GUÍA DEL SISTEMA DE INTERCEPTACIÓN DE LAS COMUNICACIONES – GPJ - 6

1. OBJETIVOS

Esta guía tiene dos propósitos. El primero es unificar criterios para el desarrollo de las diferentes actividades adelantadas en el marco del Sistema de Interceptación de Comunicaciones (en adelante, SIC). Y el segundo es garantizar la funcionalidad e integridad del SIC en el marco del respeto a los principios, reglas, parámetros y garantías previstas en el sistema jurídico.

2. ALCANCE

La presente guía está dirigida a los servidores públicos con funciones de policía judicial, en todo el territorio nacional, que participan dentro del trámite de interceptación de las comunicaciones regido bajo la Ley 906 de 2004. En lo pertinente, esta guía también será aplicable cuando dicha actividad investigativa sea ordenada en el marco de la cooperación judicial internacional, de la articulación y coordinación entre la jurisdicción ordinaria y la jurisdicción especial indígena, y bajo lo prescrito en las leyes 600 de 2000, 975 de 2005 y 1708 de 2014 y las normas que las modifiquen, adicionen y/o sustituyan.

3. TÉRMINOS, DEFINICIONES Y SIGLAS

Administrador de Tecnologías de la Información y las Comunicaciones: es el servidor público encargado del soporte, manejo y cuidado de los sistemas de información de la sala de recepción y análisis de comunicaciones interceptadas.

Alerta: es toda aquella información difundida con el fin de prevenir la posible ocurrencia de hechos que puedan revestir las características de un delito.

Análisis de las comunicaciones: es el conjunto de métodos y técnicas mediante las cuales el (la) analista de comunicaciones escucha, observa, interpreta y correlaciona los componentes semánticos, formales y relevantes de la información registrada, a través de un criterio de interceptación.

Analista de comunicaciones: es el servidor público con funciones de policía judicial, debidamente capacitado, encargado de escuchar, identificar, relacionar, analizar y registrar las comunicaciones interceptadas.

Interceptación de comunicaciones: es un mecanismo de seguridad pública que, en el marco de la Constitución y la Ley, busca optimizar la labor de investigación de delitos que adelantan los servidores públicos con funciones de policía judicial.[1]

Criterios de interceptación (IC): es el número de identificación del suscriptor en la red de comunicación que es susceptible de ser interceptado. Los criterios de interceptación

[1] Decreto 1078 de 2015, artículo 2.2.2.6.1, compilatorio del Decreto 1704 de 2012, artículo 1.

pueden ser: el número de teléfono (MSISDN), el número de identificación único para cada dispositivo de telefonía móvil integrado a la SIM Card (IMSI), la identificación del medio de comunicación, y/o información relacionada con el medio de comunicación a interceptar (IMEI), entre otros.

Departamento de Interceptación de las Comunicaciones (DIC): es la dependencia de la Fiscalía General de la Nación (en adelante FGN) que está encargada de la articulación del SIC, y que le corresponde asegurar la gestión y operatividad del sistema, de acuerdo con los parámetros establecidos en la Constitución Política, la ley, los reglamentos (decretos y/o resoluciones) y las políticas adoptadas por el Fiscal General de la Nación[2].

Jefe de Sala: es el servidor público con funciones de policía judicial, encargado de la administración y correcto funcionamiento de la sala de recepción y análisis de las comunicaciones interceptadas correspondiente.

Programador: es el servidor público con funciones de policía judicial, encargado de verificar los documentos que soportan la orden de interceptación y realizar el registro de los criterios de interceptación en la plataforma tecnológica de la sala de recepción y análisis de las comunicaciones interceptadas y en el sistema autorizado por el DIC para el envío de las solicitudes de interceptación.[3]

Reporte verbal o escrito: es la transmisión de información de interés realizada por el analista de comunicaciones al investigador y al fiscal delegado que ordenó la interceptación de comunicaciones.

Sala de recepción y análisis de comunicaciones interceptadas: es el espacio físico, logístico y tecnológicamente adaptado “para la recepción, análisis y procesamiento de la información interceptada legalmente, generada por el Sistema de Mediación o Plataforma Tecnológica del Sistema de Interceptación de las Comunicaciones”[4].

Sistema de Interceptación de Comunicaciones (SIC): es un conjunto de áreas funcionales, herramientas técnicas y tecnológicas de investigación, integradas para lograr la materialización de las órdenes de interceptación de comunicaciones y el análisis de las comunicaciones interceptadas por la FGN, en el marco de un proceso judicial, previo cumplimiento de los requisitos constitucionales y legales.

Sistema de mediación o Plataforma tecnológica del Sistema de Interceptación de las Comunicaciones: es aquel que “permite gestionar, integrar y realizar técnicamente la interceptación de las comunicaciones que cursan por las redes de los proveedores de redes y servicios de telecomunicaciones, por medio de la infraestructura lógica y tecnológica de hardware y software”[5].

---

[2] Véanse: FGN, resoluciones No. 0-0328 del 2 de abril de 2018 y 0-0362 del 4 de marzo de 2020.
[3] FGN, resolución No. 0-0328 de 2 de abril de 2018, artículo 26.
[4] Ibíd., artículo 10.
[5] Ibíd., artículo 8.

Sistema de recepción y análisis de comunicaciones interceptadas: es la herramienta tecnológica utilizada por los órganos con funciones de policía judicial para la recepción, grabación, decodificación de audio y almacenamiento temporal de información derivada de la interceptación de comunicaciones para su posterior análisis.

Trámite urgente: es la solicitud de interceptación de comunicaciones que debe ser atendida de manera inmediata, y que debe ser priorizada debido a que (*i*) existe una posible afectación a la seguridad nacional, (*ii*) es un caso de connotación nacional, (*iii*) está en riesgo la vida de una o varias personas y/o (*iv*) deben desarrollarse actividades operativas relevantes en el marco de la actuación penal.

4. ASPECTOS RELEVANTES DE LAS SALAS DE RECEPCIÓN Y ANÁLISIS DE COMUNICACIONES INTERCEPTADAS

Con base en la política de dirección, administración y control del SIC, la FGN tiene la facultad de establecer los aspectos relacionados con los componentes de este. En concreto, puede fijar los parámetros administrativos, técnicos, tecnológicos y de seguridad de las salas de recepción y análisis de comunicaciones interceptadas como uno de los componentes del SIC[6]. Sin perjuicio de lo anterior, los siguientes acápites definen las principales características y requisitos que coadyuven al control y seguimiento del funcionamiento de estas.

4.1 Estructura física de las salas de recepción y análisis de comunicaciones interceptadas

Todas las salas de recepción y análisis de comunicaciones interceptadas deben contar, como mínimo, con áreas de trabajo que permitan asegurar los niveles de seguridad necesarios para el desarrollo de la interceptación de comunicaciones. Estos son los siguientes:

a. **Área de recepción o ventanilla de radicación:** es un espacio físico y/o virtual, independiente a la entrada de la sala de recepción y análisis de comunicaciones interceptadas, en donde son realizados los controles de acceso físico y el registro de todo aquel personal ajeno a esta. Además, en este espacio puede recibirse la documentación de manera virtual o física.
b. **Área de análisis de comunicaciones interceptadas:** es un espacio físico independiente, exclusivo y con un sistema de control de acceso, acondicionado para la realización de las actividades de análisis de comunicaciones interceptadas a cargo de los analistas de comunicaciones.
c. **Área de reuniones y contextualización:** es un espacio físico y/o virtual independiente y adecuado para que los analistas de comunicaciones, investigadores y fiscales delegados puedan adelantar la contextualización del caso, y para que el analista de comunicaciones dé a conocer los avances en la actividad investigativa. El uso de este espacio debe ser autorizado por el jefe de sala.

[6] Constitución Política de Colombia, artículo 250, numerales 3 y 8. Cfr. Ley 906 de 2004, artículo 114, numerales 4 y 5.

d. **Área de extracción de evidencia física:** es un espacio físico independiente al área de análisis de comunicaciones, destinado a la extracción de información y recolección de la evidencia, en donde están los equipos destinados para el efecto. Podrá ser parte del área de jefatura de la sala.
e. **Área de infraestructura tecnológica y de equipos de comunicación**: es un espacio físico independiente, exclusivo y con un sistema de control de acceso, donde están ubicados los equipos de infraestructura tecnológica y la interconexión con el sistema de mediación o plataforma tecnológica del SIC de la FGN.
f. **Área de jefatura de la sala:** es un espacio exclusivo para el jefe de la sala.
g. **Área de archivo y gestión documental:** es un espacio físico independiente, exclusivo y con un sistema de control de acceso, donde se gestiona y conserva la documentación relacionada con la ejecución de la actividad investigativa. Este espacio puede ser virtual, de acuerdo con lo que disponga el organismo con funciones de policía judicial en la materia.

4.2 Medidas de seguridad para las salas de recepción y análisis de comunicaciones interceptadas

Las salas de recepción y análisis de comunicaciones interceptadas deben adoptar una serie de medidas que les permitan preservar y garantizar la seguridad en diferentes niveles. Estos son los siguientes:

4.2.1 Seguridad física

Las salas de recepción y análisis de comunicaciones interceptadas deben estar ubicadas en un lugar administrado por los organismos con funciones de policía judicial. Este sitio debe ser independiente, con el objetivo de delimitar su área de trabajo e impedir el acceso no autorizado.

Para su funcionamiento, es indispensable que las salas de recepción y análisis de comunicaciones interceptadas cuenten con un estudio de seguridad, emitido por la dependencia competente de cada organismo con funciones de policía judicial, para analizar la seguridad de las instalaciones y el riesgo de esta. De igual forma, cada área de trabajo debe contar con un circuito cerrado de televisión (CCTV) y sistemas de control electrónico de acceso físico que permitan identificar el ingreso y salida de todo el personal interno como externo.

4.2.2 Seguridad de la información

4.2.2.1 Gestión de ciberseguridad

Los equipos y servidores tecnológicos deberán contar con políticas de seguridad que garanticen la conectividad únicamente a los equipos registrados y autorizados por el jefe de sala, con el fin de asegurar la protección de los activos tecnológicos de las salas de recepción y análisis de comunicaciones interceptadas. De igual manera, debe realizarse el registro de todo incidente de carácter tecnológico que ocurra allí, así como las anomalías o manipulación indebida de los equipos.

4.2.2.2 Gestión de la prestación de servicios por terceros

El Director del organismo con funciones de policía judicial asumirá la responsabilidad de las actividades, intercambios de información y demás acciones que ejecuten terceros. Por ejemplo, el proveedor del sistema en su plataforma tecnológica. Adicionalmente, hay que tener en cuenta lo siguiente:

- ✓ Las conexiones remotas por VPN de terceros para la gestión y soporte técnico a los equipos de la plataforma de la sala deberán ser autorizadas por el Director del organismo con funciones de policía judicial o su delegado(a). Asimismo, estas deben ser controladas y supervisadas por parte de la dependencia competente para el efecto, en cada entidad.
- ✓ Las terceras partes deben cumplir a cabalidad con todas las directrices de seguridad, manejo y custodia de la información y las comunicaciones establecidas en el presente documento y todas aquellas que soliciten los organismos con funciones de policía judicial.
- ✓ Cualquier actividad realizada por un tercero debe reportarse y registrarse, con el fin de ejecutar acciones de seguimiento y control.

4.2.2.3 Gestión de activos

Todos los activos de las salas de recepción y análisis de comunicaciones interceptadas deben estar identificados, inventariados y con su información actualizada, así:

Nombre del activo	Identificación del activo dentro de las salas de recepción y análisis de comunicaciones interceptadas.	
Descripción del activo	Reseña sobre el contenido del activo.	
Tipo de activo	Activo de Información	Son datos e información almacenada, física o electrónicamente como: bases de datos, contratos, acuerdos de confidencialidad, guías, procedimientos, informes, entre otros.
	Activo de software	Son interfaces, programas, aplicaciones, herramientas de desarrollo que se utilizan en las salas.
	Activos de recurso humano	Son las personas que, por su conocimiento, son consideradas activos de información.
	Activos de hardware	Son equipos de cómputo y comunicaciones que, por el cúmulo de información que albergan, se consideran activos de información.
	Otros activos	Activos de información que no correspondan a ninguno de los tipos anteriormente descritos.
Ubicación del activo	Definir el lugar físico o electrónico donde está el activo.	
Propietario del activo	Es el responsable de garantizar que la información se clasifique adecuadamente.	
Custodio del activo	Es la parte designada para hacer efectivos las restricciones de acceso de acuerdo con lo definido por el propietario.	
Usuario del activo	Son quienes generan, transforman y utilizan la información.	

Toda la información y los activos deberán estar asignados al servidor público que corresponda, de acuerdo con su rol, quién deberá contar, como mínimo, con los siguientes elementos para desarrollar su labor: *(i)* oficina modular (puestos de trabajo), *(ii)* muebles y enseres necesarios, *(iii)* equipos de cómputo, *(iv)* pantalla adicional, *(v)* audífonos, *(vi)* fotocopiadora, *(vii)* escáner e *(viii)* impresora.
El responsable del activo asignado no podrá trasladar, destapar, desmantelar, modificar o conectar a otras redes no autorizadas los equipos suministrados para la ejecución de la actividad investigativa. Estos cambios los podrá realizar el administrador de tecnologías de la información y las comunicaciones, siempre que sean autorizados por el jefe de sala y estén plenamente justificados.

4.2.2.4 Gestión documental

El área de archivo y gestión documental debe cumplir las condiciones necesarias para garantizar la custodia y protección de los documentos que reposan en la sala de recepción y análisis de comunicaciones interceptadas, de acuerdo con lo establecido en la tabla de retención documental (TRD) de cada entidad. Adicionalmente, para cada uno de los trámites de interceptación de comunicaciones deben contar con los documentos que soportan dicha solicitud, así como el registro de todas las novedades técnicas y administrativas relacionadas con ella.

4.2.2.5 Seguridad industrial

Las salas de recepción y análisis de comunicaciones interceptadas deben adoptar buenas prácticas en seguridad industrial para el desarrollo de sus actividades con el fin de contar con áreas de trabajo seguras. Para ello, deben propiciarse medidas como: *(i)* orden, limpieza y mantenimiento; *(ii)* puestos de trabajo ergonómicos; *(iii)* extintores de fuego; *(iv)* instalaciones eléctricas; *(v)* condiciones ambientales adecuadas; *(vi)* iluminación; *(vii)* señalización de áreas; entre otros.

4.2.2.6 Seguridad del recurso humano

Los servidores públicos, contratistas y terceros de las salas de recepción y análisis de las comunicaciones interceptadas deben contar con el respectivo estudio de seguridad y confiabilidad. De igual forma, deberán firmar acuerdos de confidencialidad y no divulgación de información, para comprometerse a no revelar información de carácter confidencial que le sea suministrada en el ejercicio de sus funciones dentro de las salas. El incumplimiento de este acuerdo puede ocasionar sanciones disciplinarias y penales.

En consecuencia, los servidores públicos con funciones de policía judicial de las salas de recepción y análisis de comunicaciones interceptadas deben tener conocimientos en ofimática, en la normatividad relacionada con la actividad investigativa y en las políticas y procedimientos pertinentes para el ejercicio de sus funciones; cursos de policía judicial y en análisis de comunicaciones interceptadas; y responsabilidad acerca de la seguridad de la información en el desarrollo de la interceptación de comunicaciones. Los Directores de los organismos con funciones de policía judicial procurarán el cumplimiento de esta labor.

5. DESCRIPCIÓN DE ACTIVIDADES

5.1 DESARROLLO DE LA INTERCEPTACIÓN DE LAS COMUNICACIONES

NO.	ACTIVIDAD	RESPONSABLE	REGISTRO
1	**Verificaciones previas a la orden de interceptación de las comunicaciones** En articulación y bajo la dirección, coordinación y control jurídico de los fiscales delegados, deben desarrollar todas aquellas actividades que les permitan corroborar la información obtenida en el marco del proceso judicial. Particularmente, este deber tiene mucha más relevancia cuando se trata de la interceptación de comunicaciones. Por ello, cuando los investigadores tengan conocimiento que un criterio de interceptación (en adelante, IC) podría contribuir con el avance de la actuación, establecerán lo siguiente: ✓ Un resumen de las **actuaciones que fueron adelantadas para establecer el origen y la existencia del IC** y la importancia de la interceptación de las comunicaciones para la actuación. Por ejemplo, esta puede provenir de información que reposa en la carpeta, de los informes de policía judicial que presenten los analistas de comunicaciones en la ejecución de la actividad investigativa, de una búsqueda selectiva en bases de datos públicas o privadas, declaraciones juradas, inspecciones, entrevistas, análisis de redes, interrogatorios, análisis de registros de llamadas y, en general, de informes sobre el desarrollo de otras actividades investigativas y demás resultados de la indagación e investigación. ✓ La **identificación del IC**, es decir, si este es el número de teléfono (MSISDN), el número de identificación único para cada dispositivo de telefonía móvil integrado a la SIM Card (IMSI), la información relacionada con el medio de comunicación a interceptar (IMEI), entre otros. ✓ El **estado del IC** de (activo o inactivo) en la red del proveedor de redes y servicios de telecomunicaciones. ✓ La verificación de la **portabilidad numérica del IC**, cuando sea procedente[7]. ✓ La información relacionada con la **identificación y confiabilidad de la fuente**	Servidores públicos con funciones de policía judicial	Formato de verificaciones previas

[7] Al respecto, es necesario puntualizar que no es posible realizar la verificación de la portabilidad numérica cuando el IC sea el IMEI.

NO.	ACTIVIDAD	RESPONSABLE	REGISTRO
	(formal o no formal) que dio origen al criterio de interceptación. Una vez adelantadas las anteriores actividades, el jefe inmediato de cada investigador corroborará que los resultados de las actuaciones adelantadas efectivamente arrojen información sobre un posible IC, y que el servidor público con funciones de policía judicial haya adelantado las demás verificaciones previas antes señaladas. Por supuesto, estas gestiones quedarán consignadas en los sistemas de información correspondiente, en el formato que sea adoptado para el efecto y en el informe que sea rendido al fiscal delegado a cargo de la actuación.		
2	**Orden de interceptación de las comunicaciones** A partir de las verificaciones previas que adelante el investigador, el fiscal delegado decidirá si ordena o no la interceptación de las comunicaciones. En concreto, el funcionario judicial determinará, con base en la información suministrada por el servidor público con funciones de policía judicial, (*i*) si cuenta con los elementos materiales probatorios (en adelante, EMP), evidencia física (en adelante, EF) e información legalmente obtenida (en adelante, ILO) para justificar la expedición de la orden, de cara a los hechos jurídicamente relevantes (motivos fundados[8]); (*ii*) si la afectación de los derechos fundamentales respeta los principios de razonabilidad y proporcionalidad[9]; y (*iii*) la urgencia de la medida, siempre que la información provenga de fuentes no formales[10]. Así, cuando la autoridad judicial ordene la interceptación de comunicaciones, tendrá en cuenta lo siguiente: ✓ La orden de interceptación de comunicaciones debe fundamentarse y constar por escrito[11]. ✓ El fiscal delegado determinará la(s) finalidad(es) por las cuales ordena la interceptación de comunicaciones. De acuerdo con los objetivos de la actuación, esta actuación puede ser ordenada para:	Fiscal delegado	Formato orden de allanamiento y registro, retención de correspondencia – interceptación de comunicaciones

[8] Ley 906 de 2004, artículo 235. Cfr. FGN, Directiva No. 0004 del 2 de noviembre de 2021, lineamiento 8.
[9] Véase: Corte Constitucional, sentencia C-594 de 2014. Cfr. FGN, Directiva No. 0004 del 2 de noviembre de 2021, lineamiento 9 y 14.
[10] FGN, Directiva No. 0004 del 2 de noviembre de 2021, lineamiento 10.
[11] Ley 906 de 2004, artículo 235, inciso segundo. Cfr. Ley 600 de 2000, artículo 301, inciso tercero; Ley 1708 de 2014, artículo 167, inciso tercero.

NO.	ACTIVIDAD	RESPONSABLE	REGISTRO
	- Buscar EMP y EF e ILO[12]. - Buscar y ubicar imputados, indiciados o condenados[13]. ✓ Asimismo, el fiscal delegado deberá especificar el delito que, preliminarmente, es objeto de la actuación. ✓ La orden de interceptación de comunicaciones tiene un término máximo de 180 días. Este plazo podrá prorrogarse, siempre que subsistan los motivos fundados[14]. ✓ Las prórrogas de interceptaciones de las comunicaciones deben someterse a control previo de legalidad ante el juez con función de control de garantías[15]. En ese sentido, la orden de prórroga debe venir acompañada con el acta expedida por la autoridad judicial que corresponda, con fin el continuar con el trámite. ✓ Con base en la orden de interceptación de comunicaciones pueden ser adelantadas tres (3) acciones. La primera es el ingreso de un IC al sistema de recepción y análisis de comunicaciones interceptadas, es decir, implica que inicie el procedimiento de interceptación de las comunicaciones. La segunda es la prórroga de la orden respecto a uno(s) IC. Y la tercera es la cancelación de aquellas órdenes vigentes. Las órdenes de interceptación de las comunicaciones son remitidas a través de los canales institucionales autorizados, que permitan asegurar su trazabilidad.		
3	**Trámite de la orden de interceptación de las comunicaciones** **Recepción** La recepción es la etapa en la cual es recibida y registrada la documentación para dar inicio al trámite de la interceptación de comunicaciones. Esta actividad está a cargo de los organismos con	Servidores públicos con funciones de policía judicial	*Formato orden de allanamiento y registro, retención de correspondencia – interceptación de comunicaciones *Formato solicitud de interceptación, prorroga o

[12] En los procesos regidos por la Ley 600 de 2000 y en los trámites de extinción del derecho de dominio, la única finalidad de la interceptación de comunicaciones es “buscar pruebas judiciales”. Véanse: Ley 600 de 2000, artículo 301, inciso primero y Ley 1708 de 2014, artículo 167, inciso primero.
[13] Ley 906 de 2004, artículo 235, inciso primero.
[14] Ibíd., artículo 235, inciso cuarto. Cfr. FGN, Directiva No. 0004 del 2 de noviembre de 2021, lineamientos 11 y 14.
[15] Ibíd., artículo 235, Inciso quinto.

NO.	ACTIVIDAD	RESPONSABLE	REGISTRO
	funciones de policía judicial. Para ello, tenga en cuenta lo siguiente: ✓ La documentación requerida para el trámite de interceptación de comunicaciones es la siguiente: - Verificaciones previas, dentro del formato dispuesto para ello. - Consulta pública en el sistema de información misional, en caso de que aplique. - Verificación de la portabilidad numérica del IC, cuando sea procedente. - Orden de interceptación de comunicaciones, dentro del formato que adopte la FGN para el efecto. - Solicitud de interceptación, prórroga o cancelación, dentro del formato que adopte la FGN para el efecto. - En caso de prórroga o cancelación de la orden de interceptación de comunicaciones, debe adjuntarse el acta de la audiencia efectuada ante el juez penal con función de control de garantías. - Contextualización del caso y IC, dentro del formato dispuesto para ello. ✓ Es necesario que el fiscal delegado y el **investigador** revisen y diligencien la documentación requerida para la materialización de la orden de interceptación de las comunicaciones. ✓ Una vez esté diligenciada la documentación, el **investigador** podrá radicar la documentación a través del medio destinado para este propósito, previa verificación por parte del jefe inmediato. ✓ Cuando la documentación sea radicada, el **jefe de sala** debe verificar que la sala de recepción y análisis de comunicaciones interceptadas cuente con la capacidad para tramitar la orden de interceptación de comunicaciones. En concreto, debe verificar si cuenta con (*i*) la cantidad de cupos de IC disponibles y (*ii*) el talento humano. En caso de que no cuente con alguna o ninguna de las dos, empleará el formato correspondiente. ✓ Posteriormente, el **programador** debe establecer que los documentos que soportan la solicitud de interceptación de		cancelación de las comunicaciones móviles *Formato solicitud de interceptación, prorroga o cancelación de datos móviles *Formato trámites urgentes

NO.	ACTIVIDAD	RESPONSABLE	REGISTRO
	comunicaciones cumplan con los requisitos establecidos en la normatividad vigente. En caso de que no cumplan con ello, serán devueltos a la autoridad judicial competente para que subsane lo que corresponda. ✓ Asimismo, el **programador** debe corroborar que (*i*) la documentación esté completa (que el número de folios, hojas o páginas corresponda; que sean diligenciados los campos obligatorios en los formatos; que sean aportados todos los documentos; entre otros) y (*ii*) que sean empleados los formatos vigentes. ✓ Además de recibir y registrar la solicitud, la recepción también implica garantizar la confidencialidad y seguridad de la información proporcionada. Para ello, es posible que los organismos con funciones de policía judicial empleen sistema de seguridad que permitan la encriptación de datos para las solicitudes y de otros productos que generen en el sistema. En caso de que la solicitud sea realizada a través de medios físicos, debe asegurarse el almacenamiento seguro y el cumplimiento de protocolos de seguridad de la información. ✓ La solicitud de interceptación de comunicaciones será surtida bajo un trámite urgente sólo cuando (*i*) exista una posible afectación a la seguridad nacional, (*ii*) es un caso de connotación nacional, (*iii*) está en riesgo la vida de una o varias personas y/o (*iv*) deben desarrollarse actividades operativas inmediatas y relevantes en el marco de la actuación penal. En cualquiera de estos casos deberá diligenciarse el formato destinado para el efecto y atender las instrucciones dadas por cada organismo con funciones de policía judicial. Cuando el investigador radique la documentación de un trámite urgente, el **jefe de sala** verificará que (*i*) no hayan transcurrido más de veinticuatro (24) horas desde la suscripción de la orden de interceptación de comunicaciones y la solicitud de interceptación, prórroga o cancelación; (*ii*) no hayan transcurrido más de veinticuatro (24) horas desde la suscripción de la documentación antes referida y su radicación; (*iii*) cuente con la disponibilidad de cupos de IC; y (*iv*) cuente con el recurso humano para adelantar el trámite urgente.		

NO.	ACTIVIDAD	RESPONSABLE	REGISTRO
4	**Gestión de la solicitud de interceptación de las comunicaciones** Una vez recibida y avalada la documentación, el **programador** debe remitir la solicitud de interceptación de comunicaciones al Departamento de Interceptaciones de las Comunicaciones (en adelante, DIC). Al respecto, tendrán en cuenta lo siguiente: ✓ El **programador** debe verificar e informar, oportunamente, cualquier tipo de novedad presentada con relación a la solicitud de interceptación de las comunicaciones. - Cuando <u>la solicitud es rechazada</u> por el DIC, el **programador** deberá informar inmediatamente al investigador. Adicionalmente, diligenciará el formato destinado para el efecto, con el fin de informar al fiscal delegado acerca del trámite de la solicitud. En ese sentido, deberá informarle los motivos por los cuales fue rechazada la solicitud, de acuerdo con lo que aparezca en el sistema de gestión administrativa. - Cuando exista una <u>falla técnica</u> en la sala de recepción y análisis de comunicaciones Interceptadas, el **programador** deberá informar inmediatamente al jefe de sala y al administrador de tecnologías de la información y las comunicaciones, con el fin de que adopten las acciones que correspondan. En este evento, el **jefe de sala**, el **programador** y el **administrador de tecnologías de la información y las comunicaciones** deben contar con un plan de contingencia para atender las solicitudes de trámites urgentes. ✓ Cuando las solicitudes de interceptación de comunicaciones son aprobadas por el DIC, el **programador** debe continuar con el trámite en el sistema de recepción y análisis de comunicaciones interceptadas destinado para el efecto, de acuerdo con la normativa, procedimientos y protocolos vigentes en la materia.	Servidor público con funciones de jefe de sala, el programador y el administrador de tecnologías de la información y las comunicaciones	*Formato solicitud de interceptación, prorroga o cancelación de las comunicaciones móviles *Formato solicitud de interceptación, prorroga o cancelación de datos móviles *Sistema de gestión administrativa *Formato de respuesta a solicitud de interceptación de comunicaciones

NO.	ACTIVIDAD	RESPONSABLE	REGISTRO
	Luego de que la solicitud sea aprobada y programada dentro de los sistemas, el **jefe de sala** debe realizar la asignación de la actividad a uno de los analistas de comunicaciones, con el fin de que sea materializada la orden de interceptación de comunicaciones.		
5	**Ejecución de la orden de interceptación de las comunicaciones** Los organismos con funciones de policía judicial deben capacitar a los analistas de comunicaciones en el ejercicio de sus funciones. Esto significa que debe garantizarse la aprehensión de conocimientos, en general, acerca de las limitaciones del derecho fundamental a la intimidad[16], del principio del interés superior del menor y del derecho fundamental al *habeas data*. En especial, debe garantizarse que los **analistas de comunicaciones** conozcan y apliquen la normatividad vigente a nivel constitucional, legal y reglamentario, además de la jurisprudencia, acerca de la interceptación de las comunicaciones. Por ello, en desarrollo de su actividad deben tener en cuenta lo siguiente: ✓ Una vez el **analista de comunicaciones** reciba la asignación de la actividad, es necesario que: - Verifique que la documentación esté completa. - Realice una lectura detenida de cada uno de los documentos que le fueron entregados, a efectos de determinar: ▪ El delito(s) objeto de la actuación. ▪ La finalidad de la orden de interceptación de comunicaciones. ▪ Los motivos fundados que sustentan la orden judicial[17]. ▪ El término de la orden de interceptación de comunicaciones.	Servidores públicos con funciones de analista de comunicaciones y jefe de sala	*Formato orden de allanamiento y registro, retención de correspondencia – interceptación de comunicaciones *Formato solicitud de interceptación, prorroga o cancelación de las comunicaciones móviles *Formato solicitud de interceptación, prorroga o cancelación de datos móviles *Formato de contextualización previa para el analista de comunicaciones interceptadas

[16] La jurisprudencia de la Corte Constitucional ha reconocido la relación entre el secreto profesional y el derecho fundamental a la intimidad. En particular, en la sentencia C-301 de 2012, el Alto Tribunal indicó que existe una relación inescindible entre estos y que "el secreto profesional tiene un alcance distinto en cada profesión, dependiendo del radio de cercanía que la misma tenga sobre el derecho a la intimidad personal y familiar y del control del Estado sobre las mismas" (se omite pie de página). Por ejemplo, entre médico y paciente, clérigo con el feligrés, periodista con su fuente, abogado con su cliente, entre otros.

[17] El **analista de comunicaciones** debe tener en cuenta que los motivos fundados aparecen en la orden de interceptación de comunicaciones y en el formato de verificaciones previas que sea adoptado para el efecto.

NO.	ACTIVIDAD	RESPONSABLE	REGISTRO
	▪ La autoridad que ordena la interceptación de comunicaciones y el investigador asignado al caso. ▪ Las generalidades del caso[18]. ▪ Las personas que están siendo investigadas, en caso de que aparezca dicha información. - Corrobore que los IC están debidamente programados (por ejemplo, que el IC corresponda con el programado en el sistema de recepción y análisis de las comunicaciones), asignados a su usuario, y que generan registros. Asimismo, debe comprobar que la información relacionada en la unidad documental corresponda con lo que aparece en la solución tecnológica. - Reporte inmediatamente al jefe de sala y/ o a su superior inmediato cualquier inconsistencia que encuentre, con el fin de que sean adoptadas las medidas pertinentes. ✓ Dentro de los cinco (5) días siguientes a la asignación de la actividad, y en caso de que no haya inconsistencias en la documentación entregada, el **analista de comunicaciones** deberá solicitarle al investigador y al fiscal delegado la reunión de contextualización sobre las necesidades investigativas[19], los medios de difusión y la manera en que será presentada la información. En este espacio, dicho servidor público procurará obtener toda la información que le permita enfocar la actividad que va a realizar. En ese sentido, es recomendable que indague, entre otras, acerca de lo siguiente: - Características de la(s) personas(s) presuntamente vinculada(s) a la actuación. - La forma o la manera en que vienen operando los posibles indiciados en su actuar criminal. - Si se trata o no de una estructura criminal. En caso afirmativo, es		

[18] En cuanto a las generalidades del caso, estas aparecen en la orden de interceptación de comunicaciones y en el formato de contextualización previa que sea adoptado para este fin.
[19] FGN, Directiva No. 0004 del 2 de noviembre de 2021, lineamiento 17.

NO.	ACTIVIDAD	RESPONSABLE	REGISTRO
	aconsejable preguntar acerca de la caracterización y denominación de esta, la territorialidad (el lugar de los hechos, el territorio donde ejercen sus actividades ilícitas y el interés estratégico en este, entre otros), la temporalidad del delito o actividad ilícita investigada, el organigrama judicial y la tipología organizacional, sus integrantes (roles, cargos y rangos), cabecillas (experiencia y experticia), *modus operandi*, los tipos de control que ejercen, las dinámicas sociales y/o las formas que han establecido para relacionarse con la comunidad, la manera en que sus miembros atienden las órdenes, las economías ilegales en que actúan, entre otros aspectos que puedan guiar su labor. - Algunos aspectos sobre el lenguaje criminal (por ejemplo, muletillas que puedan identificarse) que usan las personas presuntamente vinculadas con la conducta criminal. - Alias o seudónimos de quienes intervienen en las comunicaciones. - Cuál es la participación de las personas que intervienen en las comunicaciones, de cara a las hipótesis delictivas del caso. - Información acerca de las actividades ilícitas o lícitas de la persona vinculada a la conducta punible investigada. - La necesidad de ubicar bienes o activos relacionados con la conducta punible investigada. ✓ Los **jefes de sala** y/o el superior inmediato de los analistas de comunicaciones deben verificar que dicho servidor público solicite, dentro de los cinco (5) días siguientes a la asignación de la actividad, la reunión de contextualización, los medios de difusión y la manera en que será presentada la información. ✓ La reunión de contextualización debe constar en el formato dispuesto para el efecto. El **jefe de sala** y/o el superior inmediato del analista de comunicaciones debe verificar que este espacio sea desarrollado.		

NO.	ACTIVIDAD	RESPONSABLE	REGISTRO
	✓ Cuando inicie la actividad, el **analista de comunicaciones** debe verificar[20] la titularidad y uso del IC para establecer que las comunicaciones interceptadas (*i*) son de la persona vinculada a la conducta punible objeto de la actuación, (*ii*) pueden aportar información acerca de la ubicación del procesado o condenado, (*iii*) si la persona es un aforado constitucional o legal[21]. Para ello, es aconsejable que dicho servidor público tenga en cuenta la información suministrada en la reunión de contextualización. ✓ Cuando el **analista de comunicaciones** pueda inferir y/o determinar que el titular y/o usuario del IC es el abogado defensor[22] del procesado o condenado dentro de la actuación judicial, informará a la autoridad judicial competente acerca de esto, dentro de las veinticuatro (24) horas siguientes a que haya constatado este hecho[23]. ✓ Cuando el **analista de comunicaciones** evidencia conversaciones entre el procesado o condenado y su abogado defensor acerca de asuntos judiciales, estas serán informadas a la autoridad judicial competente, y no serán tenidas en cuenta ni referenciadas dentro del análisis que realice[24]. En caso de que las conversaciones muestran que el profesional del derecho podría estar involucrado en la comisión de un delito, deberá informarse al fiscal delegado para que adopte las decisiones correspondientes[25]. ✓ Si dejan de producirse registros en el sistema de recepción y análisis de comunicaciones		

[20] En la medida de lo posible, esto significa que el **analista de comunicaciones** informará al investigador los datos obtenidos sobre la posible identificación del titular y/o usuario del IC. Esto, con el propósito de que el **investigador** adelante las actividades correspondientes.
[21] FGN, Directiva No. 0004 del 2 de noviembre de 2021, lineamiento 17.
[22] La jurisprudencia de la Corte Suprema de Justicia ha precisado que la calidad de defensor no puede inferirse simplemente por el hecho de que una persona tenga un título como abogada(o), sino que debe acreditarse conforme a las reglas procesales aplicables. Al respecto, véanse: Corte Suprema de Justicia, Sala Especial de Instrucción, auto AEI 00156-2020 del 3 de agosto de 2020, radicado No. 52240; Ley 906 de 2004, artículos 118 y ss.; y Ley 600 de 2000, artículos 128 y ss.
[23] Ley 906 de 2004, artículo 235, inciso tercero.
[24] Ibid., artículo 345, numeral 1.
[25] La Corte Constitucional ha afirmado que existen circunstancias excepcionales en las que podría revelarse información reservada, con el fin de salvaguardar derechos de terceros. Por ejemplo, cuando sea necesario impedir la comisión de un delito o el daño a terceros. Esto último coincide con los deberes legalmente establecidos para los servidores públicos en cuanto a denunciar la comisión de delitos. Al respecto, véanse: Ley 1952 de 2019, artículos 38, numeral 25; 61, numeral 3; y 65; y Ley 599 de 2000, artículos 219B, adicionado por la Ley 679 de 2001; artículo 35, parágrafo transitorio; 340A, adicionado por la Ley 1908 de 2018, artículo 6; y 417. Cfr. Corte Constitucional, sentencia C-301 de 2012.

NO.	ACTIVIDAD	RESPONSABLE	REGISTRO
	interceptadas, el **analista de comunicaciones** debe: - Determinar, de acuerdo con el delito(s) y la contextualización, si la ausencia de registros podría obedecer al manejo del equipo móvil por parte de las personas objeto de esta actividad investigativa y/o a su actuar criminal. - Verificar, en el sistema de recepción y análisis de comunicaciones interceptadas, si el IC continúa en uso o no. - Si el analista de comunicaciones establece que este es un evento anormal, puesto que (*i*) no tiene relación con el actuar criminal, (*ii*) ni con el uso del IC, solicitará al **programador** y al **administrador de tecnologías de la información y las comunicaciones** las revisiones correspondientes. De ser necesario, **la sala** podrá escalar el requerimiento al **DIC**, para que adelante una revisión técnica. ✓ En caso de que los registros que produce el sistema de recepción y análisis de comunicaciones interceptadas correspondan a un IC diferente al que está programado, el **analista de comunicaciones** solicitará al **programador** una verificación técnica del IC programado en el sistema de recepción y análisis de comunicaciones interceptadas. Si el IC está correctamente programado, el **programador** deberá solicitar una revisión técnica al **DIC**. ✓ En cualquiera de los eventos antes referidos, el **analista de comunicaciones** debe informar acerca de estos sucesos al fiscal delegado y al investigador. Asimismo, deberá informar los resultados de las revisiones técnicas del DIC, en caso de que estas deban surtirse. Para el efecto, rendirá los informes correspondientes. ✓ En general, el analista de comunicaciones debe reportar las fallas en los elementos de hardware y software de las salas de recepción y análisis de comunicaciones interceptadas al **administrador de tecnologías de la información y las comunicaciones**, quien efectuará la revisión y generará los correctivos que sean necesarios.		

NO.	ACTIVIDAD	RESPONSABLE	REGISTRO
	✓ Asimismo, el **jefe de sala** hará seguimiento a las respuestas técnicas emitidas por el programador, administrador de tecnologías de la información y las comunicaciones o por el DIC. Igualmente, pondrá en conocimiento del analista de comunicaciones las respuestas que sean emitidas. Conforme a los resultados, el analista de comunicaciones podrá sugerir la (*i*) prórroga, (*ii*) cancelación, (*iii*) interceptación de nuevos IC o (*iv*) el desarrollo de otros actos de indagación e investigación		

5.2 INFORMES DE POLICÍA JUDICIAL Y DIFUSIÓN DE INFORMACIÓN

Los informes de policía judicial son el medio legal a través del cual los **analistas de comunicaciones**, en este caso, comunican los avances y/o resultados de la interceptación de las comunicaciones a la autoridad competente[26]. Para ello, dichos servidores públicos pueden presentar informes parciales o definitivos. Los primeros –los informes parciales– son aquellos que comunican el avance y/o cualquier eventualidad en el desarrollo de la actividad investigativa, los cuales pueden ser solicitados por el fiscal delegado en cualquier momento[27]. Estos pueden ser de dos tipos:

- ✓ Inmediatos: son aquellos que deben presentar los analistas de comunicaciones a los fiscales delegados cuando concurra alguna de las siguientes circunstancias[28]:

  (i) El analista de comunicaciones encuentre información que amerita una actuación inmediata para recolectar EMP y EF.
  (ii) Deba impedirse la comisión de un delito(s).
  (iii) El analista de comunicaciones evidencia, de acuerdo con los avances y hallazgos, que la interceptación de comunicaciones ha desbordado el objeto legítimo de la actuación, puesto que la información recaudada (*a*) es ajena al hecho investigado, (*b*) alude a aspectos relacionados con el derecho fundamental a la intimidad y (*c*) carece de relevancia penal.
  (iv) El analista de comunicaciones evidencia que la interceptación de comunicaciones no está produciendo resultados para la actuación judicial, "en términos de esclarecimiento y judicialización de hechos que se adecúen a la estructura típica de un delito"[29].

[26] Para una definición más detallada de "informes de policía judicial", véase: Consejo Nacional de Policía Judicial, "Manual Único de Policía Judicial", documento vigente.
[27] Al respecto, véase: FGN, Directiva No. 0004 del 2 de noviembre de 2021, lineamiento 19.
[28] FGN, Directiva No. 0004 del 2 de noviembre de 2021, lineamientos 17 y 18.
[29] Ibídem.

(v) Cuando se trata de un aforado constitucional o legal[30].[31]

- ✓ Periódicos: son aquellos que deben presentarse al cumplirse los días 30 y 120 desde el inicio del cumplimiento de la orden de interceptación de comunicaciones o de su prórroga, en caso de que no se advierta ninguna de las circunstancias antes descritas[32] o de que no hayan sido solicitados por el fiscal delegado[33].

Y los segundos –los informes definitivos– son aquellos que deben presentarse al finalizar el plazo de la orden de interceptación de las comunicaciones, y que contienen los resultados de la actividad investigativa. Eventualmente, los informes parciales inmediatos rendidos bajo las circunstancias relacionadas arriba en los numerales (iii), (iv) y (v), pueden tratarse de informes definitivos, de acuerdo con la valoración que hagan los fiscales delegados de estos[34].

Adicionalmente, los servidores públicos con funciones de policía judicial que intervienen en la ejecución de la orden de interceptación de comunicaciones deben tener en cuenta lo siguiente:

- ✓ Los **analistas de comunicaciones** deberán rendir los informes parciales inmediatos dentro de las veinticuatro (24) horas siguientes a la constatación de los eventos antes descritos. Adicionalmente, deberán informar al **jefe de sala** y/o a su superior inmediato, con el fin de que supervise la ejecución de esta labor dentro de los términos aquí dispuestos.
- ✓ Sin perjuicio de lo anterior, al día quince (15) desde que inició la ejecución de la actividad investigativa, los **analistas de comunicaciones** rendirán un informe parcial inmediato cuando constaten que la interceptación de comunicaciones no está produciendo resultados para la actuación judicial.
- ✓ Los **analistas de comunicaciones** deben usar los formatos vigentes para rendir los informes de policía judicial a que haya lugar. Asimismo, el diligenciamiento de estos debe estar acorde con los diferentes documentos (directivas, resoluciones, guías, procedimientos, entre otros) generados en esta materia.

NO.	ACTIVIDAD	RESPONSABLE	REGISTRO
1	**Elaboración y presentación de informes de policía judicial:** Para la elaboración de los informes de policía judicial, los **analistas de comunicaciones** y los **jefes de sala** y/o sus superiores jerárquicos deben tener en cuenta lo siguiente:	Servidores públicos con funciones de analista de comunicaciones y jefe de sala y/o el superior inmediato del	Formato Informe Investigador de Campo FPJ-11

[30] Véanse: Constitución Política de Colombia, artículos 174 y 235, numerales 3 y 5; Ley 1957 de 2019, artículo 105; Ley 906 de 2004, artículos 32, numeral 8; 33, numeral 2 y 34, numeral 2; Ley 600 de 2000, artículos 75, numeral 9 y 77, numeral 2; y FGN, Directiva No. 0003 del 7 de febrero de 2022.
[31] FGN, Directiva No. 0004 del 2 de noviembre de 2021, lineamiento 17.
[32] Ibíd., lineamiento 22.
[33] Ibíd., lineamiento 19.
[34] Ibíd., lineamientos 17, 18 y 20.

NO.	ACTIVIDAD	RESPONSABLE	REGISTRO
	✓ El contenido de los informes de policía judicial debe ajustarse a lo establecido en la presente guía. ✓ El formato para la presentación de los informes de policía judicial debe ser diligenciarse en su totalidad, sin modificarlo. Para ello, aquellos campos vacíos o que no apliquen deben estar consignados con un “N/A” (no aplica). ✓ En cualquier caso, los informes deben redactarse de manera clara, detallada, precisa, lógica, coherente, cronológica y estructurada, en párrafos cortos, de acuerdo con los temas principales, a fin de permitir una mayor comprensión por parte del lector. Esto adquiere mayor relevancia cuando se trata de presentar los resultados de la actividad investigativa. ✓ El contenido de los informes de policía judicial debe estar relacionado con los fines de la investigación, la(s) hipótesis delictiva(s), la finalidad y los motivos fundados de la orden de interceptación de comunicaciones. En consecuencia, lo consignado allí debe aportar elementos para confirmar, desvirtuar o ampliar la(s) hipótesis delictiva(s). En ese sentido, en estos deben: - Describir el fundamento por el cual se rinde el informe, basado en la información contenida en la finalidad y los motivos fundados de la orden de interceptación. - Indicar a la autoridad judicial competente las razones que le permiten hacer sugerencias (interceptar nuevos IC, adelantar nuevos actos de indagación e investigación, prorrogar o cancelar la orden de interceptación de comunicaciones), de acuerdo con la información obtenida en el curso de la actividad investigativa. En esa medida, los analistas de comunicaciones podrán dar alcance a los informes de policía judicial que hayan sido rendidos previamente. - Es aconsejable contextualizar a la autoridad judicial competente sobre la información relacionada en los registros de la actividad investigativa. En este caso, el analista de comunicaciones deberá presentar esta información de manera orientativa. - En la presentación de los resultados deben emplearse una terminología que garantice la presunción de inocencia, permita identificar a los usuarios, posibles ubicaciones, presuntas	analista de comunicaciones.	

NO.	ACTIVIDAD	RESPONSABLE	REGISTRO
	actividades ilícitas, contactos relacionados, entre otros. - Diligenciar los datos correspondientes a los diferentes grados de intimidad (personal, familiar, social y gremial). ✓ Los informes de policía judicial no deben contener juicios de valor o informaciones que no estén sustentadas en los registros del IC. ✓ Los informes de policía judicial deben contener una síntesis de la información más relevante para los fines de la investigación, utilizando las observaciones del analista (en adelante, ODA) en aquellos casos en que sea necesario aclarar, relacionar eventos o ampliar informaciones obtenidas en otros ID. ✓ Es recomendable que los resultados de la actividad investigativa sean presentados bajo el siguiente esquema: - Fecha, hora e ID de la primera actividad o registro en el sistema de recepción y análisis de comunicaciones interceptadas. - Datos que coadyuven a la identificación del usuario del IC. - Las presuntas actividades ilícitas que desarrolla el usuario de la comunicación interceptada. En caso de no obtener información relevante para la actuación, pueden relacionarse las actividades a las que se dedica el usuario de la comunicación interceptada. - Las personas con las cuales mantiene comunicación el usuario del IC para planear y ejecutar presuntas actividades ilícitas, relacionando el rol de cada uno. Para efectos de ubicación, pueden relacionarse los interlocutores, aportando los números de teléfono u otros datos de las comunicaciones que usan. - Número(s) telefónico(s) u otro tipo de comunicación(es) que pueden resultar de interés para la actuación. Por ejemplo, números de teléfono, correos electrónicos, perfiles en redes sociales, finanzas criminales, números de cuentas, entre otros. - *Modus operandi*. - Lenguaje criminal o jerga utilizada por los interlocutores que integran la presunta organización criminal o delincuencial. - Bienes muebles, inmuebles y activos señalados por los interlocutores.		

NO.	ACTIVIDAD	RESPONSABLE	REGISTRO
	- Eventos de importancia, relacionando los ID. - Otras informaciones de importancia. - Convenciones o abreviaturas. - Sinopsis y ODA de las comunicaciones de importancia para los fines de la actuación. - Sugerencias respetuosas al **investigador** y a la autoridad judicial competente que ordenó la interceptación, para la ejecución de otros actos de indagación e investigación. - Una relación de los informes de policía judicial emitidos con relación a la actividad investigativa y el IC objeto de esta, con fechas y el número de(l) (los) informe(s). En el caso de extracción de información, también debe relacionarse la cantidad de evidencias entregadas previamente. Posterior a su elaboración, los informes de policía judicial deben ser revisados por el **jefe de sala** y/o el superior inmediato del analista de comunicaciones. Así, una vez aprobado el informe, este debe ser remitido al investigador y al fiscal delegado a través de canales que garanticen la autenticidad, completitud, confidencialidad, inalterabilidad, integridad y seguridad de la información allí contenida. En otras palabras: deben evitarse adiciones, modificaciones o supresiones de datos tales como números de informes, fechas, ID, entre otros. Para esto, preferiblemente deben emplearse medios digitales que permitan verificar las fechas y horas de envío y recepción, además de cumplir con lo anteriormente señalado.		
2	**Difusión de información** El **analista de comunicaciones** debe difundir, oportunamente, la información que sea de interés para los fines de la actuación judicial. Para ello, podrá realizar: ✓ Reportes, los cuales deben quedar consignados en el formato, sistema de información y/o plataformas de mensajería instantánea autorizadas para estos efectos. ✓ Alertas, las cuales deben ser emitidas de forma inmediata al (*i*) jefe de sala y/o superior inmediato del analista de comunicaciones (*ii*) al investigador y (iii) autoridad judicial competente. Para esto, deben emplearse los canales y/o medios que garanticen la confidencialidad y reserva de la información, de tal manera que no sea afectada la actuación judicial. Asimismo, el **investigador** debe comunicar a la autoridad judicial competente que ordenó la interceptación de las comunicaciones la información obtenida, las	Servidores públicos con funciones de analista de comunicaciones y jefe de sala	Sistema de información o formato vigentes

NO.	ACTIVIDAD	RESPONSABLE	REGISTRO
	actuaciones realizadas y desplegar las acciones que eviten la comisión de un delito(s). Asimismo, el **investigador** debe controlar los resultados obtenidos a través de los IC con el fin de mantener informado al fiscal delegado y de adelantar las gestiones pertinentes con su jefe inmediato. Para el efecto, podrá coordinar reuniones de difusión y avances, las cuales buscan conocer los progresos de la actividad investigativa, la información obtenida para los fines de la actuación judicial y utilidad de esta. Este tipo de espacios deben ser autorizados por el **jefe de sala** y podrán desarrollarse en el sitio asignado para estos efectos en la sala de recepción y análisis de comunicaciones interceptadas. En el evento que la reunión no pueda desarrollarse presencialmente, podrán emplearse las herramientas tecnológicas autorizadas para la realización de esta, a través de videoconferencia o teleconferencia. De cualquier forma, estas reuniones deben cumplir con los siguientes parámetros: ✓ La reunión debe desarrollarse bajo los protocolos de seguridad que garanticen la reserva y confidencialidad de la información. ✓ Debe dejarse constancia de la reunión (sea presencial o virtual) en acta y/o en el sistema de información vigente, en caso de que este lo permita. ✓ Si en el desarrollo de la reunión son escuchados y/u observados audios y/o datos obtenidos a través de interceptación de las comunicaciones, deberán registrarse en mencionada acta y/o sistema de información vigente, en caso de que este lo permita, los eventos relevantes que fueron objeto de este espacio. Para el efecto, deben identificarse los eventos escuchados y/u observados. ✓ Única y exclusivamente podrán adelantarse reuniones de difusión y avances con los investigadores que estén registrados en la orden de interceptación de comunicaciones. En caso de que haya cambios en los servidores públicos con funciones de policía judicial asignados a la actuación judicial, el **investigador** y su jefe inmediato deberán comunicar de este hecho al **jefe de sala**, quien informará sobre esto al analista de comunicaciones por escrito. ✓ Para las reuniones de difusión y avances realizadas a través de videoconferencia o teleconferencia, el **analista de comunicaciones**, el **investigador** y el fiscal delegado deben estar		

NO.	ACTIVIDAD	RESPONSABLE	REGISTRO
	en sitios seguros que garanticen la confidencialidad y reserva de la información. ✓ Asimismo, únicamente podrán realizar reuniones de difusión y avances a través de las herramientas tecnológicas autorizadas para el efecto. Esto significa que solamente deben usarse los equipos institucionales autorizados y configurados para ello. El **analista de comunicaciones** sólo podrá reproducir audios y/o datos en reuniones presenciales. En ningún caso podrá hacerlo a través de videoconferencia o teleconferencia o de otras herramientas tecnológicas autorizadas para el efecto.		

5.3. EXTRACCIÓN DE INFORMACIÓN

NO.	ACTIVIDAD	RESPONSABLE	REGISTRO
1	La extracción de la información para evidencia debe ser ordenada por la autoridad judicial competente[35], mediante el formato definido para tal fin por la FGN[36]. Para ello, el **analista de comunicaciones**, previo a la solicitud, coordinará con el investigador y la autoridad judicial competente la fecha de realización de la extracción de la información recolectada[37], con el fin de que sean adelantadas las diligencias correspondientes[38]. Así, una vez sea emitida la orden, el **investigador** la comunicará a la sala de recepción y análisis de comunicaciones interceptadas para que sean iniciados los trámites respectivos.	Servidores públicos con funciones de analista de comunicaciones, jefe de sala, investigador y autoridad judicial competente	Formato Orden de Extracción Producto Interceptación de Comunicaciones
	Al respecto, debe tenerse en cuenta lo siguiente: ✓ Cuando sea recibida la orden de extracción de la información, el **jefe de sala** y/o el **administrador de tecnologías de la**	Servidor público con funciones de Jefe de Sala o administrador de tecnologías de la	Formato Orden de Extracción Producto Interceptación de Comunicaciones

[35] Ibíd., lineamiento 23.
[36] Ibíd., lineamiento 27.
[37] Si bien la extracción de información es realizada por orden de la autoridad judicial competente, esta actividad está supeditada por la capacidad técnica y la cantidad de eventos que registre el sistema de recepción y análisis de comunicaciones interceptadas para cada IC. En consecuencia, el tiempo que dure esta actividad no dependerá, en principio, de las salas de recepción y análisis de comunicación interceptada, de los analistas de comunicaciones ni de los organismos con funciones de policía judicial. Por este motivo, es necesario que exista coordinación y articulación, con el fin de evitar traumatismos en las diligencias que deban adelantarse con posterioridad a la extracción de la información.
[38] Constitución Política de Colombia, artículo 250, numeral 2, modificado por el Acto Legislativo 03 de 2002, artículo 2; Ley 906 de 2004, artículo 237, modificado por la Ley 1453 de 2011, artículo 68; Ley 975 de 2005, artículo 62; Ley 1708 de 2014, artículos 26, numeral 2; 33, parágrafo 1; y 116, numeral 1Los procesos penales y los trámites de extinción del derecho de dominio, adelantados bajo las leyes 906 de 2004 y 1708 de 2014, requieren un control judicial posterior, a cargo de jueces con función de control de garantías. Al respecto, véanse.

NO.	ACTIVIDAD	RESPONSABLE	REGISTRO
	información y las comunicaciones de las salas de recepción y análisis de comunicaciones interceptadas debe: - Verificar que los datos contenidos en la orden de extracción de información (NUNC, IC referidos, nombre de la autoridad judicial que emite la orden y del investigador, fiscalía delegada, entre otros) corresponda con la registrada en el sistema de recepción y análisis de comunicaciones interceptadas, en el sistema de información y/o bases de datos que maneje el organismo de policía judicial, y en la orden y la solicitud de interceptación de comunicaciones. Particularmente, debe confirmar que los IC referidos en la orden sean los mismos que aparecen en la orden de interceptación de las comunicaciones, es decir, que estén en el marco de la actuación judicial respecto a la cual es requerida la extracción. - Revisar el (los) período(s) solicitado(s) de los IC. - Corroborar que la orden de extracción de información tiene su origen en el canal institucional que defina cada organismo con funciones de policía judicial, y que permita asegurar la trazabilidad. Lo anterior, debido a que la siguiente extracción iniciará desde la fecha, hora y evento (ID) siguientes a la registrada en la primera extracción de información. Esto, con el fin de no interrumpir la continuidad en la recolección de la información[39] y optimizar los recursos asignados a las salas de recepción y análisis de comunicaciones interceptadas. Una vez el **jefe de sala** haya autorizado la extracción, el **administrador de tecnologías de la información y las comunicaciones** realizará la actuación antes referida.	información y las comunicaciones	
	✓ Posteriormente, el **administrador de tecnologías de la información y las comunicaciones** dará el tiempo estimado[40]	Servidor público con funciones de Jefe de Sala o	Formato Orden de Extracción Producto

[39] FGN, Directiva No. 0004 del 2 de noviembre de 2021, lineamiento 24.
[40] Véase: supra cit. 37.

NO.	ACTIVIDAD	RESPONSABLE	REGISTRO
	que tomará el proceso y supervisará su adecuada ejecución. Al respecto, informará al analista de comunicaciones. ✓ Cuando el sistema de recepción y análisis de comunicaciones interceptadas concluya el proceso de exportación, grabación y rotulado, el **jefe de sala** y/o el **administrador de tecnologías de la información y las comunicaciones** verificarán que la evidencia haya sido correctamente generada y que cuente con los protocolos de seguridad respectivos; recogerán la evidencia; y harán el registro de la información correspondiente en el libro, formato y/o sistemas de información establecidos para la entrega de evidencias. En cada caso, deberá identificar los eventos (ID) y la cantidad de EMP contentivos de estos.	administrador de tecnologías de la información y las comunicaciones	Interceptación de Comunicaciones
	✓ Luego de esto, el **analista de comunicaciones** revisará, entre otros, lo siguiente: - La cantidad de registros que fueron grabados, identificando el primero y el último evento (ID), en cada caso. - Que el contenido haya sido correctamente grabado, es decir, que no haya ninguna novedad técnica con relación a la extracción. ✓ Si hay alguna novedad técnica con relación a la evidencia obtenida (por ejemplo, fallos en la reproducción de la grabación), el **administrador de tecnologías de la información y las comunicaciones** realizará la verificación correspondiente. En caso de requerirse una nueva extracción debido a una novedad técnica, dicho servidor público realizará el borrado seguro de los contenedores de la evidencia y dejará constancia de ello en formato, libro, base de datos y/o sistema de información destinado para el efecto. ✓ Asimismo, el **analista de comunicaciones** registrará, en el sistema de información misional correspondiente, los EMP y EF o ILO anexos al informe de policía judicial que presenta.[41] ✓ El **analista de comunicaciones** entregará al investigador los EMP y EF o ILO.	Servidor público con funciones de analista de comunicaciones, Jefe de Sala, administrador de tecnologías de la información e investigador.	Formato, libro, acta, base de datos y/o sistema de información destinado para el efecto

[41] FGN, Directiva No. 0004 del 2 de noviembre de 2021, lineamiento 23.

NO.	ACTIVIDAD	RESPONSABLE	REGISTRO
	✓ Una vez recibidos los EMP y EF, el **investigador** realizará el registro de continuidad en el sistema de información misional correspondiente. Consecuentemente, los entregará al almacén de evidencias. ✓ En general, el **analista de comunicaciones** y el **investigador** deberán diligenciar el registro de cadena de custodia, de acuerdo con lo establecido en el "Manual del Sistema de Cadena de Custodia" y en la normatividad vigente. ✓ Si la autoridad judicial ordena la extracción de información dentro del plazo de ejecución de la orden de interceptación de las comunicaciones, con el fin de comparecer a una diligencia judicial, el **jefe de sala** solicitará copia del acta de audiencia a los ocho (8) días siguientes a la entrega de la evidencia, siempre que esta no haya sido allegada a la sala de recepción y análisis de comunicaciones interceptadas. En caso de que no sea suministrado dicho documento, el jefe de la sala podrá dirigirse al superior inmediato del fiscal delegado para reiterar la solicitud. Este mismo procedimiento debe seguirse cuando la diligencia judicial no pueda realizarse. En este evento, el jefe de sala solicitará información acerca de las razones por las cuales no fue realizada la audiencia. ✓ En el evento de que la autoridad judicial ordene la extracción de información dentro del plazo de ejecución de la orden de interceptación de las comunicaciones, con el fin de comparecer a una diligencia judicial, y el investigador no recoja los EMP y EF, el **jefe de sala** solicitará al fiscal delegado, a los ocho (8) días siguientes a la generación de la evidencia, que decida acerca de la disposición de los EMP y EF, de acuerdo con lo establecido en el "Manual del Sistema de Cadena de Custodia" y en la normatividad vigente. Si el fiscal delegado no da respuesta, el **jefe de sala** podrá dirigirse al superior inmediato de la autoridad judicial. ✓ Las solicitudes de extracción referidas a información previamente recolectada y sometida a las reglas de cadena de custodia, es decir, a EMP y EF que ya fueron		

NO.	ACTIVIDAD	RESPONSABLE	REGISTRO
	entregados, serán denegadas[42]. Lo anterior, teniendo en cuenta que, por regla general, esta actividad es realizada una única vez en dos ejemplares[43], con el fin de que las copias idénticas pueden ser "obtenidas de la evidencia extraída y debidamente legalizada que reposa en el almacén de evidencias"[44], de acuerdo con la política de almacenamiento y disposición de EMP y EF derivada de la interceptación de comunicaciones que sea adoptada para el efecto. ✓ En caso de que una autoridad judicial diferente a la que ordenó la interceptación de las comunicaciones solicite copia de la extracción de información ya realizada en el marco de otra actuación, el **jefe de sala** remitirá o trasladará esta solicitud a aquella autoridad judicial que ordenó la actividad investigativa. ✓ Aun cuando los IC aporten o no elementos de juicio para los fines de la actuación judicial, es necesario que sea extraída la información obtenida con la actividad investigativa, de acuerdo con la orden que emita la autoridad judicial.		

5.4. AUDIENCIAS

Luego de la extracción de la información obtenida con la actividad investigativa, el **analista de comunicaciones** presentará el informe de policía judicial, bajo las previsiones establecidas en los numerales anteriores. Luego de ello, dicho servidor público podrá ser convocado a diferentes diligencias judiciales, en las diferentes fases del proceso penal. Sobre estas, debe tenerse en cuenta lo siguiente:

- ✓ En general, el **analista de comunicaciones** participará en las diligencias judiciales a las cuales sea convocado, siempre y cuando medie citación y/o el requerimiento de la autoridad judicial competente dentro un tiempo razonable. Para el efecto, estas serán canalizadas a través del **jefe de sala** llevará un registro de estas para el control y seguimiento que corresponda.
- ✓ Una vez el **analista de comunicaciones** tenga conocimiento de la diligencia judicial, surtirá todos los trámites administrativos que correspondan, con el fin de asegurar su asistencia y participación.
- ✓ El **jefe de sala** que reciba una citación y/o requerimiento judicial para que un servidor público que fungió como analista de comunicaciones, y que continúa prestando sus

[42] Excepcionalmente, podrán concederse este tipo de solicitudes cuando estén debidamente justificadas bajo eventos de caso fortuito, fuerza mayor o hechos de un tercero ajenos a la voluntad de las autoridades judiciales y actores del SIC.
[43] FGN, Directiva No. 0004 del 2 de noviembre de 2021, lineamiento 23.
[44] Ibídem.

servicios en la correspondiente entidad, asista a una diligencia judicial, deberá trasladarla a la dependencia de talento humano de cada organismo con funciones de policía judicial. El mismo trámite deberá surtirse cuando la persona ya no labore en la entidad.

Para las audiencias de control de legalidad, los servidores públicos con funciones de policía judicial deben tener en cuenta lo siguiente:

- ✓ Una vez el fiscal delegado reciba el informe de policía judicial empezarán a correr el término para que acuda a la audiencia de control de legalidad previa[45] o posterior[46].
- ✓ En caso de que sea necesaria la presencia del analista de comunicaciones en la audiencia de control de legalidad, el **jefe de sala** verificará que medie solicitud de la autoridad judicial competente. En ese evento, el **analista de comunicaciones** coordinará su intervención con el fiscal delegado y acudirá con los elementos y las herramientas que considere necesarias para participar dentro de la diligencia.
- ✓ Los EMP y EF o ILO deben estar disponibles, en el evento de ser requeridos por el juez penal con función de control de garantías.
- ✓ Luego de surtir la audiencia de control de legalidad, el fiscal delegado remitirá el acta de la audiencia, con el fin de (*i*) continuar con la actividad investigativa, en caso de que haya sido prorrogada, o (*ii*) para que esta sea cancelada. Para el efecto, el **investigador** fungirá como canal entre el fiscal delegado y la sala de recepción y análisis de comunicaciones interceptadas. Si la autoridad judicial no remite el acta, el **jefe de sala** podrá requerirlo para ello.

Por último, es posible que el **analista de comunicaciones** sea convocado al juicio oral. Si ello es así, coordinará su participación con el fiscal delegado. Para esto, el mencionado servidor público, una vez sea citado a esta diligencia, establecerá contacto con el fiscal delegado y su investigador, y solicitará los informes y EMP derivados de la ejecución de la actividad investigativa con el fin de preparar su intervención.

6. ANEXOS

Se presentan como documentos adjuntos para el desarrollo para el manejo de las actividades de interceptación:

1. FORMATO DE CONTEXTUALIZACIÓN PREVIA PARA EL ANALISTA DE COMUNICACIONES INTERCEPTADAS
2. FORMATO VERIFICACIONES PREVIAS PARA LA SOLICITUD DEINTERCEPTACIÓN DE COMUNICACIONES
3. FORMATO DE RESPUESTA A SOLICITUD DE INTERCEPTACIÓN DE COMUNICACIONES
4. FORMATO DE SOLICITUD DE TRÁMITES URGENTES INTERCEPTACIÓN, PRÓRROGA O CANCELACIÓN

[45] Ley 906 de 2004, artículo 235, inciso quinto. FGN, Directiva No. 0004 del 2 de noviembre de 2021, lineamiento 14
[46] Ibíd., artículo 237, inciso primero. FGN, Directiva No. 0004 del 2 de noviembre de 2021, lineamientos 12 y 13.

		Número Único de Noticia Criminal								
Radicado Interno		Departamento	Municipio	Entidad	Unidad Receptora			Año	Consecutivo	
	FORMATO DE CONTEXTUALIZACIÓN PREVIA PARA EL ANALISTA DE COMUNICACIONES INTERCEPTADAS									
Departamento		Municipio		Fecha	AAAA	MM	DD	Hora		

I. INFORMACIÓN GENERAL

Estado de la actuación	Indagación		Investigación		Juicio	

Delito	Artículo
1.	
2.	
3.	

II. PARTICIPANTES

PARTICIPANTES*				
#	Nombre	Cargo	Dependencia	Correo electrónico

*Campo obligatorio

III. INFORMACIÓN RELEVANTE

Contextualización del caso:

Se debe diligenciar la información que brinde el investigador del caso y la autoridad competente en relación con los hechos jurídicamente relevantes y el objetivo de la interceptación de comunicaciones.

SERVIDOR DE POLICÍA JUDICIAL			
Nombres y apellidos		Identificación	Entidad
Cargo	Teléfono / Celular	Correo electrónico	Firma

El servidor de policía judicial, está obligado en todo tiempo a garantizar la reserva de la información, esto conforme a las disposiciones establecidas en la Constitución y la Ley.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada.

		Número Unico de Noticia Criminal					
Radicado Interno		Departamento	Municipio	Entidad	Unidad Receptora	Año	Consecutivo

FORMATO DE VERIFICACIONES PREVIAS PARA LA SOLICITUD DE INTERCEPTACIÓN DE COMUNICACIONES

Departamento		Municipio		Fecha	AAAA	MM	DD	Hora	

I. INFORMACIÓN GENERAL

Estado de la actuación	Indagación		Investigación		Juicio	

Delito	Artículo
1.	
2.	
3.	

II. VERIFICACIONES PREVIAS

Respetuosamente, me permito informar que, respecto a los criterios de interceptación enunciados a continuación, fueron adelantadas las siguientes actividades de verificaciones previas:

CRITERIO DE INTERCEPTACIÓN	3XXXXXXXXX

TIPO DE ACTIVIDAD	SOPORTE
Identificación del criterio de interceptación.	
Estado del criterio de interceptación (activo o inactivo) en la red del proveedor de redes y servicios de telecomunicaciones.	
Verificación de la portabilidad numérica del criterio a interceptar.	
Información relacionada con la identificación y confiabilidad de la fuente de información que dio origen al criterio de interceptación.	
Análisis de fuentes abiertas.	
Otra(s).	

Manifiesto que la información que consagra en este formato corresponde a la realidad y es veraz.

Nota: Es responsabilidad de los investigadores, bajo la dirección, coordinación y control jurídico de los fiscales delegados[1], verificar, previamente, cada uno de los criterios de interceptación, con el propósito de corroborar la veracidad de la información y evitar la vulneración de los derechos fundamentales como la intimidad, claramente restringida con la interceptación de comunicaciones dentro de la causa penal.

SERVIDOR DE POLICÍA JUDICIAL			
Nombres y apellidos		Identificación	Entidad
Cargo	Teléfono / Celular	Correo electrónico	Firma

[1] Ley 906 de 2004, artículo 200.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada.

								Número Único de Noticia Criminal			
Radicado Interno				Departamento	Municipio	Entidad	Unidad Receptora		Año		Consecutivo
	FORMATO DE RESPUESTA A SOLICITUD DE INTERCEPTACIÓN DE COMUNICACIONES										
Departamento		Municipio		Fecha	AAAA	MM	DD	Hora			

I. INFORMACIÓN GENERAL

Estado de la actuación	Indagación		Investigación		Juicio	

Delito	Artículo
1.	
2.	
3.	

II. RESPUESTA

Nombre del Fiscal
Unidad
Despacho
NUNC

ASUNTO: Viabilidad del trámite solicitud de interceptación de comunicaciones.

Cordial saludo:

Por medio de la presente, comedidamente me permito manifestarle que NO es viable llevar a cabo la solicitud de interceptación ordenada bajo la actuación identificada con el número único de noticia criminal XXXXXXXXXXXXXXXXXXXXX, en atención de que una vez verificados los recursos disponibles de la sala de recepción y análisis de comunicaciones interceptadas se pudo evidenciar lo siguiente:

RAZÓN	SELECCIONE
No se cuenta con capacidad técnica[1]	☐
No se cuenta con capacidad humana[2]	☐

En atención a la imposibilidad de continuar con el trámite, se devuelve la documentación para los fines que estime pertinentes.

SERVIDOR DE POLICÍA JUDICIAL			
Nombres y apellidos		Identificación	Entidad
Cargo	Teléfono / Celular	Correo electrónico	Firma

El servidor de policía judicial está obligado en todo tiempo a garantizar la reserva de la información, esto conforme a las disposiciones establecidas en la Constitución y la Ley.

[1] No existen cupos de interceptación disponibles para realizar la interceptación.
[2] No se cuenta con personal suficiente para escuchar la cantidad de líneas solicitadas, debido a la carga laboral existente.

Versión: 01
Aprobación: 2025-10-30 CTPJ
Publicación: 2025-12-26

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga es considerada una Copia No Controlada

								Número Único de Noticia Criminal		
Radicado Interno							Departamento	Municipio	Entidad	Unidad Receptora	Año	Consecutivo
	FORMATO DE SOLICITUD DE TRÁMITES URGENTES DE INTERCEPTACIÓN, PRORROGA O CANCELACIÓN											
Departamento		Municipio		Fecha	AAAA	MM	DD	Hora				

I. INFORMACIÓN GENERAL

Estado de la actuación	Indagación		Investigación		Juicio	

Delito	Artículo
1.	
2.	
3.	

II. CAUSAL PARA SOLICITAR EL TRÁMITE URGENTE

Seguridad nacional ☐

Connotación nacional ☐

Riesgo a la vida ☐

Contra la libertad inidividual ☐

Actividades operativas ☐

III. VERIFICACIÓN DE LA DOCUMENTACIÓN

DOCUMENTACIÓN	FECHA	HORA
Orden de interceptación de las comunicaciones	AAAA/MM/DD	
Solicitud de interceptación de las comunicaciones	AAAA/MM/DD	

IV. DESCRIPCIÓN DE LA SOLICITUD

Justificación del requerimiento de trámite urgente

SERVIDOR DE POLICÍA JUDICIAL			
Nombres y apellidos		Identificación	Entidad
Cargo	Teléfono / Celular	Correo electrónico	Firma

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada.