LINEAMIENTOS DE FILTRADO WEBCUMPLIMIENTO CONTROL 8.23 (FILTRADO WEB)

Sistema de Gestión de Seguridad de la Información
Secretaría de Educación Del Distrito

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE EDUCACIÓN
BOGOTÁ

Versión 1.0
Junio 2026

Tabla de Contenido

Índice de Tablas

GLOSARIO

AV (Anti-Virus): es un programa informático diseñado para detectar, prevenir y eliminar software malicioso (malware) de dispositivos electrónicos, como ordenadores, servidores y teléfonos móviles.

Abortion / Aborto: Sitios web sobre datos, información, cuestiones jurídicas y organizaciones relacionadas con el aborto.

Advertising / Publicidad: Sitios que proporcionan gráficos publicitarios u otros archivos de contenido publicitario, incluidos los servidores de anuncios (nombre de dominio a menudo con «ad.», como ad.yahoo.com). Si un sitio es principalmente para transacciones en línea, se clasifica como Compras y Subastas. Incluye los programas de pago por navegar y de publicidad afiliada.

Advocacy Organizations / Organizaciones de defensa: Esta categoría engloba a las organizaciones que hacen campaña o ejercen presión en favor de una causa sensibilizando a la opinión pública, recabando apoyos, influyendo en las políticas públicas, etc.

Alcohol: Sitios web que promocionan o venden legalmente productos y accesorios relacionados con el alcohol.

Alternative Beliefs / Creencias alternativas: Sitios web que proporcionan información sobre o promueven creencias espirituales no incluidas en Religión Global, u otras creencias y prácticas no convencionales o folclóricas, incluyendo, pero sin limitarse a sitios que promueven u ofrecen métodos, medios de instrucción u otros recursos para afectar o influir en hechos reales mediante el uso de hechizos, maldiciones, poderes mágicos, satánicos o seres sobrenaturales.

Aplication Control / Control de aplicaciones: capa de seguridad basada en software que aplica una lista explícita de software que se permite ejecutar en un equipo.

Armed Forces / Fuerzas Armadas: Sitios web relacionados con fuerzas armadas y militares organizadas, excluidas las organizaciones civiles y militares extremas.

Artificial Intelligence Technology / Tecnología de Inteligencia Artificial: Sitios que ofrecen soluciones, conocimientos y recursos relacionados con la inteligencia artificial (IA), como el aprendizaje automático, el procesamiento del lenguaje natural, la visión por ordenador, la robótica, etc. Estos sitios pueden ofrecer productos, plataformas, herramientas, cursos, artículos de investigación o noticias basados en la IA.

Arts and Culture / Arte y Cultura: Sitios web dedicados a las bellas artes, comportamientos y antecedentes culturales, incluidas convenciones, obras de arte y pintura, música, idiomas, costumbres, etc. También incluye instituciones como museos, bibliotecas y sitios históricos. Sitios que promueven el patrimonio histórico y cultural de una zona determinada, pero no promocionan viajes a propósito.

Auction / Subasta: Sitios web que ofrecen promoción o venta en línea de bienes y servicios generales como electrónica, flores, joyas, música, etc., excluidos los bienes inmuebles. También incluye servicios de subastas en línea como eBay, Amazon, Priceline.

Brokerage and Trading / Corretaje y comercio: Sitios que apoyan el comercio activo de valores y la gestión de inversiones. Los intermediarios inmobiliarios no se incluyen en esta categoría, sino en la de compras y subastas. Los sitios que proporcionan información/anuncios sobre proveedores y compradores tampoco se aplican aquí, ya que no realizan actividades comerciales.

Business / Negocios: Sitios patrocinados o dedicados a empresas, asociaciones empresariales, grupos industriales o empresas en general. Las empresas de tecnología de la información están excluidas de esta categoría y se incluyen en Tecnología de la información.

Categorías web: sistema de organización de contenidos en una página web que se basa en temas, formatos u otras pautas.

Charitable Organizations / Organizaciones benéficas: Sitios para organizaciones cuya misión sirve a un fin público y son de naturaleza filantrópica. Esta categoría excluye a las organizaciones de defensa o políticas.

Child Education / Educación infantil: Sitios web desarrollados para niños de 12 años o menos. Incluye juegos educativos, herramientas, organizaciones y escuelas. Tenga en cuenta que los hospitales infantiles están clasificados como Salud.

Child Sexual Abuse / Abuso sexual infantil: Sitios web que, según ha comprobado la Internet Watch Foundation, contienen o distribuyen imágenes de niños no adultos que aparecen en estado de abuso.

Content Servers / Servidores de contenidos: Sitios web que alojan servidores que distribuyen contenidos para los sitios web suscritos. Incluye servidores de imágenes y web.

Crypto Mining / Minería de criptomonedas: Sitios que proporcionan herramientas de minería de criptomonedas, pools de minería, agrupación de recursos por mineros, que comparten su potencia de procesamiento a través de una red, para repartirse la recompensa a partes iguales, según la cantidad de trabajo que hayan aportado a la probabilidad de encontrar un bloque.

Cryptocurrency / Criptomoneda: Sitios especializados en monedas digitales o virtuales protegidas por criptografía y que operan en redes descentralizadas. Estos sitios pueden ofrecer servicios e información para comerciar, invertir, minar, almacenar o aprender sobre criptomonedas. Excluya los sitios web de servicios financieros convencionales que sólo mencionan las criptodivisas como una de sus opciones.

Dating / Citas: Sitios web que permiten a las personas ponerse en contacto y comunicarse entre sí a través de Internet, normalmente con el objetivo de desarrollar una relación personal, romántica o sexual.

Digital Postcards / Postales digitales: Sitios para enviar/ver postales digitales.

Discrimination / Discriminación: Sitios que promueven la identificación de grupos raciales, la denigración o el sometimiento de grupos, o la superioridad de cualquier grupo.

Domain Parking / Aparcamiento de dominios: Sitios que simplemente son titulares de dominios sin contenido significativo.

Drug Abuse / Abuso de Drogas: Sitios web que ofrecen información sobre actividades relacionadas con drogas ilegales, como la promoción, preparación, cultivo, tráfico, distribución, captación, etc. de drogas.

Dynamic Content / Contenido Dinámico: URL generadas dinámicamente por un servidor web.

Dynamic DNS / DNS Dinámicos: Sitios que utilizan servicios DNS dinámicos para asignar un Nombre de Dominio Completamente Cualificado (FQDN) a una dirección IP específica o a un conjunto de direcciones bajo el control del propietario del sitio; a menudo se utilizan en ciberataques y servidores de mando y control de botnets.

Education / Educación: Instituciones educativas: Sitios patrocinados por escuelas, otros centros educativos e instituciones de investigación no académicas, y sitios relacionados con eventos y actividades educativas. Materiales educativos: Sitios que proporcionan información sobre materiales

curriculares, los venden o los ofrecen. Sitios que dirigen la instrucción, así como revistas académicas y publicaciones similares donde académicos y profesores envían artículos académicos/de investigación.

Entertainment / Entretenimiento: Sitios que informan o promocionan películas, radio y televisión no informativas, música y guías de programación, libros, humor, cómics, cines, galerías, artistas o crítica sobre entretenimiento, y revistas. Incluye sitios de libros que tienen un sabor personal o material extra de los autores para promocionar los libros.

Explicit Violence / Violencia Explicita: Esta categoría incluye sitios que muestran material ofensivo sobre brutalidad, muerte, crueldad, actos de abuso, mutilación, etc.

Extremist Groups / Grupos Extremistas: Sitios en los que aparecen grupos o movimientos de milicias radicales con convicciones o creencias agresivas contra el gobierno.

File Sharing and Storage / Compartir y almacenar archivos: Sitios web que permiten a los usuarios utilizar servidores de Internet para almacenar archivos personales o para compartirlos, por ejemplo, con fotos.

Finance and Banking / Finanzas y banca: Datos y servicios financieros -- Sitios que ofrecen noticias y cotizaciones sobre acciones, bonos y otros instrumentos de inversión, asesoramiento sobre inversiones, pero no negociación en línea. Incluye bancos, cooperativas de crédito, tarjetas de crédito y seguros. Los corredores de hipotecas/seguros se aplican aquí en contraposición a Corretaje y Comercio.

Folklore / Folclore: Ovnis, adivinación, horóscopos, fen shui, quiromancia, tarot e historias de fantasmas.

Freeware and Software Downloads / Descargas de freeware y software: Sitios cuya función principal es ofrecer descargas gratuitas de software y programas informáticos. En esta categoría se incluyen tonos/imágenes/juegos para móviles, actualizaciones de programas informáticos de descarga gratuita.

Gambling / Juego: Sitios dedicados a actividades de juego como apuestas, loterías y casinos, que incluyen información, instrucciones y estadísticas sobre el juego.

Games / Juegos: Sitios que informan o promocionan juegos electrónicos, videojuegos, juegos de ordenador, juegos de rol o juegos en línea. Incluye sorteos y regalos. Los juegos deportivos no se incluyen en esta categoría, pero sí los sitios de juegos matemáticos que consumen mucho tiempo y tienen escasa finalidad educativa.

General Organizations / Organizaciones generales: Sitios que atienden a grupos, clubes u organizaciones de individuos con intereses similares, ya sean de naturaleza profesional, social, humanitaria o recreativa. Organizaciones sociales y de afiliación: Sitios patrocinados por lo que apoyan u ofrecen información sobre organizaciones dedicadas principalmente a la socialización o a intereses comunes distintos de la filantropía o la promoción profesional. No confundir con Grupos de Defensa y Grupos Políticos.

Global Religion / Religión mundial: Sitios que proporcionan información o promueven creencias espirituales mundiales con un número significativo de seguidores, como el budismo, el bahaísmo, el cristianismo, la ciencia cristiana, el hinduismo, el islamismo, el judaísmo, el mormonismo, el sintoísmo y el sijismo, así como el ateísmo.

Government and Legal Organizations / Organizaciones gubernamentales y jurídicas: Gobierno: Sitios patrocinados por ramas, oficinas o agencias de cualquier nivel de gobierno, excepto las fuerzas armadas, incluidos tribunales, instituciones policiales, instituciones gubernamentales a

nivel de ciudad. Organizaciones legales: Sitios que discuten o explican leyes de diversas entidades gubernamentales.

Hacking / Hackear: Sitios web que describen actividades ilícitas en torno a la modificación o el acceso no autorizados a programas, ordenadores, equipos y sitios web.

Health and Wellness / Salud y bienestar: Sitios que ofrecen información o asesoramiento sobre salud personal o servicios médicos, procedimientos o dispositivos, pero no medicamentos. Incluye grupos de autoayuda. Esta categoría incluye proveedores de cirugía estética, hospitales infantiles, pero no sitios de atención médica para mascotas, que entran en Sociedad y Estilo de vida.

Illegal or Unethical / Ilegal o poco ético: Sitios web que ofrecen información, métodos o instrucciones sobre acciones fraudulentas o conductas ilícitas (no violentas) como estafas, falsificaciones, evasión fiscal, pequeños hurtos, chantaje, etc.

Information and Computer Security / Seguridad informática y de la información: Sitios que proporcionan información o herramientas de descarga gratuita para la seguridad informática, pero no para la descarga ordinaria de freeware y software.

Information Technology / Tecnologías de la información: Periféricos y servicios de tecnologías de la información, servicios de telefonía móvil, proveedores de televisión por cable/Internet.

Instant Messaging / Mensajería instantánea: Sitios que permiten a los usuarios comunicarse en tiempo real a través de Internet.

Internet Radio and TV / Internet Radio y TV: Sitios web que emiten comunicaciones de radio o televisión por Internet.

Internet Telephony / Telefonía por Internet: Sitios web que permiten las comunicaciones telefónicas a través de Internet.

Job Search / Búsqueda de Trabajo: Sitios que ofrecen información o apoyan la búsqueda de empleo o empleados. Incluye agentes de carrera y servicios de consultoría que ofrecen ofertas de empleo.

Lingerie and Swimsui / Lencería y bañadores: Sitios web que utilizan imágenes de modelos semidesnudas en lencería, ropa interior y trajes de baño con el fin de vender o promocionar dichos artículos.

Malicious Websites / Sitios Web Maliciosos: Sitios que alojan software que se descarga de forma encubierta en la máquina de un usuario para recopilar información y controlar su actividad, y sitios infectados con software destructivo o malicioso, diseñado específicamente para dañar, perturbar, atacar o manipular sistemas informáticos sin el consentimiento del usuario, como virus o troyanos.

Marijuana / Marihuana: Sitios que proporcionan información o promueven el cultivo, la preparación o el consumo de marihuana.

Meaningless Content / Contenido sin sentido: En esta categoría se incluyen las URL que no pueden clasificarse definitivamente debido a la falta de contenido o a la ambigüedad de éste.

Medicine / Medicina: Medicamentos prescritos: Sitios que ofrecen información sobre medicamentos aprobados y su uso médico. Suplementos y compuestos no regulados: Sitios que proporcionan información sobre o promueven la venta o el uso de sustancias químicas no reguladas por la FDA (como compuestos de origen natural). Esta categoría incluye los sitios de compra de medicamentos en línea, ya que se trata de una categoría sensible separada de la compra habitual.

Newly Observed Domain / Dominio recién observado: Dominios recién configurados o activos, pero no necesariamente recién registrados.

Newly Registered Domain / Dominio recién registrado: Dominios registrados muy recientemente.

News and Media / Noticias y medios de comunicación: Sitios que ofrecen noticias de actualidad y opinión, incluidos los patrocinados por periódicos, revistas de circulación general u otros medios de comunicación. Esta categoría incluye los sitios de televisión y radio, siempre que no sean exclusivamente de entretenimiento, pero excluye las revistas académicas. Revistas alternativas: Equivalentes en línea a los tabloides de los supermercados y otras publicaciones marginales.

Newsgroups and Message Boards / Grupos de noticias y tablones de anuncios: Sitios para clubes personales y empresariales en línea, grupos de debate, tablones de mensajes y servidores de listas; incluye «blogs» y «revistas por correo».

NGFW (Next-Generation Firewall): dispositivo de seguridad de red que evoluciona más allá de los cortafuegos tradicionales. Combina filtrado de tráfico estándar con inspección profunda de paquetes, control basado en aplicaciones, prevención de intrusiones integrada e inteligencia de amenazas en tiempo real para bloquear ataques complejos.

Nudity and Risque / Desnudez y riesgo: Sitios web de contenido adulto (mayores de 18 años) que muestran el cuerpo humano en desnudez total o parcial sin intención de excitar sexualmente.

Online Meeting / Reuniones en Línea: Sitios que permiten celebrar reuniones, compartir pantallas y colaborar en documentos a través de Internet.

Other Adult Materials / Otros Materiales para Adulto: Sitios web de contenido maduro (mayores de 18 años) que presentan o promueven la sexualidad, clubes de striptease, sex shops, etc., excluida la educación sexual, sin intención de excitar sexualmente.

Peer-to-peer File Sharing / Compartir archivos entre iguales: Sitios web que permiten a los usuarios compartir archivos y almacenamiento de datos entre sí.

Perfil Application Control: Definición de alcance en el proceso de evaluación de aplicaciones web.

Perfil AV: Definición de alcance en el proceso de evaluación de firmas de virus informáticos.

Personal Privacy / Privacidad personal: Sitios que ofrecen servicios de banca en línea, comercio, atención sanitaria y otros que contienen información personal sobre privacidad.

Personal Vehicles / Vehículos personales: Sitios web que contienen información sobre el uso privado o la venta de automóviles, barcos, aviones, motocicletas, etc., incluidas piezas y accesorios.

Personal Websites and Blogs / Sitios web y blogs personales: Páginas web privadas que alojan información personal, opiniones e ideas de sus propietarios.

Phishing / Suplantación: Páginas web falsificadas que duplican páginas web comerciales legítimas con el fin de obtener información financiera, personal u otra información privada de los usuarios.

Plagiarism / Plagio: Sitios web que proporcionan, distribuyen o venden redacciones, proyectos o diplomas escolares.

Política WEB: Conjunto definido de acciones a tomar (permitir, denegar o monitorear) sobre un grupo de categorías web.

Political Organizations / Organizaciones políticas: Sitios patrocinados o que ofrecen información

sobre partidos políticos y grupos de interés centrados en elecciones o legislación. No debe confundirse con organizaciones gubernamentales y jurídicas, ni con grupos de defensa.

Pornography / Pornografía: Sitios web de contenido maduro (mayores de 18 años) que presentan o muestran actos sexuales con la intención de excitar y excitar sexualmente.

Potentially Unwanted Program / Programa potencialmente no deseado: Sitios que utilizan tecnologías que alteran el funcionamiento del hardware, software o red de un usuario de forma que disminuye el control sobre la experiencia del usuario, la privacidad o la recopilación y distribución de información personal, incluidos adware, spyware, secuestradores de navegadores, ventanas emergentes no deseadas y dominios de «typo-squatting».

Proxy Avoidance / Evitar la delegación: Sitios web que proporcionan información o herramientas sobre cómo eludir los controles de acceso a Internet y navegar por la Red de forma anónima, incluidos los servidores proxy anónimos.

Real Estate / Inmobiliario: Sitios web que promueven la venta o el alquiler de propiedades inmobiliarias.

Reference / Referencia: Sitios web que proporcionan datos de referencia generales en forma de bibliotecas, diccionarios, tesauros, enciclopedias, mapas, directorios, normas, etc.

Remote Access / Acceso Remoto: Sitios que facilitan el acceso autorizado y el uso de ordenadores o redes privadas a distancia a través de Internet.

Restaurant and Dining / Restaurantes y Cenas: Sitios web relacionados con restaurantes y cenas, incluye ubicaciones, reseñas gastronómicas, recetas, servicios de catering, etc.

Search Engines and Portals / Motores de Búsqueda y Portales: Sitios que apoyan la búsqueda en la Web, grupos de noticias o índices/directorios. Sin embargo, los sitios de motores de búsqueda que proporcionan información exclusivamente para comprar o comparar precios entran en la categoría de Compras y Subastas.

Secure Websites / Sitios web seguros: Sitios que instituyen medidas de seguridad como autenticación, contraseñas, registro, etc.

Sex Education / Educación Sexual: Sitios web educativos que proporcionan información o hablan de sexo y sexualidad, sin utilizar material pornográfico.

SGSI (Sistema de Gestión de Seguridad de la Información): enfoque sistemático, documentado y basado en riesgos que utilizan las organizaciones para establecer, implementar, operar, monitorear y mejorar su seguridad. Su objetivo es proteger los activos de información garantizando su confidencialidad, integridad y disponibilidad.

Shopping / Compras: Sitios web que ofrecen promoción o venta en línea de bienes y servicios generales como electrónica, flores, joyas, música, etc., excluidos los bienes inmuebles. También incluye servicios de subastas en línea como eBay, Amazon, Priceline.

Social Networking / Redes Sociales: Un sitio de redes sociales es una plataforma para construir redes sociales o relaciones sociales entre personas que comparten intereses, actividades, antecedentes o conexiones en la vida real similares. Un servicio de red social consta de una representación de cada usuario (a menudo un perfil), sus enlaces sociales y una variedad de servicios adicionales. Los sitios de redes sociales son servicios basados en la web que permiten a los individuos crear un perfil público, crear una lista de usuarios con los que compartir conexiones, y ver y cruzar las conexiones dentro del sistema.

Society and Lifestyles / Sociedad y estilos de vida: Esta categoría contiene sitios que tratan temas y preferencias de la vida cotidiana, como aficiones pasivas (jardinería, filatelia, mascotas), diarios, blogs, etc.

Spam URLs / URL spam: Sitios o páginas web cuyas URL se encuentran en correos electrónicos de spam. Estas páginas suelen anunciar sitios de sexo, productos fraudulentos y otros materiales potencialmente ofensivos.

Sports / Deportes: Incluye sitios relacionados con deportes recreativos y aficiones activas como pesca, caza, footing, piragüismo, tiro con arco, ajedrez, así como deportes organizados, profesionales y de competición.

Sports Hunting and War Games / Caza deportiva y juegos de guerra: Páginas web sobre caza deportiva, juegos de guerra, instalaciones de paintball, etc. Incluye todos los clubes, organizaciones y grupos relacionados.

Streaming Media and Download / Streaming multimedia y descargas: Sitios web que permiten la descarga de MP3 u otros archivos multimedia.

Terrorism / Terrorismo: Sitios web con contenidos que muestren actos relacionados con el terrorismo que sean, o parezcan ser, ilegales en la jurisdicción del autor de la clasificación, o sitios que inciten ilegalmente a la captación de individuos para organizaciones terroristas.

Tobacco / Tabaco: Sitios web que promocionan o venden legalmente productos y accesorios del tabaco, incluidos todos los tipos de cigarrillos electrónicos y vapes.

Travel / Viaje: Los sitios web de esta categoría ofrecen recursos relacionados con los viajes, como alojamientos, transportes (ferrocarril, líneas aéreas, cruceros), agencias, lugares de vacaciones, atracciones turísticas, avisos, etc.

URL Shortening / Acortamiento de URL: Sitios que prestan servicios de acortamiento de URL, lo que hace que una URL sea sustancialmente más corta y siga dirigiendo a la página requerida.

Weapons (Sales) / Armas (Ventas): Sitios web que promocionan o venden legalmente armas como pistolas, cuchillos, rifles, explosivos, etc.

Web Analytics / Analítica web: Sitios que se utilizan para recopilar y evaluar datos de tráfico web.

Web Chat / Chat en Internet: Sitios que alojan servicios de chat en la Web, o que admiten o proporcionan información sobre chat a través de HTTP o IRC.

Web Hosting / Alojamiento web: Sitios de organizaciones que prestan servicios de alojamiento, o páginas de dominio de primer nivel de comunidades Web.

Web-based Applications / Aplicaciones web: Sitios que imitan las aplicaciones de escritorio, como procesadores de texto, hojas de cálculo y presentaciones de diapositivas.

Web-based Email / Correo electrónico basado en web: Sitios que permiten a los usuarios utilizar servicios de correo electrónico.

1. JUSTIFICACIÓN

La Secretaría de Educación del Distrito implementa esta política para mitigar riesgos de seguridad, garantizar la protección de datos personales de menores (Ley 2489 de 2025) y optimizar el uso de los recursos tecnológicos. Se adopta un enfoque de Seguridad Proactiva, donde la navegación es una herramienta estrictamente institucional y pedagógica.

1.1 Marco de implementación en el MSPI de la SED:

Estos lienamientos se implementan en el marco del Modelo de Seguridad y Privacidad de la Información (MSPI) de la Secretaría de Educación del Distrito, específicamente dentro de las fases de Iniciación y Protección, bajo el eje de Implementación de Controles, conforme a los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y el Modelo de Gestión de Seguridad y Privacidad de la Información para entidades del Estado colombiano.

2. OBJETIVO

Establecer los lineamientos técnicos, jurídicos y administrativos para el control y filtrado del acceso a contenidos web desde la infraestructura tecnológica de la Secretaría de Educación del Distrito, garantizando:

- La protección de la información institucional.
- La protección reforzada de niños, niñas y adolescentes.
- El cumplimiento de la normativa nacional en materia de protección de datos personales.
- La preservación de la confidencialidad, integridad y disponibilidad de la información.

3. ALCANCE

Aplica a:

- Funcionarios
- Contratistas
- Docentes
- Personal administrativo
- Estudiantes
- Usuarios con acceso a la red institucional (alámbrica, inalámbrica y VPN)

Incluye:

- Navegación web
- Aplicaciones basadas en Internet
- Plataformas en la nube
- Redes sociales
- Servicios de mensajería y colaboración

4. MARCO NORMATIVO

- ISO/IEC 27001:2022 – Control 8.23 (Filtrado Web)
- ISO/IEC 27002 – Directrices de implementación
- Ley 1581 de 2012 – Protección de datos personales
- Ley 1098 de 2006 – Protección al menor
- Ley 2489 de 2025 y Decreto de 2026

- Política de Seguridad de la Información de la entidad

5. PRINCIPIOS RECTORES

- Interés superior del menor. Constitución, art. 44; Ley 1098 de 2006.
- Protección de datos personales. Constitución, art. 15; Ley 1581 de 2012; Ley 1266 de 2008; Decreto 1377 de 2013.
- Minimización del riesgo tecnológico. Ley 1341 de 2009; lineamientos de Gobierno Digital; normas de gestión del riesgo tecnológico y seguridad digital.
- Uso adecuado de recursos tecnológicos. Ley 1341 de 2009; lineamientos TIC del Estado; políticas internas de uso aceptable.
- Proporcionalidad en la restricción de acceso. Ley 1581 de 2012; Constitución, art. 15.
- La protección de los niños, niñas y adolescentes en entornos digitales es una responsabilidad compartida que vincula a todos los actores de la comunidad educativa y del ecosistema digital. La Secretaría de Educación del Distrito, como garante del derecho a la educación y de la protección de datos de menores, implementará controles técnicos de filtrado web y monitoreo en su infraestructura. Sin embargo, estos controles no son suficientes por sí mismos. La corresponsabilidad exige la participación activa de las familias, los docentes, los directivos docentes, los contratistas y los operadores de red (ISP, proveedores de servicios en la nube, plataformas educativas, entre otros) en la construcción de entornos digitales seguros, en el marco del interés superior del menor y su desarrollo integral.

6. CLASIFICACIÓN DE PERFILES

6.1. Usuario Estándar

Enfoque:
Productividad y cumplimiento misional.

Permitido:

- Sitios educativos.
- Plataformas institucionales.
- Acceso a redes sociales según lo definido en la Matriz de Control Filtrado WEB (Tabla 2) y Matriz de Control de Aplicaciones (Tabla 1).

Restringido o Bloqueado:

- Streaming no misional.
- Descargas P2P.
- Almacenamiento en nube no autorizado.
- Herramientas de anonimización.
- Control remoto no autorizado.
- Sitios que impliquen fuga de información.
- herramientas de evasión de seguridad (VPN/Proxy).

6.2. Usuario VIP

Enfoque:
Facilitar gestión directiva y representación institucional.

Permitido:

- Según lo definido en la matriz.
- Herramientas de colaboración.

- Plataformas multimedia.

Siempre Bloqueado:

- Malware.
- Botnets.
- Anonymizers.
- P2P.
- Cripto minería.
- Remote access no institucional.

6.3. Usuario Colegios

Enfoque:
Entorno educativo seguro y blindaje contra contenido nocivo.

Permitido:

- Contenido pedagógico.
- Plataformas institucionales.
- Plataformas educativas autorizadas
- Redes sociales con funciones limitadas (según configuración técnica definida).

Bloqueo obligatorio:

- Contenido adulto.
- Juegos de azar.
- Violencia explícita.
- Drogas.
- Redes sociales abiertas.
- Chats públicos.
- Streaming recreativo.
- VPN públicas.
- Proxy avoidance.
- Nube pública no institucional.

6.4. Asignación de Perfiles y Mecanismo de Autenticación

La asignación del perfil de filtrado web se realizará según la capacidad tecnológica de cada sede o dependencia, diferenciando entre Nivel Central (con infraestructura de directorio) y Colegios / DLE (sin directorio centralizado).

6.4.1. Nivel Central (SED Central)

El filtrado se realizará mediante autenticación integrada al Directorio Activo (DA) institucional o al sistema de identidad central de la Entidad, garantizando la interoperabilidad con el Sistema de Gestión de Identidades y Accesos (IAM) que la Secretaría de Educación del Distrito está implementando para dar cumplimiento a los controles de acceso lógico establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI) y en la Política de Seguridad de la Información de la Entidad.

Queda prohibido el filtrado por IP estática o por red en esta sede.

6.4.2. Colegios y Direcciones Locales de Educación (DLE)

Dada la ausencia de infraestructura LDAP o gestor de usuarios centralizado en estas sedes, la asignación de perfiles se realizará mediante reglas basadas en segmentos de red (VLANs) o rangos de IP.

6.5. Criterios de Pertenencia por Perfil

Tabla 1 Criterios de Pertenencia por Perfil

Perfil	Aplica a	Método de Asignación
Perfil Estándar	Funcionarios, contratistas, docentes y personal administrativo de la SED Central que no pertenezcan al perfil VIP. Perfil por defecto en Nivel Central.	Autenticación DA en SED Central. No aplica en colegios.
Perfil VIP	Exclusivamente a: (a) Despacho de la Secretaría de Educación, (b) Directores y Subdirectores de Oficina, (c) Oficina de Comunicaciones y Prensa, (d) Jefes de Área.	Autenticación DA en SED Central. Requiere solicitud formal y renovación anual. No aplica en colegios ni DLE.
Perfil Colegios	Todos los usuarios en sedes educativas (estudiantes, docentes, rectores, administrativos) sin distinción de roles.	Asignación por VLAN o rango de IP en cada colegio o DLE. Es el perfil único para estas sedes.
Perfil Invitado / BYOD	Dispositivos no gestionados por la Entidad y visitantes en sede Nivel Central.	Portal cautivo con aceptación de términos de uso. Es el perfil más restrictivo.

6.6. Restricciones Adicionales por Perfil

Tabla 2 Restricciones Adicionales por Perfil

Perfil	Restricciones Específicas
Perfil Colegios	Entorno educativo seguro. Bloqueo de: contenido adulto, juegos de azar, violencia explícita, drogas, redes sociales abiertas, chats públicos, streaming recreativo, VPN públicas, proxy avoidance, nube pública no institucional.
Perfil Invitado / BYOD	Todas las restricciones del perfil "Colegios", más el bloqueo de: webmail externo (Gmail, Hotmail, Outlook.com, Yahoo Mail, etc.), servicios de almacenamiento en la nube (Dropbox, Mega, MediaFire, etc.), y cualquier funcionalidad de subida/upload de archivos a servicios no institucionales.

6.7. Excepciones para Pruebas Piloto o Concepto

Para proyectos de prueba que requieran desviaciones temporales de estos lineamientos, se habilitará un mecanismo de excepción controlada:

- Duración máxima: 30 días calendario, prorrogable una sola vez por 15 días adicionales.
- Alcance: Restringido a un grupo específico de usuarios (máximo 10) o a una sede piloto.
- Aprobación: Requiere visto bueno de la Oficina de Tecnología y de Seguridad de la

Información.
- Prohibición: No se concederán excepciones para contenido de las categorías "Potentially Liable" (abuso infantil, terrorismo, etc.) ni "Adult/Mature" (pornografía, etc.).

7. CATEGORÍAS DE BLOQUEO GENERAL Y OBLIGATORIO

Las categorías relacionadas a continuación hacen parte de los perfiles no autorizados por la entidad:

1. Malware y phishing.
2. Botnet.
3. Proxy avoidance.
4. VPN públicas.
5. Peer-to-peer.
6. Remote control no autorizado.
7. Gambling.
8. Adult content.
9. Crypto mining.
10. File sharing no autorizado.

Justificación:
Protección de la confidencialidad, integridad y disponibilidad.

8. CATEGORÍAS EN MONITOREO GENERAL

- Business no misional.
- Cloud storage externo.
- Plataformas colaborativas no institucionales.
- Se aplicarán las acciones (Permitir/Bloquear/Monitorear) definidas en la Tabla 2 para cada perfil.

Se aplicarán controles de:
- Inspección SSL.
- Registro de eventos.
- Alertamiento.

9. APLICACIONES Y CATEGORIAS WEB BLOQUEADAS

En cumplimiento del Control 8.23 (Filtrado Web) y para garantizar la integridad, disponibilidad y confidencialidad de la red institucional, se establece el bloqueo total de las categorías lógicas de aplicaciones detalladas a continuación para TODOS los perfiles (Estándar, VIP y Colegios), sin excepción, a menos que medie una autorización expresa por parte de Seguridad de la Información con justificación técnica o pedagógica validada.

3La actualización de esta lista estará a cargo de la Oficina de Tecnología (OTIC). El Anexo A del presente documento contiene un listado ilustrativo de aplicaciones específicas que ejemplifican estas categorías, sin que dicho listado tenga carácter taxativo.

- ✓ Aplicaciones de Descarga P2P y Torrent (Riesgo de malware y saturación de red)

BitTorrent, uTorrent, Vuze, Transmission, qBittorrent, Deluge, Tixati, rTorrent, Halite, BitComet, FrostWire, Tribler, PeerBlock, Popcorn Time.

- ✓ Aplicaciones de Anonimización, Proxy y VPN (Evasión de controles)

Tor Browser, Tails, Whonix, I2P, Freenet, Psiphon, Ultrasurf, Hotspot Shield, TunnelBear, Windscribe, ProtonVPN, CyberGhost, Hide.me, NordVPN, ExpressVPN, SoftEther VPN, OpenVPN.

- ✓ Aplicaciones de Mensajería Instantánea y Chat no institucional (Riesgo de fuga de información y distracción)

Telegram, Signal, Line, Viber, WeChat, Snapchat, Discord, Slack, ICQ, IRC clients, Trillian, Pidgin, Miranda IM.

- ✓ Aplicaciones de Streaming y Multimedia (Consumo de ancho de banda)

Netflix, Hulu, Amazon Prime Video, Disney+, HBO Max, Paramount+, YouTube (solo se permite para fines pedagógicos, con monitoreo activo), Twitch, Spotify, Apple Music, Deezer, Tidal, SoundCloud, Vimeo (monitorear), Kodi, Plex.

- ✓ Aplicaciones de Almacenamiento en la Nube no autorizado (Fuga de datos)

Dropbox, OneDrive (solo permitido el institucional), Box, Mega, pCloud, Sync.com, Tresorit, MediaFire, 4Shared, WeTransfer, SendAnywhere.

- ✓ Aplicaciones de Control Remoto y Acceso no institucional (Riesgo de acceso no autorizado)

TeamViewer, AnyDesk, LogMeIn, VNC, RDP (excepto acceso a servidores institucionales), Chrome Remote Desktop, Splashtop, GoToMyPC, UltraVNC, TightVNC, RealVNC, Ammyy Admin, Remote Utilities.

- ✓ Aplicaciones de Juegos y entretenimiento (No misionales)

Steam, Epic Games Store, Origin, Uplay, GOG Galaxy, Battle.net, Roblox, Minecraft (solo permitido si se usa versión educativa), Fortnite, League of Legends, World of Warcraft, Xbox Live, PlayStation Network, Nintendo eShop, Discord (categoría juegos).

- ✓ Aplicaciones de Minería de Criptomonedas (Riesgo de seguridad y recursos).

CGMiner, BFGMiner, EasyMiner, NiceHash, MinerGate, Claymore, Ethminer, PhoenixMiner, TeamRedMiner, T-Rex, XMRig.

- ✓ Otras aplicaciones de alto riesgo

- Herramientas de hacking: Nmap, Wireshark (solo para TI), Metasploit, Aircrack-ng, John the Ripper, Hydra, Burp Suite (excepto TI), Cain & Abel, Ettercap, Kismet, Reaver.
- Clientes FTP no institucionales: FileZilla, WinSCP (solo para TI autorizado), Cyberduck.
- Aplicaciones de eDonkey, Gnutella, Soulseek, Ares Galaxy, Shareaza.

9.1. Matriz de Control de Aplicaciones (Application Control)

A continuación, se define la acción por tipo de aplicación:

Tabla 3 Matriz de Control Filtrado por Aplicación

Categoría	Perfil		
	Estándar	VIP	Colegios
Botnet	Bloquear	Bloquear	Bloquear
Business	Monitorear	Monitorear	Monitorear
Cloud.IT	Monitorear	Monitorear	Monitorear

Categoría	Perfil		
	Estándar	VIP	Colegios
Collaboration	Bloquear (excepto Teams, zoom y correo institucional)	Bloquear (excepto Teams, zoom y correo institucional)	Bloquear (excepto Teams y correo institucional)
Email	Bloquear (excepto correo institucional)	Bloquear (excepto correo institucional)	Bloquear (excepto correo institucional)
File.Sharing	Bloquear (excepto correo institucional)	Bloquear (excepto correo institucional)	Bloquear (excepto correo institucional)
Game	Bloquear	Bloquear	Bloquear
General.Interest	Monitorear	Monitorear	Monitorear
IM	Bloquear	Bloquear	Bloquear
Industrial	Monitorear	Monitorear	Monitorear
Mobile	Monitorear	Monitorear	Monitorear
Network.Service	Bloquear	Bloquear	Bloquear
P2P	Bloquear	Bloquear	Bloquear
Proxy	Bloquear	Bloquear	Bloquear
Remote.Access	Bloquear (excepto herramientas corporativas autorizadas)	Bloquear (excepto herramientas corporativas autorizadas)	Bloquear (excepto herramientas corporativas autorizadas)
Social.Media	Bloquear	Monitorear	Bloquear
Special	Monitorear	Monitorear	Monitorear
Storage.Backup	Bloquear	Bloquear	Bloquear
Update	Monitorear	Monitorear	Monitorear
Video/Audio	Bloquear	Bloquear	Bloquear
VoIP	Bloquear	Bloquear	Bloquear
Web.Others	Monitorear	Monitorear	Monitorear
Web.Client	Monitorear	Monitorear	Monitorear
Unknown	Bloquear	Bloquear	Bloquear

Nota: Para la sede del Nivel Central (NVC), se permitirá el uso de la plataforma Zoom exclusivamente para servicios de Telefonía IP institucional, previa configuración técnica de la OTIC y monitoreo activo

9.2. Matriz de Control Filtrado WEB

A continuación, se define la acción por categoría WEB:

Tabla 4 Matriz de Control Filtrado WEB

Categoría	Subcategoria	Perfil		
		Estándar	VIP	Colegios
Content Adult/Mature	Abortion	Monitorear	Monitorear	Bloquear
	Advocacy Organizations	Monitorear	Monitorear	Monitorear
	Alcohol	Bloquear	Bloquear	Bloquear
	Alternative Beliefs	Bloquear	Bloquear	Bloquear
	Dating	Bloquear	Bloquear	Bloquear
	Gambling	Bloquear	Bloquear	Bloquear
	Lingerie and Swimsuit	Bloquear	Bloquear	Bloquear
	Marijuana	Bloquear	Bloquear	Bloquear
	Nudity and Risque	Bloquear	Bloquear	Bloquear
	Other Adult Materials	Bloquear	Bloquear	Bloquear
	Pornography	Bloquear	Bloquear	Bloquear
	Sex Education	Monitorear	Monitorear	Monitorear
	Sports Hunting and War Games	Bloquear	Bloquear	Bloquear
	Tobacco	Bloquear	Bloquear	Bloquear
	Weapons (Sales)	Bloquear	Bloquear	Bloquear
Bandwidth Consuming	File Sharing and Storage	Bloquear (excepto correo institucional)	Bloquear (excepto correo institucional)	Bloquear (excepto correo institucional)
	Freeware and Software Downloads	Bloquear	Bloquear	Bloquear
	Internet Radio and TV	Bloquear	Monitorear	Bloquear
	Internet Telephony	Bloquear (excepto Zoom institucional para NVC)	Bloquear (excepto Zoom institucional para NVC)	Bloquear
	Peer-to-peer File Sharing	Bloquear	Bloquear	Bloquear
	Streaming Media and Download	Bloquear	Bloquear	Bloquear
General Interest - Business	Armed Forces	Bloquear	Bloquear	Bloquear
	Artificial Intelligence Technology	Monitorear	Monitorear	Monitorear
	Business	Monitorear	Monitorear	Monitorear
	Charitable Organizations	Monitorear	Monitorear	Monitorear
	Cryptocurrency	Bloquear	Bloquear	Bloquear
	Finance and Banking	Monitorear	Monitorear	Monitorear
	General Organizations	Bloquear	Bloquear	Bloquear
	Government and Legal Organizations	Monitorear	Monitorear	Monitorear
	Information Technology	Monitorear	Monitorear	Monitorear
	Information and Computer Security	Monitorear	Monitorear	Monitorear

Categoría	Subcategoria	Perfil		
		Estándar	VIP	Colegios
	Online Meeting	Bloquear (excepto zoom y correo institucional)	Bloquear (excepto zoom y correo institucional)	Bloquear (excepto correo institucional)
	Remote Access	Bloquear	Bloquear	Bloquear
	Search Engines and Portals	Monitorear	Monitorear	Monitorear
	Secure Websites	Monitorear	Monitorear	Monitorear
	URL Shortening	Bloquear	Bloquear	Bloquear
	Web Analytics	Bloquear	Bloquear	Bloquear
	Web Hosting	Monitorear	Monitorear	Monitorear
	Web-based Applications	Monitorear	Monitorear	Monitorear
General Interest - Personal	Advertising	Bloquear	Bloquear	Bloquear
	Arts and Culture	Monitorear	Monitorear	Monitorear
	Auction	Bloquear	Bloquear	Bloquear
	Brokerage and Trading	Bloquear	Bloquear	Bloquear
	Child Education	Monitorear	Monitorear	Monitorear
	Content Servers	Monitorear	Monitorear	Monitorear
	Digital Postcards	Bloquear	Bloquear	Bloquear
	Domain Parking	Bloquear	Bloquear	Bloquear
	Dynamic Content	Monitorear	Monitorear	Monitorear
	Education	Monitorear	Monitorear	Monitorear
	Entertainment	Bloquear	Bloquear	Bloquear
	Folklore	Monitorear	Monitorear	Monitorear
	Games	Bloquear	Bloquear	Bloquear
	Global Religion	Bloquear	Bloquear	Bloquear
	Health and Wellness	Monitorear	Monitorear	Monitorear
	Instant Messaging	Bloquear	Monitorear	Bloquear
	Job Search	Bloquear	Bloquear	Bloquear
	Meaningless Content	Bloquear	Bloquear	Bloquear
	Medicine	Monitorear	Monitorear	Monitorear
	News and Media	Monitorear	Monitorear	Monitorear
	Newsgroups and Message Boards	Bloquear	Bloquear	Bloquear
	Personal Privacy	Bloquear	Bloquear	Bloquear
	Personal Vehicles	Bloquear	Bloquear	Bloquear
	Personal Websites and Blogs	Bloquear	Monitorear	Monitorear
	Political Organizations	Bloquear	Bloquear	Bloquear
	Real Estate	Bloquear	Bloquear	Bloquear
	Reference	Monitorear	Monitorear	Monitorear
	Restaurant and Dining	Bloquear	Monitorear	Bloquear
	Shopping	Monitorear	Monitorear	Monitorear
	Social Networking	Bloquear	Monitorear	Bloquear
	Society and Lifestyles	Monitorear	Monitorear	Monitorear

Categoría	Subcategoria	Perfil		
		Estándar	VIP	Colegios
	Sports	Monitorear	Monitorear	Monitorear
	Travel	Monitorear	Monitorear	Monitorear
	Web Chat	Bloquear	Monitorear	Bloquear
	Web-based Email	Bloquear (excepto correo institucional)	Bloquear (excepto correo institucional)	Bloquear (excepto correo institucional)
Potentially Liable	Child Sexual Abuse	Bloquear	Bloquear	Bloquear
	Crypto Mining	Bloquear	Bloquear	Bloquear
	Discrimination	Bloquear	Bloquear	Bloquear
	Drug Abuse	Bloquear	Bloquear	Bloquear
	Explicit Violence	Bloquear	Bloquear	Bloquear
	Extremist Groups	Bloquear	Bloquear	Bloquear
	Hacking	Bloquear	Bloquear	Bloquear
	Illegal or Unethical	Bloquear	Bloquear	Bloquear
	Plagiarism	Bloquear	Bloquear	Bloquear
	Potentially Unwanted Program	Bloquear	Bloquear	Bloquear
	Proxy Avoidance	Bloquear	Bloquear	Bloquear
	Terrorism	Bloquear	Bloquear	Bloquear
Security Risk	Dynamic DNS	Bloquear	Bloquear	Bloquear
	Malicious Websites	Bloquear	Bloquear	Bloquear
	Newly Observed Domain	Monitorear	Monitorear	Monitorear
	Newly Registered Domain	Monitorear	Monitorear	Monitorear
	Phishing	Bloquear	Bloquear	Bloquear
	Spam URLs	Bloquear	Bloquear	Bloquear
Unrated	Not Rated	Bloquear	Bloquear	Bloquear

Nota:
Se entiende por acción "MONITOREAR" la capacidad de la plataforma de filtrado para permitir el tráfico, pero generando un registro detallado (log) de la transacción (usuario, origen, destino, categoría, bytes transferidos, timestamp). En plataformas que no cuenten con una función nativa denominada "Monitor", esta acción será implementada mediante la combinación de "Permitir" + "Logging Forzoso" + "Generación de Alerta" (si el volumen supera un umbral). Queda prohibido interpretar "MONITOREAR" como "no hacer nada".

9.3. Regla de Excepción para Servicios Institucionales

Cuando las matrices de control (Tablas 1 y 2) establezcan la acción "Bloquear" para las categorías de Email, Online Meeting, Collaboration, Cloud Storage o File Sharing, dicha acción se entenderá aplicable a todos los servicios no institucionales que caigan dentro de esas categorías.

Quedan expresamente exceptuados (es decir, permitidos) exclusivamente los siguientes servicios institucionales, debidamente gestionados por la Oficina de Tecnología:

Tabla 5 Regla de Excepción para Servicios Institucionales

Categoría	Servicios Institucionales Permitidos
Email	Microsoft 365 (Outlook, Exchange Online), Google Workspace institucional (Gmail corporativo), o la solución de correo electrónico corporativo que defina la Entidad.
Online Meeting / Collaboration	Microsoft Teams, Google Meet institucional, Zoom institucional (exclusivamente para servicios de Telefonía IP en NVC), o la plataforma de colaboración corporativa definida por la Entidad.
Cloud Storage / File Sharing	OneDrive for Business, SharePoint Online, Google Drive institucional, o la solución de almacenamiento corporativo definida por la Entidad.

Regla de interpretación: La inclusión de un servicio en el listado anterior no implica su permiso automático si dicho servicio es utilizado para funciones no autorizadas (ej: uso de OneDrive personal con cuenta Microsoft gratuita, en lugar de OneDrive for Business institucional). La OTIC definirá los parámetros técnicos (ej: restricción por dominio del correo electrónico, autenticación SSO, etc.) para garantizar que solo se permita el uso institucional y no el personal.

9.4. Política de Acceso Remoto (Remote Access)

El acceso remoto a equipos, servidores o infraestructura de la Entidad se regirá por los siguientes principios:

Tabla 6 Política de Acceso Remoto

Tipo de Acceso Remoto	Acción	Condiciones
Herramientas no institucionales (TeamViewer, AnyDesk, LogMeIn, VNC, Chrome Remote Desktop, Splashtop, GoToMyPC, Ammyy Admin, etc.)	Bloqueado para TODOS los perfiles, sin excepción	Estas herramientas no están licenciadas, ni gestionadas, ni auditadas por la Entidad. Su uso representa un riesgo de seguridad inaceptable.
RDP (Remote Desktop Protocol)	Bloqueado por defecto	Se permite exclusivamente bajo demanda y con autorización expresa de Seguridad de la Información (CSIRT), para casos específicos como: soporte externo autorizado, mantenimiento de servidores, o acceso a equipos en condiciones excepcionales. No es un permiso permanente.
Microsoft Teams (control remoto)	Permitido (solo funcionalidad dentro de Teams)	Es la herramienta corporativa oficial de colaboración. Toda sesión remota realizada a través de Teams queda registrada y auditada. Aplica exclusivamente para la mesa de servicio y personal autorizado.

Tipo de Acceso Remoto	Acción	Condiciones
Herramienta MDM / RMM institucional (ej: Microsoft Intune, SCCM, o la solución corporativa definida por la OTIC)	Permitido (solo para la mesa de servicio)	Herramienta licenciada, gestionada y operada por la Oficina de Tecnología. Su uso está restringido al personal de la mesa de servicio debidamente autorizado.

Procedimiento para solicitar una excepción de RDP:

1. El área o contratista externo debe radicar una solicitud formal ante la mesa de servicio.
2. Debe justificar técnicamente la necesidad (ej: "soporte a proveedor de software X para actualización del servidor Y", "configuración de equipo fuera de la red corporativa").
3. La solicitud debe ser aprobada por Seguridad de la Información (CSIRT).
4. La excepción tendrá un tiempo de vigencia definido (máximo 15 días hábiles, prorrogable previa justificación).

10. PROTECCIÓN ANTIVIRUS (AV) A TRAVÉS DE DISPOSITIVOS UTM

La protección antivirus en la capa de red es un control obligatorio, independiente del perfil de usuario (Estándar, VIP, Colegios, Invitados). Por lo tanto, el perfil AV_SED (o el nombre institucional que defina la OTIC) será aplicado de manera transversal y obligatoria a la totalidad del tráfico que ingrese, egrese o transite por la infraestructura tecnológica de la Entidad, sin excepción, en los protocolos definidos a continuación.

10.1. Configuración del perfil AV_SED

El perfil de antivirus para dispositivos UTM deberá observar obligatoriamente los siguientes parámetros de configuración:

Tabla 7 Perfil AV_SED

Parámetro	Configuración obligatoria	Justificación
AntiVirus scan	Block	El escaneo antivirus debe estar activo y en modo de bloqueo, no solo en monitoreo, para prevenir activamente la ejecución o descarga de malware.
Feature set	Modo de Inspección	Se deberá priorizar un modo de inspección que garantice el análisis del tráfico continuo (ej: streaming, flujo o proxy según el fabricante) con el menor impacto posible en la latencia de la red institucional, asegurando siempre la capacidad de bloquear malware antes de que complete su descarga. Se debe documentar el modo elegido y su justificación técnica.

10.2. Protocolos inspeccionados

El perfil AV_SED deberá aplicar escaneo antivirus de manera obligatoria sobre los siguientes protocolos:

Tabla 8 Protocolos Inspeccionados

Protocolo	Inspección obligatoria	Observación
HTTP	Sí	Tráfico web y navegación
SMTP	Sí	Correo electrónico entrante y saliente
POP3	Sí	Correo electrónico (recepción)
IMAP	Sí	Correo electrónico (sincronización)
FTP	Sí	Transferencia de archivos

10.3. Protección avanzada contra amenazas persistentes (APT)

Con el fin de fortalecer la capacidad de detección de amenazas avanzadas, el perfil AV_SED deberá habilitar las siguientes opciones de protección APT (Advanced Persistent Threat):

Tabla 9 Protección ATP

Opción de protección	Configuración obligatoria	Descripción
Treat Windows executables in email attachments as viruses	Activado	Los archivos ejecutables (.exe, .dll, .scr, .msi, etc.) enviados como adjuntos en correos electrónicos serán tratados directamente como virus, Independientemente de su firma, debido al alto riesgo que representan.
Capacidad de Sandboxing	Activado	El sistema deberá contar con un módulo de análisis dinámico (sandbox) interno o integrado por API, al cual se enviarán automáticamente archivos sospechosos no clasificables por firmas tradicionales, para su ejecución en un entorno aislado y análisis conductual.
Include mobile malware protection	Activado	Extiende la protección a amenazas dirigidas a dispositivos móviles (Android, iOS) que se conecten a la red institucional.
Quarantine	Activado	Los archivos o tráfico identificados como maliciosos serán puestos en cuarentena automáticamente, impidiendo su entrega al destinatario y generando una alerta de seguridad.

10.4. Prevención de brotes virales (Virus Outbreak Prevention)

Para mitigar el impacto de brotes virales de rápida propagación (zero-day o variantes emergentes), el perfil AV_SED deberá configurarse conforme a lo siguiente:

Tabla 5 Prevención de brotes virales

Parámetro	Configuración obligatoria	Justificación
Base de Inteligencia para Brotes (Outbreak)	Activado	Se utilizará una base de inteligencia de amenazas del fabricante o fuente equivalente, con capacidad de actualización continua (streaming updates) y firma temporal (hash/patrón) para contener brotes de cero horas (zero-hour) mientras se desarrollan las firmas definitivas.
Action	Block	Ante la detección de un patrón de brote viral, el tráfico asociado será bloqueado de manera inmediata. No se acepta el modo "Monitor" para esta funcionalidad, dado que permitiría la propagación del brote mientras solo se genera una alerta.

10.5. Política de Inspección SSL y Protección de la Privacidad

Para garantizar la seguridad sin vulnerar el derecho fundamental a la privacidad y la protección de datos personales, conforme a lo establecido en la Ley 1581 de 2012, se establece lo siguiente:

1. Inspección por defecto**:** Todo el tráfico web cifrado (HTTPS) será inspeccionado por defecto, utilizando un certificado raíz institucional instalado en los equipos gestionados.
2. Excepciones obligatorias (NO inspeccionar): Se configurará una lista de exclusión (SSL Bypass) para los siguientes dominios o categorías, donde el contenido está protegido por secrecía o privacidad legal:
    - Banca y Finanzas: Dominios de entidades financieras supervisadas por la Superintendencia Financiera (ej: *.bancolombia.com, *.davivienda.com).
    - Salud: Portales de citas médicas, historia clínica electrónica y EPS (dominios con categoría "Medicine" y "Health and Wellness" serán evaluados caso a caso).
    - Correo Electrónico Personal**:** Acceso web a servicios de correo no institucionales (ej: gmail.com, outlook.com, yahoo.com) solo para el perfil Estándar y VIP.
    - Gobierno y Autenticación: servicios que utilizan mecanismos de validación estricta, certificados y autenticación segura que pueden verse afectados por la inspección SSL/TLS. Esto reduce riesgos de incompatibilidad, fallas de acceso y exposición de información sensible.
    - Collaboration / Messaging: las plataformas de mensajería utilizan cifrado, validación de certificados y mecanismos de autenticación sensibles que pueden verse afectados por la inspección SSL/TLS. Esto ayuda a evitar problemas de conectividad, degradación del servicio y fallas en aplicaciones como correo, videoconferencia y mensajería corporativa.
    - Software Update: Los servicios de actualización validan estrictamente certificados y firmas digitales para garantizar la integridad del software. La inspección SSL/TLS puede interferir en estas validaciones y generar fallas en descargas, actualizaciones o validación de parches.

- Certificate Authorities: Los servicios de autoridades certificadoras gestionan validaciones criptográficas y certificados digitales sensibles. La inspección SSL/TLS puede alterar la cadena de confianza y provocar errores de validación, autenticación y establecimiento seguro de conexiones.
- Institucional / VPN: Se utilizan cifrado de extremo a extremo y mecanismos de autenticación sensibles que pueden verse afectados por la inspección SSL/TLS. Esto evita fallas de conectividad, degradación del túnel seguro e interrupciones en servicios institucionales críticos.

3. Garantía de privacidad para menores**:** En el perfil "Colegios", la inspección SSL será total (sin estas excepciones), dado el interés superior del menor y la naturaleza pedagógica del entorno. La Entidad actuará como responsable del tratamiento de datos en el contexto educativo.
4. Registro de auditoría**:** La decisión de excluir un dominio de la inspección SSL quedará registrada en un log, con su justificación (ej: "privacidad financiera", "secreto bancario") y aprobador.

11. ANEXO A – APLICACIONES Y FUNCIONALIDADES PERMITIDAS Y BLOQUEADAS

En el Anexo A del presente documento, el cual forma parte integral de estos lineamientos, se presentan de manera puntual, taxativa el cual aplica de manera trasversal para cualquiera de los perfiles previamente definidos, las aplicaciones, herramientas, servicios y funcionalidades expresamente permitidas y aquellas estrictamente bloqueadas en el entorno de filtrado web y control de aplicaciones de la Secretaría de Educación del Distrito.

La actualización de este anexo estará a cargo de la Oficina de Tecnología y deberá revisarse semestralmente o cuando se identifiquen nuevas amenazas.

12. APLICABILIDAD Y ÁMBITO DE CUMPLIMIENTO

12.1 Vinculación con el Proyecto PRY-29

Fortalecer la Seguridad Digital del PETI
Los presentes Lineamientos de Filtrado WEB constituyen un instrumento técnico del Proyecto PRY-29: "Fortalecer la Seguridad Digital del PETI" , en el marco de las estrategias definidas por la Secretaría de Educación del Distrito para la modernización, seguridad y resiliencia de su infraestructura tecnológica.

El Proyecto PRY-29 tiene como objetivo general fortalecer la seguridad digital del Plan Estratégico de Tecnologías de la Información (PETI) de la Entidad, mediante la implementación de controles técnicos, normativos y operativos que garanticen la confidencialidad, integridad y disponibilidad de la información institucional, con especial énfasis en la protección de los niños, niñas y adolescentes en entornos digitales.

En este contexto, los lineamientos aquí definidos desarrollan específicamente el Control 8.23 (Filtrado Web) del Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001, y materializan las siguientes acciones del PRY-29:

Acción del PRY-29	Desarrollo en estos lineamientos
Implementación de controles de filtrado web por perfiles de usuario	Capítulo 6 (CLASIFICACIÓN DE PERFILES), Capítulo 9 (MATRICES DE CONTROL)

Acción del PRY-29	Desarrollo en estos lineamientos
Protección antivirus transversal en la capa de red	Capítulo 10 (PROTECCIÓN ANTIVIRUS)
Inspección SSL con protección de la privacidad	Capítulo 10.5 (POLÍTICA DE INSPECCIÓN SSL Y PRIVACIDAD)
Bloqueo de categorías de alto riesgo (malware, phishing, proxy, P2P, etc.)	Capítulo 7 (CATEGORÍAS DE BLOQUEO GENERAL)
Corresponsabilidad en la protección del menor en entornos digitales	Capítulo 5 (PRINCIPIOS RECTORES – CORRESPONSABILIDAD)

12.2 Mecanismo de Implementación Obligatoria

La presente política y sus lineamientos de filtrado web, control de aplicaciones y AV (Anti-Virus) serán implementados y aplicados exclusivamente a través de dispositivos última generación (Next-Generation Firewall - NGFW), o tecnologías equivalentes que ofrezcan capacidades de inspección profunda de paquetes (DPI), filtrado por categorías web, control de aplicaciones independiente del puerto o protocolo, e inspección SSL/TLS. En ningún caso se aceptarán mecanismos de filtrado basados exclusivamente en listas de acceso por puerto o dirección IP, por considerarse insuficientes frente a las amenazas actuales.

12.3 Vinculatoriedad para Proyectos y Dependencias

Cualquier proyecto, iniciativa, desarrollo, adquisición o contratación liderada por cualquier área, dependencia, contratista o tercero vinculado a la Secretaría de Educación del Distrito, que implique el suministro, configuración, operación o modificación de infraestructura tecnológica (incluyendo, pero sin limitarse a: redes, conectividad, acceso a Internet, plataformas en la nube, soluciones de conectividad remota, desarrollo de aplicaciones web, implementación de redes inalámbricas, o cualquier otra solución que permita el acceso a contenidos o aplicaciones desde la red institucional), deberá cumplir obligatoriamente con los lineamientos de filtrado web, control de aplicaciones y AV (Anti-Virus) aquí definidos.

12.4 Condiciones para Nuevos Proyectos

Para garantizar el cumplimiento irrestricto de estos lineamientos, los responsables de cualquier proyecto o dependencia deberán garantizar los siguientes puntos:

Tabla 10 Condiciones para Nuevos Proyectos

Condición	Descripción
Inclusión en términos de referencia	Los pliegos de condiciones, términos de referencia, especificaciones técnicas o documentos equivalentes deberán incluir explícitamente la obligación de cumplir con los presentes lineamientos de filtrado web.
Validación previa por Tecnología	Ningún proyecto que involucre conectividad a Internet o acceso a aplicaciones web podrá ser aprobado sin el visto bueno de la Oficina de Tecnologías de la Información y las Comunicaciones, quien

Condición	Descripción
	verificará la compatibilidad con el esquema de filtrado definido.
Garantía de cumplimiento de la política	Todo proyecto independiente de su alcance y cuyo objetivo busque entregar un servicio que permita la navegación Web deberá implementar y garantizar el cumplimiento efectivo de todos los lineamientos de filtrado web, control de aplicaciones y AV (Anti-Virus) definidos en el presente documento, sin que ello implique necesariamente el tránsito por los dispositivos NGFW institucionales. El responsable del proyecto o dependencia deberá demostrar, mediante la documentación técnica que corresponda, cómo se asegura el bloqueo de categorías prohibidas, el monitoreo de categorías controladas y la restricción de aplicaciones no permitidas para cada perfil de usuario, bajo cualquier esquema de conectividad.
Excepciones documentadas	Cualquier desviación a estos lineamientos deberá ser tramitada conforme al capítulo de EXCEPCIONES del presente documento, con aprobación de Seguridad de la Información.
Responsabilidad del ordenador del gasto	El área o dependencia que ordene el gasto o contrate soluciones que incumplan estos lineamientos asumirá las consecuencias operativas, legales y de seguridad derivadas de dicho incumplimiento.

12.5 Irrenunciabilidad de los Controles

Ningún proyecto, independientemente de su alcance, tecnología empleada, ubicación (on-premise, nube, híbrida), proveedor, plataforma, o esquema de conectividad, podrá argumentar condiciones técnicas, arquitectónicas, contractuales o administrativas para eludir, atenuar o modificar los controles de filtrado web y de aplicaciones establecidos en el presente documento.

El principio de cumplimiento obligatorio de estos lineamientos prevalece sobre cualquier otra consideración.

12.6 Obligaciones Específicas para ISP en Colegios

Contexto operativo actual:

La Secretaría de Educación del Distrito reconoce que, en las condiciones actuales de infraestructura tecnológica de los colegios y sedes educativas:

- No existe una solución centralizada de gestión de equipos de dominio para colegios.
- Los equipos institucionales en colegios no se encuentran en un dominio administrado centralmente.
- Los ISP no tienen acceso ni gestión sobre los equipos terminales de los colegios.
- La inspección SSL profunda se encuentra actualmente en fase de piloto, evaluada mediante un agente externo especializado.

En consecuencia, las obligaciones para los ISP se definen de manera progresiva y proporcional a las capacidades técnicas actuales y futuras de la Entidad.

Obligaciones inmediatas (exigibles desde la entrada en vigencia del presente lineamiento):

#	Obligación	Descripción
1	Capacidad técnica de inspección SSL	La solución de filtrado web provista por el ISP deberá tener capacidad de inspección SSL/TLS, aunque esta funcionalidad no se encuentre activada en el momento de la firma del contrato, deberá estar disponible para su activación futura cuando la SED lo requiera.
2	Disponibilidad del certificado raíz	El ISP deberá proporcionar a la SED el certificado raíz de su solución de filtrado, en formato estándar (ej. .crt, .pem), para que la Entidad, a través de sus propios medios, realice la instalación en los equipos institucionales que gestiona.
3	Colaboración en pruebas piloto	El ISP deberá colaborar activamente con la SED en las pruebas piloto de inspección SSL, permitiendo la configuración, ajuste y validación de la funcionalidad en entornos controlados.
4	No bloqueo por defecto	Mientras la inspección SSL no esté activada y validada, el ISP no podrá bloquear por defecto el tráfico cifrado (HTTPS) que no pueda inspeccionar, garantizando la conectividad institucional.

Obligaciones futuras (exigibles una vez la SED cuente con la infraestructura necesaria):

Una vez la Secretaría de Educación del Distrito haya implementado una solución centralizada de gestión de equipos (MDM, GPO basado en nube, o herramienta equivalente) que permita la instalación forzosa y gestionada de certificados raíz en los equipos de los colegios, se activarán las siguientes obligaciones contractuales para los ISP:

#	Obligación	Descripción
1	Activación de inspección SSL	El ISP deberá activar la inspección SSL en su solución de filtrado web, utilizando el certificado raíz proporcionado a la SED.
2	Instalación del certificado raíz	La SED, a través de su herramienta de gestión centralizada, instalará el certificado raíz del ISP en todos los equipos institucionales de los colegios. El ISP no tendrá acceso directo a los equipos.
3	Verificación periódica	El ISP deberá permitir verificaciones periódicas por parte de la OTIC para confirmar que la inspección SSL se encuentra activa y funcionando conforme a los lineamientos.

El incumplimiento de las obligaciones inmediatas por parte del ISP podrá ser causal de sanciones contractuales, alineándose con la Política de Relación con Proveedores (A.15) de la norma ISO/IEC 27001:2022.

El incumplimiento de las obligaciones futuras solo será exigible una vez la SED haya cumplido con su parte correspondiente (implementación de la solución de gestión centralizada y actualización contractual), y se aplicarán las mismas consecuencias.

13. RESPONSABILIDADES

Oficina de Tecnología de la Información y las Comunicaciones

- Configurar y mantener el sistema de filtrado.
- Actualizar categorías.
- Monitorear eventos.
- Garantizar la interoperabilidad del filtrado web con el Sistema de Gestión de Identidades y Accesos (IAM).

Equipo técnico Seguridad de la Información

- Evaluar riesgos asociados al filtrado web y proponer mejoras.
- Definir y aprobar excepciones justificadas a los bloqueos establecidos.
- Auditar el cumplimiento de los presentes lineamientos.
- Coordinar la respuesta a incidentes de seguridad derivados de la navegación web.

Usuarios (funcionarios, Contratistas, Docentes, Administrativos y Estudiantes)

- Cumplir los presentes lineamientos de filtrado web.
- Reportar incidentes de seguridad (phishing, malware, contenido inapropiado) a través de la Mesa de Servicio.
- No evadir los controles de filtrado mediante VPN no autorizadas, proxies o herramientas de anonimización.

Vinculación con la Política de Tratamiento de Datos Personales de la SED:
Los funcionarios y contratistas que, durante la navegación web institucional, accedan a información personal, datos sensibles o información financiera, contable y presupuestal, están sujetos al deber de reserva y confidencialidad establecido en la Política de Tratamiento de Datos Personales de la SED y en la Ley 1581 de 2012.

En consecuencia, deberán:

- No divulgar dicha información a terceros no autorizados.
- Utilizarla exclusivamente para fines institucionales.
- No almacenarla, copiarla o transferirla a través de servicios no institucionales (correos personales, nube no autorizada, etc.).

El incumplimiento será reportado a la Oficina de Control Interno Disciplinario y podrá dar lugar a sanciones disciplinarias, penales (Ley 1273 de 2009) o contractuales.

14. EXCEPCIONES

Cualquier solicitud de acceso a una URL o aplicación bloqueada deberá ser tramitada mediante la Oficina de Tecnología de la SED, adjuntando la justificación pedagógica o administrativa, validando que no contravenga el interés superior del menor ni ponga en riesgo la red.

Las excepciones deberán:

- Estar debidamente justificadas.
- Ser aprobadas por Seguridad de la Información.
- Tener tiempo definido.
- Quedar registradas.

15. MONITOREO Y AUDITORÍA

Se mantendrán registros de navegación conforme a:

- Principio de finalidad.
- Principio de proporcionalidad.
- Normativa de protección de datos.

Los logs serán utilizados exclusivamente para:

- Gestión de incidentes.
- Análisis de riesgos.
- Cumplimiento normativo.

MILENA DEL PILAR SANDOVAL GOMEZ
Jefe Oficina de las Tecnologías de la Información y Las Comunicaciones

Elaboró: Juan Carlos Parra Moreno – Oficial Seguridad I ca

Reviso: Henry Alexander Moyan Montenegro – Oficial Seguridad de Información

Reviso: Luz Dary Vargas. – Profesional Especializado OTIC

Reviso: Jasson Smith Castro L. – Profesional Especia do OTIC

ANEXO A

El presente anexo forma parte integral de los lineamientos y debe leerse en concordancia con lo establecido en el Capítulo 9 – APLICACIONES Y CATEGORÍAS WEB BLOQUEADAS.

Las siguientes tablas presentan un listado enunciativo e ilustrativo de aplicaciones específicas, agrupadas por su categoría lógica. Este listado no es taxativo ni limitativo. La acción de bloqueo o monitoreo se define por la pertenencia de una aplicación a una categoría lógica según las Tablas 1 y 2 del Capítulo 9, y no por su inclusión o exclusión en este anexo.

Actualización: La OTIC actualizará este listado semestralmente o cuando se identifiquen nuevas amenazas, incorporando nuevos ejemplos representativos que faciliten la operación del filtrado.

BLOQUEADAS			
Adobe.Connect	Edgio	QQ	WeCom.Large.File.Transfer
Adobe.Connect_Meeting.Remote.Control	Engine.Yard.Cloud	QQ_Call	WeCom.Picture.Download
Adobe.Connect_Meeting.Share.Document.Upload	Ethereum.Cryptocurrency.Miner	QQ_File.Transfer	WeCom.Picture.Upload
Adobe.Connect_Meeting.Share.My.Screen	Evernote_File.Download	QQ_Login	WeCom.Video.Download
Adobe.Connect_Meeting.Share.Whiteboard	Evernote_File.Upload	QQ_Logout	WeCom.Video.Upload
AIM.Webmail_Attachment	Facebook_File.Download	QQ_Picture.Transfer	WhatsApp_File.Transfer
AirWatch.MDM	Facebook_File.Upload	QQ_QQDownload	WhatsApp_Web.File.Download
Amazon.AWS	Facebook_Messenger.Image.Transfer	QQ_QQLive	WhatsApp_Web.File.Upload
Amazon.AWS_EC2	Facebook_Messenger.Video.Transfer	QQ_Remote.Control	Whereby
Amazon.AWS_S3	Facebook_Messenger.Voice.Message	Rapid7.Insight.Agent	YY.Voice_File.Transfer
Amazon.AWS_S3.Download	Facebook_Messenger.VoIP.Call	Razor	Zello
Amazon.AWS_S3.Upload	Facebook_Video.Play	RDT	Zoho_File.Download
Amazon.AWS_SageMaker	File.Upload.HTTP	RSS	Zoho_File.Upload
Amazon.AWS_SageMaker.Create.Project	Forcepoint.Cloud.Proxy	Salesforce_File.Download	Zoom
Amazon.AWS_SageMaker.Delete.Project	Free.Download.Manager	Salesforce_File.Upload	Zoom_File.Download
Amazon.CloudFront	FTP	SAP.RFC	Zoom_File.Upload
Amazon_Login	FTP_Command	SAP.RFC.WebSocket	Zoom_Login
Any.Do	Fuze.Meeting_File.Transfer	SAP.SNC	Zoom_Meeting
Apple_Login	Gadu.Gadu	Skype_Audio	Zoom_Meeting.Remote.Control
AppScale	Genesys	Skype_Data	Zoom_Team.Chat
Arvixe	Google.Chat_Video.Call	Skype_File.Transfer	Gmail_Attachment
AT&T.Connect	Google.Docs_File.Download	Skype_Video	Gmail_Attachment.Download
AT&T.Synaptic	Google.Translate_Websites	Slack_Call	Gmail_Attachment.Upload
Atlassian.Cloud	H.248	SourceForge	YouTube.Downloader.YTD
Atlassian.Jira.Confluence_File.Download	HCL.Notes	SourceForge_File.Upload	YouTube_HD.Streaming
Atlassian.Jira.Confluence_File.Upload	HTTP.Download.Accelerator	TeamCity	YouTube_Search.Safety.Mode.Off

Atlassian_Login	HTTP.Segmented.Download	Telegram_VoIP.Call	YouTube_Video.Embedded
Baidu.Cloud_File.Download	Huddle_File.Download	Time.Warner.Cable	YouTube_Video.Upload
Baidu.Cloud_File.Upload	Huddle_File.Upload	Time.Warner.Cable_Video	RDP
Baidu.Hi_Audio.Video.Chat	ICQ_File.Transfer	Trello_File.Download	DNS.Over.HTTPS
Baidu.Hi_File.Transfer	Jabber	Trello_File.Upload	NVP.II
BambooHR_File.Download	Java.Debug.Wire.Protocol	UserVoice_File.Download	WeChat_Video.Upload
BambooHR_File.Upload	KakaoTalk_File.Transfer	UserVoice_File.Upload	Distributed.Net
Bitcoin.Cryptocurrency.Miner	KakaoTalk_Voice.Chat	Vsee	NiceHash.BeamV3.Cryptocurrency.Miner
Cardano.Cryptocurrency	Lifesize	Webex_Desktop.Sharing	Directory.Replication.Service.Remote.Protocol.DSGetNCChanges
ClickView	Mailchimp_File.Upload	Webex_File.Download	Naver.Line_Call
Cloudify.Co	Meraki.Cloud.Controller	Webex_File.Sharing	WeChat_Video.Download
Cloudmark	Mercurial_Upload	Webex_File.Upload	WeChat_Picture.Upload
Conduit.Toolbar	Microsoft.Intune	WeChat_File.Download	WeCom.File.Upload
CPUminer.Cryptocurrency.Miner	MinerGate.Cryptocurrency.Miner	WeChat_File.Upload	Prezi_File.Upload
Cradlepoint.Netcloud	Mipony	WeChat_LargeFile.Download	Docker_Push.Manifest
CryptoTab.Mining	Monero.Cryptocurrency.Miner	WeChat_Location.Share	Docker_Push.Blob
Daum.Mail_Attachment	NateOn_File.Transfer	WeChat_Picture.Download	Prezi_File.Download
WeCom.File.Download	Docker_Pull.Blob	Okta	WeChat_VoIP.Call
DNS.Over.TLS	NZBVortex	WeChat_Voice.Chat	
MONITOREADAS			
Facebook	OneDrive	Microsoft.Outlook	Gmail_Personal
Facebook_AppName	OneDrive_File.Download	Microsoft.Outlook.Web.App	Gmail_Workspace
Facebook_Apps	OneDrive_File.Share	Microsoft.Outlook_Attachment	Microsoft.Copilot
Facebook_Like.Button	OneDrive_File.Upload	Microsoft.Outlook_Attachment.Download	Microsoft.Quick.Assist
Facebook_Login	YouTube_Video.Play	Microsoft.Outlook_Attachment.Upload	MS.Netlogon
Facebook_Messenger	YouTube	Microsoft.Outlook_Read.Message	YouTube_Video.Access
Facebook_Personal	YouTube_Category.Control	Microsoft.Outlook_Send.Message	YouTube_Search.Video
Facebook_Plugins	YouTube_Channel.Access	Yahoo.Mail	YouTube_Music
Facebook_Search	YouTube_Channel.Control	Yahoo.Mail_Read.Message	YouTube_Comment.Posting
Gmail	YouTube_Channel.ID	YouTube_Video.Info	

Si una aplicación no aparece en ninguna de las tablas anteriores, se aplicará la acción definida para su categoría en las Tablas 1 y 2 del Capítulo 9. En caso de duda sobre la clasificación de una aplicación, la OTIC emitirá un concepto técnico vinculante dentro de los cinco (5) días hábiles siguientes a la consulta.