



La seguridad
es de todos

Mindefensa



Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETIC V1

Vigencia 2022 – 2025

**UNIDAD ADMINISTRATIVA ESPECIAL DE
LA JUSTICIA PENAL MILITAR Y
POLICIAL**





1	INTRODUCCIÓN	6
2	OBJETIVO GENERAL	6
3	OBJETIVOS	6
4	ALCANCE DEL DOCUMENTO	7
5	MARCO NORMATIVO	7
5.1	Leyes	7
5.2	Decretos	8
6	RESPONSABLES	8
7	RUPTURAS ESTRATÉGICAS	9
7.1	La tecnología como valor estratégico en la JPMYP	9
7.2	La información como activo de la JPMYP	9
7.3	La necesidad del aumento del análisis de la información	10
7.4	El liderazgo para la gestión de sistemas de información	11
8	ANÁLISIS DE LA SITUACIÓN ACTUAL	12
8.1.1	Principales expectativas	14
8.1.2	Oportunidades de mejora al interior de la entidad	14
8.1.3	Comportamiento de la mesa de ayuda	14
8.1.4	Uso de las herramientas colaborativas	16
8.2	Estrategia de TI	18
8.3	Uso y apropiación de la tecnología	19
8.4	Sistemas de Información	19
8.4.1	Sistemas misionales de gestión	19
8.4.2	Sistemas misionales de prestación	21
8.4.3	Servicios de información digital, incluidos portales	24
8.5	Servicios Tecnológicos	28
8.5.1	Conectividad de los despachos	28
8.5.2	Comunicaciones unificadas	40
8.5.3	Servicios de tecnología	42
8.5.4	Equipos de cómputo personal	43



8.6	Gestión de Información	44
8.7	Gobierno de T.I.....	44
8.7.1	Estructura organizacional y talento humano.....	44
8.8	Análisis financiero	46
9	ENTENDIMIENTO ESTRATÉGICO	47
9.1	Modelo operativo.....	47
9.2	Necesidades de información.....	50
9.3	Alineación de TI con los procesos	51
10	MODELO DE GESTIÓN DE TI	53
10.1	Estrategia de TI	53
10.1.1	Definición de los objetivos estratégicos de T.I.	53
10.2	Dominios de la Arquitectura Institucional	54
10.2.1	Dominio de planeación de la arquitectura.....	55
10.2.2	Alineación de la estrategia de TI con el plan sectorial territorial 60	
10.2.3	Alineación de la estrategia de TI con la estrategia de la institución pública	61
10.3	Gobierno de TI	63
10.3.1	Cadena de valor de TI.....	67
10.3.2	Indicadores y riesgos	68
10.3.3	Plan de implementación de procesos	69
10.4	Gestión de información	69
10.4.1	Herramientas de análisis.....	74
10.4.2	Arquitectura de información.....	74
10.5	Sistemas de información	75
10.5.1	Arquitectura de sistemas de información	79
10.5.2	Implementación de sistemas de información	82
10.5.3	Servicios de soporte técnico	83
10.6	Modelo de gestión de servicios tecnológicos.....	86
10.6.1	Criterios de calidad y procesos de gestión de servicios de TI.....	90
10.6.2	Infraestructura	90



10.6.3	Conectividad	90
10.6.4	Servicios de operación	90
10.6.5	Mesa de servicios.....	90
10.6.6	Procedimientos de gestión	91
10.7	Uso y apropiación.....	91
11	MODELO DE PLANEACIÓN.....	91
11.1	Lineamientos y/o principios que rigen el plan estratégico de TI.....	91
11.2	Estructura de actividades estratégicas	92
11.3	Plan maestro o Mapa de Ruta.....	92
11.3.1	Definición de indicadores	93
11.4	Proyección de presupuesto área TI.....	94
11.5	Plan de intervención de sistemas de información.....	95
11.6	Plan de proyectos de servicios tecnológicos	96
11.6.1	Conectividad y servicios de comunicaciones a nivel nacional de las sedes de la Justicia Penal Militar y Policial	96
11.6.2	Sistema de Información.....	97
11.6.3	Adquisición del licenciamiento servidor de productos MICROSOFT.....	98
11.6.4	Prestación del servicio de horas proactivas y reactivas, configuración, parametrización y capacitación de productos MICROSOFT II	100
11.6.5	Adquisición de Equipos de Cómputo de Escritorio, Portátiles y Licencias de Ofimática	100
11.6.6	Renovación del licenciamiento del software de protección de equipos	101
11.7	Plan de proyecto de inversión	103
12	PLAN DE COMUNICACIONES DEL PETI	103



Ilustración 1 Expectativas en la JPMP.....	13
Ilustración 2 Priorización de obstáculos de JPMP.....	13
Ilustración 3 Histórico de la mesa de ayuda 2021	15
Ilustración 4 Histórico de la mesa de ayuda 2020	15
Ilustración 5 Histórico de la mesa de ayuda julio – octubre 2021	16
Ilustración 6 Adopción de Office 365.....	16
Ilustración 7 Uso de herramientas de ofimática	17
Ilustración 8 Movilidad TEAMS	17
Ilustración 9 Portal web actual.....	25
Ilustración 10 Nuevo portal web.....	25
Ilustración 11 Topología de red JPMYP	28
Ilustración 12 Despachos de la zona 1, Córdoba, Sucre y Bolívar	33
Ilustración 13 Despachos de la zona2, Atlántico, Magdalena, Cesar y la Guajira	34
Ilustración 14 Despachos de la zona 3 - parte 1, Antioquia	34
Ilustración 15 Despachos de la zona 3 - parte 2, Antioquia.....	35
Ilustración 16 Despachos de la zona 3 - parte 3, Chocó	35
Ilustración 17 Despachos de la zona 4, Santander, Norte de Santander y Arauca	36
Ilustración 18 Despachos de la zona 5 – parte 1, Bogotá D.C.....	36
Ilustración 19 Despachos de la zona 5 parte 2, Bogotá	37
Ilustración 20 Despachos de la zona 5 - parte 3, Cundinamarca y Boyacá.....	37
Ilustración 21 Despachos de la zona 6 - parte 1, Tolima	38
Ilustración 22 Despachos de la zona 6 - parte 2, Caquetá, Huila y Tolima	38
Ilustración 23 Despachos de la zona 7, Quindío, Risaralda y Valle.....	39
Ilustración 24 Despachos de la zona 8, Cauca, Pasto, Nariño y Putumayo	39
Ilustración 25 Despachos de la zona 9, Amazonas	40
Ilustración 26 Despachos de la zona 10, Vichada, Mitú, Guaviare y Meta	40
Ilustración 27 Organigrama OTIC	45
Ilustración 28 Gasto tecnológico histórico 2017 - 2021	46
Ilustración 29 Estructura orgánica funcional, a) Estructura administrativa.....	48
Ilustración 30 Estructura orgánica funcional, b) Estructura judicial.....	49
Ilustración 31 Estructura orgánica funcional, b) Estructura Judicial - vigencia 2022	49
Ilustración 32 Mapa de procesos.....	50
Ilustración 33 Mapa de procesos de MDN	60
Ilustración 34 Cadena de valor de T.I.....	67
Ilustración 35 Plan Maestro - Hoja de ruta.....	92



1 INTRODUCCIÓN

El siguiente Plan Estratégico de Tecnologías de la Información y las Comunicaciones, permite conocer a la comunidad, entidades del sector y otras interesadas en los planes de actualización y modernización tecnológica que tiene la Unidad Administrativa Especial de la Justicia Penal Militar para la vigencia 2022 – 2025 y que van a permitir el cumplimiento de sus objetivos estratégicos, su visión y su misión.

2 OBJETIVO GENERAL

Desarrollar el Plan Estratégico de Tecnologías de la Información y las Comunicaciones en alineación con los objetivos estratégicos de la Unidad Administrativa Especial de la Justicia Penal Militar y Policial para el periodo 2022 – 2025

3 OBJETIVOS

1. Implementar el Sistema Penal Oral Acusatorio en la Justicia Penal Militar y Policial, con el fin de transformarla y modernizarla
2. Diseñar e implementar una estrategia institucional de comunicaciones que visibilice la Justicia Penal Militar y Policial.
3. Desarrollar y fortalecer los procesos misionales que permitan satisfacer las necesidades de la Jurisdicción Especializada
4. Estructurar y ejecutar los planes de formación y capacitación, de acuerdo con las necesidades actuales y futuras de la Jurisdicción.
5. Fortalecer la infraestructura y el suministro de recursos para los despachos de la Justicia Penal Militar y Policial.
6. Desarrollar e implementar un modelo de gestión humana ético e integral, basado en la satisfacción de las necesidades de los servidores públicos de la Justicia Penal Militar y Policial.
7. Implementar sistemas de información que apoyen la gestión y toma de decisiones de la Justicia Penal Militar y Policial, mediante una plataforma tecnológica moderna, que permita obtener información oportuna, veraz y confiable de /os procesos de la entidad.
8. Implementar y fortalecer la Policía Judicial de la Justicia Penal Militar y Policial.



4 ALCANCE DEL DOCUMENTO

Este documento del plan estratégico de tecnologías de la información y las comunicaciones tiene dentro de su alcance:

La misión y la visión de T.I, los objetivos de T.I, la Estrategia de TI, Gobierno de TI, Información, Sistemas de Información, Servicios Tecnológicos, Uso y apropiación.

5 MARCO NORMATIVO

5.1 Leyes

1. Ley 80 de 1993 “Por la cual se expide el Estatuto General de Contratación de la Administración Pública”.
2. Ley 522 de 1999 “Por medio de la cual se expide el Código Penal Militar”.
3. Ley 940 de 2005 “Por el cual se expiden normas sobre requisitos para el desempeño de cargos en la Jurisdicción Penal Militar”.
4. Ley 1058 de 2006 “Por medio del cual se establece un procedimiento especial en el Código Penal Militar, se adiciona un artículo y se modifica el artículo 367 del mismo Código”.
5. Ley 1150 de 2007 “Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con recursos públicos”.
6. Ley 1407 de 2010 “Por la cual se expide el Código Penal Militar”.
7. Ley 1437 de 2011 “Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo”.
8. Ley 1474 de 2011 “Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública”.
9. Ley 1765 de 2015 “Por la cual se reestructura la Justicia Penal Militar y Policial, se establecen requisitos para el desempeño de sus cargos, se implementa su Fiscalía General Penal Militar y Policial, se organiza su Cuerpo Técnico de Investigación, se señalan disposiciones sobre competencia para el tránsito al Sistema Penal Acusatorio y para garantizar su plena operatividad en la Jurisdicción Especializada y se dictan otras disposiciones”.
10. Ley 1755 de 2015 “Por medio de la cual se regula el derecho fundamental de petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo”.
11. Ley 1882 de 2018 “Por la cual se adicionan, modifican y dictan disposiciones orientadas a fortalecer la contratación pública en Colombia, la Ley de infraestructura y se dictan otras disposiciones”



5.2 Decretos

1. Decreto 312 del Ministerio de Defensa Nacional del 26 de marzo de 2021, *“Por el cual se fija la estructura interna de la Unidad Administrativa Especial de la Justicia Penal Militar y Policial”*
2. Decreto Ley 1765 del 23 de julio 2015 *“por la cual se reestructura la Justicia Penal Militar y Policial, se establecen requisitos para el desempeño de sus cargos, se implementa su Fiscalía General Penal Militar y Policial, se organiza su cuerpo técnico de investigación, se señalan disposiciones sobre competencia para el tránsito al sistema penal acusatorio y para garantizar su plena operatividad en la Jurisdicción Especializada y se dictan otras disposiciones”*
3. Decreto 1070 de 2015 *“Por el cual se expide el Decreto Único Reglamentario del Sector Administrativo de Defensa”*.
4. Decreto 1082 de 2015 *“Por medio del cual se expide el Decreto Único Reglamentario del Sector Administrativo de Planeación Nacional”*.
5. Decreto 1068 de 2015 *“Por medio del cual se expide el Decreto Único Reglamentario del Sector Hacienda y Crédito Público”*
6. Decreto 1575 de 2017 *“Por el cual se adoptan medidas para implementar el Sistema Penal Acusatorio en la Jurisdicción Penal Militar y Policial, y se modifica parcialmente el Decreto 1070 de 2015 "Por el cual se expide el Decreto Único Reglamentario del Sector Administrativo de Defensa".*
7. Decreto 491 de 2020 *“Por el cual se declara un Estado de Emergencia Económica, Social y Ecológica en todo el territorio Nacional”*.
8. Decreto 417 de 2020 *“Por el cual se adoptan medidas de urgencia para garantizar la atención y la prestación de los servicios por parte de las autoridades y los particulares que cumplan funciones públicas y se toman medidas para la protección laboral y de los contratistas de prestación de servicios de las entidades públicas, en el marco del Estado de Emergencia Económica”*
9. Decreto 1768 de 2020 *“Por el cual se modifica el artículo 2.2.2.2 del Título 2 "Adaptación de medidas para implementar el Sistema Penal Acusatorio en la Jurisdicción Penal Militar", del Decreto 1070 de 2015 "Por el cual se expide el Decreto Único Reglamentario del Sector Administrativo de Defensa"*

6 RESPONSABLES

El Jefe de la Oficina Asesora de Tecnologías de la Información y las Comunicaciones, el Coordinador del Grupo de Sistemas de Información, el Coordinador de Plataforma Tecnológica y el Coordinador del Grupos de Redes de Comunicaciones de la Unidad Administrativa Especial de la Justicia Penal Militar y Policial.

7 RUPTURAS ESTRATÉGICAS

7.1 La tecnología como valor estratégico en la JPMYP

El reto del manejo de información de los casos de la Justicia especial es enorme, aún más teniendo en cuenta el rezago que en materia de tecnologías de la información y las comunicaciones tiene la Entidad, es bien conocido en el país que la justicia tiene una deuda con la modernización de sus procesos y actividades para hacer uso de las bondades que ofrece la técnica moderna, y la Justicia Especial no es la excepción¹, hecho que quedó en evidencia durante la pandemia de SARS COV2 19 en donde se pudo evidenciar las dificultades de acceso a la justicia a través del uso de la tecnología y los medios digitales. Consciente de esto la Unidad Administrativa Especial de la Justicia Penal Militar a través de la Oficina de Tecnologías de la Información y las Comunicaciones, presenta este plan estratégico poniendo presente que el acceso a la tecnología es una prioridad para dar manejo a los volúmenes y complejidades de la información que se deben gestionar para cumplir su misión de la forma en la que el país espera de ella.

Las tecnologías adquiridas y en parte desarrolladas a su interior deben alinearse con los objetivos estratégicos de alto valor que nos hemos planteado como Entidad, permitiendo que su uso enriquezca la cadena de valor de los procesos que funcionarios administrativos y misionales desarrollan en el día a día, en aras de una justicia eficaz y de unos resultados cada vez mejores. El uso y la apropiación van a ser aspectos determinantes a la hora de medir los resultados de su aplicación y su efectividad en la administración.

7.2 La información como activo de la JPMYP

El activo más importante en la era digital es la información, este activo debe como otro bien de valor ser explotado, protegido, almacenado, aumentado y enriquecido a través de procesos de transformación que permitan sacar provecho de él, en la Justicia Penal Militar este hecho viene a ser aún más relevante debida la naturaleza de entidad y a el principio de transparencia en la justicia que pretende promover.

Las investigaciones penales son complejas y variadas en información documental generada y allegada, así como en material probatorio recolectado en la fase investigativa, es necesario hacer una catalogación, estructuración y uso adecuado de esta, para que se apoyen fuertemente las decisiones investigativas y judiciales con información pertinente, es una tarea que se debe hacer con cuidado y técnica,

¹ <https://telecomunicaciones.uexternado.edu.co/hacia-la-modernizacion-de-la-justicia-en-colombia-de-la-justicia-de-papel-a-la-justicia-digital/>



se deben por tanto observar los principios de seguridad de la información, la disponibilidad, la confidencialidad e integridad. Esta complejidad presenta varios aspectos que deben ser analizados en conjunto, porque la falta de análisis en alguno de ellos hará que el agregado falle, por tanto, cualquier tratamiento de la información que se haga deberá contemplar desde su concepción los principios antes mencionados.

El primero de ellos es la disponibilidad, que es la característica que debe tener la información de presentarse en la forma y el tiempo adecuados a los distintos actores, en este caso a los intervinientes en el proceso penal para que en todos los momentos dentro de las etapas procesales los datos relevantes en cualquiera de sus formas y formatos digitales se consulten, se estudien y se comparen, sirviendo así a la toma de las decisiones. En la época en la que nos encontramos, los lugares vienen a ser más que físicos, virtuales a través de dispositivos de conexión portátiles como teléfonos, tabletas y estaciones, estos accesos deben ser suficientes para que se aprovechen las ventajas tecnológicas y puedan establecerse de forma inmediata los recursos y la disponibilidad de estos datos.

De igual manera la disponibilidad de la información documental, el acervo probatorio, y los elementos probatorios deben mantener la reserva suficiente para que se garantice el debido proceso, constituye uno de los garantes de la imparcialidad de la investigación permitiendo a los investigadores conservar el sigilo propio de su labor, y así mismo las decisiones judiciales que necesitan de la discreción para ser efectivas estarán protegidas por esta característica que se debe observar durante todo el ciclo de vida del caso, la captura, el tránsito y el reposo de los datos. Por último, e igual de importante es necesario tener la certeza de la integridad de la información constitutiva de los procesos, la alteración por adición o sustracción debe ser impedida y sus intentos de violación registrados e investigados con la ayuda de las herramientas tecnológicas adecuadas.

Parte de la transformación digital propuesta a la Entidad tiene que ver con ese paso de la información consignada en medios físicos como el papel hacia medios digitales que pueden conservar mejor las características de seguridad antes mencionadas, el entendimiento de que estas deben ser adoptada por todos los miembros de la Justicia especial; es un reto que también debe ser gestionado para que se entienda la importancia del activo de la información digital.

7.3 La necesidad del aumento del análisis de la información

Una vez disponibles los medios técnicos, tecnológicos y la información en medio digital se abrirán a la entidad posibilidades para darle mayor sentido a su estrategia, su visión y su misión, la virtualización de los datos permite su explotación, su análisis y su estudio en miras de valorar el comportamiento de

distintos aspectos relevantes como su eficiencia y eficacia administrativa y operativa².

La Justicia especial en este particular tiene una oportunidad importante para conocer el comportamiento de sus investigaciones, su carga laboral y sus resultados operativos, la visibilidad que ofrece el conocer que se realiza en cada una de las etapas procesales dará tranquilidad a la ciudadanía de que lo hecho por la entidad se ajusta a los recursos de todo tipo que se invierten y para dar a conocer el compromiso de sus funcionarios y colaboradores a nivel nacional.

7.4 El liderazgo para la gestión de sistemas de información

El sistema de información de la JPMP tiene previsto el manejo del expediente electrónico en todas las fases del proceso penal, tanto en la Ley 522 de 1999 como en la Ley 1407 de 2010.

Inicia con la recepción de la denuncia, la asignación automática al despacho que la atenderá, el establecimiento de la vocación del éxito y la generación del borrador del programa metodológico. Continúa con las actuaciones de los jueces y/o fiscales: ordenes de policía judicial, informes de policía judicial, autos inhibitorios, archivos, escritos de acusación y solicitudes de audiencia ante jueces de garantías o jueces de conocimiento, entre otras.

Posteriormente, el agendamiento de las audiencias, el desarrollo y las actas de estas, independiente de si se realizan en forma presencial o virtual, quedarán almacenadas y conformando el expediente electrónico, al igual que las actuaciones que realice el juez de ejecución de penas y los informes de las actividades de las personas que están privadas de la libertad.

Se tendrá el control de los bienes que se encuentran implicados en los procesos penales, y la administración de los almacenes de evidencias, permitiendo también su disposición final.

El hecho de que bajo la sombrilla de la Unidad Administrativa Especial de la Justicia Penal Militar y Policial se encuentren todos los actores del proceso penal (jueces de instrucción penal militar, fiscales, policías judiciales, jueces de conocimiento, jueces de garantías y jueces de ejecución de penas, magistrados del tribunal, fiscales ante el tribunal), facilita la automatización de todo el proceso penal bajo una misma arquitectura, sin tener que realizar las transferencias de la información entre una y otra plataforma tecnológica, como sucede con el sistema penal ordinario, en donde hay sistemas de información diferentes, principalmente, en la Fiscalía General de la Nación y en el Consejo Superior de la Judicatura.

² <https://publications.iadb.org/publications/spanish/document/Tecnologias-digitales-para-mejorar-los-sistemas-de-justicia-un-conjunto-de-herramientas-para-la-accion.pdf>

No obstante, se tiene previsto el intercambio de información con otras entidades, especialmente, con la Fiscalía, la Policía Nacional (DIJIN) y Medicina Legal para el intercambio de documentos e interacción entre las plataformas de investigación y gestión de casos.

8 ANÁLISIS DE LA SITUACIÓN ACTUAL

Al inicio de la administración, en agosto de 2020, era nulo el apoyo tecnológico a la operación de la JPMPYP: no existía un sistema misional para atender los procesos de la Ley 522 de 1999 ni de la Ley 1407 de 2010, el seguimiento a la gestión se venía realizando a través de mecanismos rudimentarios como hojas de Excel que mensualmente se envían desde los despachos y que requieren procesos posteriores de consolidación, y las estadísticas tan solo arrojan la contabilidad de los casos que ingresan y salen cada mes de los despachos, teniendo un reporte con retraso entre su recolección y sus estudio.

La obsolescencia, tanto en hardware como en software, de los equipos de cómputo era cercano al 90%, se requería la reposición urgente de los servidores centrales y de 847 equipos de escritorio. Los despachos que se encuentran fuera de Bogotá no tenían ninguna conexión con la sede central de la JPMP.

Por lo anterior, se realizó un plan de modernización a 4 años que busca tener una operación automatizada a nivel nacional con el apoyo de un sistema misional y comunicaciones unificadas para cada uno de los despachos. El plan fue aprobado por el Comité de TIC'S – CITI del Ministerio de Defensa en octubre del año 2020.

El proyecto de modernización tecnológica incluye la renovación de los equipos de cómputo de escritorio, la conectividad de los despachos a nivel nacional, la actualización del software de Microsoft, y la construcción de un sistema de información basado en tecnología de punta que incorpore un expediente digital y un tablero de control para el seguimiento en línea de los casos de la JPMP.

En el año 2020 se actualizó el software de Microsoft de los servidores centrales, la adquisición de Office 365 y la adquisición de 251 equipos de cómputo que fueron distribuidos entre los despachos de la JPMP.

Con el concurso del Comando General de las Fuerzas Militares y de la Dirección de Telemática de la Policía Nacional, en el segundo semestre del 2020, se conectaron a la JPMP, 83 despachos de las Fuerzas Militares y 98 de la Policía Nacional. Los 88 despachos restantes requieren de adecuaciones y conexión física a las redes de las Fuerzas Militares, labor que se viene realizando y que durará hasta el año 2022.

Para el año 2021, se planeó y presupuestado la adquisición de 392 computadores, la renovación de los servidores del centro de cómputo, la primera fase de las adecuaciones de las redes de los despachos de jueces y fiscales a nivel nacional, y la primera fase de la construcción del sistema de información misional, labores que continuarán durante los años 2022 y 2023, hasta obtener el reemplazo de todos

los equipos obsoletos de la JPMP y la implementación del sistema de información misional.

El proyecto de modernización tecnológica de la JPMP se armoniza con las fases de implementación del sistema acusatorio, para los años 2023, 2024 y 2025, de acuerdo con el cubrimiento geográfico que el decreto 1768 de diciembre 24 de 2020 tiene previsto.

Durante el año 2021 se realizó una encuesta a nivel nacional para la consulta de la expectativa que en materia de tecnologías de la información y comunicaciones tiene la entidad actualmente, encontrando que existe la percepción que la entidad debe modernizar su infraestructura física y adoptar sistemas de información que brinden facilidades en la gestión y en la toma de decisiones, a continuación, se presentan algunos resultados.

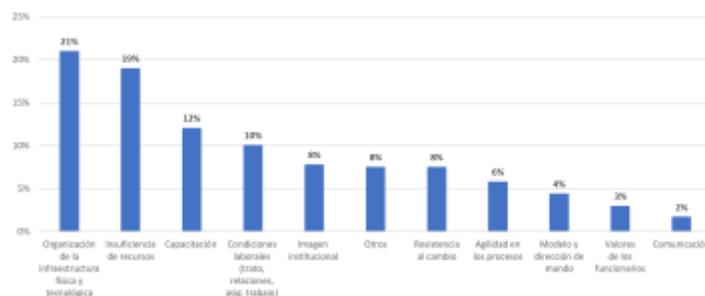


Ilustración 1 Expectativas en la JPMP

De lo anterior se puede concluir que:

- No se dispone de herramientas tecnológicas para el seguimiento de los procesos, ausencia de información digitalizada.
- La ausencia de plataformas que permitan administrar datos sobre la gestión judicial.
- Computadores obsoletos, no hay herramientas básicas de trabajo, espacios de trabajo insuficientes, falta personal en los despachos, no se dispone de medios de transporte en lugares lejanos de difícil acceso.



Ilustración 2 Priorización de obstáculos de JPMP

En la Ilustración 2 Priorización de obstáculos de JPMP, se evidencia la importancia que los funcionarios le dan a la Infraestructura tecnológica situando esta como la segunda dificultad en la Entidad para el cumplimiento de los objetivos misionales.

8.1.1 Principales expectativas

Dentro del ejercicio estadístico se observaron las siguientes expectativas:

- El posicionamiento y reconocimiento de la entidad ante la sociedad como una entidad eficiente, confiable y transparente
- La puesta en marcha de la UAEJPMP, con independencia y autonomía.
- La implementación del SPOA.
- Transparencia, legitimidad y celeridad.
- Descongestión de los procesos judiciales - Distribución de cargas de trabajo.
- Mayor apoyo de Policías Judiciales – La Policía Judicial debe depender de la UAEJPMP

8.1.2 Oportunidades de mejora al interior de la entidad

- Cambio de la cultura organizacional y comportamiento de los funcionarios (compromiso, entrega, cuidado de los recursos, diligencia en los trámites, actitud de servicio, aptitud frente al cambio, disposición y disponibilidad).
- Mejorar la infraestructura física
- Mejorar la infraestructura tecnológica
- Entregar los recursos e insumos necesarios para el desempeño de los funcionarios de los despachos y de la Policía Judicial
- Mejorar la gestión del talento humano en cuanto a procesos de selección, estabilidad, desarrollo y crecimiento profesional
- Disponer de programas y estrategias para la formación del personal, de manera que se mantengan y mejoren las competencias.

8.1.3 Comportamiento de la mesa de ayuda

La mesa de ayuda se contrataba en la vigencia 2020 a través de un proceso contractual de condiciones uniformes por subasta inversa fuera de Colombia compra eficiente que no contaba con bolsa de repuestos, donde se tenían formas de pago distintas para los ítems requeridos con un cubrimiento de agentes sólo para el nivel central, lo que implicaba un nivel de servicio bajo de atención a las zonas geográficas distintas a las de Bogotá.



Ilustración 3 Histórico de la mesa de ayuda 2021



Ilustración 4 Histórico de la mesa de ayuda 2020

En la vigencia 2021, utilizando la tienda virtual de Colombia compra eficiente, aumentando los agentes para las zonas distintas a Bogotá y con un descuento de alrededor del 7%, se mejoran los niveles de servicio en dichas zonas, y se realizan visitas correctivas cubriendo las necesidades de los despachos en zonas de difícil acceso.



Ilustración 5 Histórico de la mesa de ayuda julio – octubre 2021

8.1.4 Uso de las herramientas colaborativas

Con la suscripción al servicio en la nube de Microsoft office 365 a través de la tienda virtual, la unidad ha logrado aumentar el uso y adopción de dichas herramientas en las labores diarias de la entidad, logrando adicionalmente compartir datos, co-crear documentos, utilizar herramientas de planeación de actividades, reuniones y audiencias, entre otras, que ha permitido aumentar la agilidad, movilidad y trabajo en casa de la unidad a nivel central y de los despachos judiciales a nivel nacional.



Ilustración 6 Adopción de Office 365

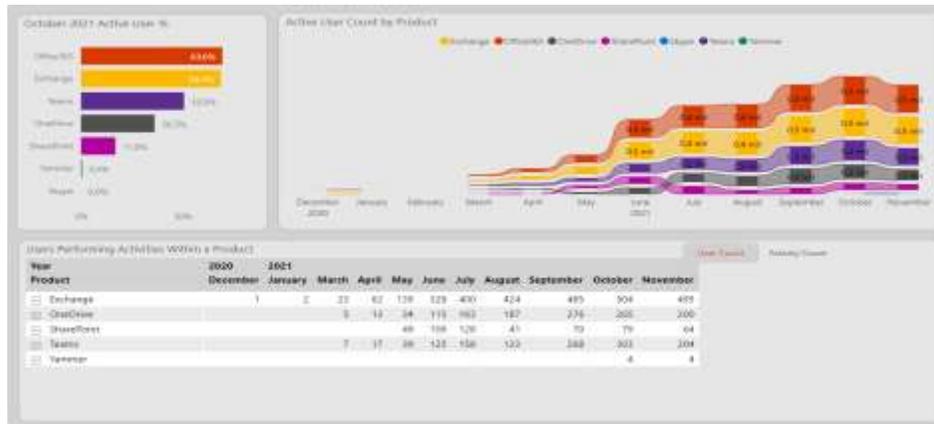


Ilustración 7 Uso de herramientas de ofimática



Ilustración 8 Movilidad TEAMS

Como se observa en las gráficas anteriores desde la implementación de las herramientas colaborativas su uso recurrente por parte de los usuarios ha venido en incremento con un retorno del 96,3% por parte de los usuarios los que ya han apropiado el uso de estas dentro de su quehacer diario y en las comunicaciones institucionales para fines administrativos, misionales y en la comunicación externa con otras entidades y del sector. Otro aspecto por destacar es el de que se ha visto a su vez un incremento del uso de estas a través de dispositivos móviles como teléfonos y tabletas y el uso web a través de un navegador, esta tendencia de uso se debe ver incrementada en los próximos años debido a la implementación de la Ley 1407 de 2010 a nivel nacional cuando se realicen las múltiples audiencias necesarias en el proceso. Se tiene previsto la continuación y el fortalecimiento de esta suite colaborativa en las próximas vigencias en temas de seguridad, uso y apropiación para que se consolide dentro de la justicia especial y se sigan explotando sus ventajas por todos los funcionarios y actores de la justicia especial.

8.2 Estrategia de TI

La Oficina de Tecnologías de la Información y las Comunicaciones, como parte constitutiva de la Unidad Administrativa Especial de la Justicia Penal Militar y Policial esta alineada con su estrategia y busca a través de sus funciones apoyar el cumplimiento de los objetivos, que como se puede extraer de lo consignado en los decretos que tratan la materia, van orientados a la modernización y al apoyo tecnológico en la gestión de los casos penales y a la gestión administrativa mediante sistemas de información y plataforma tecnológicas modernas. La OTIC a su vez se ha apropiado de estos objetivos estratégicos con la operación de sus tres grupos: Grupo de Redes de Telecomunicaciones, Grupo de Sistemas de Información y Grupo de Plataforma Tecnológica; los pilares fundamentales de esta estrategia son: la modernización y renovación de equipos de cómputo y las telecomunicaciones, implementación del sistema de gestión de casos penales y la administración de la plataforma tecnológica en un modelo de nube híbrida.

Dentro del primer objetivo estratégico TIC *“Modernización y renovación de equipos tecnológicos y las comunicaciones”*, se plantea continuar con la renovación de equipos de cómputo de escritorio y algunos portátiles, para los jueces, fiscales, secretarios y de forma particular para la policía judicial, así como para el personal administrativo de la Unidad, con el fin de atender sus problemas de obsolescencia, y el de la conectividad a red de comunicaciones, esto para hacer el tránsito hacia lo digital y la adopción de procedimientos y procesos que involucren sistemas de información. En el segundo objetivo estratégico *“Apoyo a la gestión misional y gestión administrativa a través de sistemas de información”*, el grupo de Sistemas de Información ha adelantado el diseño, adquisición, implementación y divulgación de programas informáticos que van a impactar positivamente el quehacer de los funcionarios en las áreas misionales y administrativas, la estrategia en esta área es aprovechar las herramientas existentes en el mercado, haciendo un estudio juicioso y una evaluación de las soluciones propuestas en otras entidades y hacer una adaptación rápida a los procesos de la Entidad para reducir la brecha tecnológica que existe en la administración de la Justicia Especial, esta estrategia está acompañada por una capacitación técnica, un aumento de la fuerza laboral en el área de desarrollo de software y una divulgación a la Entidad a través del uso y la apropiación de las herramientas.

Como tercer objetivo estratégico tenemos el de *“Actualización y modernización de la plataforma tecnológica”*, este objetivo busca fortalecer el ecosistema de productos de hardware y software combinado las características de alta disponibilidad, resiliencia a fallos y aumento del poder de cómputo, en un esquema de nube híbrida, para soportar los servicios y sistemas de información que hacen parte de la estrategia global de tecnología permitiendo disfrutar de las bondades que estas

soluciones ofrecen a la administración de redes, disponibilidad de servicios y que soporten las herramientas informáticas.

8.3 Uso y apropiación de la tecnología

Las cambiantes tecnologías de la información y las comunicaciones requieren un continuo aprendizaje pasando por lo técnico hasta lo funcional, los usuarios finales de los sistemas de información en la Entidad, en su mayoría no son nativos digitales, y por ende necesitan adaptarse a los modelos y herramientas de gestión de la información que rompen los paradigmas aprendidos y las concepciones que se tienen, por ejemplo, en cuanto a la seguridad de la información, la reserva de los procesos en las distintas etapas investigativas y judiciales, las comunicaciones y audiencias mediante medios tecnológicos, por citar algunos casos. Conscientes de estas situaciones la OTIC tiene en cuenta que es necesario hacer un plan de uso y apropiación de estas nuevas herramientas que muestren las ventajas del uso de la tecnología, pero que también enfrenten a los usuarios a los nuevos modelos, de los que necesitan apersonarse y retarse para el avance y modernización de la Entidad; es una tarea compleja ya que algunos funcionarios pueden mostrar reticencia y desconfianza, es por esto que los pasos avanzados que logren en la confianza no pueden ser perdidos por fallas en la seguridad, el rendimiento o la disponibilidad de los sistemas.

El uso es el primer paso de esta estrategia, este puede ser uno inherente a las herramientas por virtud de las funciones que desempeñe un funcionario, pero debemos lograr ir más allá a través de la apropiación, que es un estadio en el que los usuarios sienten como propias las herramientas, se ha vencido por tanto la resistencia y empieza una etapa de colaboración armónica para superar los retos y posibilidades de mejora que tienen los sistemas en su normal devenir, su evolución y mejora continua dependerá por tanto de que la implementación a través de campañas, capacitaciones, colaboración y tutoría de los usuarios destacados. Una vez superados esos escollos, la Entidad podrá en colaboración proponer mejoras y ofrecer mejores soluciones de justicia a los interesados.

8.4 Sistemas de Información

8.4.1 Sistemas misionales de gestión

8.4.1.1 Sistema de información misional de casos penales Ley 522 de 1999 y Ley 1407 de 2010

Con el objeto de atender en forma adecuada el cumplimiento de sus funciones, la UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL



viene adelantando un plan de modernización que busca tener una operación automatizada a nivel nacional con el apoyo de un sistema misional y comunicaciones unificadas para cada uno de los despachos. El plan fue aprobado por el Comité de TICS – CITI del Ministerio de Defensa en octubre del año 2020.

El proyecto de modernización tecnológica incluye la renovación de equipos de cómputo, la conectividad de los despachos a nivel nacional, la actualización del software de Microsoft, y la construcción de un sistema de información basado en tecnología de punta que incorpore un expediente digital y un tablero de control para el seguimiento en línea de los casos de la JPMP.

El proyecto de modernización tecnológica de la JPMP se armoniza con las fases de implementación del sistema acusatorio, para los años 2022, 2023, 2024 y 2025 de acuerdo con el cubrimiento geográfico que el decreto 1768 de 2020 tiene previsto. La primera fase: inicia con un piloto en la ciudad de Bogotá que va desde el 1 de enero del año 2022 hasta el 30 de junio de 2022; la fase II, inicia con un piloto en los departamentos de Boyacá, Caldas, Cauca, Cundinamarca, Huila, Nariño, Quindío, Risaralda, Tolima, Valle del Cauca el primero de enero del año 2023, y finaliza el 30 de junio del mismo año para así empezar su aplicación definitiva en estos departamentos el 1 de julio de ese año; la fase III inicia el primero de enero del año 2024 y va hasta el 30 de junio de ese año en los departamentos de Antioquia, Atlántico, Bolívar, San Andrés y Providencia, Cesar, Choco, Córdoba, Guajira, Magdalena, Norte de Santander y Sucre, para su adopción definitiva el primero de julio de 2024, y la última, fase IV, inicia con un piloto que va desde el primero de enero hasta el 30 de junio de 2025 en los departamentos de Amazonas, Arauca, Caquetá, Casanare, Guainía, Guaviare, Meta, Putumayo, Vaupés y Vichada, para la adopción definitiva en todo el país a partir del 1 de julio del año 2025.

De manera que para la adecuada gestión de los casos que se adelantan en los despachos de jueces magistrados y fiscales de la Justicia Especial, tanto en la Ley 522 de 1999 como en la Ley 1407 de 2010, se requiere de un sistema de información que maneje las diferentes etapas del proceso penal, entre otras: la recepción de la denuncia, las órdenes a la policía judicial, los informes de Medicina Legal, las actuaciones de jueces de instrucción, fiscales, policías judiciales y jueces de instancia, la grabación de audiencias y el seguimiento a presos. Además, que cuente con un tablero de control que presente en línea indicadores y estadísticas que faciliten el seguimiento de la gestión de cada uno de los despachos garantizando la integridad y veracidad de la información gestionada.

Como parte de las iniciativas de transformación digital y en cumplimiento de su misionalidad, la entidad requiere de un sistema de información que maneje todos sus procesos, en especial, los que tienen que ver con los procesos misionales, de manera que se permita la gestión y el control y seguimiento de los casos que se adelantan en la jurisdicción.

Este sistema debe permitir que los diferentes actores de los procesos puedan gestionar la información de cada una de las etapas ofreciéndoles las características de seguridad necesarias de confidencialidad, confiabilidad y acceso a la información, en especial en lo atinente a la toma de decisiones. Se contempla así mismo que esta herramienta permita auditar lo ejecutado por los actores en cada una de las etapas de acuerdo con lo requerido por las autoridades competentes, así como los indicadores y estadísticas de la jurisdicción.

Los procesos, en especial los penales, tienen expedientes documentales que en algunos casos son voluminosos y que comienzan a conformarse con la denuncia y los archivos digitales o físicos que se anexan, pasando por las actuaciones de los fiscales y jueces en las distintas etapas, así como los documentos que se intercambian en el desarrollo del ejercicio de la justicia con las partes procesales y entre entidades de la Rama Judicial, órganos de control y otros interesados.

8.4.2 Sistemas misionales de prestación

8.4.2.1 Sistema de información de procesos de calidad MIPG

En el decreto 312 del 26 de marzo 2021, la Oficina de Planeación dentro una de sus funciones, tiene que definir criterios, en coordinación con la Oficina de Tecnologías de la Información y de las Comunicaciones, para la implementación de tecnologías y sistemas que incentiven la innovación institucional.

La Oficina de Tecnologías de la información y las comunicaciones entre algunas funciones debe Liderar el desarrollo, implementación, adquisición, administración y mantenimiento de los sistemas de información, la infraestructura tecnológica y servicios digitales de la Unidad y de la Jurisdicción Especializada, de acuerdo con lo establecido en el Plan Estratégico de Tecnologías de la Información y las Comunicaciones.

Así mismo la Oficina Asesora de planeación tiene como función Dirigir, administrar y promover el desarrollo, implementación y sostenibilidad del modelo integrado de planeación y gestión (MIPG), tomando en cuenta que desde la fecha de creación la entidad cuenta con dos años para la implementación de las políticas establecidas en el marco normativo, por lo anterior, El decreto 1499 de 2017 actualiza, por el Departamento Administrativo de la Función Pública, el Modelo Integrado de Planeación y Gestión - MIPG, con un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión Institucional del MEN y sus Entidades Adscritas y Vinculadas, en términos de calidad e integridad del servicio, con el fin de que se entreguen resultados que atiendan y resuelvan las necesidades y problemas de los grupos de valor.

Con base en el MIPG, la entidad debe realizar la implementación de las siguientes políticas:

1. Planeación Institucional
2. Gestión presupuestal y eficiencia del gasto público
3. Talento humano
4. Integridad
5. Transparencia, acceso a la información pública y lucha contra la corrupción
6. Fortalecimiento organizacional y simplificación de procesos
7. Servicio al ciudadano
8. Participación ciudadana en la gestión pública
9. Racionalización de trámites
10. Gobierno digital
11. Seguridad digital
12. Defensa jurídica
13. Mejora normativa
14. Gestión del conocimiento y la innovación
15. Gestión documental
16. Gestión de la información estadística
17. Seguimiento y evaluación del desempeño institucional
18. Control interno
19. Compras y contratación público

El software del Sistema de gestión de calidad será una herramienta que facilitará la implementación de las siguientes políticas.

- Planeación Institucional

A través de la herramienta se realizará la consolidación de los planes de acción, así como los indicadores de eficacia, eficiencia y efectividad de los procesos, también se realizará el monitoreo y seguimiento de estos para la toma oportuna de acciones.

Oficina de Tecnologías de la Información y las Comunicaciones – Unidad Administrativa Especial de la Justicia Penal Militar y Policial

Carrera 46 No. 20 C – 1 Cantón Militar Occidental “coronel Francisco José de Caldas”,

Palacio de la Justicia Penal Militar y Policial “TF. Laura Rocío Prieto Forero”, Bogotá,

www.justiciamilitar.gov.co

Conmutador: (57 1) 3150111

Se diseñarán los mapas de riesgos y controles a implementar en los procesos para garantizar la eficacia, eficiencia y efectividad de entidad en su actuar diario.

- Fortalecimiento Organizacional y Simplificación de procesos

La entidad debe establecer procesos, procedimientos y formatos, que establezcan los mecanismos de funcionamiento para las diferentes áreas, dependencias y procesos, por lo tanto, la herramienta facilitará el control de los documentos, la trazabilidad de los cambios, el acceso a la información requerida a nivel nacional para la operación.

Así mismo debe establecer planes de mejoramiento que propendan por la simplificación de procesos, el software contara con módulo de acciones de mejora para el análisis, planes de mejora, seguimiento y control a la eficacia de estas.

- Seguimiento y evaluación del desempeño institucional

Facilitará el seguimiento al cumplimiento de metas definidos en los objetivos estratégicos e indicadores definidos para los procesos.

- Control interno

La herramienta facilitara la planificación, programación, ejecución, generación de informes e implementación y seguimiento de auditorías internas.

Por lo anterior para cumplir con las funciones antes mencionadas y los ordenamientos de la ley, es necesario contar con un software que permita:

- Consolidar documentación de los procesos, control y trazabilidad de los cambios y acceso de la información requerida por los funcionarios de la entidad.
- Registrar y hacer seguimiento a los planes de acción, desplegados de la planeación estratégica institucional y las necesidades de los procesos y dependencias.
- Diseñar e implementar los mapas de riesgos y los controles para la prevención de la materialización y sus impactos a los grupos de valor y de interés.
- Establecer y monitorear los indicadores para medir el desempeño de la entidad.
- Establecer los programas de auditorías internas, y realizar el seguimiento a los planes de mejoramiento implementados por los procesos.
- Establecer e implementar las acciones de mejoramiento necesario para prestar servicios conforme a lo dispuesto en la ley.

8.4.2.2 SIATH

Sistema Integrado de Talento Humano, esta aplicación pertenece al Ministerio de Defensa, y hace parte de los sistemas de información que se siguen usando en virtud del contrato interadministrativo celebrado en el año 2022, este aplicativo se accede mediante canal dedicado y se utiliza para la consulta de hojas de vida, tiempos de servicios, situaciones laborales. En próximas vigencias se debe evaluar la adición de este contrato o evaluar la adquisición de una solución propia por parte de la Unidad para la gestión del talento humano.

8.4.2.3 PAOYER

Sistema de información que permite enviar las novedades de nómina de la Justicia Penal Militar al Ministerio de Defensa para su procesamiento, este software también hace parte del contrato interadministrativo celebrado por los próximos 18 meses, contados a partir del mes de enero de 2022.

8.4.2.4 SAP

El sistema de Sinergia Logística, SILOG, fue creado por el Ministerio de Defensa Nacional como una herramienta que permite determinar, en tiempo real, el estado de los inventarios de la Fuerza Pública y compartir sus existencias, le permite a la Justicia Penal Militar automatizar sus inventarios, también parte del mismo contrato.

8.4.3 Servicios de información digital, incluidos portales

8.4.3.1 Portal Web

Hasta finales del 2021 la página Web de la Justicia Penal Militar – <https://www.justiciamilitar.gov.co>. - se encontraba desarrollada en la infraestructura SAP del MDN, como uno de los subsitios de la página Web del Ministerio de Defensa Nacional <https://www.mindefensa.gov.co>.



Ilustración 9 Portal web actual

Durante diciembre de 2021 y enero de 2022 el sitio web de la UAESJPMP, ha iniciado un proceso de rediseño, adecuación y modernización que busca tener un contacto más cercano con nuestros usuarios y hacer del acceso a la información de la Justicia Especial una experiencia más intuitiva y amigable, además de facilitar el acceso desde dispositivos móviles, tabletas y equipos portátiles, aumentando su velocidad de respuesta y permitiendo la respuesta a los cambios de la Entidad, es por esto que desde el día 31 de enero de 2022, se pone en producción el nuevo portal de la Unidad.

En este portal transaccional busca posicionarse como el canal institucional de comunicación con los usuarios, la ciudadanía, el personal uniformado, las entidades externas y los entes de control, en le ejecución de los planes y procesos contractuales se prevé en la vigencia 2021 y 2022 llevar los trámites de correspondientes a denuncias y demás peticiones, quejas, reclamos y sugerencias en las modalidades de presentación, consulta y ampliación lo que permitirá una mayor interacción para la prestación de los servicios de justicia.



Ilustración 10 Nuevo portal web

Este nuevo portal está desarrollado con tecnologías de última generación en una infraestructura de nube pública que cuenta con el respaldo y los mecanismos de seguridad y contingencia que se esperan de este tipo de soluciones para la interacción ciudadana y con una actualización de contenido gestionada y en permanente evolución. Este portal será el vehículo mediante el cual se pondrán a disposición los servicios de atención ciudadana, los datos abiertos y demás requisitos de ley que en cuanto a publicación de información y transparencia se le piden a la Entidad.

8.4.3.2 Servicio de PQRSD

Este proceso de apoyo maneja la radicación de entrada, salida entre dependencias de las peticiones, quejas, reclamos, sugerencias y denuncias que tengan los ciudadanos con relación a los asuntos que maneja la UAEJPMP y en la fecha de construcción de este Plan se encuentra en fase de desarrollo, se tiene provisto la gestión de:

- a. Tutelas: tienen que ver con un requerimiento judicial cuyo objeto es la protección de los derechos fundamentales presuntamente amenazados o vulnerados por acción u omisión de cualquier despacho judicial o aérea administrativa.
- b. Petición: una persona natural o jurídica en desarrollo del artículo 23 de la constitución nacional presenta derecho de petición a la entidad que debe ser atendida de acuerdo con los términos que prevé la Ley.
- c. Quejas: Este módulo debe permitir el registro de una queja en forma presencial, correo electrónico o el portal de un descontento o inconformidad que formula una persona en relación con una conducta de uno varios funcionarios de UAEJPMP.
- d. Reclamos: En esta opción se registra la insatisfacción de un servicio que haya prestado la UAEJPMP o que no cumple con los compromisos adquiridos con clientes internos o externos. Debe ser atendida de acuerdo con el tipo de reclamo por la dependencia competente.
- e. Comisorios: Consiste en una orden dirigida a un despacho judicial para que ejecute unas actuaciones y de respuesta a dicho requerimiento. Debe ser atendida de acuerdo con las instrucciones impartidas por la autoridad judicial.
- f. Solicitudes: Consiste en un requerimiento administrativo o de un proceso a la UAEJPMP.
- g. Denuncia: En este módulo el usuario podrá registrar la información de la noticia criminal sobre un hecho delictivo cometido por un miembro de la Fuerza Pública (Fuerzas Militares o Policía Nacional).

h. Ampliación de la denuncia: Una vez creada la noticia criminal, el denunciante u otra persona, pueden enviar información adicional del hecho denunciado a través de cualquiera de los métodos mencionados para la recepción de la denuncia. En este caso la información debe recibirse, según corresponda, y enviarse al despacho que tenga a su cargo el trámite de la denuncia.

Entre otros, el sistema debe tener en cuenta los siguientes aspectos:

- Ventanilla única: a este módulo le corresponde radicar la correspondencia de entrada y salida de la entidad y la que se produzca entre las diferentes dependencias, generando automáticamente un número de radicación, y cuando la radicación llegue en papel, un rótulo con código de barras que debe ser impreso para adherir al papel. Además, se debe hacer la notificación con el servicio postal que cuenta la entidad a los funcionarios, ciudadanos y entidades involucradas en el proceso.

Si la radicación es de entrada, debe distribuir las comunicaciones a las áreas que de acuerdo con su competencia deban atenderlas, y si es de salida, se deben enviar al destinatario que se haya descrito, a través del notificador electrónico o del servicio postal de la entidad. Debe tenerse en cuenta que, en la radicación de salida, en algunos casos, además del destinatario debe enviarse la comunicación con anexos a otras entidades como el Ministerio Público.

Los documentos reposarán en el expediente electrónico y deben quedar clasificados en documentos públicos, privados o reservados, según corresponda, para lo cual se debe tener en cuenta las tablas de retención documental de la UAEJPMP.

8.4.3.3 Intranet

Esta herramienta tecnológica está concebida como un canal de integración institucional desde el cual el personal administrativo y misional de la Unidad pueda tener una comunicación fluida del contenido necesario para el desarrollo de sus funciones, promoviendo el trabajo colaborativo y la visibilidad de novedades administrativas e información relevante.



8.5 Servicios Tecnológicos

8.5.1 Conectividad de los despachos

Este servicio tecnológico está orientado a brindar una comunicación fluida de los despachos con la red pública de internet y con el Palacio de Justicia y busca tener una experiencia colaborativa del trabajo y un uso de los sistemas de comunicación si delaciones que impidan su uso y apropiación.

Fue por estos motivos como se inició un proceso de diagnóstico en donde se identificaron 45 dispositivos de red y de comunicación distribuidos según su uso: con las herramientas que cuenta la entidad Fortinet, SolarWinds, CISCO Management, McAfee.

A continuación, se puede visualizar la topología de red:

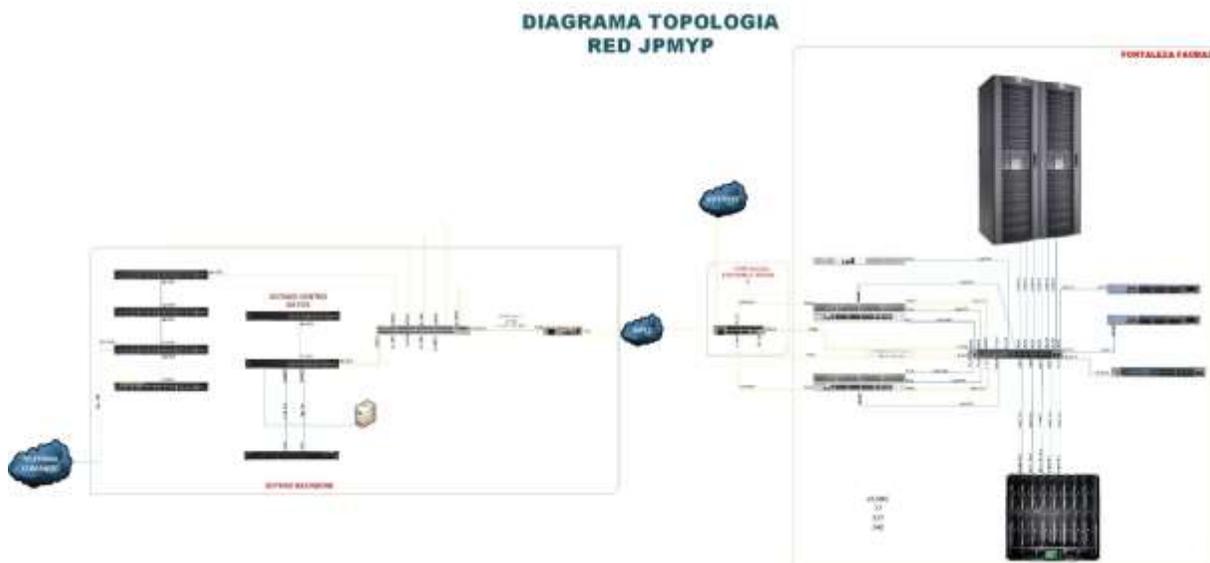


Ilustración 11 Topología de red JPMYP

En los despachos judiciales de La Unidad Administrativa Especial de la Justicia Penal Militar y Policial ubicados en el Palacio de Justicia de Bogotá y a nivel nacional, se realizó un diagnóstico sobre la infraestructura técnica de conectividad y de sus necesidades de componentes tecnológicos, se identificaron así ciento treinta y tres (133) despachos los cuales no cuentan con elementos de la información actualizados o carecen de ellos para su operación tecnológica.

En tal sentido, con el fin de permitir el acceso a los diferentes servicios soportados por los sistemas de información, con los que cuenta y contará la Entidad, se ha identificado la necesidad de conexión de los diferentes despachos de la UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL a la RIC (Red Integrada de Comunicaciones). En algunos de los despachos de las fuerzas militares se instaló una Red de Área Local (LAN), con sus respectivos equipos de comunicación de red, con lo que no solo se permite la interconexión de todos los computadores de los funcionarios, servidores y empleados, sino el acceso a los diferentes servicios informáticos misionales y corporativos, como: el correo electrónico, acceso a Internet y Sistemas de Información vitales para apoyar la gestión de la UAEJPMP.

En la actualidad, los despachos cuentan con elementos de cableado estructurado categorías 5E con más de 20 años de funcionamiento, es decir, desde en el año 2000 cumplieron el tiempo estimado de vida útil para ese tipo de tecnología, adicionalmente no cuentan con garantías, soporte técnico o mantenimiento preventivo ni correctivo, situación que afecta el servicio de comunicación, es decir, la conexión con los sistemas misionales y de apoyo, por cuanto, se han presentado fallas en los puntos de datos debido al crecimiento de la Unidad y la fragilidad de estos componentes.

De igual manera, se identificó la necesidad de equipos de comunicación (switches) los cuales tienen más de 10 años en funcionamiento y a la fecha no cuentan con la debida garantía que los respalde, se encuentran por tanto descontinuados, sus tecnologías no son administrables ni de fácil gestión centralizada, lo que aumenta los riesgos de fallas, obtención de repuestos y servicios especializados para la reparación, impactando negativamente la infraestructura de los centros de comunicaciones, y los servicios de información, que garantizan la misionalidad de la UAEJPMP. Tampoco se cuenta a la fecha con sistemas de potencia (UPS) que contribuyan a incrementar la eficiencia y eficacia en los diferentes despachos judiciales de la Jurisdicción Especializada al poder brindar la continuidad en el suministro eléctrico, en los equipos de cómputo y de telecomunicaciones, con la garantía y la vida útil que ofrezcan de unas condiciones óptimas de alimentación de corriente y voltaje regulado, que en los casos de falla, corte del fluido eléctrico y cambios en el voltaje, puedan continuar garantizando la protección del software y hardware de los equipos de cómputo y de comunicaciones con los que cuenta la Entidad en sus diferentes despachos.

Dadas las anteriores consideraciones, se inició el proceso de mejoramiento de conectividad LAN para reducir los factores de riesgo a los que están expuestos actualmente y en el futuro las plataformas misionales y de apoyo en el desarrollo de las siguientes actividad

es y distribución en tres fases de intervención:



Instalación y certificación de los puntos de cableado estructurado utilizando para ello, una denominada bolsa de puntos de cableado estructurado, con el fin de mejorar y optimizar la red LAN de los diferentes despachos de la UAEJPMP.

Adquisición, Instalación y puesta en funcionamiento de equipos activos de red LAN (switch) en los despachos de la UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL.

Adquisición, Instalación y puesta en funcionamiento de UPS, en los sitios indicados y conectadas a las redes de potencia.

Adquisición, Instalación y puesta en funcionamiento de aires acondicionados en los despachos, ya que es sumamente necesario aplicar las medidas que permitan a la Entidad reducir las condiciones de riesgo a las que están expuestas actualmente las plataformas misionales y de apoyo, esto mediante la contratación de acuerdo con las normas técnicas establecidas para tal fin.

Se tiene previsto según lo expuesto un plan de intervención por fases, en grupos de despachos priorizados según su criticidad y carga de procesos, así:

FASE I

La fase I comprende de 71 despachos los cuales se encuentran en adecuación de conformidad con las necesidades establecidas en el año 2021 con la siguiente distribución:

DISTRIBUCION DE DESPACHOS A NIVEL NACIONAL FUERZAS MILITARES						
ZONAS A NIVEL NACIONAL	NUMEROS DE DESPACHOS A INTERVENIR NECESIDAD REAL	NUMEROS DE DESPACHOS A INTERVENIR	CANTIDAD DE PUNTOS DE CABLEADO ESTRUCTURADO POR BOLSA EN ZONAS	CANTIDAD DE EQUIPOS ACTIVOS RED LAN	CANTIDAD DE UPS	CANTIDAD DE AIRES ACONDICIONADOS
ZONA 1 - CORDOBA, SUCRE Y BOLÍVAR	7	0	0	0	0	0
ZONA 2 - ATLÁNTICO, MAGDALENA, GUAJIRA Y CESAR	10	9	54	7	6	5
ZONA 3 - ANTIOQUÍA Y CHOCÓ	23	18	108	14	14	5



ZONA 4 - SANTANDER, NORTE DE SANTANDER Y ARAUCA	12	11	66	8	6	6
ZONA 5 - BOGOTÁ, BOYACÁ, CUNDINAMAR CA Y CASANARE	15	2	12	2	2	2
ZONA 6 - TOLIMA, HUILA Y CAQUETÁ	10	8	48	5	5	2
ZONA 7 - QUINDIO, RISARALDA, CALDAS Y VALLE DEL CAUCA	18	13	78	9	9	0
ZONA 8 - CAUCA, NARIÑO Y PÚTUMAYO	12	0	0	0	0	0
ZONA 9 - AMAZONAS	1	1	6	1	1	1
ZONA 10 - VICHADA, VAUPÈS, GUAVIARE Y META	12	9	54	5	5	5
TOTAL	120	71	426	51	48	26

FASE II

La fase II comprende la intervención de 33 despachos, los cuales se tienen previstos para la vigencia 2022 de conformidad con la reestructuración de supresión y reubicación de despachos así:

ZONAS A NIVEL NACIONAL	NUMEROS DE DESPACHOS A INTERVENIR NECESIDAD REAL	NUMEROS DE DESPACHOS A INTERVENIR FASE II	CANTIDAD DE PUNTOS DE CABLEADO FASE II	CANTIDAD DE EQUIPOS ACTIVOS RED LAN FASE II	CANTIDAD DE UPS FASE II	CANTIDAD DE AIRES ACONDICIONADOS FASE II
ZONA 1 - CORDOBA, SUCRE Y BOLÍVAR	5	4	20	3	3	2
ZONA 2 - ATLÁNTICO, MAGDALENA,	2	1	5	1	1	1



GUAJIRA CESAR	Y						
ZONA 3 ANTIOQUÍA CHOCÓ	- Y	8	7	35	7	7	1
ZONA 4 SANTANDER, NORTE DE SANTANDER Y ARAUCA	- DE Y	6	2	10	2	2	2
ZONA 5 BOGOTÁ, BOYACÁ, CUNDINAMARCA Y CASANARE	-	6	3	15	3	3	0
ZONA 6 TOLIMA, HUILA Y CAQUETÁ	-	5	1	5	1	1	1
ZONA 7 QUINDIO, RISARALDA, CALDAS Y VALLE DEL CAUCA	-	4	0	0	0	0	0
ZONA 8 CAUCA, NARIÑO Y PÚTUMAYO	-	11	11	55	9	9	3
ZONA 9 AMAZONAS	-	0	0	0	0	0	0
ZONA 10 VICHADA, VAUPÉS, GUAVIARE Y META	- Y	5	4	20	4	4	4
TOTAL		52	33	165	30	30	14

FASE III

La fase III comprende de 19 despachos los cuales se tienen previstos para su intervención en la vigencia 2023 de conformidad con la reestructuración, supresión y reubicación de despachos con la siguiente distribución:

ZONAS A NIVEL NACIONAL	NUMEROS DE DESPACHOS A INTERVENIR NECESIDAD REAL	NUMEROS DE DESPACHOS A INTERVENIR FASE III	CANTIDAD DE PUNTOS DE CABLEADO FASE III	CANTIDAD DE EQUIPOS ACTIVOS RED LAN FASE III	CANTIDAD DE UPS FASE III	CANTIDAD DE AIRES ACONDICIONADOS FASE III
ZONA 1 CORDOBA, SUCRE BOLÍVAR	- Y	1	1	5	1	1
ZONA 2 ATLÁNTICO, MAGDALENA, GUAJIRA CESAR	- Y	1	1	5	1	1
ZONA 3 ANTIOQUÍA CHOCÓ	- Y	1	1	5	1	1



ZONA 4 - SANTANDER, NORTE DE SANTANDER Y ARAUCA	4	4	20	3	3	3
ZONA 5 - BOGOTÁ, BOYACÁ, CUNDINAMARCA Y CASANARE	3	3	15	1	1	1
ZONA 6 - TOLIMA, HUILA Y CAQUETÁ	4	4	20	3	3	3
ZONA 7 - QUINDIO, RISARALDA, CALDAS Y VALLE DEL CAUCA	4	4	20	3	3	3
ZONA 8 - CAUCA, NARIÑO Y PÚTUMAYO	0	0	0	0	0	0
ZONA 9 - AMAZONAS	0	0	0	0	0	0
ZONA 10 - VICHADA, VAUPÉS, GUAVIARE Y META	1	1	5	1	1	1
TOTAL	19	19	95	14	14	14

A continuación, se presenta un listado y un mapa de ubicación de los despachos por zonas de intervención de las fases de implementación.

ZONA 1

Identificación	Estado	Acción	Actividad	Ubicación de implementación
1	Activo	Atención	Apoyo a la PDI	Despacho de implementación en Bogotá
2	Activo	Atención	Apoyo a la PDI	Despacho de implementación en Bogotá
3	Activo	Atención	Apoyo a la PDI	Despacho de implementación en Bogotá
4	Activo	Atención	Apoyo a la PDI	Despacho de implementación en Bogotá
5	Activo	Atención	Apoyo a la PDI	Despacho de implementación en Bogotá
6	Activo	Atención	Apoyo a la PDI	Despacho de implementación en Bogotá
7	Activo	Atención	Apoyo a la PDI	Despacho de implementación en Bogotá
8	Activo	Atención	Apoyo a la PDI	Despacho de implementación en Bogotá
9	Activo	Atención	Apoyo a la PDI	Despacho de implementación en Bogotá
10	Activo	Atención	Apoyo a la PDI	Despacho de implementación en Bogotá
11	Activo	Atención	Apoyo a la PDI	Despacho de implementación en Bogotá
12	Activo	Atención	Apoyo a la PDI	Despacho de implementación en Bogotá
13	Activo	Atención	Apoyo a la PDI	Despacho de implementación en Bogotá
14	Activo	Atención	Apoyo a la PDI	Despacho de implementación en Bogotá
15	Activo	Atención	Apoyo a la PDI	Despacho de implementación en Bogotá
16	Activo	Atención	Apoyo a la PDI	Despacho de implementación en Bogotá
17	Activo	Atención	Apoyo a la PDI	Despacho de implementación en Bogotá
18	Activo	Atención	Apoyo a la PDI	Despacho de implementación en Bogotá
19	Activo	Atención	Apoyo a la PDI	Despacho de implementación en Bogotá



Ilustración 12 Despachos de la zona 1, Córdoba, Sucre y Bolívar



La seguridad es de todos

Mindefensa



ZONA 2

ESTADO	DEPARTAMENTO	CUIDAD	FURSA	DESPACHO	ESTADO DE CONECTIVIDAD
	ATLANTICO	BARRANQUILLA	POLICIA NACIONAL	Juzgado del Departamento de Policía Atlántico	CONECTADO A LA RED IPM
	ATLANTICO	BARRANQUILLA	POLICIA NACIONAL	Fiscalía 151 ante Juzgado del Departamento de Policía	CONECTADO A LA RED IPM
	ATLANTICO	BARRANQUILLA	POLICIA NACIONAL	Juzgado 173 de Instrucción Penal Militar	CONECTADO A LA RED IPM
	ATLANTICO	BARRANQUILLA	POLICIA NACIONAL	Juzgado 174 de Instrucción Penal Militar	CONECTADO A LA RED IPM
	ATLANTICO	BARRANQUILLA	EJERCITO NACIONAL	Juzgado 1 de Brigada	CONECTADO A LA RED IPM (pendiente instalar puntos de cableado estructurado)
	ATLANTICO	BARRANQUILLA	EJERCITO NACIONAL	Fiscalía 12 ante Juzgado de Brigada	CONECTADO A LA RED IPM (pendiente instalar puntos de red y ups)
	ATLANTICO	BARRANQUILLA	EJERCITO NACIONAL	Juzgado 90 de Instrucción Penal Militar	DIAGNOSTICADO (instalación última milla en fibra óptica y sistemas estructurados)
	MAGDALENA	MALAMBO	EJERCITO NACIONAL	Juzgado 16 de Instrucción Penal Militar	CONECTADO A LA RED IPM (instalar puntos de red)
	MAGDALENA	SANTA MARTA	EJERCITO NACIONAL	Juzgado 17 de Instrucción Penal Militar	CONECTADO A LA RED IPM (pendiente instalar puntos de red y ups)
	MAGDALENA	SANTA MARTA	EJERCITO NACIONAL	Juzgado 19 de Instrucción Penal Militar	CONECTADO A LA RED IPM (pendiente instalar puntos de red y ups)
	MAGDALENA	SANTA MARTA	POLICIA NACIONAL	Juzgado del Departamento de Policía Magdalena	CONECTADO A LA RED IPM
	MAGDALENA	SANTA MARTA	POLICIA NACIONAL	Fiscalía 113 ante Juzgado del Departamento de Policía	CONECTADO A LA RED IPM
	MAGDALENA	SANTA MARTA	POLICIA NACIONAL	Juzgado 176 de Instrucción Penal Militar	CONECTADO A LA RED IPM
	CSAR	VALLEDUPAR	EJERCITO NACIONAL	Juzgado 15 de Instrucción Penal Militar	CONECTADO A LA RED IPM (pendiente instalar puntos de red y ups)
	CSAR	VALLEDUPAR	EJERCITO NACIONAL	Fiscalía 23 ante Juzgado de Brigada	CONECTADO A LA RED IPM (pendiente instalar puntos de red y ups)
	CSAR	VALLEDUPAR	EJERCITO NACIONAL	Juzgado 6 de Instrucción Penal Militar	CONECTADO A LA RED IPM (pendiente instalar puntos de red y ups)
	CSAR	VALLEDUPAR	EJERCITO NACIONAL	Juzgado 21 de Instrucción Penal Militar	CONECTADO A LA RED IPM (pendiente instalar puntos de red y ups)
	CSAR	VALLEDUPAR	EJERCITO NACIONAL	Juzgado 31 de Instrucción Penal Militar	LEVANTAMIENTO DE INFORMACIÓN (instalación última milla en fibra óptica y cableado estructurado)
	CSAR	VALLEDUPAR	POLICIA NACIONAL	Juzgado 170 de Instrucción Penal Militar	CONECTADO A LA RED IPM
	GUAJIRA	RIOCHACHA	EJERCITO NACIONAL	Juzgado 20 de Instrucción Penal Militar	CONECTADO A LA RED IPM (instalación última milla en fibra óptica y cableado estructurado)
	GUAJIRA	RIOCHACHA	POLICIA NACIONAL	Juzgado 177 de Instrucción Penal Militar	CONECTADO A LA RED IPM
	GUAJIRA	BUENAVISTA	EJERCITO NACIONAL	Juzgado 88 de Instrucción Penal Militar	LEVANTAMIENTO DE INFORMACIÓN (pendiente instalar puntos de red y ups)



Ilustración 13 Despachos de la zona 2, Atlántico, Magdalena, Cesar y la Guajira

ANTIOQUIA

ESTADO	DEPARTAMENTO	CUIDAD	FURSA	DESPACHO	ESTADO DE CONECTIVIDAD
	ANTIOQUIA	PUERTO BERRIO	EJERCITO NACIONAL	Juzgado 14 de Brigada	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	ANTIOQUIA	PUERTO BERRIO	EJERCITO NACIONAL	Fiscalía 21 ante Juzgado de Brigada	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	ANTIOQUIA	PUERTO BERRIO	EJERCITO NACIONAL	Juzgado 40 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	ANTIOQUIA	PUERTO BERRIO	EJERCITO NACIONAL	Juzgado 43 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	ANTIOQUIA	PUERTO BERRIO	EJERCITO NACIONAL	Juzgado 92 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	ANTIOQUIA	BELO	EJERCITO NACIONAL	Juzgado 24 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	ANTIOQUIA	APARTADO	POLICIA NACIONAL	Juzgado 167 de Instrucción Penal Militar	CONECTADO A LA RED IPM
	ANTIOQUIA	SEGOVIA	EJERCITO NACIONAL	Juzgado 128 de Instrucción Penal Militar	PENDIENTE POR DIAGNOSTICAR
	ANTIOQUIA	RONEGRO	FURSA AIBBA	Juzgado 122 de Instrucción Penal Militar	CONECTADO A LA RED IPM (pendiente instalar puntos de cableado estructurado)
	ANTIOQUIA	RONEGRO	EJERCITO NACIONAL	Juzgado 25 de Instrucción Penal Militar	CONECTADO A LA RED IPM
	ANTIOQUIA	ANDES	EJERCITO NACIONAL	Juzgado 27 de Instrucción Penal Militar	PENDIENTE POR DIAGNOSTICAR
	ANTIOQUIA	CAREPA	EJERCITO NACIONAL	Juzgado 28 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	ANTIOQUIA	CAREPA	EJERCITO NACIONAL	Juzgado 30 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	ANTIOQUIA	CAREPA	EJERCITO NACIONAL	Juzgado 62 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	ANTIOQUIA	CAREPA	EJERCITO NACIONAL	Juzgado 94 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	ANTIOQUIA	CAUCASIA	EJERCITO NACIONAL	Juzgado 42 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	ANTIOQUIA	CAUCASIA	EJERCITO NACIONAL	Juzgado 97 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)

ZONA 3 – PARTE 1



Ilustración 14 Despachos de la zona 3 - parte 1, Antioquia



ZONA 3 – PARTE 2

MEDELLÍN

Ubicación	Entidad	Ciudad	Fuerza	Despacho	Estatus de Conectividad
ANTIOQUIA	MEDELLÍN	EJÉRCITO NACIONAL	Juzgado 8 de brigada	DIAGNOSTICADO (estas instalaciones van a ser demolidas)	
ANTIOQUIA	MEDELLÍN	EJÉRCITO NACIONAL	Fiscalía 11 ante juzgado de brigada	DIAGNOSTICADO (estas instalaciones van a ser demolidas)	
ANTIOQUIA	MEDELLÍN	EJÉRCITO NACIONAL	Fiscalía 27 ante juzgado de brigada	DIAGNOSTICADO (estas instalaciones van a ser demolidas)	
ANTIOQUIA	MEDELLÍN	EJÉRCITO NACIONAL	Juzgado 22 de instrucción Penal Militar	DIAGNOSTICADO (instalación última milla en fibra óptica y cableado estructurado)	
ANTIOQUIA	MEDELLÍN	EJÉRCITO NACIONAL	Juzgado 23 de instrucción Penal Militar	DIAGNOSTICADO (instalación última milla en fibra óptica y cableado estructurado)	
ANTIOQUIA	MEDELLÍN	EJÉRCITO NACIONAL	Juzgado 32 de instrucción Penal Militar	DIAGNOSTICADO (estas instalaciones van a ser demolidas)	
ANTIOQUIA	MEDELLÍN	EJÉRCITO NACIONAL	Juzgado 87 de instrucción Penal Militar	DIAGNOSTICADO (instalación última milla en fibra óptica y cableado estructurado)	
ANTIOQUIA	MEDELLÍN	POLICÍA NACIONAL	Juzgado de Policía Metropolitana del Valle de Aburrá	CONECTADO A LA RED IPM	
ANTIOQUIA	MEDELLÍN	POLICÍA NACIONAL	Fiscalía 148 ante juzgado de Policía Metropolitana del Valle de Aburrá	CONECTADO A LA RED IPM	
ANTIOQUIA	MEDELLÍN	POLICÍA NACIONAL	Juzgado de Departamento de Policía Antioquia	CONECTADO A LA RED IPM	
ANTIOQUIA	MEDELLÍN	POLICÍA NACIONAL	Fiscalía 157 ante juzgado de Departamento de Policía	CONECTADO A LA RED IPM	
ANTIOQUIA	MEDELLÍN	POLICÍA NACIONAL	Fiscalía 158 ante juzgado de Departamento de Policía	CONECTADO A LA RED IPM	
ANTIOQUIA	MEDELLÍN	POLICÍA NACIONAL	Juzgado 153 de instrucción Penal Militar	CONECTADO A LA RED IPM	
ANTIOQUIA	MEDELLÍN	POLICÍA NACIONAL	Juzgado 154 de instrucción Penal Militar	CONECTADO A LA RED IPM	
ANTIOQUIA	MEDELLÍN	POLICÍA NACIONAL	Juzgado 155 de instrucción Penal Militar	CONECTADO A LA RED IPM	
ANTIOQUIA	MEDELLÍN	POLICÍA NACIONAL	Juzgado 162 de instrucción Penal Militar	CONECTADO A LA RED IPM	
ANTIOQUIA	MEDELLÍN	POLICÍA NACIONAL	Juzgado 163 de instrucción Penal Militar	CONECTADO A LA RED IPM	
ANTIOQUIA	MEDELLÍN	POLICÍA NACIONAL	Juzgado 187 de instrucción Penal Militar	CONECTADO A LA RED IPM	
ANTIOQUIA	MEDELLÍN	POLICÍA NACIONAL	Juzgado 188 de instrucción Penal Militar	CONECTADO A LA RED IPM	
ANTIOQUIA	MEDELLÍN	POLICÍA NACIONAL	Juzgado 189 de instrucción Penal Militar	CONECTADO A LA RED IPM	

POLICÍA	12
EJÉRCITO	7



Ilustración 15 Despachos de la zona 3 - parte 2, Antioquia

ZONA 3 – PARTE 3

CHOCÓ

ESTADO	DEPARTAMENTO	CIUDAD	FUERZA	DESPACHO	ESTADO DE CONECTIVIDAD
	CHOCÓ	QUIBDO	EJÉRCITO NACIONAL	Juzgado 7 de instrucción Penal Militar	PENDIENTE POR DIAGNOSTICAR
	CHOCÓ	QUIBDO	POLICÍA NACIONAL	Juzgado 165 de instrucción Penal Militar	CONECTADO A LA RED IPM
	CHOCÓ	LAS ANIMAS	EJÉRCITO NACIONAL	Juzgado 26 de instrucción Penal Militar	PENDIENTE POR DIAGNOSTICAR



Ilustración 16 Despachos de la zona 3 - parte 3, Chocó



La seguridad es de todos
Mindefensa



ZONA 4

ESTADO	DEPARTAMENTO	CIUDAD	FUERZA	DESPACHO	ESTADO DE CONECTIVIDAD
	SANTANDER	BUCARAMANGA	POLICIA NACIONAL	Juzgado 44 de Departamento de Policía Santander	CONECTADO A LA RED IPM
	SANTANDER	BUCARAMANGA	POLICIA NACIONAL	Fiscalía 159 ante Juzgado de Departamento de Policía	CONECTADO A LA RED IPM
	SANTANDER	BUCARAMANGA	POLICIA NACIONAL	Juzgado 168 de Instrucción Penal Militar	CONECTADO A LA RED IPM
	SANTANDER	BUCARAMANGA	EJERCITO NACIONAL	Juzgado 2 de Brigada	DIAGNOSTICADO (instalación última milla en fibra óptica y cableado estructurado)
	SANTANDER	BUCARAMANGA	EJERCITO NACIONAL	Fiscalía 25 ante Juzgado de Brigada	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	SANTANDER	BUCARAMANGA	EJERCITO NACIONAL	Juzgado 33 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	SANTANDER	BUCARAMANGA	EJERCITO NACIONAL	Juzgado 34 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	SANTANDER	BARRANCABIEMA	EJERCITO NACIONAL	Juzgado 38 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	NORTE DE SANTANDER	CUCUTA	EJERCITO NACIONAL	Juzgado 13 de Brigada	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	NORTE DE SANTANDER	CUCUTA	EJERCITO NACIONAL	Fiscalía 17 ante Juzgado de Brigada	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	NORTE DE SANTANDER	CUCUTA	EJERCITO NACIONAL	Juzgado 36 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	NORTE DE SANTANDER	CUCUTA	EJERCITO NACIONAL	Juzgado 86 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	NORTE DE SANTANDER	OCAÑA	EJERCITO NACIONAL	Juzgado 37 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	NORTE DE SANTANDER	CUCUTA	POLICIA NACIONAL	Juzgado 4 de Departamento de Policía Norte de Santander	CONECTADO A LA RED IPM
	NORTE DE SANTANDER	CUCUTA	POLICIA NACIONAL	Fiscalía 160 ante Juzgado de Departamento de Policía	CONECTADO A LA RED IPM
	NORTE DE SANTANDER	CUCUTA	POLICIA NACIONAL	Juzgado 171 de Instrucción Penal Militar	CONECTADO A LA RED IPM
	NORTE DE SANTANDER	CUCUTA	POLICIA NACIONAL	Juzgado 180 de Instrucción Penal Militar	CONECTADO A LA RED IPM
	ARAUCA	ARAUCA	EJERCITO NACIONAL	Juzgado 46 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	ARAUCA	ARAUCA	POLICIA NACIONAL	Juzgado 172 de Instrucción Penal Militar	CONECTADO A LA RED IPM
	ARAUCA	SARAVENA	EJERCITO NACIONAL	Juzgado 47 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	ARAUCA	TAME	EJERCITO NACIONAL	Juzgado 48 de Instrucción Penal Militar	PENDIENTE POR CONECTAR (El CGPM indica que se puede conectar este despacho al red IPM)
	ARAUCA	TAME	EJERCITO NACIONAL	Juzgado 95 de Instrucción Penal Militar	PENDIENTE POR CONECTAR (El CGPM indica que se puede conectar este despacho al red IPM)

NORTE DE SANTANDER



ARAUCA



Ilustración 17 Despachos de la zona 4, Santander, Norte de Santander y Arauca

ZONA 05 - PARTE 1

ESTADO	DEPARTAMENTO	CIUDAD	FUERZA	DESPACHO	ESTADO DE CONECTIVIDAD
	BOGOTÁ	BOGOTÁ	EJERCITO NACIONAL	Juzgado de Inspección de Ejército	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	EJERCITO NACIONAL	Fiscalía 7 ante Juzgado de Inspección	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	EJERCITO NACIONAL	Fiscalía 8 ante Juzgado de Inspección	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	EJERCITO NACIONAL	Juzgado 1 de División	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	EJERCITO NACIONAL	Juzgado 2 de División	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	EJERCITO NACIONAL	Fiscalía 4 ante Juzgado de División	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	EJERCITO NACIONAL	Fiscalía 10 ante Juzgado de División	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	EJERCITO NACIONAL	Juzgado 5 de Brigada	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	EJERCITO NACIONAL	Juzgado 6 de Brigada	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	EJERCITO NACIONAL	Juzgado 11 de Brigada	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	EJERCITO NACIONAL	Fiscalía 13 ante Juzgado de Brigada	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	EJERCITO NACIONAL	Fiscalía 24 ante Juzgado de Brigada	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	EJERCITO NACIONAL	Fiscalía 26 ante Juzgado de Brigada	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	EJERCITO NACIONAL	Fiscalía 28 ante Juzgado de Brigada	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	EJERCITO NACIONAL	Fiscalía 29 ante Juzgado de Brigada	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	EJERCITO NACIONAL	Juzgado 49 de Instrucción Penal Militar	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	EJERCITO NACIONAL	Juzgado 60 de Instrucción Penal Militar	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	EJERCITO NACIONAL	Juzgado 71 de Instrucción Penal Militar	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	EJERCITO NACIONAL	Juzgado 74 de Instrucción Penal Militar	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	EJERCITO NACIONAL	Juzgado 75 de Instrucción Penal Militar	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	EJERCITO NACIONAL	Juzgado 76 de Instrucción Penal Militar	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	EJERCITO NACIONAL	Juzgado 77 de Instrucción Penal Militar	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	EJERCITO NACIONAL	Juzgado 84 de Instrucción Penal Militar	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	ARMADA NACIONAL	Inspección de Inspección de la Armada	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	ARMADA NACIONAL	Fiscalía ante Juzgado de Inspección de la Armada	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	ARMADA NACIONAL	Juzgado de Primera Instancia de la Fuera Naval del Pacífico	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	ARMADA NACIONAL	Juzgado de Primera Instancia de la Fuera Naval del Sur	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	ARMADA NACIONAL	Fiscalía ante Juzgado de Primera Instancia de la Fuera Naval del Sur	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	ARMADA NACIONAL	Juzgado de Primera Instancia de la Brigada Fluvial y Segunda Brigada de Infantería de Marina	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	ARMADA NACIONAL	Fiscalía ante Juzgado de Primera Instancia de la Primera y Segunda Brigada de I. M. y de la Brigada Fluvial de Infantería de Marina	CONECTADO AL RED IPM
	BOGOTÁ	BOGOTÁ	ARMADA NACIONAL	Juzgado 105 de Instrucción Penal Militar	CONECTADO AL RED IPM

BOGOTÁ D. C.



Ilustración 18 Despachos de la zona 5 – parte 1, Bogotá D.C.



ZONA 05 - PARTE 2

ESTADO	DEPARTAMENTO	CIUDAD	FUERZA	DESPACHO	ESTADO DE CONECTIVIDAD
🟢	BOGOTÁ	BOGOTÁ	POLICIA NACIONAL	Juzgado de Inspección General de la Policía Nacional	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	POLICIA NACIONAL	Juzgado de Dirección General de la Policía	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	POLICIA NACIONAL	Fiscalía 141 ante Juzgado de Dirección General	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	POLICIA NACIONAL	Fiscalía 142 ante Juzgado de Inspección General	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	POLICIA NACIONAL	Fiscalía 143 ante Juzgado de Inspección General	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	POLICIA NACIONAL	Fiscalía 144 ante Juzgado de Inspección General	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	POLICIA NACIONAL	Fiscalía 145 ante Juzgado de Inspección General	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	POLICIA NACIONAL	Juzgado de Policía Metropolitana de Bogotá	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	POLICIA NACIONAL	Fiscalía 146 ante Juzgado de Policía Metropolitana de Bogotá	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	POLICIA NACIONAL	Fiscalía 147 ante Juzgado de Policía Metropolitana de Bogotá	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	POLICIA NACIONAL	Auditor de Guerra 141 de Policía Metropolitana	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	POLICIA NACIONAL	Juzgado de Departamento de Policía Cundinamarca1	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	POLICIA NACIONAL	Juzgado de Departamento de Policía Cundinamarca2	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	POLICIA NACIONAL	Fiscalía 150 ante Juzgado de Departamento de Policía	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	POLICIA NACIONAL	Fiscalía 151 ante Juzgado de Departamento de Policía	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	POLICIA NACIONAL	Auditor de Guerra 147 ante Juzgado de Instancia de Departamento de Policía Cundinamarca	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	POLICIA NACIONAL	Juzgado 141 de Instrucción Penal Militar	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	POLICIA NACIONAL	Juzgado 142 de Instrucción Penal Militar	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	POLICIA NACIONAL	Juzgado 143 de Instrucción Penal Militar	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	POLICIA NACIONAL	Juzgado 144 de Instrucción Penal Militar	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	POLICIA NACIONAL	Juzgado 146 de Instrucción Penal Militar	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	POLICIA NACIONAL	Juzgado 147 de Instrucción Penal Militar	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	POLICIA NACIONAL	Juzgado 148 de Instrucción Penal Militar	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	POLICIA NACIONAL	Juzgado 150 de Instrucción Penal Militar	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	POLICIA NACIONAL	Juzgado 185 de Instrucción Penal Militar	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	POLICIA NACIONAL	Juzgado 186 de Instrucción Penal Militar	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	POLICIA NACIONAL	Juzgado 189 de Instrucción Penal Militar	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	FUERZA AÉREA	Juzgado de Inspección de la Fuerza Aérea	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	FUERZA AÉREA	Fiscalía ante Juzgado de Inspección de la Fuerza Aérea	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	FUERZA AÉREA	Juzgado de Comando Aéreo 121	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	FUERZA AÉREA	Fiscalía ante Comando Aéreo 121	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	FUERZA AÉREA	Juzgado 121 de Instrucción Penal Militar	CONECTADO AL ARED IPM
🟢	BOGOTÁ	BOGOTÁ	FUERZA AÉREA	Juzgado 125 de Instrucción Penal Militar	CONECTADO AL ARED IPM

BOGOTÁ D. C



Ilustración 19 Despachos de la zona 5 parte 2, Bogotá

ZONA 05 - PARTE 3

ESTADO	DEPARTAMENTO	CIUDAD	FUERZA	DESPACHO	ESTADO DE CONECTIVIDAD
🟢	BOYACÁ	CHINQUIPIRA	EJÉRCITO NACIONAL	Juzgado 5 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instaurar surtos de cableado/estructurado)
🟢	BOYACÁ	TUNJA	EJÉRCITO NACIONAL	Juzgado 45 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instaurar surtos de cableado/estructurado)
🟢	BOYACÁ	TUNJA	POLICIA NACIONAL	Juzgado de Departamento de Policía Boyacá	CONECTADO A LA RED IPM
🟢	BOYACÁ	TUNJA	POLICIA NACIONAL	Fiscalía 162 ante Juzgado de Departamento de Policía	CONECTADO A LA RED IPM
🟢	BOYACÁ	TUNJA	POLICIA NACIONAL	Juzgado 391 de Instrucción Penal Militar	CONECTADO A LA RED IPM
🟢	BOYACÁ	DUITAMA	EJÉRCITO NACIONAL	Juzgado 78 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instaurar surtos de cableado/estructurado)
🟢	CUNDINAMARCA	TOLEMAIDA	EJÉRCITO NACIONAL	Juzgado 59 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instaurar surtos de cableado/estructurado)
🟢	CUNDINAMARCA	TOLEMAIDA	EJÉRCITO NACIONAL	Juzgado 82 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instaurar surtos de cableado/estructurado)
🟢	CUNDINAMARCA	TOLEMAIDA	EJÉRCITO NACIONAL	Juzgado 83 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instaurar surtos de cableado/estructurado)
🟢	CUNDINAMARCA	TOLEMAIDA	EJÉRCITO NACIONAL	Juzgado 88 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instaurar surtos de cableado/estructurado)
🟢	CUNDINAMARCA	FUSAGASUGA	EJÉRCITO NACIONAL	Juzgado 96 de Instrucción Penal Militar	PENDIENTE POR DIAGNOSTICAR
🟢	CUNDINAMARCA	PUERTO SALGAR	FUERZA AEREA	Juzgado de Comando Aéreo 122	CONECTADO A LA RED IPM
🟢	CUNDINAMARCA	PUERTO SALGAR	FUERZA AEREA	Fiscalía ante Comando Aéreo 122	CONECTADO A LA RED IPM
🟢	CUNDINAMARCA	PUERTO SALGAR	FUERZA AEREA	Juzgado 123 de Instrucción Penal Militar	CONECTADO A LA RED IPM

BOYACA



Ilustración 20 Despachos de la zona 5 - parte 3, Cundinamarca y Boyacá



ZONA 06 – PARTE 1

TOLIMA

ESTADO	DEPARTAMENTO	CIUDAD	FUERZA	DESPECHO	ESTADO DE CONECTIVIDAD
	TOLIMA	BAGUE	EJERCITO NACIONAL	Juzgado 7 de Brigada	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	TOLIMA	BAGUE	EJERCITO NACIONAL	Fiscalia 19 ante Juzgado de Brigada	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	TOLIMA	BAGUE	EJERCITO NACIONAL	Juzgado 79 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	TOLIMA	BAGUE	POLICIA NACIONAL	Juzgado de Departamento de Policia Tolima	CONECTADO A LA RED IPM
	TOLIMA	BAGUE	POLICIA NACIONAL	Fiscalia 163 ante Juzgado de Departamento de Policia	CONECTADO A LA RED IPM
	TOLIMA	BAGUE	POLICIA NACIONAL	Fiscalia 164 ante Juzgado de Departamento de Policia	CONECTADO A LA RED IPM
	TOLIMA	BAGUE	POLICIA NACIONAL	Juzgado 179 de Instrucción Penal Militar	CONECTADO A LA RED IPM
	TOLIMA	BAGUE	POLICIA NACIONAL	Juzgado 188 de Instrucción Penal Militar	CONECTADO A LA RED IPM
	TOLIMA	BAGUE	POLICIA NACIONAL	Juzgado 192 de Instrucción Penal Militar	CONECTADO A LA RED IPM

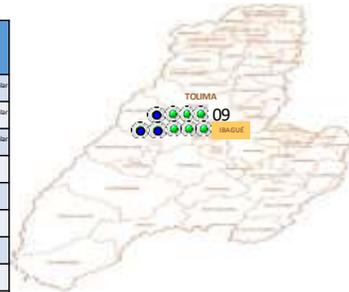


Ilustración 21 Despachos de la zona 6 - parte 1, Tolima

ZONA 06 – PARTE 2

ESTADO	DEPARTAMENTO	CIUDAD	FUERZA	DESPECHO	ESTADO DE CONECTIVIDAD
	CAQUETA	FLORENCIA	EJERCITO NACIONAL	Juzgado 12 de Brigada	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	CAQUETA	FLORENCIA	EJERCITO NACIONAL	Fiscalia 15 ante Juzgado de Brigada	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	CAQUETA	LARAN DIA	EJERCITO NACIONAL	Juzgado 51 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	CAQUETA	FLORENCIA	EJERCITO NACIONAL	Juzgado 66 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	CAQUETA	SAN VICENTE DEL CAQUI	EJERCITO NACIONAL	Juzgado 67 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	CAQUETA	LARAN DIA	EJERCITO NACIONAL	Juzgado 68 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	CAQUETA	LARAN DIA	EJERCITO NACIONAL	Juzgado 85 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	CAQUETA	TRIS ESQUINAS	FUERZA AEREA	Juzgado 127 de Instrucción Penal Militar	PENDIENTE POR CONECTAR (El cableado que se puede conectar está disponible a la Red de IPM)
	CAQUETA	FLORENCIA	POLICIA NACIONAL	Juzgado 181 de Instrucción Penal Militar	CONECTADO A LA RED IPM
	HUILA	NEIVA	EJERCITO NACIONAL	Juzgado 64 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	HUILA	GARZON	EJERCITO NACIONAL	Juzgado 65 de Instrucción Penal Militar	DIAGNOSTICADO (pendiente instalar puntos de cableado estructurado)
	HUILA	NEIVA	POLICIA NACIONAL	Juzgado 151 de Instrucción Penal Militar	CONECTADO A LA RED IPM
	HUILA	NEIVA	POLICIA NACIONAL	Juzgado 180 de Instrucción Penal Militar	CONECTADO A LA RED IPM
	TOLIMA	HONDA	POLICIA NACIONAL	Juzgado 80 de Instrucción Penal Militar	CONECTADO A LA RED IPM
	TOLIMA	CHARRARRAL	POLICIA NACIONAL	Juzgado 81 de Instrucción Penal Militar	CONECTADO A LA RED IPM

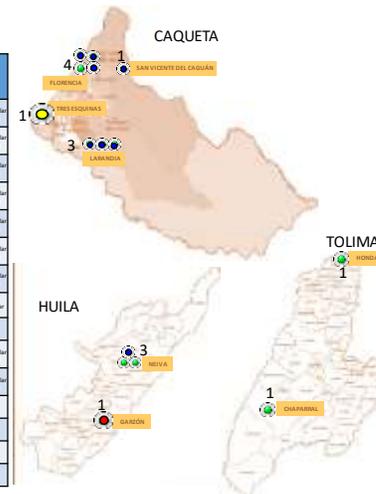


Ilustración 22 Despachos de la zona 6 - parte 2, Caquetá, Huila y Tolima



ZONA 07

Órgano	Departamento	Ciudad	Órgano	Unidad	Estado	Observaciones
ER	QUINDIO	ARMENIA	SEERCTO NACIONAL	Sección 9 de Inteligencia	DIAGNOSTICADO	(pendiente instalar puntos de cabecera estructurados)
ER	QUINDIO	ARMENIA	SEERCTO NACIONAL	Sección 28 de Inteligencia de Brigada	DIAGNOSTICADO	(pendiente instalar puntos de cabecera estructurados)
ER	QUINDIO	MONTENEGRO - PUEBLO DIPADO	SEERCTO NACIONAL	Sección 55 de Intercambio Penal Militar	DIAGNOSTICADO	(pendiente instalar puntos de cabecera estructurados)
ER	QUINDIO	ARMENIA	POLICIA NACIONAL	Sección 181 de Intercambio Penal Militar	CONECTADO A LA RED JPM	
ER	RISARALDA	FERRERA	SEERCTO NACIONAL	Sección 56 de Intercambio Penal Militar	CONECTADO A LA RED JPM	
ER	RISARALDA	FERRERA	POLICIA NACIONAL	Sección de Departamento de Policía de Ferrera alta	CONECTADO A LA RED JPM	
ER	RISARALDA	FERRERA	POLICIA NACIONAL	Sección 215 de Intercambio de Personal de Ferrera	CONECTADO A LA RED JPM	
ER	RISARALDA	FERRERA	POLICIA NACIONAL	Sección 159 de Intercambio Penal Militar	CONECTADO A LA RED JPM	
ER	VALLE	CAU	SEERCTO NACIONAL	Sección 8 de Inteligencia	DIAGNOSTICADO	(pendiente instalar puntos de cabecera estructurados)
ER	VALLE	CAU	SEERCTO NACIONAL	Sección 14 de Inteligencia de Brigada	DIAGNOSTICADO	(pendiente instalar puntos de cabecera estructurados)
ER	VALLE	CAU	SEERCTO NACIONAL	Sección 28 de Inteligencia de Brigada	DIAGNOSTICADO	(pendiente instalar puntos de cabecera estructurados)
ER	VALLE	CAU	SEERCTO NACIONAL	Sección 14 de Intercambio Penal Militar	CONECTADO A LA RED JPM	
ER	VALLE	CAU	SEERCTO NACIONAL	Sección 54 de Intercambio Penal Militar	CONECTADO A LA RED JPM	
ER	VALLE	CAU	SEERCTO NACIONAL	Sección 52 de Intercambio Penal Militar	CONECTADO A LA RED JPM	
ER	VALLE	CARTAGO	SEERCTO NACIONAL	Sección 53 de Intercambio Penal Militar	DIAGNOSTICADO	(pendiente instalar puntos de cabecera estructurados)
ER	VALLE	CAU	SEERCTO NACIONAL	Sección 71 de Intercambio Penal Militar	CONECTADO A LA RED JPM	
ER	VALLE	BUENAVENTURA	ARMADA NACIONAL	Sección 102 de Intercambio Penal Militar	DIAGNOSTICADO	(pendiente instalar puntos de cabecera estructurados)
ER	VALLE	BUENAVENTURA	ARMADA NACIONAL	Sección 108 de Intercambio Penal Militar	DIAGNOSTICADO	(pendiente instalar puntos de cabecera estructurados)
ER	VALLE	CAU	SUBDIR ARMA	Sección de Escuela de Formación	DIAGNOSTICADO	(pendiente instalar puntos de cabecera estructurados)
ER	VALLE	CAU	MERID ABBA	Sección de Escuela de Formación	DIAGNOSTICADO	(pendiente instalar puntos de cabecera estructurados)
ER	VALLE	CAU	MERID ABBA	Sección 126 de Intercambio Penal Militar	CONECTADO A LA RED JPM	
ER	VALLE	CAU	POLICIA NACIONAL	Sección de Policía Metropolitana de Santiago de Cali	CONECTADO A LA RED JPM	
ER	VALLE	CAU	POLICIA NACIONAL	Sección de Intercambio de Personal de Policía de Cali	CONECTADO A LA RED JPM	
ER	VALLE	CAU	POLICIA NACIONAL	Sección de Departamento de Policía de Valle	CONECTADO A LA RED JPM	
ER	VALLE	CAU	POLICIA NACIONAL	Sección 155 de Intercambio de Departamento de Policía	CONECTADO A LA RED JPM	
ER	VALLE	CAU	POLICIA NACIONAL	Sección 156 de Intercambio Penal Militar	CONECTADO A LA RED JPM	
ER	VALLE	CAU	POLICIA NACIONAL	Sección 156 de Intercambio Penal Militar	CONECTADO A LA RED JPM	
ER	VALLE	CAU	POLICIA NACIONAL	Sección 157 de Intercambio Penal Militar	CONECTADO A LA RED JPM	
ER	VALLE	CAU	POLICIA NACIONAL	Sección 158 de Intercambio Penal Militar	CONECTADO A LA RED JPM	
ER	VALLE	BILIA	POLICIA NACIONAL	Sección 194 de Intercambio Penal Militar	CONECTADO A LA RED JPM	



Ilustración 23 Despachos de la zona 7, Quindío, Risaralda y Valle

ZONA 08

Órgano	Departamento	Ciudad	Órgano	Unidad	Estado	Observaciones
ER	CAUCA	POPAYAN	SEERCTO NACIONAL	Sección 12 de Intercambio Penal Militar	PENDIENTE POR DIAGNOSTICAR	
ER	CAUCA	POPAYAN	SEERCTO NACIONAL	Sección 35 de Intercambio Penal Militar	PENDIENTE POR DIAGNOSTICAR	
ER	CAUCA	POPAYAN	SEERCTO NACIONAL	Sección 54 de Intercambio Penal Militar	PENDIENTE POR DIAGNOSTICAR	
ER	CAUCA	POPAYAN	POLICIA NACIONAL	Sección 183 de Intercambio Penal Militar	CONECTADO A LA RED JPM	
ER	NARIÑO	PASTO	SEERCTO NACIONAL	Sección 9 de Intercambio Penal Militar	DIAGNOSTICADO	(pendiente instalar puntos de cabecera estructurados)
ER	NARIÑO	IPAILES	SEERCTO NACIONAL	Sección 70 de Intercambio Penal Militar	DIAGNOSTICADO	(pendiente instalar puntos de cabecera estructurados)
ER	NARIÑO	IPAILES	SEERCTO NACIONAL	Sección 89 de Intercambio Penal Militar	DIAGNOSTICADO	(pendiente instalar puntos de cabecera estructurados)
ER	NARIÑO	PASTO	SEERCTO NACIONAL	Sección 91 de Intercambio Penal Militar	DIAGNOSTICADO	(pendiente instalar puntos de cabecera estructurados)
ER	NARIÑO	TUMACOC	ARMADA NACIONAL	Sección 107 de Intercambio Penal Militar	PENDIENTE POR DIAGNOSTICAR	
ER	NARIÑO	PASTO	POLICIA NACIONAL	Sección de Departamento de Policía de Pasto	CONECTADO A LA RED JPM	
ER	NARIÑO	PASTO	POLICIA NACIONAL	Sección 145 de Intercambio de Departamento de Policía de Pasto	CONECTADO A LA RED JPM	
ER	NARIÑO	PASTO	POLICIA NACIONAL	Sección 189 de Intercambio Penal Militar	CONECTADO A LA RED JPM	
ER	NARIÑO	PASTO	POLICIA NACIONAL	Sección 182 de Intercambio Penal Militar	CONECTADO A LA RED JPM	
ER	PUTUMAYO	SANTA ANA	SEERCTO NACIONAL	Sección 39 de Intercambio Penal Militar	PENDIENTE POR DIAGNOSTICAR	
ER	PUTUMAYO	MOCCA	SEERCTO NACIONAL	Sección 58 de Intercambio Penal Militar	DIAGNOSTICADO	(pendiente instalar puntos de cabecera estructurados)
ER	PUTUMAYO	PUERTO ASIS	SEERCTO NACIONAL	Sección 72 de Intercambio Penal Militar	PENDIENTE POR DIAGNOSTICAR	
ER	PUTUMAYO	PUERTO LEGUIZAMO	ARMADA NACIONAL	Sección 106 de Intercambio Penal Militar	PENDIENTE POR DIAGNOSTICAR	
ER	PUTUMAYO	MOCCA	POLICIA NACIONAL	Sección 184 de Intercambio Penal Militar	CONECTADO A LA RED JPM	



Ilustración 24 Despachos de la zona 8, Cauca, Pasto, Nariño y Putumayo

La implementación de estos servicios implica realizar una revisión y redefinición de la tecnología y los servicios utilizados actualmente por la JPMYP para los siguientes propósitos:

- Comunicación en tiempo real (sincrónica)
- Mensajería Instantánea.
- Telefonía IP (VoIP).
- Video conferencias.
- Comunicación asíncrona
- Correo electrónico
- Mensaje de voz
- SMS

Actualmente, la JPMYP cuenta con algunos de estos servicios, pero no están articulados de forma que apoyen las labores y en muchos casos, no han sido totalmente apropiados por los funcionarios (ej. correo electrónico). Adicionalmente, al estar todos gestionados de forma local, conllevan una alta carga operativa y de soporte interno.

Se plantea la tercerización de estos servicios por medio de la selección de un solo proveedor. La solución que se implemente deberá tener por lo tanto las siguientes características:

- Movilidad

Todos los funcionarios de la JPMYP deben contar con un número de extensión que pueda ser configurado en un “*Softphone*” (teléfono por software) o en un teléfono IP (Teléfono físico), siempre con la misma extensión sin importar su ubicación.

Se debe propender por el trabajo remoto permitiendo el acceso a los servicios de comunicación desde diversos dispositivos como celulares, tabletas, portátiles y equipos de escritorio.

- Integración de medios - Debe ser posible el reenvío de llamadas a la extensión al celular o dispositivo móvil asignado al funcionario, así como la revisión de mensajes de voz desde el correo electrónico.
- Gestión de la presencia - Esta característica busca permitir a los funcionarios el conocer la presencia de los usuarios en los diferentes medios para su fácil ubicación.
- Conferencias - busca que ya sean estas, telefónicas o video conferencias, el que no dependan de costosos equipos para su establecimiento, por ejemplo, utilizando la cámara de los equipos portátiles, el teléfono celular o el equipo de escritorio.

Por lo anterior, se contempla la implementación de los nuevos proyectos de unificación de sedes, como: las sedes de Palacio de la Justicia Penal Militar y Policial “TF. Laura Rocío Prieto Forero”, Bogotá, D.C, zona 1 - Córdoba, Sucre y Bolívar, zona 2 - Atlántico, Magdalena, Guajira y Cesar, zona 3 - Antioquía y Chocó,

zona 4 -Santander, Norte de Santander y Arauca, zona 5 - Bogotá, Boyacá, Cundinamarca y Casanare, zona 6 -Tolima, Huila y Caquetá, zona 7 - Quindío, Risaralda, Caldas y Valle del Cauca, zona 8 - Cauca, Nariño y Putumayo, zona 9 – Amazonas, zona 10 - Vichada, Vaupés, Guaviare y Meta.

8.5.3 Servicios de tecnología

8.5.3.1 Mesa de ayuda

Es el servicio de soporte a los usuarios que requieran de ayuda en la solución de incidentes o en la configuración de aplicaciones, conectividad, solución de fallos en el hardware o los periféricos, servicios de impresión y preguntas sobre la funcionalidad ofrecida por las aplicaciones provistas por la OTIC. Este conjunto de servicios fue adquirido usando el vehículo de compra de la tienda virtual de Colombia compra eficiente, y permite el soporte a nivel nacional con un conjunto de horas de soporte reactivo y prescriptivo, así como de un conjunto de repuestos para los equipos personales de cómputo.

Teniendo en cuenta los beneficios obtenidos en la vigencia 2021, en cuanto a cobertura geográfica y el mantenimiento correctivo, se continuará adquiriendo a través de la tienda virtual de Colombia Compra Eficiente a mediano plazo y por tres vigencias, se busca también paralelamente alinearse a las mejores prácticas de gestión de Tecnología y estándares internacionales ITIL, enfocando el servicio a la operación y a la adopción del sistema judicial oral acusatorio.

8.5.3.2 Administración de sistemas de información

La Oficina de Tecnologías de la Información y las Comunicaciones realiza la administración de los sistemas de información que apoyan los procesos de apoyo y misionales, al ser creada como una nueva entidad no se cuenta en principio con sistemas de información propios, durante la vigencia 2021 – 2024 y a través de los planes de acción se prevé una ejecución contractual que va a permitir el desarrollo e implementación de los sistemas misionales y de apoyo más importantes para llevar a cabo esos objetivos estratégicos así como su misión y visión.

8.5.3.3 Administración de la conectividad y las redes

La Unidad Administrativa Especial de la Justicia Penal Militar y Policial (UAEJPMP) actualmente tiene una infraestructura tecnológica de hardware, software y comunicaciones, instalada en el centro de datos del Ministerio de Defensa Nacional y en el edificio de la sede principal de la UAEJPMP.

Para cumplir con la monitorización, se cuenta con licencias de un software para este fin denominado “SolarWinds” el cuál ofrece mediciones de rendimiento detalladas que realizan diagnósticos, detección y permiten la resolución de

problemas de red en forma proactiva, ya que es posible observar el tráfico de la red. Se pone además en funcionamiento el software de Orión, y se realiza el seguimiento de los indicadores de rendimiento y del estado del hardware, del sistema operativo y del desempeño de la infraestructura física y virtual.

8.5.3.4 Administración de la plataforma tecnológica

El servicio de administración de plataforma tecnológica, permite gestionar los recursos físicos y lógicos que soportan la operación de los servicios de infraestructura, software y gestión de los recursos de red, este servicio seguirá desarrollándose con los recursos especializados y contratados con terceros avalados o certificados por los fabricantes de dichos componentes o servicios, En plataformas “*on premise*”(locales) o en la nube, con proveedores como Microsoft, AWS, HP, Dell, McAfee, Fortinet, entre otros, para así mantener los niveles de servicios altos de acuerdo con necesidades de nuestros usuarios y gestionados por la Oficina de Tecnologías de la Información y las Comunicaciones de la Unidad Administrativa Especial de la Justicia Penal Militar y Policial.

Para la vigencia 2022 se planea reemplazar los servidores, el almacenamiento, los switches tanto en el centro de datos Fortaleza del Ministerio de Defensa Nacional, como en el Palacio de Justicia, actualizando las versiones de todo el software a las versiones soportadas por los fabricantes e implementando una solución de respaldo y con redundancia que permita aumentar los niveles de disponibilidad.

Además se planea continuar con la suscripción a los recursos y servicios actualmente disponibles de la nube pública AWS, para el desarrollo de los servicios misionales y de apoyo como el portal, el sistema de gestión de calidad, el sistema judicial, los servicios de red y operación de TIC de plataforma dominio de directorio activo; entre otros, se continuará también con la suscripción a la suite de ofimática y de herramientas colaborativas con el fin de mantener las comunicaciones unificadas para los funcionarios de la entidad y mantener y mejorar la productividad lograda, así como el desarrollo de nuevos productos a ser implementados.

8.5.4 Equipos de cómputo personal

Teniendo en cuenta la obsolescencia observada y manifestada por los funcionarios en los equipos de cómputo personal, se planea continuar con la renovación de estos hasta llegar a un nivel de reposición del 20% anual, por lo que se tiene planeado para la vigencia 2022 adquirir 340 equipos adicionales y, con ello cumplir la meta propuesta desde la vigencia 2020.

También se continuará con el esquema de impresión tercerizada por convenio con fabricantes, con el fin de mantener dicho servicio actualizado a través de equipos de altas prestaciones.

8.6 Gestión de Información

La gestión de la información de los procesos actualmente es llevada en documentos físicos en papel, estos documentos en contadas ocasiones son digitales por lo que obtener datos de estos implica su revisión y estudio con ocasión de obtener los datos de casos puntuales o de obtener información estadística. La información de procesos de apoyo como el de Talento Humano reposan en sistemas y plataformas gestionadas por el MDN y su conservación respaldo y seguridad están fuera de la Oficina TIC y son gestionadas por los usuarios de esa área, así mismo ocurre con la información de otros procesos de apoyo como el financiero con el sistema SIIF y el control de inventarios y almacén a través del sistema SAP.

Otros procesos como el de gestión de la correspondencia, gestión de PQRSD, gestión de contratos, control disciplinario, no cuentan con sistemas de software que apoyen su gestión así que la información concerniente a cada una de ellas se maneja principalmente a través de documentos físicos, hojas de cálculo y el correo electrónico.

Para la gestión de parte de la información concerniente al listado de usuarios de los servicios tecnológicos, actualmente se tiene contratada un conjunto de horas para administración de las bases de datos. En el área de planeación se cuenta con funcionario que procesa los volúmenes de información en formato de hojas electrónicas remitida por los despachos más de 221 mensualmente, se planea soportar el procesamiento de dicha información con herramientas y mecanismos desarrollados dentro del sistema misional de gestión de casos judiciales, permitiendo un procesamiento automático de la información del proceso judicial para dar un conjunto de herramientas de alto nivel que permitan observar de primera mano el desarrollo de la gestión y el comportamiento de la justicia especial en su conjunto. Se espera también en colaboración con otras áreas de la entidad realizar la identificación y catalogación de los activos de información y así permitir de esta forma controlar el ciclo de vida de los datos que se consumen y generan dentro de los procesos de la Entidad, facilitando su conservación y seguridad.

8.7 Gobierno de T.I

8.7.1 Estructura organizacional y talento humano

La OTIC está conformada por tres grupos:

1. Grupo de Redes de Comunicaciones (3 funcionarios)
2. Grupo de Plataforma Tecnológica (5 funcionarios)
3. Grupo de Sistemas de Información (4 funcionarios)

Los funcionarios que hacen parte de cada uno de los grupos son de la planta de la Entidad, y son del nivel profesional y técnico.



La oficina se apoya en servicios especializados contratados con terceros avalados por los prestadores de servicios o fabricantes de productos. Para la mesa de ayuda se cuenta con el siguiente personal: un coordinador y un agente para recibo de llamadas telefónicas, dos (2) técnicos en el Palacio de Justicia y dos (2) técnicos a nivel nacional, que soportan el uso tecnológico de los distintos despachos de la Justicia Especial, de forma presencial y remota. Complementario a los servicios de nivel 1 (soporte presencial), se cuenta con servicios prestados por horas de nivel 2(escalamiento con especialista) para la administración de los servidores y de los incidentes con las redes y canales de comunicación; Los servicios de nivel 2 también se complementan con administración de servicios por horas, así: Software, Plataforma Windows, Antivirus McAfee, Seguridad Perimetral Fortinet, Almacenamiento NetApp, Monitorización SolarWinds y Redes de Comunicaciones Cisco.

La constitución de los grupos y sus respectivas funciones están consignadas en las resoluciones 000122 del 22 de julio de 2021 y 00027 del 18 de enero de 2022.

A continuación, se muestra el organigrama de la oficina: para la vigencia

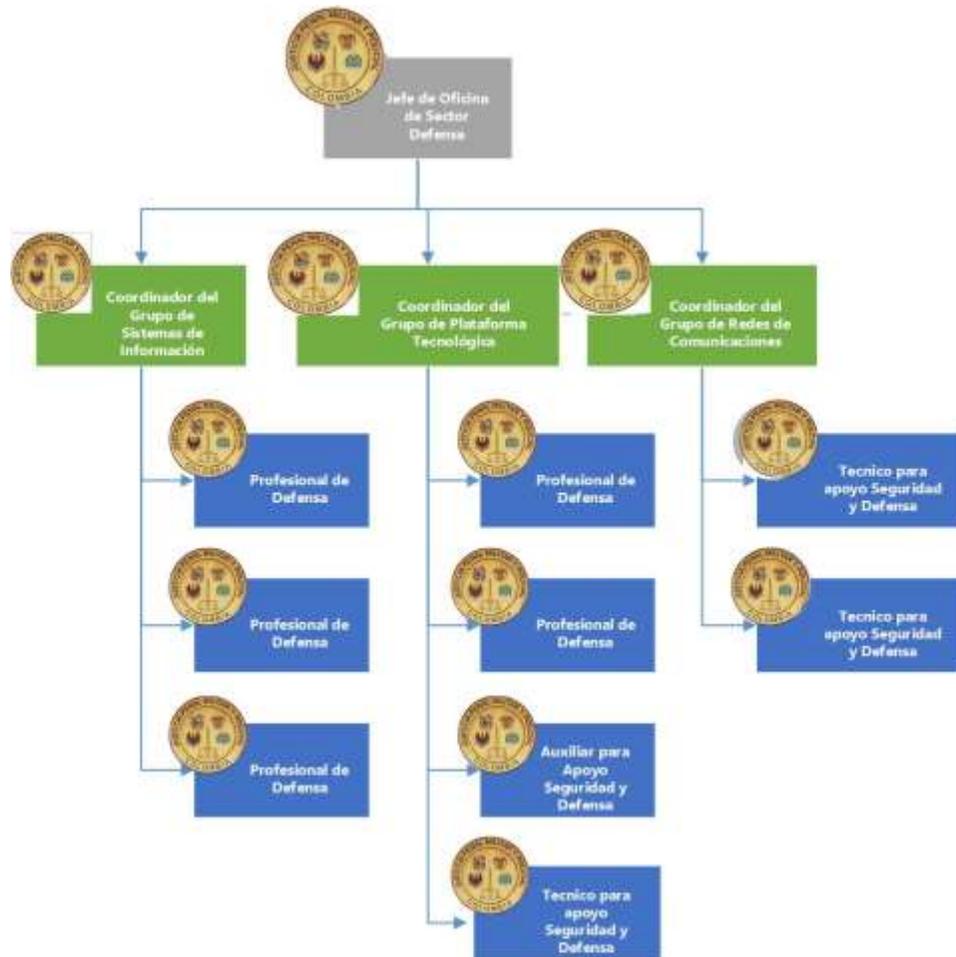


Ilustración 27 Organigrama OTIC



8.8 Análisis financiero

Desde poco después del nacimiento de la Unidad se ha contado con los recursos financieros con los que se ha buscado disminuir la brecha digital y la obsolescencia tecnológica en los equipos de escritorio y portátiles, servidores, infraestructura y servicios de conectividad, almacenamiento en los centros de datos y adquisición de los sistemas misionales y de apoyo, realizando una inversión de recursos por valor de 10 mil 780 millones de pesos durante el 2020 y 2021.

Para la vigencia 2022, se tiene planeada la inversión de alrededor de 9 mil 620 millones para conservar y aumentar los servicios de tecnología, culminar con la renovación de la plataforma tecnológica, de redes y conectividad proyectadas desde la vigencia 2020 de acuerdo con las necesidades de los despachos y de los sistemas misionales, que se deben desarrollar de acuerdo con la normatividad vigente.

Para las vigencias siguientes y hasta el 2025, consideramos se debe mantener la inversión para los servicios logrados hasta el momento y se deben proyectar algunos recursos adicionales con el fin de transformar e innovar la administración del sistema judicial y de la Unidad Administrativa Especial, por lo que se proyecta solicitar 10 mil quinientos millones para la vigencia 2023, 11 mil 500 millones para la vigencia 2024 y 12 mil millones para vigencia 2025.

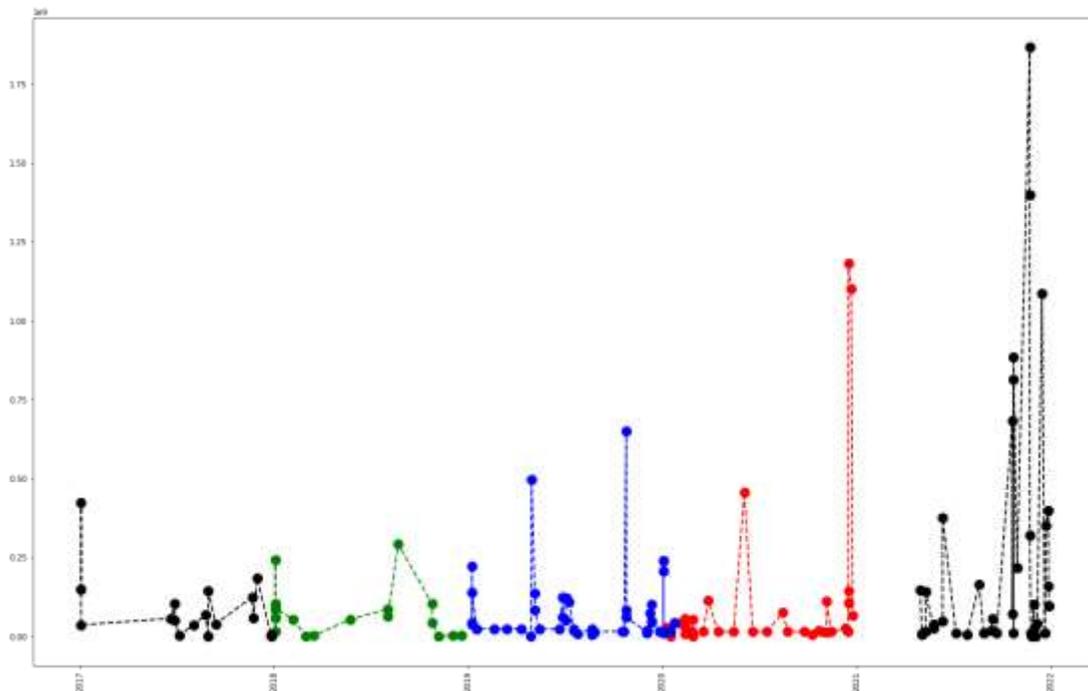


Ilustración 28 Gasto tecnológico histórico 2017 - 2021

En la gráfica anterior se puede ver la inversión que en materia tecnológica se ha hecho en la Entidad desde el 2017 y hasta el 2021.³

9 ENTENDIMIENTO ESTRATÉGICO

La UAESJPMP tiene una estructura orgánica compuesta así:

Estructura administrativa

1. Consejo Directivo
2. Dirección Ejecutiva
 - 2.1. Oficina Asesora de Planeación
 - 2.2. Oficina Asesora Jurídica
 - 2.3. Oficina de Tecnologías de Información y de las Comunicaciones
 - 2.3.1. Grupo de Sistemas de Información
 - 2.3.2. Grupo de Plataforma Tecnológica
 - 2.3.3. Grupo de Redes de Comunicaciones
 - 2.4. Oficina de Control Interno de Gestión
3. Subdirección General
4. Secretaría General
 - 4.1. Grupo de Talento Humano
 - 4.2. Grupo Financiero
 - 4.3. Grupo de Contratos
 - 4.4. Grupo de Control Disciplinario
 - 4.5. Grupo Administrativo
5. Escuela de la Justicia Penal Militar y Policial
6. Órganos de Asesoría y Coordinación
 - 6.1. Comité de Gestión y Desempeño Institucional
 - 6.2. Comisión de Personal

9.1 Modelo operativo

1. Tribunal Superior Militar y Policial
 - 1.1. Juzgados de Conocimiento Especializado de Justicia Penal Militar y Policial
 - 1.2. Juzgados de Conocimiento de Justicia Penal Militar y Policial
 - 1.3. Juzgados de Ejecución de Penas y Medidas de Seguridad de Justicia Penal Militar y Policial
 - 1.4. Juzgados de Control de Garantías de Justicia Penal Militar y Policial
Fiscalía General Penal Militar y Policial

³ El salto observado entre la línea roja y la negra corresponde al tránsito desde la Dirección Ejecutiva, hasta la Unidad Administrativa Especial. Se puede ver el aumento en inversión tecnológica desde el año 2020



La seguridad es de todos

Mindefensa



2. Fiscalías delegadas ante el Tribunal Superior Militar y Policial

2.1. Fiscalías ante Jueces de Conocimiento Especializado de Justicia Penal Militar y Policial

2.2. Fiscalías ante Jueces de Conocimiento de Justicia Penal Militar y Policial

2.3. Cuerpo Técnico de Investigación de la Justicia Penal Militar y Policial

Integración del comité directivo

1. El Ministro de Defensa Nacional, quien lo presidirá.
2. El Ministro de Justicia y del Derecho.
3. El Comandante General de las Fuerzas Militares.
4. El Director General de la Policía Nacional.
5. El Presidente de la Corte Suprema de Justicia.

A continuación, se ilustra la estructura orgánica y el mapa de procesos de la Entidad.

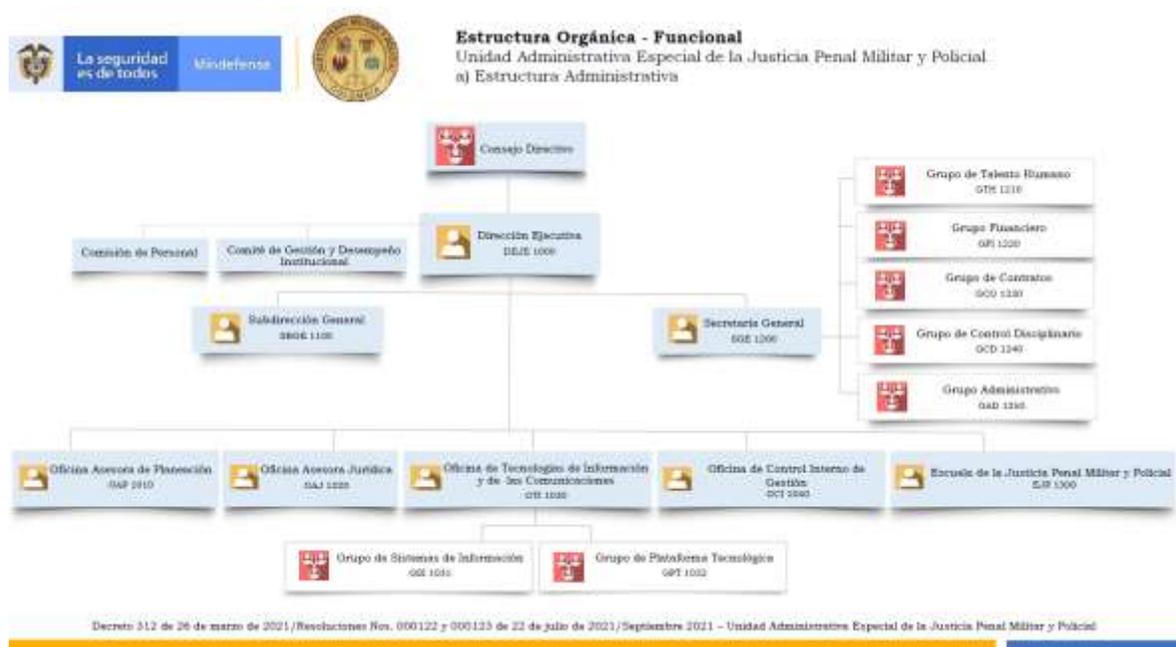


Ilustración 29 Estructura orgánica funcional, a) Estructura administrativa



La seguridad es de todos

Mindefensa



La seguridad es de todos

Mindefensa



Estructura Orgánica - Funcional

Unidad Administrativa Especial de la Justicia Penal Militar y Policial
b) Estructura Judicial



Ley 322 de 12 de agosto de 1999/Septiembre 2021 – Unidad Administrativa Especial de la Justicia Penal Militar y Policial

Ilustración 30 Estructura orgánica funcional, b) Estructura judicial



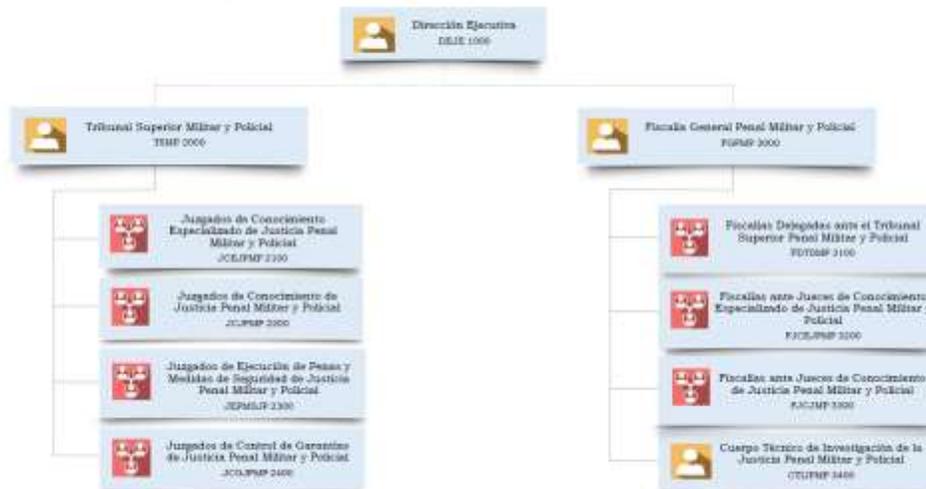
La seguridad es de todos

Mindefensa



Estructura Orgánica - Funcional

Unidad Administrativa Especial de la Justicia Penal Militar y Policial
b) Estructura Judicial



Ley 1407 de 17 de agosto de 2010/Decreto 312 de 26 de marzo de 2021/Septiembre 2021 – Unidad Administrativa Especial de la Justicia Penal Militar y Policial/Estructura judicial que entrará en funcionamiento durante la vigencia 2022

Ilustración 31 Estructura orgánica funcional, b) Estructura Judicial - vigencia 2022

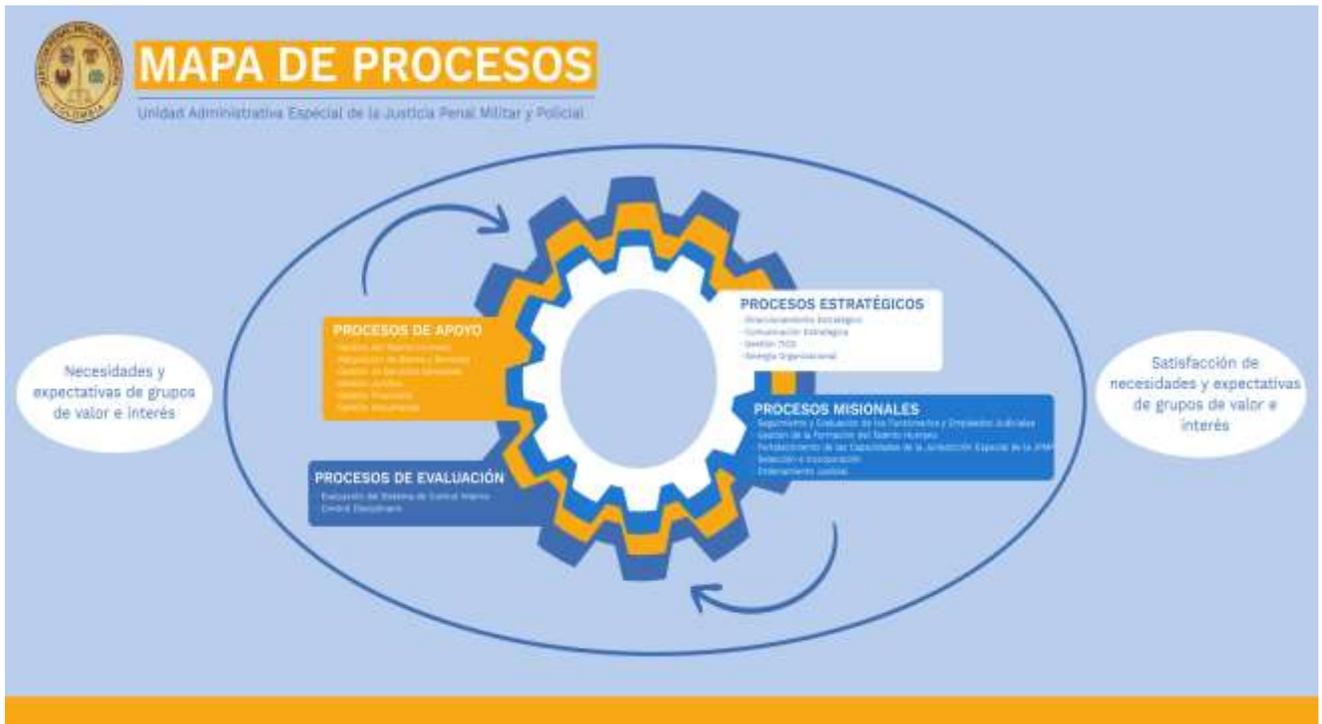


Ilustración 32 Mapa de procesos

9.2 Necesidades de información

Durante el ejercicio de diagnóstico de la situación actual de la Entidad se han evidenciado múltiples necesidades de información siendo las más relevantes para el cumplimiento de los objetivos misionales: la información de gestión de los procesos penales y la estadística asociada. Las distintas aristas de la información necesaria a ser visualizada pasan por la información relevante de KPI'S de la gestión procesal, contadas como cantidades de acciones hechas por los distintos actores dentro del proceso, así también se identifican las necesidades de soportes documentales gestionados de forma electrónica y segura como de consulta rápida y fiable de la información necesaria para operar justicia con mayor celeridad y brindando respuestas adecuadas a los solicitantes, partes interesadas, entidades externas y entes de control.

En los procesos de apoyo también se han diagnosticado estas brechas ya que como se ha mencionado no existen sistemas de información adecuados para la gestión de los procesos lo que retrasa la consecución de la información y es susceptible a los errores, lo que genera reprocesos y retrasan las labores de los funcionarios.

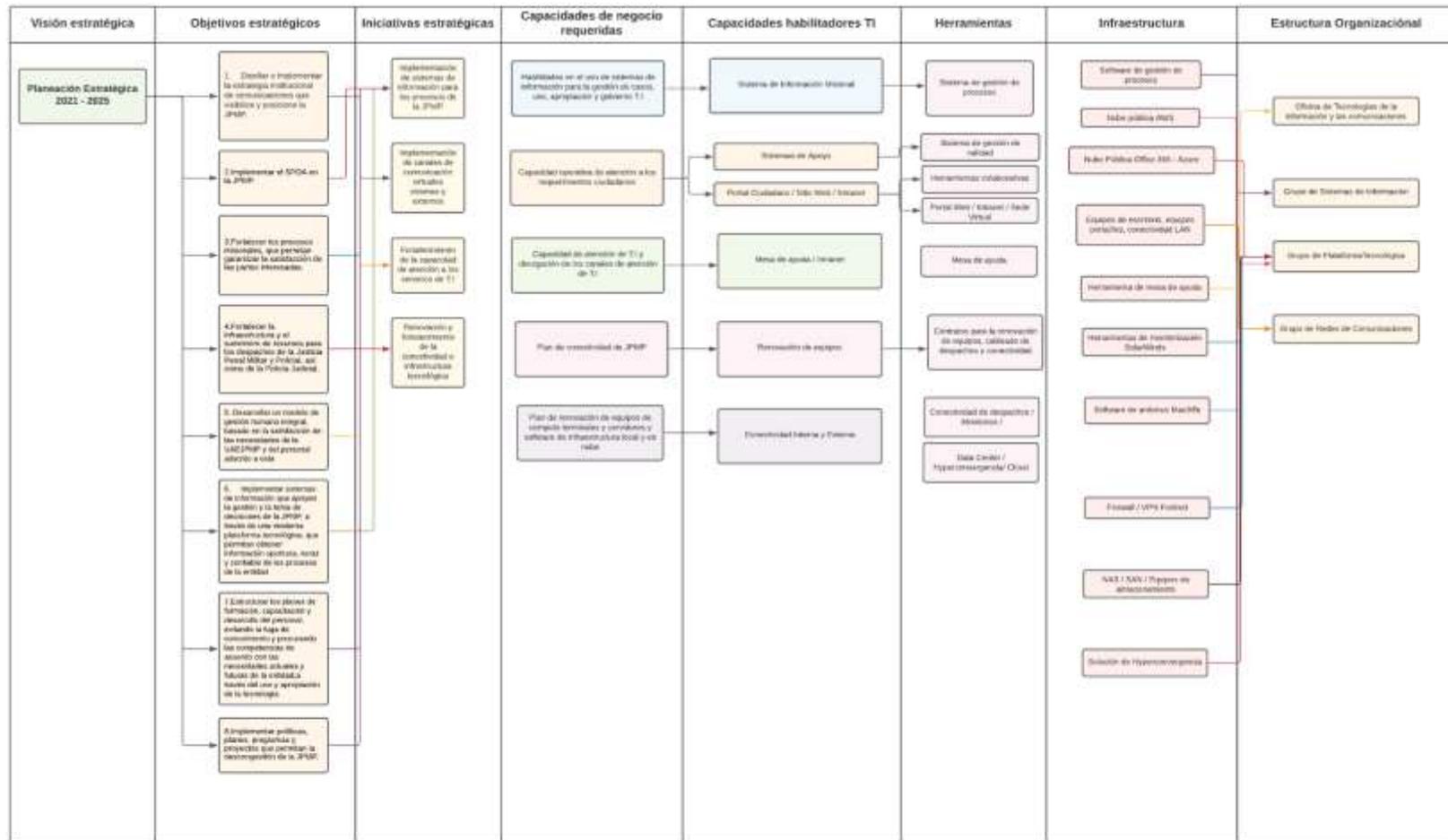
Es por esto por lo que se diseña este Plan de Tecnologías de la Información y las Comunicaciones PETIC, para servir de Plan Maestro y hoja de ruta de la gestión tecnológica por los próximos cuatro años.

9.3 Alineación de TI con los procesos

Teniendo en cuenta el decreto 1768 de 2020 que le da vida a la nueva Unidad Administrativa Especial, y a los lineamientos estratégicos definidos a través de la resolución 00010 del 7 de enero de 2022, el proceso de gestión TIC de la unidad se define como de apoyo en la cadena de valor de la Unidad para cumplir su misión y visión, teniendo en cuenta el objetivo estratégico de:

“Implementar sistemas de información que apoyen la gestión y la toma de decisiones de la Justicia Penal Militar y Policial, sobre una plataforma tecnológica moderna, que permita obtener la información oportuna, veraz y confiable de los procesos de la entidad.”

Presentamos el siguiente mapa de Alineación estratégica para el área TIC.



10 MODELO DE GESTIÓN DE TI

A continuación, se describe la situación deseada en materia de TI, desde el punto de vista de los dominios del Marco de Referencia de la Arquitectura Empresarial, Dominio de Planeación de la Arquitectura, Dominio de Arquitectura Misional, Dominio de Arquitectura de Información, Dominio de Arquitectura de Sistemas de Información, Dominio de Arquitectura de Infraestructura T.I, Dominio de Uso y Apropiación de la Arquitectura y Dominio de Arquitectura de Seguridad, alineado con la estrategia institucional y la del entorno sectorial, permitiendo el desarrollo de la gestión y generando valor estratégico para la comunidad, el sector, las dependencias y mejorando los procesos, facilitando el la administración y los recursos públicos a través del uso de la tecnología.

10.1 Estrategia de TI

La estrategia de TI para la UAESJPMP busca el cumplimiento de los objetivos estratégicos a través del uso y apropiación de habilitadores tecnológicos y el fortalecimiento de las capacidades institucionales, esta estrategia busca poner en las manos de los funcionarios de las áreas administrativas y misionales herramientas para el mejor desempeño de sus labores fortaleciendo el trabajo colaborativo, la seguridad de la información y la disponibilidad y oportunidad de esta.

Para esto se busca impactar de forma positiva todo el ecosistema que conforman la entidad y las instituciones del sector, mediante el uso y la apropiación de la tecnología por parte de los funcionarios, los elementos físicos de acceso a la tecnología como terminales de cómputo personal, sistemas de impresión y captura de documentos, redes de comunicación y adecuación de las redes internas y externas, sistemas de información oportunos y seguros, apoyo a los procesos misionales y de apoyo y fortalecimiento de la estrategia institucional, basadas en los principios de transparencia en la administración, economía en los recursos y eficacia en la ejecución.

10.1.1 Definición de los objetivos estratégicos de T.I.

A continuación, se definen los objetivos estratégicos del área de T.I en concordancia con los objetivos estratégicos de la UAESJPMP, en especial el objetivo número 7. *“(..). Implementar sistemas de información que apoyen la gestión y toma de decisiones de la Justicia Penal Militar y Policial, mediante una plataforma tecnológica moderna, que permita obtener información oportuna, veraz y confiable de los procesos de la entidad. (..)”*

10.1.1.1 Modernización y renovación de equipos tecnológicos

Sobre el entendimiento estratégico de que sobre una plataforma tecnológica moderna se construyen los sistemas de información que apoyan a la gestión por procesos, la OTIC adelantará los respectivos procesos internos de gestión y contractuales para la modernización de los equipos de cómputo, de escritorio y portátiles, cerrar la brecha de obsolescencia con la que se cuenta actualmente, este objetivo busca brindar herramientas adecuadas y modernas al personal de la entidad para el desarrollo de sus labores y el acceso adecuado a la gestión de la información en el ejercicio de sus labores. Se contempla dentro de este la modernización de equipos de conectividad y de adecuación del entorno tecnológico a nivel físico en todos sus aspectos como conexión entre despachos, conectividad externa y adecuación del entorno de operación.

10.1.1.2 Apoyo a la gestión misional y gestión administrativa a través de sistemas de información

Sobre una plataforma tecnológica moderna se busca a través del uso, la gestión y la operación de los sistemas de software ofrecer soluciones pertinentes a las áreas de la entidad unificando procesos y haciendo que las labores misionales cuenten con la disponibilidad de la información acelerando los procesos de toma de decisiones frente a las decisiones judiciales y administrativas, teniendo información de calidad y con la oportunidad necesaria para dar la ciudadanía las garantías de su labor misional.

10.1.1.3 Actualización y modernización de la plataforma tecnológica

Objetivo de plataforma tecnológica:

Invertir efectivamente en tecnología buscando formas de optimizar el rendimiento de las inversiones y reducir los costos:

- Estandarizar y simplificar la tecnología para aumentar la eficiencia.
- Mejorar la efectividad organizacional a través de servicios compartidos y abastecimiento estratégico.

10.2 Dominios de la Arquitectura Institucional

Durante el primer ejercicio de la arquitectura institucional se busca crear un mapa de ruta a seguir en futuros ejercicios, que contemplen los dominios

anteriormente mencionados y que además deberá contemplar los siguientes lineamientos y evidencias

10.2.1 Dominio de planeación de la arquitectura

ID	Nombre	Lineamiento	Evidencia
LI.ES.01	Entendimiento estratégico	La Unidad Administrativa Especial de la Justicia Penal Militar y Policial-UAESJPMP debe contar con una estrategia de TI que esté alineada con el plan estratégico institucional. La estrategia de TI debe estar orientada a generar valor y a contribuir al logro de los objetivos estratégicos.	Que el Plan Estratégico de Tecnologías de la Información – PETI, incorpore los objetivos estratégicos de TI alineados con el contexto organizacional y el entorno. Donde se presente de manera clara y concisa la alineación.
LI.ES.02	Definición de la arquitectura empresarial	La institución debe contar con una definición de Arquitectura Empresarial. Para ello, debe definir una arquitectura de negocio y una arquitectura de TI, en esta última deberá aplicar el Marco de Referencia de Arquitectura Empresarial para la gestión de TI del país. El ejercicio de Arquitectura Empresarial debe ser liderado conjuntamente por la alta dirección de la entidad y la Dirección de Tecnologías de la Información o quien haga sus veces. Mediante un trabajo articulado, la cabeza del sector debe contar con una definición de	Documentos o herramienta informática que refleje la Arquitectura Empresarial de la Entidad. La Arquitectura TI de la entidad debe ser desarrollada a partir de los 6 dominios del Marco de Referencia de AE para la gestión TI. Las entidades cabeza de sector deben contar adicionalmente con un equivalente de definición de AE para el sector.



		Arquitectura Empresarial a nivel sectorial que permita materializar su visión estratégica utilizando la tecnología como agente de transformación.	
LI.ES.03	Mapa de ruta de la arquitectura empresarial	La institución debe actualizar el Plan Estratégico de Tecnologías de la Información (PETI) con los proyectos priorizados en el mapa de ruta que resulte de los ejercicios de Arquitectura Empresarial e implementar dichos proyectos.	Plan Estratégico de TI que incluya un portafolio de proyectos priorizado y actualizado de acuerdo con los resultados de los ejercicios de arquitectura empresarial realizados en la entidad y en el sector
LI.ES.04	Proceso para evaluar y mantener la arquitectura empresarial	Cada institución debe diseñar e implementar un proceso de gobierno, que permita evaluar y mantener actualizada su Arquitectura Empresarial, acorde con los cambios estratégicos, organizacionales, regulatorios y nuevas tendencias tecnológicas. A nivel sectorial, la entidad cabeza de sector deberá coordinar la definición de un proceso de Arquitectura Empresarial o de Planeación Estratégica, que permita evaluar y mantener actualizada la Arquitectura Empresarial del sector.	Proceso definido de Planeación Estratégica y/o arquitectura empresarial en la entidad que contemple mecanismo de actualización y evaluación de la AE.y/o.
		La dirección de Tecnologías y Sistemas de la Información o	



LI.ES.05	Documentación de la estrategia de TI en el PETI	quien haga sus veces debe contar con una estrategia de TI documentada en el Plan Estratégico de las Tecnologías de la Información y Comunicaciones - PTI. El PTI debe contener la proyección de la estrategia para 4 años, y deberá ser actualizado anualmente a razón de los cambios de la estrategia del sector o de la institución, normatividad y tendencias tecnológicas. A nivel sectorial, la entidad cabeza de sector deberá definir los lineamientos, políticas y estrategia de TI sectoriales y plasmarlos en un Plan Estratégico de Tecnologías de la Información sectorial.	Plan Estratégico de Tecnologías de la Información o Plan Estratégico Institucional que incluya un capítulo o anexo específico de Tecnologías de la Información
LI.ES.06	Políticas y estándares para la gestión y gobernabilidad de TI	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe identificar y definir las políticas y estándares que faciliten la gestión y la gobernabilidad de TI, contemplando por lo menos los siguientes temas: seguridad, continuidad del negocio, gestión de información, adquisición tecnológica, desarrollo e implantación de sistemas de información, acceso a la tecnología y uso de las facilidades por	Políticas y estándares de TI a nivel institucional.



		parte de los usuarios. Así mismo, se debe contar con un proceso integrado entre las instituciones del sector que permita asegurar el cumplimiento y actualización de las políticas y estándares de TI.	
LI.ES.07	Plan de comunicación de la estrategia de TI	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir e implementar el plan de comunicación de la estrategia, las políticas, los proyectos, los resultados y los servicios de TI.	Plan de comunicación de la estrategia y gestión de TI
LI.ES.08	Participación en proyectos con componentes de TI	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe participar de forma activa en la concepción, planeación y desarrollo de los proyectos de la institución que incorporen componentes de TI. Así mismo, debe asegurar la conformidad del proyecto con los lineamientos de la Arquitectura Empresarial definidos para la institución, en lo que respecta a los dominios de TI. La conformidad del proyecto con la arquitectura misional es responsabilidad de las áreas funcionales.	Análisis del impacto de los proyectos que requieren apoyo tecnológico y participación en el comité de arquitectura de la entidad (en caso de estar conformado en la entidad). Cartas de proyecto, actas de seguimiento y cronogramas de los proyectos donde apoya TI o lidera. Contratos firmados donde se verifica la supervisión compartida entre TI y las áreas funcionales en los proyectos que tienen componentes tecnológicos, que implican el liderazgo de TI.



LI.ES.09	Control de los recursos financieros	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe realizar de manera periódica el seguimiento y control de la ejecución del presupuesto y el plan de compras asociado a los proyectos estratégicos definidos en el PTI.	Reportes, informes o actas de seguimiento y control de la ejecución del presupuesto asociados a los proyectos del PTI en desarrollo.
LI.ES.10	Gestión de proyectos de inversión	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe ser la responsable de formular, administrar, ejecutar y hacer seguimiento de las fichas de los proyectos de inversión requeridos para llevar a cabo la implementación de la Estrategia TI. El proceso de gestión de proyectos de inversión debe cumplir con los lineamientos que para este efecto establezca el Departamento Nacional de Planeación (DNP).	Fichas de proyectos de inversión de los proyectos que implementan la estrategia TI en la entidad.
LI.ES.11	Catálogo de servicios de TI	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe diseñar y mantener actualizado el catálogo de servicios de TI con los Acuerdos de Nivel de Servicio (ANS) asociados. La cabeza del sector consolidará los Catálogos de servicios de TI del sector.	Catálogo o portafolio de servicios de TI de la entidad. Las entidades cabeza de sector deben contar adicionalmente con un equivalente de catálogo TI para el sector.



LI.ES.12	Evaluación de la gestión de la estrategia de TI	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe realizar de manera periódica la evaluación de la Estrategia de TI, para determinar el nivel de avance y cumplimiento de las metas definidas en el PTI.	Soporte de las acciones derivadas producto del análisis y seguimiento a los indicadores asociados al cumplimiento de la estrategia de TI.
LI.ES.13	Tablero de Indicadores	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe contar con un tablero de indicadores, que permita tener una visión integral de los avances y resultados en el desarrollo de la Estrategia TI. A nivel sectorial, la entidad cabeza de sector, debe contar con un tablero de indicadores del sector.	Tablero de control actualizado con los indicadores asociados al cumplimiento de la estrategia de TI. Las entidades cabeza de sector deben contar adicionalmente con un equivalente de tablero de control para el sector

10.2.2 Alineación de la estrategia de TI con el plan sectorial territorial



Ilustración 33 Mapa de procesos de MDN

El Ministerio de Defensa Nacional expidió la Resolución 4240 de 2018, "Por la cual se adopta el Modelo integrado de Planeación y Gestión/ se integra el Modelo Estándar de Control Interno en el Sector Defensa/ se crea el Comité de Gestión y Desempeño para el Sector Defensa/ el Comité de Coordinación del Sistema de Control Interno/ el Comité Sectorial de Auditoría Interna/ se establecen otros lineamientos y se derogan unas resoluciones"

Esta Resolución define, en su artículo 5, que el Modelo Integrado de Planeación y Gestión (MIPG) para el Sector Defensa está constituido sobre siete (7) dimensiones: i) Talento Humano, ii) Direccionamiento Estratégico y Planeación, iii) Gestión con Valores para Resultados, iv) Evaluación de Resultados, v) Información y Comunicación, vi) Gestión del Conocimiento y la Innovación, y vii) Control Interno. Adicionalmente señala que cada dimensión se desarrolla a través de una o varias políticas de gestión y desempeño institucional, a saber: 1) Talento Humano, 2) Integridad, 3) Planeación Institucional, 4) Gestión presupuestal y eficiencia del gasto público, 5) Fortalecimiento organizacional y simplificación de procesos, 6) Transparencia, acceso a la información pública y lucha contra la corrupción, 7) Gestión documental, 8) Servicio al ciudadano, 9) Participación ciudadana en la gestión pública, 10) Racionalización de trámites, 11) Gobierno Digital, 12) Seguridad Digital, 13) Defensa Jurídica, 14) Seguimiento y evaluación del desempeño institucional, 15) Gestión del conocimiento y la innovación y 16) Control Interno.

Asimismo, la Resolución 7144 de 2018, modificada por la Resolución 2702 de 2020 crea el Modelo de Planeación y Desarrollo de Capacidades de la Fuerza Pública, entendido como el conjunto de procesos, instancias responsables y productos que de manera articulada y continua, traducen los lineamientos políticos y las prioridades estratégicas de defensa y seguridad, en las capacidades requeridas para la proyección y desarrollo en el mediano y largo plazo de una Estructura de Fuerza flexible, adaptable y sostenible.

Es de aclarar que las entidades adscritas y vinculadas al Sector Defensa gozan de autonomía e independencia en materia administrativa, presupuestal, financiera y jurídica, por tal razón la contribución de cada iniciativa o necesidad no obedece al Modelo de Planeación y, Desarrollo de capacidades de la Fuerza Pública.

10.2.3 Alineación de la estrategia de TI con la estrategia de la institución pública

Con el propósito de construir un Estado más eficiente, transparente y participativo, el Gobierno Nacional ha generado diferentes iniciativas para que las entidades públicas logren excelencia en la gestión y generen mayor confianza en la ciudadanía a partir del uso estratégico de la tecnología, mediante la

implementación de la Estrategia de Gobierno en Línea. Al respecto, el Gobierno Nacional en el año 2008 fijó los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia.

Posteriormente, transformó la estrategia de Gobierno en Línea en la Política de Gobierno Digital que conforme a lo dispuesto en el artículo 2.2.9.1.1.1 del Decreto 1078 de 2015, modificado por el artículo 1 del Decreto 1008 de 2018, estableció que esta nueva política debe ser entendida como el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital.

La Política de Gobierno Digital se fundamenta en dos componentes que orientan su desarrollo e implementación: TIC para el Estado y TIC para la Sociedad. El primero de ellos, tiene como objetivo mejorar el funcionamiento de las entidades públicas y su relación con otras entidades públicas, a través del uso de las Tecnologías de la Información y las Comunicaciones. A través de este componente se busca que las entidades fortalezcan sus competencias en Tecnologías de la Información (TI), a nivel de su arquitectura institucional y las competencias de sus funcionarios como elementos generadores de valor en la gestión pública.

Asimismo, la política de Gobierno Digital establece tres habilitadores transversales definidos como los elementos fundamentales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los componentes y el logro de los propósitos de la Política. El habilitador transversal de Arquitectura, busca que las entidades apliquen en su gestión un enfoque de Arquitectura Empresarial para el fortalecimiento de sus capacidades institucionales y de gestión de TI. Este habilitador soporta su uso e implementación en el Marco de Referencia de Arquitectura Empresarial del Estado que es el instrumento que establece la estructura conceptual, define lineamientos, incorpora mejores prácticas y traza la ruta de implementación que una entidad pública debe realizar.

El Manual de Gobierno Digital, emitido por el Ministerio TIC en enero de 2010 y con versión vigente de abril de 2019, indica que todo proyecto que haga uso de las TIC, debe ser analizado y estructurado desde las dimensiones de la arquitectura empresarial (arquitectura misional o de negocio, sistemas de información, información, infraestructura tecnológica, gobierno de TI, estrategia de TI y uso y apropiación), de tal manera que todos los proyectos que incorporen el uso de tecnología, contribuyan al cumplimiento de los objetivos estratégicos

de la entidad, garanticen la calidad de los resultados esperados y estén alineados con los procesos estratégicos, misionales y operativos de la entidad.

10.3 Gobierno de TI

La toma de decisiones en temas de tecnología se realiza a través de una mesa de trabajo en donde participan:

- El asesor del Despacho del señor Director para temas de tecnología
- El jefe de la Oficina de Tecnologías de la Información y las Comunicaciones
- El coordinador del Grupo de Plataforma Tecnológica
- El coordinador del Grupo de Sistemas de Información
- El coordinador del Grupo de Redes de Comunicaciones

Este grupo se reúne semanalmente para evaluar el desempeño de la gestión de las TIC, se revisan los avances en los planes de contratación y de acción de la Entidad y se toman decisiones de priorización de las tareas orientadas al fortalecimiento y la implementación. En promedio durante la última vigencia se desarrollaron 22 reuniones de este grupo.

Este dominio brinda directrices para implementar esquemas de gobernabilidad de TI y para adoptar las políticas que permitan alinear los procesos y planes de la institución con los del sector.

ID	Nombre	Lineamiento	Evidencia
LI.GO.01	Alineación del gobierno de TI	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir e implementar un esquema de Gobierno TI alineado con la estrategia misional y con el Modelo de Gestión de la UAESJPMP, que estructure y dirija el flujo de las decisiones de TI.	La entidad debe poseer una política de TI actualizada, aprobada y comunicada, acorde con la estrategia de la entidad y el sistema integrado de gestión. Modelo de gobierno de TI.
LI.GO.02	Apoyo de TI a los procesos	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe apoyar la especificación de las necesidades de sistematización y demás apoyo tecnológico requerido por los procesos de la institución, de tal manera que se incorporen facilidades tecnológicas que contribuyan a mejorar la articulación, calidad, eficiencia, seguridad y reducir	Documento de necesidades de sistematización y apoyo tecnológico a los procesos de la institución.



		los costos de operación.	
LI.GO.03	Conformidad	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir e incorporar dentro de su plan estratégico, acciones que permitan corregir, mejorar y controlar procesos de TI que se encuentren dentro de la lista de no conformidades generada en el marco de las auditorías de control interno y externo, a fin de contribuir con el compromiso de mejoramiento continuo de la administración pública de la institución.	Definición y medición de los indicadores de resultado o impacto de las soluciones de TI. Plan de acción producto de la evaluación de las mediciones de los indicadores o impacto de las soluciones de TI. Plan de acción específico para la atención de aquellos procesos que se encuentren dentro de la lista de no conformidad del marco de las auditorías de control interno y externo de gestión. Evidencias de seguimiento y realización de acciones definidas en el plan de acción para la atención de no conformidades asociada a la gestión de TI.
LI.GO.04	Macroproceso de gestión de TI	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe estructurar e implementar un macroproceso de gestión de TI, según los lineamientos del Modelo de Gestión de la UAESJPMP y teniendo en cuenta las buenas prácticas del Modelo de gestión estratégica de TI.	Proceso de gestión de TI definido en el mapa de procesos de la entidad. Evidencias de implementación del proceso de gestión de TI.
LI.GO.05	Capacidades y recursos de TI	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe generar, direccionar, evaluar y monitorear las capacidades de TI, asegurando el adecuado aprovisionamiento del talento humano y los recursos necesarios para ofrecer los servicios de TI de la institución.	Plan de capacidad de TI para cada uno de los servicios de TI establecidos en el catálogo de Servicios de TI. Mediciones de capacidades de TI.
LI.GO.06	Optimización de las compras de TI	La entidad debe realizar las compras de bienes o servicios de Tecnología a través de Acuerdos Marco de Precios (AMP) existentes, en caso de que apliquen, y dar prioridad a adquisiciones en modalidad de servicio o por demanda.	Contratos firmados de adquisición de servicios o bienes por AMP. Contratos de adquisición de bienes o servicios en modalidad de servicio o por demanda.



		Debe además propender por minimizar la compra de bienes de hardware.	
LI.GO.07	Criterios de adopción y de compra de TI	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir los criterios y metodologías que direccionen la toma de decisiones de inversión en Tecnologías de la Información (TI), buscando el beneficio económico y de servicio de la institución.	Metodología y criterios de evaluación de alternativas de solución e inversión en TI. Resultados de evaluación de alternativas de solución e inversión de TI a partir de la aplicación de la metodología y criterios utilizados.
LI.GO.08	Retorno de la inversión de TI	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe establecer la relación costo-beneficio y justificar la inversión de los proyectos de TI mediante casos de negocio e indicadores financieros.	Metodología y criterios de evaluación de alternativas de solución e inversión en TI. Resultados de evaluación de alternativas de solución e inversión de TI.
LI.GO.09	Liderazgo de proyectos de TI	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe liderar la planeación, ejecución y seguimiento a los proyectos de TI. En aquellos casos en que los proyectos estratégicos de la institución incluyan componentes de TI y sean liderados por otras áreas, la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, deberá supervisar el trabajo sobre el componente de TI conforme con los lineamientos de la Arquitectura Empresarial de la institución.	Cartas de proyecto, actas de seguimiento y cronogramas de los proyectos donde apoya TI o lidera. Contratos firmados donde se verifica la supervisión compartida entre TI y las áreas funcionales en los proyectos que tienen componentes tecnológicos, que implican el liderazgo de TI.
LI.GO.10	Gestión de proyectos de TI	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe gestionar todas las iniciativas y proyectos de TI, utilizando una metodología formal de gestión de proyectos que incorpore el uso de lecciones aprendidas y un esquema de gestión de cambios.	Evidencias de gestión de los Planes de Proyecto de TI. Carpeta de los contratos de los proyectos de TI actualizada. Carpeta de los proyectos de TI, cuando fueron realizados por personal interno.
LI.GO.11	Indicadores de gestión de los proyectos de TI	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, debe monitorear y hacer seguimiento a la ejecución de	Actas de reunión de seguimiento a proyectos. Tablero de control de gestión de TI, con



		los proyectos de TI, por medio de un conjunto de indicadores de alcance, tiempo, costo y calidad que permitan identificar desviaciones y tomar las acciones correctivas pertinentes.	indicadores de seguimiento a proyectos.
LI.GO.12	Evaluación del desempeño de la gestión de TI	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe realizar el monitoreo y evaluación de desempeño de la gestión de TI a partir de las mediciones de los indicadores del macroproceso de Gestión TI y demás que haya definido la entidad.	Indicadores de gestión de TI definidos y documentados. Encuestas de satisfacción del proceso de gestión de TI y/o instrumentos utilizados para realizar las mediciones, junto con los resultados obtenidos en cada una de las mediciones realizadas, que permitan evidenciar la evaluación del desempeño de la gestión de TI Tablero de control con resultados de mediciones de los indicadores de desempeño de la gestión de TI.
LI.GO.13	Mejoramiento de los procesos	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe identificar oportunidades de mejora en los procesos de TI, de modo que pueda focalizar esfuerzos en la optimización de estos a través de las TI para contribuir con el cumplimiento de los objetivos institucionales y del sector o territorio.	Proyectos o iniciativas de mejoramiento de los procesos de TI para contribuir al cumplimiento de las metas institucionales y los indicadores de desempeño de la gestión de TI.
LI.GO.14	Gestión de proveedores de TI	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe administrar todos los proveedores y contratos asociados con los proyectos de TI. Durante el proceso contractual se debe aplicar un esquema de dirección, supervisión, seguimiento, control y recibo a satisfacción de los bienes y servicios contratados.	Actas de aprobación y recibo a satisfacción de productos o servicios. Criterios de calidad y aceptación de los productos y servicios contratados. Documentos y demás soportes de supervisión, seguimiento y control generados durante los proyectos de TI, que evidencien gestión del proveedor.



LI.GO.15	Transferencia de información y conocimiento	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe gestionar la adecuada transferencia de información y conocimiento asociado a los bienes y servicios de TI contratados por la institución.	Procedimiento de gestión y/o transferencia de conocimiento asociado a los bienes y/o servicios de TI contratados por la entidad. Documentación funcional y técnica cuando aplique de cada uno de los servicios y bienes contratados por la entidad publicados en un repositorio institucional. Actas de sesiones de transferencia, capacitación y entrega de bienes y servicios de TI y recibo a satisfacción.
-----------------	---	--	--

10.3.1 Cadena de valor de TI

Cadena de valor TI

Donaldo Jinette | March 29, 2022

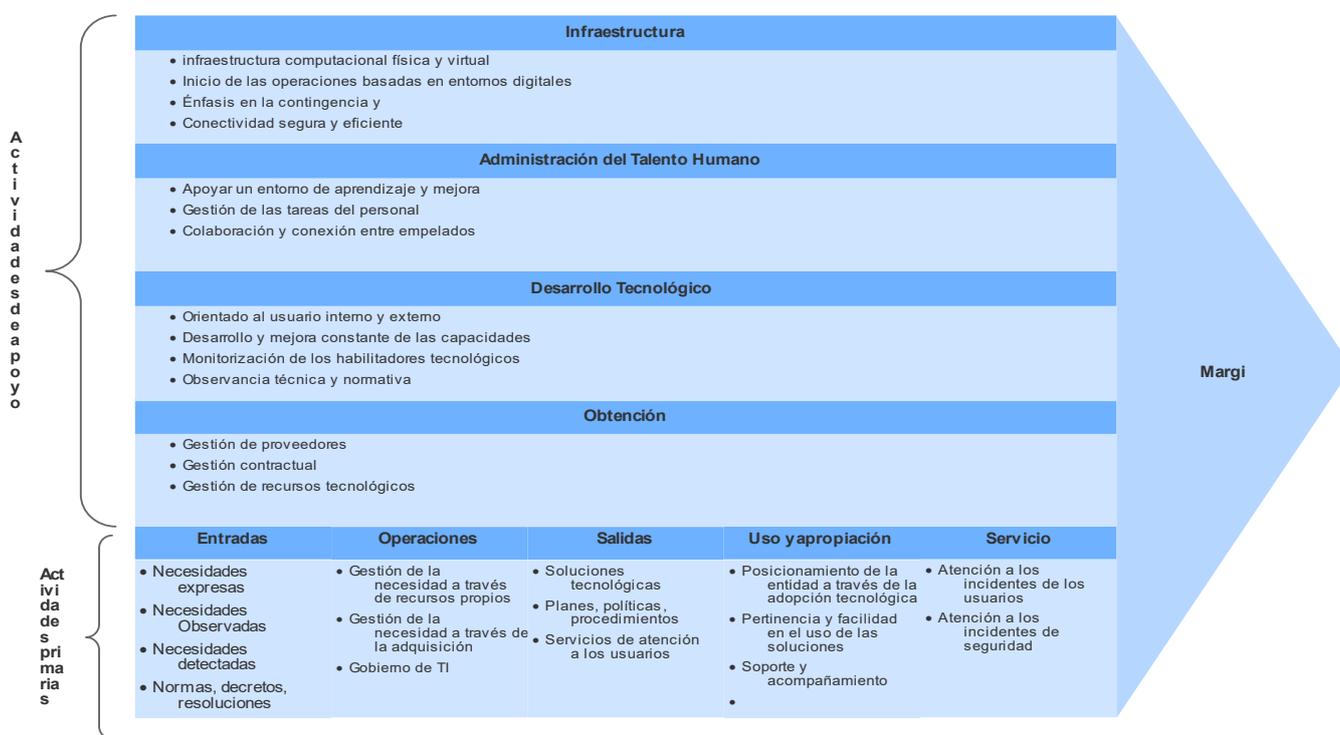


Ilustración 34 Cadena de valor de T.I

10.3.2 Indicadores y riesgos

UNIDAD ADMINISTRATIVA ESPECIAL JUSTICIA PENAL MILITAR Y POLICIAL		Mapa de Riesgos por Procesos de UAEJMPM								
Código	Proceso	Responsable	Causas Inmediatas	Causa Raíz	Descripción del Riesgo	Tipo de Riesgo	Frecuencia	Probabilidad	Impacto	Zona de Riesgo Inherente
001	GESTIÓN DE LAS TIC	Jefe de las Tic	Por vulneración a los controles de acceso o por Falta en la definición de controles de los mismos.	Intereses indebidos en el acceso de la información de procesos misionales	Pérdida reputacional y/o económica por quejas, demandas o sanciones de los grupos de valor debido a pérdida de confidencialidad en activos que contiene información privada, reservada o sensible administrados por la OTIC.	Corrupción	diaria	muy alta	catastrófico	Crítica
001	GESTIÓN DE LAS TIC	Jefe de las Tic	Por fallas técnicas o por vulneración a los servicios de plataforma tecnológica y de comunicaciones	Intereses indebidos en impedir el acceso de la información de procesos misionales o falta o falla en los controles de disponibilidad de la plataforma tecnológica	Pérdida reputacional y/o económica por la indisponibilidad de los servicios tecnológicos y/o sistemas de información administrados por OTIC.	Corrupción	diaria	muy alta	catastrófico	Crítica
001	GESTIÓN DE LAS TICS	Jefe de las Tic	Por vulneración a los controles o por fallas humanas en el registro de la información o por falta en la definición de controles en la protección de los datos.	Falta de controles que garanticen el registro de información confiable o vulnerabilidades técnicas que permitan la modificación no permitida de los datos.	Pérdida de credibilidad por realizar modificación a los registros realizados en sistemas de información misionales o estratégicos violando el carácter de confiabilidad y veracidad de lo allí registrado en cada una de las etapas del proceso.	Corrupción	diaria	muy alta	catastrófico	Crítica

Descripción del control	Tipo de control	Implementación	Calificación	Documentación	Frecuencia del control	Evidencia	Probabilidad Residual	Impacto Residual	Zona del Riesgo Final	Tratamiento
Parametrizar los componente de seguridad en los diferentes sistemas de información por parte de los dueños de los sistemas de información y de la Otics	Preventivo	Manual	15%	no esta documentado	diario	Con registro	Baja	catastrófico	Crítica	Compartir
Parametrizar los controles de acceso perimetral para bloquear cualquier intento de acceso no autorizado a la infraestructura TIC.	Preventivo	Manual	15%	no esta documentado	diario	Con registro	Baja	catastrófico	Crítica	Compartir
Adquirir e implementar herramientas y artefactos tecnológicos que refuercen y amplien la cobertura que impida el acceso a la activos de información privada, reservada o sensible.	Preventivo	Manual	15%	no esta documentado	diario	Con registro	Baja	catastrófico	Crítica	Compartir
Verificar disponibilidad de los Acuerdos de Niveles de Servicio (ANS) pactados con los proveedores de los servicios de plataforma para garantizar la prestación a los grupos de valor de manera permanente y continua.	Preventivo	Manual	15%	Documentado	Anual	Con registro	Baja	Mayor	Alto	Compartir
Realizar seguimiento mensual al cumplimiento y disponibilidad de los ANS firmados con los proveedores de los servicios de conectividad para garantizar la prestación del servicio a los grupos de valor de manera permanente y continua.	Preventivo	Automático	25%	Documentado	Mensual	Con registro	Baja	Mayor	Alto	Compartir
Mantener actualizado el plan de continuidad y recuperación para la prestación de los servicios tecnológicos	Correctivo	Manual	15%	Documentado	Anual	Con registro	Baja	catastrófico	Crítica	Compartir
Establecer perfiles y roles de acceso a los sistemas (se puede definir la instancia a la que puede acceder)	Preventivo	Manual	15%	no esta documentado	diario	Con registro	Baja	catastrófico	Crítica	Compartir
Implementar controles en el software que impidan la modificación accidental o intencional de la información gestionada.	Detectivo	Automático	25%	no esta documentado	diario	Con registro	Baja	catastrófico	Crítica	Compartir

 UNIDAD ADMINISTRATIVA ESPECIAL JUSTICIA PENAL MILITAR Y POLICIAL		Mapa de Riesgos por Procesos de UAEJPM			
Plan de Acción	Responsable	fecha Implementación	Fecha de seguimiento	Seguimiento	Estado
Parametrizar los componente de seguridad en los diferentes sistemas de información por parte de los dueños de los sistemas de información y de la Otics	Jefe de las Tics	30/03/2022			En curso
Parametrizar los controles de acceso perimetral para bloquear cualquier intento de acceso no autorizado a la infraestructura de TIC para prevenir accesos no autorizados.	Jefe de las Tics	31/03/2022			En curso
Adquirir e implementar herramientas y artefactos tecnológicos que refuercen y amplien la cobertura que impida el acceso a la activos de información privada, reservada o sensible.	Jefe de las Tics	01/04/2022			En curso
Verificar los niveles de acuerdos de servicio ANS de los proveedores de plataforma en la nube y equipos "on premise" con los que cuenta la UAESJPM	Jefe de las Tics	02/04/2022			En curso
Realizar seguimiento al cumplimiento de los niveles de acuerdos de servicio ANS de los proveedores de equipos de comunicación y canales de datos con los que cuenta la UAESJPM	Jefe de las Tics	03/04/2022			En curso
Elaborar y/o actualizar los planes de continuidad y recuperación de los servicios tecnológicos	Jefe de las Tics	04/04/2022			En curso
Realizar una revisión de los perfiles, roles y privilegios de acceso que tienen los distintos usuarios sobre los sistemas de información y plataformas de acceso a los recursos tecnológicos con los líderes de procesos	Jefe de las Tics	05/04/2022			En curso
Revisar junto con los proveedores de software y los líderes de procesos y dueños del software los controles existentes y ver la necesidad de aplicar controles nuevos que impidan la modificación accidental o intencional de la información	Jefe de las Tics	05/04/2022			En curso

10.3.3 Plan de implementación de procesos

Procesos / Procedimientos	Responsable	Fecha de entrega
Caracterización del proceso	Jefe de la Oficina de las Tics	Mayo 2022
Procedimiento para Gestión de las Tics	Jefe de la Oficina de las Tics	Junio 2022
Procedimiento de gestión de cambios tecnológico	Coordinador de grupo de sistemas de información	Julio 2022
Procedimiento de atención por mesa de ayuda	Coordinador de grupo de plataforma tecnológica	Agosto 2022

10.4 Gestión de información

Este dominio permite definir el diseño de los servicios de información, la gestión del ciclo de vida del dato, el análisis de información y el desarrollo de capacidades para el uso estratégico de la misma.



ID	NOMBRE	LINEAMIENTO	EVIDENCIA
LI.INF.01	Responsabilidad y gestión de componentes de información	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir las directrices y liderar la gestión de los Componentes de información durante su ciclo de vida. Así mismo, debe trabajar en conjunto con las dependencias para establecer acuerdos que garanticen la calidad de la información.	Documento de Política de TI, actualizado y aprobado en la entidad, publicado en la Intranet o de fácil acceso para los funcionarios de la entidad. Modelo o esquema de gobierno de Información documentado, con evidencias de su aplicación. Proceso de gestión del ciclo de vida de los componentes de información. Existencia de roles y perfiles que desempeñen las funciones de gestión de los componentes de información. Acuerdos entre áreas que establezcan criterios de calidad para la producción, intercambio y consumo de componentes de información.
LI.INF.02	Plan de calidad De los componentes de información	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe contar con un plan de calidad de los componentes de información que incluya etapas de aseguramiento, control e inspección, medición de indicadores de calidad, actividades preventivas, correctivas y de mejoramiento continuo de la calidad de los componentes.	Plan de calidad evidencias de implementación del plan.
LI.INF.03	Gobierno de la Arquitectura de Información	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir, implementar y gobernar la Arquitectura de Información, estableciendo métricas e indicadores de seguimiento, gestión y evolución de dicha arquitectura.	Artefactos y documentos que expresan la Arquitectura de componentes de información, actualizados. Documento de Modelo de Gobierno de Arquitectura de Información. Tablero de Control y gestión de TI.
LI.INF.04	Gestión de documentos electrónicos	La dirección de Tecnologías y Sistemas de la Información o	Procesos y procedimientos de gestión documental que incorporen la gestión de



		quien haga sus veces debe establecer un programa para la gestión de documentos y expedientes electrónicos y contemplar dichos componentes dentro de la Arquitectura de Información de la institución.	documentos y expedientes electrónicos. Artefactos y evidencias de la Arquitectura de Información que incorpore elementos de gestión del ciclo de vida de la gestión documental.
LI.INF.06	Lenguaje común de intercambio de componentes de información	Se debe utilizar el lenguaje común para el intercambio de información con otras instituciones. Si el lenguaje no incorpora alguna definición que sea requerida a escala institucional o sectorial, la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces deberá solicitar la inclusión al Ministerio de las TIC para que pueda ser utilizada por otras instituciones y quede disponible en el portal de Lenguaje común de intercambio de información del Estado colombiano.	Certificación de nivel 2 o 3 del Lenguaje Común de Intercambio de Datos. Solicitud (es) de incorporación de nuevos elementos de datos en el Lenguaje Común de Intercambio de Datos. Cuando aplique
LI.INF.07	Directorio de servicios de Componentes de información	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe crear y mantener actualizado un directorio de los Componentes de información. La institución es responsable de definir el nivel de acceso de este directorio teniendo en cuenta la normatividad asociada. Este directorio debe hacer parte del directorio de Componentes de información sectorial, el cual debe ser consolidado a través de la cabeza de sector, con el fin de promover y facilitar el consumo, reúso, ubicación y	Directorio de componentes de Información actualizado.



		entendimiento, entre otros de los Componentes de información.	
LI.INF.08	Publicación de los servicios de intercambio de Componentes de información	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe publicar los servicios de intercambio de información a través de la Plataforma de Interoperabilidad del Estado colombiano.	Servicios web publicados en la Plataforma de Interoperabilidad y en el directorio de servicios de Intercambio de Información del MINTIC. Certificación Nivel 3 del Lenguaje común de intercambio.
LI.INF.09	Canales de acceso a los Componentes de información	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe garantizar los mecanismos que permitan el acceso a los servicios de información por parte de los diferentes grupos de interés, contemplando características de accesibilidad, seguridad y usabilidad.	Catálogo de Componentes de Información. Canales de acceso implementados y disponibles de acuerdo con la normatividad y las características de los grupos de interés
LI.INF.10	Mecanismos para el uso de los Componentes de información	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe impulsar el uso de su información a través de mecanismos sencillos, confiables y seguros, para el entendimiento, análisis y aprovechamiento de la información por parte de los grupos de interés.	Mecanismos implementados que impulsen el uso de los servicios de información.
LI.INF.11	Acuerdos de intercambio de Información	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe establecer los Acuerdos de Nivel de Servicio (ANS) con las dependencias o instituciones para el intercambio de la información de calidad, que contemplen las características de	Documentos de los acuerdos de nivel de servicio (ANS) vigentes para el intercambio de información, firmados y aprobados por las áreas y/o entidades que participan en el intercambio.



		oportunidad, disponibilidad y seguridad que requieran los Componentes de información.	
LI.INF.12	Fuentes unificadas de información	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe garantizar la existencia de fuentes únicas de información, para que el acceso sea oportuno, relevante, confiable, completo, veraz y comparable.	Catálogo de componentes de Información donde este identificadas las Fuentes oficiales y únicas de información.
LI.INF.13	Hallazgos en el acceso a los Componentes de información.	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe generar mecanismos que permitan a los consumidores de los Componentes de información reportar los hallazgos encontrados durante el uso de los servicios de información.	Proceso o procedimiento de gestión de hallazgos sobre los servicios de información. Mecanismo de reporte de hallazgos sobre los servicios de información.
LI.INF.14	Protección y privacidad de Componentes de información	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe incorporar, en los atributos de los Componentes de información, la información asociada con los responsables y políticas de la protección y privacidad de la información, conforme con la normativa de protección de datos de tipo personal y de acceso a la información pública.	Catálogo de componentes de información.
LI.INF.15	Auditoría y trazabilidad de Componentes de información	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir los criterios necesarios para asegurar la trazabilidad y auditoría sobre las acciones de creación,	Registro de auditoría y trazabilidad desarrollados en la entidad.

	actualización, modificación o borrado de los Componentes de información. Estos mecanismos deben ser considerados en el proceso de gestión de dicho Componentes. Los sistemas de información deben implementar los criterios de trazabilidad y auditoría definidos para los Componentes de información que maneja.	
--	---	--

10.4.1 Herramientas de análisis

Actualmente la entidad se encuentra en proceso de implementación de la herramienta de inteligencia empresarial negocios, Microsoft POWER B.I. para generación de estadísticas de los procesos judiciales que se adelantan mensualmente en la jurisdicción especializada. Para el conteo de los casos e información en tableros de control.

10.4.2 Arquitectura de información

A continuación, se detallan la estructura de la información de acuerdo con los repositorios de datos que se tendrán disponibles a partir de la implementación de los sistemas de información de acuerdo con el mapa de ruta.

	Sistema de gestión de casos penales	Sistema de PQRS	Sistema de gestión de Correspondencia	SAP	PYOER	SIATH	Sistema de gestión de calidad
Intervinientes en el proceso (denunciados, víctimas y testigos)	X						
Expediente Digital (Denuncia, Autos, Sentencias, Providencias.)	X						
Proceso Penal Ley 522 de 1999	X			X			
Proceso Penal Ley 1407 de 2010	X						
Petición		X					
Queja		X					
Reclamo		X					

Denuncia	X	X	X				
Política							
Informe supervisión							
Decreto							
Resolución							
Planes de acción							X
Planes de Mejora							X
Indicadores							X

10.5 Sistemas de información

Este dominio permite planear, diseñar la arquitectura, el ciclo de vida, las aplicaciones, los soportes y la gestión de los sistemas que facilitan y habilitan las dinámicas en una institución

ID	NOMBRE	LINEAMIENTO	EVIDENCIA
LI.SIS.01	Definición estratégica de los sistemas de información	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir y documentar la arquitectura de los sistemas de información de la institución identificando los diferentes componentes y la forma en que interactúan entre sí, así como la relación con los demás dominios de la Arquitectura Empresarial.	Documento y/o artefacto que describa la arquitectura de los sistemas de información.
LI.SIS.02	Catálogo de sistemas de información	La institución debe disponer un catálogo actualizado de sus sistemas de información, que incluya atributos que permitan identificar la información relevante que facilite la gobernabilidad de estos. Las entidades cabeza de sector adicionalmente deben consolidar y mantener actualizado el catálogo de sistemas de información sectorial.	Catálogo de los sistemas de información.
LI.SIS.03	Arquitecturas de referencia de los sistemas de información	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces es la responsable de definir y evolucionar las arquitecturas de referencia de los sistemas de información, con el propósito de orientar el diseño de cualquier arquitectura de solución bajo parámetros, patrones y atributos de calidad definidos.	Arquitecturas de referencia definidas por la entidad.
LI.SIS.04	Arquitecturas de solución de sistemas de información	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe garantizar la documentación y actualización de la arquitectura de solución de los sistemas de información de la institución bajo los parámetros de las arquitecturas de referencia definidas.	Arquitecturas de Solución para los proyectos de sistemas de información.
LI.SIS.05	Metodología de referencia para el desarrollo de	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir una metodología formal para el	Metodologías para el ciclo de vida de desarrollo Software.



	Sistemas de información	desarrollo y mantenimiento de software, que oriente los proyectos de construcción o evolución de los sistemas de información que se desarrollen a la medida, ya sea internamente o a través de terceros.	
LI.SIS.06	Derechos patrimoniales sobre los sistemas de información	Cuando se suscriban contratos con terceras partes bajo la figura de "obra creada por encargo" o similar, cuyo alcance incluya el desarrollo de elementos de software, la entidad debe incluir en dichos contratos, la obligación de transferir a la institución los derechos patrimoniales sobre los productos desarrollados.	Contratos de cesión de derechos para los proyectos liquidados y para los contratos en curso que se evidencie la cesión de derechos de parte del proveedor.
LI.SIS.07	Guía de estilo y usabilidad	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir o adoptar una guía de estilo y usabilidad para la institución. Esta guía debe estar aplicada de acuerdo con la caracterización de usuarios y según el canal utilizado por los sistemas de información y, así mismo, debe estar alineada con los principios de usabilidad definidos por el Estado colombiano, asegurando la aplicación de la guía en todos sus sistemas de información. Para los componentes de software, que sean propiedad de terceros, se debe realizar su personalización hasta donde sea posible de manera que se pueda brindar una adecuada experiencia de usuario.	Documento y/o artefacto donde se describa y detallen los lineamientos de estilo y usabilidad para el desarrollo de sistemas de información en la entidad, que se encuentre accesible en un repositorio documental de consulta a cualquier usuario. Sistemas de Información de la entidad que aplican la guía de estilo y usabilidad.
LI.SIS.08	Apertura de datos	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe asegurar que en el diseño e implementación de sus sistemas de información se incorporen funcionalidades que faciliten la generación de datos abiertos. Así mismo, se deben automatizar los procesos de extracción de los sistemas de información fuente, para la generación y publicación de conjuntos de datos abiertos.	Conjunto de datos abiertos generados a partir de los procesos automatizados y de acuerdo con los criterios de calidad de la guía de apertura de datos de gobierno en línea.
LI.SIS.09	Interoperabilidad	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, debe desarrollar los mecanismos necesarios para compartir su información haciendo uso del Modelo de Interoperabilidad definido por el Estado a partir de las necesidades de intercambio de información con otras entidades.	Servicio habilitado y funcionando en la Plataforma de Interoperabilidad del Estado colombiano.
LI.SIS.10	Soporte a los Componentes de información	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, debe garantizar que los sistemas de información soporten la arquitectura y componentes de información establecidos por la entidad.	Matriz de correlación entre los componentes de información y los sistemas de información de la entidad.
LI.SIS.11	Accesibilidad	Los sistemas de información que estén	Plan de pruebas que



		disponibles para el acceso a la ciudadanía o aquellos que de acuerdo con la caracterización de usuarios lo requieran, deben cumplir con las funcionalidades de accesibilidad que indica la estrategia de Gobierno en Línea.	incorpore un criterio de aceptación para accesibilidad de acuerdo con la caracterización de usuarios realizada sobre el sistema.
LI.SIS.12	Ambientes independientes en el ciclo de vida de los sistemas de información	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe identificar y mantener la independencia de los ambientes requeridos durante el ciclo de vida de los sistemas de información, ya sea directamente o través de un tercero. Ejemplos de ambientes son: desarrollo, pruebas, capacitación, producción.	La entidad debe evidenciar la existencia, durante el ciclo de vida de los sistemas de información, de ambientes independientes y controlados.
LI.SIS.13	Análisis de requerimientos de los sistemas de información	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe incorporar un proceso formal de análisis y gestión de requerimientos de software en el ciclo de vida de los sistemas de información de manera que se garantice su trazabilidad y cumplimiento.	Dentro de la metodología de referencia de desarrollo de sistemas de información, dentro de la fase de gestión de requerimientos se define y detalla el proceso que contemple dentro de la gestión la identificación, levantamiento, análisis, validación y trazabilidad de los requerimientos.
LI.SIS.13	Integración continua durante el ciclo de vida de los sistemas de información	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe garantizar que, dentro del proceso de desarrollo de sistemas de información, se ejecuten estrategias de integración continua sobre los nuevos desarrollos de sistemas de información.	Dentro de las metodologías de referencia de desarrollo de sistemas de información y como parte del esquema de operación de ambientes dentro del ciclo de vida de los sistemas de información, se deben incluir actividades o procedimiento de integración continua.
LI.SIS.14	Plan de pruebas durante el ciclo de vida de los sistemas de información	En el proceso de desarrollo y evolución de un sistema de información, la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe contar con un plan de pruebas que cubra lo funcional y lo no funcional. La aceptación de cada una de las etapas de este plan debe estar vinculada a la transición del sistema de información a través de los diferentes ambientes.	Dentro de los planes de proyecto de desarrollo de sistemas de información se debe contar con planes de pruebas funcionales y no funcionales. Documentos, artefactos e informes que evidencien la aprobación de las pruebas por las partes involucradas.
LI.SIS.15	Plan de capacitación y entrenamiento para los sistemas de información	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe realizar constantemente capacitación y entrenamiento funcional y técnico a los usuarios, con el fin de fortalecer el uso y	Dentro de los planes de proyecto de desarrollo de sistemas de información se debe contar con planes de capacitación y entrenamiento.



		apropiación de los sistemas de información.	Los informes de la ejecución de los planes de capacitación y entrenamiento.
LI.SIS.16	Manual del usuario, técnico y de operación de los sistemas de información	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe asegurar que todos sus sistemas de información cuenten con la documentación técnica y funcional debidamente actualizada.	Dentro de las metodologías de referenciade desarrollo de sistemas de información y como parte del esquema de operación de ambientes dentro del ciclo de vida de los sistemas de información, se deben definir entregables del producto, la documentación de usuario, técnica y de operación necesaria para cada sistema de información.
LI.SIS.17	Gestión de cambios de los sistemas de información	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir e implementar formalmente un procedimiento de control de cambios para los sistemas de información de la institución.	Procedimiento documentado y formalizado de un proceso o procedimiento de gestión de cambios.
LI.SIS.18	Estrategia de mantenimiento de los sistemas de información	Para el mantenimiento de los sistemas de información, la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe hacer un análisis de impacto ante cualquier solicitud de cambio en alguno de sus componentes, con el fin de determinar la viabilidad del cambio y las acciones a seguir.	Procedimiento documentado y formalizado de un proceso o procedimiento de gestión de cambios.
LI.SIS.19	Servicios de mantenimiento de sistemas de información con terceras partes	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe establecer criterios de aceptación y definir Acuerdos de Nivel de Servicio (ANS) cuando se tenga contratado con terceros el mantenimiento de los sistemas de información. Los ANS se deben aplicar en las etapas del ciclo de vida de los sistemas de Información que así lo requieran y se debe velar por la continuidad del servicio.	Los ANS para la prestación del servicio de mantenimiento de los sistemas de información, que deben ser validados en conjunto al inicio del contrato y se define un periodo de transición para empezar a aplicar los mismos.
LI.SIS.20	Plan de calidad de los sistemas de información	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar un plan de aseguramiento de la calidad durante el ciclo de vida de los sistemas de información	Dentro de los planes de proyecto de desarrollo de sistemas de información se debe contar con planes de calidad. Estos planes deben estar en el repositorio documental del proyecto y ser validados y aprobados por el área de calidad de software o quien haga

			sus veces. En el repositorio se debe encontrar los documentos, artefactos e informes de la ejecución del plan de calidad.
LI.SIS.21	Criterios no funcionales y de calidad de los sistemas de información	En la construcción o modificación de los Sistemas de Información, la Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, debe identificar los requisitos no funcionales aplicables, garantizando su cumplimiento una vez entre en operación el sistema.	Documento de especificación de requerimientos funcionales y no funcionales (atributos de calidad).
LI.SIS.22	Seguridad y Privacidad de los sistemas de información	Durante todas las fases del ciclo de vida de los sistemas de información, la Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe analizar e incorporar aquellos componentes de seguridad y privacidad de la información que sean necesarios.	Implementación del Modelo de Seguridad y privacidad de la Información del MinTIC.

10.5.1 Arquitectura de sistemas de información

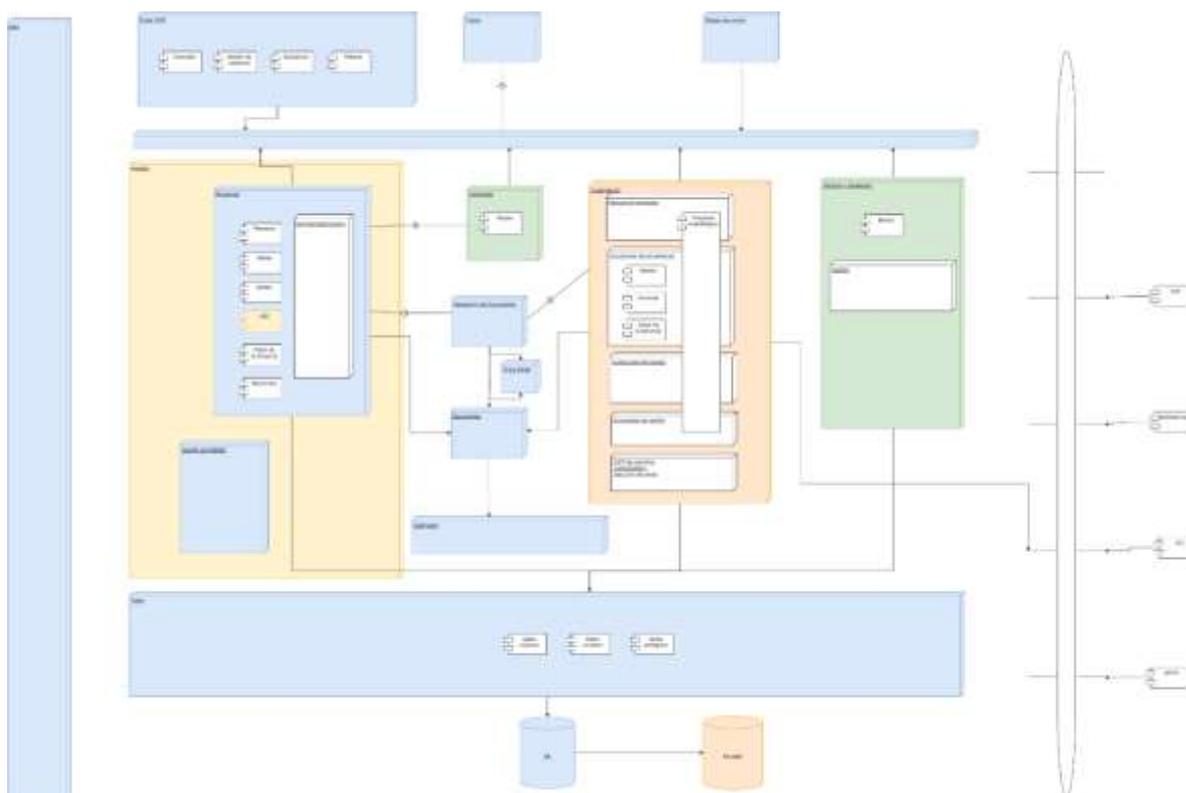
Sistemas de información de la Entidad

Respecto a la organización de Sistemas de información de la Entidad, se cuenta con diferentes sistemas de apoyo y un sistema misional que permitirá gestionar el proceso tanto de la Ley 522 como de la ley 1407. A continuación, se listan los diferentes Sistemas de Información:

Nombre Sistema	Descripción del sistema	Categoría	Tipo	Plataforma de aplicaciones	Oficina
Secretaria Fiscalía del Tribunal Superior	Se registra el ingreso de los recursos de segunda instancia para la Fiscalía	Administrativo	Cliente - Servidor	Access	Secretaria de la Fiscalía del Tribunal Superior
Secretaria Tribunal Superior	Se registra el ingreso de los recursos de segunda instancia	Administrativo	Cliente - Servidor	Oracle Forms	Secretaria del Tribunal Superior
ANTARES	Sistema de registro y consulta de providencias del Tribunal Superior Militar	Administrativo	Cliente - Servidor	Foxpro	Tribunal Superior

SIATH	Sistema de gestión de Talento Humano de la Entidad	Administrativo	Web con base de datos central	Oracle Forms	Talento Humano
PAOYER	Liquidación de la nómina	Administrativo	Web con base de datos central	Oracle Forms	Talento Humano
SAP	Ingresos de inventarios	Administrativo	Web con base de datos central	SAP	Área administrativa y financiera
Portal WEB	Gestión de contenidos para ofrecer información al ciudadano	Administrativo	Web con base de datos central	Drupal	OTIC
Service Manager	Mesa de servicios	Administrativo	Web con base de datos central	Service Manager	OTIC
Daruma	Sistema de calidad de la entidad	Administrativo	Web con base de datos central	PHP	Oficina de Planeación
Correspondencia	Sistema de gestión de correspondencia de la entidad	Administrativo	Web con base de datos central	Auraquantic	OTIC
SIJPMP	Sistema de gestión de casos de la JPMP para las leyes 522 y 1407	Misional	Web con base de datos central	Auraquantic	OTIC

Estos sistemas de información de la entidad se encuentran enmarcados en una distribución lógica que parte de diferentes módulos o componentes independientes que se integran mediante una capa de servicios a otros sistemas o incluso interactúan entre sí.



Integración de servicios externos

Se ha definido un punto de integración de servicios externos que se realizará mediante una VPN punto a punto y que tendrá un único origen en los servicios desplegados en la plataforma de AWS, de manera que se genere una correcta gestión y administración de integraciones teniendo el gobierno de estos centralizado.

Acceso a datos

Para el acceso a datos de los diferentes sistemas se ha establecido la caracterización de datos públicos, privados y reservados, de manera que se pueda administrar correctamente la publicación o restricción de esta.

Gestión de archivos o documentos

La arquitectura definida por la Entidad establece una gestión de archivos unificada, de manera que en un futuro pueda integrarse con un ECM sin tener que afectar de manera particular a los diferentes sistemas reduciendo el impacto de adaptación.

Firma digital

De la misma manera, la arquitectura permite el uso en un punto unificado del servicio de Firma Digital, sin importar el origen técnico de los documentos ya que, siempre que se encuentren dentro de la arquitectura institucional, permitirá el uso del módulo de firma.

AAA

Todos los movimientos y registros de acciones de los sistemas de la entidad contenidos dentro de la arquitectura cumplen con características de AAA específicas que permiten tener un seguimiento de ejecución de acciones mediante auditorías específicas respondiendo a solicitudes de gestión de información.

10.5.2 Implementación de sistemas de información

La entidad cuenta con dos líneas diferentes de necesidades, la primera de ellas está relacionada con objetivos específicos que no se encuentran en el mercado y la segunda con soluciones que se alinean con necesidades generales.

Respecto a las necesidades, se define un proceso basado en la metodología SCRUM, de manera que tenemos un alcance anual proyectado con necesidades a cumplir con un nivel de documentación general que permite tener una estimación preliminar. El documento que define estas necesidades se denomina “Product Backlog”.

En cada ciclo de SCRUM (Sprint) proyectado a 2 semanas se toma un grupo de estas necesidades y se documentan en un “Sprint Backlog”. A partir de dicho artefacto, se inicia el proceso de implementación con las siguientes actividades:

1. Análisis de las necesidades: Al inicio del Sprint se realiza un análisis preliminar de las necesidades asignando a los desarrolladores las necesidades. Estos desarrolladores tendrán comunicación directa y constante con los usuarios funcionales permitiendo avanzar rápidamente y sin contratiempos en el desarrollo de la solución
2. Implementación: Una vez analizada la necesidad se iniciará el proceso de desarrollo donde estarán involucrados tanto el desarrollador como el diseñador como el usuario funcional dando solución a la necesidad y validando constantemente con el usuario funcional los desarrollos
3. Despliegue en entorno de pruebas: Finalizando el Sprint se realiza un despliegue en ambiente de pruebas para que el usuario funcional pueda realizar las pruebas de validación, al mismo tiempo que el equipo técnico realiza las pruebas de carga, estrés y de regresión confirmando que ningún artefacto previo sea afectado por los nuevos desarrollos. En caso de surgir algún incidente se deberá evaluar si se soluciona en el sprint actual o, de ser necesario, se asignará el incidente para el siguiente sprint permitiendo desplegar los demás desarrollos sin afectar el alcance total.
4. Despliegue en producción: La última tarea de cada sprint es el despliegue en producción de las soluciones realizadas que hayan sido validadas tanto por los usuarios funcionales como por el equipo técnico.

10.5.3 Servicios de soporte técnico

N.	ACTIVIDAD Y DESCRIPCIÓN	RESPONSABLE	REGISTRO
1	<p>Emitir la solicitud de software</p> <p>El líder funcional de la dependencia que requiere el ajuste, creación o modificación del Sistema de Información realiza el requerimiento por medio del formato solicitud de requerimientos; en caso de recibir solicitudes por medio de correo electrónico y oficio, el servidor responsable devolverá esta solicitud exigiendo el diligenciamiento del formato diseñado para este fin.</p>	Líder de proceso / funcional	Formato de solicitud de requerimientos.
2	<p>Recibir y Clasificar la solicitud</p> <p>El funcionario responsable del departamento de Sistemas de Información recibe y clasifica el requerimiento validando la viabilidad de este.</p> <p>Nota 1: En caso de que el requerimiento no sea viable el responsable informará a través del formato de solicitud de requerimientos con el concepto de viabilidad al líder funcional el motivo por el cual la solicitud no podrá ser atendido.</p> <p>Nota 2: En caso de que el requerimiento consista en la creación de un sistema nuevo o la modificación de uno existente que afecte la arquitectura institucional, se informará al líder funcional que se requiere aprobación por parte del comité de arquitectura institucional.</p> <p>Nota 3: Si el requerimiento es viable el responsable realiza la clasificación y priorización de acuerdo con los parámetros establecidos por la Oficina de Tecnologías de la Información y las Comunicaciones se asigna al líder técnico responsable el cual ejecutará la actividad.</p>	Servidor responsable del Grupo de Sistemas de Información de la Oficina TIC	Formato de solicitud de requerimientos, correo electrónico
3	<p>Diseñar y enviar requerimiento para aprobación</p> <p>El analista técnico realiza el análisis del requerimiento diligenciando el formato de especificación de requerimientos y diseña el sistema diligenciando el formato diseño de la solución, en los cuales se detalla técnicamente el desarrollo de la solicitud.</p> <p>Si la solicitud corresponde a la implementación de un proceso automatizado se diligencia el formato de especificación de procesos automatizados y si la solicitud corresponde a la implementación de webservices para el intercambio</p>	Analista técnico la oficina de tecnologías de la Información	Formato de especificación de requerimientos Formato diseño de la solución. Formato de especificación de procesos



	<p>de información se diligencia el formato de especificación de webservices. Dichos formatos serán enviados al comité de aprobación.</p> <p>Nota: El comité de aprobación está conformado por el Líder funcional, Coordinador del grupo de sistemas de información</p>		<p>automatizados.</p> <p>Formato de especificación de webservices</p>
4	<p>Aprobación del diseño del requerimiento</p> <p>El comité de aprobación en mesa de trabajo revisa y determina si aprueba o no el diseño del requerimiento.</p> <p>Nota 1: Si el diseño no es aprobado se devuelve al analista técnico para que haga los ajustes solicitados por el comité mediante el Formato de especificación de requerimientos.</p> <p>Nota 2: Si el diseño es aprobado este será remitido al arquitecto de soluciones para que se defina la arquitectura tecnológica de la solución.</p>	Comité de aprobación	Formato de especificación de requerimientos
5	<p>Verificación de la arquitectura de solución</p> <p>El departamento de ARQUITECTURA DE TI define la arquitectura tecnológica de la solución con las siguientes opciones:</p> <ol style="list-style-type: none"> Define los componentes para los nuevos sistemas de información. Convalida la arquitectura sobre la cual se encuentra dispuesta las soluciones tecnológicas actuales. Define nuevos componentes tecnológicos para que interactúen con las soluciones existentes. 	Servidor responsable del departamento de arquitectura de TI	Documento de arquitectura de solución
6	<p>Mantenimiento, actualización o creación del sistema de información</p> <p>Se realizan las tareas de configuración de bases de datos, escritura de códigos, diseños de reportes, pruebas técnicas, aseguramiento de código fuente y otras requeridas para atender la necesidad detallada en el requerimiento.</p>	Funcionario responsable del equipo de desarrollo	Repositorio de código fuente de las aplicaciones
7	<p>Preparar documentación y requisitos para el despliegue</p> <p>Se organiza el paquete que contiene la nueva versión de producto de software en el cual se incluyen los programas compilados, imágenes, scripts de bases de datos y se diligencia el formato de despliegue. Para el caso de implementación de webservices se requiere diligenciar el formato guía de consumo de webservices.</p>	Funcionario responsable del equipo de desarrollo	<p>Formato de despliegue</p> <p>Formato guía de consumo web services</p> <p>Manual Técnico</p>



	Adicionalmente se elabora el manual técnico en caso de requerirse.		
8	<p>Ejecutar despliegue ambiente de pruebas</p> <p>El responsable del grupo de infraestructura ejecuta las instrucciones entregadas en el formato de despliegue en el ambiente de pruebas y el sistema de información que se está creando o modificando y le informa al “tester” para que el inicie el plan de pruebas.</p>	Servidor encargado en el Grupo de Infraestructura	Sistema en ambiente de pruebas
9	<p>Diseñar el plan de pruebas y validar el sistema de información actualizando el plan de pruebas.</p> <p>El tester diseña el plan por medio del cual valida el sistema de información que se está creando o modificando y actualiza el plan de acuerdo con los resultados obtenidos</p> <p>Nota1: Si el producto entregado no cumple con la necesidad o presenta fallas se informa al equipo de desarrollo y se devuelve a la actividad No 6</p> <p>Nota 2: Si el software cumple con la necesidad, se aprueba y se informa al área funcional para que inicie las pruebas funcionales.</p>	Funcionario de pruebas del equipo de desarrollo	Formato plan de pruebas
10	<p>Realizar pruebas funcionales y validar</p> <p>El servidor responsable (líder funcional) ejecuta el plan de pruebas validando que cumpla con lo diseñado en la especificación de requerimientos.</p> <p>Nota1: Si el producto entregado no cumple con la necesidad o presenta fallas se informa al equipo de desarrollo y se devuelve a la actividad No 6</p> <p>Nota 2: Si el software cumple con la necesidad se aprueba y se informa al líder técnico para que inicie el despliegue en producción.</p>	Área o líder funcional	Formato plan de pruebas
11	<p>Revisar requisitos para el despliegue en producción</p> <p>El analista técnico de la OTIC revisa los requisitos e inicia el despliegue en producción solicitado por el área funcional.</p> <p>Se solicita al comité técnico la aprobación para el paso a producción, enviando el formato de aprobación paso a producción.</p>	Analista técnico y comité de aprobación	Formato aprobación paso a producción
12	<p>Revisar requisitos para el paso a producción</p> <p>El comité técnico revisa que se cumplan todos los requisitos de la lista de chequeo para el paso a producción.</p>	Servidores responsables del comité técnico.	Formato aprobación paso a producción



	<p>Nota 1: Si el comité no aprueba el paso a producción se devuelve al analista técnico para que complete o ajuste los requisitos necesarios para el despliegue.</p> <p>Nota 2: Si el paso a producción requiere ventana de mantenimiento, se define la fecha y la duración de la ventana de mantenimiento y se comunica la aprobación del paso a producción.</p> <p>Nota 3: Si el paso a producción no requiere ventana de mantenimiento se comunica el paso a producción.</p>		
13	<p>Anunciar ventana de mantenimiento</p> <p>El funcionario responsable del departamento de infraestructura recibe la aprobación del despliegue y la información para anunciar a los usuarios la ventana de mantenimiento.</p>	El funcionario responsable del departamento de infraestructura	Correo electrónico
14	<p>Ejecutar despliegue ambiente de producción</p> <p>El departamento de infraestructura realiza el despliegue en ambiente de producción del sistema de información</p> <p>Nota 1: si el despliegue es exitoso se anuncia la puesta en marcha del sistema y la finalización de la ventana de mantenimiento.</p> <p>Nota 2: en caso de presentar fallas durante la ejecución se ejecuta el RollBack descrito en el formato de despliegue y notifica los errores encontrados al grupo de desarrollo y se regresa a la actividad No 7 para realizar los ajustes necesarios.</p>	Funcionarios responsables del departamento de infraestructura	Formato de despliegue

10.6 Modelo de gestión de servicios tecnológicos

Este dominio permite gestionar con mayor eficacia y transparencia la infraestructura tecnológica que soporta los sistemas y servicios de información en las instituciones.

ID	NOMBRE	LINEAMIENTO	EVIDENCIA
LI.ST.01	Directorio de servicios tecnológicos	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe contar con un directorio actualizado de sus Servicios Tecnológicos, que le sirva de	Directorio de servicios tecnológicos



		insumo para administrar, analizar y mejorar los activos de TI.	
LI.ST.02	Elementos para el intercambio de información	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe incluir dentro de su arquitectura de Servicios tecnológicos los elementos necesarios para poder realizar el intercambio de información entre las áreas de la institución y las organizaciones externas a escala sectorial y nacional.	Diagramas arquitectónicos que representen los elementos de infraestructura involucrados en el intercambio de información al interior de la entidad y con sistemas externos.
LI.ST.03	Gestión de los Servicios tecnológicos	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, debe gestionar la operación y el soporte de los servicios tecnológicos, en particular, durante la implementación y paso a producción de los proyectos de TI, se debe garantizar la estabilidad de la operación de TI y responder acorde al plan de capacidad.	Políticas de despliegue de proyectos de TI o servicios tecnológicos, encaminadas a garantizar la estabilidad de la operación
LI.ST.04	Acceso a servicios en la Nube	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe evaluar como primera opción la posibilidad de prestar o adquirir los Servicios Tecnológicos haciendo uso de la Nube (pública, privada o híbrida), para atender las necesidades de los grupos de interés.	Análisis de operación de los servicios tecnológicos contemplando escenarios con servicios en la nube.
LI.ST.16	Disposición de residuos tecnológicos	La institución debe implementar un programa de correcta disposición final de los residuos tecnológicos, teniendo en cuenta los lineamientos técnicos con los que cuente el gobierno nacional.	"Procedimiento de disposición de residuos tecnológicos. Evidencias de cumplimiento del procedimiento.
LI.ST.05	Continuidad y disponibilidad de los Servicios tecnológicos	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe garantizar la continuidad y disponibilidad de los servicios Tecnológicos, así como la capacidad de atención y resolución de	"Planes, procedimientos y políticas para garantizar la continuidad de los servicios tecnológicos. Sistemas de respaldo y controles implementados para



		incidentes para ofrecer continuidad de la operación y la prestación de todos los servicios de la entidad y de TI.	garantizar la continuidad de los servicios tecnológicos.
LI.ST.06	Alta disponibilidad de los Servicios tecnológicos	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar capacidades de alta disponibilidad para las infraestructuras críticas y los Servicios Tecnológicos que afecten la continuidad del servicio de la institución, las cuales deben ser puestas a prueba periódicamente.	Documentación del mecanismo implementado para la garantizar la disponibilidad de los servicios tecnológicos.
LI.ST.07	Capacidad de los Servicios tecnológicos	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe velar por la prestación de los servicios de TI, identificando las capacidades actuales de los Servicios Tecnológicos y proyectando las capacidades futuras requeridas para un óptimo funcionamiento.	"Plan de capacidad de los servicios tecnológicos. Sistema de monitoreo de capacidad de los servicios tecnológicos."
LI.ST.08	Acuerdos de Nivel de Servicios	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe velar por el cumplimiento de los Acuerdos de Nivel de Servicio (ANS) establecido los Servicios Tecnológicos.	"Acuerdo de Niveles de Servicio definidos con cada uno de los operadores. Reportes de medición de los ANS con la
LI.ST.09	Soporte a los servicios tecnológicos	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir e implementar el procedimiento para atender los requerimientos de soporte de primer, segundo y tercer nivel, para sus servicios de TI, a través de un único punto de contacto como puede ser una mesa de servicio.	"Procedimientos de atención de requerimientos de soporte para los servicios de TI o Modelo Operativo de la Mesa de Servicio"
LI.ST.10	Planes de mantenimiento	La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar un plan de mantenimiento preventivo y evolutivo sobre toda la infraestructura y demás Servicios Tecnológicos de la institución.	"Plan de mantenimiento preventivo de la infraestructura y los Servicios Tecnológicos. Informes de mantenimientos realizados."



LI.ST.11	Control de consumo de los recursos compartidos por Servicio tecnológicos	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe identificar, monitorear y controlar el nivel de consumo de los recursos críticos que son compartidos por los Servicios Tecnológicos y administrar su disponibilidad.	"Mecanismo de monitoreo de consumo de los recursos compartidos de los servicios tecnológicos. Reportes de consumo de recursos tecnológicos críticos. Definición de umbrales y generación de alertas."
LI.ST.12	Gestión preventiva de los Servicio tecnológicos	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe asegurarse de que la infraestructura y demás recursos tecnológicos de la institución cuenten con mecanismos de monitoreo para generar alertas tempranas ligadas a los umbrales de operación que tenga definidos.	"Sistemas de monitoreo de recursos tecnológicos con alertas configuradas. Definición de umbrales y generación de alertas."
LI.ST.13	Respaldo y recuperación de los Servicios tecnológicos	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe contar con mecanismos de respaldo para los servicios tecnológicos críticos de la entidad, así como con un proceso periódico de respaldo de la configuración y de la información almacenada en la infraestructura tecnológica, incluyendo la información clave de las estaciones de trabajo de los funcionarios de la entidad. Este proceso debe ser probado periódicamente y debe permitir la recuperación íntegra de los Servicios Tecnológicos.	"Políticas de respaldo y copias de seguridad. Informes/actas satisfactorias de simulacros realizados sobre restauración de respaldos y copias de seguridad"
LI.ST.14	Análisis de riesgos	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe realizar el análisis y gestión de los riesgos asociados a su infraestructura tecnológica haciendo énfasis en aquellos que puedan comprometer la seguridad de la información o que puedan afectar la prestación de un	"Plan de pruebas de seguridad de la información. Matriz de riesgos de seguridad de la información. Informes de análisis de vulnerabilidades realizados. "

		servicio de TI.	
LI.ST. 15	Seguridad informática	La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar controles de seguridad informática para gestionar los riesgos que atenten contra la disponibilidad, integridad y confidencialidad de la información.	"Inventario de servicios tecnológicos detallando los controles de seguridad informática asociados al acceso, trazabilidad, modificación o pérdida de información Matriz de riesgos que analice aspectos que atenten contra la disponibilidad, integridad y confidencialidad de la información y proponga los controles necesarios." "

10.6.1 Criterios de calidad y procesos de gestión de servicios de TI

Los criterios de calidad se definirán de acuerdo con marco de mejores prácticas de gestión como ITIL y teniendo en cuenta los criterios que defina la oficina de Planeación.

10.6.2 Infraestructura

Se utilizarán mecanismos de monitoreo de consumo de los recursos como memoria, procesador y disco de los activos tecnológicos de forma trimestral, con el fin de verificar la adecuada capacidad de estos.

10.6.3 Conectividad

Los servicios de conectividad se controlarán con los niveles de disponibilidad de estos a nivel de conectividad, pérdida de paquetes, y caídas durante el trimestre.

10.6.4 Servicios de operación

Los servicios de operación se controlarán con los niveles de disponibilidad de estos, expresados en el tiempo disponible sobre el tiempo total durante el trimestre.

10.6.5 Mesa de servicios

La mesa de ayuda se orientará a las mejores prácticas de ITIL, para ello se medirá inicialmente con el nivel de solicitudes atendidas en los tiempos acordados sobre el total de solicitudes registradas en el mes.

10.6.6 Procedimientos de gestión

Se definirá los procedimientos de la mesa de servicios y de la gestión de incidentes, teniendo en cuenta las recomendaciones que expida la oficina de Planeación.

10.7 Uso y apropiación

Dentro de la estrategia de transformación digital se tiene previsto el ejercicio de uso y apropiación de las herramientas y capacidades adquiridas por la Entidad y se busca, por lo tanto, fortalecer la operación y trabajo de las áreas misionales.

Atributo	Descripción
Grupo de interés	Funcionarios de las áreas operativas
Descripción	Funcionarios, Magistrados, Jueces, Fiscales, secretarios y Policía Judicial de JPMP
Objetivo	Apropiación de la herramienta tecnológica de gestión de los casos penales
Rol de involucramiento	Oficina TIC – Patrocinador Áreas Misionales - Impactado Empresa contratista – Agente de cambio

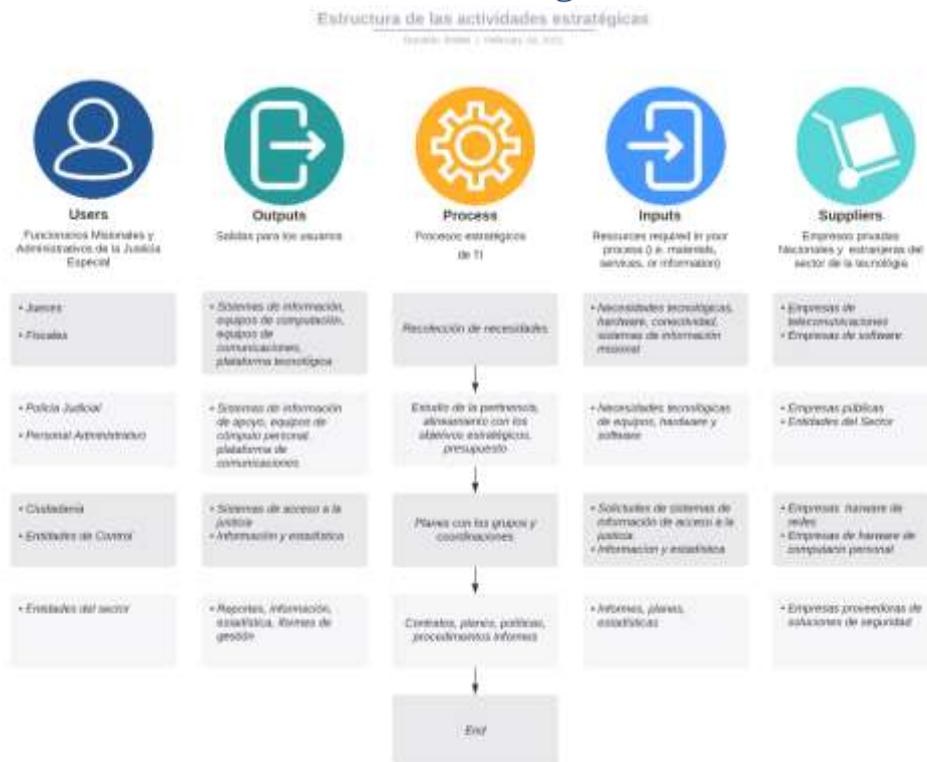
11 MODELO DE PLANEACIÓN

11.1 Lineamientos y/o principios que rigen el plan estratégico de TI

Los planes de Tecnologías de la Información y las Comunicaciones, consignados en el presente documento se rigen por los principios de planeación, pertinencia y alineación con los objetivos estratégicos de la entidad. La planeación se inicia con el conocimiento de la entidad y las necesidades que han sido manifiestas expresamente por los usuarios de la JPMP a través de encuestas, en donde se les consulta sobre que necesidades tiene la entidad en materia de tecnologías de la información y las comunicaciones TIC o a través de necesidades presentadas formalmente a la OTIC o por medio de observación de los procesos misionales y administrativos, posteriormente se planean los frentes de acción asociados a los grupos que constituyen la oficina y se plantean acciones pertinentes y orientadas a cumplir con las necesidades observadas en los ejercicios de consulta con los usuarios y que estén alineados con la estrategia institucional. Estas acciones y estrategias se ven plasmadas en el plan de contratación de la UASJPMP.



11.2 Estructura de actividades estratégicas



11.3 Plan maestro o Mapa de Ruta

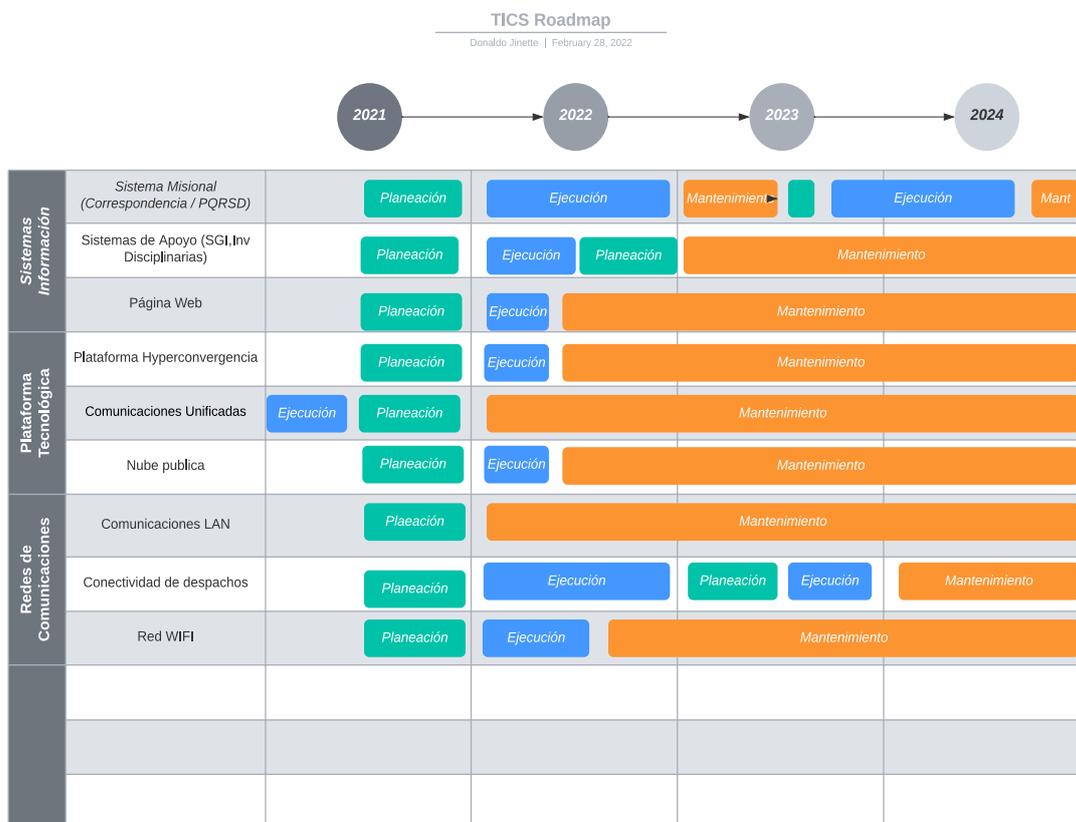


Ilustración 35 Plan Maestro - Hoja de ruta

11.3.1 Definición de indicadores

Se han definido para el proceso de T.I, el siguiente grupo de indicadores de proceso.

Objetivo Estratégico	Responsable	Entregable	Plan de Acción UAE/JMPP - 2022		Nombre del Indicador	Estado de avance 2022												% de Ejecución				
			Ponderación actividades	Actividad		Planeado (P)/Ejecutado (E)	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov		Dic			
Implementar sistemas de información que apoyen la gestión y la toma de decisiones de la Justicia Penal Militar y Policial, sobre una plataforma tecnológica moderna, que permita obtener la información oportuna, veraz y confiable de los procesos de la entidad.	Coordinador del grupo de sistemas de información	Software sistema de información Misional	30%	Definición de requisitos del modelo del proceso de gestión de casos penales de ley 522/1999 y 1407 del 2010	Actividades ejecutadas / Actividades programadas * 100	P			25%				50%			75%			100%			
			40%	Construcción de los artefactos de software para la gestión de los casos penales de ley 522/1999 y 1407 del 2010																		
			30%	Pruebas de funcionamiento del sistema de información e interacciones con otros sistemas de información internos y externos		E																
	Director Escuela	Plan de divulgación y soportes de asistencia	100%	100%	Divulgación del uso y apropiación de la herramienta	Numero de personal capacitado / Total de personal de los despachos	P							50%						100%		
							E															
	Coordinador del grupo de sistemas de información	Sistema de Información Gestión de calidad	30%	30%	Definición de requisitos del sistema de gestión de calidad	Actividades ejecutadas / Actividades programadas * 100	P			25%				50%			75%			100%		
							E															
							40%	Implementación de la herramienta														
	Director Escuela	planillas de asistencia a capacitaciones	100%	100%	Divulgación del uso y apropiación de la herramienta	Numero de personal capacitado / Total de personal de los despachos	P							50%						100%		
							E															
	Coordinador del grupo de sistemas de información	Pagina Web de la UAE JMPP	100%	100%	Diseño, parametrización e instalación de la página web	Actividades ejecutadas / Actividades programadas * 100	P	20%	40%	60%	80%	90%	100%									
							E															
	Coordinador del grupo de sistemas de información	Sistema de información para la gestión de PQRSD	100%	100%	Definición de requisitos del sistema de gestión de PQRSD	Actividades ejecutadas / Actividades programadas * 100	P		25%					50%			75%			100%		
							E															
							30%	Configuración y parametrización de la herramienta														
	Personal capacitado	100%	100%	100%	Divulgación del uso y apropiación de la herramienta	Numero de personal capacitado / Total de personal de los despachos	P							50%						100%		
							E															
	Coordinador del grupo de redes y comunicaciones	Infraestructura tecnológica actualizada	50%	50%	Plan Modernización de plataforma tecnológica	Actividades ejecutadas / Actividades programadas * 100	P		25%					50%			75%			100%		
							E															
		Informe de solicitudes cerradas	100%	100%	100%	Soporte mesa de ayuda	Solicitudes atendidas / total Solicitudes	P			80%				82%			85%			87%	
E																						
Coordinador del grupo de plataforma tecnológica	Despachos con redes modernizadas	50%	50%	Modernización de plataforma tecnológica (Centro de datos)	Actividades ejecutadas / Actividades programadas * 100	P			50%				100%									
						E																
Equipos PC renovados	50%	50%	50%	Adquisición de equipos de computo	modernización de PC fiscales y jueces / Total de jueces y fiscales	P			50%				100%									
						E																

Los cuales se calculan con la siguiente formulación:

$$\frac{\text{Actividades Ejecutadas}}{\text{Actividades Planeadas}} \times 100$$

$$\frac{\text{Numero de Personal Capacitado}}{\text{Total del personal de los despachos}} \times 100$$

$$\frac{\text{Actividades Ejecutadas}}{\text{Actividades Planeadas}} \times 100$$

$$\frac{\text{Solicitudes Atendidas}}{\text{Total de las solicitudes}} \times 100$$

$$\frac{\text{Numero de puntos instalados}}{\text{Puntos programados}} \times 100$$

$$\frac{\text{Modernizacion de PCs Fiscales y Jueces}}{\text{Total de jueces y fiscales}} \times 100$$

11.4 Proyección de presupuesto área TI

Para la vigencia 2022 la OTIC tiene en su plan anual de adquisiciones los siguientes proyectos

Objeto	Responsable	Fecha inicio	Fecha Final	Total, Plan de Compras 2022
Suscripción certificados digitales servicios TI	Tecnología	01/03/2022	30/03/2022	\$ 5.000.000,00
Adecuación centro de datos JPMP	Tecnología	01/04/2022	30/09/2022	\$ 100.000.000,00
Plataforma de Almacenamiento NetApp	Tecnología	01/08/2022	31/07/2023	\$ 198.488.632,94
Actualización NOC - licencias SolarWinds	Tecnología	01/08/2022	31/07/2023	\$ 68.713.200,00
Soporte horas Microsoft	Tecnología	01/08/2022	31/07/2023	\$ 307.951.131,28
Adición de elementos de conectividad para la red WAN de los despachos de la JPMP	Tecnología	01/07/2021	31/11/2022	\$ 1.250.215.012,50
Red LAN: ampliación de garantías de hardware, actualización de software, soporte de fábrica y asistencia técnica	Tecnología	01/08/2022	15/11/2023	\$ 91.885.920,00
Adquisición de elementos para la Red Wifi JPMP	Tecnología	01/08/2021	15/12/2021	\$ 96.165.342,00
Canal internet y datos, incluye traslado	Tecnología	01/08/2022	31/07/2023	\$ 66.466.185,50



Adquisición computadores para los despachos de la JPMP	Tecnología	01/07/2022	31/11/2022	\$ 1.730.000.000,00
Migración de McAfee a la versión Emvisión	Tecnología	01/10/2022	31/12/2022	\$ 178.207.491,25
Infraestructura en nube pública para los sistemas de información misionales de la JPMYP - 2021 (Dev - julio 2021 - marzo de 2022)	Tecnología	01/10/2022	30/09/2023	\$ 63.846.597,42
Sistema de Información para la JPMP	Tecnología	01/10/2022	31/07/2023	\$ 2.300.000.000,00
Adquisición de un software para el sistema de gestión de calidad	Tecnología	01/11/2022	31/12/2022	\$ 26.742.575,18
Adquisición de Firmas Digitales	Tecnología	01/03/2022	30/03/2022	\$ 25.000.000,00
Integración firma digital	Tecnología	01/03/2022	30/03/2022	\$ 150.000.000,00
Renovación de derechos, Actualización de software incluido soporte y asistencia del Firewall Fortinet	Tecnología	01/12/2021	31/12/2023	\$ 394.149.999,92
Suscripción de Windows Server office 365	Tecnología	31/12/2022	31/12/2023	\$ 1.300.000.000,00
Mesa de servicios	Tecnología	01/12/2022	30/11/2023	\$ 1.047.019.882,27
Servicio internet móvil	Logística	12/11/2022	31/10/2022	\$ 155.505.649,83
Total				\$9.555.357.620,09

11.5 Plan de intervención de sistemas de información

La carencia de sistemas de información en el ejercicio de la Justicia Especial presenta un reto para la OTIC, de una parte la aplicación de la ley 522 llevada a través de documentos físicos y las complejidades del tratamiento de los casos de una ley que lleva más de 20 años de ejercicio, deben ser plasmadas en un proceso digital que controle sus variables, estados y controle la seguridad de la información a lo largo de los pasos y los actores involucrados en el ejercicio de justicia, además estos sistemas de información deben controlar la aplicación de la ley 1407 para el control de la aplicación del sistema Penal Oral Acusatorio con las complejidades del control de las audiencias y la seguridad documental, notificaciones y firma digital de documentos.

El plan de intervención de los sistemas de información de la UAESJPM inicia con los procesos misionales de las leyes mencionadas, sus procesos administrativos de apoyo circundante, proceso general de correspondencia y

Oficina de Tecnologías de la Información y las Comunicaciones – Unidad Administrativa Especial de la Justicia Penal Militar y Policial

Carrera 46 No. 20 C – 1 Cantón Militar Occidental “coronel Francisco José de Caldas”,

Palacio de la Justicia Penal Militar y Policial “TF. Laura Rocío Prieto Forero”, Bogotá,

www.justiciamilitar.gov.co

Conmutador: (57 1) 3150111

proceso de PQRS, conformando un núcleo de negocio operativo, funcional que soporta las operaciones principales de la misionalidad institucional. Posteriormente en las siguientes fases de intervención se intervendrán los demás procesos de apoyo de una forma integrada que soporte la operación integral de la entidad de forma controlada, garantizando los principios de integridad, confidencialidad y disponibilidad de la información.

Estos procesos entre otros incluyen, procesos de gestión disciplinaria, proceso de gestión contractual, proceso de gestión financiera y procesos jurídicos.

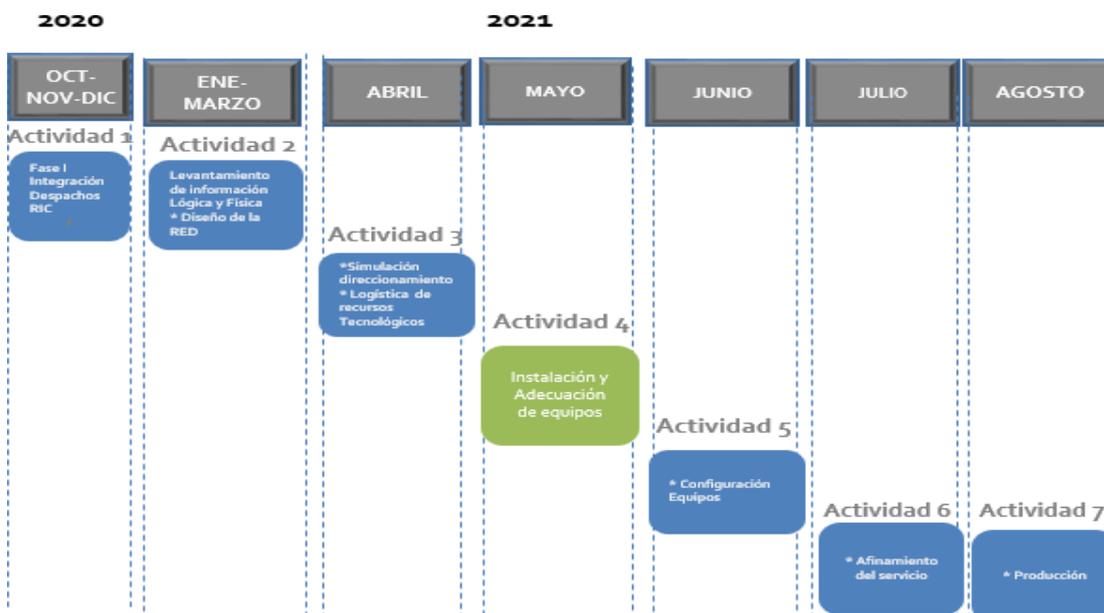
11.6 Plan de proyectos de servicios tecnológicos

A continuación, se describe el plan de proyectos de servicios tecnológicos

11.6.1 Conectividad y servicios de comunicaciones a nivel nacional de las sedes de la Justicia Penal Militar y Policial

El proyecto busca fortalecer las capacidades de servicios de comunicaciones unificadas, tanto en las sedes centrales y administrativas, en una nube híbrida que permita el acceso móvil y local a dichos servicios como portales, archivos, herramientas de trabajo, mensajería, de difusión, videoconferencia, programación de trabajo en equipo virtuales y remotos desde cualquier lugar de forma segura

Objeto	Se requiere de servicios de comunicaciones unificadas tanto en las sedes centrales y administrativas en una nube híbrida que permita el acceso móvil y local a dichos servicios como portales, archivos, herramientas de trabajo, mensajería, de difusión, videoconferencia, programación de trabajo en equipo virtuales y remotos desde cualquier lugar de forma segura.		
Tipo de Proyecto	Nuevo	Horizonte del Proyecto	2020-2021
Presupuesto Total	\$5.504.000.000,00	Presupuesto Total TIC	\$5.504.000.000,00
Vigencia a aprobar	2020 - 2021	Presupuesto TIC para la vigencia a aprobar	\$5.504.000.000,00
Fuente de Recursos	Propios	Código BPIN	No Aplica
Dependencia Líder	Dirección Ejecutiva de la Justicia Penal Militar	Gerente de Proyecto	Fabio Espitia Garzón Director Ejecutivo de la Justicia Penal Militar



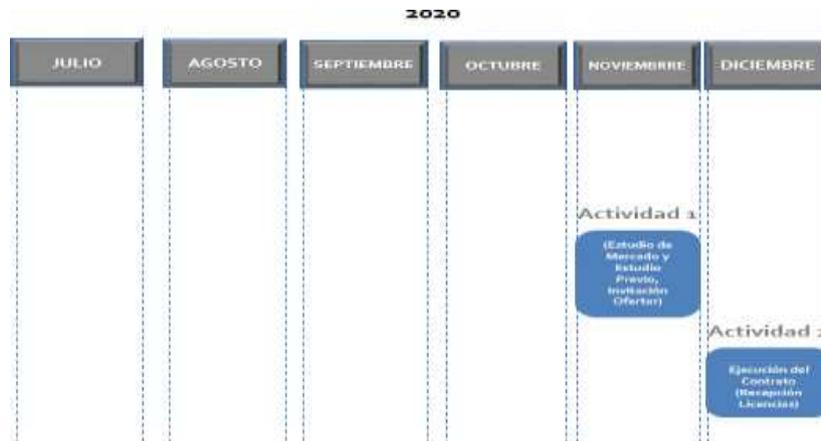
Descripción	Cantidad	Precio Total	Número de la Actividad
HARDWARE			
Switches-Routers	104	4.553.000.000,00	
Wifi (Access point)	14	42.000.000,00	
Concentradores	2	50.000.000,00	
SOFTWARE			
Comunicación Unificada en la nube	350	504.000.000,00	
SERVICIO			
Capacitación (uso de herramientas unificadas a los funcionarios del Despacho)	350	355.000.000,00	
TOTAL		\$5.504.000.000,00	

11.6.2 Sistema de Información

El proyecto busca, en el marco del fortalecimiento de la Justicia Penal Militar y de Policía, desarrollar e implementar un Sistema de información que coadyuve bajo los principios de transparencia, eficiencia y agilidad en cada uno de las investigaciones penales adelantadas por esta jurisdicción, en este sentido el sistema de información deberá sistematizar las etapas de los procesos enmarcados en la Ley 522 de 1999 (Instrucción, Calificación y Juicio) y la ley 1407 de 2010 (Indagación e Investigación y Juicio).



Objeto	Con la contratación de la renovación del licenciamiento de Server Microsoft, tiene como objetivo de contar con la plataforma actualizada y funcional para los usuarios de la Justicia Penal Militar y Policial.		
Tipo de Proyecto	Nuevo	Horizonte del Proyecto	2020
Presupuesto Total	\$1.300.000.000,00	Presupuesto Total TIC	\$1.300.000.000,00
Vigencia a aprobar	2020	Presupuesto TIC para la vigencia a aprobar	\$1.300.000.000,00
Fuente de Recursos	Propios	Código BPIN	No Aplica
Dependencia Lider	Dirección Ejecutiva de la Justicia Penal Militar	Gerente de Proyecto	Fabio Espitia Garzón Director Ejecutivo de la Justicia Penal Militar



Descripción	Cantidad	Precio Total	Número de la Actividad
SOFTWARE			
Microsoft@Windows@ServerCAL License/ <u>SoftwareAssurancePack</u> Government OLP 1License NoLevel UsrCAL	1200	305.526.312,00	
Microsoft@ExchangeServerEnterprise License/ <u>SoftwareAssurancePack</u> Government OLP 1License NoLevel	4	113.635.998,84	
Microsoft@ExchangeEnterpriseCAL License/ <u>SoftwareAssurancePack</u> Government OLP 1License NoLevel UsrCAL WithoutServices	1200	446.259.996,00	
Microsoft@SysCtrDataCenterCore License/ <u>SoftwareAssurancePack</u> Government OLP 2Licenses NoLevel CoreLic Qualified	30	63.072.582,30	
Microsoft@SysCtrConfigMgrClitMgmtLic License/ <u>SoftwareAssurancePack</u> Government OLP 1License NoLevel PerUsr	700	258.888.903,00	
Microsoft@SysCtrServiceMgrClitMgmtLic License/ <u>SoftwareAssurancePack</u> Government OLP 1License NoLevel PerUsr	700	112.616.207,86	
TOTAL		\$1.300.000.000,00	

11.6.4 Prestación del servicio de horas proactivas y reactivas, configuración, parametrización y capacitación de productos MICROSOFT II

La finalidad del proyecto corresponde a la contratación de prestación de servicios de horas proactivas y reactivas configuración, parametrización y capacitación productos Microsoft II, con la seguridad, optimización y detección de anomalías y estabilidad de la plataforma monitoreando la disponibilidad para la gestión de los requerimientos de la Dirección Ejecutiva de la Justicia Penal Militar y Policial

Objeto	Se requiere la contratación de prestación de servicios de horas proactivas y reactivas configuración, parametrización y capacitación productos Microsoft, con la seguridad, optimización y detección de anomalías y estabilidad de la plataforma.		
Tipo de Proyecto	Nuevo	Horizonte del Proyecto	2020 - 2021
Presupuesto Total	\$240.000.000,00	Presupuesto Total TIC	\$240.000.000,00
Vigencia a aprobar	2020 -2021	Presupuesto TIC para la vigencia a aprobar	\$240.000.000,00
Fuente de Recursos	Propios	Código BPIN	No Aplica
Dependencia Lider	Dirección Ejecutiva de la Justicia Penal Militar	Gerente de Proyecto	Fabio Espitia Garzón Director Ejecutivo de la Justicia Penal Militar

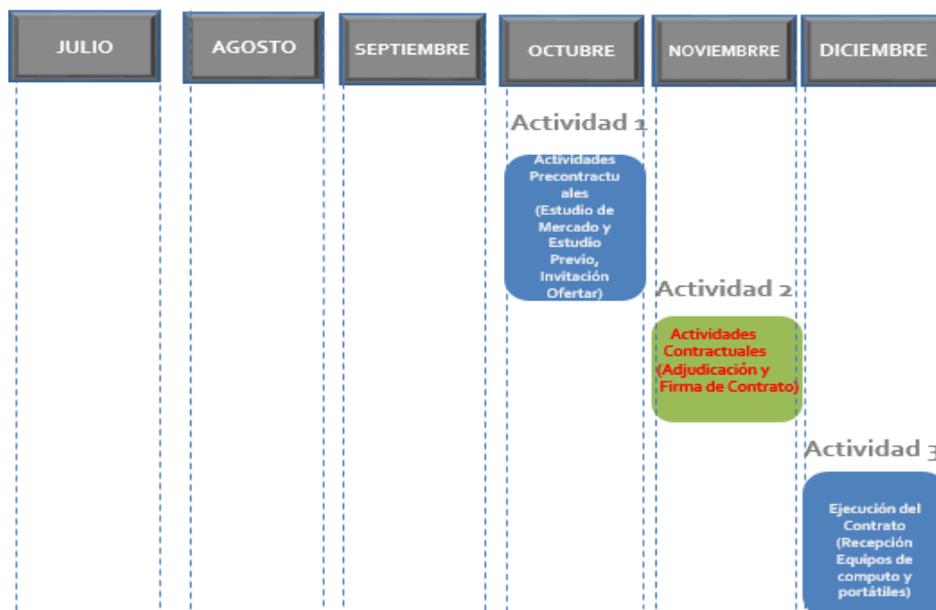
11.6.5 Adquisición de Equipos de Cómputo de Escritorio, Portátiles y Licencias de Ofimática

El proyecto tiene como fin la renovación tecnológica de los equipos de cómputo por fases garantizando con ello el suministro de equipos de escritorio y portátiles con su respectivo paquete ofimático para cumplir con las necesidades requeridas por los Magistrados, Jueces, Fiscales, Policía Judicial y de más funcionarios.

Objeto	Se requiere el reemplazo de 847 computadores que fueron adquiridos en el año 2010, 2011, 2012 y 2013, toda vez que están obsoletos.		
Tipo de Proyecto	Nuevo	Horizonte del Proyecto	2020
Presupuesto Total	\$5.000.000.000,00	Presupuesto Total TIC	\$3.166.000.000,00
Vigencia a aprobar	2020	Presupuesto TIC para la vigencia a aprobar	\$3.166.000.000,00
Fuente de Recursos	Propios	Código BPIN	No Aplica
Dependencia Lider	Dirección Ejecutiva de la Justicia Penal Militar	Gerente de Proyecto	Fabio Espitia Garzón Director Ejecutivo de la Justicia Penal Militar



2020



Descripción	Cantidad	Precio Total	Número de la Actividad
HARDWARE			
Computador	400	2.339.000.000,00	
Portátil	124	589.000.000,00	
SOFTWARE			
Licencias Ofimáticas (Office 365 Empresarial)	524	238.000.000,00	
TOTAL		\$3.166.000.000,00	

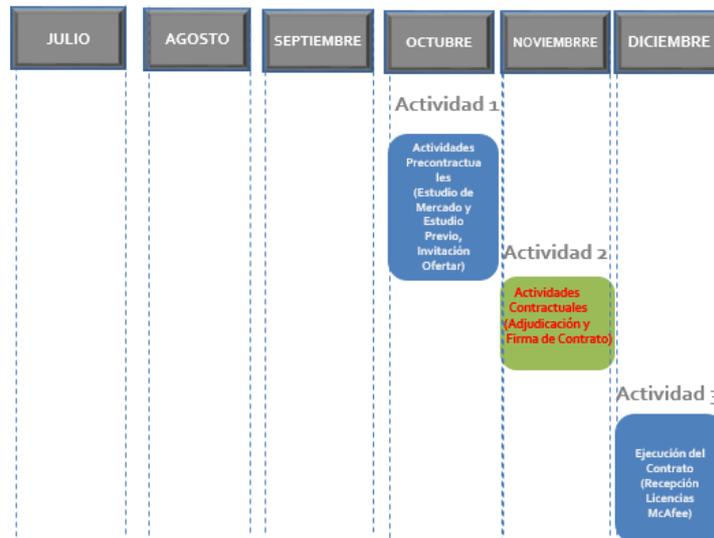
11.6.6 Renovación del licenciamiento del software de protección de equipos

El proyecto tiene como fin renovar los antivirus para la protección y seguridad de los portátiles. El objetivo del proyecto es la renovación del antivirus en los computadores y equipos portátiles para la protección y seguridad de estos.



Objeto	Se requiere la renovación del antivirus por la protección y seguridad de los computadores de escritorio y portátiles con la herramienta McAfee en la Dirección Ejecutiva de la Justicia Penal Militar.		
Tipo de Proyecto	Nuevo	Horizonte del Proyecto	2020
Presupuesto Total	\$100.000.000,00	Presupuesto Total TIC	\$100.000.000,00
Vigencia a aprobar	2020	Presupuesto TIC para la vigencia a aprobar	\$100.000.000,00
Fuente de Recursos	Propios	Código BPIN	No Aplica
Dependencia Líder	Dirección Ejecutiva de la Justicia Penal Militar	Gerente de Proyecto	Fabio Espitia Garzón Director Ejecutivo de la Justicia Penal Militar

2020



Descripción	Cantidad	Precio Total	Número de la Actividad
SOFTWARE			
Licencias Existentes de Suite McAfee(CEB)	600	48.000.000,00	
Licencias THREAT INTELLIGENCE EXCHANGE (TIE)	600	22.200.000,00	
Licencias de McAfee Suite CDA	200	29.800.000,00	
TOTAL		\$100.000.000,00	

11.7 Plan de proyecto de inversión

Para la presente vigencia el área de Tecnologías de la Información y las Comunicaciones no tiene un Plan de Proyecto de Inversión.

12 PLAN DE COMUNICACIONES DEL PETI

Este plan deberá facilitar la socialización y apropiación del PTI dentro de la JEP, a través de diferentes medios con el fin de sensibilizar a la organización de los proyectos estratégicos de TI alineados con los objetivos estratégicos de la entidad.

A continuación, se describen las acciones del plan.

1. Se harán publicaciones anuales del PTI, de acuerdo con los ajustes que se hayan hecho con base en las necesidades de la UAESJPMP.
2. El PETI aprobado por la Secretaría Ejecutiva se presentará en el órgano de gobierno de la JEP para su conocimiento.
3. El documento se publicará en la página WEB oficial de la Entidad y en la INTRANET.
4. En apoyo con el área de Comunicaciones hacer folleto que resuma los temas más importantes del PETI para su difusión por correo electrónico a todos los funcionarios de la UAESJPMP.

13 CONTROL DE CAMBIOS

Versión	Fecha	Descripción
1	28/03/2022	Formulación y Aprobación del Plan Estratégico de tecnologías de la Información y las Comunicaciones PETIC 2022. Aprobado por el Comité Institucional de Gestión y Desempeño, en sesión 2 del 28 de marzo de 2022.