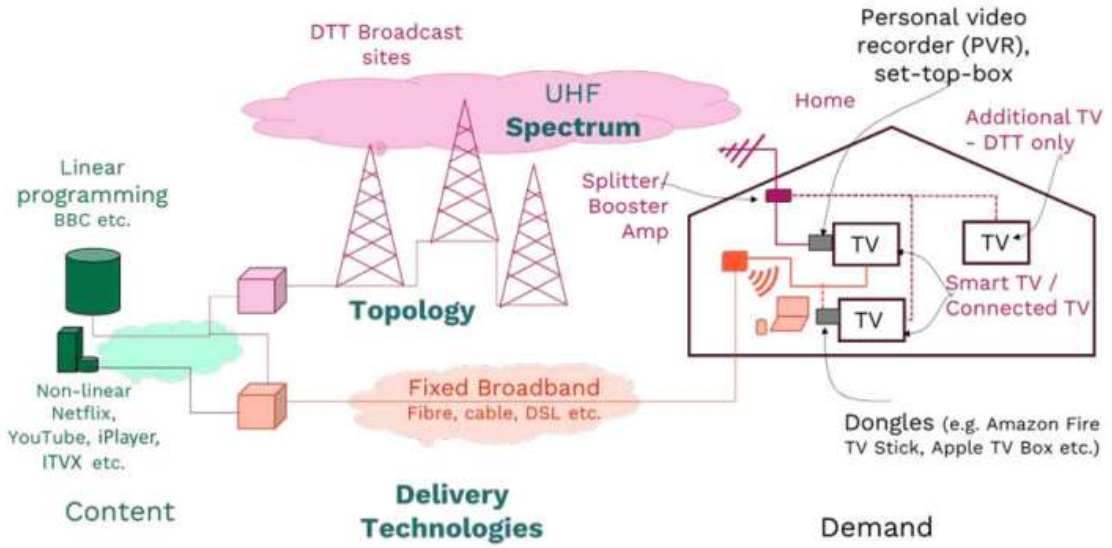


Figura 1: Cadena de entrega de TDT, OTT e IPTV [24].

2.2.2 Televisión por protocolos de internet (IPTV)

La IPTV, se la puede definir mediante la ITU-T FG IPTV (Focus Group on IPTV) y el estudio desarrollado por Patricia Sánchez como: un sistema de distribución de señales multimedia utilizando conexiones de banda ancha sobre protocolo de internet (IP). Por medio de la ITU-T FG IPTV el cual fue un grupo especializado creado por el sector de Normalización de las telecomunicaciones de la UIT con el objetivo de así establecer fundamentos técnicos, arquitecturas de referencia, requisitos de interoperabilidad y lineamientos de calidad para los servicios de IPTV. Por medio de este grupo se definió se definieron aspectos esenciales como los parámetros de calidad de servicio (QoS), calidad de experiencia (QoE), protocolos de transporte empleados en la transmisión de audio y video, así como los mecanismos de seguridad necesarios para garantizar la autenticidad, integridad y protección de contenidos. Por medio de estas recomendaciones IPTV ha podido desarrollarse sobre bases estandarizadas tanto para servicios de difusión (streaming) como para retransmisión de video, permitiendo su adopción bajo criterios técnicos unificados [25], [26], [27].

Este tipo de sistemas emplean tecnologías de compresión basados en H.265/HEVC (High Efficiency video coding), para de esta manera optimizar el ancho de banda para reducir significativamente el tamaño de los archivos de video de esta manera garantizando la calidad de transmisión en alta definición (HD) y ultra alta definición (UHD) incluso en redes con limitaciones de capacidad [28].

En la figura 2 se muestra, de forma esquemática, cómo funciona un servicio de IPTV, ilustrando la ruta que sigue la señal televisiva, desde la cabecera hasta los distintos equipos del usuario final, usando una única infraestructura IP.

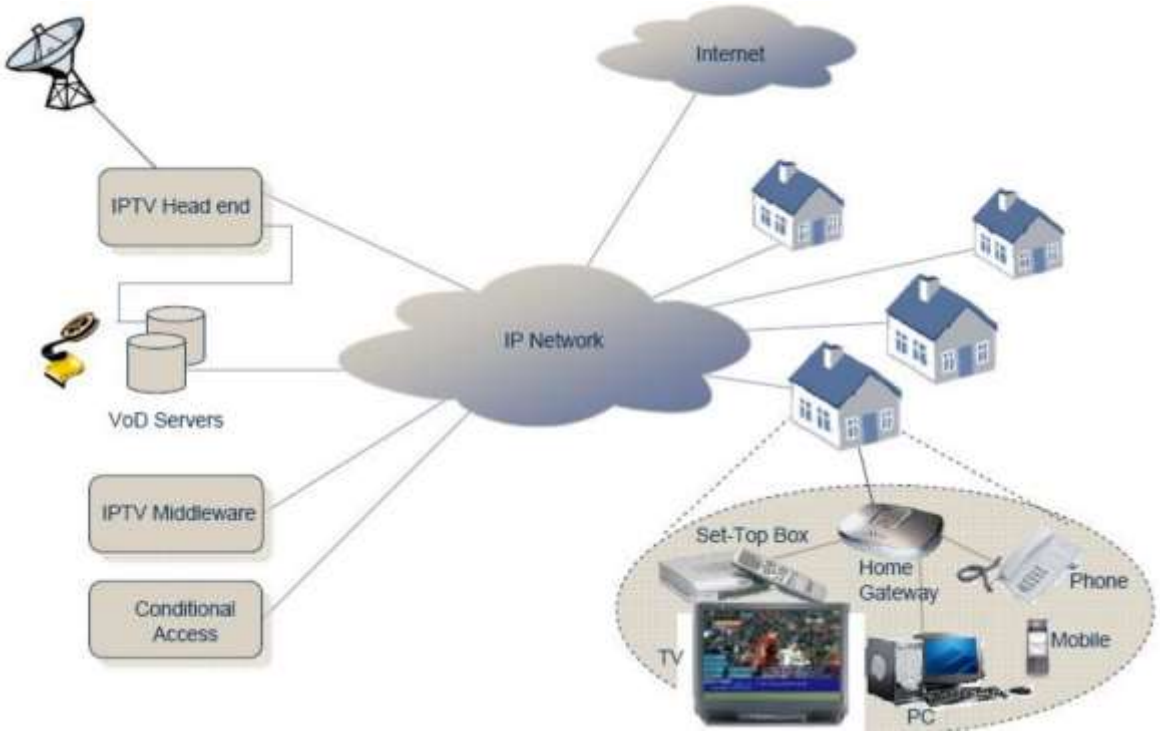


Figura 2: Esquema de red y entrega de contenidos IPTV/VoD [27].

2.2.3 Over the top (OTT)

OTT son plataformas que distribuyen contenidos multimedia, audio y servicios de comunicación directa con los usuarios finales de internet sin la intermediación de proveedores de televisión por cable o mediante satélite. Mediante estos servicios se permite el acceso a contenido bajo demanda o en tiempo real mediante dispositivos conectados a internet [20], [29].

OTT abarca diferentes categorías como Video bajo demanda (VoD), streaming de audio, mensajería instantánea y llamadas de voz sobre IP (VoIP), entre otras.

La Figura 3 muestra de manera esquemática la arquitectura de distribución de contenidos empleada por una plataforma OTT, desde el servidor principal de origen hasta los servidores de borde ubicados en estaciones remotas. En el diagrama se distinguen las diferentes topologías de red que intervienen en el proceso de entrega, iniciando con una topología centralizada en el servidor de origen, seguida de una transmisión sobre redes IP mediante un modelo cliente servidor a través de Internet y conexiones seguras tipo VPN. Posteriormente, el contenido es distribuido desde un hub de agregación mediante enlaces satelitales que responden a una topología punto multipunto, permitiendo alcanzar múltiples ubicaciones geográficamente dispersas. Finalmente, la entrega al usuario se optimiza mediante una topología distribuida basada en servidores de borde, característica de las redes de distribución de contenido (CDN), cuyo objetivo es reducir la latencia, mejorar la disponibilidad del servicio y garantizar una adecuada calidad de experiencia.

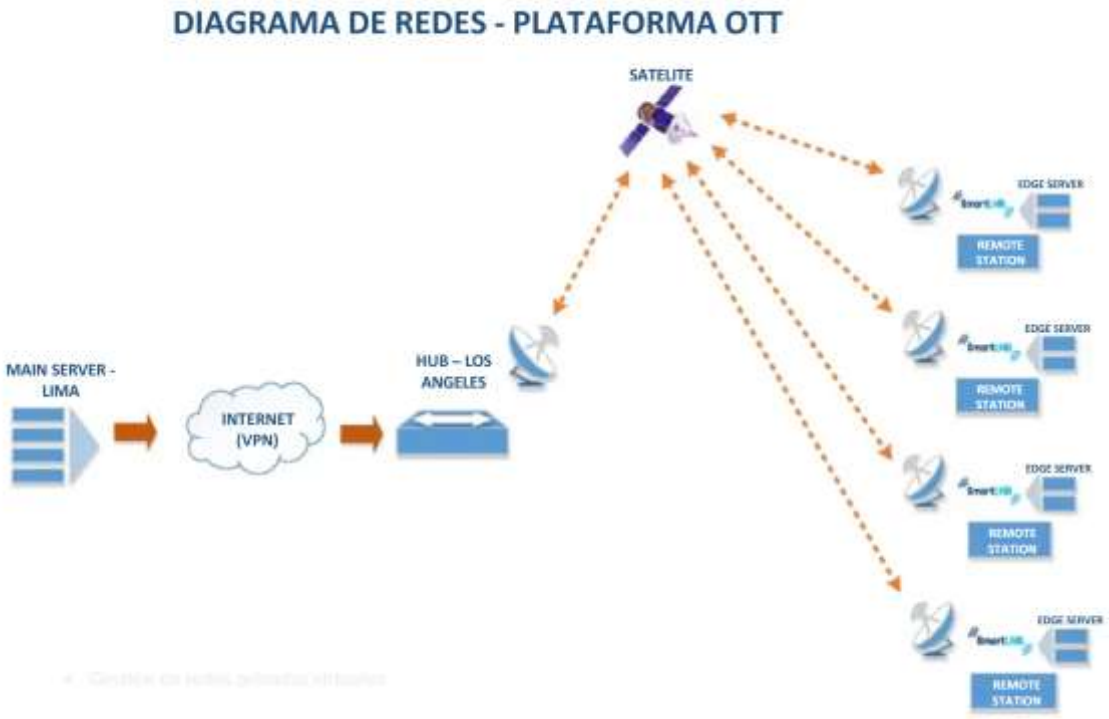


Figura 3: Esquema de distribución de OTT [30].

2.3 Fundamentos técnicos de la seguridad en TDT, IPTV y OTT.

La protección de contenidos digitales en plataformas de transmisión como TDT, IPTV y OTT exigen una infraestructura tecnológica robusta que asegure la integridad, confidencialidad y disponibilidad de la información transmitida. Para ello, es necesario implementar un conjunto de mecanismos que permitan controlar el acceso, garantizar la autenticidad de los usuarios, proteger la señal frente a ataques externos y reducir vulnerabilidades asociadas a sistemas desactualizadas. A continuación, se presentan los conceptos fundamentales que sustentan los mecanismos de seguridad involucrados:

- **DRM (Digital Rights Management):** constituye un conjunto de tecnologías diseñadas para controlar el acceso, copia y distribución de contenidos digitales. Por medio de este se puede restringir acciones como la duplicación, grabación o reenvió no autorizado de los archivos audio visuales. Este tipo de sistemas es comúnmente utilizado en plataformas de video bajo demanda como Netflix o Amazon Prime, con el fin de proteger los derechos de autor garantizando el uso legítimo del contenido audiovisual.
- **CAS (Conditional Access System):** Utilizado específicamente en transmisiones de televisión como es TDT, permite que solo los usuarios autorizados accedan a ciertos canales o servicios. Funciona como una especie de llave digital que se activa solo si el usuario cumple con ciertos requisitos, como estar suscripto al servicio.
- **E2EE (End to End Encryption):** Este hace referencia al cifrado de extremo a extremo, un mecanismo que asegura que solo el emisor y el receptor legítimos puedan leer la información transmitida. Mediante se protege las transmisiones frente a intercepciones externas.
- **MFA (Multi Factor Authentication):** Sistema de autentificación que refuerza la seguridad mediante la combinación de factores como son contraseñas, token, biométrica, etc.

Además de estos mecanismos, las normativas internacionales relacionadas con la seguridad de contenidos incorporan prácticas complementarias que fortalecen la protección integral del sistema como son:

- **IDS/IPS (Intrusion Detection and Prevention Systems):** Son sistemas destinados a monitorear el tráfico y las actividades dentro de la red con el fin de identificar, alertar e incluso bloquear comportamientos anómalos o ataques DDoS, intrusiones o manipulación de datos. Según la ETSI, forman parte esencial de la arquitectura de seguridad para servicios de difusión digital y plataformas OTT [6].
- **Políticas de actualización y parches de seguridad:** Consiste en la aplicación periódica de parches y actualizaciones en servidores, middleware, CND y aplicaciones cliente para eliminar vulnerabilidades conocidas y evitar que atacantes exploten fallos del sistema. Estándares como ISO/IEC 27001 y las guías de la ITU recomiendan este proceso como parte de la gestión continua de riesgos [31].
- **Control de acceso y filtrado geográfico (GEO-Blocking):** Mecanismo utilizado para restringir el acceso a contenidos según la ubicación geográfica del usuario o el tipo de red desde la cual se realiza la conexión. Este control es utilizado tanto para reforzar la seguridad y cumplir con acuerdos de distribución territorial, siendo reconocido por la ITU y WIPO como práctica de protección complementaria [32], [33].

Todas estas tecnologías y prácticas son esenciales para garantizar que los contenidos digitales lleguen de forma segura a los usuarios sin ser interceptados, copiados ilegalmente o modificados. Además, forman parte de los requisitos mínimos establecidos en estándares internacionales como los promovidos por el Digital Video Broadcasting (DVB), ETSI y la UIT [12], [34].

2.4 Marco normativo nacional e internacional

En el contexto ecuatoriano, las siguientes normas definen el marco jurídico aplicable:

- **Ley Orgánica de Telecomunicaciones:** Mediante este se regula el acceso, distribución y transmisión de contenidos en sistemas de telecomunicaciones [35].
- **Ley de protección de datos personales:** En esta se establece principios de tratamiento seguro y consentimiento informado para los datos de usuarios [36].
- **Norma técnica ISDB-Tb:** Se definen los requisitos técnicos para la transmisión de señales digitales terrestres [37].
- **Reglamentos de la ARCOTEL:** Mediante esta se regula los operadores y servicios audiovisuales en cuanto a licencias y uso del espectro [38].

A nivel internacional, se consideran los siguientes instrumentos normativos:

- **DMCA (Digital Millennium Copyright Act):** norma de EE. UU. que penaliza la evasión de DRM [39].
- **GDPR (General Data Protection Regulation):** Norma de la Unión Europea que regula el tratamiento de datos personales [40].
- **AVMSD (Audiovisual Media Services Directive):** Directiva de la UE que establece obligaciones para proveedores OTT e IPTV [41].
- **WCT (WIPO Copyright Treaty):** Tratado internacional de la OMPI que protege obras digitales frente a la piratería [42].

Estas normas han sido citadas por organismos como la UIT y estudios como los Martin y Copara y León, quienes señalan la urgencia de armonizar marcos nacionales con estas disposiciones globales [15], [20], [21].

2.5 Comparativa entra cada tecnología.

Conociendo los conceptos de cada tecnología, es importante definir las características de cada una. En la tabla 1, se realiza una comparativa a nivel técnico de TDT, IPTV y OTT.

Tabla 1: Cuadro comparativo de características: TDT vs IPTV vs OTT

Aspecto / Tecnología	**TDT (Televisión Digital Terrestre)**	**IPTV (Televisión sobre IP)**	**OTT (Over The Top)**
Calidad de transmisión típica	Alta calidad (HD/UHD); robusta frente a interferencias locales.	HD/UHD optimizada con códecs avanzados (H.265/HEVC).	Calidad adaptativa (ABR) dependiendo del ancho de banda disponible.
Método de distribución	Multiplexación en una frecuencia de RF (broadcast).	Unicast / multicast sobre red IP privada del operador.	Unicast sobre Internet (CDN/nube publica).
Infraestructura necesaria	Torres y repetidores terrestres; receptores ISDB-Tb o decodificadores.	Red de acceso de banda ancha y middleware del operador.	Servidores en la nube/CDN; solo conexión a Internet del usuario.
Interactividad	Limitada (EPG, botones).	Alta: VoD, time-shift, pausa, retroceso, publicidad interactiva.	Muy alta: recomendaciones, perfiles, control, multipantalla.
Compatibilidad de dispositivos	TV con sintonizador digital o set-top-box.	Smart-TV, STB IP, PC, móviles dentro de la red del operador.	Cualquier dispositivo conectado como Smart-TV, smartphone, tablets, etc.
Modelo de monetización	Gratuita y abierta: financiamiento por publicidad de canal.	Suscripción mensual, "prepago" o venta de paquetes premium.	Suscripción (SVOD), publicidad (AVOD), transacción puntual (TVOD) o híbridos.
Seguridad de protección de contenidos	Acceso condicional (CAS) y cifrado de señal para evitar piratería.	E2EE y DRM integrados; autentificación estricta de usuario.	DRM, control de acceso y técnicas de watermarking, aunque más vulnerable a piratería masiva.
Gestión de QoS / Prioridad	Garantizada por el propio canal RF	QoS controlada por el operador.	No hay QoS nativa; mejora mediante

	(clase 0 ó 1 del modelo Y.1541 según servicio).		DPI/SDN para clasificar y priorizar tráfico OTT crítico.
Dependencia de red	Cobertura y obstáculos geográficos.	Capacidad de la red IP y última milla de ISP.	Condiciones variables de la Internet publica como es la latencia o congestión.
Ventajas claves	Cobertura gratuita y universal; uso eficiente del espectro; resiliencia.	Experiencia personalizada, VoD y control de reproducción; menor piratería gracias a DRM.	Flexibilidad, portabilidad global y gran catálogo bajo demanda.
Limitaciones principales	Baja interactividad; requiere inversión en transmisión y recepción compatibles.	Limitada al alcance de la red del operador, coste de ancho de bando.	Sensible a congestión, QoS/latencia no garantizada; alta exposición a piratería.

2.6 Análisis de brechas y problemáticas.

A partir del marco técnico y normativo analizado, se puede identificar las siguientes brechas en el ámbito ecuatoriano, considerando tanto la infraestructura de seguridad como el cumplimiento regulatorio aplicable a TDT, IPTV y OTT.

- Insuficiente implementación del DRM en plataformas nacionales, especialmente en OTT locales, lo que incrementa la exposición a la copia, redistribución no autorizada y piratería de contenidos.
- Ausencia de mecanismos obligatorios de autenticación fuerte (MFA) en la mayoría de las plataformas digitales ecuatorianas, lo que facilita el acceso no autorizado mediante robo de credenciales o ataques de fuerza bruta.
- Falta de integración de sistemas IDS/IPS en redes de distribución de contenidos, limitando la capacidad de detección temprana y mitigación de ataques como intrusiones, DDOS o manipulación de flujos audiovisuales.
- Implementación incompleta o irregular de políticas de actualización y parches de seguridad específicamente en proveedores emergentes, lo que deja expuestos componentes del sistema a vulnerabilidades conocidas
- Uso limitado de controles de acceso y filtrado geográfico lo cual dificulta la redistribución territorial de contenidos y permite accesos desde regiones con actividad maliciosa o desde redes no autorizadas.
- Desfase normativo en la regulación de los servicios de OTT que no están adecuadamente cubiertos por la Ley Orgánica de Telecomunicaciones ni por los reglamentos de ARCOTEL, generando vacíos para la supervisión, requisitos de seguridad y mecanismos de fiscalización.
- Capacidad reducida de vigilancia y sanción frente a portales ilegales de distribución de contenidos lo que afecta la protección de derechos de autor y la piratería audiovisual en el país.

CAPÍTULO III. METODOLOGIA.

3.1 Enfoque de la investigación

La presente investigación adopta un enfoque metodológico documental y teórico, sustentado en el análisis y comparación de información proveniente de fuentes secundarias, tales como artículos científicos, normas internacionales, informes técnicos y legislación nacional.

No se realiza experimentación ni recolección de datos empíricos, en su lugar, se emplea un análisis analítico comparativo para así examinar la relación entre las vulnerabilidades, riesgos y mecanismos de protección de contenidos en los sistemas de TDT, IPTV y OTT.

El enfoque documental nos permite interpretar fenómenos complejos mediante la revisión sistemática de evidencia técnica y normativa, aplicando criterios de clasificación, contraste y síntesis. El objetivo no es medir variables de campo, sino evaluar conceptualmente la adopción de mecanismos de seguridad y el grado de cumplimiento de normas internacionales dentro del contexto ecuatoriano.

3.2 Tipo y diseño de investigación.

El estudio se enmarca en un diseño no experimental, debido a que no se manipulan variables ni se aplican tratamientos de dato, sino que se analiza información preexistente obtenida de fuentes técnicas, académicas y normativas.

El tipo de investigación es descriptiva y explicativa por lo que se busca caracterizar los mecanismos de seguridad empleados en los sistemas de TDT, IPTV y OTT. Explicar las brechas existentes entre la normativa ecuatoriana con respecto a los estándares internacionales.

Así mismo se clasifica como una investigación documental y comparativa, debido a que se fundamenta en el análisis sistemático de documentos técnicos, legales y académicos, cuyo contenido contrasta para evaluar el vinel de cumplimiento y adopción de mecanismos de seguridad establecidos en organismos internacionales como la UIT, ETSI e ISO/IEC.

Esta comparación se centra en tres niveles los cuales se explican a continuación:

1. Nivel técnico mediante el cual se evaluaron los seis mecanismos de seguridad definidos en el marco teórico.
2. Nivel normativo se realizaron comparaciones entre leyes y reglamentos de la legislación ecuatoriana (LOTT, Ley de protección de datos personales, reglamentos ARCOTEL) con respecto a los estándares internacionales (ITU-T H.701, ETSI TS 103 829, ISO/IEC 27001, WIPO).
3. Nivel de brechas de riesgos, donde se analizaron las principales problemáticas identificadas en el contexto ecuatoriano en función de los hallazgos técnicos y regulatorios expuestos en el capítulo II.

El diseño de investigación planteado permitió comprender la relación entre vulnerabilidad, mecanismos de protección y regulación asegurando así coherencia en el enfoque teórico del proyecto de investigación.

3.3 Técnicas de recolección de datos.

La recolección de información se realizó mediante técnicas de análisis documental orientada a identificar, seleccionar y sistematizar fuentes confiables y actualizadas

relacionadas con la seguridad de contenidos; para lo cual se emplearon las siguientes técnicas:

- Revisión bibliográfica especializada.
- Análisis normativo.
- Revisión de informes técnicos e institucionales.
- Sistematización documental.

Para sintetizar de una mejor manera las técnicas metodológicas empleadas, se presenta la siguiente tabla que vincula cada técnica con sus instrumentos y propósito dentro del marco analítico documental.

Tabla 2: Técnicas de recolección de datos.

Técnica	**Instrumento**	**Propósito**
Revisión bibliográfica especializada.	Artículos científicos indexados, fichas de lectura.	Identificar fundamentos conceptuales, vulnerabilidades y mecanismos de seguridad descritos en la literatura.
Análisis documental.	Fichas normativas, matrices comparativas.	Evaluar cumplimiento de estándares internacionales.
Revisión de informes.	Informes técnicos e institucionales.	Analizar mecanismos de protección implementados.
Sistematización documental.	Matrices de análisis, codificación proporcional (1, 0.5, 0, NEP (No Existe Evidencia Pública)).	Organizar, clasificar y comparar la información para determinar patrones y brechas.

3.4 Población y muestra.

La población del presente está constituida por un total de catorce elementos, correspondiente a seis mecanismos técnicos de protección de contenidos y ocho normativas relevantes, tanto a nivel nacional como internacional, que inciden en la seguridad de las plataformas TDT, IPTV y OTT.

La muestra fue definida por medio de muestreo no probabilístico por conveniencia, basado en la disponibilidad de información confiable, la relevancia frente al objeto de estudio y el valor comparativo frente a los estándares internacionales. La muestra concreta incluye:

Seis mecanismos técnicos de protección.

- Gestión de derecho digitales (DRM).
- Cifrado de contenido (AES, RSA, etc.).
- Autenticación multifactor (MFA).
- Sistemas de detección y prevención de intrusos (IDS/IPS).
- Políticas de actualización y parches de seguridad.
- Control de accesos y filtrado geográfico.

Ocho normativas por su aplicabilidad directa al objeto de estudio:

- **Normativa Nacional.**

- Ley orgánica de Telecomunicaciones.
- Ley de protección de dato personales.

- Noma técnica de radiodifusión de televisión digital terrestre (ISDB-Tb).
- Reglamento de servicios de valor agregado – ARCOTEL.
  - **Normativa internacional:**
- DMCA (Digital Millennium Copyrigth Act).
- GDPR (General Data Proteccion Regulation).
- AVMSD (Audiovisual Media Services Directive).
- WCT (WIPO Copyright Treaty).

Mediante esta selección, se garantizó una cobertura representativa de los principales marcos regulatorios y mecanismos técnicos que influyen en la seguridad de las plataformas digitales de transmisión de contados, considerando la disponibilidad y relevancia de la información.

3.5 Hipótesis.

3.5.1 Hipótesis general

Si los sistemas TDT, IPTV y OTT en Ecuador implementan mecanismos de seguridad integrales como E2EE, DRM, CAS y MFA alineados con los estándares internacionales de seguridad digital, se reduciría significativamente el riesgo de vulnerabilidades técnicas, accesos no autorizados y pérdida de integridad de los contenidos audiovisuales.

3.5.2 Hipótesis especificas

- H1: Las vulnerabilidades presentes en los sistemas TDT, IPTV y OTT en Ecuador se deben a la limitada implementación de mecanismos técnicos de protección, como el cifrado integral y MFA.
- H2: El cumplimiento parcial de los estándares internacionales de seguridad digital y derechos de autor incide en la eficacia de los mecanismos de protección de contenidos aplicados en Ecuador.
- H3: Las brechas regulatorias y la falta de fiscalización en la aplicación de políticas de seguridad limitan la protección integral de los contenidos audiovisuales transmitidos por TDT, IPTV y OTT.

3.6 Variables y Operacionalización.

Las variables se conciben como categorías analíticas de carácter teórico, cuyo propósito es estructurar el análisis documental y comparar la existencia o ausencia de los mecanismos de seguridad descriptos en la normativa y literatura técnica.

Tabla 3:Operacionalización de variables

Variable	**Tipo**	**Descripción operativa**	**Indicador**
Frecuencia de ataques cibernéticos.	Teórica de análisis.	Documentación de incidentes y vulnerabilidades en TDT, IPTV y OTT.	Implementación de IDS/IPS y políticas de actualización.
Uso de DRM.	Teórica de análisis.	Nivel de adopción de sistemas de DRM.	Uso de Widevine, PlayReady o FairPlay.
Eficiencia del cifrado.	Teórica de análisis.	Implementación de mecanismos de cifrado.	AES, RSA, TLS (Completo / parcial / no implementado).

Cumplimiento normativo de seguridad.	Teórica de correspondencia.	Alineación entre normativa ecuatoriana y estándares internacionales.	Evaluación transversa de los seis mecanismos.
Protección de datos y privacidad.	Teórica de correspondencia.	Medidas de control de acceso implementadas.	MFA y geo blocking presente o no.

3.7 Métodos de análisis y procesamiento de datos.

3.7.1 Métodos de análisis

Para el desarrollo de la presente investigación se emplearon tres métodos principales los cuales son analítico comparativo y deductivo. Cada uno de estos aporto una perspectiva distinta al proceso de evaluación y permitió abordar el problema de investigación desde un enfoque integral y coherente con la naturaleza documental del estudio.

En primer lugar, se aplicó el método analítico el cual permitió descomponer los seis mecanismos de seguridad identificados en el marco teórico como son DRM, CAS, cifrado E2EE, MFA, IDS/IPS y políticas de actualización y control geográfico. Este proceso facilitó la identificación de características técnicas, requisitos operativos y criterios de evaluación presentes en los estándares internacionales permitiéndonos así establecer dimensiones claras para su análisis.

Posteriormente se utilizó el método comparativo, por medio del cual se contrastaron los mecanismos y disposiciones de seguridad definidos en estándares internacionales con respecto a la normativa vigente en Ecuador. Este resulto ser un método fundamental para poder determinar brechas, convergencias y divergencias entre la legislación nacional y marcos normativos como ITU-Y H.701, ETSI TS 103 829, ISO/IEC 27001, GDPR, WIPO y la DMCA. Así mismo posibilitó comparar el nivel de adopción de dichos mecanismos en las tecnologías TDT, IPTV y OTT presentes en el país.

Finalmente se incorporó el método deductivo, que permitió interpretar los resultados obtenidos a partir de las matrices comparativas y la revisión normativa. Con este método se fundamentaron las conclusiones considerando los principios establecidos en las mejores prácticas internacionales en seguridad digital, derivando juicios sustentados sobre el nivel de cumplimiento, las debilidades estructurales y las oportunidades de mejorar dentro del contexto ecuatoriano.

El conjunto de todos estos métodos proporcionó un marco de análisis sólido y coherente, permitiendo una interpretación ordenada y sistemática de los hallazgos documentales asegurando la rigurosidad metodológica requerida para un estudio de carácter teórico.

3.7.2 Procesamiento de datos

El procesamiento de datos en esta investigación se desarrolló mediante procedimientos propios del análisis documental sistemático, orientados a organizar, clasificar y evaluar la información extraída de normas, informes técnicos y literatura científica. El objetivo

fue transformar los contenidos cualitativos obtenidos en insumos comparables que permitieran estructurar los resultados del estudio.

En primer lugar, se elaboraron matrices de análisis que permitieron organizar la información en función de los seis mecanismos de seguridad definidos en el marco teórico: DRM, CAS, cifrado E2EE, MFA, IDS/IPS y políticas de actualización y control geográfico. Para cada mecanismo se identificaron los criterios de evaluación presentes en estándares internacionales, así como su correspondencia con la normativa ecuatoriana y su presencia en los sistemas TDT, IPTV y OTT.

Posteriormente, se aplicó un proceso de codificación binaria y proporcional, asignando valores según el nivel de implementación o evidencia documental disponible. Los valores utilizados fueron:

- 1: cumplimiento o implementación total.
- 0.5: Cumplimiento parcial.
- 0: Ausencia de cumplimiento.
- NEP: No existe evidencia pública disponible.

La mencionada codificación permitió estandarizar la información proveniente de diferentes documentos y fuentes, facilitando el análisis comparativo entre tecnologías y marcos normativos.

Una vez codificados los datos, se procedió a realizar un cálculo porcentual de cumplimiento, mediante el cual se obtuvo un índice para cada mecanismo de seguridad y para cada tipo de plataforma TDT, IPTV y OTT. Estos porcentajes fueron interpretados bajo tres rangos de evaluación:

- Cumple: ≥ 75%.
- Cumplimiento parcial: 40% - 70 %.
- No cumple: < 40%.

A continuación, los valores obtenidos fueron integrados en una matriz global de correspondencia normativa, que permitió evaluar la alineación entre los estándares internacionales y las disposiciones ecuatorianas en materia de seguridad y protección de contenidos.

Finalmente, se emplearon técnicas de visualización de resultados, como gráficos de barras y mapas de calor, que facilitaron la interpretación de las comparativas inter dimensionales. Estas visualizaciones ofrecieron una perspectiva clara de las brechas, niveles de cumplimiento y patrones de adopción de mecanismos de seguridad en los sistemas analizados.

En conjunto, este procesamiento de datos posibilitó transformar información cualitativa dispersa en un conjunto ordenado, comparable y trazable, permitiendo la elaboración de un análisis robusto en el capítulo de resultados.

3.8 Fases del Proyecto.

El presente proyecto se desarrolló a lo largo de cuatro fases metodológicas fundamentales, orientadas a garantizar la coherencia entre los objetivos, las variables, la recolección de datos y los métodos de análisis. Estas fases están representadas en la figura 4 mediante un diagrama de flujo.

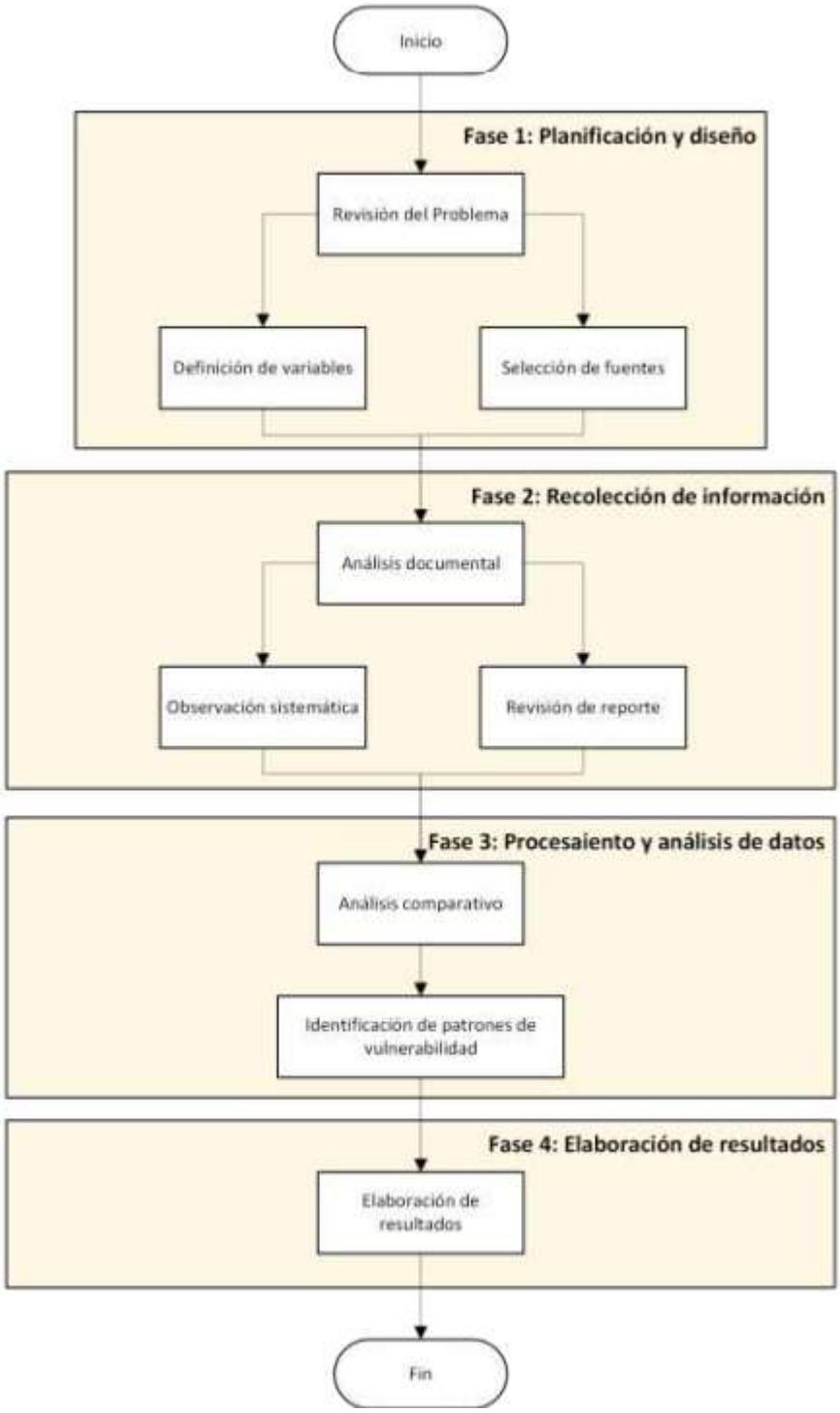


Figura 4: fases del trabajo de titulación

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

4.1 Resultados.

Los resultados se organizan en tres niveles complementarios que permiten evaluar la seguridad de contenidos en TDT, IPTV y OTT desde una perspectiva técnica y normativa. En primer lugar, se desarrolla el nivel técnico, en el cual se analiza la existencia e implementación de los seis mecanismos de seguridad definidos en el marco teórico, aplicando la codificación metodológica establecida (1, 0.5, 0 y NEP). Estos resultados se basan estrictamente en evidencia pública verificable, tal como lo exige la metodología del estudio, evitando cualquier tipo de inferencia no documentada. En segundo lugar, se presenta el nivel normativo, que compara las prácticas identificadas en Ecuador con los requisitos y recomendaciones de organismos internacionales como UIT, ETSI, ISO/IEC, AVMSD, DMCA y WIPO. Finalmente, se aborda el nivel de brechas de riesgo, que cuantifica el grado de distancia entre la situación nacional y los estándares internacionales mediante las categorías Alta, Media y Baja. Este esquema permite integrar la evidencia técnica y regulatoria para determinar el nivel real de protección de contenidos en cada tecnología.

4.1.1 Análisis técnico de implementación de mecanismos de seguridad.

En la Tabla 4 se presentan los mecanismos de seguridad identificados para TDT, junto con la evidencia pública documentada y la justificación correspondiente.

Tabla 4: Existencia de mecanismos de seguridad en TDT

MECANISMOS	Resultado	Evidencia Publica	Justificación
DRM	NEP	No existe evidencia pública en ARCOTEL, MINTEL, ni estudios técnicos.	La norma ISDB-Tb ecuatoriana no menciona DRM.
CAS	1	Sí existe evidencia técnica en estudios de TDT Ecuador.	El CAS aparece descrito en trabajos técnicos sobre ISDB-Tb.
Cifrado	0.5	Evidencia parcial (cifrado dentro del CAS).	No documentado oficialmente en normativas de ARCOTEL.
MFA	NEP	No hay mención en normativa o estudios.	No existe MFA en receptores TDT en Ecuador.
IDS/IPS	NEP	Ningún documento oficial lo menciona.	No hay despliegue documentado.
Parches / Actualizaciones	NEP	No existe política pública documentada.	No descrito en la norma ISDB-Tb.

Geo-Blocking	0	No aplicable por naturaleza RF.	La TDT usa UHF/VHF, no IP por ende no existe geobloqueo.

Los resultados de TDT en Ecuador presentan un nivel limitado de adopción de mecanismos avanzados de seguridad. En base a la revisión documental, no existe evidencia pública sobre el uso de DRM en la implementación nacional del estándar ISDB-Tb [16], [43], [44]. Ni en la norma de la ARCOTEL, resoluciones técnicas del MINTEL y estudios académicos publicados mencionan la presencia de DRM. Esto coincide con la literatura internacional, donde se señala que ISDB-Tb emplea CAS pero no DRM avanzado [43].

Por esta razón el mecanismo de DRM se lo ha codificado como NEP.

En cuanto al CAS, sí se identificó evidencia real sobre su uso en implementación ecuatorianas. Estudios técnicos sobre ISDB-Tb verifican la existencia de mecanismos CAS aplicados a la señal digital terrestre [45]. Debido a esto se le asigno el valor de 1, el cual nos indica la implementación total.

Respecto al cifrado, si bien ISDB-Tb permite el cifrado como parte de CAS, no existe documentación oficial que confirme la presencia de cifrado robusto (AES, RSA) en la infraestructura TDT ecuatoriana. Sin embargo, los estudios técnicos revisados sugieren el uso de cifrado interno del CAS en implementaciones ISDB-Tb en Ecuador [45], [46]. Mas no un cifrado de transmisión independiente, por ende, se le asigno un valor de 0.5 lo cual equivale a una implementación parcial.

En el caso de MFA no se encontró ninguna referencia normativa, técnica o académica que la mencione, lo cual es coherente con la naturaleza abierta de la radiodifusión. Por ello, el mecanismo se clasificó como NEP.

Asimismo, no se halló evidencia de mecanismos IDS/IP aplicados a la red de transmisión TDT. Estos sistemas suelen implementarse en infraestructuras IP, no en redes basadas en UHF/VHF. La ausencia de documentación oficial justifica su clasificación como NEP.

Del mismo modo, tampoco existe evidencia de políticas de actualización o parches de seguridad aplicados a la infraestructura TDT, ya que la norma ISDB-Tb no contempla este tipo de mantenimiento a nivel de software. Este mecanismo también fue calificado como NEP.

Finalmente, el geo-blocking recibió una valoración de 0, ya que, por su naturaleza de difusión en espectro radioeléctrico, la TDT no admite restricciones territoriales mediante

software. La cobertura está definida por la potencia de transmisión y no por mecanismos de filtrado geográfico.

Figura 5: Distribución del nivel de cumplimiento de mecanismos de seguridad en TDT.

La Figura 5 representa de manera visual la proporción de implementación de los mecanismos de seguridad evaluados en TDT. Se observa una marcada concentración de valores en "0" y "NEP", lo que confirma la ausencia de mecanismos avanzados como DRM, MFA, IDS/IPS, parches de seguridad y geo-blocking. El único mecanismo plenamente implementado es CAS, mientras que el cifrado aparece parcialmente representado con un valor intermedio, coherente con la evidencia limitada disponible. En conjunto, el gráfico evidencia un nivel de seguridad bajo y dependiente casi exclusivamente del CAS integrado en el estándar ISDB-Tb.

En la Tabla 5 se presentan las brechas normativas identificadas para IPTV, basadas en la comparación entre la evidencia ecuatoriana y los estándares internacionales.

Tabla 5: Existencia de mecanismos de seguridad en IPTV

MECANISMOS	**Resultado**	**Evidencia Publica**	**Justificación**
DRM	0.5	Evidencia global, no local.	No hay documentación de operadores ecuatorianos.
CAS	1	Evidencia ecuatoriana real.	Tesis ESPOL confirma uso por operadores.
Cifrado	0.5	Evidencia parcial.	Confirmado globalmente, no localmente.
MFA	NEP	No existe evidencia.	Ningún operador ecuatoriano publica uso.
IDS/IPS	NEP	No existe evidencia.	No documentado públicamente.
Parches / Actualizaciones	0.5	Evidencia global, no local.	Se documenta en OTT pero no en IPTV Ecuador.

Geo-Blocking	NEP	No existen documentos.	No documentado en Ecuador.

IPTV muestran un nivel de implementación superior al de TDT, aunque con limitaciones derivadas de la ausencia de evidencia pública disponible sobre ciertos mecanismos en los operadores ecuatorianos, según los criterios establecidos en la metodología

En primer lugar, el mecanismo DRM presenta un valor de 0.5, debido a que existe evidencia global ampliamente verificable del uso de sistemas como Widevine o PlayReady [47], [48]; sin embargo no se encontró documentación oficial que confirme su adopción en operadores IPTV del Ecuador. Por lo tanto, se asignó una implementación parcial, sustentada únicamente en evidencia internacional.

El mecanismo CAS obtuvo valoración 1, ya que existe evidencia ecuatoriana concreta documentada en trabajos académicos del país que confirman la utilización de sistemas como Nagravisión y Conax por operadores de TV pagada sobre infraestructura IP [47], [48].

Para el cifrado, se asignó un valor de 0.5, ya que, aunque los sistemas IPTV a nivel internacional utilizan cifrado mediante AES/TLS, no existe confirmación explícita sobre la presencia de estos mecanismos en operadores ecuatorianos. Esta calificación representa la falta de evidencia local, aunque existe documentación global sólida.

En el caso de la autenticación MFA, el resultado fue NEP, pues ningún operador ecuatoriano publica información relativa a la implementación de este mecanismo, ni existe evidencia en informes técnicos o normativos [15].

Asimismo, el mecanismo IDS/IPS también fue clasificado como NEP, debido a la ausencia de reportes públicos que confirmen su despliegue en las redes IPTV ecuatorianas.

En cuanto a parches y actualizaciones, se asignó un valor de 0.5. La evidencia global indica que plataformas IPTV incorporan procesos de mantenimiento continuo, pero no existe documentación específica en Ecuador sobre estas prácticas.

Finalmente, el geo-blocking fue clasificado como NEP, ya que no se hallaron documentos que confirmen su utilización por proveedores IPTV en Ecuador, aun cuando su uso es común en otros países para licencias de contenido.

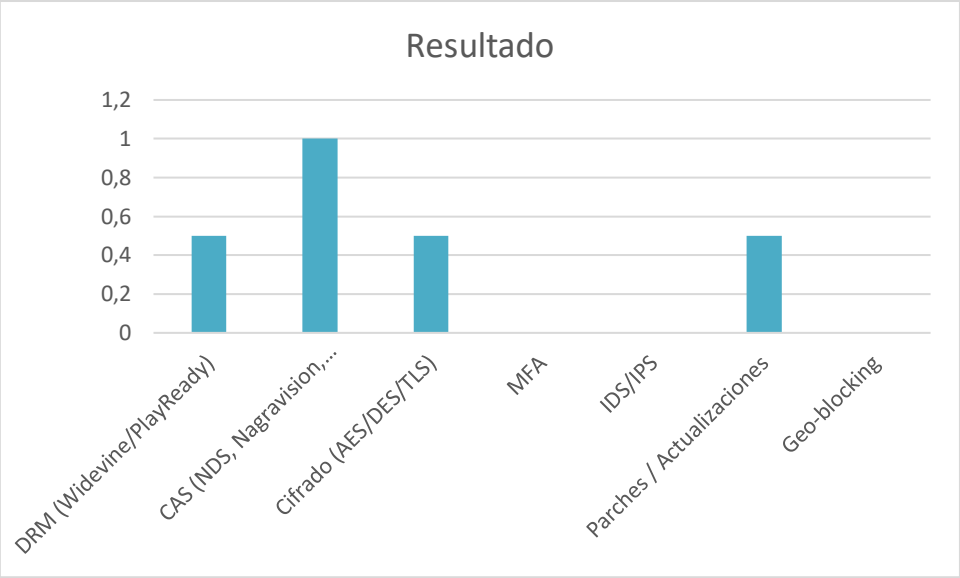


Figura 6: Distribución del nivel de cumplimiento de mecanismos de seguridad en IPTV.

La Figura 6 muestra un panorama más equilibrado en comparación con TDT. En el gráfico se aprecia que IPTV presenta valores altos en mecanismos como CAS, mientras que DRM, cifrado y parches se ubican en niveles intermedios (0.5), reflejando evidencia internacional pero no local. Los mecanismos MFA, IDS/IPS y geo-blocking se mantienen en categoría NEP, debido a la ausencia de documentación verificable que confirme su adopción. Visualmente, la figura demuestra un nivel de implementación mayor al de TDT, pero aún insuficiente para cumplir los estándares internacionales.

En la Tabla 6 se presentan las brechas normativas identificadas para OTT, donde se evidencia un alto grado de alineación internacional.

Tabla 6: Existencia de mecanismos de seguridad en OTT

Mecanismos	**Resultado**	**Evidencia Publica**	**Justificación**
DRM (Widevine, PlayReady, FairPlay)	1	Evidencia directa y verificable	OTT global implementa DRM universalmente
Cifrado (TLS/HTTPS + AES)	1	Evidencia directa (Netflix Tech Blog)	TLS más cifrado de contenido
MFA	0.5	Evidencia parcial	Amazon tiene MFA; Netflix no para usuarios
IDS/IPS / Anti-DDoS	1	Evidencia directa (Akamai)	OTT global usa mitigación avanzada DDoS
Parches / Actualizaciones	1	Evidencia directa	Actualización continua (CI/CD)
Geo-Blocking	1	Evidencia directa (WIPO)	Geo-blocking requerido por licencias territoriales

Las plataformas OTT presentan el mayor nivel de implementación de mecanismos de seguridad entre las tres tecnologías analizadas, debido a que operan mediante infraestructura global y estándares internacionales de protección de contenido.
El mecanismo DRM recibió un valor de 1, sustentado en evidencia directa de la implementación de sistemas como Widevine, PlayReady y FairPlay en servicios como Netflix, Disney+ y Amazon Prime [47], [48], [49]. La documentación oficial disponible confirma un cumplimiento total a nivel global.
En cuanto al cifrado, se asignó también un valor de 1, respaldado por la evidencia técnica expuesta en el Netflix Tech Blog y otros reportes oficiales que detallan el uso de TLS/HTTPS combinado con cifrado AES para proteger el contenido en tránsito [50].
Respecto a la autenticación MFA, la evidencia fue parcial. Algunas plataformas como Amazon Prime Video implementan MFA [51], mientras que Netflix no lo ofrece de forma obligatoria para cuentas de usuario. Por esta razón, el mecanismo recibió un valor de 0.5.
Para IDS/IPS, la evidencia es contundente. Proveedores de CDN como Akamai documentan el uso de mitigación avanzada contra ataques DDoS y mecanismos de seguridad distribuidos, por lo cual este mecanismo recibió una valoración de 1.
En el caso de los parches y actualizaciones, la evidencia también es completa. Plataformas OTT operan bajo modelos de despliegue continuo (CI/CD), como lo describe oficialmente Netflix [52] , justificando el valor 1.
Finalmente, el mecanismo de geo-blocking fue clasificado con 1, puesto que las plataformas OTT aplican restricciones de contenido basadas en territorios debido a licencias internacionales, tal como se evidencia en documentos de WIPO [42].

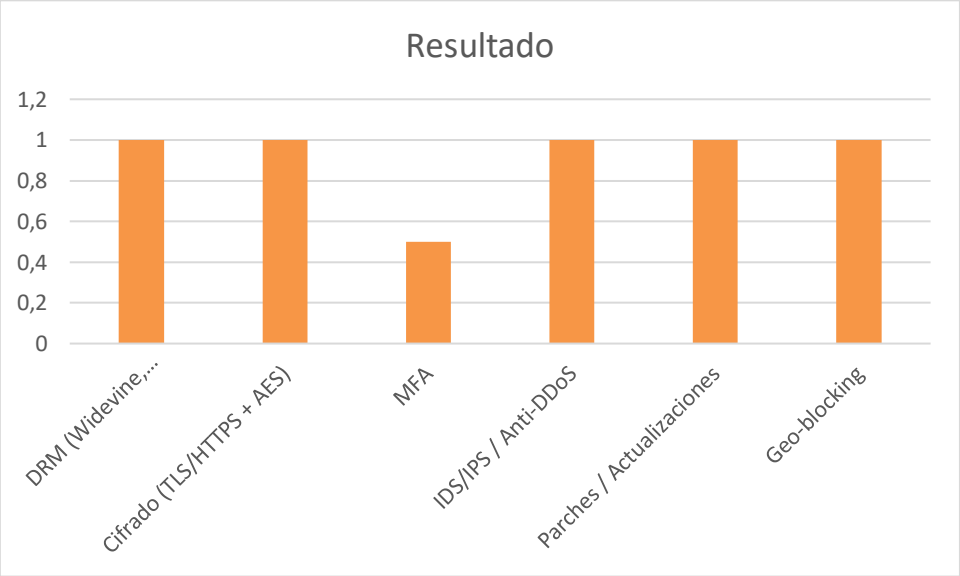


Figura 7: Distribución del nivel de cumplimiento de mecanismos de seguridad en plataformas OTT.

La Figura 7 evidencia un alto nivel de adopción de mecanismos de seguridad en plataformas OTT. Todos los controles evaluados DRM, cifrado, IDS/IPS, parches y geo-blocking alcanzan un valor de cumplimiento total (1), con excepción de MFA, que se representa por un valor intermedio (0.5) debido a su implementación parcial entre proveedores globales. El gráfico confirma visualmente que OTT presenta la infraestructura de seguridad más robusta entre las tres tecnologías evaluadas, alineándose casi completamente con los estándares internacionales.

4.1.2 Evaluación normativa frente a estándares internacionales.

En la Tabla 7 se presentan las brechas normativas de TDT, comparando su situación actual frente a estándares emitidos por UIT, ETSI, ISO/IEC y organismos internacionales.

Tabla 7: Brechas normativas en TDT

Mecanismo	Estándar internacional	Situación en Ecuador	Brecha	Justificación
DRM	UIT-R, ITU-T H.701 recomienda DRM.	NEP.	Alta	Ecuador no regula ni implementa DRM en TDT pública.
CAS	UIT, ISDB-Tb recomienda el uso de CAS.	Implementación parcial.	Media	Existe CAS en estudios, pero no se encuentra normado por la ARCOTEL.
Cifrado	UIT y ETSI recomiendan cifrado TS.	Evidencia parcial (Solo existe CAS).	Media	Existe cifrado a nivel técnico, no en normativa oficial.
MFA	ETSI e ISI/IEC recomiendan autenticación fuerte.	NEP.	Alta	Ninguna evidencia de MFA en TDT ecuatoriana.
IDS/IPS	ETSI TS 103829 exige monitoreo.	NEP.	Alta	No existe evidencia de IDS/IPS en la red de TDT ecuatoriana.
Parches / Actualizaciones	ISO/IEC 27001 exige gestión de parches.	NEP.	Alta	No hay política pública ni documentos técnicos.
Geo-blocking	WIPO/OMPI lo reconoce como control.	No aplica (TDT terrestre RF).	Media	No aplica por su naturaleza, pero es una brecha de control lógico.

En este apartado se presentan los resultados del análisis comparativo entre los mecanismos de seguridad recomendados por los estándares y normativa internacionales como es la UIT, ETSI, ISO/IEC, AVMSD, DMCA y WIPO. La situación regulatoria y técnica reportan en Ecuador para las tecnologías de TDT, IPTV y OTT. Las brechas se determinan mediante una matriz aplicando las categorías definidas en la metodología de Alta, Media y Baja; según el grado de cumplimiento o ausencia de evidencia pública.

Los resultados evidencian que la TDT ecuatoriana posee las brechas más significativas entre todas las tecnologías analizadas. La ausencia de DRM constituye una brecha Alta, dado que tanto por la UIT como la recomendación ITU-T H.701 establecen que DRM es un mecanismo esencial para la protección de contenidos multimedia [43]. La normativa nacional (ISDB-Tb) no incluye la disposiciones relacionadas con DRM, ni se encontraron referencias en la ARCOTEL o MINTEL.

Respecto al CAS, se identificó un cumplimiento parcial representado así como una brecha Media, debido a que estudios técnicos confirman su aplicación en implementaciones TDT ecuatorianas [53]; sin embargo la ARCOTEL no lo regula explícitamente.

En relación con el cifrado, la UIT y ETSI recomiendan cifrado robustos en transmisiones digitales [15], [44]. No obstante en Ecuador solo existe evidencia parcial derivada de CAS, sin documentación oficial que confirme cifrado independiente o avanzado, lo que resulta en una brecha Media.

Los mecanismos de MFA, IDS/IPS y parches de seguridad presentan brechas Altas, debido a que organismos como la ITSI e ISO/IEC (ISO/IEC 27001) recomiendan autenticación fuerte, monitoreo continuo y gestión de actualizaciones [31], [44]; sin embargo, no existe evidencia publica de que estos mecanismos estén implementados en TDT.

Finalmente, el geo-blocking genera brecha Media, ya que aunque no aplica por la naturaleza de RF (difusión abierta), estándares como WIPO reconocen el control geográfico como mecanismos de protección cuando la tecnología lo permite [42]. Su ausencia constituye una brecha lógica, aunque no técnica.

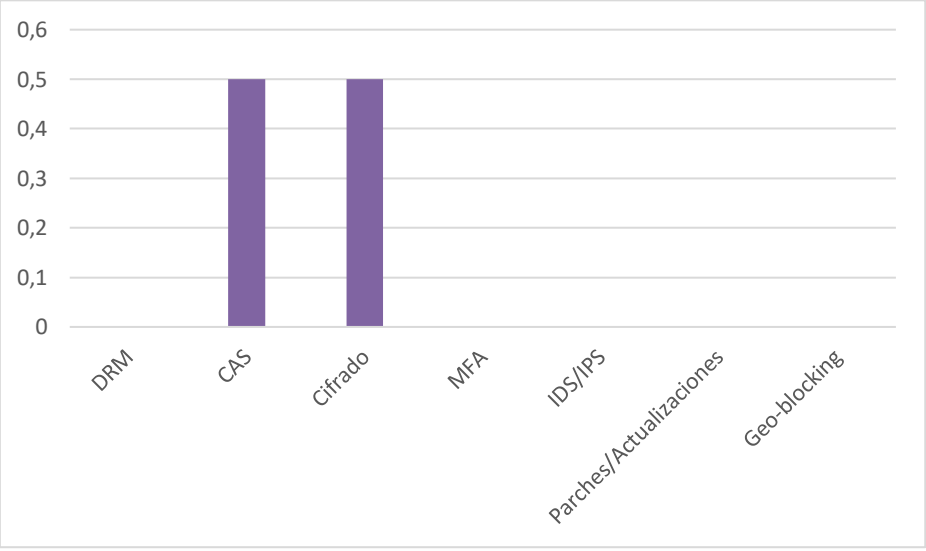


Figura 8: Nivel de cumplimiento de mecanismos de seguridad en TDT

La Figura 8 muestra el predominio de brechas Altas, lo que confirma el rezago significativo de TDT respecto a estándares internacionales. Las brechas Medias reflejan mecanismos parcialmente implementados, pero sin regulación que los formalice.

En la Tabla 8 se presentan las brechas normativas en IPTV, contemplando su correspondencia con marcos internacionales de seguridad digital.

Tabla 8: Brechas normativas en IPTV

Mecanismos	Estándar Internacional	Situación del Ecuador	Brecha	Justificación
DRM (Widevine/PlayReady)	Recomendado por UIT, ETSI AVMSD.	Nep local (solo existe evidencia global).	Media – Alta	No existe evidencia pública de uso local.
CAS	Requisito en DVB/ETSI.	Si (NDS / Nagravision / Conxx).	Baja	Confirmado en operadores ecuatorianos.
Cifrado	AES/TLS .recomendado por UIT/ETSI.	Solo global.	Media	No está documentado por operadores ecuatorianos.
MFA	ISO/IEC 27001 exige MFA.	NEP.	Alta	No existe evidencia pública.
IDS/IPS	ETSI TS 103 829.	NEP	Alta	No hay evidencia en operadores ecuatorianos.
Parches	ISO/IEC 27001 exige actualización.	NEP local, si global.	Media	OTT si, IPTV Ecuador no documenta.
Geo-blocking	Recomendado por WIPO/DMCA.	NEP.	Alta	No existe evidencia en Ecuador.

Las brechas normativas en IPTV son menores que las encontradas en TDT, pero aun significativas. En lo referente a DRM, los estándares internacionales (ITU-T H.701, ETSI TS 103 829 y la AVMSD europea) recomiendan su implementación obligatoria en servicios audiovisuales [15], [47], [48]. Sin embargo, no existe evidencia publica de su uso por operadores ecuatorianos, lo que nos genera una brecha Media – Alta.

EL mecanismo CAS constituye la brecha más baja, debido a que estudios académicos confirman el uso de sistemas como Nagravisión y Conax por proveedores ecuatorianos [54].

En cuanto al cifrado , aunque UIT y ETSI establecen el uso de AES/TLS como requisito de seguridad en redes IP [43], [55]; no se encontró evidencia local, solo global lo cual genera una brecha Media.

La usencia de MFA presenta una brecha Alta, ya que la ISO/OEC 27001 exige autenticación fuerte como principio de seguridad de acceso [31]. Pero no existe reportes de operadores locales aplicándola.

En cuanto a los parches de y actualizaciones, se asigna una brecha media, debido a que ISO/IEC 27001 exige gestión de actualizaciones, pero no existe evidencia pública local; únicamente se documenta para OTT global [50].
Finalmente, el geo-blocking presenta una brecha Alta, dado que WIPO y DMCA reconoce este mecanismo como obligatorio para la gestión territorial de licencias [42]; no obstante, ningún operador IPTV ecuatoriana lo evidencia.

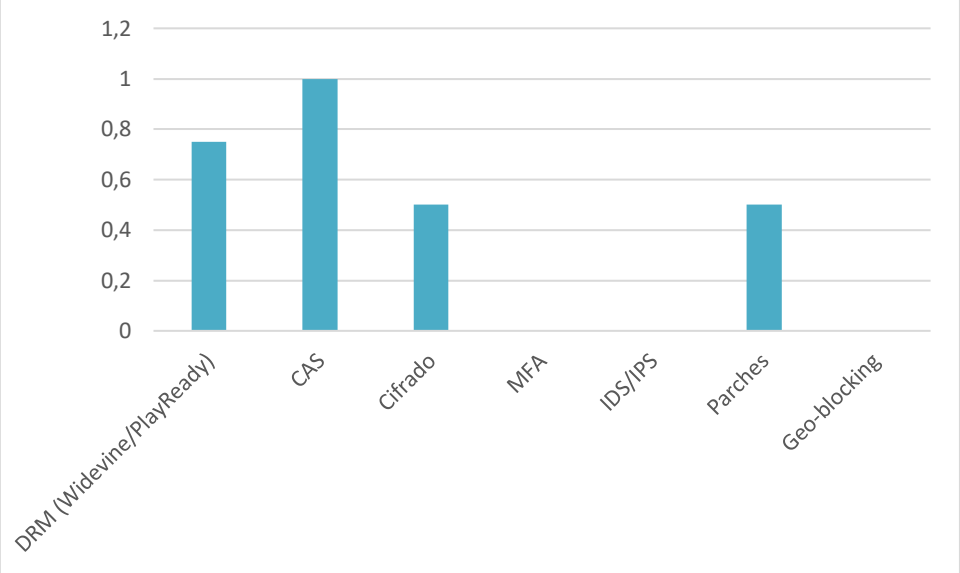


Figura 9: Nivel de cumplimiento de mecanismos de seguridad en IPTV

La figura 9 demuestra que IPTV se encuentra en un punto intermedio, con una mezcla de brechas Medias y Altas. CAS destaca como el mecanismo mejor posicionado; sin embargo, la falta de mecanismos avanzados reduce su alineación normativa.
En la Tabla 9 se presentan las brechas normativas para OTT, mostrando su relación con estándares internacionales de seguridad.

Tabla 9: Brecha normativa de OTT

Mecanismo	**Estándar Internacional**	**Situación OTT global**	**Brecha**	**Justificación**
DRM	Obligatorio en AVMSD, DMCA, UIT.	Widevine / PlayReady / FairPlay.	Baja	Total cumplimiento.
Cifrado TLS/AES	Recomendado UIT.	Documentado (Netflix, AWS).	Baja	Cumplimiento Pleno.
MFA	ISO/IEC recomienda MFA.	Parcial (Amazon si, Netflix no.	Media	No uniformemente implementado.
IDS/IPS (Anti DDOS)	ETSI, UIT.	Akamai / CDNs.	Baja	Amplia evidencia.
Parches / Actualizaciones	ISO/IEC 27001.	CI/CD continuo.	Baja	Muy sólido.

Geo-blocking	WIPO/DMCA exige geo control.	Totalmente implementado.	Baja	Requisito legal en licencia territoriales.

En el caso de las plataformas de OTT, las brechas frente a los estándares internacionales son globalmente bajas, debido a que estas plataformas suelen adoptar directamente los requisitos de protección establecidos por entidades como AVMSD, DMCA, UIT, ISO/IEC y WIPO.

El mecanismo de DRM demuestra cumplimento total, sin brechas gracias a la implementación documentada de sistemas como Widevine, PlayReady y FairPlay [47], [48], [49].

El cifrado también presenta brecha Baja, ya que plataformas como Netflix, Disney+ y Amazon lo aplican [56], mientras que Netflix no lo ha integrado plenamente en su flujo de usuarios.

Los mecanismos IDS/IPS, utilizados por proveedores de CDN como Akamai, cumplen plenamente los requisitos de ETSI y UIT [57], lo que genera una brecha baja.

De igual forma, las actualizaciones y parches presentan una brecha Baja, debido a la existencia de despliegue continuo y gestión automatizada de versiones (CI/CD) documentada por Netflix [50].

Finalmente, el geo-blocking también presenta una brecha Baja debido a que es un requisito legal para licencias territoriales y está plenamente implementado según WIPO [42].

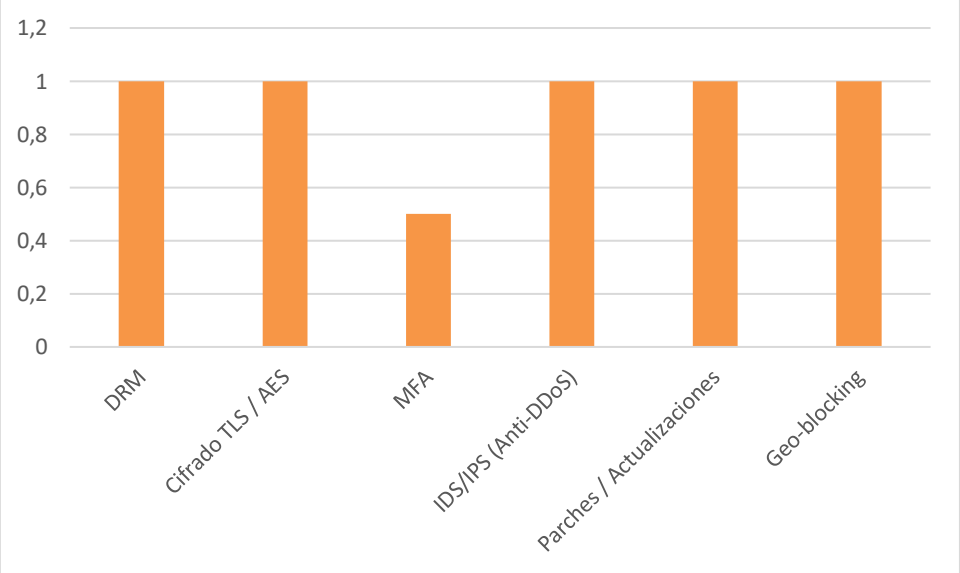


Figura 10: Nivel de cumplimiento de mecanismos de seguridad en OTT

En base a la figura 10, OTT presenta la menor cantidad de brechas, caracterizándose por su alineación casi total con estándares como DMCA, AVMSD e ISO/IEC 27001. Solo MFA presenta brecha Media debido a su implementación no uniforme.

En la Tabla 10 se presenta la comparación transversal de las brechas normativas identificadas en TDT, IPTV y OTT, integrando los resultados de los análisis individuales realizados para cada tecnología. Esta matriz permite observar de manera comparativa la magnitud de las brechas y el grado de alineación con los estándares internacionales aplicables a la protección de contenidos digitales.

Tabla 10: Comparación de las brechas normativas de TDT, IPTV y OTT

Tecnología	Brechas altas	Brechas medias	Brechas bajas	Nivel general
TDT	4	2	0	Muy Alto
IPTV	3	3	1	Medio – Alto
OTT	0	1	5	Bajo

La tabla 10 muestra diferencias claras en la magnitud de las brechas normativas entre las tres tecnologías evaluadas. En el caso de TDT, se identifica el mayor número de brechas clasificadas como Altas, derivadas de la ausencia de mecanismos clave como DRM, MFA y sistemas IDS/IPS, los cuales son considerados fundamentales por organismos internacionales como ITU, ETSI e ISO/IEC para garantizar la protección de contenidos digitales [31], [43], [44].

Por su parte, IPTV presenta un nivel de brechas intermedio, debido a que incorpora parcialmente mecanismos recomendados, como CAS y cifrado, pero carece de evidencia pública sobre controles avanzados exigidos por estándares internacionales, tales como MFA y sistemas de detección de intrusiones [54].

Finalmente, OTT muestra el nivel más bajo de brechas, resultado de su alineación directa con estándares globales como AVMSD, DMCA y las directrices de WIPO, lo que permite una adopción amplia de mecanismos como DRM, cifrado, actualizaciones continuas y geo-blocking [42], [49].

Este comportamiento evidencia que la madurez normativa y técnica varía significativamente entre tecnologías, y que aquellas sustentadas en infraestructuras y marcos globales tienden a presentar menor distancia frente a los estándares internacionales.

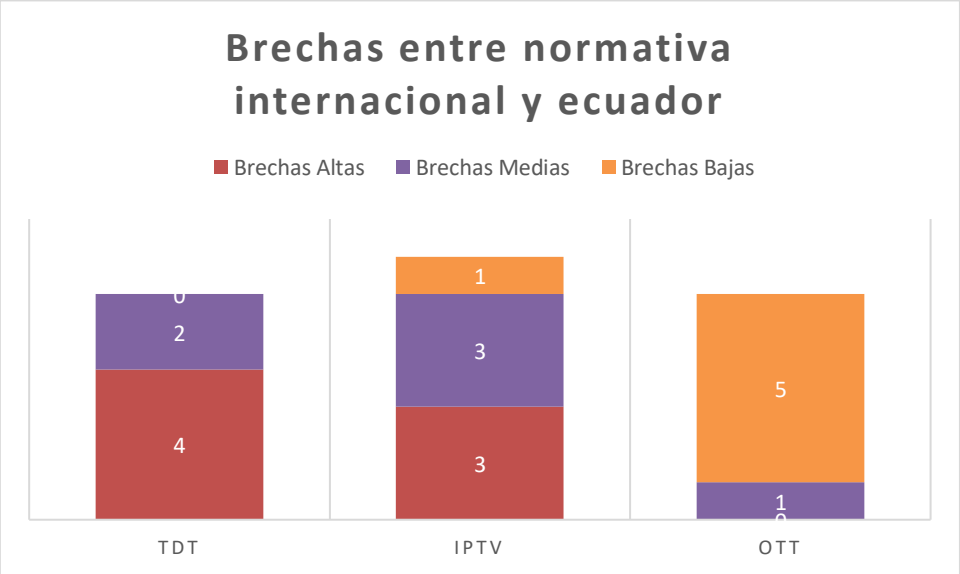


Figura 11: Distribución proporcional de brechas en TDT, IPTV y OTT

La figura 11 representa visualmente la proporción de brechas Altas, Medias y Bajas para cada una de las tecnologías analizadas. El gráfico evidencia que TDT concentra la mayor cantidad de brechas Altas, lo que confirma su mayor distancia frente a los marcos regulatorios internacionales. IPTV presenta un comportamiento intermedio, con una distribución equilibrada entre brechas Medias y Altas. En contraste, OTT exhibe una

predominancia de brechas Bajas, reflejando su alto grado de alineación con los estándares internacionales de seguridad digital. En conjunto, la figura refuerza la tendencia observada en la Tabla 10 y permite una interpretación clara del contraste entre tecnologías.

4.1.3 Análisis de brechas de riesgos en la protección de contenidos.

En este nivel se integran los resultados técnicos y normativos previamente evaluados para determinar el grado de cumplimiento final de los mecanismos de seguridad en TDT, IPTV y OTT. Este análisis permite identificar el nivel de alineación de cada tecnología frente a los estándares internacionales, mediante la valoración consolidada de los seis mecanismos evaluados: DRM, CAS, cifrado, MFA, IDS/IPS, parches y geo-blocking. Los valores finales se obtuvieron promediando las puntuaciones asignadas en cada caso, según la metodología establecida.

En la Tabla 11 se presentan los niveles de cumplimiento final de los mecanismos de seguridad en TDT, considerando la evidencia técnica disponible y las brechas normativas identificadas previamente.

Tabla 11: Nivel de cumplimiento final de mecanismos de seguridad en TDT

Mecanismo	**Existencia de mecanismo de seguridad**	**Brechas entre normativa internacional y ecuatoriana**	**Cumplimiento final**	**Interpretación**
DRM	NEP	Alta	0	No existe evidencia, gran brecha.
CAS	1	Media	0.5	Existe implementación parcial sin normativa.
Cifrado	0.5	Media	0.5	Cifrado técnico, no normativo.
MFA	NEP	Alta	0	Sin autenticación fuerte.
IDS/IPS	NEP	Alta	0	No hay monitoreo de intrusiones.
Parches	NEP	Alta	0	Sin políticas documentadas.
Geo-blocking	0	Media	0	No aplica y no existe mecanismo equivalente.

El análisis del nivel de cumplimiento final de los mecanismos de seguridad en TDT evidencia importantes limitaciones, reflejadas en la ausencia casi total de mecanismos alineados con estándares internacionales. Como se observa en la tabla 11, TDT únicamente alcanza un valor de cumplimiento parcial (0.5) en los mecanismos CAS y

cifrado, debido a que la evidencia técnica indica la existencia de acceso condicional básico integrado en el estándar ISDB-Tb, aunque sin normativa clara que regule su adopción en Ecuador [43], [46].

Los mecanismos DRM, MFA, IDS/IPS, parches de seguridad y geo-blocking presentan un cumplimiento final de 0, resultado de la inexistencia de evidencia pública que confirme su implementación y de la ausencia de requisitos específicos en la normativa ecuatoriana. Esto coincide con las recomendaciones de ITU-T H.701 y ETSI TS 103 829, que consideran estos mecanismos fundamentales para la protección audiovisual [43], [44].

En conjunto, TDT presenta un nivel del 21.4%, lo cual refleja un ecosistema de seguridad limitado y distante de las prácticas internacionales.

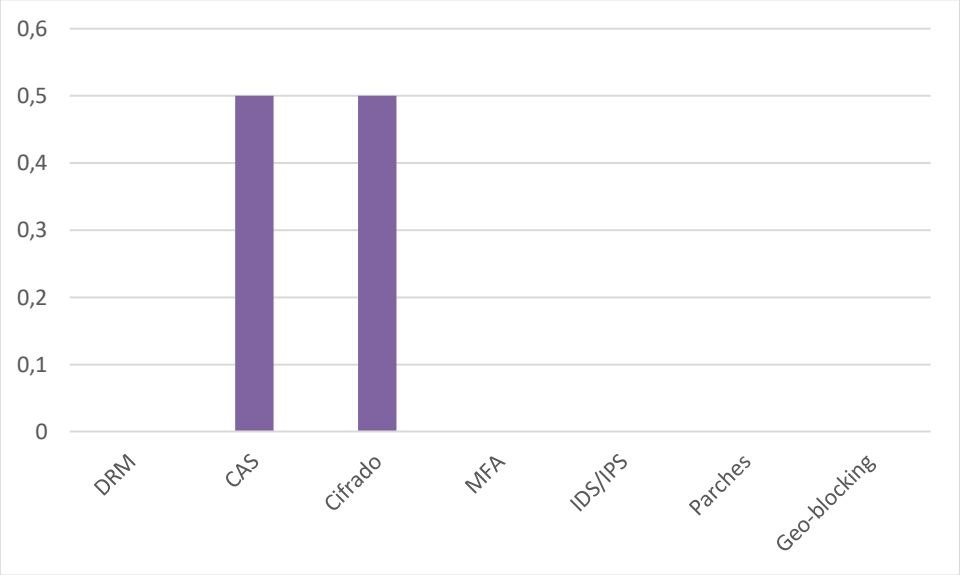


Figura 12: Nivel de cumplimiento final de los mecanismos de seguridad en TDT

La figura 12 representa visualmente la valoración final de cumplimiento para cada mecanismo evaluado. Se observa que TDT solo presenta niveles parciales en CAS y cifrado, mientras que los demás mecanismos permanecen en cumplimiento nulo. El gráfico confirma las limitaciones estructurales para integrar mecanismos avanzados de protección en entornos ISDB-Tb.

En la Tabla 12 se presenta el nivel de cumplimiento final de los mecanismos de seguridad en IPTV, integrando tanto la evidencia técnica como las brechas normativas documentadas en el análisis previo.

Tabla 12: Nivel de cumplimiento final de mecanismos de seguridad en IPTV

Mecanismo	**Existencia de mecanismos de seguridad**	**Brechas entre la normativa internacional y ecuatoriana**	**Cumplimiento final**	**Interpretación**
DRM	0.5	Media – Alta	0.5	Solo evidencia global, no local.
CAS	1	Baja	1	Confirmado en Ecuador (NDS,

				Nagravision, Conax).
Cifrado	0.5	Media	0.5	Presente globalmente, no documentado en Ecuador.
MFA	NEP	Alta	0	No implementada en operadores ecuatorianos.
IDS/IPS	NEP	Ala	0	Sin evidencia de monitoreo.
Parches	0.5	Media	0.5	Existe globalmente, no localmente.
Geo-blocking	NEP	Alta	0	No documentado en Ecuador.

El análisis muestra que IPTV alcanza un nivel de cumplimiento intermedio. La matriz evidencia que CAS presenta un cumplimiento total (1), respaldado por documentación que confirma el uso de sistemas como Nagravisión y Conax en operadores ecuatorianos [45]. El cifrado obtiene un valor de 0.5, sustentado en evidencia global de su adopción, aunque sin documentación verificable a nivel nacional [55].

Por otro lado, los mecanismos DRM, MFA e IDS/IPS registran un cumplimiento final de 0, debido a la ausencia de publicaciones oficiales que indiquen su implementación. Esto contrasta con los lineamientos de ITU y ETSI, que catalogan estos mecanismos como esenciales para servicios audiovisuales sobre redes IP [12], [44].

El mecanismo parches de seguridad obtiene un valor de 0.5, debido a la existencia de evidencia internacional, aunque sin registro público específico para Ecuador. En conjunto, IPTV alcanza un cumplimiento final del 35.7%, ubicándose en un nivel de madurez intermedio.

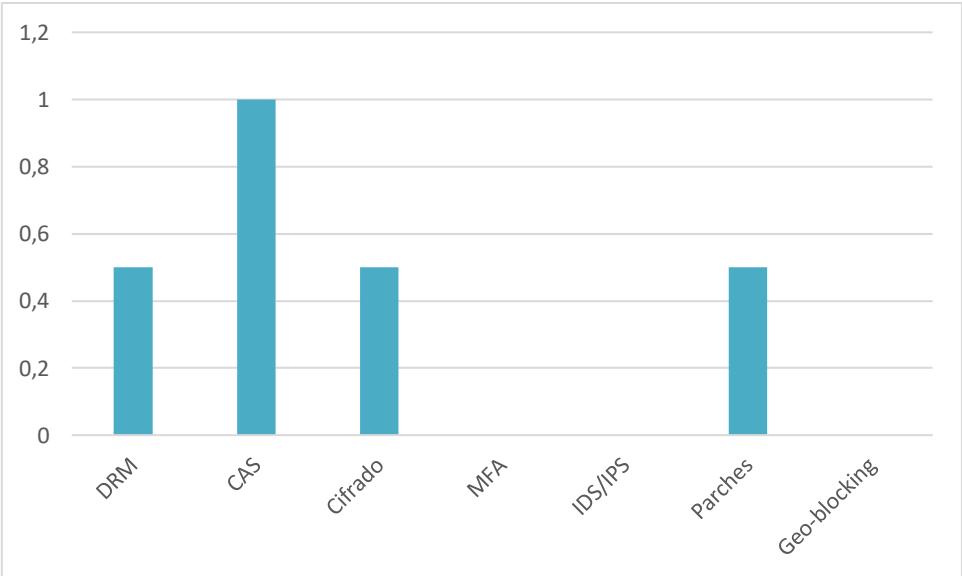


Figura 13: Nivel de cumplimiento final de los mecanismos de seguridad en IPTV

La figura 13 evidencia la combinación de mecanismos con cumplimiento total, parcial y nulo. IPTV presenta mayores avances que TDT, pero aún enfrenta brechas significativas en controles avanzados como DRM, MFA e IDS/IPS. El gráfico confirma la distribución intermedia observada en la matriz.

En la Tabla 13 se sintetizan los niveles de cumplimiento final de los mecanismos de seguridad en plataformas OTT, reflejando la documentación técnica de proveedores globales.

Tabla 13: Nivel de cumplimiento final de mecanismos de seguridad en OTT

Mecanismos	**Existencia de mecanismos de seguridad**	**Brechas entre la normativa internacional y ecuatoriana**	**Cumplimiento final**	**Interpretación**
DRM	1	Baja	1	Implementación total (Widevine / PlayRead / FairPlay).
Cifrado	1	Baja	1	TLS + AES verificado.
MFA	0.5	Media	0.5	Parcial: Amazon si, Netflix no.
IDS/IPS	1	Baja	1	OTT protegido por Akamai / Prolexic.
Parches	1	Baja	1	Actualización continua (CI/CD).
Geo-blocking	1	Baja	1	Requisito legal en licencias territoriales.

Las plataformas OTT muestran el nivel de cumplimiento más alto entre las tecnologías analizadas. Los mecanismos DRM, cifrado, IDS/IPS, parches y geo-blocking alcanzan un cumplimiento de 1, sustentado en evidencia técnica documentada por proveedores como Netflix, Amazon, Disney+ y Akamai [42], [50], [52].

El mecanismo MFA obtiene un valor de 0.5 debido a su implementación heterogénea mientras servicios como Amazon Prime Video lo aplican de forma robusta, otros como Netflix aún no lo integran en su flujo de autenticación [56]. Esta diferencia genera una brecha Media, aunque no compromete significativamente el nivel general de protección de OTT.

OTT alcanza un cumplimiento final del 91.7%, lo que refleja una alineación casi total con marcos regulatorios internacionales como DMCA, AVMSD e ISO/IEC 27001 [42], [49].

Figura 14: Nivel de cumplimiento final de los mecanismos de seguridad en plataformas OTT

La figura 14 muestra una distribución casi uniforme de valores máximos (1), lo que evidencia una implementación consolidada de mecanismos de seguridad. La única excepción corresponde a MFA, cuyo valor intermedio no afecta significativamente el desempeño general de OTT.

4.1.4 Comparación transversal del cumplimiento entre TDT, IPTV y OTT

En esta sección se integra la valoración final de los mecanismos de seguridad para TDT, IPTV y OTT con el propósito de identificar tendencias generales de cumplimiento y su alineación frente a los estándares internacionales. Este análisis transversal permite comparar el grado de madurez técnica y normativa de cada tecnología, a partir de los resultados obtenidos en las Tablas 11, 12 y 13.

Los resultados comparativos muestran diferencias claras en el nivel de cumplimiento final alcanzado por cada tecnología. TDT registra el menor nivel de cumplimiento, con valores de 0 en cinco de los seis mecanismos evaluados (DRM, MFA, IDS/IPS, parches y geo-blocking). Esta situación refleja la ausencia de lineamientos regulatorios que integren mecanismos modernos de seguridad en la implementación nacional de ISDB-Tb, lo cual coincide con lo establecido en las recomendaciones UIT y ETSI, donde se consideran indispensables mecanismos como DRM, cifrado robusto y autenticación fuerte para la protección de contenidos audiovisuales [43], [44]. El único mecanismo con cumplimiento parcial corresponde a CAS / cifrado técnico, sustentando en evidencia técnicas de la operación del estándar ISDB-Tb en el país [46]. En conjunto TDT presenta un nivel de protección básica y distante de los estándares internacionales.

Por su parte, IPTV muestra un nivel intermedio de cumplimiento. El mecanismo mejor posicionado es CAS, con cumplimiento total (1), sustentado en el uso documentado de sistemas como Nagravisión y Conax por parte de operadores ecuatorianos [45]. El cifrado obtiene un cumplimiento de 0.5, dado que su adopción está ampliamente documentada a nivel global, aunque no existe confirmación oficial a nivel nacional [55]. En contraste, mecanismos como DRM, MFA e IDS/IPS obtienen un valor de 0, debido a la ausencia

de evidencia técnica o normativa que respalde su implementación en Ecuador. En consecuencia, IPTV presenta un cumplimiento final del 35.7%, superior al de TDT, pero aún distante de estándares como ITU-T H.702 e ISO/IEC 27001 [10], [43].

Finalmente, OTT se posiciona como la tecnología con el mayor nivel de cumplimiento final entre las tres evaluadas. Cinco de los seis mecanismos analizados DRM, cifrado, IDS/IPS, parches y geo-blocking alcanzan un cumplimiento total (1), respaldado por evidencia técnica proveniente de proveedores globales como Netflix, Amazon, Disney+ y Akamai [42], [50], [52], [56]. La única excepción corresponde a MFA, cuyo cumplimiento parcial (0.5) se debe a su implementación no uniforme entre distintas plataformas comerciales. OTT alcanza un cumplimiento final del 91.7%, mostrando un alineamiento casi completo con marcos regulatorios internacionales como AVMSD, DMCA y las directrices de WIPO [42], [49].

Interpretación transversal

La comparación general evidencia que el nivel de cumplimiento final está directamente relacionado con el modelo tecnológico y regulatorio de cada plataforma:

- TDT depende de una infraestructura no IP de una normativa local limitada, lo que restringe la integración de mecanismo modernos de seguridad.
- IPTV presenta una estructura híbrida, con avances parciales y vacíos documentados que dificultan su alineación plena con estándares internacionales.
- OTT, en cambio, se sustenta en arquitectura y marcos regulatorios globales, lo que facilita la adopción de mecanismos avanzados de protección y reduce significativamente las brechas de cumplimiento.

En síntesis, la comparación transversal confirma que OTT presenta el mayor nivel de cumplimiento, seguida por IPTV con un nivel intermedio, mientras que TDT exhibe el cumplimiento más bajo. Estos resultados refuerzan la necesidad de fortalecer los lineamientos técnicos y normativos en Ecuador para reducir la brecha existente con respecto a los estándares internacionales de seguridad digital.

4.2 Discusión

La discusión integra los hallazgos obtenidos a partir de los tres ejes metodológicos definidos en este estudio nivel técnico, normativo y de brechas de riesgo con el propósito de interpretar de manera estructurada las diferencias observadas entre TDT, IPTV y OTT. Este enfoque permite analizar cómo la capacidad de implementación tecnológica, el grado de alineación con estándares internacionales y la magnitud de las brechas identificadas inciden conjuntamente en la protección de contenidos audiovisuales en el contexto ecuatoriano.

4.2.1 Capacidad operativa y solidez tecnológica de TDT, IPTV y OTT.

El análisis técnico revela diferencias substanciales entre las tres tecnologías. TDT presenta el rezago más notable, limitado a mecanismos básicos como CAS y cifrado interno inherentes al estándar ISDB-Tb. La ausencia total de DRM, MFA, IDS/IPS, geo-blocking y parches de seguridad refleja una arquitectura con escasa capacidad para integrar controles modernos, lo cual coincide con estudios previos que identifican

debilidades estructurales en sistemas de radiodifusión digital ante amenazas contemporáneas [58].

En el caso de IPTV, se observa un nivel técnico intermedio. La presencia documentada de CAS y la disponibilidad internacional de cifrado evidencian avances en comparación con TDT; sin embargo, la falta de evidencia pública sobre la implementación de mecanismos críticos como DRM, MFA e IDS/IPS muestra vacíos importantes frente a estándares como ITU-T H.702 e ISO/IEC 27001 [31], [42]. Esto sugiere que, si bien IPTV posee mayor flexibilidad técnica, su capacidad de protección depende de decisiones operativas individuales más que de lineamientos regulados.

Finalmente, OTT presenta la arquitectura técnica más madura. La adopción comprobada de DRM (Widevine, PlayReady, FairPlay), cifrado TLS + AES, servicios de mitigación anti DDoS, IDS/IPS distribuidos por proveedores como Akamai, geo-blocking y actualizaciones continuas posiciona a OTT como la tecnología más robusta en términos de seguridad [50], [56]. La única limitación parcial corresponde a MFA, cuya implementación varía entre plataformas, aunque esta variabilidad no compromete el nivel técnico global.

4.2.2 Coherencia regulatoria y alineación con estándares internacionales.

El nivel normativo refuerza las diferencias previamente identificadas. TDT presenta las brechas regulatorias más amplias. La normativa ecuatoriana basada en ISDB-Tb no contempla la implementación obligatoria de mecanismos modernos como DRM, autenticación fuerte, cifrado reforzado ni monitoreo de intrusiones, todos ellos recomendados por ITU, ETSI e ISO/IEC como pilares para la protección de contenidos audiovisuales [15], [44]. Esta limitación regulatoria contribuye al bajo nivel de cumplimiento técnico observado.

En IPTV, aunque existen implementaciones parciales como CAS, tampoco se identifican normativas que exijan controles avanzados. La ausencia de regulaciones específicas para DRM, MFA, IDS/IPS y parches de seguridad deriva en brechas normativas medias y altas. El análisis evidencia que IPTV depende de decisiones internas de los operadores, más que de obligaciones regulatorias, lo que dificulta la alineación con estándares internacionales como ITU-T H.701 y ETSI TS 103 829.

Por el contrario, OTT opera bajo marcos regulatorios internacionales como AVMSD, DMCA y las directrices de WIPO, que regulan explícitamente la implementación de mecanismos de protección de contenido. Esto explica su mayor nivel de alineación y cumplimiento, ya que la presión normativa extranjera impulsa obligaciones de seguridad que no dependen de la regulación ecuatoriana [18], [42].

4.2.3 Brechas estructurales y riesgos asociados a la protección de contenidos.

La integración del nivel técnico y normativo permite caracterizar la magnitud de las brechas de riesgo presentes en cada tecnología. TDT concentra el mayor número de brechas catalogadas como Altas, lo que evidencia su mayor vulnerabilidad frente a los estándares internacionales. Este resultado coincide con informes del MINTEL, que

señalan limitaciones persistentes en infraestructura y adopción plena de TDT, particularmente en zonas rurales [53].

IPTV presenta brechas Medias y Altas, reflejando un perfil de riesgo menor que TDT, pero aún lejos del ideal. Aunque presenta algunos mecanismos implementados, la falta de requerimientos normativos específicos amplía su distancia frente a marcos internacionales de seguridad digital.

Por su parte, OTT demuestra brechas predominantemente Bajas, resultado lógico de su alineación técnica y normativa global. La única brecha Media corresponde a MFA, debido a su implementación heterogénea entre proveedores [29].

4.2.4 Relación entre factores técnicos, regulatorios y brechas de seguridad.

La relación entre los tres nivel metodológicos muestra patrones consistentes:

- Una implementación técnica limitada sin respaldo normativo, como en TDT, genera brechas de riesgos altas.
- Una implementación parcial con ausencia de obligaciones normativas, como en IPTV, deriva en brechas medias y altas.
- Una implementación técnica robusta respaldada por marcos estrictos, como en OTT, produce brechas bajas.

La comparación entre tecnologías confirma que el nivel de protección de contenidos audiovisuales depende directamente de la interacción entre:

1. La capacidad técnica para implementar mecanismos avanzados.
2. La existencia de normativas que obliguen su adopción.
3. La magnitud de brechas resultantes cuando estos dos factores no se alinean.

Estos patrones coinciden con estudios de CETLA y Martin, los cuales señalan que entornos con marcos regulatorios débiles presentan mayor exposición a piratería, accesos no autorizados y fallas de integridad en la distribución de contenidos [14], [20].

4.2.5 Síntesis interpretativa sobre el comportamiento comparado de las tres tecnologías.

El análisis transversal muestra que OTT es la tecnología que presenta mayor madurez técnica y normativa, lo cual se refleja en un nivel de brechas bajo y en una protección sólida de contenidos audiovisuales. IPTV se sitúa en un nivel intermedio: presenta avances en ciertos mecanismos, pero carece de una estructura regulatoria que impulse la integración plena de controles avanzados. TDT, por su parte, evidencia limitaciones tanto técnicas como normativas, lo que explica su brecha elevada frente a los estándares internacionales.

En conjunto, los resultados sugieren que la seguridad de las plataformas audiovisuales en Ecuador depende no solo de la capacidad técnica de cada tecnología, sino también del marco regulatorio que respalda su operación. La ausencia de exigencias normativas nacionales en mecanismos clave amplía la brecha entre TDT e IPTV con respecto a OTT, lo que resalta la necesidad de fortalecer los lineamientos técnicos y regulatorios para mejorar la protección del ecosistema audiovisual ecuatoriano.

4.3 Evaluación de hipótesis

La presente sección contrasta los resultados obtenidos con las hipótesis formuladas en el Capítulo I, con el propósito de determinar si la evidencia documental permite aceptarlas en su totalidad, aceptarlas parcialmente o rechazarlas. Dado el carácter teórico y no experimental de la investigación, la evaluación se sustenta exclusivamente en la información derivada del análisis documental, las matrices comparativas y la verificación de evidencia pública.

4.3.1 Evaluación de la hipótesis general

Si los sistemas TDT, IPTV y OTT en Ecuador implementan mecanismos de seguridad integrales como E2EE, DRM, CAS y MFA alineados con los estándares internacionales de seguridad digital, se reduciría significativamente el riesgo de vulnerabilidades técnicas, accesos no autorizados y pérdida de integridad de los contenidos audiovisuales.

Evaluación

En base a los resultados se muestran niveles de cumplimiento muy distintos entre tecnologías indicándonos que:

- OTT implementa de manera plena la mayoría de los mecanismos (DRM, cifrado, IDS/IPS, parches, geo-blocking) y parcialmente MFA.
- IPTV presenta un cumplimiento intermedio, con mecanismos como CAS y cifrado parcialmente implementados, pero sin evidencia de DRM, MFA o IDS/IPS.
- TDT exhibe el nivel más bajo, con ausencia total de DRM, MFA, IDS/IPS y mecanismos de actualización, y solo cuenta con CAS y cifrado parcial dentro del estándar ISDB-Tb.

Los hallazgos demuestran que solo las plataformas de OTT cumplen las condiciones planteadas en la hipótesis general, mientras que TDT e IPTV no alcanzan la implementación integral requerida.

Por ende, la hipótesis general se acepta parcialmente; debido a que OTT confirma la relación planteada, mostrado menor brecha y mayor seguridad, pero TDT e IPTV no implementan de forma íntegra los mecanismos exigidos por estándares como ITU-T H.701, ETSI TS 103 829 e ISO/IEC 27001 [31], [43], [44]. Por lo tanto, la hipótesis solo se válida para tecnologías con adopción plena de dichos mecanismos.

4.3.2 Evaluación de las hipótesis específicas.

H1: Las vulnerabilidades presentes en los sistemas TDT, IPTV y OTT en Ecuador se deben a la limitada implementación de mecanismos técnicos de protección, como el cifrado integral y la MFA.

Evaluación.

Los resultados evidencian que TDT carece de cinco de los siete mecanismos esenciales, lo que refleja una vulnerabilidad estructural alta. En el caso de IPTV, se identifica una implementación parcial que se traduce en una vulnerabilidad intermedia. Por su parte, OTT implementa la mayoría de los mecanismos analizados, lo que se asocia con una vulnerabilidad considerablemente baja.

La matriz confirma que donde existen menos mecanismos implementados, las brechas sin más altas, lo cual concuerda con estudios de Zeadally y CETLA [14], [18].

Especialmente crítico es el caso de MFA, ausente en TDT e IPTV, el cual se encuentra aplicado parcialmente en OTT confirmando así su rol determinante en la protección frente a accesos no autorizados.

Por ende, la hipótesis H1 es aceptada, ya que la evidencia confirma que la falta de mecanismos como cifrado, MFA, IDS/IPS y DRM se correlacionan directamente con la presencia de vulnerabilidades.

H2: El cumplimiento parcial de los estándares internacionales de seguridad digital y derechos de autor incide en la eficacia de los mecanismos de protección de contenidos aplicados en Ecuador.

Evaluación

Con base en las matrices de brechas normativas, se evidencia que TDT presenta una brecha significativamente alta, con cuatro brechas clasificadas como Altas y dos como Medias. En el caso de IPTV, los valores obtenidos reflejan una brecha Media-Alta, situándola relativamente cerca de los resultados de TDT. En contraste, OTT presenta una brecha Baja, atribuida a su alineación con normativa internacional.

Ecuador carece de los siguientes aspectos:

- Obligatoria implementación de DRM
- Exigencia de MFA
- Mandados regulatorios de cifrado robustos
- Reglas claras para IDS/IPS
- Fiscalización de actualizaciones y parches

Los estándares internacionales establecen estos requisitos como mínimos [31], [43], [44], [49]. Pero la normativa ecuatoriana solo cubre parcialmente CAS y ciertos lineamientos de protección. La falta de alineación normativa explica por qué TDT e IPTV presentan menor eficiencia en protección de contenidos, mientras que OTT al operar bajo marcos internacionales alcanza mejores resultados.

Por consecuencia de esto la hipótesis H2 es aceptada, ya que la evidencia confirma que el cumplimiento normativo parcial afecta directamente la eficacia de los mecanismos de protección aplicados en Ecuador.

H3: Las brechas regulatorias y la falta de fiscalización en la aplicación de políticas de seguridad limitan la protección integral de los contenidos audiovisuales transmitidos por TDT, IPTV y OTT.

Evaluación

En base a los resultados obtenidos se muestra que en TDT no existe fiscalización sobre mecanismos de seguridad y ARCOTEL no exige DRM, MFA, IDS/IPS ni políticas de actualización, en IPTV la aplicación de mecanismos depende exclusivamente de los operadores, sin supervisión estatal documentada, por otro lado, OTT aplica los mecanismos por exigencias globales, pero Ecuador no fiscaliza debido a que estos servicios no están regulados por LOTT ni por reglamentos de ARCOTEL.

La literatura indica que la ausencia de fiscalización incrementa la exposición a piratería, distribución ilegal y acceso no autorizados [14], [20]. Esto coincide con la brecha estructural identificada, donde el marco regulatorio es débil, la protección es insuficiente.

CAPÍTULO V. CONCLUSIONES y RECOMENDACIONES

5.1 Conclusiones.

El análisis realizado permite identificar el estado actual de la seguridad y protección de contenidos en TDT, IPTV y OTT en Ecuador, en correspondencia con el objetivo general planteado. Los resultados obtenidos evidencian diferencias significativas entre tecnologías, derivadas de tres factores fundamentales la capacidad técnica de cada plataforma, la alineación con marcos normativos nacionales e internacionales y la magnitud de las brechas de riesgo frente a los estándares de seguridad digital.

El análisis técnico permite evidenciar que las vulnerabilidades identificadas en TDT, IPTV y OTT se encuentran directamente relacionadas con la disponibilidad y madurez de los mecanismos de protección implementados. TDT presenta la mayor vulnerabilidad debido a la ausencia de mecanismos esenciales como DRM, MFA, IDS/IPS y parches de seguridad, lo que limita su capacidad para mitigar riesgos. IPTV muestra un nivel intermedio, con mecanismos parcialmente implementados (CAS, cifrado), pero sin controles avanzados recomendados por estándares internacionales. En contraste, OTT demuestra la arquitectura más robusta, integrando sistemas DRM comerciales (Widevine, FairPlay, PlayReady), cifrado TLS/AES, geo-blocking, IDS/IPS y procesos continuos de actualización, lo que reduce significativamente su exposición a riesgos. En síntesis, la capacidad técnica de implementación es el principal determinante del nivel de vulnerabilidad de cada tecnología.

El análisis normativo revela que el cumplimiento de estándares internacionales de seguridad digital y derechos de autor es limitado y desigual entre tecnologías. TDT e IPTV, al estar reguladas principalmente por normativa nacional, presentan brechas significativas debido a que la LOTT, la Ley Orgánica de Protección de Datos Personales y los reglamentos asociados no incluyen requisitos obligatorios para mecanismos como DRM, MFA, cifrado robusto, IDS/IPS o actualizaciones continuas. En contraste, OTT presenta un elevado nivel de cumplimiento, ya que opera bajo lineamientos internacionales como AVMSD, DMCA y las directrices de WIPO. Por lo tanto, la alineación normativa constituye un factor determinante para la eficacia de los mecanismos de protección.

Las brechas regulatorias y la falta de procesos de fiscalización se identificaron como factores críticos que limitan la protección integral de contenidos en Ecuador. TDT presenta brechas predominantemente Altas debido a la falta de modernización normativa; IPTV presenta brechas Medias y Altas debido a la ausencia de lineamientos nacionales que obliguen la implementación de mecanismos avanzados; mientras que OTT presenta brechas bajas, atribuibles a su adopción directa de marcos regulatorios globales. En conjunto, se concluye que la falta de regulaciones actualizadas y de mecanismos de supervisión estatal afecta directamente el nivel de seguridad alcanzado por cada tecnología.

La investigación permite concluir que la seguridad de contenidos en el Ecuador presenta un desarrollo heterogéneo. OTT constituye la tecnología con mayor nivel de protección, al alinearse directamente con prácticas y estándares internacionales; IPTV ocupa una posición intermedia, con implementaciones parciales y dependientes de prácticas

internas; mientras que TDT presenta el rezago más notable debido a limitaciones técnicas y regulatorias. Este panorama evidencia la urgente necesidad de fortalecer el marco normativo nacional y promover la adopción obligatoria de mecanismos avanzados de seguridad para garantizar la integridad, confidencialidad y disponibilidad de los contenidos audiovisuales transmitidos en el país.

5.2 Recomendaciones.

Se recomienda que los operadores de TDT e IPTV incorporen mecanismos de seguridad avanzados, tales como DRM, MFA, E2EE, sistemas IDS/IPS y políticas formales de actualización continua. La integración de estos mecanismos permitiría reducir las brechas identificadas y elevar el nivel de protección frente a amenazas técnicas.

Es necesario que ARCOTEL y MINTEL actualicen los marcos regulatorios relacionados con TDT e IPTV, incorporando requisitos obligatorios de seguridad digital acordes con estándares internacionales, especialmente en lo relativo a protección de contenidos, derechos de autor y ciberseguridad. Asimismo, se sugiere desarrollar lineamientos específicos que complementen el estándar ISDB-Tb con mecanismos de seguridad adicionales.

Se recomienda fortalecer los mecanismos de supervisión estatal mediante auditorías técnicas periódicas orientadas a verificar el cumplimiento real de los mecanismos de seguridad implementados. En el caso de IPTV, deberá considerarse la creación de protocolos nacionales uniformes para garantizar una evaluación coherente entre operadores.

Dado el impacto creciente de OTT en el ecosistema audiovisual, se sugiere evaluar la creación de un marco regulatorio específico para estos servicios, que permita abordar vacíos existentes en materia de protección de datos, derechos de autor y supervisión de mecanismos de seguridad, sin contravenir sus lineamientos internacionales actuales.

Desde el ámbito académico, se recomienda promover investigaciones orientadas al análisis comparativo de mecanismos de seguridad, evaluación de nuevas tecnologías de protección y estudios sobre la integración de buenas prácticas internacionales en el contexto ecuatoriano. La generación continua de evidencia técnica contribuirá al fortalecimiento normativo y a la toma de decisiones informada en instituciones del sector.

BIBLIOGRÁFIA

[1] G. Giannakopoulos, P. Adegbenro, y M. A. Perez, "The Future of IPTV: Security, AI Integration, 5G, and Next-Gen Streaming", el 20 de marzo de 2025, *arXiv*: arXiv:2503.13450. doi: 10.48550/arXiv.2503.13450.

[2] M. Sichach, "Media Convergence and Artificial Intelligence: Transforming Communication and Content Creation", el 5 de septiembre de 2024, *Social Science Research Network, Rochester, NY*: 4947632. doi: 10.2139/ssrn.4947632.

[3] "2023 Volume 3 Securing Next Generation Broadcast Media Enterprises Against Cyberthreats", ISACA. Consultado: el 12 de octubre de 2025. [En línea]. Disponible en: https://www.isaca.org/resources/isaca-journal/issues/2023/volume-3/securing-next-generation-broadcast-media-enterprises-against-cyberthreats

[4] S. M. Altowaijri y M. Ayari, "The Synergistic Impact of 5G on Cloud-to-Edge Computing and the Evolution of Digital Applications", *Mathematics*, vol. 13, núm. 16, p. 2634, ene. 2025, doi: 10.3390/math13162634.

[5] Geneva, "Content Protection and Rights Management in IPTV Services". Consultado: el 12 de octubre de 2025. [En línea]. Disponible en: https://www.itu.int/rec/T-REC-H.701-200903-I/es

[6] "TR 103 829 - V1.1.1 - Lawful Interception (LI); IP address retention and traceability".

[7] ARCOTEL, "Boletín Estadístico de Cierre 2023: Servicios de Telecomunicaciones y Audiovisuales".

[8] "Guide To OTT Technology For Network Operators". Consultado: el 12 de octubre de 2025. [En línea]. Disponible en: https://www.uniqcast.com/ott-iptv/ott-technology-guide-network-operators

[9] HUGO DEL POZO BARREZUETA, "Ley organica de telecomunicaciones".

[10] "ISO/IEC 27001:2022", ISO. Consultado: el 12 de octubre de 2025. [En línea]. Disponible en: https://www.iso.org/es/norma/27001

[11] L. H. Gonsioroski *et al.*, "Advanced ISDB-T—Next Generation Digital TV System: Performance in Field Tests in Brazil", *IEEE Trans. Broadcast.*, vol. 69, núm. 2, pp. 538–551, jun. 2023, doi: 10.1109/TBC.2022.3226657.

[12] "Recomendaciones UIT-R - Aprobación", ITU. Consultado: el 22 de enero de 2025. [En línea]. Disponible en: https://www.itu.int:443/es/ITU-R/publications/Pages/rec-approval.aspx

[13] Gonzales P, "En Ecuador, 61% de las visitas a sitios web de videos es a portales ilegales", Primicias. Consultado: el 27 de noviembre de 2024. [En línea]. Disponible en: https://www.primicias.ec/economia/ecuador-sitios-web-ilegales-pirateria-magistv-77841/

[14] CETLA, "Dimensión e impacto de la piratería online de contenidos audiovisuales en América Latina - Edición 2024", cet.la. Consultado: el 27 de noviembre de 2024. [En línea]. Disponible en: https://cet.la/estudios/cet-la/dimension-e-impacto-de-la-pirateria-online-de-contenidos-audiovisuales-en-america-latina-edicion-2024/

[15] “ITU-T IPTV Global Standards Initiative”, ITU. Consultado: el 14 de julio de 2025. [En línea]. Disponible en: https://www.itu.int:443/en/ITU-T/gsi/iptv/pages/default.aspx

[16] MINTEL, “Plan Nacional de Telecomunicaciones”. [En línea]. Disponible en: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2024/09/elecomunicaciones_2024_2025_vf-signed-signed-signed-signed01551280017220057900459811001722369479.pdf

[17] E.-P. Fernández-Manzano y M.-I. González-Vasco, “Analytic surveillance: Big data business models in the time of privacy awareness”, *Prof. Inf.*, vol. 27, núm. 2, Art. núm. 2, abr. 2018, doi: 10.3145/epi.2018.mar.19.

[18] S. Zeadally, H. Moustafa, y F. Siddiqui, “Internet Protocol Television (IPTV): Architecture, Trends, and Challenges”, *IEEE Syst. J.*, vol. 5, núm. 4, pp. 518–527, dic. 2011, doi: 10.1109/JSYST.2011.2165601.

[19] “‘Apagón analógico’ en Ecuador inicia en el año 2016 – Ministerio de Telecomunicaciones y de la Sociedad de la Información”. Consultado: el 14 de julio de 2025. [En línea]. Disponible en: https://www.telecomunicaciones.gob.ec/tdt/

[20] J. B. A. Martín, “Convergencia de medios. Plataformas audiovisuales por Internet (Over-The-Top) y su impacto en el mercado audiovisual en España”, *Rev. Lat. Comun. Soc.*, núm. 79, Art. núm. 79, mar. 2021, doi: 10.4185/RLCS-2021-1496.

[21] H. J. Copara Morocho y L. F. León Salinas, “PROPUESTA DE UN MODELO DE “PROPUESTA DE UN MODELO DE NEGOCIO BASADO EN EL DESARROLLO NEGOCIO BASADO EN EL DESARROLLO DE APLICACIONES INTERACTIVAS PARA DE APLICACIONES INTERACTIVAS PARA TELEVISIÓN DIGITAL TERRESTRE, TELEVISIÓN DIGITAL TERRESTRE, USANDO SOFTWARE LIBRE GINGA”, Universidad Politécnica Salesiana, Cuenca, 2015. Consultado: el 22 de enero de 2025. [En línea]. Disponible en: https://d1wqtxts1xzle7.cloudfront.net/100693680/84692444-libre.pdf?1680641603=&response-content-disposition=inline%3B+filename%3DPropuesta_de_un_modelo_de_negocio_basado.pdf&Expires=1737574205&Signature=QH9ewx1XMIDtTur8d6FLbmQI2CySSIEKKBHV1irgzMeemipHXRgODyGRNg~tqnFhPmxCzDfEGxbEQ~7MMMibVzTKRUOa9Jr2ENL0tRCNlq3exLzGkqqemNJDZe0m8UsmpLc2CHSSeNIEOgBwrN7cczUP7MfGSmXvxltI9WASwdlhFUxdX~Htcg4ALL0mnytbCM94cbSSBcDpJst3I1smOoqX1UKOiEtsVxCY80Xk5NPKZoEs74r21vuJTuouudprgCT-cSpv2jsMmGVqDDkgQk1XVbxSlg7dnvbbDTtYZPBwSWCQNowgLP8PqFLthMbGW1r5Kz6KsfiKH2PiED6AIQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

[22] Luque Ordoñez, *TDT: Televisión Digital Terrestre*. Madrid: Ediciones Generales, 2011.

[23] García Leiva y L. Albornoz, *Televisión digital terrestre: caracterización, antecedentes e importancia*. Madrid: Universidad Carlos III, 2012. [En línea]. Disponible en: https://e-archivo.uc3m.es/bitstream/handle/10016/14621/digital_garcialeiva_2012.pdf

[24] Jezz Vernon, *et al.*, “Future of TV Distribution: A report prepared by the University of Exeter with the University of Leeds, MTM, 3 Reasons and Real

Wireless", nov. 2024, [En línea]. Disponible en: https://eprints.whiterose.ac.uk/219808/

[25] Unión Internacional de Telecomunicaciones (UIT), "Accessibility Modifications to Working Document: IPTV Services Requirements". FG IPTV (Focus Group on IPTV), mayo de 2007. [En línea]. Disponible en: https://www.itu.int/dms_pub/itu-t/md/05/fg.iptv/c/T05-FG.IPTV-C-0761%21%21MSW-E.doc

[26] P. Sánchez Vaquero, "Diseño de una sala de continuidad para distribución IPTV", Articulo Digital UPM. Consultado: el 22 de enero de 2025. [En línea]. Disponible en: https://oa.upm.es/73255/

[27] E. Cadena, "IPTV Internet Protocol Televevision", febrero de 2010.

[28] J. Kim, C. Nam, y M. H. Ryu, "IPTV vs. emerging video services: Dilemma of telcos to upgrade the broadband", *Telecommun. Policy*, vol. 44, núm. 4, p. 101889, may 2020, doi: 10.1016/j.telpol.2019.101889.

[29] C. Yang, L. Wang, H. Cao, Q. Yuan, y Y. Liu, "User Behavior Fingerprinting With Multi-Item-Sets and Its Application in IPTV Viewer Identification", *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 2667–2682, 2021, doi: 10.1109/TIFS.2021.3055638.

[30] Machaca Jimenez, "Diagrama Ott-Tvsapiens PDF | PDF", Scribd. Consultado: el 28 de mayo de 2025. [En línea]. Disponible en: https://it.scribd.com/document/393550554/DIAGRAMA-OTT-TVSAPIENS-1-pdf

[31] "ISO/IEC 27001:2022(en), Information security, cybersecurity and privacy protection — Information security management systems — Requirements". Consultado: el 18 de noviembre de 2025. [En línea]. Disponible en: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en

[32] "¿Qué es la Propiedad Intelectual?".

[33] "H.741.5 : Application event handling: Overall aspects of personalized IPTV services". Consultado: el 18 de noviembre de 2025. [En línea]. Disponible en: https://www.itu.int/rec/T-REC-H.741.5-202404-I/en

[34] "Specification for Service Information (SI) in DVB systems", DVB. Consultado: el 14 de julio de 2025. [En línea]. Disponible en: https://dvb.org/?standard=specification-for-service-information-si-in-dvb-systems

[35] de Octubre y S. Piso, "ING. HUGO DEL POZO BARREZUETA DIRECTOR".

[36] H. D. P. Barrezueta, "DIRECTOR DEL REGISTRO OFICIAL".

[37] ARCOTEL, "Norma Técnica ISDB-Tb". agosto de 2015. [En línea]. Disponible en: https://www.arcotel.gob.ec/wp-content/uploads/2015/08/Resumen_observaciones_Norma_TDT.pdf

[38] "Página no encontrada – Agencia de Regulación y Control de las Telecomunicaciones". Consultado: el 26 de noviembre de 2025. [En línea]. Disponible en: https://www.arcotel.gob.ec/reglamentos/

[39] "The Digital Millennium Copyright Act of 1998", 1998.

[40] "REGLAMENTO (UE) 2016/ 679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO - de 27 de abril de 2016 - relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre

circulación de estos datos y por el que se deroga la Directiva 95/ 46/ CE (Reglamento general de protección de datos)".
[41] European Parliament, "Audiovisual Media Services Directive". 2010. [En línea]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32010L0013
[42] WIPO, "WIPO Lex". Consultado: el 26 de noviembre de 2025. [En línea]. Disponible en: https://www.wipo.int/wipolex/en/text/295166
[43] I. Citaristi, "International Telecommunication Union—ITU", en *The Europa Directory of International Organizations 2022*, 24a ed., Routledge, 2022.
[44] ETSI, "TS 133 501 - V17.11.1 - 5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 17.11.1 Release 17)", 2023, [En línea]. Disponible en: https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/17.11.01_60/ts_133501v171101p.pdf
[45] M. Flores Marín, L. Benavides Castillo, F. G. Martinez Coca, y S. Cherrez, "Análisis Técnico del Sistema de Transmisión de Televisión Digital Terrestre en Guayaquil". 2019. [En línea]. Disponible en: https://revistas.uees.edu.ec/index.php/IRR
[46] J. A. Galarza Agual, "Diseño de instalación técnica de producción y transmisión audio-video para un canal de televisión, basado en estándar ISDB-Tb de televisión digital terrestre.", bachelorThesis, Quito: Universidad de las Américas, 2017, 2017. Consultado: el 2 de diciembre de 2025. [En línea]. Disponible en: http://dspace.udla.edu.ec/handle/33000/8317
[47] Google, "Widevine DRM Architecture Overview". 2017. Consultado: el 2 de diciembre de 2025. [En línea]. Disponible en: https://www.whymatematica.com/wp-content/uploads/2018/08/Widevine_DRM_Architecture_Overview.pdf
[48] "Enhanced Content Protection - Microsoft PlayReady". Consultado: el 2 de diciembre de 2025. [En línea]. Disponible en: https://www.microsoft.com/playready/features/EnhancedContentProtection/
[49] "FairPlay Streaming - Apple Developer". Consultado: el 2 de diciembre de 2025. [En línea]. Disponible en: https://developer.apple.com/streaming/fps/
[50] N. T. Blog, "Protecting Netflix Viewing Privacy at Scale", Medium. Consultado: el 2 de diciembre de 2025. [En línea]. Disponible en: https://netflixtechblog.com/protecting-netflix-viewing-privacy-at-scale-39c675d88f45
[51] "Manage two-step verification (2SV) for your account". Consultado: el 2 de diciembre de 2025. [En línea]. Disponible en: https://help.aconex.com/lobby/manage-two-step-verification-2sv-for-your-account/
[52] "State of the Internet Reports | Security Research | Akamai". Consultado: el 2 de diciembre de 2025. [En línea]. Disponible en: https://www.akamai.com/security-research/the-state-of-the-internet
[53] MINTEL, "PROCESO DE IMPLEMENTACIÓN DE LA TELEVISIÓN DIGITAL EN EL ECUADOR". Consultado: el 2 de diciembre de 2025. [En línea]. Disponible en: https://www.telecomunicaciones.gob.ec/wp-

content/uploads/downloads/2015/02/PRESENTACIO%CC%81N_TDT_MINTEL-Febrero-2015.pdf

[54] A. F. Coro Luzuriaga y D. F. Cruz Palaquibay, “DISEÑO DE UN PLAN DE ACCIÓN PARA LA IMPLEMENTACIÓN LA TELEVISIÓN DIGITAL BASADA EN LA TECNOLOGÍA IPTV EN EL ECUADOR”, 2016.

[55] UIT, “H.702 : Perfiles de accesibilidad para los sistemas de TVIP”. Consultado: el 2 de diciembre de 2025. [En línea]. Disponible en: https://www.itu.int/rec/T-REC-H.702-202008-I/es

[56] “¿Qué es la verificación en dos pasos? - Servicio al Cliente de Amazon”. Consultado: el 2 de diciembre de 2025. [En línea]. Disponible en: https://www.amazon.com/gp/help/customer/display.html?nodeId=G3PWZPU52FKN7PW4

[57] “Protecting the Bank of OTT”, Akamai. Consultado: el 2 de diciembre de 2025. [En línea]. Disponible en: https://www.akamai.com/resources/product-brief/protecting-the-bank-of-ott

[58] V. Maino Isaías, F. Chang calvache, D. Hurtado, y V. Palacios, “Agenda-transformacion-digital-2022-2025”. Ministerio de Telecomunicaciones y Sociedad de la Información, 2022. Consultado: el 2 de diciembre de 2025. [En línea]. Disponible en: https://www.arcotel.gob.ec/wp-content/uploads/2022/08/Agenda-transformacion-digital-2022-2025.pdf