Ejercicio de Arquitectura Empresarial
Optimización del Proceso para la Atención de Solicitudes de Informática Forense en el Nivel Central de la Fiscalía General de la Nación

Oscar Javier Mendivelso Cortés
Yeny Patricia Segura Gil

Trabajo de grado presentado como requisito para optar al título de:
Magister en Gerencia Estratégica de Tecnologías de Información

Tutor:
Mgtr. Hazbleydi Cervera Veráztegui

Línea de Investigación:
Arquitectura Empresarial

Universidad Externado de Colombia
Administración de Empresas
Bogotá D.C, Colombia

2019

Nota de Aceptación

_____

_____

_____

_____

_____
Firma Director
Trabajo de Grado

_____
Firma del jurado

_____
Firma del jurado

Bogotá DC. Junio de 2019

Dedicatoria

Este trabajo está dedicado a nuestras familias ya que es fruto no solo de nuestro esfuerzo sino también de su apoyo y comprensión; pasamos largas horas fuera de casa o frente a un computador y siempre estuvieron allí, alentándonos con palabras que motivaban a lograrlo, esperando pacientemente a que nuestro tiempo pudiera ser compartido con ellos, es una etapa compleja que debimos recorrer, pero siempre con el firme propósito de alcanzar nuestra meta. Aquí estamos, juntos, finalizando uno de nuestros propósitos. Gracias a Dios por haberlo logrado.

Agradecimiento

En primer lugar, agradecemos a Dios por darnos la fortaleza al emprender un nuevo reto para nuestra vida profesional, a nuestras familias por acompañarnos y alentarnos en nuestros momentos de dificultad, a la Universidad Externado por acogernos en tan honorable claustro educativo y brindarnos todas las herramientas que nos permitieron aprovechar al máximo nuestras clases y a los docentes que dieron lo mejor por compartir su conocimiento e inspirar en nosotros el logro de nuevos retos.

A nuestros compañeros de clase que compartieron sus vivencias y nos permitieron conocer de otras realidades profesionales, además aportaron con su alegría al compartir cada noche en el aula de clase.

Agradecemos muy especialmente a nuestra Directora de tesis quien a través de su experiencia y conocimiento generó valiosos aportes que orientaron el rumbo de nuestro trabajo.

A los funcionarios de la Fiscalía General de la Nación, en especial a los del Grupo de Informática Forense, quienes a través de su disposición y conocimiento hicieron posible la ejecución de este proyecto.

Tabla de contenido

Índice de tablas

Índice de figuras

Índice de anexos

Introducción

En Colombia, la Fiscalía General de la Nación (FGN) es la entidad encargada de ejercer "acción penal y de extinción de dominio en el marco del derecho constitucional al debido proceso; (…) garantiza el acceso efectivo a la justicia, la verdad y la reparación de las víctimas de los delitos; y genera confianza en la ciudadanía" (Fiscalía General de la Nación, 2017b, p. 7); en la estructura orgánica de la FGN, las labores de planificación, ejecución y control de las funciones de policía judicial están a cargo del Cuerpo Técnico de Investigación (CTI), quien además se encarga de asesorar al Fiscal General en la definición de políticas y estrategias relacionadas con temas de "investigación criminal, servicios forenses y de genética y en la administración de la información técnica y judicial que se requiera para la investigación penal" (Decreto Ley 898, 2017, art. 34). Bajo el mando de la Dirección del CTI, se encuentra el Grupo de Informática Forense Nivel Central de la FGN, el cual tiene a su cargo las actividades de recolección y examen forense de evidencia digital, enmarcadas en el proceso misional de investigación y judicialización; entendiendo por evidencia "información con valor probatorio almacenada o transmitida en formato digital, de tal manera que una parte o toda puede ser utilizada en el juicio" (Scientific Working Group on Digital Evidence [SWGDE], 2016); (Informática Forense Colombia, 2017, párr 1).

El uso masificado de dispositivos electrónicos hace de la evidencia digital un medio de prueba cada vez más común dentro de las investigaciones judiciales; de acuerdo con las cifras reveladas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), en Colombia, el número de abonados en el servicio de telefonía móvil tuvo un aumento del 6,3%, entre el primer trimestre del año 2017 y el mismo trimestre del año 2018, alcanzando una cifra cercana a los 63 millones de dispositivos móviles, que equivale a un índice de penetración de 126,1% (Ministerio de Tecnologías de Información y las Comunicaciones, 2018b); este incremento constante en el nivel de adopción de las tecnologías de información, sumado a la aparición de nuevos y más sofisticados dispositivos para el intercambio de datos, impacta directamente el nivel de respuesta que tiene el Grupo de Informática Forense Nivel Central de la FGN, debiendo afrontar un crecimiento continuo en el número y la complejidad de las solicitudes que atiende.

El protagonismo que ha adquirido la evidencia digital en las investigaciones judiciales, los desafíos que plantea cada aparición de una nueva tecnología y el compromiso de "aportar mayor valor social en el cumplimiento de sus funciones (...) y contribuir a la satisfacción del derecho al acceso a la justicia de los colombianos"(FGN, 2017b, p. 6), demuestran la pertinencia de realizar estudios que contribuyan a la construcción de un proceso más eficiente para la atención de los requerimientos de informática forense en la FGN. Este trabajo de investigación, combina métodos de investigación cualitativos y cuantitativos, con lineamientos del marco de arquitectura empresarial TOGAF, buscando elaborar una propuesta de

optimización que potencie la entrega de valor en cada una de las solicitudes atendidas por el Grupo de Informática Forense Nivel Central de la Fiscalía General de la Nación.

El primer capítulo de este documento inicia con una breve contextualización sobre la Fiscalía General de la Nación, el Grupo de Informática Forense y los conceptos de evidencia digital y arquitectura empresarial; continúa con la descripción de los servicios que ofrece el Grupo de Informática Forense, el proceso para atender cada solicitud recibida, algunas ineficiencias detectadas en las distintas fases del proceso y finaliza con el planteamiento de las preguntas de investigación, los objetivos del trabajo, el alcance y limitaciones del estudio.

En el segundo capítulo se relaciona el marco teórico que sustenta el desarrollo del trabajo de investigación; allí se detalla el concepto de arquitectura empresarial y sus marcos de referencia más representativos, haciendo énfasis en la descripción del ciclo ADM, componente central del marco de arquitectura TOGAF; también se hace referencia a las técnicas de priorización de proyectos, profundizando en los conceptos del método analítico jerárquico.

En los capítulos tres y cuatro se describe la metodología de investigación utilizada para comprender el funcionamiento del Grupo de Informática Forense, se presentan los métodos de recolección de información aplicados en el estudio y se analizan los resultados obtenidos buscando identificar oportunidades de mejora en la atención de requerimientos relacionados con obtener evidencia digital.

En el capítulo final, se elabora una propuesta de mejora al proceso para la atención de solicitudes de informática forense, enmarcada en los lineamientos de las primeras siete fases del ciclo ADM TOGAF; esta propuesta incluye la definición de un proceso objetivo, la identificación de brechas de negocio y brechas tecnológicas, el planteamiento de proyectos que permitan la Entidad trascender de su estado actual al estado objetivo y la elaboración de un mapa de ruta para la ejecución de los proyectos planteados.

1 Planteamiento del Problema

1.1 Antecedentes

La Fiscalía General de la Nación (FGN) es una entidad adscrita a la Rama Judicial del poder público en Colombia, sus funciones están definidas en el artículo 250 de la Constitución Política de 1991, tiene por obligación ejercer la acción penal y realizar la investigación de los hechos que lleguen a su conocimiento por distintos medios y que revistan las características de delito (Const., 1991, art. 250). La acción penal se origina a partir de un delito y supone la imposición de un castigo conforme a lo establecido en la ley, sobre quien lo haya cometido; la acción penal es el punto de partida de un proceso judicial.

El papel investigativo de la Fiscalía se adelanta a través de los organismos de policía judicial, quienes bajo la coordinación de un Fiscal del Caso desarrollan actividades de investigación y recaudan todo el material probatorio que permita sustentar ante los jueces la ocurrencia de un delito y la identidad del autor o los partícipes (Avella Franco, 2007)

El uso masificado de dispositivos digitales como los smartphone, tabletas digitales y computadores, el intercambio de información a través de correo electrónico, aplicaciones de mensajería instantánea, redes sociales y el almacenamiento de datos en sistemas de información, bases de datos y la nube; han generado un espacio digital en el cual se almacenan insumos de información cada vez más valiosos para el esclarecimiento de hechos penales investigados por la FGN, los participantes en la más reciente reunión de expertos en Delito Cibernético de la Oficina de Naciones Unidas contra la Droga y el Delito – UNODC, coinciden en que “la prueba electrónica (evidencia digital) está adquiriendo cada vez mayor importancia en la detección, investigación y persecución de todos tipo de delitos” (United Nations Office on Drugs and Crime, 2019).

Evidencia digital es información con valor probatorio almacenada o transmitida de forma binaria (Scientific Working Group on Digital Evidence [SWGDE], 2016); para acceder a ella se requiere la aplicación de conocimiento, técnicas y herramientas especializadas a cargo de expertos que desempeñan su labor en los grupos encargados de ejecutar actividades de Informática Forense. Informática forense se define como, la aplicación de la ciencia para la identificación, recolección, examen y análisis de datos preservando la integridad de la información y manteniendo una estricta cadena de custodia de los datos (National Institute of Standards and Technology [NIST], 2006).

El Grupo de Informática Forense en el Nivel Central de la FGN, bajo la Dirección del Cuerpo Técnico de Investigación (CTI), ejerce sus actividades enmarcadas en el

proceso misional de Investigación y Judicialización, cumple funciones de policía judicial y tiene a su cargo la recolección y examen forense de evidencia digital, inmersa en todo tipo de delitos investigados por la FGN.

Considerando lo importante que ha resultado ser la evidencia digital en muchas investigaciones adelantadas por la FGN, en los últimos años se ha incrementado la demanda de solicitudes que debe atender el grupo de Informática Forense, situación que en ocasiones desborda la capacidad de respuesta que tiene el grupo y está evidenciando ineficiencias existentes en el proceso para la atención de las solicitudes, especialmente en lo que respecta al esquema actual de asignación de las órdenes de trabajo, actividad que se desarrolla de forma manual; esto crea la necesidad de plantear nuevas formas de operar, basados en estándares y buenas prácticas de la industria, apalancados en el uso de las tecnologías de la información.

Con el avance acelerado de los desarrollos tecnológicos las organizaciones se enfrentan a la necesidad de dar solución a dos dificultades incrementales en la gestión de TI que son, "la capacidad de gestionar la creciente complejidad de los sistemas de información en las organizaciones" (Arango Serna, Londoño Salazar & Zapata Cortes, 2010, p.103) y la dificultad para generar valor real a partir de los mismos (Arango Serna, et al., 2010). Una estrecha relación entre estos dos desafíos de la gestión tecnológica puso en evidencia la necesidad de contar con métodos y recursos adecuados para enfrentarse a la evolución de los sistemas de información. En el ámbito Colombiano, las entidades públicas no estaban acostumbradas a trabajar con base en estándares, según indica María Isabel Mejía ex viceministra de TI, para finales del año 2013, cada entidad operaba como "una isla separada, desconectada y sin ninguna coordinación con las demás entidades" (Ministerio de Tecnologías de la Información y las Comunicaciones [MINTIC], 2013, p. 3) lo que se traducía en trámites repetitivos para el ciudadano; diversos problemas de seguridad en los sistemas de información y altos costos económicos en la gestión de TI; bajo este escenario, el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) inició una campaña para incorporar el concepto de arquitectura empresarial en las Entidades del estado, orientada a "definir políticas, dar lineamientos y establecer estándares que permitan un Estado coordinado y eficiente" (MINTIC, 2013, p. 3)

El concepto de arquitectura empresarial surge en 1987 con la publicación del artículo "Un marco para la arquitectura de sistemas de información" escrito por Jhon Zachman quien para la época trabajaba en IBM; Zachman estableció una relación directa entre el éxito del negocio y los sistemas de información y planteó la necesidad de "mantener el enfoque y la disciplina para la gestión de los mismos" (Arango Serna, et al., 2010, p. 104); dicho planteamiento fue de gran influencia para otros grupos dedicados a la elaboración de marcos de referencia para la gestión tecnológica, entre ellos el Departamento de Defensa de los Estados Unidos, quienes en 1994 publicaron su Technical Architecture Framework for Information

Management (TAFIM), el cual fue retomado en 1995 por The open group, dando como resultado el The Open Group Architectural Framework (TOGAF), cuya orientación inicial fue evolucionando mediante versiones sucesivas, hasta alcanzar su madurez conceptual (Arango Serna, et al., 2010).

1.2 Problemática u oportunidad

En la actualidad, el uso masificado de la tecnología ha generado un aumento de investigaciones judiciales en las que resulta de gran ayuda para esclarecer un hecho, la información obtenida de un computador o teléfono celular; ésta situación conlleva al incremento de solicitudes para que se adelante un estudio forense de evidencia digital; es posible anticipar que esta tendencia se mantenga a futuro y que las próximas investigaciones requieran el análisis de dispositivos electrónicos nuevos, modernos y con mayores capacidades de almacenamiento, lo que se traduce en desafíos constantes para los investigadores forenses en el campo de la evidencia digital (Lillis, Becker, O'Sullivan, & Scanlon, 2016)

El aumento de solicitudes para la recolección y examen forense de evidencia digital atendidas por el grupo de Informática Forense de la F.G.N – Nivel Central, ha puesto en evidencia una serie de ineficiencias presentes en el proceso, que van desde la asignación de órdenes de trabajo hasta la generación de resultados que aporten valor real a las investigaciones penales lideradas por la Entidad u otras Entidades del Estado.

El grupo de Informática Forense atiende diversos requerimientos, dentro de los cuales se encuentran, la recolección de evidencia digital en diligencias judiciales de registro y allanamiento, inspección o entrega voluntaria; la extracción de evidencia digital almacenada en dispositivos como teléfonos celulares, computadores, memorias, entre otros; extracción de evidencia digital de sistemas informáticos y bases de datos; análisis de información digital (logs, bases de datos, código fuente, malware, etc.); entre otras, todas ellas enmarcadas en el desarrollo de investigaciones penales, cuyo objetivo es obtener información útil para esclarecer un hecho delictivo.

Las diligencias judiciales en las que participa el grupo de Informática Forense (registro y allanamiento, inspección o entrega voluntaria) se rigen bajo lo dispuesto en los artículos 219 al 226 del Código de Procedimiento Penal Colombiano. El registro y allanamiento se define como el acceso que realiza la policía judicial, por orden de un Fiscal; a un inmueble, nave o aeronave, "con el fin de obtener elementos materiales probatorios y evidencia física (…)" (Código de Procedimiento Penal, 2004, p.6), por su parte la entrega voluntaria se lleva a cabo en el momento en que una persona en calidad de víctima, testigo o indiciado aporta información digital para que sea considerada en la investigación. En este tipo de diligencias, la función del personal de Informática Forense es, con previa orden de Fiscal o

autoridad competente, recolectar información en formato digital o dispositivos de almacenamiento digital que contengan información útil para la investigación penal, aplicando procedimientos técnicos especializados que preserven la integridad de la información y cumpliendo con la cadena de custodia, a fin de garantizar que la evidencia digital sea aceptada como medio de prueba en estrados judiciales.

El proceso para la atención de solicitudes de informática forense inicia con la recepción de la orden junto con los elementos sobre los que se realizará el examen forense (Elemento material probatorio EMP / Evidencia física EF), la orden es un documento físico expedido por un Fiscal o Autoridad competente en el que se emite autorización para realizar la actividad judicial; una vez se recibe la solicitud, el Coordinador del Grupo se encarga de asignar una orden de trabajo a un investigador o grupo de investigadores para que sea atendida, seguidamente los funcionarios del Grupo de Informática Forense a los que le fue asignada la orden de trabajo, ejecutan la actividad técnica que corresponda. El proceso finaliza cuando los investigadores o peritos del Grupo entregan a la autoridad solicitante el informe de policía judicial (investigador de laboratorio o campo) que es un documento impreso que contiene la descripción y documentación fotográfica de los elementos (EMP/EF) objeto de estudio, el procedimiento técnico realizado y los resultados obtenidos, adicionalmente se entrega, por lo general, un medio de almacenamiento digital (CD, DVD, Blu-ray, Disco Duro) con la información obtenida (evidencia derivada) en el examen forense realizado. En la Entidad, el proceso continua con la recepción del informe por parte del Fiscal o Autoridad solicitante y el respectivo análisis y valoración de la información obtenida para ser presentada ante estados judiciales; es de aclarar que el alcance del presente ejercicio de arquitectura empresarial solo cubre el proceso a cargo del Grupo de Informática Forense, sin embargo, la propuesta de optimización busca generar cambios que reflejen mejoras en el paso siguiente, ya sea con la disminución de los tiempos de espera o la entrega de resultados más ajustados a las necesidades del solicitante y que generen mayor valor para el cumplimiento de los objetivos estratégicos de la Entidad.

En cuanto a las ineficiencias presentes en el proceso para la atención de solicitudes de informática forense sobresale el hecho que a lo largo del proceso se hace uso de tres sistemas de información (Orfeo, SPOA y SIG) en los que se generan reprocesos, demoras y no satisfacen las necesidades del grupo, esto se sustenta con los hallazgos referidos en el Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETIC) 2017-2020 de la Entidad, en el cual se indica que “las integraciones de los aplicativos es insuficiente, por lo cual manualmente se debe registrar en más de una aplicación la misma información” (Fiscalía General de la Nación [FGN], 2017a, p.12) y que según “la percepción de los funcionarios menos de 70% considera que las aplicaciones SPOA, SIG, Orfeo y SIAF cubren los procesos” (FGN, 2017a, p.12).

Por otra parte, en la actualidad no se conoce de forma precisa o aproximada el tiempo necesario para la atención de cada uno de los diferentes requerimientos que se reciben en el Grupo, tampoco se conoce de manera exacta el grado de ocupación del recurso humano; ésta falta de información para la toma de decisiones está dificultando la labor de asignar efectiva y equitativamente las órdenes de trabajo; se suma a las ineficiencias, los requerimientos que se reciben en el Grupo y no describen de forma clara la necesidad específica, por tanto la definición de tiempos y recursos para la atención de las solicitudes se vuelve más compleja, de igual forma se reciben solicitudes que no tienen claridad de lo que se busca, exigiendo la extracción de la totalidad de información contenida en medios de almacenamiento digital o sistemas de información lo cual genera un alto consumo de recursos tanto humanos como técnicos que impiden la atención de otros requerimientos. Finalmente, la mayoría de requerimientos llegan al Grupo con tiempos de atención ya definidos por la Autoridad solicitante, esto sin contemplar los atributos técnicos que exige la atención de cada requerimiento, generalmente son tiempos muy cortos que no están acordes a las exigencias del procedimiento técnico.

En la etapa posterior a la asignación de la orden de trabajo, cuando los peritos atienden técnicamente la solicitud, se observan dificultades por cuanto no existe un estándar formal de tiempos de respuesta para los diferentes tipos de solicitudes, razón por la cual los investigadores deben acatar los plazos impuestos, comprometiendo regularmente la calidad de sus entregables.

Lo expuesto anteriormente, demuestra que existe la necesidad de optimizar el proceso para la atención de solicitudes dispuesto en el grupo de Informática Forense del Nivel Central de la Fiscalía General de la Nación, en este particular la arquitectura empresarial se aplica como instrumento que permite a la Entidad “afrontar de manera articulada (…) los retos asociados con alcanzar la eficiencia operativa, al facilitar la alineación entre la estrategia, los aspectos de negocio, las tecnologías de la información y las capacidades operativas” (Arango Serna, Branch Bedoya & Londoño Salazar, 2014, p.2)

1.3 Preguntas de investigación

1.3.1 Principal

¿Cómo hacer más eficiente el proceso para la atención de solicitudes en el grupo de Informática Forense del Cuerpo Técnico de Investigaciones – Fiscalía General de la Nación, aplicando conceptos del marco de arquitectura empresarial TOGAF?

1.3.2 Secundarias

- ¿Cuáles son los aspectos del proceso que presentan ineficiencias?
- ¿Qué capacidades se requieren para superar las ineficiencias del proceso?

- ¿Cómo aumentar la entrega de valor en cada uno de los requerimientos atendidos por el grupo de informática forense?

1.4 Objetivos

1.4.1 General

Realizar una propuesta de optimización del proceso para la atención de solicitudes en el Grupo de Informática Forense del CTI, alineada con la arquitectura institucional y los objetivos estratégicos definidos en el Plan 2016-2020 de la Fiscalía General de la Nación.

1.4.2 Específicos

- Conocer el proceso actual para la atención de solicitudes en el grupo de informática forense.
- Identificar ineficiencias en la atención de las solicitudes de informática forense
- Proponer mejoras al proceso que incrementen la entrega de valor y apoyen el cumplimiento de los objetivos estratégicos de la Entidad, a través del uso de tecnologías de la información.
- Plantear una estrategia de implementación para los cambios propuestos sobre el proceso de atención de solicitudes de informática forense.

1.5 Limitaciones y alcance

1.5.1 Limitaciones

En la elaboración del presente trabajo de investigación se tienen limitaciones de acceso a información confidencial a cargo de dependencias diferentes al área en la que se adelanta el estudio, por otro lado, no se cuenta con datos históricos que permitan tener una visión clara del rendimiento actual del equipo de trabajo ni proyectar con exactitud la demanda futura, adicional a esto, el tiempo disponible de los investigadores no es suficiente para llegar al planteamiento de una solución de software específica, por tanto solo se hará entrega del diseño de la arquitectura empresarial; por último, la posible implementación de la solución planteada queda sujeta a una evaluación de viabilidad realizada por la Entidad, teniendo en cuenta que sus adquisiciones dependen de la asignación de recursos a través del presupuesto nacional.

1.5.2 Alcance

El trabajo de investigación inicia con una fase exploratoria en la cual se realiza un análisis detallado del proceso para la atención de solicitudes en el grupo de Informática Forense, incluyendo la revisión de los objetivos estratégicos de la

Entidad, la estructura del proceso actual, la demanda de solicitudes, las capacidades técnicas y de recurso humano y la legislación aplicable al proceso; finalizado este análisis, se elabora un modelo arquitectónico con base en los lineamientos del marco de arquitectura TOGAF, en donde se representan el estado actual del proceso y un estado objetivo propuesto; por último, se lleva a cabo un análisis de brechas y se plantean los proyectos que permitirán optimizar el proceso.

1.6 Supuestos

A través de un ejercicio de arquitectura empresarial es posible conocer el proceso para la atención de solicitudes en el grupo de Informática Forense, identificar los factores que degradan la prestación del servicio y proponer un proceso objetivo, que apoye de forma eficiente los objetivos estratégicos de la Entidad.

Los cambios en la arquitectura tecnológica de la Entidad, propuestos en el Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETIC) 2017-2020, serán implementados en su totalidad.

1.7 Justificación

El pacto por la transformación digital de Colombia del plan nacional de desarrollo 2018-2022 considera que, “la transformación digital de la sociedad es el mecanismo fundamental para aumentar la productividad pública y mejorar la competitividad” (Departamento Nacional de Planeación [DNP], 2019, p. 570). “En el Estado, la transformación digital implica el cambio de procesos, la modernización de las herramientas tecnológicas, entre otros, para aumentar la eficiencia y generar mayor valor agregado social y económico” (DNP, 2019, p. 570).

La estrategia de Gobierno en Línea del Estado colombiano dio inicio a la incorporación de tecnologías de la información y las comunicaciones en la mejora de la eficiencia en la administración pública, actualmente la política de Gobierno Digital sigue liderando dicha iniciativa y busca ampliar el espectro para incorporar soluciones tecnológicas avanzadas; el Gobierno nacional considera que “la transformación digital de la administración pública puede apalancar la transformación de toda la sociedad, pues desde las organizaciones públicas se puede generar un efecto multiplicador sobre las actividades productivas y los ciudadanos” (DNP, 2019, p. 570).

El CONPES 3784 del 9 de diciembre de 2013 adopta el modelo de gestión pública eficiente, dirigido a mejorar la calidad de la gestión, como la prestación de los servicios provistos por las entidades de la Administración pública.

El plan estratégico de la Fiscalía General de la Nación 2016-2020 busca una Entidad que se caracterice por un modelo de gerencia pública y apoya sus objetivos estratégicos en objetivos de gestión que buscan la “estandarización de los procesos y procedimientos” necesarios para el funcionamiento de la Entidad, el “mejoramiento tecnológico y el desarrollo de un nuevo sistema de información” además contribuir a la “consolidación de la política para el manejo estratégico de la carga de trabajo al interior de la entidad” (FGN, 2017b, p. 7)

> La aplicación de lineamientos de Arquitectura Empresarial y de TI en la Entidad, permite la adecuada identificación de necesidades tecnológicas; la efectiva formulación e implementación de políticas y directrices; la eficaz gestión de procesos y de actividades; y la efectiva adquisición y suministro de medios, herramientas y servicios tecnológicos a las Áreas, en el óptimo apoyo y fortalecimiento tecnológico, para la consecución de logros. (FGN, 2017b, p.153)

Conforme a lo anterior, la mejora en los procesos al interior de las Entidades públicas apoya al cumplimiento de sus objetivos estratégicos y refleja mayor eficiencia en la atención que el Estado da a la ciudadanía.

Optimizar el proceso para atención de solicitudes del grupo de informática forense, busca beneficiar el proceso misional de Investigación y Judicialización de la Fiscalía General de la Nación; mediante la aplicación de los conceptos de arquitectura empresarial se pretende identificar la forma en que este proceso puede apoyar de manera más eficiente los objetivos estratégicos de la Entidad y promover la prestación de mejores servicios a los ciudadanos en los que se disminuyan los tiempos de investigación y judicialización dando respuesta efectiva.

2 Revisión de Literatura

Las organizaciones de hoy se enfrentan a un entorno cambiante que exige transformaciones continuas. Mercados globalizados, innovaciones tecnológicas disruptivas y nuevas regulaciones legales exigen a las empresas, que se adapten con flexibilidad a estos requisitos (Buckl, Schweda & Matthes, 2010).

En Colombia, “la constante evolución de la sociedad y el avance del país hacia una economía digital caracterizada por factores como el conocimiento, la digitalización de la información, la interconexión y la innovación” (Ministerio de Tecnologías de la Información y las Comunicaciones, 2018, p.6) han motivado a que al interior del Estado se deban implementar estrategias que permitan a las entidades públicas satisfacer necesidades y resolver problemáticas a través del aprovechamiento de las tecnologías de la información y las comunicaciones, a fin de mejorar la calidad de los servicios que se prestan a los ciudadanos (MINTIC, 2018).

La política de gobierno digital emprendida en los últimos años por el Estado colombiano tiene por objeto fundamental la “generación de valor público en un entorno de confianza digital” (MINTIC, 2018, p.14) en este sentido no solo se busca que las entidades públicas usen la tecnología, sino lograr que la tecnología ayude en la resolución de problemas reales.

Para muchas entidades resulta difícil la ejecución de los proyectos “por la falta de visión compartida de la empresa actual y del panorama de TI” (MINTIC, 2013, p. 6), las áreas de tecnología en las entidades públicas y en otras organizaciones aún son vistas como de soporte a la operación, generadoras de altos costos para la gestión de los recursos de TI; esta visión debe cambiar, es claro que la tecnología debe ir más allá y convertirse en la clave para mejorar la eficiencia y la productividad, además de reducir tiempo y costos (MINTIC, 2013); para ello es fundamental lograr la alineación de las inversiones de TI con las metas de la organización, la arquitectura empresarial (AE) resulta ser un instrumento comúnmente aceptado para guiar la transformación que requieren las organizaciones (Buckl, et al., 2010).

En las entidades públicas del Estado colombiano se viene impulsando la adopción del concepto de arquitectura empresarial para la gestión de TI, referida como el “proceso de estudio, diseño y creación de un plan para que los proyectos sean exitosos” (MINTIC, 2013, p. 28), se busca un gobierno más ordenado, en el que la tecnología esté alineada a los objetivos de las entidades, se integren los sistemas de información que en su mayoría funcionan de manera aislada y la información que se encuentra en silos, para así lograr que las entidades puedan compartir información en tiempo real y se beneficie a los ciudadanos (MINTIC, 2013).

Los sistemas de TI que no satisfacen las necesidades del negocio son un despilfarro, los procesos de negocio sin un buen soporte de TI son ineficientes. (Session, 2008).

Si bien no existe una definición única de arquitectura empresarial (AE), se entiende como el proceso de planificación y representación de una vista de alto nivel del negocio, los procesos y sistemas de TI de una organización, sus interrelaciones y el grado en que estos procesos y sistemas se comparten por diferentes partes de la organización; la representación hace referencia a las salidas directas y tangibles del proceso de planificación (artefactos de AE, incluyendo dibujos de arquitectura, hojas de ruta y otra documentación). El objetivo principal de la AE es definir el estado futuro deseable de la organización, procesos de negocios y sistemas de TI (generalmente referidos como el "TO-BE" o arquitectura destino) y proporcionar una hoja de ruta para lograr este objetivo desde el estado actual ("AS-IS" o arquitectura de referencia) (Tamm, Seddon, Shanks & Reynolds, 2011).

La arquitectura empresarial busca optimizar en toda la organización el legado de procesos (tanto manuales como automatizados) generalmente fragmentados, en un

entorno integrado que responda al cambio y apoye la ejecución de la estrategia empresarial (The Open Group, 2018).

El aprovechamiento efectivo de la información y la transformación digital son factores clave para el éxito empresarial y un medio indispensable para lograr una ventaja competitiva. Una arquitectura empresarial responde a esta necesidad, al proporcionar un contexto estratégico para la evolución y el alcance de la capacidad digital en respuesta a las necesidades en constante cambio del entorno empresarial (The Open Group, 2018). La AE genera impacto positivo en la organización, beneficios que van desde la disminución de costos, mayor agilidad estratégica y una plataforma operativa más confiable; grandes organizaciones con un ambiente complejo se ven ampliamente beneficiadas (Tamm et al., 2011).

Los problemas en el ámbito de las empresas públicas y privadas son ciertamente complejos. Las organizaciones están luchando para adoptar nuevas tecnologías, lidiar con requisitos reglamentarios cada vez más estrictos, altos niveles de competitividad, retos de la globalización y el mercado, nuevas formas organizativas, todos ellos constituyen variables que generan complejidad (Arango Serna et al., 2014). En el lado de TI, la complejidad también es la norma, los sistemas informáticos y tecnológicos actuales son complejos, especialmente cuando son responsables de gran parte de las actividades productivas de la mayoría de las organizaciones, los servidores físicos y en la nube, las aplicaciones y el software se están volviendo más distribuidos, más heterogéneos, más conectados, más críticos para las organizaciones. A medida que los sistemas empresariales y la tecnología se vuelven más complejos, las relaciones entre ellos se vuelven más difíciles de mantener alineadas. Cada uno se vuelve más especializado en el ámbito que trabaja y desarrollan sus propios idiomas, incluso su propia cultura, tienen menos tiempo para relacionarse con aquellos que no comparten sus preocupaciones. Una creciente separación se desarrolla entre la empresa y las organizaciones de TI. En la mayoría de las organizaciones, el abismo entre TI y el negocio está aumentando (Watts, 2018; Session, 2008).

Con el fin de adaptarse y dar respuesta efectiva a los retos que implica la complejidad, las organizaciones deben orientar constantemente sus estrategias de negocio y hacer los ajustes con mayor agilidad, estos cambios deben verse reflejados en el modelo de negocio, los procesos operativos y las tecnologías de la información; la arquitectura empresarial es una herramienta que ayuda a consolidar la estrategia de negocio a través de la materialización de los cambios que requiere la organización (Arango Serna et al., 2014).

Crear una arquitectura empresarial desde ceros puede resultar una tarea complicada, para ello fueron creados los marcos de trabajo (framework) que sirven para simplificar el proceso y guiar a los arquitectos a través de todas las áreas de desarrollo de la arquitectura. Los marcos de trabajo representan el lenguaje a través del cual es posible la comunicación entre todos los participantes de una AE, proveen

un conjunto de normas, herramientas, buenas prácticas, plantillas y procesos que orientan el desarrollo de arquitecturas de manera uniforme, (Suarez Fernández, Jiménez Rubido, Villar Ledo & Infante Abreu, 2017) como lo menciona the Open Group (2018) los framework pueden ser usados como herramienta para estructurar el pensamiento, garantizando la coherencia y la integridad, estos ayudan a comprender los procesos de negocio y cómo soportar mejor dichos procesos con tecnología (Session, 2008).

Existe una amplia variedad de marcos de Arquitectura Empresarial, cada uno con fortalezas y debilidades; algunos se enfocan en modelar la arquitectura existente, otros en encontrar soluciones a problemáticas de negocios. Con frecuencia los marcos se clasifican en: gubernamentales, de código abierto, desarrollados por grupos, propietarios y de la industria de defensa (Watts, 2018)

El análisis de publicaciones de Suarez Fernandez et al. (2017) muestra que los marcos DoDAF, FEAF, Zachman y TOGAF son los más mencionados en la literatura, siendo Zachman y TOGAF los más referenciados; a continuación, se presenta una breve descripción de los marcos más representativos:

DoDAF: Marco de arquitectura del Departamento de Defensa de los Estados Unidos (DoD), es requisito que las agencias y contratistas del DoD lo empleen en el desarrollo de sus arquitecturas, este marco se ha convertido en estándar internacional para las organizaciones de defensa, aeroespaciales y de seguridad más grandes del mundo. Es aplicable a todas las grandes organizaciones que requieren métodos estructurados y repetibles para planificar e implementar cambios organizativos y desplegar nuevas tecnologías. Se utiliza para visualizar, representar y comprender arquitecturas operativas y de sistemas complicadas, además proporciona soporte para la toma de decisiones, basadas en descripciones estándar (Raynham, 2009).

FEAF: Marco Federal de Arquitectura Empresarial, es una metodología de proceso de arquitectura empresarial para el Gobierno Federal de los Estados Unidos de América. Este marco tiene un proceso para crear una arquitectura empresarial utilizando las mejores prácticas de arquitectura federal de empresas, además tiene un proceso de transición para migrar del estado actual a un estado futuro de una empresa y emplea una taxonomía para catalogar los activos de la arquitectura empresarial y un enfoque para medir el éxito del uso de la arquitectura empresarial (Kommadi, 2015).

Zachman: Bente, Bombosch & Langade (2012) citados por Bondel (2016) mencionan que el marco Zachman es uno de los primeros enfoques de AE, Zachman (2016) citado por Bondel (2016) lo describe como un esquema para clasificar y organizar un conjunto de modelos o artefactos utilizados para describir una arquitectura empresarial completa. Este esquema se deriva de otras disciplinas como la arquitectura y la ingeniería, las cuales ya exploraron la organización de

artefactos resultantes de la producción de elementos físicos complejos como edificios o aviones. Este marco proporciona una perspectiva holística de toda la empresa y al mismo tiempo, permite centrarse en ciertos aspectos del objeto. Por lo tanto, permite la toma de decisiones informadas con respecto a la creación, operación y transformación de la empresa. Una deficiencia que presenta este marco es que no proporciona información sobre las relaciones entre modelos individuales, además, no especifica cómo recopilar, administrar o interpretar la información que se organiza en el marco. El Marco de Zachman constituye una estructura para documentar una arquitectura empresarial. Esto significa que no está proporcionando un proceso de AE para la transformación empresarial, por lo tanto, se utiliza mejor en combinación con otros marcos Bondel (2016)

TOGAF: Marco desarrollado por miembros del Open Group, es un método detallado y un conjunto de herramientas de apoyo, para desarrollar una arquitectura empresarial. Puede ser utilizado libremente por cualquier organización que desee desarrollar una arquitectura empresarial para uso de la misma, el desarrollo de la versión original en el año 1995 se basó en el Marco de Arquitectura Técnica para la Gestión de la Información (TAFIM), desarrollado por el Departamento de Defensa de los Estados Unidos (DoD). El Departamento de Defensa le dio a The Open Group un permiso explícito y un estímulo para crear TOGAF basándose en el TAFIM (The Open Group, 2018). TOGAF proporciona un lenguaje, un enfoque y un conjunto de recomendaciones que abarcan todos los aspectos de la arquitectura empresarial, la estrategia de la organización, el negocio, la tecnología, planeación y la gestión del cambio, manteniendo una naturaleza genérica que no busca imponer una única solución (Desfray & Raymond, 2014).

En Colombia, el Marco de Referencia de Arquitectura Empresarial para la gestión de TI, creado en 2014 es uno de los habilitadores transversales de la política de Gobierno Digital, por medio del cual, el Estado busca que las entidades públicas apliquen el enfoque de arquitectura empresarial para el fortalecimiento de las capacidades institucionales y de gestión de TI (MINTIC, 2018); por competencia del MINTIC (2016) este marco orienta el desarrollo de un proceso de arquitectura empresarial en lo que respecta al diseño de la arquitectura de TI, la arquitectura de negocio debe ser apoyada en otros marcos de referencia.

En la práctica de arquitectura empresarial, cada uno de los marcos hace importantes contribuciones. Aunque se pudiera llegar a considerar que son mutuamente excluyentes, en realidad son complementarios (Session, 2008).

TOGAF proporciona un marco de mejores prácticas para agregar valor y permite a la organización crear soluciones viables y económicas que aborden sus problemas y necesidades comerciales, provee métodos y herramientas para ayudar en la aceptación, producción, uso y mantenimiento de una arquitectura empresarial. Se

basa en un modelo de proceso iterativo respaldado por las mejores prácticas y un conjunto reutilizable de activos de arquitectura existentes (The Open Group, 2018).

El marco TOGAF proporciona un lenguaje, un enfoque y un conjunto de recomendaciones que cubren todas las facetas de la arquitectura empresarial, desde la organización y la estrategia hasta el negocio y la tecnología, la planificación y la gestión del cambio. TOGAF propone un desglose de alto nivel en cuatro grandes dominios:

1. Arquitectura de negocio: Abarca estrategia, objetivos, procesos de negocio, funciones y organización.
2. Arquitectura de datos: Dedicada a la organización y gestión de la información.
3. Arquitectura de aplicaciones: Presenta aplicaciones, componentes de software y sus interacciones.
4. Arquitectura de tecnología: Describe las técnicas y componentes implementados, así como las redes y la infraestructura física sobre la que se ejecutan las aplicaciones y las fuentes de datos (Desfray & Raymond, 2014).

La clave del marco de arquitectura TOGAF es su método de desarrollo de arquitectura (ADM por sus siglas en inglés), el cual “describe cómo obtener una arquitectura empresarial que sea específica para la organización y que responda a los requerimientos del negocio” (The Open Group, 2013) el ADM es el método para el desarrollo y gestión del ciclo de vida de arquitectura, “ayuda a conocer el negocio y las necesidades de TI de la organización, la metodología involucra a los interesados en diferentes niveles y en diferentes fases” (Canabal, Cabarcas & Martelo, 2017) .

Como lo menciona The Open Group (2018), el método de desarrollo ADM proporciona un proceso probado y repetible para desarrollar arquitecturas. El ADM está conformado por las siguientes fases:

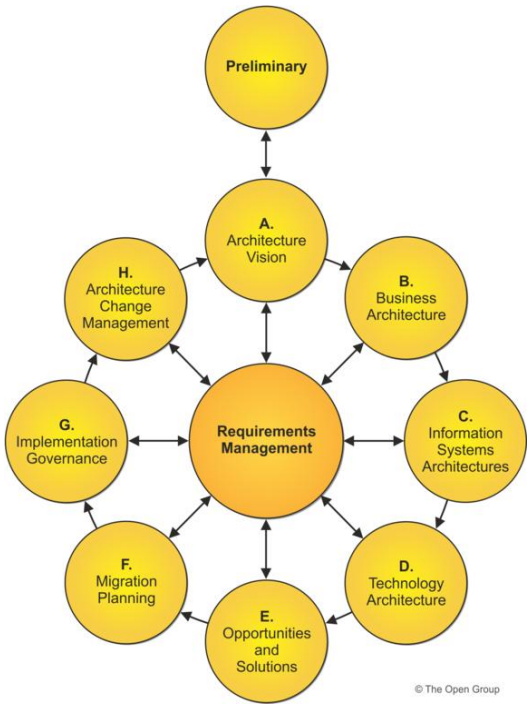


Figura 1. Ciclo del método de desarrollo ADM de TOGAF. Fuente: The Open Group. (2018). TOGAF® standard, version 9.2. Recuperado de http://pubs.opengroup.org/architecture/togaf92-doc/arch/

- Preliminar: Describe las actividades de preparación e iniciación necesarias para crear una capacidad de arquitectura, incluida la personalización del marco TOGAF y la definición de los principios de arquitectura.

- Fase A – Visión: Describe la fase inicial de un ciclo de desarrollo de la arquitectura. Incluye información sobre la definición del alcance de la iniciativa de desarrollo de la arquitectura, la identificación de las partes interesadas, la creación de la Visión de la Arquitectura y la obtención de la aprobación para continuar con el desarrollo de la arquitectura.

- Fase B – Arquitectura de negocio: Describe el desarrollo de una arquitectura negocio para respaldar la visión de arquitectura.

- Fase C – Arquitectura de sistemas de información: Describe el desarrollo de arquitecturas de sistemas de información para respaldar la visión de arquitectura.

- Fase D – Arquitectura tecnológica: Describe el desarrollo de la arquitectura tecnológica para respaldar la visión de arquitectura.

- Fase E – Oportunidades y Soluciones: Lleva a cabo la planificación de la implementación inicial y la identificación de los vehículos de entrega para la arquitectura definida en las fases anteriores.

- Fase F – Planificación de la migración: Explica cómo pasar de la línea de base a las arquitecturas de destino al finalizar un plan detallado de implementación y migración.

- Fase G – Gobernanza de la implementación: Proporciona una supervisión arquitectónica de la implementación.

- Fase H – Gestión de cambios de la arquitectura: Establece procedimientos para gestionar los cambios en la nueva arquitectura.

A continuación, se presenta una descripción general de la progresión de un ciclo de ADM, desde la fase preliminar hasta la fase H:

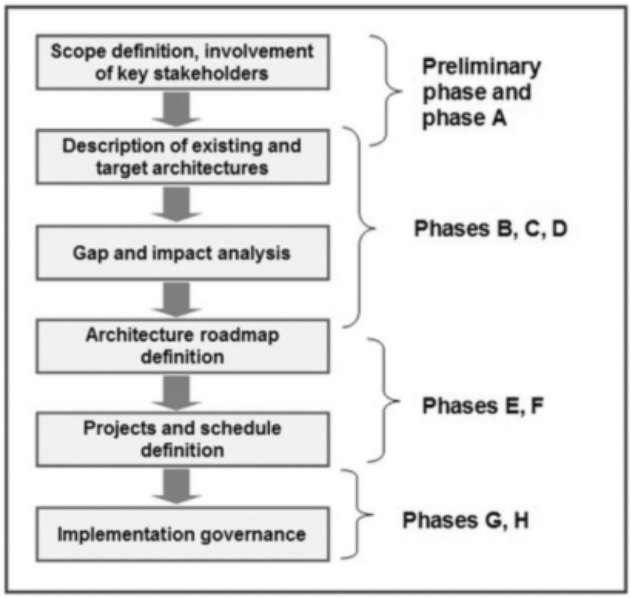


Figura 2. Camino típico de aplicación ADM. Fuente: Desfray, P., & Raymond, G. (2014). Modeling enterprise architecture with TOGAF: A practical guide using UML and BPMN. Burlington: Elsevier Science.

Este camino típico se guía por un objetivo principal: la necesidad de obtener el resultado esperado al dominar cada paso del proceso. Este objetivo requiere una preparación rigurosa, una descripción del objetivo con respecto a lo que ya existe para todas las facetas (negocios, sistema de información y tecnología), una evaluación precisa de las brechas y riesgos que determinan la elección de la

trayectoria, y finalmente una evaluación de los resultados y manejo cuidadoso de cualquier ajuste realizado (Desfray & Raymond, 2014).

Archimate

Archimate es un estándar de modelado que fue construido para representar arquitecturas empresariales y su evolución se encuentra estrechamente ligada al framework de arquitectura empresarial TOGAF (Desfray & Raymond, 2014), se trata de un lenguaje visual con una iconografía definida que permite describir, analizar y comunicar gran cantidad de elementos de las arquitecturas empresariales, que suelen cambiar con el tiempo; este lenguaje ofrece un enfoque arquitectónico para modelar los diferentes dominios de arquitectura, con representaciones construidas a partir de conceptos abstractos (elementos y sus relaciones) (The open group, 2017)

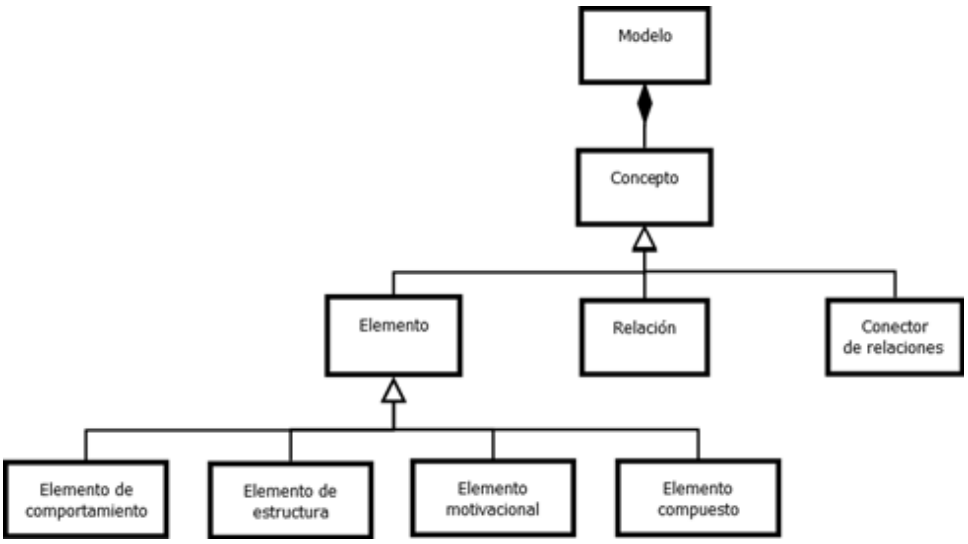


Figura 3. Metamodelo del lenguaje archimate. Fuente: Adaptado de The open group. (2017). ArchiMate® 3.0.1 Specification. Recuperado de http://pubs.opengroup.org/architecture/archimate3-doc/chap01.html#_Toc489945947
Nota: Adaptación de la figura 1: Top-Level Hierarchy of ArchiMate Concepts

Archimate está compuesto por un lenguaje de modelado central (arquitectura de negocio, arquitectura de aplicaciones y arquitectura de tecnología) y algunas extensiones recientes como el aspecto motivacional o la capa de implementación y migración (Desfray & Raymond, 2014); cada una de las capas del lenguaje contiene elementos de estructura activa, elementos de estructura pasiva y elementos de comportamiento.

- **Elementos de estructura activa**: Cualquier entidad capaz de realizar un comportamiento.
- **Elementos de comportamiento**: Representan las actividades realizadas por uno o varios elementos de estructura activa
- **Elemento de estructura pasiva**: Son elementos sobre los cuales se realiza una actividad; por ejemplo, los objetos de datos.

En la versión 3.0.1 del estándar archimate, los elementos de la capa física son añadidos a la capa de tecnología para el modelado de instalaciones, equipos físicos y redes de distribución (The open group, 2017); así mismo, los elementos de la capa de estrategia fueron adheridos a la capa de negocio.

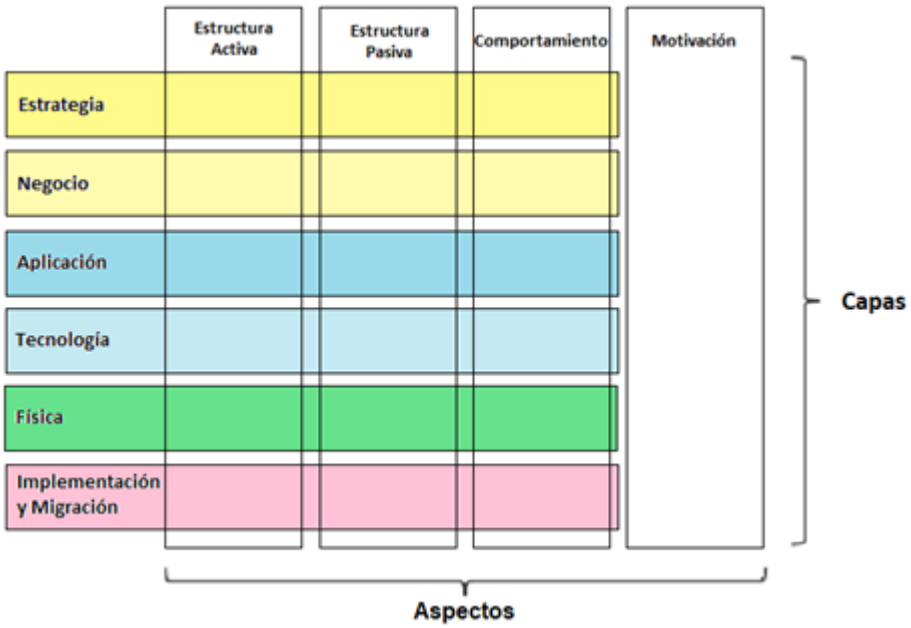


Figura 4. Framework archimate. Fuente: Adaptado de The open group. (2017). ArchiMate® 3.0.1 Specification. Recuperado de http://pubs.opengroup.org/architecture/archimate3-doc/chap01.html#_Toc489945947
Nota: Adaptación de la figura 3: Full ArchiMate Framework.

Además de los elementos descritos anteriormente, el lenguaje ArchiMate define una serie de relaciones genéricas, que sirven para conectar un conjunto predefinido de conceptos origen y destino (elementos u otras relaciones); muchas de estas relaciones están sobrecargadas; es decir, su significado exacto varía según los conceptos de origen y destino que se estén conectando (The open group, 2017). Las relaciones en archimate se clasifican en cuatro grupos:

- **Relaciones estructurales**: Modelan la construcción o la composición de elementos.
- **Relaciones de dependencia**: Describen la forma en que algunos elementos son utilizados por otros.
- **Relaciones dinámicas**: Representan dependencias temporales entre varios elementos de una arquitectura.
- **Otros tipos de relaciones**: Relaciones definidas en el lenguaje archimate que no encajan en alguna de las clasificaciones definidas.

Grupo de relaciones	Relación	Descripción	Notación
Relaciones Estructurales	Composition	Indica que un elemento está compuesto por uno o más conceptos	
	Aggregation	indica que un elemento agrupa una serie de otros conceptos	
	Assignment	Expresa la asignación de responsabilidad o ejecución	
	Realization	Indica que una entidad desempeña un papel crítico en la creación, el mantenimiento o el funcionamiento de una entidad más abstracta	
Relaciones de Dependencia	Serving	Indica que un elemento proporciona su funcionalidad a otro elemento	
	Access	Indica la capacidad de un elemento para observar o actuar sobre otro elemento de estructura pasiva	
	Influence	Indica que un elemento afecta la implementación o el logro de otro elemento motivacional	+/-
Relaciones Dinámicas	Triggering	Describe una relación causal o temporal entre dos elementos	
	Flow	Describe la transición de un elemento a tro	
Otro tipo de relaciones	Specialization	Indica que un elemento es un tipo particular de otro elemento	
	Association	Modela una relación no especificada, o una que no está representada por otra relación de ArchiMate	
	Junction	Se usa para conectar varias relaciones del mismo tipo	(And) Junction Or Junction

Figura 5. Tabla de relaciones lenguaje archimate. Fuente: Adaptado de The open group. (2017). ArchiMate® 3.0.1 Specification. Recuperado de http://pubs.opengroup.org/architecture/archimate3-doc/chap01.html#_Toc489945947
Nota: Adaptación de la tabla 3: Relationships.

Priorización de proyectos

La relevancia de un proceso de priorización de proyectos radica principalmente en la existencia de recursos limitados a la hora ejecutar los programas que una empresa se propone implementar; contar con un modelo apropiado de priorización de proyectos permite organizar y realizar las acciones necesarias, con el fin de ejecutar aquellos proyectos que sean más beneficiosos para los interesados, evitando así la dispersión de esfuerzos (Salas Villegas, 2011). En Pérez Vélez (2012), los métodos para la selección de portafolios de proyectos se clasifican cinco grupos:

- **Métodos financieros**: Este grupo hace referencia a los métodos de evaluación financiera de proyectos, donde se analizan factores como el Valor

Presente Neto, el retorno de la inversión y el valor comercial esperado, entre otros.

- **Alineación con la estrategia del negocio**: Los proyectos se agrupan en diferentes componentes o áreas del negocio, las cuales tienen asignados unos recursos, luego, por medio de un ejercicio de puntuación y análisis individual, se asignan recursos para cada proyecto.
- **Mapeo de portafolio o burbujas**: En este método los proyectos se califican en una gráfica de dos ejes que resumen los criterios de relevancia definidos, (por ejemplo, probabilidad de éxito vs retorno de inversión) y a partir de esto, se establece una calificación.
- **Modelos de Calificación**: En estos métodos se le asigna un puntaje a cada proyecto con base en una serie de criterios que se contestan a través de preguntas realizadas a un grupo de expertos.
- **Lista de chequeo**: En este tipo de métodos se asignan recursos a los proyectos o se eliminan con base en las respuestas de un formulario de preguntas con respuestas de Sí o No.

Dentro del grupo de modelos de calificación están incluidas algunas herramientas de jerarquización que son altamente aplicadas dentro de la gestión de proyectos. Los métodos multicriterio, como se les conoce, resultan ser muy adecuados para abordar procesos de priorización, ya que "permiten generar un consenso entre los diferentes intereses y puntos de vista de los involucrados" (Uribe Ramírez, González Rengifo, Osorio Gómez, & Manotas Duque, 2010, p. 2) y propician el establecimiento de un orden de prioridad basado en los objetivos planteados y en un conjunto de criterios cualitativos y cuantitativos. "Los principales métodos de evaluación y decisión multicriterio discreto que se pueden utilizar para priorizar son: Ponderación Lineal, Relaciones de Superación y el Proceso Analítico Jerárquico" (Uribe Ramírez et al., 2010, p. 3).

Proceso analítico jerárquico

"El Proceso de Análisis Jerárquico, es un método basado en la evaluación de diferentes criterios que permiten jerarquizar un proceso y su objetivo final consiste en optimizar la toma de decisiones gerenciales" (Taoufikallah, 1990, p. 1), propuesto por Thomas L Saaty, este método está diseñado para resolver problemas complejos que involucran múltiples criterios, permitiendo organizar de manera eficiente la información relacionada con un problema, descomponerla y analizarla por partes (Hurtado & Bruno, 2005).

El Proceso Analítico Jerárquico, AHP por sus siglas en inglés, es una de las técnicas multicriterio con mayor implantación práctica en casi todos los ámbitos de la toma de decisiones, sin describir en detalle las causas que han motivado su gran aplicabilidad, se pueden mencionar la flexibilidad de su técnica, la adaptación a numerosas situaciones, su facilidad de uso, la posibilidad de aplicarla de forma

individual o en grupo, y la existencia de herramientas de software para su implementación (Moreno Jiménez, 2002).

La técnica AHP requiere de tres insumos principales: Una lista de alternativas que se deseen comparar, priorizar u ordenar; un conjunto de criterios (cualitativos o cuantitativos) usados para valorar cada una de las alternativas y un objetivo que refleje claramente el propósito y el alcance de la priorización (Vidal H et al., 2012).

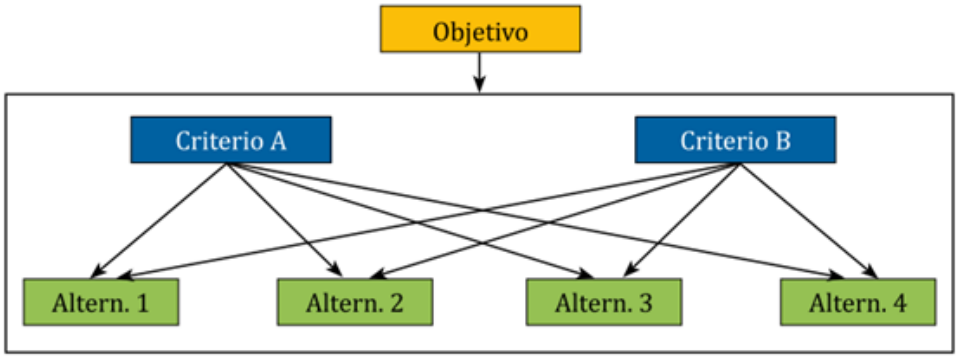


Figura 6. Esquema jerárquico del AHP. Fuente: Vidal H, C. J., Bravo B, J. J., Cajiao G, E., Meza H, P. P., Arango S, S., Franco L, D., & Calserón S, J. H. (2012). Guía metodológica para la priorización de proyectos: Un enfoque aplicado a la infraestructura, logística y la conectividad. Cali, Colombia. Recuperado de vitela.javerianacali.edu.co/bitstream/handle/11522/3451/Guia Metodologica_Infraestructura.pdf?sequence=1&isAllowed=y

El proceso de priorización de alternativas inicia con una confrontación de criterios por pares utilizando la escala de comparación de Saaty, el resultado es una matriz cuadrada, donde cada recuadro está asociado a la comparación de un par de criterios (Vidal H et al., 2012).

Tabla 1

Escala de comparación de Saaty

Escala numérica	Escala verbal
1	Igual importancia
3	Ligeramente más importante
5	Mucho más importante
7	Fuertemente más importante
9	Extremadamente más importante

Nota. Adaptado de: Vidal H, C. J., Bravo B, J. J., Cajiao G, E., Meza H, P. P., Arango S, S., Franco L, D., & Calserón S, J. H. (2012). Guía metodológica para la

priorización de proyectos: Un enfoque aplicado a la infraestructura, logística y la conectividad. Cali, Colombia. Recuperado de vitela.javerianacali.edu.co/bitstream/handle/11522/3451/Guia Metodologica_Infraestructura.pdf?sequence=1&isAllowed=y

la prioridad relativa de cada criterio se puede obtener calculando el promedio de las filas de la matriz de comparación normalizada.

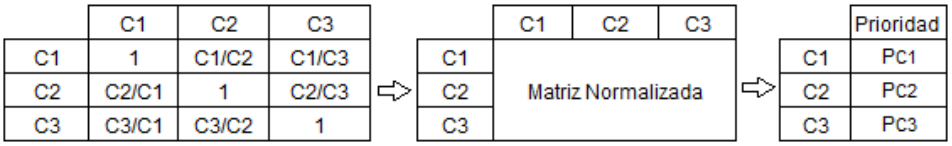


Figura 7. Cálculo del vector de prioridades relativas. Fuente: elaboración propia.

A continuación, siguiendo el mismo proceso de comparación, se enfrentan las diferentes alternativas con base en cada uno de los criterios de priorización; el resultado es un vector de prioridad de alternativas por cada criterio, con los cuales se conforma una matriz de prioridades locales (Vidal H et al., 2012). Por último, la prioridad general de cada alternativa se obtiene multiplicando la matriz de prioridades locales por el vector de prioridad de criterios.

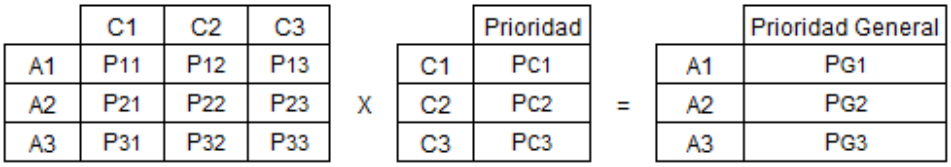


Figura 8. Cálculo de prioridades generales por alternativa. Fuente: elaboración propia.

3 Diseño metodológico

En este capítulo se exponen los fundamentos que justifican el uso de una metodología mixta de investigación para abordar los objetivos de estudio, además se describen las técnicas y elementos de recolección de información que serán empleados para el desarrollo del presente trabajo.

3.1 Contexto de estudio

Por mandato Constitucional, la Fiscalía General de la Nación es la Entidad del Estado colombiano encargada de "adelantar el ejercicio de la acción penal y realizar la investigación de los hechos que revistan las características de un delito que lleguen a su conocimiento" (Const., 1991, art. 250), además garantiza a la ciudadanía el acceso efectivo a la administración de justicia (Fiscalía General de la Nación, 2017b).

La Fiscalía desarrolla actividades investigativas a través de organismos de policía judicial bajo dirección, coordinación y control de un Fiscal de caso. La policía judicial es el "conjunto de autoridades que colaboran con la investigación de los delitos" (Fiscalía General de la Nación, 2019a, p. 9) Los funcionarios que ejercen funciones de policía judicial se encargan de recolectar y asegurar elementos materiales probatorios, evidencia física e información legalmente obtenida que permita sustentar las pretensiones de la Fiscalía ante los Jueces de la República (FGN, 2019a).

El literal g, artículo 275 de la Ley 906 de 2004 incluye como elementos materiales probatorios y evidencia física los mensajes de datos; según lo define la ley 527 de 1999 mensaje de datos es "La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares…", esta definición se une al concepto de evidencia digital que según lo establece el Grupo de Trabajo Científico sobre Evidencia Digital de los Estados Unidos (SWGDE por sus siglas en inglés) es toda información de valor probatorio (prueba o evidencia) almacenada o transmitida de forma binaria (SWGDE, 2016)

En los últimos años la evidencia digital se ha constituido en uno de los insumos más valiosos para el esclarecimiento de cualquier tipo de hecho delictivo, razón por la cual se podría explicar el aumento en el número de solicitudes relacionadas con la recolección o análisis de evidencia digital que según cifras del Nivel Central de la FGN pasaron de 720 reportadas entre junio de 2016 y mayo de 2017 a 1412 en el periodo comprendido entre junio de 2017 y abril de 2018.

El área encargada de cumplir funciones de policía judicial encaminadas a la recolección especializada y el análisis de evidencia digital en la Fiscalía General de la Nación Nivel Central es el Grupo de Informática Forense. El aumento en las solicitudes y la complejidad de las actividades que se desarrollan en el Grupo han generado gran dificultad en el proceso que se adelanta para la atención de solicitudes de informática forense, especialmente en la etapa de asignación de órdenes de trabajo; por tanto a través de este estudio se pretende lograr un entendimiento real de cómo se desarrolla el proceso en la actualidad, diseñar un proceso objetivo en el que se optimice la atención de los requerimientos en el grupo y se apoye eficientemente los objetivos estratégicos de la Entidad, esto permitirá

elaborar un análisis en el que se detecten las brechas existentes y se proponga la forma de superarlas.

3.2 Diseño del estudio, alcance

3.2.1 Diseño

Se da inicio al presente estudio con una revisión de literatura en el tema de arquitectura empresarial, en especial aquella relacionada con el marco de arquitectura TOGAF y casos de implementación en Entidades públicas. A continuación, se hace un acercamiento a la problemática presente hoy en el Grupo de Informática Forense con el objetivo de plantear una arquitectura base que permita hacer un análisis e identificar actividades clave o que dificultan el proceso, en esta fase también resulta importante revisar literatura en temas como evidencia digital y documentos propios de la Entidad que se relacionen con el objeto de estudio. Posteriormente se elabora una arquitectura objetivo con la cual se optimice el proceso para la atención de servicios de informática forense apoyando de manera eficiente los objetivos estratégicos de la Entidad, en esta etapa se aplican fases del ADM del marco de arquitectura TOGAF a través del análisis e interpretación de los datos y la literatura previamente consultada. Para concluir se lleva a cabo un análisis de brechas entre la arquitectura base (AS-IS) y la arquitectura objetivo (TO-BE) permitiendo con ello generar propuestas con las cuales se logre cumplir el objetivo del presente estudio.

Optimizar el proceso para la atención de servicios de informática forense en el nivel central de la F.G.N requiere de un claro entendimiento del proceso actual; considerando que no se cuenta con documentación que lo describa en detalle, este estudio busca su caracterización a través de información obtenida de personas que desempeñan diferentes roles intervinientes en el proceso, de esta manera se logra una visión general de los aspectos por mejorar, basada en los diferentes puntos de vista del proceso, dicha técnica permite triangular la información recibida, confirmando su validez. En este primer acercamiento es ideal el uso de métodos cualitativos, ya que facilitan la identificación de aspectos fundamentales que podrían ignorarse en otras circunstancias (Ragin, 2007).

Una vez comprendido el funcionamiento actual, se realiza un análisis de las capacidades tecnológicas y de recurso humano disponibles para atender los diversos tipos de requerimientos de informática forense recibidos por el nivel central de la F.G.N, el objetivo de dicho análisis es identificar brechas tecnológicas y profesionales que deben ser superadas para mejorar el rendimiento actual; esta investigación se enfoca en aspectos generales de los individuos y su objetivo es reconocer patrones que se correlacionan con las dificultades evidenciadas en la primera etapa del estudio; en esta fase, el uso de métodos cuantitativos resulta ser

el más adecuado, ya que favorecen el análisis de las características generales presentes en un gran número de casos (Ragin, 2007).

La combinación de técnicas, métodos, aproximaciones, conceptos o lenguaje cualitativo y cuantitativo dentro de un mismo estudio se conoce como metodología mixta de investigación; dicho enfoque busca legitimar el uso de múltiples aproximaciones para dar respuesta a las preguntas de investigación, en lugar de restringir y obstaculizar el trabajo de los investigadores; este pluralismo metodológico según algunos de sus defensores permite derivar en un tipo de investigación de mejor nivel en comparación con otra que implique un único método, siempre y cuando los investigadores estén en capacidad de combinar lo mejor de ambas aproximaciones metodológicas con el fin de que el resultado sea el mejor reflejo del complemento de fortalezas de cada método (Tibaud, 2009).

3.2.2 Alcance

El trabajo de investigación inicia con una fase exploratoria en la cual se analiza detalladamente el proceso para la atención de solicitudes en el grupo de Informática Forense Nivel Central de la FGN, incluyendo objetivos estratégicos de la Entidad, estructura del proceso actual, demanda promedio, capacidades técnicas y de recurso humano y legislación aplicable al proceso; finalizado este análisis, se lleva a cabo un ejercicio de arquitectura empresarial, basado en el marco de referencia TOGAF, en donde se representa el estado actual y una propuesta de mejora que optimiza el proceso.

Etapa I: Conocimiento del proceso actual

En esta primera etapa, con base en la documentación existente y acceso a información propia de la Entidad se busca conocer los objetivos estratégicos de la FGN, los tipos de solicitudes que se atienden y las capacidades técnicas y de recurso humano disponibles en el grupo de Informática Forense del Nivel Central en la actualidad; posteriormente se aplica un formato de entrevista a fiscales, investigadores de informática forense y coordinador de grupo, dicho formato está orientado a obtener la información mínima necesaria sobre el funcionamiento actual del proceso para la atención de solicitudes de informática forense, para construir un modelo de negocio que sirva de base en el análisis de brechas planteado por el marco de arquitectura empresarial TOGAF.

Etapa II: Definición proceso objetivo

Se aplica un único formulario de encuesta a los investigadores que integran el grupo de informática forense nivel central de la F.G.N; la información obtenida se tabula y se identifican aspectos de tipo profesional y tecnológico que requieren ser fortalecidos dentro del grupo, esto permite plantear un proceso objetivo en el que se optimice la atención de solicitudes en el grupo.

Etapa III: Identificación de brechas tecnológicas y profesionales

Una vez entendido el funcionamiento del proceso actual y planteado el proceso objetivo, se sugieren propuestas de mejora que permitan superar las ineficiencias identificadas en etapas anteriores.

3.3 Objeto de estudio

En el presente trabajo de investigación los objetos de estudio han sido clasificados con base en las etapas definidas en el alcance del marco metodológico:

Etapa I:

En el entendimiento del proceso actual para la atención de servicios de informática forense, la información recolectada debe provenir de personas que desempeñan roles participes en el proceso:

Tabla 2

Entrevista I: Conocimiento del proceso actual

Rol	Cantidad	Criterio de Selección
Asistente de Informática Forense	1	Disponibilidad
Coordinador Informática Forense	1	Disponibilidad
Investigador Informática Forense	4	Investigadores con experiencia mínima de cinco años en las áreas de digitales y móviles
Fiscal	2	Interacción con los servicios de informática forense en al menos 5 ocasiones

Fuente: elaboración propia

Etapa II y III:

El diseño del proceso objetivo y el análisis de brechas tecnológicas y profesionales se llevan a cabo con base en información general aportada por los investigadores de informática forense pertenecientes al Nivel Central de la F.G.N.

Tabla 3

Encuesta I: Identificación de brechas tecnológicas y profesionales

Rol	Cantidad	Representatividad	Criterio de Selección
Investigador Informática Forense	18	66%	Disponibilidad

Fuente: elaboración propia

3.4 Instrumentos

Para la recolección de información se utilizaron cuatro formatos de entrevistas y un formulario de encuesta aplicados secuencialmente según lo describe el alcance del marco metodológico:

Tabla 4

Instrumentos

Etapa	Tipo de instrumento	Nombre del artefacto
Conocimiento del proceso actual	Cualitativo	Formulario guía de entrevista Coordinador
		Formulario guía de entrevista Asistente
		Formulario guía de entrevista investigador informática forense
		Formulario guía de entrevista Fiscal
Identificación de brechas tecnológicas y profesionales	Cuantitativo	Encuesta Capacidades Grupo Informática Forense

Fuente: elaboración propia

3.5 Operacionalización del evento de estudio

La operacionalización de variables es el proceso de desagregar elementos abstractos (conceptos teóricos), hasta llegar a un nivel más concreto, esto es, los hechos producidos en la realidad y que representan indicios del concepto teórico, pero que podemos observar, recoger y valorar; en otras palabras, la operacionalización es “un puente entre los conceptos y las observaciones y actitudes reales” (Reguant Alvarez & Martínez Olmo, 2014, p. 4).

Tabla 5

Operacionalización

Objetivo General	Objetivo específico	Variable	Indicador	Instrumento	Ítem
Conocer el proceso actual para la atención de solicitudes de informática forense	Conocer los roles que intervienen en el proceso	Tipos de roles	N/A	Entrevista conocimiento del proceso actual	¿Cuál es su rol dentro del proceso, qué actividades realiza?
					¿Qué otros roles identifican dentro del proceso investigativo?
					Quien origina las solicitudes que atiende el grupo (¿qué personas o autoridades puede hacer requerimientos?)
	Conocer las solicitudes que atiende el grupo de informática forense	Tipos de solicitudes	Solicitudes más comunes	Entrevista conocimiento del proceso actual	¿Qué tipo de solicitudes atiende el grupo de informática forense?
					¿Cuáles son las solicitudes más comunes?
	Conocer el tiempo de atención de los requerimientos recibidos	Tiempo de atención de solicitudes	Cantidad de días por tipo de solicitud	Entrevista conocimiento del proceso actual	¿Hay un tiempo específico para la atención de requerimiento?, ¿cómo se establece?
					¿Considera que la forma en que se asigna el tiempo para la atención del requerimiento es la adecuada? En caso negativo: ¿Cómo lo mejoraría?
	Conocer las dificultades para la atención de las solicitudes	Tipos de dificultades	Dificultades más comunes	Entrevista conocimiento del proceso actual	¿Qué tipo de requerimientos generan dificultad para elegir quien debe atenderlo?
					¿Cuáles son las dificultades más comunes al realizar su trabajo?
					¿Cuáles son las solicitudes que representan mayor desgaste o que generan complicaciones?
					¿Qué aspectos del proceso cree usted que se pueden mejorar?
					Si pudiese cambiar algo del proceso

Objetivo General	Objetivo específico	Variable	Indicador	Instrumento	Ítem
					actual. ¿Qué cambiaría? Y ¿Por qué?
	Entender la forma en que las herramientas tecnológicas apoyan el proceso para la atención de solicitudes	Desempeño de los sistemas de información	Nivel de satisfacción	Entrevista conocimiento del proceso actual	¿Considera que el SI cubre completamente las necesidades del rol que usted ejecuta?
					¿Qué mejoraría del SI para que apoye de forma más eficiente su labor?
Identificar las brechas tecnológicas y profesionales	Establecer el perfil profesional de los peritos forenses	Perfil profesional	Nivel educativo	Capacidades grupo informática forense	¿Cuál es su nivel educativo?
			Años de experiencia		Años de experiencia en la labor de informática forense
					Años de experiencia en la Fiscalía General de la Nación
	Identificar los tipos de solicitudes más comunes	Clasificación de requerimientos	Porcentaje de requerimientos por cada tipo de actividad	Capacidades grupo informática forense	En promedio, del total de órdenes de trabajo que le han asignado, que porcentaje corresponde a cada tipo de actividad forense
			Porcentaje de requerimientos por cada tipo de dispositivo		En promedio, del total de elementos que le han asignado para examen forense, que porcentaje corresponde a cada tipo de dispositivo
	Conocer el nivel de conocimiento de los peritos forenses para atender los diferentes tipos de solicitudes	Conocimiento especializado	Nivel de conocimiento por tipo de actividad forense	Capacidades grupo informática forense	Seleccione su nivel de conocimiento para realizar cada tipo de actividad forense
					Seleccione su nivel de conocimiento para realizar examen forense de cada tipo de dispositivo
			Nivel de conocimiento por tipo de dispositivo		Para usted, que nivel de complejidad se puede presentar en el desarrollo de cada tipo de actividad forense
					Para usted, que nivel de complejidad se puede presentar en el examen forense de cada tipo de dispositivo

Objetivo General	Objetivo específico	Variable	Indicador	Instrumento	Ítem
	Establecer si existe sobrecarga laboral	Solicitudes atendidas	Cantidad de solicitudes atendidas en el mes	Capacidades grupo informática forense	En promedio, cuantas ordenes de trabajo le son asignadas al mes
	Conocer el desempeño de las herramientas tecnológicas que soportan las actividades periciales	Eficiencia de las herramientas tecnológicas	Nivel de eficiencia por tipo de actividad forense	Capacidades grupo informática forense	Evalúe la forma en que las herramientas tecnológicas disponibles en el grupo apoyan la atención de cada tipo de actividad forense
			Nivel de eficiencia por tipo de dispositivo		Evalúe la forma en que las herramientas tecnológicas disponibles en el grupo apoyan los procesos técnicos para el examen forense de cada tipo de dispositivo

Fuente: elaboración propia

3.6 Plan de análisis

Planteamiento de arquitectura inicial y arquitectura objetivo

A partir de las entrevistas de conocimiento del proceso se obtiene información relacionada con su funcionamiento actual y los aspectos que pueden ser mejorados; con base en los datos obtenidos se plantean un esquema de arquitectura inicial y una arquitectura objetivo.

Reducción de brechas

Con base en los resultados de la encuesta y el planteamiento de las arquitecturas inicial y objetivo se elabora una matriz para el análisis de brechas a fin de relacionar las capacidades tecnológicas y profesionales, roles, sistemas de información y otros que puedan ser requeridos para el cumplimiento de los objetivos planteados en el trabajo de arquitectura.

4 Análisis de resultados

Los datos recuperados durante la etapa de recolección de información deben ser sometidos a un proceso de “análisis o examen crítico que permita precisar las causas que llevaron a tomar la decisión de emprender el estudio y ponderar las posibles alternativas de acción para su efectiva atención” (Carrion Ortega & Gomez Crandall, 2003, p. 49), de esta manera, se pretende establecer los principales

aspectos a mejorar y desarrollar las opciones que mejor se adapten al proceso para la atención de solicitudes de informática forense.

4.1 Conocimiento del proceso

En la primera etapa del proceso metodológico se empleó un instrumento cualitativo para recolectar información que permitiera a los investigadores conocer el proceso mediante el cual se atienden las solicitudes de informática forense, en el nivel central de la Fiscalía General de la Nación. A través de entrevistas realizadas a los diferentes actores del proceso se obtuvo una descripción del ciclo de vida de cada solicitud, que fue corroborada aplicando una estrategia de triangulación de datos con nivel de análisis agregado (Arias Valencia, 1999).

Al analizar los diferentes puntos de vista se puede inferir que la atención de un requerimiento de informática forense atraviesa un proceso de cinco fases:

Tabla 6

Descripción del ciclo de vida de un requerimiento de informática forense

Rol Entrevistado	Fase	Actividad
Asistente Informática forense	Recepción de la solicitud	Verificación de los documentos Verificación de los elementos materiales probatorios
	Asignación de perito de informática forense	Registro en el SPOA. Asignación de la misión en conjunto con el coordinador
	Atención de la orden de trabajo de informática forense	Ejecución de la actividad por parte del perito asignado Generación del informe por parte del perito
	Cierre de la solicitud de informática forense	Entrega del informe a la autoridad requerida Almacenamiento del informe en los sistemas de información.
Perito Forense I	Recepción de la solicitud	La solicitud llega al coordinador quien revisa los parámetros básicos, establece si el grupo está en la capacidad de atender el requerimiento y revisa los términos de la orden judicial El asistente debe realizar las verificaciones y el registro de la solicitud en tres diferentes sistemas de información.
	Asignación de perito de informática forense	El coordinador realiza la asignación formal del requerimiento a un perito.
	Atención de la orden de trabajo de informática forense	El perito realiza la actividad solicitada y consigna el procedimiento realizado en un informe.
	Cierre de la solicitud de informática forense	Se realiza una revisión de pares sobre el informe generado. El jefe de grupo valida el resultado de la actividad y realiza la descarga de la actividad en el sistema de información misional. Se entrega la información a la autoridad solicitante.

Rol Entrevistado	Fase	Actividad
Perito Forense II	Recepción de la solicitud	La solicitud llega al nivel asistencial, quien le informa al coordinador.
	Asignación de perito de informática forense	El coordinador designa el o los peritos que trabajarán en el caso El asistente genera las órdenes de trabajo.
	Atención de la orden de trabajo de informática forense	El o los peritos asignados desarrolla la misión de trabajo y realiza un informe.
	Cierre de la solicitud de informática forense	El coordinador revisa el informe, realiza la descarga de la orden de trabajo y hace la entrega de la información a la autoridad solicitante. El asistente realiza el archivo con la copia del recibido.
Perito Forense III	Recepción de la solicitud	Recolección del material probatorio
	Atención de la orden de trabajo de informática forense	Análisis de dispositivos Entrega de resultados
	Cierre de la solicitud de informática forense	Almacenamiento de la información
Perito Forense IV	Emisión de la orden a policía judicial	La autoridad judicial emite la solicitud
	Recepción de la solicitud	El asistente verifica que las actividades solicitadas correspondan con las actividades que realiza el grupo; adicionalmente verifica el registro de la orden en el sistema de información SPOA
	Asignación de perito de informática forense	El coordinador se encarga de dar el visto bueno a la solicitud y designar un perito para su atención. El asistente registra la orden de trabajo en el sistema de información misional SIG y le entrega la orden y los elementos probatorios al perito encargado.
	Atención de la orden de trabajo de informática forense	El perito realiza el proceso forense respectivo y plasma los resultados dentro de un informe.
	Cierre de la solicitud de informática forense	Se realiza una validación de pares sobre el informe generado. El coordinador sustituto realiza la revisión del resultado emitido por el perito. El perito genera una copia de la información y se la entrega a la autoridad solicitante. El área asistencial se encarga de archivar el requerimiento.
Coordinador II	Emisión de la orden a policía judicial	Radicación de la solicitud en la recepción del grupo, atendiendo parámetros establecidos por la Dirección (oficio, orden a policía judicial, los EMP/EF y que estén incluidos en SPOA)
	Recepción de la solicitud	El encargado de la recepción (asistente) valida que se cumplan con los requisitos (que tenga términos trabajables, prudentes para realizar la labor en el tiempo que corresponde), cuando surgen dudas el coordinador o el encargado dirime la duda que se presente a la hora de la recepción.

Rol Entrevistado	Fase	Actividad
	Asignación de perito de informática forense	El coordinador o encargado evalúa la carga de trabajo de manera manual (tabla) y se determina quién es el próximo perito que debe recibir el trabajo de acuerdo a lo que tiene. No se ha podido llegar a la automatización en este proceso. Los peritos reciben por parte del encargado de la recepción la orden a policía judicial, la orden de trabajo y los elementos que deben analizar.
	Atención de la orden de trabajo de informática forense	Pasa a las áreas de laboratorio de donde sea el tipo de evidencia digital (móviles o digitales) en donde se ejecuta el proceso técnico de acuerdo a lo que haya solicitado el fiscal. El perito presenta un informe que es presentado o auditado por la coordinación y posteriormente entregado al fiscal o investigador del caso.
	Cierre de la solicitud de informática forense	El documento con la firma de recibido va a un proceso de descarga o validación de que ya fue entregado, se entrega a las personas que recepcionan el requerimiento (asistente) para que lo lleven a un archivo físico. El archivo se encuentra un tiempo en el archivo del grupo de acuerdo a las tablas de retención documental hasta que deban enviarse al Archivo General de la Nación.

Fuente: elaboración propia.

A partir de la información reunida se describen cada una de las fases identificadas; el resultado es la caracterización del proceso actual para la atención de solicitudes de informática forense que sirve de base para el desarrollo del trabajo de arquitectura.

Emisión de la orden a policía judicial: La orden a policía judicial es el documento por medio del cual la autoridad competente (Fiscal) ordena a la policía judicial adelantar actividades investigativas, para este caso específico es el documento emitido por el Fiscal del caso, indicando las actividades que debe desarrollar el Grupo de Informática Forense respecto a EMP y EF (Elementos Materiales Probatorios y Evidencia Física) de carácter digital, este documento también indica el plazo en el que dicha actividad se debe desarrollar (Término) e incluye la exposición jurídica que sustenta la actividad.

La orden a policía judicial se realiza en el sistema de información SPOA o sobre una plantilla de Word.

El Fiscal entrega la orden impresa a un Investigador del caso para que la allegue al grupo de Informática Forense junto con los EMP/EF. En ocasiones la orden a policía judicial y los EMP/EF se remiten por correspondencia al Grupo de Informática Forense.

Recepción de la solicitud: El Asistente administrativo del grupo de Informática Forense recibe las Órdenes a Policía Judicial y los EMP/EF que llegan al Grupo; el procedimiento es el siguiente:

- Verificar la vigencia de la orden.
- Verificar la competencia de lo solicitado.
- Validar que los EMP/EF sean los registrados en la orden.
- Solicitar el número de radicado de la orden en el sistema de gestión documental ORFEO.

El Asistente consulta frecuentemente con el Coordinador del Grupo o su suplente para asegurarse que la orden puede ser recibida.

Si se aprueba la verificación, el Asistente procede a:

- Recibir la orden a policía judicial y demás documentos que hayan sido anexados por el Investigador o el Fiscal, verificando que la orden se encuentre registrada en ORFEO, en caso de no ser así, el Asistente debe hacer el registro de la orden en dicho sistema de gestión documental.
- Recibir los EMP/EF, para ello el Asistente primero debe revisar que los elementos estén incluidos en el Sistema de Información Misional (SPOA) y proceder a hacer el registro manual de la continuidad sobre la cadena de custodia de cada uno de los EMP/EF y hace el mismo registro de continuidad pero de forma digital en el sistema de información SPOA.

Asignación de perito de informática forense: Una vez se han recibido los EMP/EF y la orden a policía judicial, el Asistente los entrega al Coordinador para que él defina a qué perito del Grupo asignará la atención de la solicitud, para esta actividad el Coordinador actual tiene un archivo Excel con el cual hace seguimiento de la carga laboral de cada uno de los peritos, con base en la información de este archivo toma la decisión de a quien asignar y comunica al Asistente del grupo para que realice la Orden de Trabajo.

El Asistente del Grupo transcribe en el sistema de información SIG, lo descrito en la Orden a Policía Judicial para asignar la Orden de Trabajo al perito seleccionado por el Coordinador para atender la solicitud. El asistente se encarga de informar al Perito sobre la asignación de la orden. El Asistente entrega la documentación de la orden a policía judicial y los EMP/EF al Perito.

Atención de la orden de trabajo de informática forense: El perito a quien le fue asignada la Orden de Trabajo recibe la documentación de la orden a policía judicial

y los EMP/EF; el perito es quien determina el momento y la forma en que atenderá la solicitud, de manera general, sigue las actividades descritas a continuación:

- Registra de forma manual el recibido de la orden a policía judicial
- Registra de forma manual la continuidad de la cadena de custodia de los EMP/EF y posteriormente hace el mismo registro, pero de forma digital en el sistema de información SPOA.
- Inicia la actividad técnica con una documentación fotográfica de los EMP/EF.
- Realiza la actividad técnica que corresponda a los EMP/EF y lo solicitado en la Orden a Policía Judicial.
- Documenta las actividades técnicas realizadas en un Informe de Laboratorio (Documento Word).
- Genera los resultados y los guarda en un medio de almacenamiento digital.
- El resultado guardado en el medio de almacenamiento digital se somete a procedimiento de cadena de custodia, por lo cual se diligencia un formato en Excel denominado “cadena de custodia” y posteriormente se transcribe para hacer el registro de la descripción de dicho elemento en el sistema de información SPOA.
- Al finalizar el informe, el perito lo remite a un par para su revisión.
- Hechas las revisiones, el perito descarga del sistema de información SIG la orden de trabajo y le comunica al Coordinador.
- El Coordinador aplica lista de chequeo en el sistema de información SIG, a la orden de trabajo descargada por el perito y se genera un número de informe.
- El perito registra en el archivo Word, el número de informe generado por el sistema de información SIG e imprime dos copias del informe, una para la Autoridad solicitante y otra para el archivo del Grupo.
- El informe de laboratorio impreso, el resultado grabado en el medio de almacenamiento digital en cadena de custodia y los EMP/EF recibidos, se entregan al Investigador del Caso o al Fiscal.
- A quien el perito le entregue el informe y los elementos, firma el recibido.
- El perito transcribe en el sistema de información SPOA apartes del informe de laboratorio hecho en Word, adjunta el informe en formato PDF y lo registra en estado REVISIÓN.

Cierre de la solicitud de informática forense: Una vez se ha hecho la entrega del informe impreso a la Autoridad Solicitante:

- El perito remite la copia del informe de laboratorio con firma de recibido al Coordinador para que este pase el registro del informe en el sistema de información SPOA a estado DEFINITIVO.
- El Coordinador actualiza el archivo Excel en donde administra la carga laboral del Grupo.

- El perito hace entrega de toda la documentación referente a la orden de trabajo al Asistente del Grupo.
- El Asistente escanea la documentación y hace el cierre de la solicitud haciendo el registro y archivo en el sistema de gestión documental ORFEO.
- El Asistente almacena la documentación en el archivo físico del Grupo.

4.2 Análisis de preocupaciones

Una de las actividades primordiales al iniciar un ejercicio de arquitectura empresarial es “identificar a los interesados clave del negocio (stakeholders), sus necesidades y preocupaciones, relacionadas con los objetivos estratégicos y las metas de la institución y de su entorno” (MINTIC, 2016, p.15); durante la etapa de conocimiento del proceso se indagó a los diferentes actores sobre sus preocupaciones y los aspectos que son susceptibles de mejorar. Los comentarios más relevantes se relacionan a continuación.

Tabla 7

Relación de las preocupaciones de los stakeholders

Rol entrevistado	Preocupación
Asistente de informática forense	Los funcionarios no utilizan el sistema de información ORFEO
	Existe represamiento de su trabajo porque los peritos no entregan los informes tan pronto finalizan su actividad
	La asignación de una orden de trabajo requiere alrededor de 20 pasos en el sistema de información misional SIG.
Perito informática forense I	No existe un estándar técnico de tiempos de atención para los diferentes tipos de requerimientos, lo cual dificulta la negociación de los tiempos con los fiscales y las otras autoridades que realizan solicitudes al grupo.
	Cada solicitud recibida debe registrarse en tres sistemas de información diferentes
	Todos los peritos deberían poder atender todos los tipos de elementos.
	No se garantiza que todos los peritos conocen y saben utilizar todas las herramientas tecnológicas que el grupo tiene a su disposición.
	La falta de comunicación de los peritos con las autoridades que emiten los requerimientos genera retrabajos, adicionalmente, el resultado de las solicitudes en muchas ocasiones no es el esperado.
Perito informática forense II	Se debe garantizar que las solicitudes tengan la información de contacto de la autoridad solicitante.
	Es importante que cada requerimiento tenga unos criterios de búsqueda definidos con el fin de sacar el mayor provecho de los recursos del grupo.
	Hace falta un sistema de información que controle la asignación de las órdenes de trabajo a los peritos informáticos.

Rol entrevistado	Preocupación
	El grupo necesita contar con gente joven que se desenvuelva con mayor naturalidad en los temas relacionados con redes sociales
Perito informática forense III	Se requiere empoderamiento de los peritos para interactuar con los despachos fiscales, antes de que se generen las órdenes a policía judicial, esto con el objetivo de ser más efectivos en la atención de los requerimientos.
	Hace falta mejorar la logística para el almacenamiento de la evidencia digital.
	No se cuenta con guías detalladas para la atención de todos los tipos de requerimientos.
	Se requieren capacitaciones en el manejo de las herramientas tecnológicas.
	Debe existir un portafolio de servicios socializado con las diferentes autoridades judiciales.
	Hace falta una base de datos de los casos atendidos por el grupo para aprovechar las lecciones aprendidas en la atención de cada una de las solicitudes.
Perito informática forense IV	Hace falta establecer unos tiempos de atención de requerimientos y que estos sean aprobados por el área de calidad.
	No existe un mecanismo formal para compartir el conocimiento adquirido en cada uno de los casos atendidos.
	La falta de comunicación de los peritos con los fiscales es causa común de retrabajos.
	Los sistemas de información SIG y SPOA deben integrarse para disminuir la complejidad del proceso de asignación
Coordinador de informática forense	Participar en el planeamiento de la diligencia para avizorar lo que puede pasar y poder crear planes de contingencia ante elementos no previstos.
	El perito solo debería realizar recolección especializada: bases de datos, registros, información contable, sitios web, análisis de software malicioso.
	Existe desconocimiento de alguno Fiscales que ordenan la realización de actividades en campo y al final dan como resultado que no era necesaria la participación de un perito (recolección física de elementos que cualquier investigador lo puede realizar).
	Abolir solicitudes verbales al menos debe quedar un sustento a través de un correo electrónico.
	Definición de términos prudentes: no se tiene cálculo preciso
	Procesos ejecutados por máquinas que no siempre es el mismo, y actualmente no se tiene una medición de dicho tiempo.
	Proporcionalidad de personas que realizan actividades periciales,
	Cantidad de equipos disponibles.
	Se debe dar prioridad u orden a las asignaciones, generalmente se distribuye en fila de llegada
Fiscal I	A medida que avanza el tiempo la cantidad de evidencia digital en los procesos es cada vez mayor. Lo cual está generando que personas más capacitadas no se puedan dedicar a hacer informes (tareas) más profundos. Personas que tienen la capacidad de hacer labores complejas están desarrollando labores muy sencillas.
	No hay interacción con el grupo a través de medios digitales. Las órdenes generadas en SPOA se tratan como un documento físico únicamente

Rol entrevistado	Preocupación
Fiscal II	Se requiere la presencia de los peritos en la etapa de planeación cuando se van a emitir las ordenes técnicas o las labores de informática forense que se van a requerir para que queden debidamente redactadas y no se incurra en imprecisiones Poner a disposición de todos los sujetos procesales todos los datos recolectados para que puedan ser utilizados o refutados

Nota: Tabla elaborada con datos obtenidos en las entrevistas. Fuente: elaboración propia.

Las preocupaciones listadas anteriormente se consolidan en cinco enunciados, enumerados según su nivel de criticidad:

1. No existe un estándar técnico de tiempos de atención para los diferentes tipos de requerimientos atendidos por el grupo.
2. No existen criterios de priorización para las solicitudes de informática forense que deben ser atendidas por el grupo.
3. Algunos requerimientos deben ser atendidos más de una vez debido a la falta de comunicación entre fiscales, investigadores y peritos forenses.
4. Una misma solicitud debe ser registrada en por lo menos tres sistemas de información diferentes.
5. No existe una base de datos de conocimiento ni un registro de lecciones aprendidas en la actividad pericial.

4.3 Evaluación de capacidades grupo Informática Forense

En la segunda fase del proceso metodológico se evalúan los tipos de solicitudes recibidas por el grupo de informática forense y la forma en que las capacidades técnicas y de recurso humano disponibles apoyan el proceso actual para la atención de requerimientos. A través de un instrumento cuantitativo de recolección de información se identifican las actividades más comunes realizadas por los peritos forenses, su nivel de conocimiento para atender cada tipo de solicitud y su concepto sobre el desempeño de las herramientas tecnológicas que apoyan la actividad pericial.

4.3.1 Solicitudes atendidas por el grupo

Actualmente el grupo de informática forense está dividido en dos áreas:

- Área de dispositivos móviles
- Área de otros dispositivos de almacenamiento

En la encuesta de capacidades aplicada a **18 peritos forenses** pertenecientes a las dos áreas del grupo, cuando se les preguntó sobre la cantidad de solicitudes que cada uno atiende durante un mes, se obtuvieron los siguientes resultados.

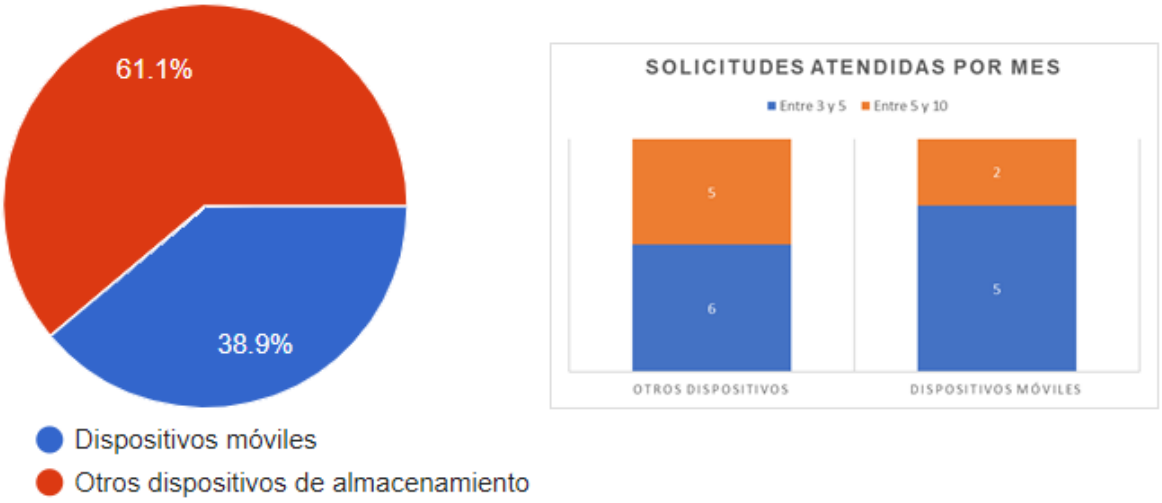


Figura 9. Promedio solicitudes atendidas por mes grupo Informática Forense, datos obtenidos de encuestas. Fuente: elaboración propia.

En el área de dispositivos móviles, el 72% de los encuestados atiende entre 3 y 5 requerimientos, mientras que el 28% restante atiende entre 5 y 10 solicitudes en el mismo periodo de tiempo; en contraste, los resultados para el área de otros dispositivos de almacenamiento reflejan que el porcentaje de peritos que atienden entre 5 y 10 solicitudes al mes asciende a un 45,4%. De lo anterior se puede inferir lo siguiente:

- Dentro de una misma área, la cantidad de asignaciones atendidas por cada perito forense no es uniforme, lo cual está generando dificultades para el cumplimiento de los tiempos de atención exigidos por las autoridades competentes, sobrecarga de trabajo en algunos peritos y subutilización de recursos técnicos y humanos disponibles.
- La cantidad promedio de requerimientos por perito en el área de dispositivos móviles es menor que la cantidad promedio atendida en el área de otros dispositivos de almacenamiento, esto hace que se subutilice el recurso destinado a la atención de dispositivos móviles y no se aproveche para atención de la demanda total de requerimientos que llegan al grupo.

4.3.2 Clasificación de las solicitudes de informática forense

En la encuesta de capacidades se preguntó a los participantes “del total de elementos que le han asignado para examen forense, qué porcentaje corresponde

a cada tipo de dispositivo"; Los resultados de las dos áreas se analizan a continuación.

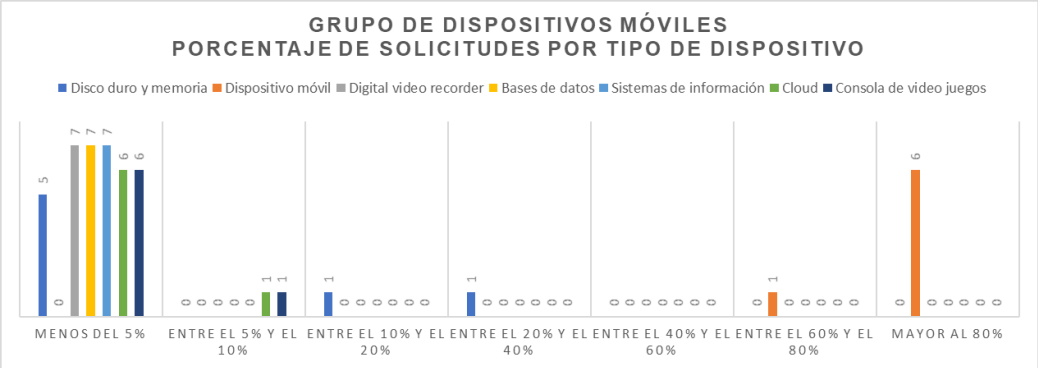


Figura 10. Porcentaje solicitudes por tipo de dispositivo, datos obtenidos de encuestas. Fuente: elaboración propia

Como era de esperarse, los peritos del grupo de dispositivos móviles dedican la gran mayoría de su tiempo a la atención de solicitudes relacionadas con dispositivos móviles, solo en casos muy específicos atienden requerimientos relacionados con otros tipos de elementos materiales probatorios. Por otro lado, en el grupo de otros dispositivos de almacenamiento, los elementos más destacados son los discos duros, las memorias extraíbles y en menor medida el digital video recorder (DVR). Las solicitudes que involucran bases de datos, sistemas informáticos, consolas de videojuegos y herramientas cloud se consideran esporádicas. La especialización por dispositivos está generando un desbalance en el aprovechamiento del recurso humano para la atención de la demanda total del grupo, más aún cuando se observa que los elementos con mayor número de requerimientos son los discos duros y otro tipo de medios de almacenamiento y se tiene personal dedicado exclusivamente para la atención de dispositivos móviles que no demuestran ser el de mayor volumen de requerimientos.

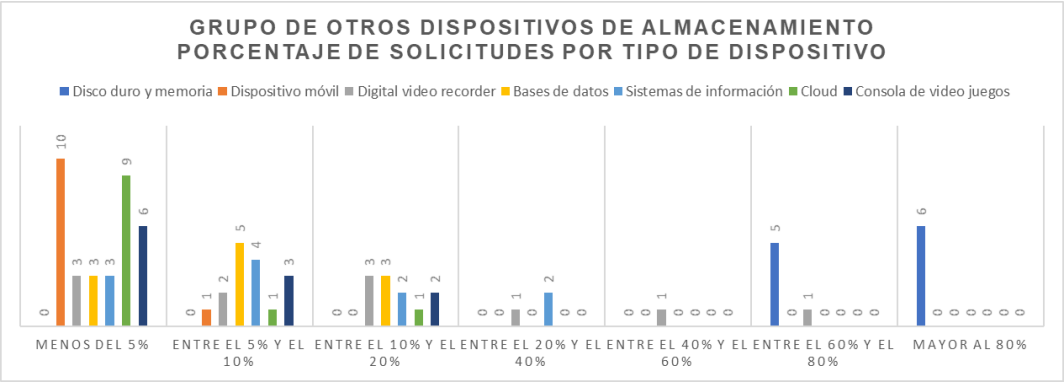


Figura 11. Porcentaje solicitudes por tipo de dispositivo, datos obtenidos de encuestas. Fuente: elaboración propia.

En otra de las preguntas se solicitó a los encuestados que confirmarán “del total de órdenes de trabajo que le han asignado, qué porcentaje corresponde a cada tipo de actividad forense”, para este caso, el análisis de resultados demuestra que las actividades más frecuentes en el grupo de informática forense son, en primer lugar, la extracción de información de dispositivos de almacenamiento, seguida por la obtención de imágenes forenses y el análisis de información. Considerando que la obtención de imágenes forenses no aplica para los dispositivos móviles, se puede inferir que este tipo de solicitudes recaen exclusivamente sobre el equipo de otros dispositivos de almacenamiento, demostrando que la división por áreas de especialización está creando ineficiencias en la atención del total de solicitudes que se reciben en el Grupo. Otros tipos de solicitudes como las diligencias judiciales y la recolección de elementos materiales probatorios se pueden clasificar como ocasionales.

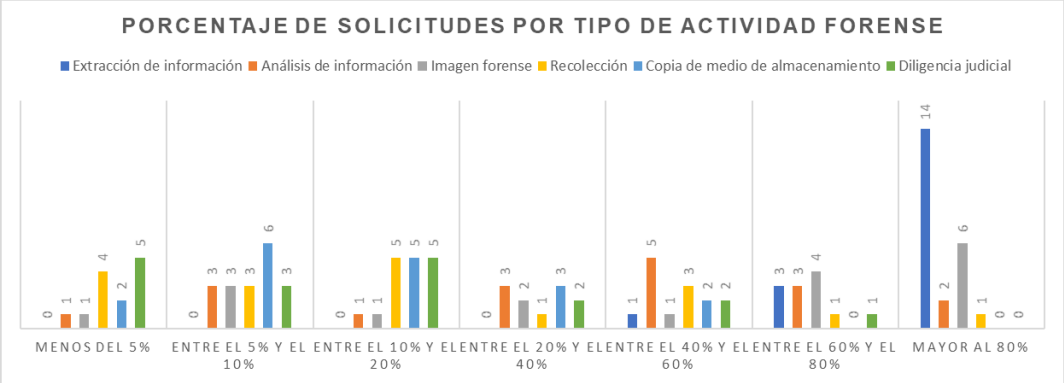


Figura 12. Porcentaje solicitudes por tipo de actividad forense, datos obtenidos de encuestas. Fuente: elaboración propia.

4.3.3 Capacidades del recurso humano

El proceso de análisis del recurso humano se inicia con el establecimiento de un perfil profesional. Los resultados de la encuesta aplicada a 18 peritos forenses indican que más del 80% de los encuestados son profesionales titulados y cerca del 61% tienen estudios de postgrado; por otro lado, el 88,9% de los participantes tienen más de 5 años de experiencia trabajando en la Fiscalía General de la Nación y un 55% tienen una experiencia superior a 10 años. En cuanto a su experiencia en actividades relacionadas con informática forense, el instrumento demuestra que el 55,5% tienen una trayectoria superior a 5 años y el 33,3% supera los 10 años de experiencia trabajando en el tema.

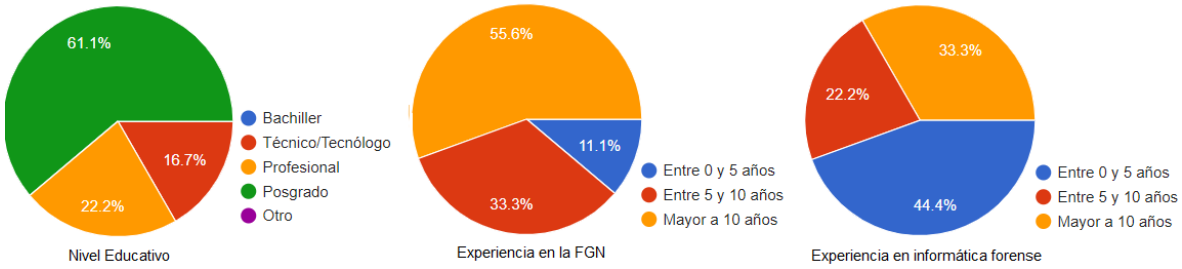


Figura 13. Perfil profesional y experiencia peritos grupo Informática Forense, datos obtenidos de encuestas. Fuente: elaboración propia.

Con base en los resultados obtenidos se establece el perfil profesional del perito forense, que corresponde a un profesional especializado con más de cinco años de experiencia en actividades relacionadas con la informática forense y una trayectoria superior a cinco años trabajando en la Fiscalía General de la Nación.

- **Conocimiento específico para la atención de solicitudes**

En este estudio de capacidades el conocimiento de los peritos forenses se evalúa en dos dimensiones, inicialmente, se indagó a los encuestados sobre su nivel de expertise para atender los diferentes tipos de solicitudes recibidas por el grupo; en general, los resultados reflejan que el equipo cuenta con un alto nivel de conocimiento para tramitar todos los tipos de requerimientos, sin embargo, el porcentaje de respuestas con nivel de conocimiento medio – bajo, en solicitudes relacionadas con imagen forense y análisis de información, debe ser tenido en cuenta como una oportunidad de mejora.

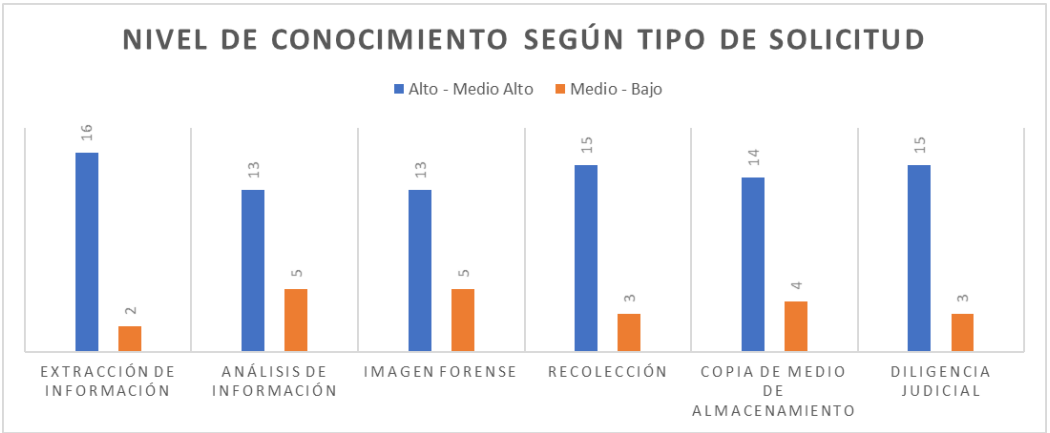


Figura 14. Conocimiento según tipo de solicitud, datos obtenidos de encuestas. Fuente: Elaboración propia.

En segundo lugar, se indagó a los participantes sobre su nivel de expertise para trabajar con diferentes tipos de elementos materiales probatorios; en este caso, los resultados demuestran que existe un nivel bajo de conocimiento para atender solicitudes relacionadas con elementos poco frecuentes como bases de datos, herramientas cloud y sistemas de información, por otro lado, se observa que el porcentaje de peritos con nivel de conocimiento medio – bajo, en elementos tan representativos como dispositivos móviles, discos duros y memorias extraíbles, alcanzan un 50% y un 45% respectivamente.

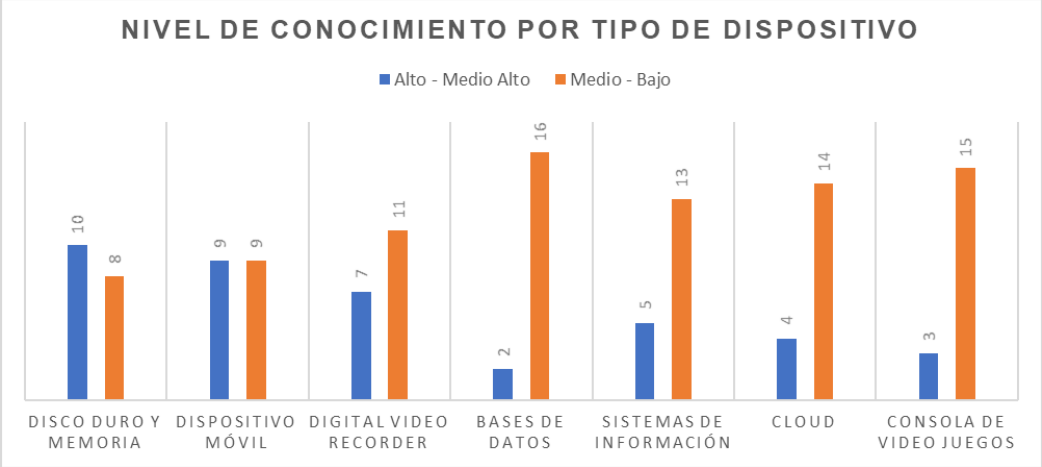


Figura 15. Conocimiento por tipo de dispositivo, datos obtenidos de encuestas. Fuente: elaboración propia.

Estas cifras demuestran que en el grupo de informática forense se requiere un fortalecimiento de los conceptos técnicos necesarios para atender requerimientos relacionados con los diferentes tipos de elementos materiales probatorios, adicionalmente, se debe trabajar en la homogenización del conocimiento de los peritos para que estén en la capacidad de atender solicitudes que involucren cualquier tipo de dispositivo de almacenamiento, este fortalecimiento puede estar a cargo del mismo grupo para un nivel básico de atención; para un nivel más avanzado se debe contar con organismos de capacitación o entidades homólogas a nivel nacional o internacional, especializados en temas de informática forense.

4.3.4 Desempeño de las herramientas tecnológicas

En la encuesta de capacidades de informática forense se les pidió a los peritos del grupo que evaluaran la forma en que las herramientas tecnológicas disponibles,

apoyan la atención de los diferentes tipos de requerimientos; los resultados de la encuesta reflejan un alto grado de eficiencia apoyando actividades relacionadas con extracción de información, copia de almacenamiento y generación de imágenes forenses; sin embargo, la calificación recibida en el ítem de **análisis de información** sugiere que los recursos tecnológicos para esta actividad en particular pueden mejorarse. En este particular los funcionarios del grupo indican que cuentan con herramientas de hardware y software para la ejecución de las diversas actividades técnicas de informática forense; en relación a la obtención de imágenes forenses el grupo cuenta con herramientas de hardware como duplicadores TD3 de Tableu y software como FTK Imager y BlackBag para equipos Mac. Para la extracción y análisis de información en dispositivos móviles se cuenta con tres herramientas que son UFED, XRY y Oxygen; para otros dispositivos de almacenamiento se emplea principalmente FTK (Forensic Tool Kit) y EnCase, BlackBag e Internet Evidence Finder para requerimientos específicos. La copia de medios de almacenamiento digital se realiza a través de software comercial como Nero, ImgBurn, entre otros. Para la recolección de medios de almacenamiento digital no se emplean herramientas ya que es un proceso netamente manual, sin embargo, cuando se requiere recolectar información digital almacenada en algún sistema de información o base de datos se emplean las herramientas de software para obtención de imágenes forenses. Los funcionarios destacan que cuentan con computadores portátiles y fijos con altas prestaciones (memoria RAM y procesador) para dar a las herramientas de software los niveles de rendimiento que requieren.

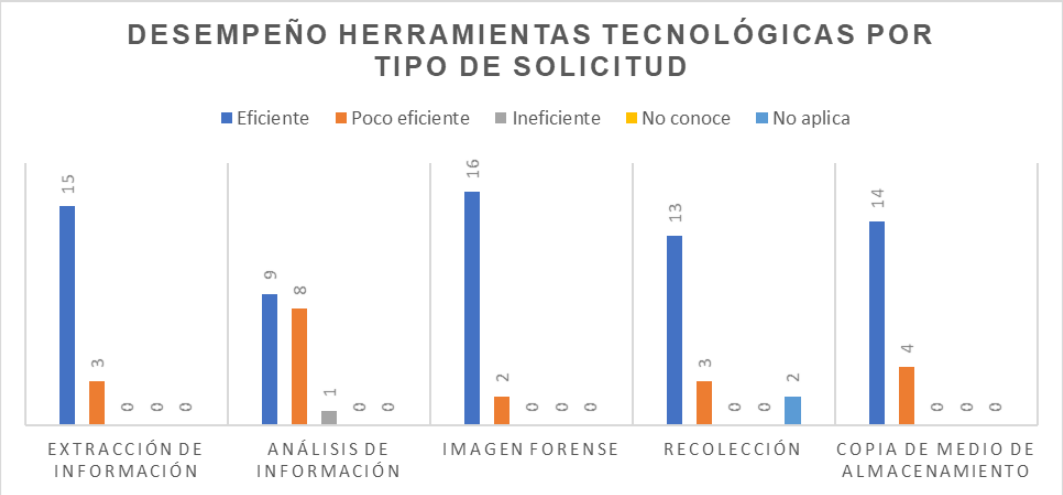


Figura 16. Desempeño herramientas tecnológicas por tipo de solicitud, datos obtenidos de encuestas. Fuente: elaboración propia

Otro de los interrogantes de la encuesta evaluó la forma en que las herramientas tecnológicas apoyan los procesos técnicos para el examen forense de diferentes tipos de dispositivos; los resultados obtenidos señalan que las herramientas son

efectivas para el procesamiento de discos duros, memorias extraíbles y dispositivos móviles, con respecto a los DVR, el porcentaje de respuestas negativas asciende al 50%, valor considerablemente alto y que debe ser tenido en cuenta como oportunidad de mejora (para ésta actividad forense los funcionarios del grupo indican que cuentan con una herramienta de software denominada DVR Examiner con la cual es posible hacer este tipo de exámenes forenses, sin embargo manifiestan que solo algunas personas están capacitadas para hacer uso de ella, además de que solo cuentan con una licencia para atender la totalidad de requerimientos de este tipo); por último, los porcentajes obtenidos para bases de datos, sistemas de información, herramientas cloud y consolas de video juegos manifiestan que las capacidades tecnológicas disponibles para procesar este tipo de dispositivos, son insuficientes, los funcionarios manifiestan que no cuentan con herramientas forenses con las cuales puedan atender este tipo de requerimientos o no conocen de su existencia en el Grupo, por lo cual estos requerimientos se atienden a través del conocimiento que tienen unos pocos funcionarios sobre la forma en que operan los diferentes sistemas de bases de datos y sistemas de información, obteniendo backup o copia de los mismos para luego ser restaurados para su análisis; en cuanto a los temas de cloud y otro tipo de dispositivos, el conocimiento de los funcionarios respecto a la forma de atender de manera adecuada un requerimiento forense de este tipo es incipiente, no todos los funcionarios saben la forma y tampoco conocen de la existencia de herramientas forenses en el grupo con las cuales se puedan soportar.

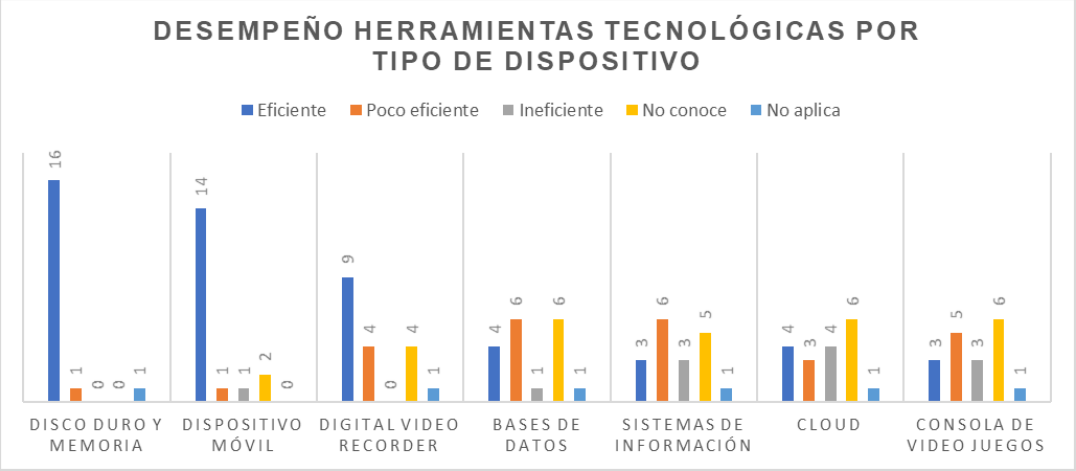


Figura 17. Desempeño herramientas tecnológicas por tipo de dispositivo, datos obtenidos de encuestas. Fuente: elaboración propia

Las conclusiones producto del análisis de capacidades se relacionan a continuación:

Tabla 8

Conclusiones encuesta de capacidades de informática forense

Pregunta de investigación	Conclusión	Nivel de Impacto
¿Cuál es su nivel educativo?	El perfil profesional del perito forense, que corresponde a un profesional especializado con más de cinco años de experiencia en actividades relacionadas con la informática forense y una trayectoria superior a cinco años trabajando en la fiscalía general de la nación.	Alto
Años de experiencia en la Fiscalía General de la Nación		
Años de experiencia en la labor de informática forense		
¿A qué área de trabajo pertenece dentro del grupo de Informática Forense?	La estrategia de dividir el equipo de peritos en dos áreas independientes dificulta la distribución uniforme de la carga laboral, lo cual se traduce en un uso ineficiente del recurso humano disponible	Alto
En promedio, cuantas ordenes de trabajo le son asignadas al mes		
En promedio, del total de órdenes de trabajo que le han asignado, que porcentaje corresponde a cada tipo de actividad	El grupo de informática forense está dedicado principalmente a la atención de solicitudes relacionadas con extracción de información, imagen forense y análisis de información. Los demás tipos de requerimientos son ocasionales.	No aplica
En promedio, del total de elementos que le han asignado para examen forense, que porcentaje corresponde a cada tipo de dispositivo	Los elementos materiales probatorios recibidos por el grupo de informática forense son en su mayoría discos duros, memorias extraíbles, dispositivos móviles y DVRs. Los demás tipos de dispositivos se catalogan como esporádicos	No aplica
Seleccione su nivel de conocimiento para realizar cada actividad forense	Se recomienda realizar capacitaciones para homogenizar el conocimiento en temas relacionados con la elaboración de imágenes forenses y el análisis de información	Medio
Seleccione su nivel de conocimiento para realizar examen forense de cada tipo de dispositivo	Se requiere un fortalecimiento de los conceptos técnicos necesarios para atender requerimientos relacionados con los diferentes tipos de elementos materiales probatorios, adicionalmente, se debe trabajar en la homogenización del conocimiento de los peritos para que estén en la capacidad de atender solicitudes que involucren cualquier tipo de dispositivo de almacenamiento.	Alto
Evalúe la forma en que las herramientas tecnológicas disponibles en el grupo apoyan la atención de los diferentes tipos de requerimientos	Evaluar el desempeño de las herramientas tecnológicas disponibles para la atención de solicitudes de análisis de información. Verificar si se requiere dar capacitación a los peritos o es necesario buscar otras opciones en el mercado	Medio
Evalúe la forma en que las herramientas tecnológicas disponibles en el grupo apoyan los procesos técnicos para el examen forense de los diferentes tipos de dispositivos	Evaluar el desempeño de las herramientas tecnológicas disponibles para la atención de solicitudes relacionadas con dispositivos DVR. Verificar si se requiere dar capacitación a los peritos o es necesario buscar otras opciones en el mercado	Medio
	Capacitar a los peritos forenses sobre la forma en que las herramientas tecnológicas disponibles pueden apoyar la atención de solicitudes relacionadas con bases de datos, y sistemas de información, locales o cloud.	Bajo
	Evaluar el desempeño de las herramientas tecnológicas disponibles para la atención de solicitudes relacionadas con bases de datos y sistemas de información. Verificar si es necesario buscar otras opciones en el mercado	Bajo

Nota: Tabla elaborada con datos analizados de las encuestas. Fuente: elaboración propia.

5 Propuesta

En desarrollo del ejercicio de arquitectura propuesto se hará un recorrido por las fases del Método de Desarrollo de Arquitectura (ADM) de TOGAF, en algunas fases será necesario complementar el ejercicio con otro marcos, buenas prácticas y estándares.

5.1 Fase preliminar

Esta fase permite preparar a la organización para realizar el trabajo de arquitectura, definiendo los principios generales, identificando los impulsores, determinando el método y las herramientas requeridas. El entregable principal de esta fase es la Solicitud de Trabajo de Arquitectura (Request for Architecture Work) (The Open Group, 2018).

5.1.1 Áreas de negocio impactadas

El ejercicio de arquitectura empresarial se enfoca en la identificación de oportunidades de mejora que permitan optimizar el proceso para la atención de solicitudes en el Grupo de Informática Forense Nivel Central del Cuerpo Técnico de investigación, Fiscalía General de la Nación. El mayor impacto se ve reflejado en el desarrollo de las actividades que conforman el proceso y las personas involucradas en el mismo, en este caso son los funcionarios del grupo y las áreas que hacen uso de los servicios que presta el mismo, principalmente Fiscales e Investigadores.

5.1.2 Alcance de la propuesta de arquitectura

Acogiendo el Método de Desarrollo de Arquitectura (ADM) de TOGAF, el ejercicio cubre hasta la fase de Migración (F: Migration Planning). Inicialmente se desarrollan las fases preliminar y visión, en las cuales se da inicio a la arquitectura empresarial y se establece una etapa conceptual en la que se define el contexto y la motivación para llevar a cabo el ejercicio, se precisan los objetivos, misión, visión, los principios de arquitectura, se identifican los stakeholder, entre otros. Continuando con lo propuesto por el ADM, se ejecutan las fases de arquitectura de negocio, sistemas de información y tecnología (B: Bussines architecture, C: Information systems architecture y D: Technolgy architecture) en las cuales se establece la línea base de arquitectura (AS-IS Architecture) y la arquitectura objetivo (TO-BE Architecture) para cada dominio, una vez definidas las arquitecturas AS-IS y TO-BE se lleva a cabo el análisis de brechas y se finaliza con la generación de recomendaciones de alto nivel en cumplimiento de las fases de oportunidad de solución y plan de migración (E: Oportunities and Solutions y F: Migration Planning).

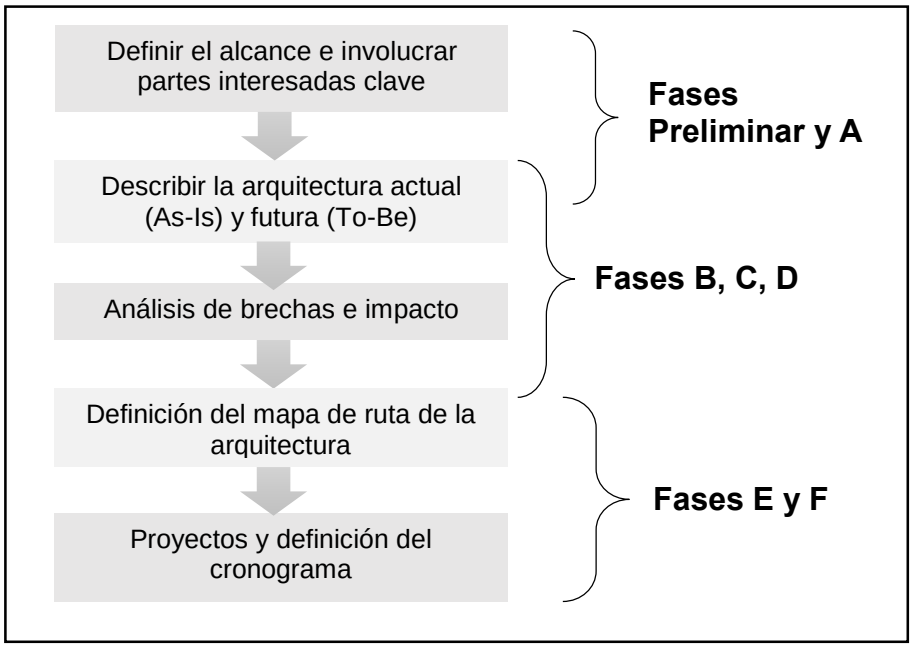


Figura 18. Fases ADM de TOGAF, Adaptada de Desfray, P., & Raymond, G. (2014). Modeling enterprise architecture with TOGAF: A practical guide using UML and BPMN. Burlington: Elsevier Science.

5.1.3 Principios de arquitectura

El estándar TOGAF versión 9.2 de The Open Group (2018) define los principios como reglas y pautas generales para el uso e implementación de todos los recursos y activos de TI en la organización que forman la base para la toma de decisiones futuras de TI.

Considerando los principios recomendados por TOGAF, el Marco de Referencia de Arquitectura TI Colombia y el PETIC 2017-2020 de la FGN, a continuación, se enumeran los principios que regirán el ejercicio de arquitectura empresarial para la optimización del proceso para la atención de solicitudes de informática forense en la FGN, los detalles de cada principio se registran en el catalogo de principios.

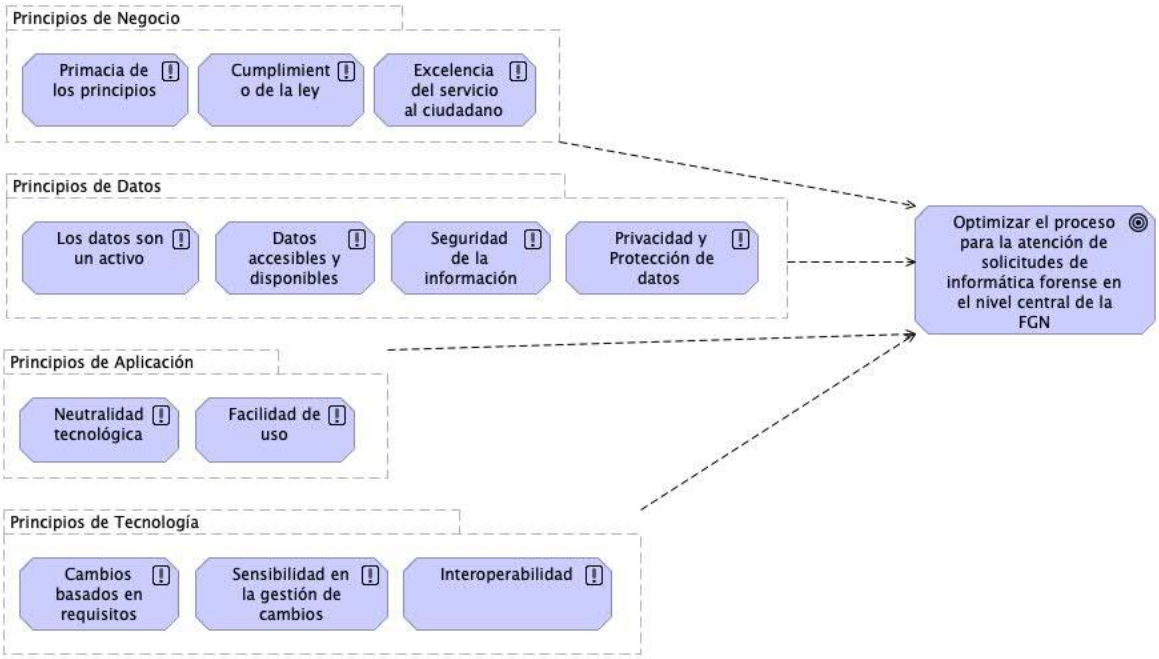


Figura 19. Diagrama archimate, principios ejercicio de arquitectura empresarial. Fuente: elaboración propia.

Tabla 9

Principios de arquitectura

Categoría	**Principio**	**Descripción**
Principios de negocio	Primacia de los principios	Los principios aplican a toda la institución
	Cumplimiento de la ley	Cumplir con los deberes de acuerdo con la Constitución y la ley, todos los procesos que se implementan en la FGN cumplen con las leyes, políticas y regulaciones vigentes
	Excelencia del servicio al ciudadano	Propender por el fin superior de fortalecer la relación de los ciudadanos con el Estado
Principios de datos	Los datos son un activo	Los datos constituyen un activo que tiene enorme valor estratégico para la institución, por lo que este activo debe ser gestionado adecuadamente
	Datos accesibles y disponibles	La arquitectura institucional debe propender por que los datos estén disponibles en el momento adecuado, en los tiempos esperados y para las personas apropiadas; con el fin de que la Institución obtenga el mayor valor de su información en la toma de decisiones.
	Seguridad de la información	La gestión de información debe contemplar la seguridad en su acceso y divulgación.
	Privacidad y protección de datos	Política de privacidad que instruye a los funcionarios en la recolección y uso de información personal, así como en los derechos que tienen los usuarios.
Principios de aplicación	Neutralidad tecnológica	El Estado garantiza la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y

Categoría	Principio	Descripción
		normativas de los organismos internacionales competentes e idóneos en la materia, que permitan fomentar la eficiente prestación de servicios, emplear contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones; garantizar la libre y leal competencia y que su adopción sea armónica con el desarrollo ambiental sostenible
	Facilidad de uso	Las aplicaciones son fáciles de usar. La tecnología subyacente es transparente para los usuarios.
Principios de tecnología	Cambios basados en requisitos	Los cambios en las aplicaciones y la tecnología solo se realizan en respuesta a las necesidades institucionales.
	Sensibilidad en la gestión de cambios	Los cambios en el entorno de información empresarial se implementan de manera oportuna.
	Interoperabilidad	Fortalecer los esquemas de Interoperabilidad que estandaricen y faciliten el intercambio de información entre entidades y sectores, manejo de fuentes únicas de información y la habilitación de servicios.

Fuente: elaboración propia.

5.1.4 Solicitud del trabajo de arquitectura

Como resultado de la fase preliminar se crea la solicitud del trabajo de arquitectura (Request for Arquitecture Work), con este documento se da inicio al ciclo de desarrollo de la arquitectura y se crea con el fin de analizar y proponer una solución que optimiza el proceso para la atención de solicitudes de informática forense; en este documento se incluye la siguiente información:

- Patrocinadores
- Misión de la organización
- Objetivos de negocio
- Plan estratégico
- Límites de tiempo
- Limitaciones organizativas
- Presupuesto y restricciones financieras.

5.2 Fase de Visión

Es la fase inicial del método de desarrollo de arquitectura ADM, prepara las siguientes fases a través de una representación general de las arquitecturas de línea base y objetivo, en esta etapa las representaciones son de muy alto nivel (Desfray & Reymon, 2014).

5.2.1 Establecer el proyecto de arquitectura

De acuerdo con lo definido en el PETIC 2017-2020 de la FGN (2017a): “Todas las iniciativas (…) que involucren componentes de TI deberán gobernarse y administrarse bajo el esquema de gestión de proyectos establecido por la Fiscalía General de la Nación”.

En este sentido, el manual para la identificación, formulación e inscripción de proyectos en el banco de proyectos de la FGN (2018a) establece una metodología de actividades dividida en tres grupos:

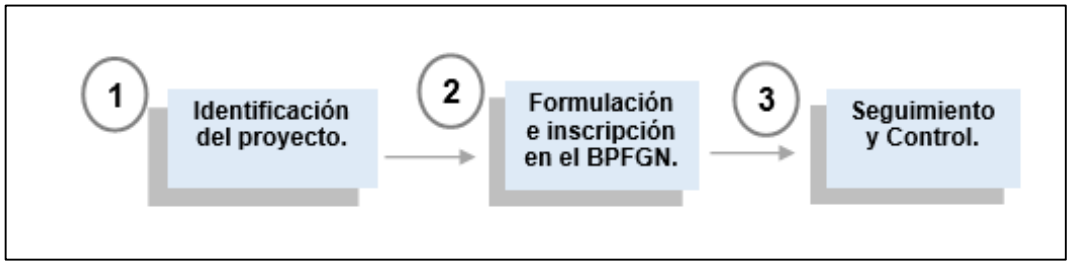


Figura 20. Fases identificación, formulación e inscripción de proyectos en el banco de proyectos de la FGN. Fuente: Fiscalía General de la Nación. (2018a). *Manual para la identificación, formulación e inscripción de proyectos en el banco de proyectos.* Manuscrito no publicado.

El primer módulo presenta los conceptos y metodologías que permiten dar forma al proyecto, el segundo hace relación a los formularios y modelos que se deben diligenciar para inscribir los proyectos en el Banco de Proyectos de la Fiscalía General de la Nación (BPFGN) y finaliza con los mecanismos para el “seguimiento y control de los proyectos” (FGN, 2018a).

5.2.2 Partes interesadas (Stakeholders)

Los grupos que pueden resultar beneficiados por el proyecto de arquitectura empresarial, se definieron con base en el organigrama de la Entidad y la información recolectada en las entrevistas.

Figura 21. Organigrama Fiscalía General de la Nación. Fuente: Fiscalía General de la Nación. (2019b). Estructura orgánica de la Fiscalía General de la Nación. Recuperado de https://www.fiscalia.gov.co/colombia/la-entidad/organigrama/

Para la identificación de las partes interesadas, se consideraron los cuestionamientos propuestos por Desfray & Reymon (2014):

- ¿Quién define metas?
- ¿Quién gana y quién pierde con este cambio?
- ¿Quién controla el proceso de transformación?
- ¿Quién diseña nuevos sistemas?
- ¿Quién tomará las decisiones?
- ¿Quién adquiere los sistemas de TI y quién decide qué comprar?
- ¿Quién controla los recursos?
- ¿Quién tiene o controla las habilidades especializadas necesarias?
- ¿Quién influye en el proyecto?

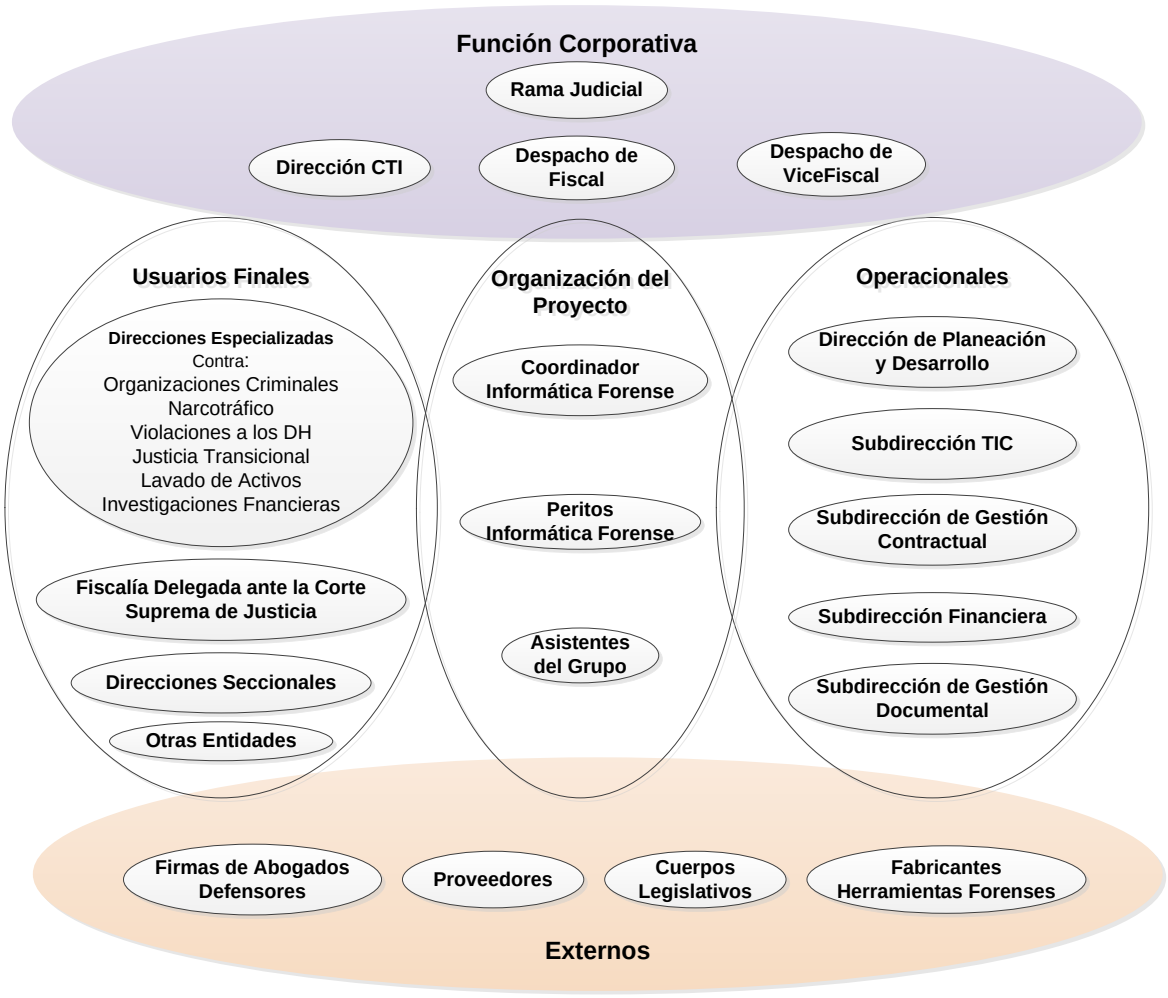


Figura 22. Partes interesadas ejercicio de arquitectura empresarial. Fuente: elaboración propia.

Una vez resueltas estas preguntas, TOGAF recomienda que se aclare el grado de involucramiento de cada parte interesada a través de una matriz de poder; esta identificación permitirá determinar cuáles son las personas o áreas clave para el proyecto de arquitectura (The Open Group, 2018), (Desfray & Reymon, 2014)

PODER	Alto	Mantener Satisfechos	Jugadores Clave
	Bajo	Mínimo Esfuerzo	Mantener Informados
		Bajo	Alto
		NIVEL DE INTERES	

Figura 23. Matriz Poder Interés. Fuente: Adaptado de The Open Group. (2018). TOGAF® standard, version 9.2. Retrieved from http://pubs.opengroup.org/architecture/togaf92-doc/arch/

PODER	Alto	• Despacho Fiscal • Despacho Vice Fiscal • Cuerpos Legislativos • Direcciones Especializadas • Fiscalía Delegada ante la Corte Suprema de Justicia • Direcciones Seccionales	• Dirección CTI • Dirección Ejecutiva • Dirección de Planeación • Subdirección TIC • Subdirección Financiera
	Bajo	• Otras Entidades • Proveedores • Fabricantes herramientas forenses. • Firmas abogados defensores • Asistentes Grupo Informática Forense.	• Personal del Grupo Informática Forense. • Subdirección Gestión Contractual. • Subdirección de Gestión Documental
		Bajo	Alto
		NIVEL DE INTERES	

Figura 24. Matriz Poder de Interés ejercicio de arquitectura empresarial. Fuente: elaboración propia.

5.2.3 Objetivos e impulsores de negocio

Con base en la información obtenida de las entrevistas de conocimiento del proceso a continuación se hace una presentación de la vista motivacional del ejercicio de arquitectura empresarial.

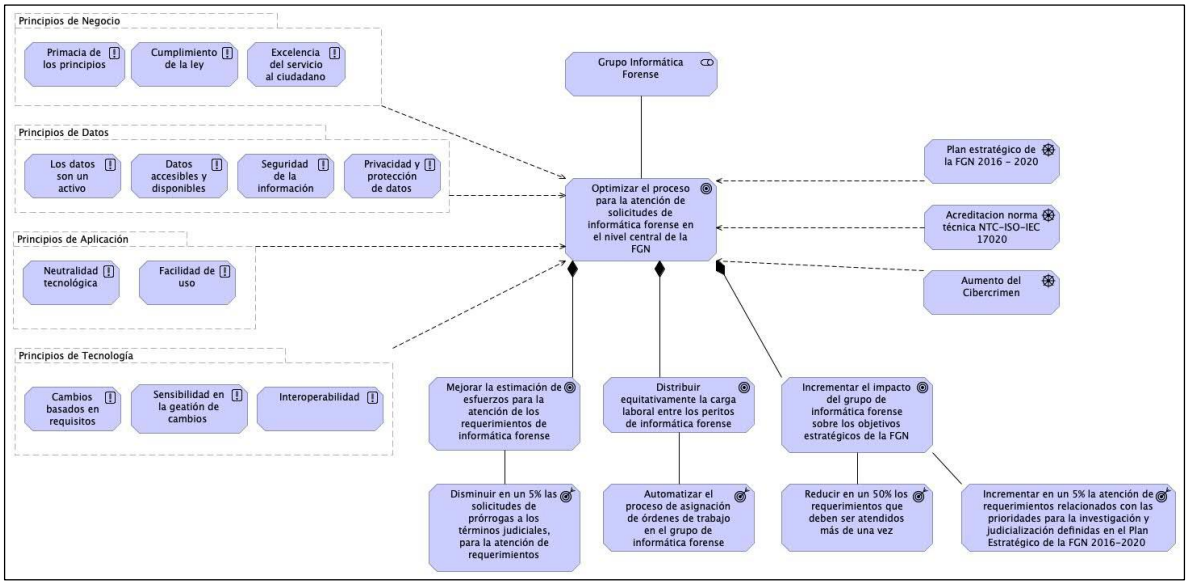


Figura 25. Diagrama motivacional. Fuente: elaboración propia

En un diagrama motivacional se modelan los conceptos motivacionales o razones, que subyacen en el diseño de la arquitectura empresarial. Estas motivaciones influyen, guían y restringen el diseño. Las motivaciones están representadas por objetivos, principios, requisitos y restricciones, las metas representan el resultado deseado (The Open Group, 2013).

5.2.4 Evaluar capacidades

Con el fin de identificar el grado de preparación que tiene el Grupo de Informática Forense para abordar los cambios propuestos por la arquitectura empresarial, se inicia con la evaluación de madurez de la Gestión de TI en la Entidad, la cual ésta documentada en el Plan Estratégico de Tecnologías de la Información y las Comunicaciones de la FGN - PETIC 2017-2020. A través de la herramienta IT4+_TOOL2_RupturasEstrategicas.xslx en el PETIC se evaluó el estado actual de los dominios de Gobierno de TI, Estrategia de TI, Gestión de Información, Sistema de información, Servicios tecnológicos, Uso y apropiación dando como resultado el siguiente panorama:

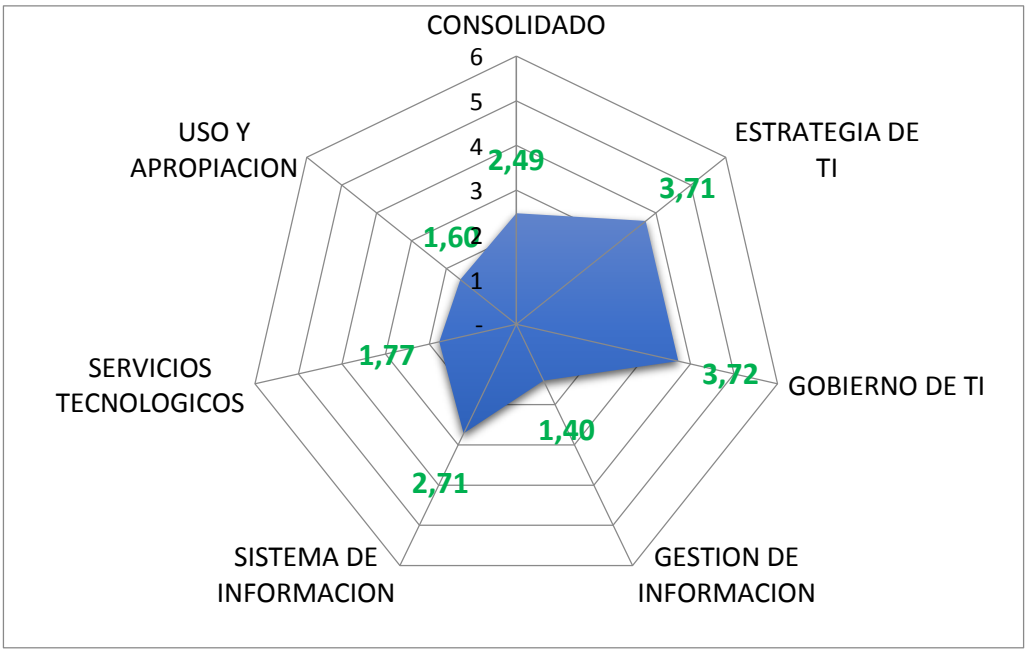


Figura 26. Consolidado madurez de gestión de TI. Fuente: Fiscalía General de la Nación. (2017a). *Plan estratégico de tecnologías de la información y las comunicaciones FGN 2017-2020*. Manuscrito no publicado.

Para el presente trabajo se considerarán solo los resultados de la evaluación de madurez para los dominios de Gestión de Información, Sistemas de información, Servicios tecnológicos, Uso y apropiación, que de forma análoga atenderían algunas de las fases del ADM de TOGAF.

- **Información**

El resultado de la evaluación es de 1.40, lo cual indicaría que en la Entidad existe la necesidad de desarrollar este dominio, llevando a cabo "acciones (…) de gestión, diseño de servicios, gestión de calidad, gestión del ciclo y (…) análisis de la información" (FGN, 2017a).

De la evaluación de madurez frente al dominio información, a continuación, se indican los factores considerados relevantes para el entendimiento del estado actual, a fin de dar inicio al ejercicio de arquitectura empresarial propuesto:

– A nivel de gestión de la información, la Entidad requiere información de calidad generada desde los procesos de gestión, registros administrativos o fuentes automatizadas; principalmente para la toma de decisiones y para mantenerla

disponible para las partes interesadas de acuerdo a los servicios que ofrece la Fiscalía. (FGN, 2017a).

- Para optimizar se deben definir “las fuentes, (..) los usuarios, los flujos” de información “y las condiciones de intercambio, que se generen a través de mecanismos sencillos, confiables y seguros” (FGN, 2017a).

- El diseño de servicios de información debe estar orientado a las necesidades de las partes interesadas y a la generación de valor.

- “El diagnóstico identificó debilidades en el modelo de operación actual”, entre ellas ésta el hecho de que se presentan “re-procesos en la investigación (…) ((...) doble creación de órdenes a PJ [Policía Judicial] en SPOA y en SIG) además el “manejo de expedientes físicos y apilamiento de los mismos” (FGN, 2017a).

- **Sistemas de Información**

El resultado de la evaluación es 2.71, lo cual indica que se debe fortalecer este dominio mediante la mejora “del modelo de gestión, arquitectura, desarrollo, mantenimiento, implantación, gestión del cambio, operación y soporte funcional de los sistemas de información” (FGN, 2017a).

Dentro de las dificultades en la operación de los sistemas de información se resaltan las siguientes:

- La misma información debe registrarse manualmente en más de una aplicación, esto debido a la insuficiente integración entre las aplicaciones (FGN, 2017a).

- Frente a la “percepción de los funcionarios, menos del 70% considera que las aplicaciones SPOA, SIG, Orfeo (…) cubren los procesos” (FGN, 2017a).

- **Servicios tecnológicos**

El resultado de la evaluación es de 1.77, por lo cual se debe fortalecer este dominio a través de la mejora “del modelo de necesidades de capacidad tecnológica, arquitectura de la infraestructura, capacidad de los servicios, gestión de la operación y prestación del servicio” (FGN, 2017a).

- **Uso y apropiación**

La evaluación es de 1.60, lo cual indica la necesidad de fortalecer este dominio optimizando entre otras acciones las siguientes:

- Planear el cambio cuando se van a modificar o introducir nuevos servicios y definir los incentivos para su adopción.
- Habilitar “herramientas para la gestión del cambio, analítica de información, gerenciales para la gestión del cambio”.

El diagnóstico para el dominio de Uso y Apropiación también registra lo siguiente:

- “Existen funcionarios que no utilizan frecuentemente los sistemas de información.
- No existe una estrategia documentada y divulgada de uso y apropiación” (FGN, 2017a)

Adicional y considerando que la Entidad ha definido que “los servicios se deben implementar bajo los lineamientos SOA (arquitectura orientada a servicios)” (FGN, 2017a), resulta óptimo evaluar las capacidades tomando como base el modelo de madurez e integración de servicios de The Open Group (OSIMM), el cual especifica cómo medir los niveles de integración de servicios de una organización, sus sistemas de TI y aplicaciones empresariales (The Open Group, 2016).

OSIMM define un conjunto de siete dimensiones que representan diferentes vistas de una organización: negocio, organización y gobierno, método, aplicación, arquitectura, información, infraestructura y gestión. Los siete niveles de madurez de SOA son: silo, integrado, componente, servicio, servicios compuestos, servicios virtualizados, servicios dinámicamente reconfigurables (The Open Group, 2016)

El nivel de madurez de cada dimensión se evalúa haciendo coincidir los indicadores de madurez con los atributos del nivel de madurez (The Open Group, 2016)

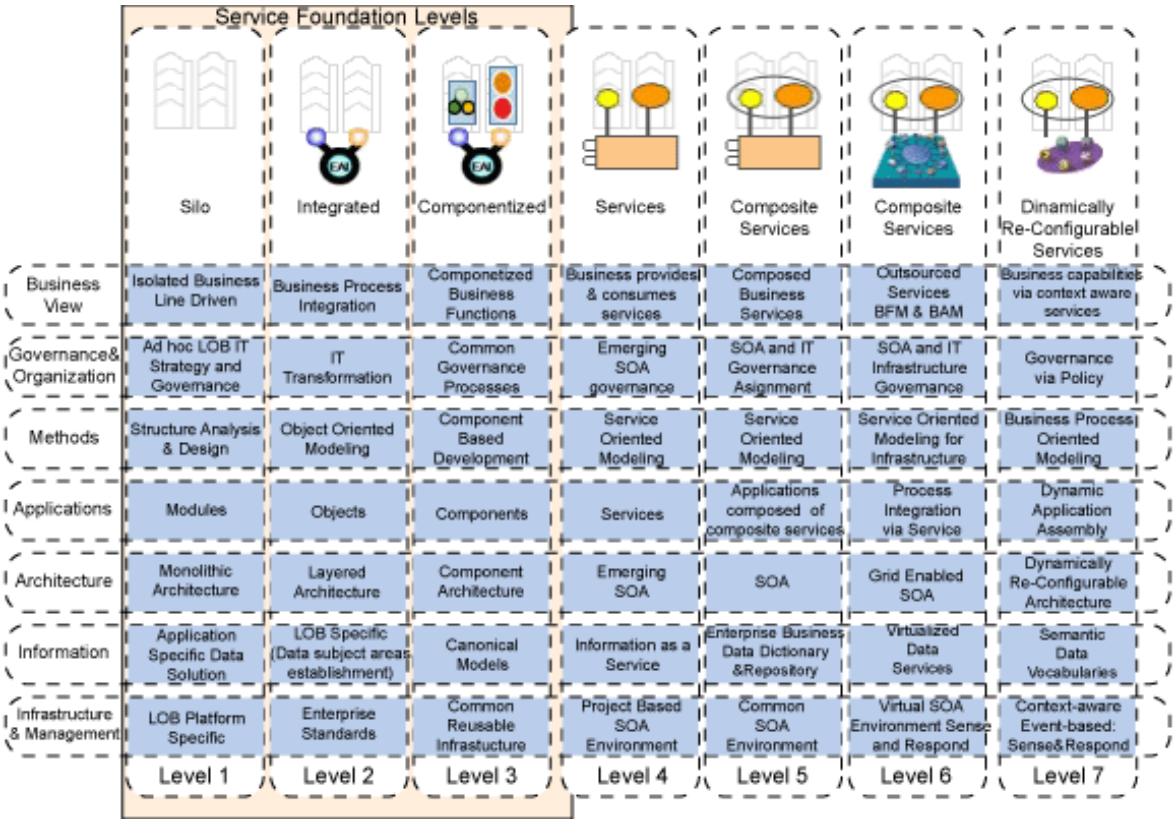


Figura 27. Matriz de madurez de OSIMM. Fuente: The Open Group. (2016). The open group service integration maturity model (OSIMM) version 2 – the model. Recuperado de http://www.opengroup.org/soa/source-book/osimmv2/p2.htm

Para evaluar las capacidades del proceso se considerarán solamente las dimensiones de negocio, información e infraestructura.

- **Dimensión de negocio**

Una vez adelantada la fase de entendimiento del proceso para la atención de solicitudes en el Grupo de Informática Forense se puede determinar que los procesos de negocio no están formalmente definidos ni documentados y que la arquitectura empresarial no es un elemento de la estrategia del Grupo; por consiguiente, el nivel de madurez para la dimensión de negocio se ubicaría en 1 es decir Silo.

- **Dimensión de información**

Los datos obtenidos a través de la evaluación permiten concluir que para el proceso de atención de solicitudes no existe un vocabulario de datos en común en torno a las aplicaciones que soportan el proceso, la información se replica y es redundante

y la arquitectura de la información no cuenta con datos maestros que implementen un vocabulario de datos común. El nivel de madurez de la dimensión de información es 1 o Silo.

- **Dimensión de infraestructura**

La información obtenida del proceso permite concluir que la infraestructura de TI relativa al proceso no admite requisitos no funcionales y operativos de los Niveles de Acuerdo de Servicio (SLA) necesarios para operar un entorno SOA, por lo cual la evaluación de la dimensión de infraestructura es 1 o Silo

Por otra parte, el análisis de capacidades, en especial lo referente al recurso humano, adelantado mediante encuesta dirigida al personal de Grupo de informática forense arroja datos como los siguientes:

- A pesar de que existe un alto nivel para atender todo tipo de requerimientos, la atención de solicitudes para la obtención de imágenes forenses y análisis de información muestran un nivel de conocimiento medio bajo, situación que se observa con preocupación considerando que este tipo de requerimientos es el más usual que se realiza al Grupo.

- De igual forma se encuentra un nivel de conocimiento medio bajo para realizar estudios forenses sobre elementos como: dispositivos móviles, discos duros y memorias extraíbles, esto puede originarse en la división interna del Grupo, dos unidades de trabajo (móviles y otros medios de almacenamiento) que atienden los requerimientos de acuerdo al nivel de especialización, esta división del trabajo puede estar disminuyendo la capacidad de los peritos para atender otro tipo de dispositivos diferentes a los de su especialidad, generando ineficiencia en la atención de todos los requerimientos que debe atender el Grupo.

- La encuesta muestra que los peritos del Grupo tienen un nivel de conocimiento medio bajo para atender solicitudes relacionadas con bases de datos, servicios cloud y sistemas de información, este dato resulta ser muy importante considerando la tendencia actual de gestión y almacenamiento de la información en el ámbito digital.

5.2.5 Evaluar la preparación para la transformación del negocio

Comprender la preparación que tiene la organización para aceptar los cambios, identificar los riesgos y definir las acciones para limitar dichos riesgos a través de planes de implementación y migración, es clave para una transformación exitosa.

El resultado de esta identificación es una comprensión más profunda de los desafíos y oportunidades que podrían presentarse en el transcurso del esfuerzo de arquitectura empresarial; muchos desafíos se traducen en riesgos que deben abordarse, monitorearse y si es posible, mitigarse. (The Open Group, 2018); (Desfray & Reymon, 2014).

Con base en el Programa de Habilitación para la Transformación Empresarial del Gobierno de Canadá – BTEP, TOGAF propone una serie de actividades para evaluar la preparación para la transformación del negocio, así:

1. Determinar los factores de preparación que impactarán a la organización.
2. Evaluar los factores de preparación
3. Evaluar los riesgos para cada factor y las acciones de mitigación.

En este sentido, para el ejercicio de arquitectura empresarial se consideraron relevantes los siguientes factores:

- **Deseo, voluntad y resolución**: Deseo de lograr los resultados, voluntad de aceptar el impacto de hacer el trabajo y resolución de seguir adelante y completar el esfuerzo.
- **Necesidad:** Existe la necesidad imperiosa de ejecutar el esfuerzo
- **Financiamiento:** Existe una fuente clara de recursos para cubrir los gastos potenciales del esfuerzo.
- **Patrocinio y liderazgo**: El liderazgo mantiene a todos comprometidos y enfocados en los objetivos estratégicos. El esfuerzo es patrocinado por un ejecutivo que está adecuadamente alineado para proporcionar el liderazgo que el esfuerzo necesita y es capaz de articular y defender las necesidades del esfuerzo a nivel de las Directivas del nivel superior.
- **Gobernanza**: Capacidad de involucrar la participación y el apoyo de todas las partes interesadas o responsables en el esfuerzo con el objetivo de garantizar que se atienden los intereses corporativos y los objetivos alcanzados.
- **Aproximación al modelo y viabilidad de la ejecución**: la organización tiene experiencia en este tipo de proyectos, de modo que los procesos, las disciplinas, la experiencia y el gobierno ya están establecidos, probados y disponibles para aplicar. al esfuerzo de transformación.

Identificados los factores de preparación, se procede a calificar cada uno con base en las siguientes escalas:

- **Urgencia**: Se necesita acción antes de que pueda comenzar una iniciativa de transformación.
- **Estado de preparación**: se califica como Bajo (requiere un trabajo sustancial antes de continuar), Regular (necesita algo de trabajo antes de continuar),

Aceptable (existen algunos problemas de preparación); Bueno (existen problemas relativamente menores) o Alto (sin preparación).

- **El grado de dificultad para corregir**: Califica el esfuerzo requerido para superar cualquier problema identificado como: No se necesita acción, Fácil, Moderado o Difícil.

Al finalizar, cada factor se evalúa con respecto al riesgo, incluyendo una estimación del impacto y la probabilidad; se deben describir las acciones de mejora diseñadas para mitigar los riesgos. Para evaluar la probabilidad y el impacto se toman como referencia los criterios establecidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas, de la Función Pública, versión 4 de octubre de 2018.

La probabilidad se evalúa a partir de los siguientes criterios:

Tabla 10

Tabla de probabilidad.

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	Casi Seguro	Es inminente que el evento se presente	Más de 1 vez al año.
4	Probable	Existe una probabilidad media (50%) de presentarse el evento	Al menos de 1 vez en el último año.
3	Posible	El evento podría ocurrir en algún momento	Al menos de 1 vez en los últimos 2 años.
2	Improbable	Rara vez se puede presentar este riesgo	Al menos de 1 vez en los últimos 5 años.
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años.

Fuente: Adaptado de Fiscalía General de la Nación. (2019c). *Mapa de riesgos.* Manuscrito no publicado.

La guía sugiere que, en caso de no tener datos históricos sobre la materialización del riesgo en un periodo determinado, los integrantes del equipo de trabajo deben calificar el nivel de probabilidad de que se presente el evento tomando como guía la matriz de priorización de la probabilidad que se muestra a continuación:

N.°	RIESGO	P1	P2	P3	P4	P5	P6	TOT	PROM	
1	Inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad	Se espera que el evento ocurra en la mayoría de las circunstancias.	**5**	**4**	**3**	**5**	**3**	**4**	**24**	**4** PROBABLE
2	Otros riesgos identificados	Es viable que el evento ocurra en la mayoría de las circunstancias.								
3	Otros riesgos	El evento podrá ocurrir en algún momento.								
Convenciones: **N.°**: número consecutivo del riesgo - **P1**: participante 1 P... - **Tot**: total puntaje - **Prom.**: promedio										

Figura 28. Matriz de priorización de probabilidad Fuente: Función Pública. (2018). *Guía para la administración del riesgo y el diseño de controles en entidades pública* Recuperado de http://www.funcionpublica.gov.co/documents/418548/34150781/Gu%C3%ADa+para+la+administraci%C3%B3n+del+riesgo+y+el+dise%C3%B1o+de+controles+en+entidades+p%C3%BAblicas+-+Riesgos+de+gesti%C3%B3n%2C+corrupci%C3%B3n+y+seguridad+digital+-+Versi%C3%B3n+4+-+Octubre+de+2018.pdf/68d324dd-55c5-11e0-9f37-2e5516b48a87?t=1542226781163&download=true

La consecuencia del riesgo o impacto se evalúa considerando la siguiente matriz de valoración cualitativa:

Tabla 11

Matriz de valoración cualitativa.

NIVEL	DESCRIPTOR	IMPACTO - CUALITATIVO
5	Catastrófico	• Interrupción de las operaciones de la entidad por más de cinco (5) días • Intervención por parte de un ente de control u otro ente regulador • Pérdida de información crítica para la entidad que no se puede recuperar • El impacto afecta en una decisión que genera vencimiento de términos y la legalidad de la actuación • El impacto genera el incumpliendo de uno o más propósitos de la ley • Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal • Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
4	Mayor	• El impacto impide el cumplimiento de los objetivos institucionales – parálisis • Sanción por parte de un ente de control u otro ente regulador • El impacto incrementa de forma adversa el presupuesto y la gestión de la entidad • Pérdida de información crítica para la entidad que puede ser recuperada de forma parcial o incompleta.

NIVEL	DESCRIPTOR	IMPACTO - CUALITATIVO
		• Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.
3	Moderado	• Interrupción de las operaciones de la entidad por un (1) día • Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. • Inoportunidad en la información ocasionando retrasos en la atención a los usuarios. • Reproceso de actividades y aumento de carga operativa. • Investigaciones penales, fiscales o disciplinarias. • Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos • El impacto afecta en una decisión o acción que tiene posibilidad de prórroga – subsanable • El impacto afecta el desempeño del servidor y su ambiente de trabajo.
2	Menor	• Interrupción de las operaciones de la entidad por algunas horas • Reclamaciones o quejas de los usuarios que implican investigaciones internas o disciplinarias. • Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos • Impacto leve en los resultados de los procesos, donde los aspectos formales no incide en las decisiones. • Impacto leve en los resultados de todos los procesos de la entidad
1	Insignificante	• No hay interrupción de las operaciones de la entidad • No se generan sanciones económicas o administrativas. • No se afecta la Imagen institucional de forma significativa.

Fuente: Adaptado de Adaptado de Fiscalía General de la Nación. (2019c). *Mapa de riesgos.* Manuscrito no publicado.

A continuación se muestran los riesgos identificados frente a la preparación que tiene la organización para aceptar los cambios propuestos con el ejercicio de arquitectura empresarial sobre el proceso para la atención de solicitudes en el Grupo de Informática Forense, como se indicó anteriormente dicha identificación y clasificación se realiza con base en lo propuesto por el Programa de Habilitación para la Transformación Empresarial del Gobierno de Canadá – BTEP, la Guía para la administración del riesgo y el diseño de controles en entidades públicas, de la Función Pública en Colombia, versión 4 de octubre de 2018 y la tablas para la valoración de riesgos definidas por la Fiscalía General de la Nación:

Tabla 12

Riesgos ejercicio arquitectura empresarial.

FACTOR	CALIFICACION			RIESGO	IMPACTO	PROBABILIDAD	MITIGACION	INDICADOR
	URGENCIA	ESTADO DE PREPARACIÓN	GRADO DE DIFICULTAD PARA CORREGIR					
Patrocinio y liderazgo	Urgencia	Bueno	Fácil	No vincular a las Directivas de la Entidad en la planificación, de los proyectos.	Insignificante	Probable	Diseñar un plan de comunicaciones efectivo.	Número de proyectos aprobados/Numero de proyectos radicados
Deseo, voluntad y resolución	Urgencia	Bueno	Fácil	No hay asignación presupuestal para ejecutar los proyectos identificados con la arquitectura	Insignificante	Probable	Documentar los beneficios esperados con el desarrollo de cada proyecto, adelantar acercamiento con las Directivas que deciden respecto a la asignación presupuestal	Presupuesto Asignado/Presupuesto Solicitado
Necesidad	Urgencia	Regular	Fácil	Los criterios de éxito no han sido comunicados claramente.	Insignificante	Posible	Diseñar un plan de comunicaciones acorde a las necesidades identificada para cada grupo de interesados.	Número de proyectos aprobados/Numero de proyectos radicados

FACTOR	CALIFICACION			RIESGO	IMPACTO	PROBABILIDAD	MITIGACION	INDICADOR
	URGENCIA	ESTADO DE PREPARACIÓN	GRADO DE DIFICULTAD PARA CORREGIR					
Financiamiento	Urgencia	Bajo	Moderado	No hay claridad en la fuente de fondos para los proyectos	Menor	Probable	Estructurar adecuadamente los proyectos y presentarlos ante las Directivas de la Entidad con el fin de buscar apoyo para su ejecución y se defina un rubro con el cual puedan ser financiados.	Presupuesto Asignado/Presupuesto Solicitado
				Equivocarse en la selección y priorización de inversiones y en la secuencia de implantación.	Menor	Improbable	Asegurarse de aplicar guías metodológicas para la priorización de proyectos antes iniciar las inversiones.	Número de inversiones efectuadas en el periodo/Número de casos de negocio identificados con la respectiva evaluación de inversión.
Gobernanza	Urgencia	Regular	Moderado	No existe una cultura que fomente la participación en el logro de los objetivos estratégicos	Menor	Probable	Diseño de estrategias de uso y apropiación	Porcentaje de cumplimiento de las estrategias de uso y apropiación
				Dificultad para recibir y apropiar los resultados del esfuerzo de arquitectura	Menor	Posible		

FACTOR	CALIFICACION			RIESGO	IMPACTO	PROBABILIDAD	MITIGACION	INDICADOR
	URGENCIA	ESTADO DE PREPARACIÓN	GRADO DE DIFICULTAD PARA CORREGIR					
Aproximación al modelo y viabilidad de la ejecución	Urgencia	Regular	Moderado	La organización no tiene mucha experiencia en proyectos de arquitectura.	Menor	Casi seguro	Campañas de socialización respecto a los conceptos y beneficios asociados a la arquitectura institucional.	Numero de ejercicio de arquitectura empresarial

Nota: Tabla para la evaluación de riesgos ejercicio arquitectura empresarial.

5.2.6 Alcance de la arquitectura

Según lo establece el ADM de TOGAF 9.2, Open Group (2018), para delimitar el alcance del esfuerzo de arquitectura se deben definir tres dimensiones, así:

Tabla 13

Dimensiones alcance de la arquitectura

Amplitud	¿Cual es la extensión total de la organización? y que parte de esa extensión será cubierta por el esfuerzo de arquitectura.
Profundidad	¿A nivel de detalle debe llegar el esfuerzo de arquitectura?
Dominios	Que dominios abarcará la arquitectura empresarial.

Fuente: Adaptado de The Open Group. (2018). TOGAF® standard, version 9.2. Recuperado de http://pubs.opengroup.org/architecture/togaf92-doc/arch/

- **Amplitud**

El ejercicio de arquitectura empresarial tiene por objeto atender una necesidad específica, en consecuencia, cubrirá el proceso para la atención de solicitudes del Grupo Informática Forense Nivel Central, Cuerpo Técnico de Investigación – Fiscalía General de la Nación.

Las funciones que desempeña el Grupo de Informática Forense se enmarcan en el proceso misional de **Investigación y Judicialización**, según lo describe el PETIC de la Entidad:

Los procesos misionales materializan la misión y objetivos institucionales a través de la ejecución de las actividades de investigación y acusación de los presuntos infractores de la Ley Penal. Es en estos procesos donde se identifica la cadena de valor de la Fiscalía General de la Nación (FGN, 2017a)

A continuación, se ilustra el mapa de procesos de la Entidad:

Figura 29. Mapa de Procesos FGN versión 02. Fuente: Fiscalía General de la Nación. (2017d). Mapa de procesos fiscalía general de la nación. Recuperado de http://web_app/Documentacion/Procesos/Mapa%20de%20procesos%202017.jpg

- **Profundidad.**

El esfuerzo de arquitectura se llevará a cabo hasta el diseño de la propuesta de mejora para la optimización del proceso para la atención de solicitudes, en la cual se elaborará una lista de proyectos y el posible orden de ejecución a fin de lograr la mejora del proceso.

- **Dominios.**

El ejercicio abarcará los cuatro dominios de la arquitectura (negocios, datos, aplicaciones y tecnología)

5.2.7 Declaración de trabajo de arquitectura (Statement of Architecture Work)

Es un documento que define el alcance y enfoque que se utilizará para completar un ciclo de desarrollo de la arquitectura. Generalmente es el documento contra el cual se medirá la ejecución exitosa del proyecto de arquitectura y puede formar la base para un acuerdo contractual entre el proveedor y el consumidor de servicios de arquitectura; contiene la siguiente información:

- Título
- Solicitud de proyectos de arquitectura y antecedentes.
- Descripción y alcance del proyecto de arquitectura.
- Visión general de la visión de la arquitectura
- Cambio específico de procedimientos de alcance.
- Roles, responsabilidades y entregables
- Criterios y procedimientos de aceptación.
- Plan de proyecto de arquitectura y calendario.
- Aprobaciones (The Open Group, 2018)

5.3 Fase de negocio

En esta fase del ciclo de arquitectura empresarial se identifican los principales procesos de negocio y se definen aspectos clave de la estrategia y el gobierno en la organización, que sirven de base para el desarrollo de una arquitectura empresarial objetivo cuya misión es describir la forma en que el grupo de informática forense debe operar para alcanzar los objetivos de negocio, y responder a los objetivos estratégicos planteados en la visión de arquitectura (Bustamante, s.f.a).

5.3.1 Desarrollo de la línea base de la arquitectura de negocio

A partir de la información obtenida en la entrevista de conocimiento del proceso para la atención de solicitudes de informática forense, cuando se indagó a los actores principales acerca del ciclo de vida de un requerimiento atendido por el grupo, se pudo establecer que la gestión de cada una de las solicitudes recibidas sigue un proceso de 5 fases:

- Emisión de la orden a policía judicial
- Recepción de la solicitud
- Asignación de perito de informática forense
- Atención de la orden de trabajo de informática forense
- Cierre de la solicitud de informática forense

Haciendo una clasificación de las acciones descritas por los entrevistados, entre las cinco etapas del proceso, se identifican las actividades principales que delimitan el alcance de cada fase.

- Emisión de la orden a policía judicial: Creación de la orden de forma manual o en sistema de información S.P.O.A, designación de un investigador del caso y entrega del elemento material probatorio (EMP) al grupo de Informática Forense.
- Recepción de la solicitud: Validación de la competencia y pertinencia de la solicitud recibida, recepción del elemento material probatorio, registro de continuidad del EMP de forma física y de forma digital en el sistema de información S.P.O.A y registro de la solicitud en la herramienta de gestión documental O.R.F.E.O.
- Asignación de perito de informática forense: Validación de la ocupación y las capacidades técnicas de los peritos para atender la solicitud, selección de perito forense y registro de la orden de trabajo en el sistema de información misional S.I.G
- Atención de la orden de trabajo de informática forense: registro de continuidad del EMP de forma física y de forma digital en el sistema de información S.P.O.A, ejecución del procedimiento técnico necesario para resolver la solicitud, recolección de la información obtenida en medios de almacenamiento digital y generación de un informe descriptivo del procedimiento forense realizado.
- Cierre de la solicitud de informática forense: Aprobación del informe forense, liberación de la orden de trabajo en sistema de información misional S.I.G., entrega del informe físico, los EMP objeto de estudio y la evidencia digital obtenida a la Autoridad solicitante, registro y descarga del informe en sistema de información S.P.O.A y descarga del informe en herramienta de gestión documental O.R.F.E.O.

Una representación más detallada del proceso para la atención de solicitudes de informática forense se consigue al descomponer las actividades identificadas en tareas puntuales, este nivel de detalle se puede observar en el siguiente diagrama de descomposición funcional.

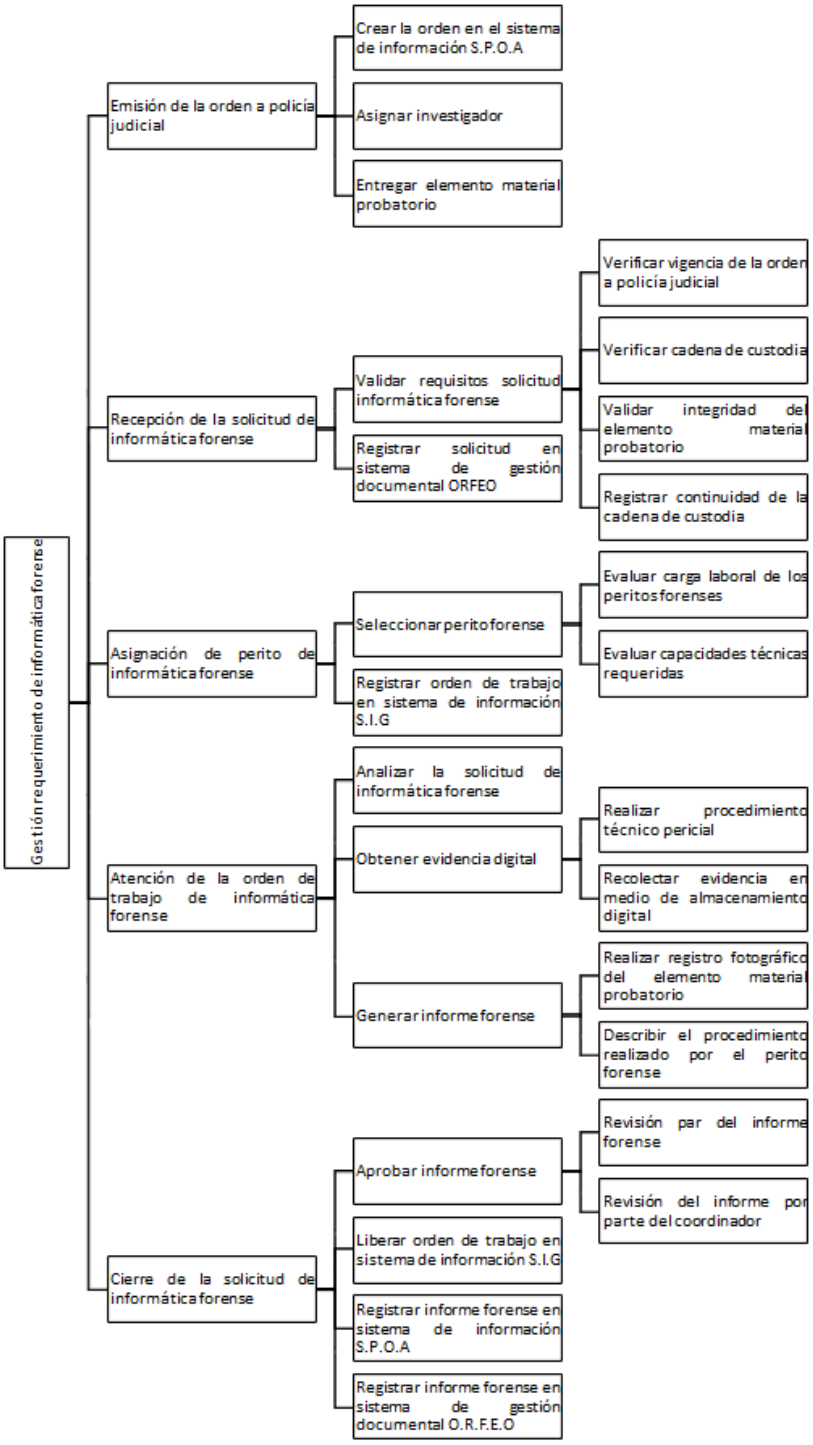


Figura 30. Diagrama de descomposición funcional del proceso para la atención de solicitudes de informática forense. Fuente: elaboración propia.

- **Roles del proceso**

Las actividades descritas en la descomposición funcional del proceso son ejecutadas en su totalidad por funcionarios de la Fiscalía General de la Nación. A continuación, se describen los roles identificados en cada una de las fases que integran el ciclo de vida de una solicitud de informática forense:

Nombre del rol: Fiscal

Propósito principal:

> Ejercer la acción penal a fin de realizar la investigación de los hechos punibles y conductas que revisten características de delito (…), así como contribuir al desarrollo e implementación de la política criminal, de acuerdo a la Constitución y la Ley (Fiscalía General de la Nación, 2017c, p. 20).

Actividades dentro del proceso: Emitir las solicitudes de informática forense mediante la creación de órdenes a policía judicial.

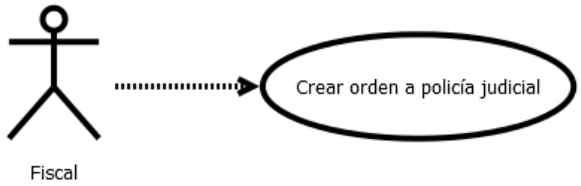


Figura 31. Casos de uso rol fiscal. Fuente: elaboración propia

Nombre del rol: Asistente de informática forense

Propósito principal: “Ejecutar actividades técnicas con el fin de dar apoyo administrativo a las funciones de la dependencia de acuerdo con la normativa vigente” (FGN, 2017c, p. 138).

Actividades dentro del proceso: Recibir las solicitudes de informática forense y realizar el registro de documentos y elementos materiales probatorios (EMP) en los sistemas de información misionales.

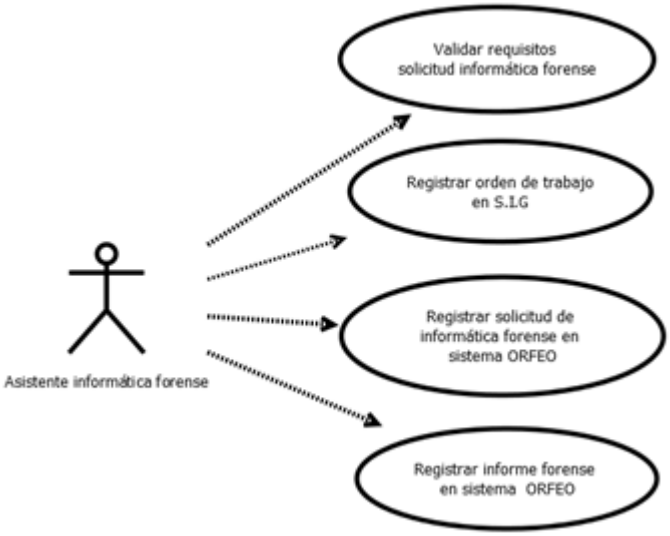


Figura 32. Casos de uso rol Asistente Informática Forense. Fuente: elaboración propia.

Nombre del rol: Perito Forense

Propósito principal:

> Realizar labores técnico-científicas de recolección, análisis e interpretación de los elementos materiales probatorios, evidencia física o información pertinente para el adecuado desarrollo de las investigaciones y las actuaciones operativas en la investigación criminal, de acuerdo con las políticas, los procedimientos y protocolos establecidos en la entidad y la normativa vigente (FGN, 2017c, p. 56).

Actividades dentro del proceso: Atender las solicitudes de informática forense y realizar revisiones de los informes forenses elaborados por sus pares.

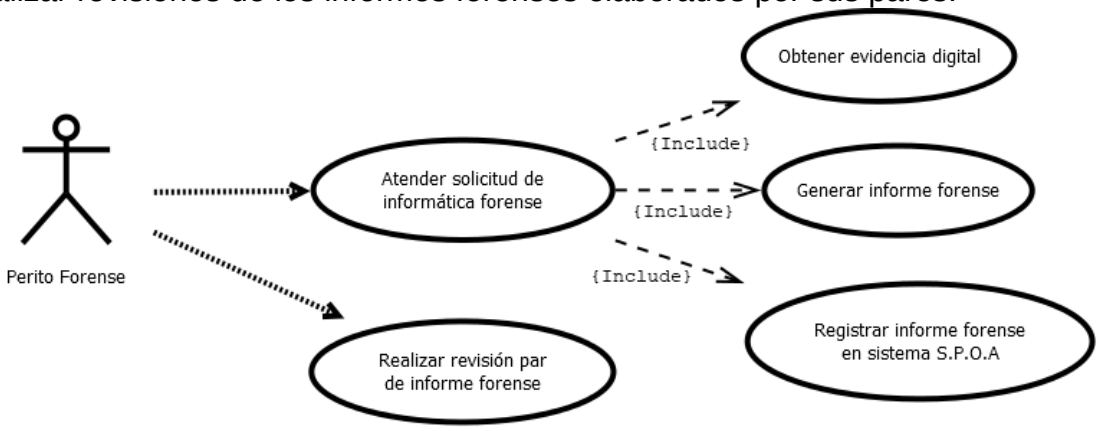


Figura 33. Casos de uso rol Perito Forense. Fuente: elaboración propia.

Nombre del rol: Coordinador Informática forense

Propósito principal:

> Orientar, diseñar, ejecutar y hacer seguimiento a las estrategias, planes, programas, proyectos y actividades de la dependencia y realizar estudios con la aplicación de su experticia y de sus conocimientos especializados tendientes al logro de las metas y objetivos establecidos y a la mejora continua, de acuerdo con las políticas institucionales y la normativa vigente (FGN, 2017c, p. 120).

Actividades dentro del proceso: Asignar las solicitudes a los peritos forense, aprobar los informes generados y liberar la orden de trabajo del sistema de información SIG.

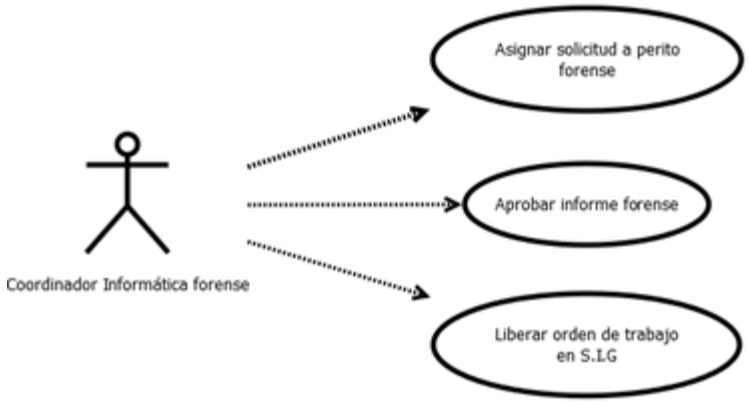


Figura 34. Casos de uso rol Coordinador Informática Forense. Fuente: elaboración propia.

5.3.2 Descripción de la línea base de arquitectura de negocio

La línea base de arquitectura de negocio corresponde a una representación del proceso actual para la atención de solicitudes de informática forense, obtenida como resultado de relacionar las actividades, los roles y los objetos de negocio identificados en la etapa de recolección de información.

A continuación, se presenta la vista de negocio del proceso elaborada en lenguaje archimate.

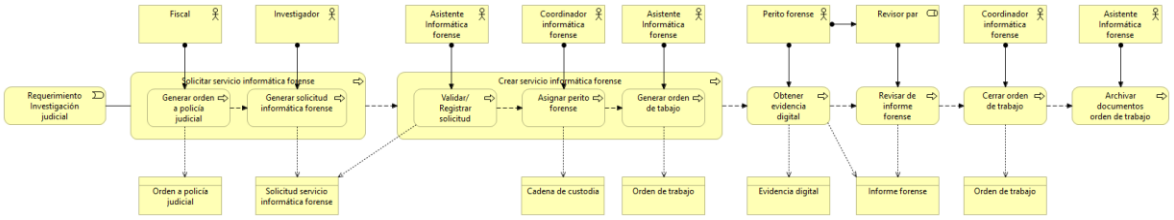


Figura 35. AS-IS de negocio. Fuente: elaboración propia.

5.3.3 Desarrollo de la arquitectura de negocio objetivo

Uno de los principales objetivos de cualquier ejercicio de arquitectura empresarial es generar representaciones que abarquen las preocupaciones de todos los involucrados (Desfray & Raymond, 2014); al analizar la información recolectada en las entrevistas de conocimiento del proceso para la atención de solicitudes de informática forense, sobresalen los siguientes aspectos que fueron referidos por los entrevistados como oportunidades de mejora.

- No existe un estándar técnico de tiempos de atención para los diferentes tipos de requerimientos atendidos por el grupo.
- Una misma solicitud debe ser registrada en por lo menos tres sistemas de información diferentes.
- Algunos requerimientos deben ser atendidos más de una vez debido a la falta de comunicación entre fiscales, investigadores y peritos forenses.
- No existe una base de datos de conocimiento ni un registro de lecciones aprendidas en la actividad pericial.
- No existen criterios de priorización para las solicitudes de informática forense atendidas por el grupo.

Adicional a las preocupaciones referidas por los funcionarios entrevistados, se identifican los siguientes focos de ineficiencia en el proceso.

- El equipo técnico se encuentra dividido en dos grupos, el primero atiende las solicitudes asociadas con dispositivos móviles y el otro se encarga de los demás dispositivos de almacenamiento, actualmente existe la percepción de que carga laboral relacionada con dispositivos móviles es mayor a la de otros dispositivos, debido a la cantidad y la frecuencia con que se reciben estos elementos en el grupo.
- No se cuenta con un mecanismo confiable para establecer la carga laboral de cada perito forense, esto posiblemente se traduzca en una mala distribución de la carga laboral entre los integrantes del equipo técnico.
- Artefactos clave del proceso como la orden a policía judicial, cadena de custodia del elemento material probatorio, solicitud de trabajo e informe forense se manejan de forma física.

Con base en las preocupaciones listadas anteriormente se plantean los objetivos de negocio que deben ser alcanzados mediante el desarrollo de la arquitectura objetivo.

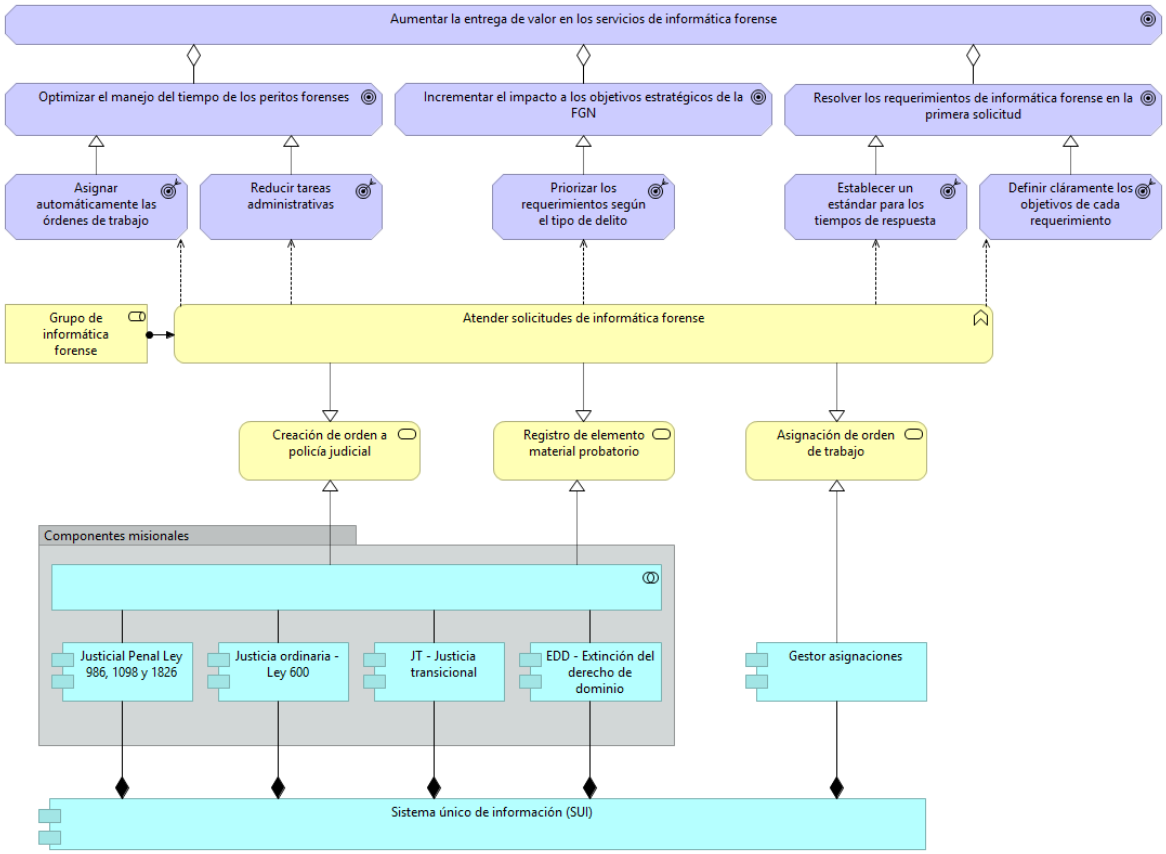


Figura 36. Diagrama huella de negocio. Fuente: elaboración propia.

En el diagrama de huella de negocio se relacionan los objetivos planteados con la función principal del grupo de informática forense; en la arquitectura objetivo, dicha función estará apalancada por servicios de negocio soportados en los sistemas de información que se proyectaron dentro del plan estratégico de tecnologías de información de la Fiscalía General de la Nación.

- **Proceso de negocio objetivo**

Alcanzar los objetivos propuestos implica una optimización del proceso actual para la atención de solicitudes de informática forense; con el modelo actualizado se pretende reducir las tareas operativas realizadas por el equipo técnico, mejorar la

estimación de tiempos de respuesta a los requerimientos recibidos y priorizar la atención de las solicitudes con base en el tipo de delito.

Entre las propuestas de mejora se incluye una evaluación preliminar de los objetos materiales probatorios con el fin de cuantificar de forma más precisa el esfuerzo requerido para atender cada solicitud, las órdenes de trabajo serán asignadas de forma automática por un sistema de información que priorizará las solicitudes y las irá asignando de acuerdo con la disponibilidad de los peritos forenses, además, se incluye una actividad de entendimiento entre la autoridad solicitante y el perito forense asignado, que busca asegurar la entrega de valor en cada requerimiento atendido y disminuir la cantidad de solicitudes que se atienden más de una vez.
El proceso completo se presenta en el siguiente diagrama de descomposición funcional, en el cual se resaltan las actualizaciones sobre el proceso actual.

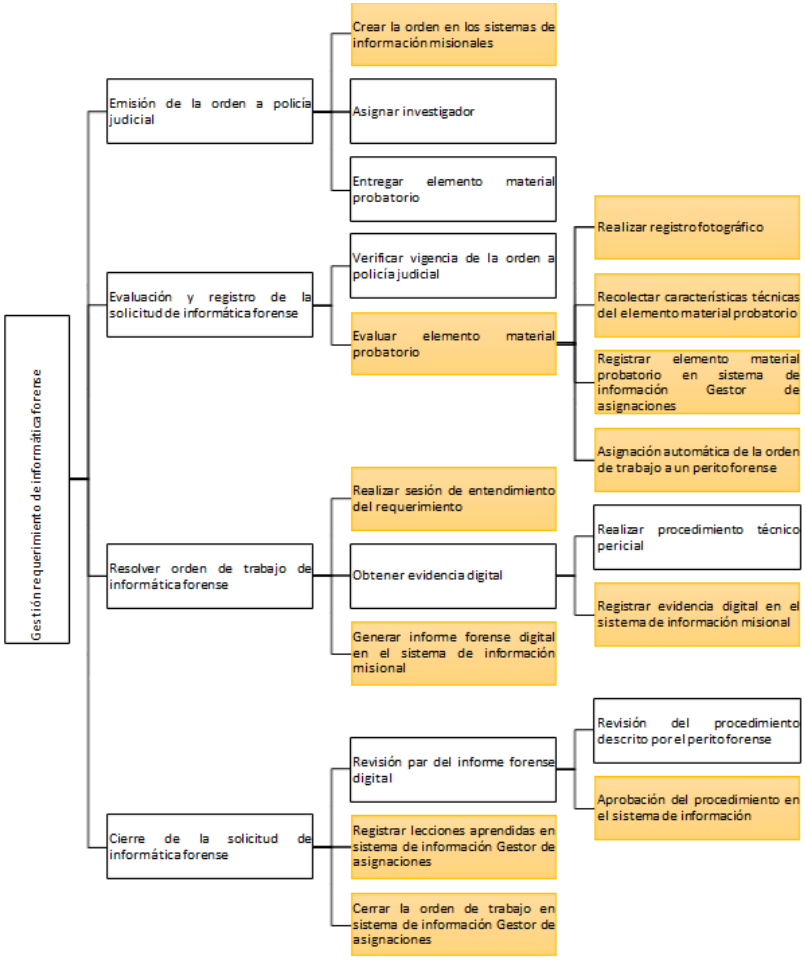


Figura 37. Diagrama de descomposición funcional del proceso. Fuente: elaboración propia.

- **Roles del proceso objetivo**

La propuesta de mejora al proceso de atención de requerimientos de informática forense implica la creación de nuevos roles, la modificación de tareas para algunos de los roles existentes y la desaparición de otros. Los roles encargados de llevar a cabo cada una de las actividades propuestas se relacionan en la matriz de responsabilidades del proceso.

RASCI	**Roles**				
Actividades	**Roles Grupo de informática forense**			**Roles ente acusatorio**	
	Coordinador	**Revisor informática forense**	Perito informática forense	Fiscal	Investigador
Crear orden a policía judicial	I			A-R	I
Verificar vigencia de la orden a policía judicial	I	A-R			I
Evaluar elemento material probatorio	I	A-R	S		
Realizar sesión de entendimiento del requerimiento	A		R		S
Obtener evidencia digital	I		R		
Generar informe forense digital	I		A-R		
Revisión par del informe forense digital	A	R	S		
Registrar lecciones aprendidas	A	S	R		
Cerrar orden de trabajo	C		A-R	I	I

Nomenclatura	**Rol**	**Responsabilidad**
R	Responsable de la ejecución	Ejecutar la tarea
A	Responsable del proceso	Velar por que la tarea se cumpla
S	Apoyo	Apoyar al rol ejecutor o ser su backup
C	Consultado	Debe ser consultado para realizar la tarea
I	Informado	Debe ser informado de la realización de la tarea

Figura 38. Matriz de responsabilidades del proceso. Fuente: elaboración propia.

En este orden de ideas, la nueva definición de actividades asociadas a cada rol se presenta a continuación.

Nombre del rol: Fiscal.

Antigüedad del rol: Actual.

Transformaciones: Crear la orden a policía judicial en el sistema de información misional.

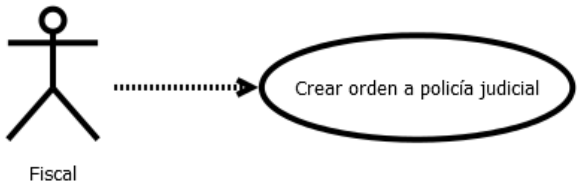


Figura 39. Casos de uso proceso objetivo, rol Fiscal. Fuente: elaboración propia.

Nombre del rol: Perito forense.

Antigüedad del rol: Actual.

Transformaciones: Coordinar una sesión de entendimiento del requerimiento con la autoridad o el investigador solicitante. El informe de actividad forense será registrado una única vez, directamente en el sistema de información.

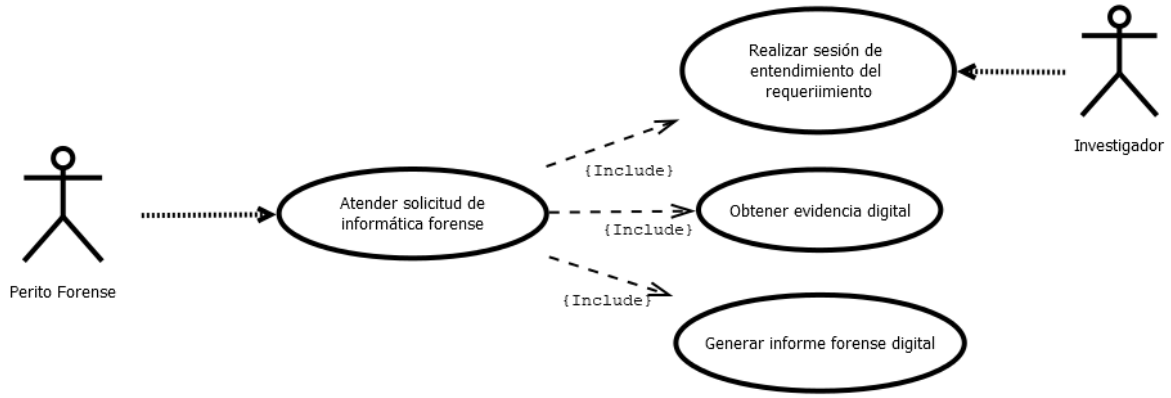


Figura 40. Casos de uso proceso objetivo, rol Perito Forense. Fuente: elaboración propia.

Nombre del rol: Investigador

Antigüedad del rol: Nuevo.

Propósito principal:

> Realizar las actuaciones operativas y técnicas en la investigación criminal, así como las actividades establecidas dentro del ámbito de la investigación penal para la búsqueda de indiciados y evidencias que permitan el esclarecimiento de hechos delictivos, de acuerdo a los programas metodológicos, las políticas establecidas y la normativa vigente (FGN, 2017c, p. 48).

Actividades principales: Entregar los elementos materiales probatorios al grupo de informática forense y participar en la sesión de entendimiento de la solicitud con el perito forense.

Figura 41. Casos de uso proceso objetivo, rol Investigador. Fuente: elaboración propia.

Nombre del rol: Revisor Informática Forense

Propósito principal:

> Realizar labores técnico-científicas de recolección, análisis e interpretación de los elementos materiales probatorios, evidencia física o información pertinente para el adecuado desarrollo de las investigaciones y las actuaciones operativas en la investigación criminal, de acuerdo con las políticas, los procedimientos y protocolos establecidos en la entidad y la normativa vigente (FGN, 2017c, p. 56).

Actividades dentro del proceso: Recibir las solicitudes de informática forense, realizar registro de las características técnicas del elemento material probatorio, revisar y aprobar los informes forenses digitales.

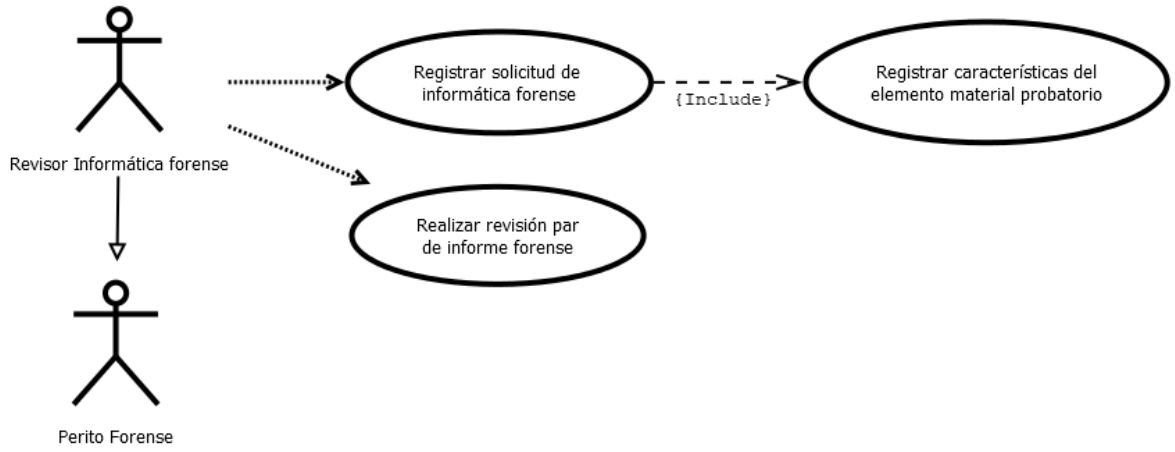


Figura 42. Casos de uso proceso objetivo, rol Revisor Informática Forense. Fuente: elaboración propia.

Adicional a los roles relacionados en la matriz de responsabilidades, algunas actividades clave del proceso objetivo serán desarrolladas por el Sistema Único de Información (SUI), proyectado en el plan estratégico de tecnologías de información de la FGN.

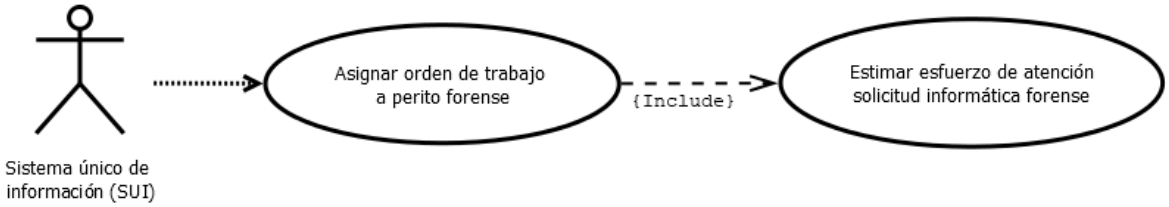


Figura 43. Casos de uso proceso objetivo, Sistema Único de Información. Fuente: elaboración propia.

5.3.4 Descripción de la arquitectura de negocio objetivo

La arquitectura de negocio objetivo corresponde a una representación del proceso para la atención de solicitudes de informática forense, obtenida como resultado de relacionar las actividades, los roles y los objetos de negocio definidos, en respuesta a los objetivos del negocio, que fueron planteados con base en las preocupaciones identificadas en la etapa de recolección de información.
A continuación, se presenta la vista de negocio del proceso objetivo elaborada en lenguaje archimate.

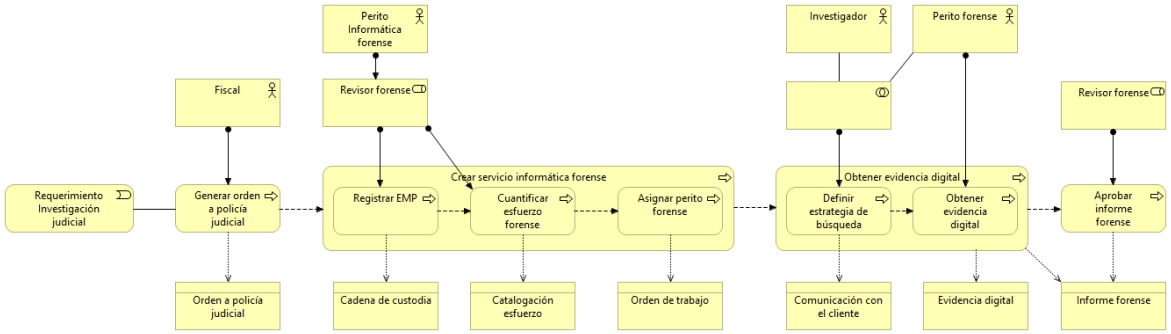


Figura 44. TO-BE de negocio. Fuente: elaboración propia.

5.3.5 Análisis de brechas

El análisis de brechas puede entenderse como el mecanismo que propicia la elección del camino más apropiado para ir de un estado actual a un estado objetivo; en un ejercicio de arquitectura, la transición entre la arquitectura de línea base y la arquitectura objetivo obedece a este mismo principio, que consiste en dar respuesta a las siguientes preguntas (Desfray & Raymond, 2014).

- Qué elementos son nuevos
- Qué elementos han sido modificados
- Qué elementos han sido eliminados
- Qué elementos permanecen sin alteraciones

En la matriz presentada a continuación se resuelven los interrogantes del análisis de brechas, mediante una confrontación entre las actividades identificadas en la línea base de arquitectura y las planteadas en la arquitectura de negocio objetivo.

		Arquitectura objetivo						
		Generar orden a policía judicial	Registrar EMP	Cuantificar esfuerzo forense	Asignar perito forense	Definir estrategia de búsqueda	Obtener evidencia digital	Aprobar informe forense
Arquitectura de línea base				**Nuevo**		**Nuevo**		
Generar orden a policía judicial		Mejorar						

		Arquitectura objetivo						
		Generar orden a policía judicial	Registrar EMP	Cuantificar esfuerzo forense	Asignar perito forense	Definir estrategia de búsqueda	Obtener evidencia digital	Aprobar informe forense
Generar solicitud informática forense	Eliminar							
Validar/Registrar solicitud			Mejorar					
Asignar perito forense					Mejorar			
Obtener evidencia digital							Mejorar	
Revisar informe forense								Mejorar
Cerrar orden de trabajo	Eliminar							
Archivar documentos orden de trabajo	Eliminar							

Figura 45. Matriz para la evaluación de brechas de negocio. Fuente: elaboración propia.

Del ejercicio anterior se obtienen las siguientes modificaciones al proceso actual:

GAP 1: La orden debe ser generada por la autoridad competente a través de un sistema de información transversal a todas las áreas que participan del proceso investigativo, dicho sistema debe notificar al grupo de informática forense sobre la creación de la orden. Los sistemas de información se describirán en detalle en la fase de aplicaciones.

GAP 2: Registrar en una nueva opción dentro del sistema de información misional, las características técnicas de cada elemento material probatorio recibido por el grupo de Informática Forense.

GAP 3: Crear un nuevo módulo en el sistema de información misional que se encargue de asignar automáticamente las órdenes de trabajo a cada perito forense; este sistema debe priorizar las solicitudes con base en el tipo de delito y establecer el tiempo máximo de atención, de acuerdo con las características técnicas de el o los elementos materiales probatorios y el nivel de ocupación del recurso humano del grupo.

GAP 4: En el proceso para atender cada solicitud de informática forense se debe incluir una sesión de entendimiento entre la autoridad solicitante y el perito forense

asignado, como resultado de dicha sesión deben quedar definidos los siguientes aspectos:

- Objetivo de la solicitud
- Procedimiento de atención
- Resultado esperado

GAP 6: El sistema misional debe contener un módulo para el registro del procedimiento técnico realizado, para ello debe contar con una plantilla de informe estándar que permita adjuntar documentos e imágenes para el registro fotográfico del elemento material probatorio; adicionalmente, se debe habilitar una opción dentro del sistema para que un revisor de informática forense pueda aprobar cada informe generado. Una vez sea aprobado el informe, este debe quedar asociado a la orden con opción de descarga para las autoridades competentes. En este sistema se debe incluir una nueva funcionalidad que informe a los interesados sobre el nivel de avance en la atención de la solicitud.

GAP 7: Dentro del proceso para la generación del informe forense debe incluirse una nueva opción donde el perito registre las lecciones aprendidas en el desarrollo de su actividad pericial; el diligenciamiento de esta opción en el sistema de información debe ser mandatorio y el coordinador del grupo debe velar porque la tarea se realice de forma adecuada.

GAP 8: Se debe implementar una nueva funcionalidad que permita alojar los resultados de los estudios forenses (evidencia derivada) de forma segura y accesible únicamente para los autorizados.

GAP 9: Los grupos de dispositivos móviles y otros dispositivos de almacenamiento deben unificarse para sacar mayor provecho del recurso humano disponible y nivelar la carga laboral.

A partir de las brechas identificadas se construye un mapa de ruta de alto nivel que será refinado en la fase de migración. En esta primera etapa se analizan únicamente las posibles dependencias entre los proyectos planteados.

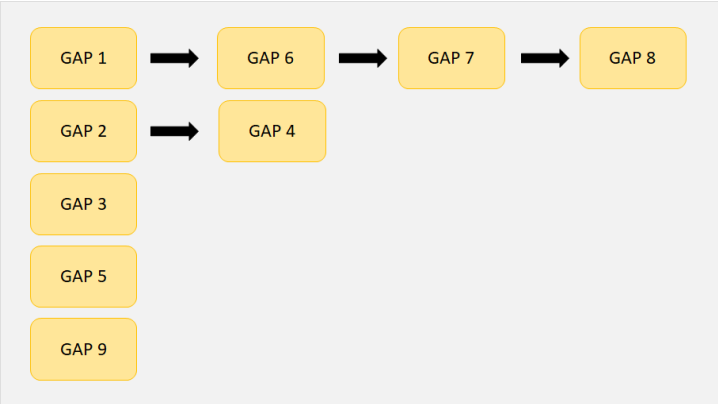


Figura 46. Mapa de ruta de alto nivel, fase de negocio. Fuente: elaboración propia.

5.4 Fase de arquitectura de información

En la fase de datos y aplicaciones se describe la forma en que los sistemas de información facilitarán la consecución de los objetivos planteados en la visión de arquitectura, atendiendo a su vez las preocupaciones de las partes interesadas (Bustamante, s.f.b).

5.4.1 Descripción de la línea base de arquitectura

El proceso actual para la atención de solicitudes de informática forense está soportado por tres sistemas de información que forman parte de la arquitectura tecnológica actual de la F.G.N.

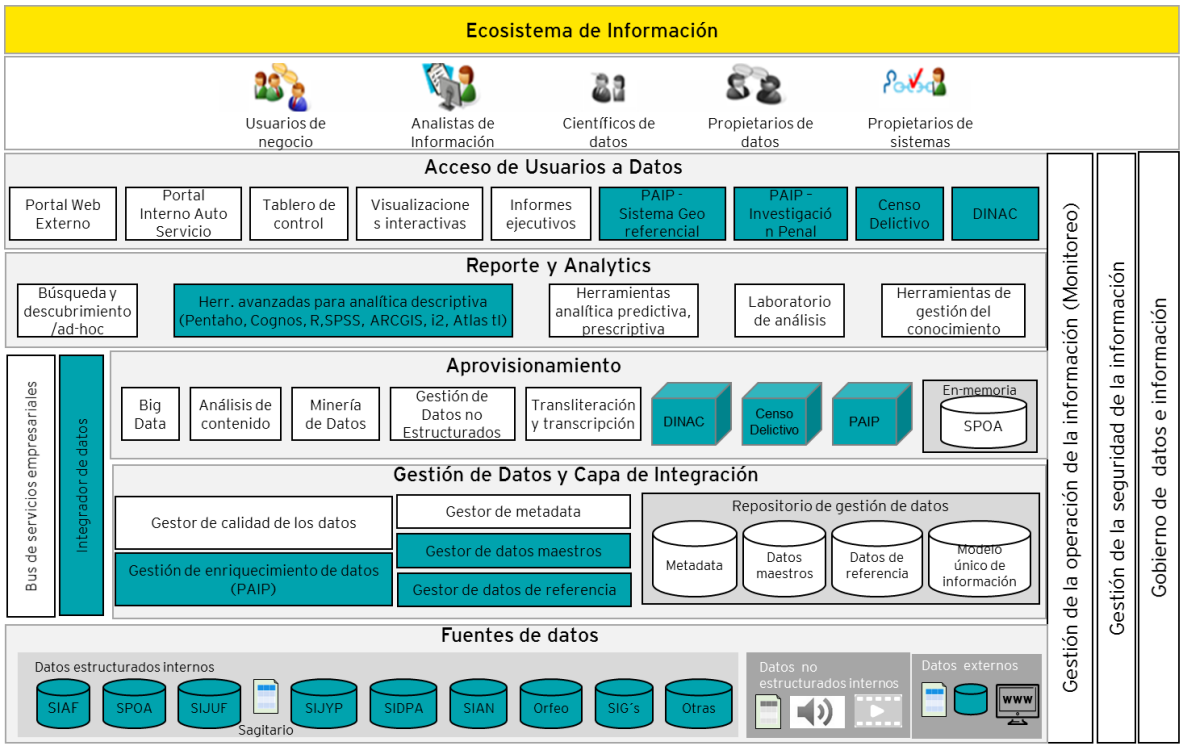


Figura 47. Arquitectura tecnológica FGN, Fuente: Fiscalía General de la Nación. (2017a, p. 50). *Plan estratégico de tecnologías de la información y las comunicaciones [PETIC] 2017-2020.* Manuscrito no publicado.

- **Sistema de información misional S.P.O.A**:

  Es el sistema de información de la Fiscalía General de la Nación para el Sistema Penal Oral Acusatorio. El mismo funciona en una plataforma a la que los funcionarios de la Fiscalía pueden acceder remota o localmente, consta de siete módulos distintos: cinco para ingresar información del sistema penal, uno para modificar las opciones de seguridad (administración de cuenta y acceso al sistema) y uno más para obtener ayuda en línea sobre el uso del sistema de información (Fiscalía General de la Nación, 2017a, p.1).

  El sistema S.P.O.A soporta todos los procesos judiciales bajo Ley 906 de 2004, en él se crea la orden a policía judicial, se realiza el registro de cadena de custodia de los elementos materiales probatorios y se describe la actividad forense realizada para atender cada requerimiento. Un diagnóstico de la situación actual incluido en el plan estratégico de tecnologías de la información y las comunicaciones de la F.G.N 2017 - 2020, reporta que "SPOA cumple once años de funcionamiento, y en el tiempo ha requerido múltiples adiciones realizadas en su mayoría de forma inorgánica y desordenada" (Fiscalía General de la Nación, 2017a, p.153) además que existe preferencia por el uso del papel para el registro de órdenes a policía

judicial en lugar de utilizar esta herramienta tecnológica; otro hallazgo del proceso de investigación es que el registro de cadena de custodia sobre los elementos materiales probatorios debe llevarse a cabo tanto en físico como en el sistema de información misional; lo anterior ocurre también con el informe de la actividad pericial generado por los peritos del grupo de Informática Forense, con el agravante que la plantilla de informe para cada perito puede variar debido al grado de personalización, ajustes o actualizaciones sobre el formato que no se realizan en debida forma.

- **SIG**: Sistema de gestión de actividades de policía judicial. En el sistema SIG se registran las órdenes de trabajo que son asignadas a cada perito forense. El diagnóstico incluido en el PETIC 2017 – 2020 refleja que no existe una integración suficiente entre las aplicaciones S.P.O.A y S.I.G, por lo que el registro de la orden a policía judicial así sea generado en SPOA debe realizarse de manera independiente en SIG.

- **Sistema de gestión documental ORFEO**: Es un Sistema de Gestión Documental desarrollado en Colombia por la Superintendencia de Servicios Públicos, que emplea normas técnicas y prácticas para la administración de flujos documentales y archivísticos (Scholarium SAS, 2017). Orfeo es la herramienta web que permite gestionar la trazabilidad de los documentos digitalizados en la Fiscalía General de la Nación. Dentro del proceso para la atención de solicitudes de informática forense, se realiza la digitalización de documentos como la orden, otros documentos que acompañen la orden y parte del informe de la actividad forense elaborado por los peritos del grupo.

La forma en que estos sistemas de información soportan las actividades de la arquitectura de negocio actual, se describe en el siguiente diagrama.

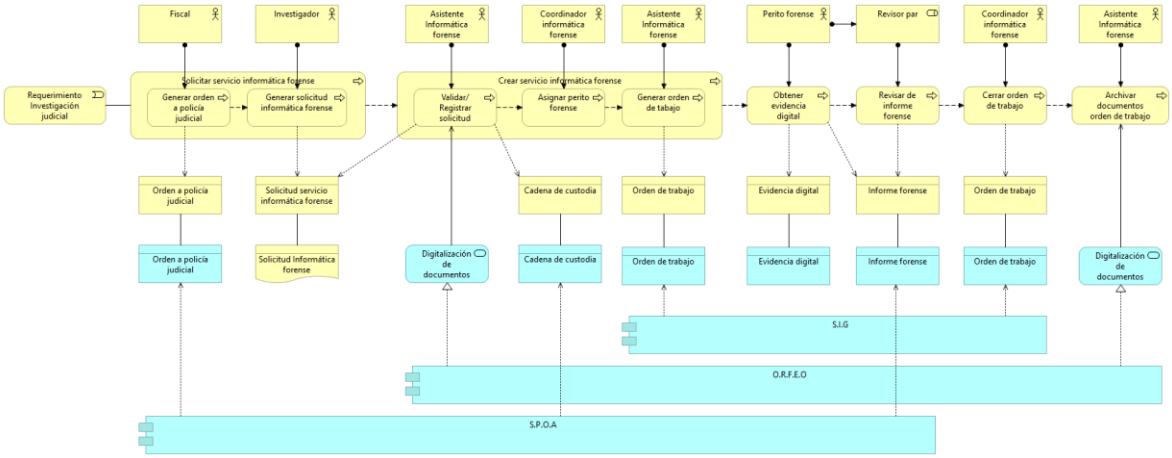


Figura 48. AS-IS fase de aplicación. Fuente: elaboración propia.

5.4.2 Descripción de la arquitectura de información objetivo

En el PETIC 2017 – 2020 de la F.G.N se planteó una arquitectura de información objetivo construida a partir de la "identificación de bloques arquitectónicos que soportan cada una de las capas funcionales de la arquitectura de la institución" (FGN, 2017a, p. 169); el resultado fue la orquestación de diversas soluciones tecnológicas para formar un sistema de información integral (Sistema único de información - SUI), que permita dar respuesta de forma ágil a los requerimientos del negocio.

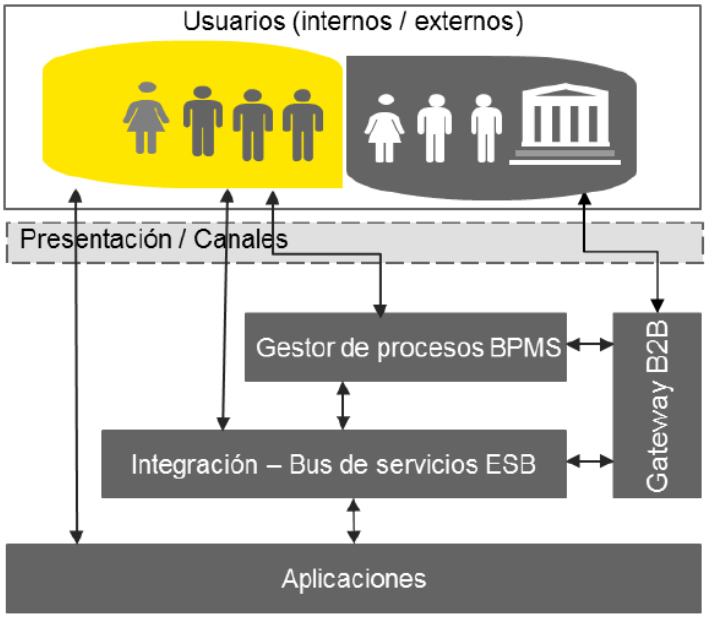


Figura 49. Integración de aplicaciones arquitectura futura FGN, Fuente: Fiscalía General de la Nación. (2017a, p. 118). *Plan estratégico de tecnologías de la información y las comunicaciones [PETIC] 2017-2020.* Manuscrito no publicado.

En la arquitectura institucional objetivo,

> los usuarios externos (personas naturales o jurídicas) acceden a las aplicaciones de la FGN de forma segura (Gateway) a través de sistemas de información y del *front-end* integrado (habilitadas para los canales digitales) que está soportado por un gestor de procesos de negocio (BPM - Business Process Management), el cual consume todos los servicios que requiere a través del componente de intermediación ESB" (FGN, 2017a, p.119),

lo anterior se complementa con un gestor de contenido empresarial (ECM - Enterprise Content Manager) "que será el repositorio de todo el material o archivos digitales asociados a las noticias criminales o casos, que conforman el Expediente Digital" (FGN, 2017a, p.108), por otro lado, los usuarios internos pueden acceder a las aplicaciones de la entidad directamente o a través del bus de servicios empresariales ESB.

Los componentes Gestor de Procesos BPMS, Gateway, Bus de servicios ESB y Aplicaciones, descritos en FGN (2017a), integran el Sistema Único de Información SUI, que está compuesto por diez componentes de aplicación; de los cuales seis participarán en el proceso para la atención de solicitudes de informática forense:

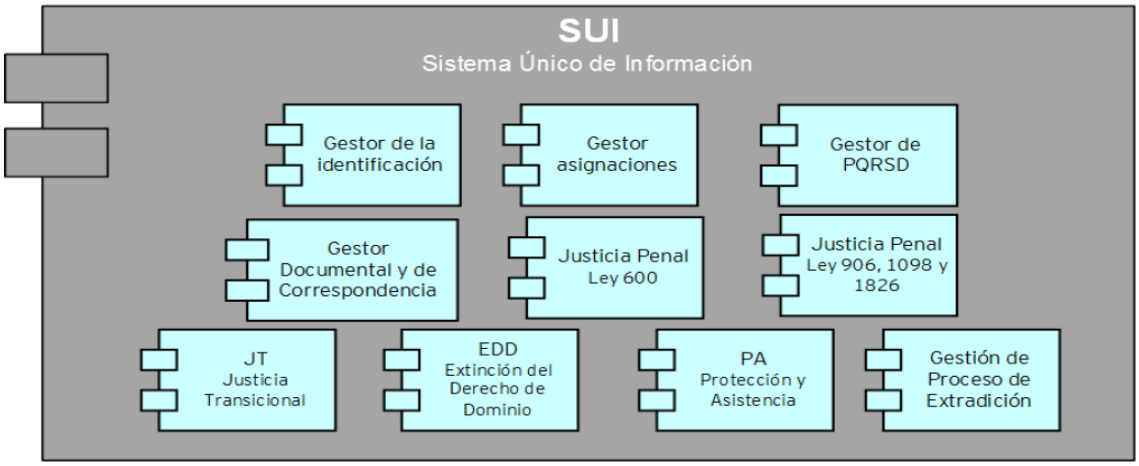


Figura 50. Bloques arquitectónicos de SUI (Sistema Único de Información), Fuente: Fiscalía General de la Nación. (2017a, p. 88). *Plan estratégico de tecnologías de la información y las comunicaciones [PETIC] 2017-2020.* Manuscrito no publicado.

- **Gestor de asignaciones**: Este componente permite la asignación inteligente de casos, orquestando el motor de reglas con sistemas de analítica para evaluar las características del delito y la carga laboral de cada funcionario.
- **Gestor documental y de correspondencia**: Este componente gestiona todos los procesos de gestión documental, incluyendo la gestión de la correspondencia y se integra con el ECM.
- **Justicia Ordinaria – Ley 600**: Componente de SUI que permite controlar y hacer seguimiento a los procesos descritos en la ley 600 del 2000 (Código de Procedimiento Legal), durante las etapas de investigación y juicio.
- **Justicia Ordinaria – Leyes 906, 1098, 1826**: Componente de SUI que permite controlar y hacer seguimiento a los procesos descritos en las leyes 906 de 2005 (Sistema Penal Oral Acusatorio), 1098 de 2006 (Infancia Adolescencia y 1826 de 2017 (Procedimiento Abreviado), para las etapas de investigación y juicio.
- **JT Justicia Transicional**: Componente de SUI que permite controlar y hacer seguimiento a los procesos relacionados con justicia y paz, desde su recepción, hasta el juicio.
- **EDD – Extinción del derecho de dominio**: Componente de SUI que permite controlar y hacer seguimiento a los procesos relacionados con todas las leyes vigentes de extinción de dominio, desde su recepción, hasta el juicio.

En la arquitectura objetivo, la creación de la orden, independiente de la ley que origina el proceso judicial, el registro de los elementos materiales probatorios y el registro de cadena de custodia serán realizados directamente en el sistema único de información SUI, haciendo uso del componente misional de aplicación correspondiente, según el tipo de delito. Adicionalmente, se creará un nuevo componente del gestor de asignaciones encargado de recibir la catalogación del esfuerzo requerido por una solicitud determinada, establecer el tiempo promedio de atención y asignar la orden de trabajo a uno de los peritos del grupo de informática forense, por último, se creará un nuevo módulo para la administración de las actividades de informática forense, en dicho módulo se registrarán los requisitos de cada solicitud que hayan sido definidos en la sesión de entendimiento con la autoridad competente, el informe de la actividad forense realizada y la evidencia contenida en el estudio forense. Este módulo interactuará con los demás componentes del sistema SUI.

“Este sistema debe ser lo suficientemente flexible para responder a la sistematización e inclusión de nuevas leyes o la realización de modificaciones de las existentes de forma oportuna para el negocio” (FGN, 2017a, p.105)

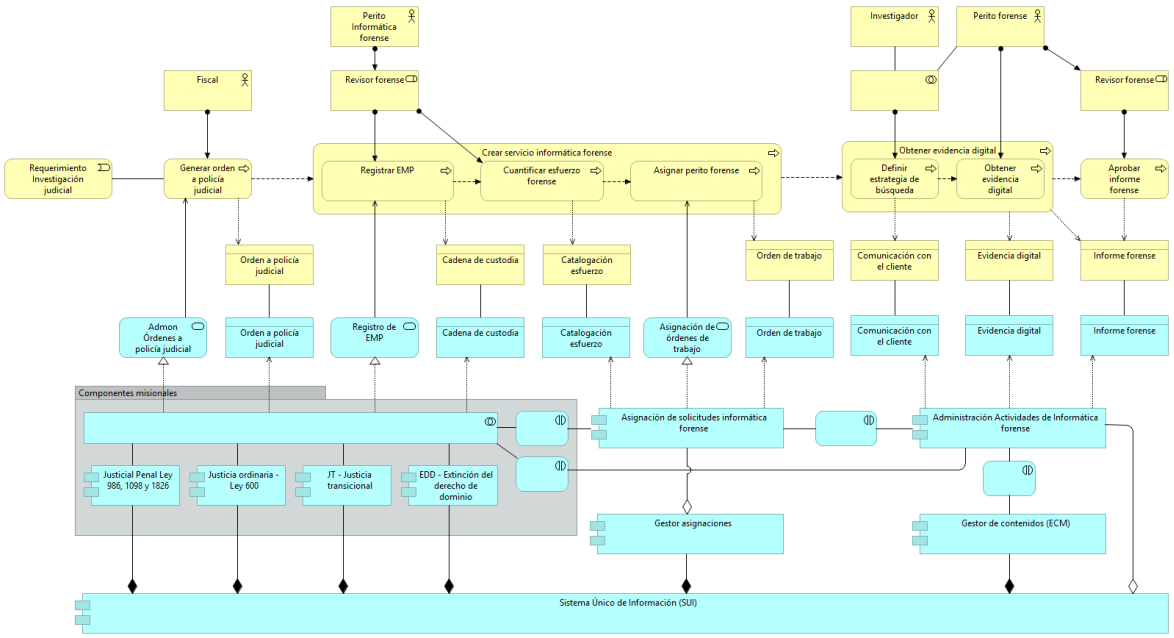


Figura 51. TO-BE fase de aplicación. Fuente: elaboración propia.

5.4.3 Análisis de brechas

De la misma forma que se hizo en la fase de negocio, se analizan las brechas de datos y aplicaciones confrontando las actividades de la línea base de arquitectura

con las planteadas en la arquitectura objetivo, el resultado se refleja en la siguiente matriz.

		Arquitectura objetivo								
		Generar orden a policía judicial	Registrar EMP	Registrar cadena de custodia	Registrar esfuerzo forense	Generar orden de trabajo	Registrar comunicación con el cliente	Generar informe forense digital	Obtener evidencia forense	Almacenar evidencia forense
Arquitectura de línea base			**Nuevo**		**Nuevo**		**Nuevo**			**Nuevo**
Generar orden a policía judicial		Mejorar								
Digitalización de orden de trabajo	Eliminar									
Digitalización solicitud de informática forense	Eliminar									
Registrar cadena de custodia				Mejorar						
Generar orden de trabajo						Mejorar				
Obtener evidencia forense									Mejorar	
Generar informe forense								Mejorar		
Digitalización de informe forense	Eliminar									

Figura 52. Análisis de brechas fase aplicación. Fuente: elaboración propia.

Con base en la información obtenida se formulan cuatro brechas de aplicación:

GAP 1: Crear una interfaz de usuario genérica en los componentes de aplicación misionales, que permita crear órdenes a policía judicial.

GAP 2: Habilitar una nueva funcionalidad, transversal a todos los componentes misionales, que permita registrar elementos materiales probatorios y relacionarlos con las órdenes a policía judicial. En este componente se debe habilitar el registro de cadena de custodia.

GAP 3: Incluir un nuevo módulo en el gestor de asignaciones con la opción de registrar características de los elementos materiales probatorios, que permitan establecer el esfuerzo requerido para atender cada solicitud. Este nuevo componente debe estimar el tiempo necesario para llevar a cabo las actividades de informática forense, seleccionar el perito que realizará el procedimiento y generar la orden de trabajo reutilizando las funcionalidades disponibles en el gestor de asignaciones.

GAP 4: Crear un nuevo componente de aplicación para administrar las actividades de informática forense, con las siguientes funcionalidades:

- Módulo para registrar los requerimientos definidos por la autoridad competente, en cada una de las solicitudes atendidas por el grupo de informática forense.
- Módulo para registrar el informe de la actividad forense realizada en cada requerimiento atendido, con opción para incluir lecciones aprendidas.
- Opción para cargue y descarga de evidencia digital, con acceso restringido de acuerdo con el perfil de cada usuario.

GAP 5: Mejorar el desempeño de las herramientas tecnológicas disponibles para la atención de solicitudes relacionadas con el análisis de información.
En el mapa de ruta de alto nivel se presentan las dependencias entre las brechas identificadas, el detalle de la implementación será descrito en la fase de migración.

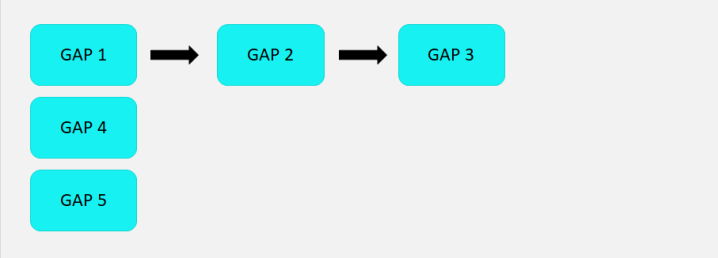


Figura 53. Mapa de ruta de alto nivel, fase de aplicación. Fuente: elaboración propia

5.5 Fase arquitectura de tecnología

Esta fase del ciclo de arquitectura empresarial busca asociar componentes de la arquitectura de aplicaciones con los componentes de tecnología representados en software y hardware. Ofrece una visión más concreta de la forma en que se realizarán y desplegarán los componentes de la aplicación. Proporciona un medio más preciso para evaluar las respuestas a las restricciones (requisitos no funcionales) relacionadas con el Sistema de Información, en particular estimando las necesidades de tamaño de red y hardware o configurando la redundancia del servidor o el almacenamiento (Desfray & Raymond, 2014)

5.5.1 Desarrollo de la línea base de la arquitectura de tecnología

A partir de la información obtenida en la entrevista de conocimiento del proceso para la atención de solicitudes de informática forense se identifican tres sistemas de información ORFEO, SIG y SPOA que son accedidos en las fases del proceso. Con base en la información registrada en el PETIC 2017-2020 facilitado por la Entidad, se pudo conocer a muy alto nivel la infraestructura tecnológica que soporta dichos sistemas, es de anotar que por la condición de la Fiscalía General de la Nación existe cierto nivel de reserva frente a la información, por lo cual no fue posible

acceder al máximo detalle de la infraestructura tecnológica que soporta dichos sistemas.

Servidores:

La Entidad cuenta con un centro de datos principal en el Bunker de la FGN y un centro de datos alterno ubicado en la ciudad de Medellín, este último atiende la sincronización de las bases de datos y mantiene disponibles los sistemas de información críticos, también sirve de contingencia en caso de presentarse algún incidente.

El PETIC documenta un total de 364 servidores, de los cuales 280 son virtuales y 84 físicos; 48 son de pruebas, 10 de desarrollo y 286 de producción; 81 servidores están soportados sobre hardware tipo enclosure.

La capacidad de nube privada que tiene implementada la Entidad permite el uso flexible de recursos de cómputo de acuerdo a los requerimientos de carga de trabajo de cada sistema de información.

Para la virtualización de servidores y ambientes de desarrollo se emplean las herramientas VMware y Hyper-V.

Almacenamiento:

Dentro de la infraestructura, la Entidad cuenta con almacenamiento de tipo SAN para 293 servidores de los 364, con configuración 5X (1 + 0), lo que representa un alto nivel de respaldo.

Bases de Datos:

En la infraestructura de TI se alojan 400 bases de datos, sobre motores Informix, Oracle, PostgreSQL y SQLServer. Más del 80% de las bases de datos corren sobre Informix y el 12% corren sobre Oracle. Las bases de datos de Oracle están montadas sobre Real Application Cluster (RAC) lo que permite tener alta disponibilidad y respuesta ante fallas; para los otros motores no se identificaron configuraciones de alta disponibilidad similares. Actualmente la Entidad maneja el motor Oracle en versiones 11g y 12c. Adicionalmente realiza esfuerzos para migrar bases de datos Informix a la tecnología Oracle.

Sistemas Operativos:

El sistema operativo predominante es Windows con 151 servidores, seguido de Linux con 128 servidores. Las versiones y distribuciones de los sistemas operativos es diversa, para los servidores virtuales el predominante es Red Hat 7.0, para los servidores físicos es Windows Server 2012 R2.

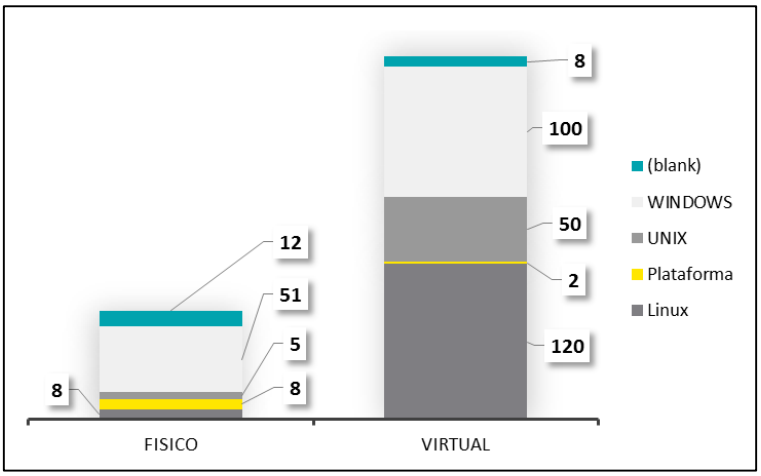


Figura 54. Sistemas operativos instalados en servidores. Fuente: Fiscalía General de la Nación. (2017a, p. 30). *Plan estratégico de tecnologías de la información y las comunicaciones [PETIC] 2017-2020.* Manuscrito no publicado.

Infraestructura de Red

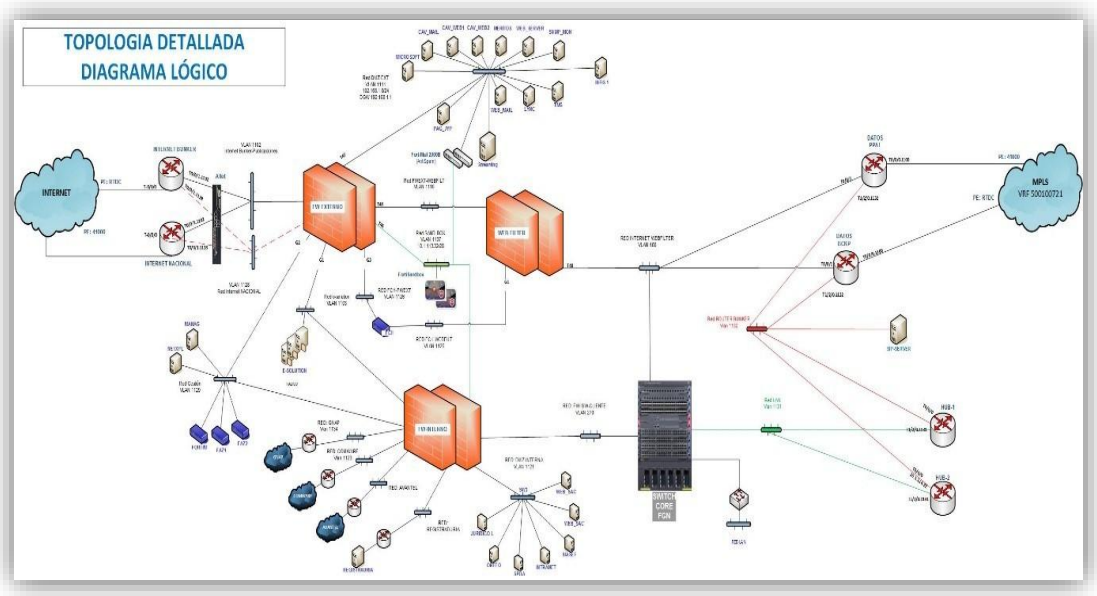


Figura 55. Topología de red. Fuente: Fiscalía General de la Nación. (2017a, p. 31). *Plan estratégico de tecnologías de la información y las comunicaciones [PETIC] 2017-2020.* Manuscrito no publicado.

La Entidad tiene identificadas 871 redes, de las cuales 850 son canal dedicado para el cubrimiento a nivel nacional. De la capacidad disponible en MB (Megabytes), el

35% es para Bogotá, el 9% para Antioquia, y los demás departamentos entre el 2 y 5 % (212 MB en promedio).

La Entidad implementa redes virtuales para segmentación de la red VLAN.

El medio de transmisión de la red principalmente es fibra óptica y en algunas zonas es satelital.

Seguridad:

Para garantizar la seguridad de la red, la Entidad cuenta con modeladores, analizadores, filtrados de contenido, antispam, controlador y switch de seguridad, plataforma de vulnerabilidades FAATS, consola de Antivirus de McAfee, DLP (Data loss prevention), plataforma de APT (amenazas persistentes avanzadas) para protección de ataques, IPS (sistema de protección de intrusos) y SIEM (Security Information Event Management).

Considerando la situación actual descrita en el PETIC 2017-2020, a continuación, se presentan las necesidades identificadas en la arquitectura de tecnología a nivel general.

Figura 56. Necesidades de mejora servicios tecnológicos. Fuente: Fiscalía General de la Nación. (2017a, p. 120). *Plan estratégico de tecnologías de la información y las comunicaciones [PETIC] 2017-2020.* Manuscrito no publicado.

Con relación a la infraestructura tecnológica que soporta los tres (3) sistemas de información documentados en el proceso para la atención de solicitudes en el Grupo

de Informática Forense (ORFEO, SPOA y SIG), se logró establecer que están soportados en servidores de aplicaciones y servidores de bases de datos, no necesariamente separados, considerando el entorno virtualizado en el que trabaja la Entidad.

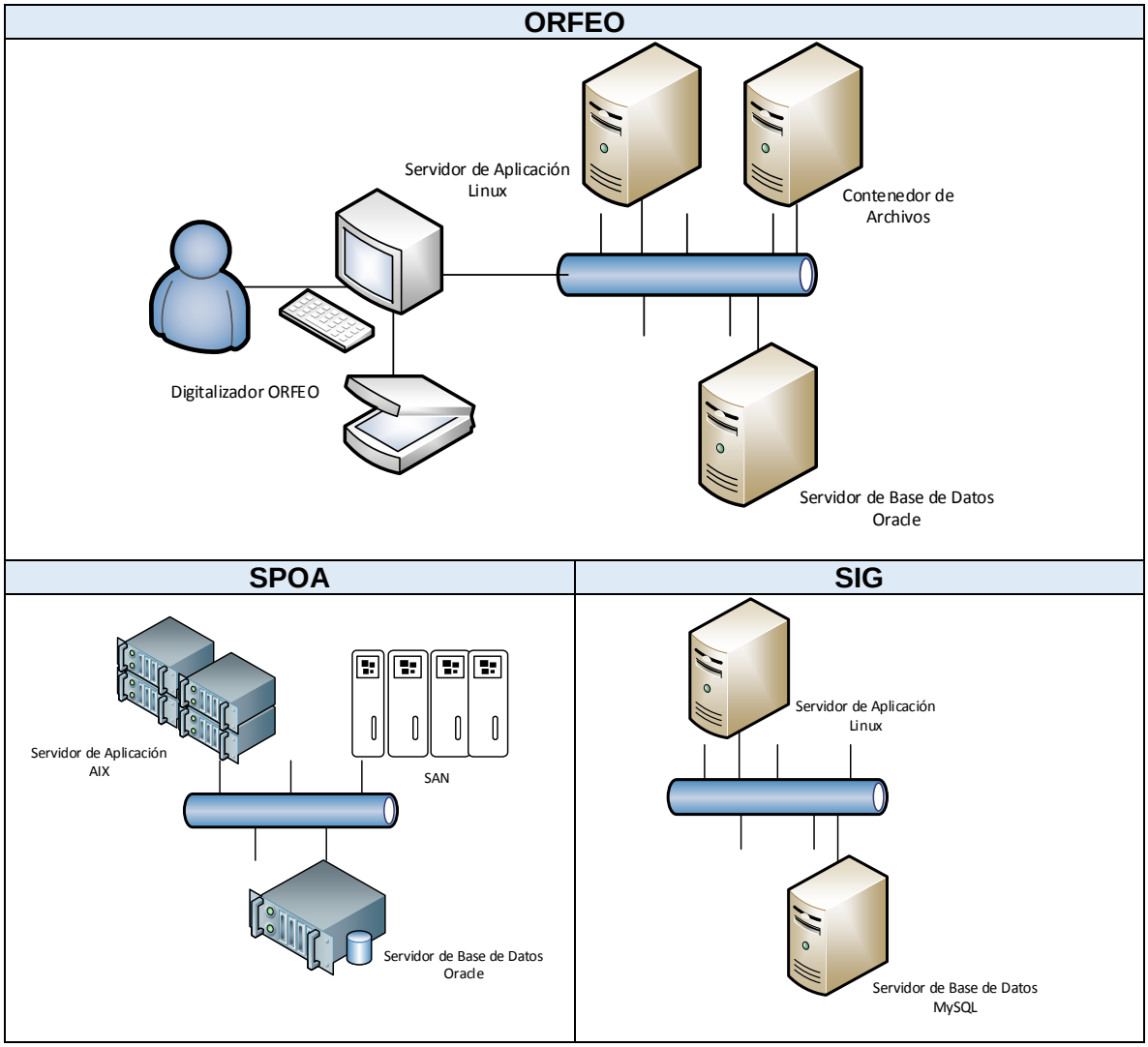


Figura 57. Infraestructura sistemas de información SPOA, SIG, ORFEO. Fuente: elaboración propia.

5.5.2 Descripción de la línea base de arquitectura de tecnología

La línea base de arquitectura de tecnología corresponde a una representación de la infraestructura tecnológica que soporta los sistemas de información intervinientes en el proceso para la atención de solicitudes en el grupo de informática forense,

esta información es obtenida como resultado de las entrevistas adelantadas y a través del PETIC 2017-2020 de la Entidad.

A continuación, se presenta la línea base de la arquitectura de tecnología en lenguaje archimate.

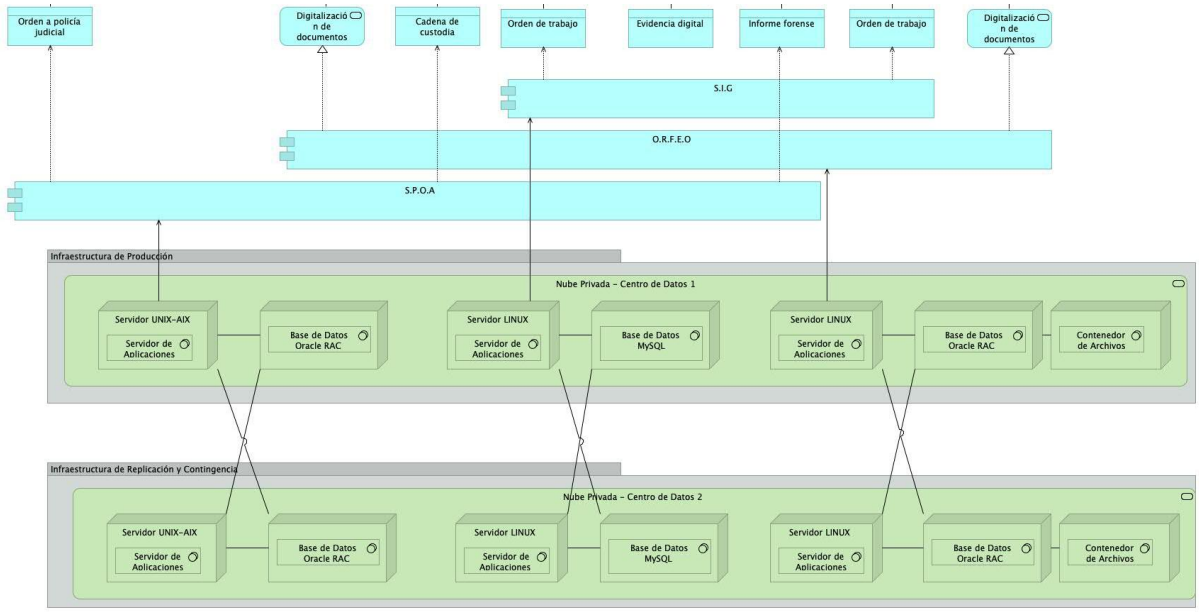


Figura 58. AS-IS capa de tecnología. Fuente: elaboración propia.

5.5.3 Desarrollo de la arquitectura de tecnología objetivo

Con la información recolectada en las entrevistas de conocimiento del proceso para la atención de solicitudes de informática forense y la información registrada en el PETIC 2017-2020, se consideran los siguientes aspectos como oportunidades de mejora en el ámbito de la arquitectura de tecnología y se enumeran según su nivel de criticidad

1. El proceso para la asignación de órdenes de trabajo en el Grupo se realiza de forma manual, considerando su complejidad se requiere una herramienta que permita sistematizar y automatizar dicho proceso.
2. Para la generación de órdenes a policía judicial y elaboración de informes se prefiere el uso de papel en lugar de hacer uso de la funcionalidad disponible en el sistema de información SPOA, según lo referenciaban las entrevistas de conocimiento del proceso, por una parte se siente desconfianza en la seguridad de los sistemas de información y por otra hay desconocimiento o falta de interés sobre la forma en que se pueden gestionar las órdenes a través del sistema de información, existe la percepción de que el papel

garantiza mayor confidencialidad de los procesos judiciales y proporciona mayor facilidad. Para el caso de informes, si bien SPOA tiene un módulo para el registro de los mismos, los campos e información incluida no corresponden a la estructura y contenido del informe que se realiza en el Grupo de Informática Forense. La FGN cuenta con el Programa para la Gestión de Documentos Electrónicos (Cero Papel) aplicable a todas las actividades misionales y servicios de la Entidad, la cual

> reducir el consumo de papel mediante la implementación de estrategias de, ahorro, aplicación de TIC'S y sensibilización a los servidores y contratistas, enfocadas al fortalecimiento de nuevos mecanismos de comunicación e información que disminuyan los costos y tiempos administrativos de los diferentes procesos y que generen un aporte social y ambiental importante (Fiscalía General de la Nación, 2018c, p.14).

3. Existe baja integración entre los sistemas de información ORFEO, SIG y SPOA; generalmente se debe registrar manualmente la misma información en más de una aplicación.
4. El aplicativo SPOA no cuenta con una interfaz que permita incluir la información digital resultante de los estudios forenses (evidencia derivada). La entrega de dichos resultados se realiza en medios de almacenamiento como CD, DVD, Blu-Ray, Discos Duros que están expuestos a fallas y daño por el manejo, transporte o almacenamiento inadecuado y el transcurrir del tiempo.
5. No se cuenta con una base de datos de conocimiento que permita el registro de lecciones aprendidas o la solución a un problema específico, con el objetivo de evitar reproceso en la actividad pericial.

5.5.4 Arquitectura de tecnología objetivo

Alcanzar los objetivos propuestos, implica optimizar el proceso actual para la atención de solicitudes de informática forense; con la arquitectura de tecnología actualizada se pretende contar con la infraestructura que soporte en los sistemas de información, nuevos módulos orientados a: disminuir los re-procesos originados al registrar la misma información en diferentes aplicativos, automatizar la asignación de órdenes de trabajo y usar de manera más eficiente las herramientas disponibles en la Entidad y que permitan generar mayor valor Institucional con la información obtenida por el Grupo.

La arquitectura de tecnología propuesta para el presente ejercicio debe estar alineada con la arquitectura institucional de la FGN, en tal sentido, a continuación se documenta la visión planteada en el PETIC 2017-2020, referente a los sistemas

de información intervinientes en el proceso para la atención de solicitudes de informática forense:

- Los dos centros de datos que alojan los sistemas críticos de la Entidad se mantendrán en infraestructura de nube privada altamente disponible, controlada por balanceadores de carga.
- La conexión de las diferentes sedes de la Entidad a los centros de datos se realiza a través de MPLS.
- Para mejorar el rendimiento de la red se emplearán dos canales activos dedicados por cada sede de la Entidad, en lo posible contratados con operadores diferentes, se solicitará al menos a uno, el suministro de balanceadores por sede; los canales dedicados se comunicarán por medio de fibra óptica oscura al centro de datos más cercano.
- En cada centro de datos, el tráfico de red WAN se gestionará a través de dos balanceadores externos y uno interno.
- La salida a internet y los datos transferidos serán controlados a través de los sistemas de seguridad dispuestos en los centros de datos.
- El tráfico de red empleará protocolo Ipv6 con IPSec y cifrамiento de todas las comunicaciones.
- La infraestructura a nivel WAN contempla canales MPLS, switches, routers, balanceadores, VPNs, firewalls, DLP, analizadores y monitoreo de red, SOC, entre otros.

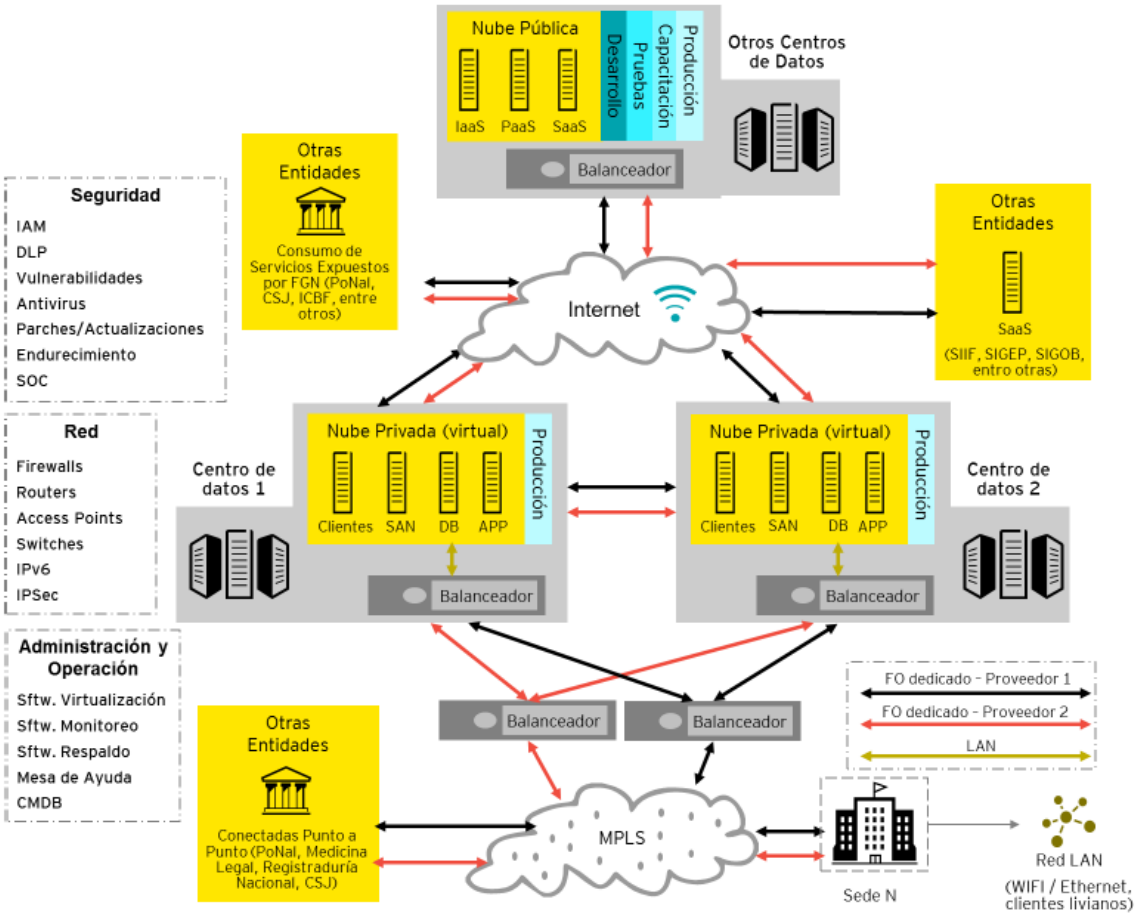


Figura 59. Diagrama general de infraestructura futura. Fuente: Fiscalía General de la Nación. (2017a, p. 121). *Plan estratégico de tecnologías de la información y las comunicaciones [PETIC] 2017-2020.* Manuscrito no publicado.

5.5.5 Descripción de la arquitectura de tecnología objetivo

La arquitectura de tecnología objetivo corresponde a una representación del proceso para la atención de solicitudes de informática forense, obtenida como resultado de relacionar las necesidades documentadas en el PETIC 2017-2020, las dificultades identificadas en las entrevistas con los diferentes roles intervinientes en el proceso y en respuesta a los objetivos del negocio, que fueron planteados con base en las preocupaciones identificadas en la etapa de recolección de información.

A continuación, se presenta la vista de tecnología del proceso objetivo elaborada en lenguaje archimate.

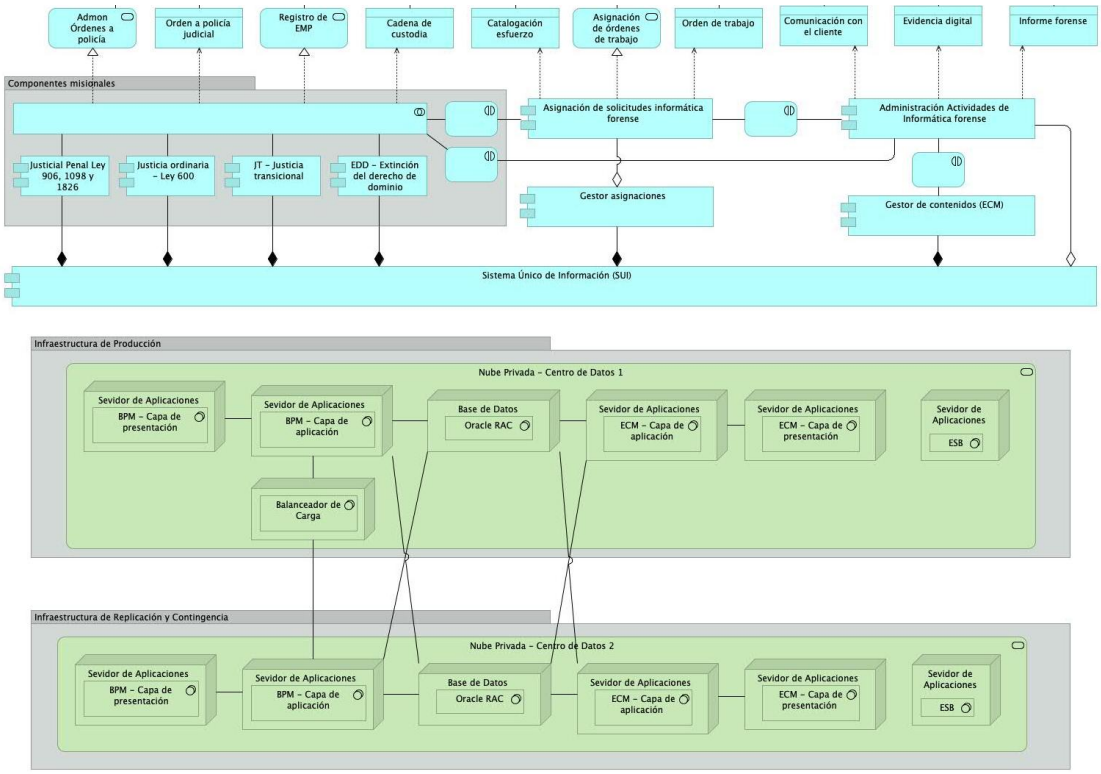


Figura 60. TO-BE capa de tecnología. Fuente: elaboración propia.

5.5.6 Análisis de brechas

El análisis parte del hecho que, en la actualidad, la Entidad se encuentra implementando la arquitectura institucional, en este sentido la SubTic está siguiendo el mapa de ruta trazado por el PETIC 2017-2020. En lo referente a los sistemas de información intervinientes actualmente en el proceso para atención de solicitudes de informática forense, la Entidad está ejecutando el proyecto del SUI (Sistema Único de Información), el cual, como se mencionó en la fase de arquitectura de aplicación, agrupa los sistemas de información que apoyan la gestión misional de la Entidad y está basado en BPM, ECM, Motor de Reglas ESB, Gateway y Gestor de Casos, agrupados en un solo bloque arquitectónico.

	Arquitectura de tecnología objetivo					
	BPM capa de presentación	BPM capa de aplicación	Base de datos	ECM capa de aplicación	ECM capa de presentación	ESB
Arquitectura de tecnología línea base						
BPM capa de presentación	Mejorar					
BPM capa de aplicación		Mejorar				
Base de datos			Mejorar			
ECM capa de aplicación				Mantener		
ECM capa de presentación					Mejorar	
ESB						Mejorar

Figura 61. Matriz para la evaluación de brechas de tecnología. Fuente: elaboración propia.

GAP 1: La infraestructura que soporta la capa de presentación del BPM requiere aumento de memoria para soportar las nuevas funcionalidades de usuario planteadas en la arquitectura de aplicaciones.

GAP 2: La infraestructura que soporta la capa de aplicación del BPM debe incrementar sus capacidades de memoria y procesamiento a fin de atender los nuevos módulos requeridos para la inclusión de información detallada sobre los EMP/EF, las órdenes a policía judicial, la asignación automática de órdenes de trabajo y la conservación de la evidencia digital.

GAP 3: Se requiere un incremento de memoria y capacidad de procesamiento en la capa de aplicación del gestor de contenidos ECM, que soporte la carga de grandes volúmenes de información no estructurada hacia la base de datos.

GAP 4: Se requiere un aumento en la capacidad de almacenamiento del gestor de contenidos ECM, con el fin de conservar y disponibilizar el resultado de los estudios de informática forense.

GAP 5: En el ESB se requiere un incremento de memoria para soportar los nuevos servicios web que habilitarán la interacción entre los componentes propuestos en la arquitectura de aplicación.

A partir de las brechas identificadas se construye un mapa de ruta de alto nivel que será refinado en la fase de migración. En esta primera etapa se analizan únicamente las posibles dependencias entre los proyectos planteados.

Figura 62. Mapa de ruta de alto nivel, fase de tecnología. Fuente: elaboración propia.

5.6 Oportunidades y soluciones

Las brechas identificadas en las fases de negocio, aplicaciones y tecnología son agrupadas en iniciativas orientadas al logro de los objetivos planteados en la visión de arquitectura; como resultado se generan cinco propuestas de mejora:

Nombre del proyecto	Brecha asociada
Proyecto Orden digital	GAP 1
	GAP 1
	GAP 1
	GAP 2
	GAP 5
Proyecto EMP virtual	GAP 2
	GAP 3
	GAP 2
	GAP 1
	GAP 2
	GAP 5
Proyecto AVIF Asistente virtual de informática forense	GAP 5
	GAP 6
	GAP 7
	GAP 8
	GAP 4
	GAP 1

Nombre del proyecto	Brecha asociada
	GAP 2
	GAP 3
	GAP 4
	GAP 5
Proyecto Orquestador Gestor de asignaciones de informática forense	GAP 4
	GAP 3
	GAP 2
Proyecto Nivelación de capacidades técnicas de informática forense	GAP 9
	GAP 5

Figura 63. Relación de proyectos y brechas identificadas. Fuente: elaboración propia.

5.6.1 Nombre del proyecto: Orden Digital

Descripción: Crear una nueva opción en el portal interno de la Fiscalía General de la Nación, en donde las autoridades competentes, a través de un formulario electrónico intuitivo, puedan crear órdenes (según corresponda en las diferentes legislaciones) y hacer seguimiento a las mismas durante todo su ciclo de vida. El sistema debe permitir relacionar las órdenes creadas con los elementos materiales probatorios que serán objeto de investigación, presentar información del perito forense encargado de atender la solicitud, reportar el tiempo estimado de atención y permitir la descarga del informe forense y la evidencia derivada; para ello este nuevo módulo debe interactuar con los componentes de aplicación misionales, el gestor de asignaciones y el gestor de contenidos, a través de una arquitectura orientada a servicios.

Los componentes impactados se presentan en la plantilla de aplicaciones:

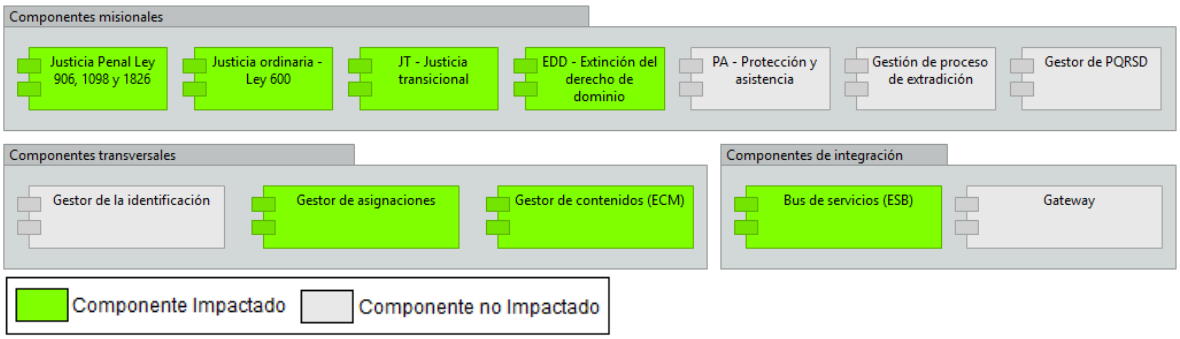


Figura 64. Plantilla de aplicaciones F.G.N Proyecto Orden digital. Fuente: elaboración propia.

Con base en los impactos identificados se realiza una estimación por juicio de expertos (esfuerzo y costo) de alto nivel; los costos unitarios se establecen promediando las tarifas de varios proveedores de tecnología que operan en el país, asumiendo una TRM de 3200 pesos colombianos (COP) y un impuesto al valor agregado (IVA) del 19%.

Nombre del proyecto **Orden digital**

ESTIMACIÓN DE ALTO NIVEL - ESFUERZO Y COSTO

Etapa	Esfuerzo Estimado	% de Holgura del esfuerzo	Esfuerzo Estimado (con holgura)	Perfil	Cantidad de recursos	% de Asignación	Duración (días)	Costo unitario	Costo total
Gestión del Proyecto	298,8	20%	358,56	Project manager	1	15%	332,0	$ 94.000	$ 33.704.640
Requerimientos									
Definición de requisitos	80	10%	88	Usuario de negocio	1	50%	24,4	$ -	$ -
Levantamiento de requerimientos	80	10%	88	Líder funcional	1	50%	24,4	$ 94.000	$ 8.272.000
Aplicación ESB									
Análisis técnico	65	10%	71,5	Líder técnico	1	100%	9,9	$ 81.000	$ 5.791.500
Diseño técnico	65	10%	71,5	Líder técnico	1	100%	9,9	$ 81.000	$ 5.791.500
Desarrollo (incluye Pruebas unitarias)	302	10%	332,2	Desarrollador ESB	2	100%	23,1	$ 81.000	$ 26.908.200
Sistemas misionales									
Análisis técnico	60	10%	66	Arquitecto de software	1	100%	9,2	$ 94.000	$ 6.204.000
Diseño técnico	60	10%	66	Arquitecto de software	1	100%	9,2	$ 94.000	$ 6.204.000
Desarrollo (incluye Pruebas unitarias)	360	10%	396	Desarrollador	2	100%	27,5	$ 65.500	$ 25.938.000
Prueba de Integración de sistemas	80	10%	88	Analista tester	2	100%	6,1	$ 65.500	$ 5.764.000
Aplicación Gestor de contenidos (ECM)					2				
Análisis técnico	24	10%	26,4	Arquitecto de software	1	100%	3,7	$ 94.000	$ 2.481.600
Diseño técnico	32	10%	35,2	Arquitecto de software	1	100%	4,9	$ 94.000	$ 3.308.800
Desarrollo (incluye Pruebas unitarias)	64	10%	70,4	Desarrollador aplicación	1	100%	9,8	$ 65.500	$ 4.611.200
Desarrollo (incluye Pruebas unitarias)	48	10%	52,8	Desarrollador PL/SQL	1	100%	7,3	$ 65.500	$ 3.458.400
Aplicación Gestor de asignaciones									
Análisis técnico	16	10%	17,6	Arquitecto de software	1	100%	2,4	$ 94.000	$ 1.654.400
Diseño técnico	24	10%	26,4	Arquitecto de software	1	100%	3,7	$ 94.000	$ 2.481.600
Desarrollo (incluye Pruebas unitarias)	72	10%	79,2	Desarrollador	1	100%	11,0	$ 65.500	$ 5.187.600
Pruebas									
Pruebas Funcionales	720	10%	792	Analista tester	3	100%	36,7	$ 65.500	$ 51.876.000
Capacitaciones									
Capacitación uso de la herramienta	133	10%	146,3	Líder funcional	5	50%	8,1	$ 94.000	$ 13.752.200
Infraestructura									
Procesamiento 8 CPUs virtuales con 32 GB de RAM. costo por 3 años	1	5%	1,05	Proveedor nube privada	0	0%	0,0	$ 20.338.528	$ 21.355.454
Memoria RAM Servidor ESB (GB)	3	5%	3,15	Proveedor infraestructura	0	0%	0,0	$ 760.000	$ 2.394.000
Esfuerzo Total	**2584,8**		**2873,11**		**26**		**Costo Total**		**$ 237.139.094**

Figura 65. Estimación proyecto orden digital. Fuente: elaboración propia.

5.6.2 Nombre del proyecto: EMP Virtual

Descripción: Crear una nueva opción en el portal interno de la Fiscalía General de la Nación, en donde los investigadores puedan registrar los elementos materiales probatorios que forman parte de las investigaciones judiciales, el sistema debe permitir que se especifiquen las características técnicas y morfológicas de los elementos materiales probatorios, ofrecer una opción de captura rápida para efectuar el registro de continuidad en la cadena de custodia, verificar el recorrido histórico de cada elemento y facilitar su relación con las órdenes digitales a policía judicial. Este nuevo módulo será incluido en los componentes de aplicación misionales y debe poder interactuar con las funcionalidades del módulo orden digital, mediante una arquitectura orientada a servicios.

Los componentes impactados se presentan en la plantilla de aplicaciones:

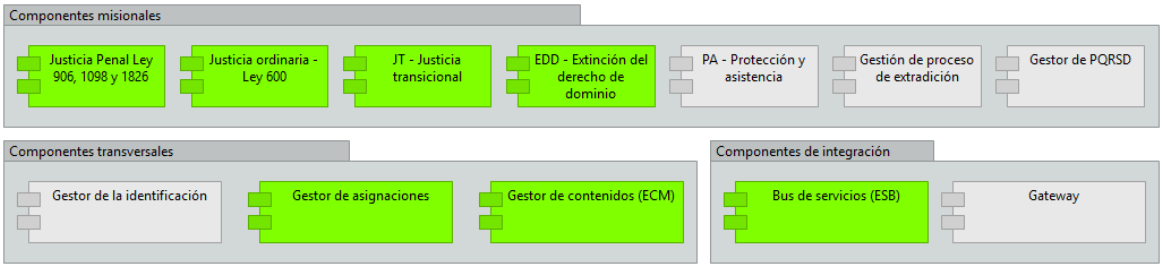


Figura 66. Plantilla de aplicaciones F.G.N Proyecto EMP Virtual. Fuente: elaboración propia.

Nombre del proyecto **EMP Virtual**

ESTIMACIÓN DE ALTO NIVEL - ESFUERZO Y COSTO									
Etapa	**Esfuerzo Estimado**	**% de Holgura del esfuerzo**	**Esfuerzo Estimado (con holgura)**	**Perfil**	**Cantidad de recursos**	**% de Asignación**	**Duración (días)**	**Costo unitario**	**Costo total**
Gestión del Proyecto	165	20%	198	Project manager	1	15%	183,3	$ 94.000	$ 18.612.000
Requerimientos									
Definición de requisitos	80	10%	88	Usuario de negocio	1	50%	24,4	$ -	$ -
Levantamiento de requerimientos	80	10%	88	Líder funcional	1	50%	24,4	$ 94.000	$ 8.272.000
Aplicación ESB									
Análisis técnico	21	10%	23,1	Líder técnico	1	100%	3,2	$ 81.000	$ 1.871.100
Diseño técnico	21	10%	23,1	Líder técnico	1	100%	3,2	$ 81.000	$ 1.871.100
Desarrollo (incluye Pruebas unitarias)	102	10%	112,2	Desarrollador ESB	2	100%	7,8	$ 81.000	$ 9.088.200
Sistemas misionales									
Análisis técnico	119	10%	130,9	Arquitecto de software	1	100%	18,2	$ 94.000	$ 12.304.600
Diseño técnico	119	10%	130,9	Arquitecto de software	1	100%	18,2	$ 94.000	$ 12.304.600
Desarrollo (incluye Pruebas unitarias)	571	10%	628,1	Desarrollador	2	100%	43,6	$ 65.500	$ 41.140.550
Prueba de Integración de sistemas	143	10%	157,3	Analista tester	2	100%	10,9	$ 65.500	$ 10.303.150
Pruebas									
Pruebas Funcionales	400	10%	440	Analista tester	2	100%	30,6	$ 65.500	$ 28.820.000
Capacitaciones									
Capacitación uso de la herramienta	40	10%	44	Líder funcional	1	50%	12,2	$ 94.000	$ 4.136.000
Infraestructura									
Procesamiento 4 CPUs virtuales con 16 GB de RAM. costo por 3 años	1	5%	1,05	Proveedor nube privada	0	0%	0,0	$ 10.171.168	$ 10.679.726
Memoria RAM Servidor ESB (GB)	1	10%	1,1	Proveedor infraestructura	0	0%	0,0	$ 760.000	$ 836.000
Esfuerzo Total	**1861**		**2063,6**		**14**		**Costo Total**		**$ 160.239.026**

Figura 67. Estimación proyecto EMP Virtual. Fuente: elaboración propia.

5.6.3 Nombre del proyecto: Asistente virtual de informática forense (AVIF)

Descripción: Nuevo módulo web de acceso interno a través del cual los peritos de informática forense podrán registrar y consultar los resultados de su actividad misional. El módulo debe contar con formularios electrónicos para ingresar los requerimientos detallados de cada solicitud, el informe de policía judicial que describe la actividad pericial realizada, lecciones aprendidas del proceso y un registro fotográfico de los elementos materiales probatorios; adicionalmente, la aplicación debe permitir el cargue de la evidencia digital obtenida, haciendo uso de las funcionalidades del gestor de contenidos. Toda la información registrada en este sistema podrá ser consultada por las autoridades competentes, a través de la opción Orden Digital en el portal interno de la F.G.N.

Los componentes impactados se presentan en la plantilla de aplicaciones:

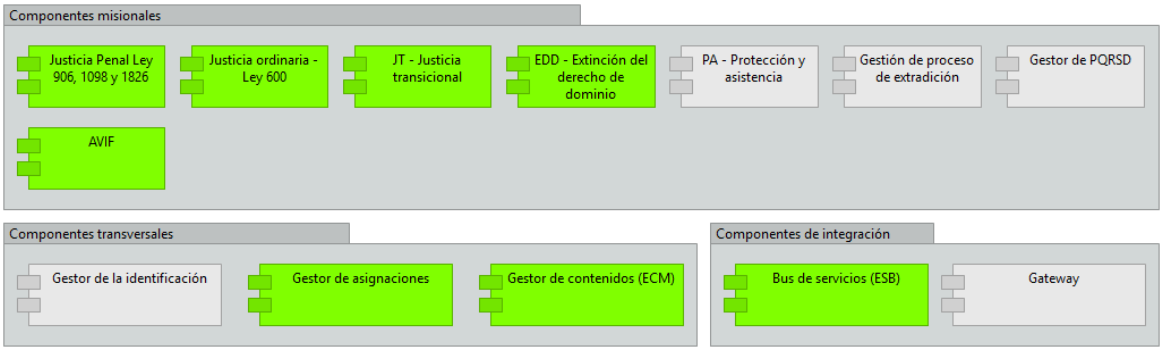


Figura 68. Plantilla de aplicaciones F.G.N Proyecto AVIF. Fuente: elaboración propia

Nombre del proyecto	Asistente virtual AVIF								
ESTIMACIÓN DE ALTO NIVEL - ESFUERZO Y COSTO									
Etapa	**Esfuerzo Estimado**	**% de Holgura del esfuerzo**	**Esfuerzo Estimado (con holgura)**	**Perfil**	**Cantidad de recursos**	**% de Asignación**	**Duración (días)**	**Costo unitario**	**Costo total**
Gestión del Proyecto	440	20%	528	Project manager	1	15%	488,9	$ 94.000	$ 49.632.000
Requerimientos									
Definición de requisitos	150	10%	165	Usuario de negocio	1	50%	45,8	$ -	$ -
Levantamiento de requerimientos	150	10%	165	Líder funcional	1	50%	45,8	$ 94.000	$ 15.510.000
Aplicación ESB									
Análisis técnico	64	10%	70,4	Líder técnico	1	100%	9,8	$ 81.000	$ 5.702.400
Diseño técnico	64	10%	70,4	Líder técnico	1	100%	9,8	$ 81.000	$ 5.702.400
Desarrollo (incluye Pruebas unitarias)	232	10%	255,2	Desarrollador ESB	2	100%	17,7	$ 81.000	$ 20.671.200
Sistemas misionales									
Análisis técnico	20	20%	24	Arquitecto de software	1	100%	3,3	$ 94.000	$ 2.256.000
Diseño técnico	20	20%	24	Arquitecto de software	1	100%	3,3	$ 94.000	$ 2.256.000
Desarrollo (incluye Pruebas unitarias)	90	20%	108	Desarrollador	1	100%	15,0	$ 65.500	$ 7.074.000
Prueba de Integración de sistemas	30	20%	36	Analista tester	1	100%	5,0	$ 65.500	$ 2.358.000
Aplicación Gestor de contenidos (ECM)					2				
Análisis técnico	16	10%	17,6	Arquitecto de software	1	100%	2,4	$ 94.000	$ 1.654.400
Diseño técnico	20	10%	22	Arquitecto de software	1	100%	3,1	$ 94.000	$ 2.068.000
Desarrollo (incluye Pruebas unitarias)	60	10%	66	Desarrollador aplicación	1	100%	9,2	$ 65.500	$ 4.323.000
Desarrollo (incluye Pruebas unitarias)	40	10%	44	Desarrollador PL/SQL	1	100%	6,1	$ 65.500	$ 2.882.000
Aplicación Gestor de asignaciones									
Análisis técnico	15	20%	18	Arquitecto de software	1	100%	2,5	$ 94.000	$ 1.692.000
Diseño técnico	15	20%	18	Arquitecto de software	1	100%	2,5	$ 94.000	$ 1.692.000
Desarrollo (incluye Pruebas unitarias)	60	20%	72	Desarrollador	1	100%	10,0	$ 65.500	$ 4.716.000
Aplicación Asistente virtual AVIF									
Análisis técnico	327	20%	392,4	Arquitecto de software	1	100%	54,5	$ 94.000	$ 36.885.600
Diseño técnico	327	20%	392,4	Arquitecto de software	1	100%	54,5	$ 94.000	$ 36.885.600
Desarrollo (incluye Pruebas unitarias)	1310	20%	1572	Desarrollador	3	100%	72,8	$ 65.500	$ 102.966.000
Prueba de Integración de sistemas	220	20%	264	Analista tester	3	100%	12,2	$ 65.500	$ 17.292.000
Pruebas									
Pruebas Funcionales	1600	20%	1920	Analista tester	4	100%	66,7	$ 65.500	$ 125.760.000
Capacitaciones									
Capacitación uso de la herramienta	16	10%	17,6	Líder funcional	1	100%	2,4	$ 94.000	$ 1.654.400
Infraestructura									
Procesamiento 2 CPUs virtuales con 8 GB de RAM. costo por 3 años	1	5%	1,05	Proveedor nube privada	0	0%	0,0	$ 5.083.680	$ 5.337.864
Memoria RAM Servidor ESB (GB)	2	5%	2,1	Proveedor infraestructura	0	0%	0,0	$ 760.000	$ 1.596.000
Almacenamiento 50 TB por un año	1	5%	1,05	Proveedor nube privada	0	0%	0,0	$ 59.404.800	$ 62.375.040
Esfuerzo Total	**5286**		**6262**		**31**		**Costo Total**		**$ 520.941.904**

Figura 69. Estimación proyecto AVIF. Fuente: elaboración propia.

5.6.4 Nombre del proyecto: Orquestador

Descripción: Crear un nuevo componente de aplicación en el gestor de asignaciones que a través de procesos de analítica experta pueda asignar automáticamente las órdenes de trabajo a cada perito forense; este componente debe estar en capacidad de priorizar las solicitudes recibidas con base en el tipo de delito, establecer el tiempo máximo de atención de acuerdo con las características técnicas de los elementos materiales probatorios y enviar alertas vía correo electrónico a la autoridad solicitante y al perito forense asignado. El nuevo módulo

debe interactuar con los componentes misionales, aplicando los principios de la arquitectura orientada a servicios.

Los componentes impactados se presentan en la plantilla de aplicaciones:

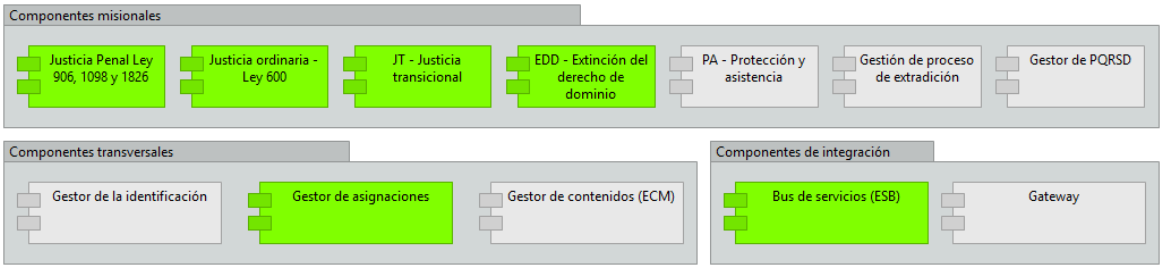


Figura 70. Plantilla de aplicaciones F.G.N Proyecto Orquestador. Fuente: elaboración propia.

Nombre del proyecto **Orquestador**

ESTIMACIÓN DE ALTO NIVEL - ESFUERZO Y COSTO									
Etapa	**Esfuerzo Estimado**	**% de Holgura del esfuerzo**	**Esfuerzo Estimado (con holgura)**	**Perfil**	**Cantidad de recursos**	**% de Asignación**	**Duración (días)**	**Costo unitario**	**Costo total**
Gestión del Proyecto	92	20%	110,4	Project manager	1	15%	102,2	$ 94.000	$ 10.377.600
Requerimientos									
Definición de requisitos	60	10%	66	Usuario de negocio	1	50%	18,3	$ -	$ -
Levantamiento de requerimientos	60	10%	66	Líder funcional	1	50%	18,3	$ 94.000	$ 6.204.000
Aplicación ESB									
Análisis técnico	15	20%	18	Líder técnico	1	100%	2,5	$ 81.000	$ 1.458.000
Diseño técnico	20	20%	24	Líder técnico	1	100%	3,3	$ 81.000	$ 1.944.000
Desarrollo (incluye Pruebas unitarias)	100	20%	120	Desarrollador ESB	1	100%	16,7	$ 81.000	$ 9.720.000
Sistemas misionales									
Análisis técnico	20	20%	24	Arquitecto de software	1	100%	3,3	$ 94.000	$ 2.256.000
Diseño técnico	20	20%	24	Arquitecto de software	1	100%	3,3	$ 94.000	$ 2.256.000
Desarrollo (incluye Pruebas unitarias)	90	20%	108	Desarrollador	1	100%	15,0	$ 65.500	$ 7.074.000
Prueba de Integración de sistemas	30	20%	36	Analista tester	1	100%	5,0	$ 65.500	$ 2.358.000
Aplicación Gestor de asignaciones									
Análisis técnico	110	20%	132	Analista BI	1	100%	18,3	$ 320.000	$ 42.240.000
Diseño técnico	82	20%	98,4	Analista BI	1	100%	13,7	$ 320.000	$ 31.488.000
Desarrollo (incluye Pruebas unitarias)	128	20%	153,6	Desarrollador Senior	1	100%	21,3	$ 320.000	$ 49.152.000
Pruebas									
Pruebas Funcionales	120	20%	144	Analista tester	1	100%	20,0	$ 65.500	$ 9.432.000
Infraestructura									
Procesamiento 2 CPUs virtuales con 4GB de RAM. costo por 3 años	1	5%	1,05	Proveedor nube privada	0	0%	0,0	$ 2.543.744	$ 2.670.931
Esfuerzo Total	**947**		**1124,4**		**13**		**Costo Total**		**$ 178.630.531**

Figura 71. Estimación proyecto orquestador. Fuente: elaboración propia.

5.6.5 Nombre del proyecto: Nivelación de capacidades técnicas

Descripción: Fortalecer las capacidades técnicas del equipo de informática forense por medio de la nivelación de conocimientos técnicos especializados entre los peritos del grupo.

Capacitaciones:

- Conocimiento interno: Los peritos más experimentados en cada tipo de actividad o dispositivo, realizarán capacitaciones a los demás miembros del grupo, el objetivo será impartir lineamientos básicos para la atención de los distintos requerimientos que deben ser atendidos por el Grupo.
- Plan padrino: Los peritos más experimentados destinarán un porcentaje de su tiempo para asesorar a otros peritos con menor grado de expertise en la

atención de determinadas solicitudes, el objetivo es desarrollar conocimiento a través de la práctica con acompañamiento.

- Conocimiento especializado: Capacitaciones dictadas por expertos en informática forense, con conocimiento especializado en sistemas informáticos y herramientas de cloud computing, el objetivo es orientar al equipo de peritos del Grupo respecto a la forma de obtener evidencia digital en nuevos entornos.

Capacitaciones en Informática forense

ESTIMACIÓN DE ALTO NIVEL - ESFUERZO Y COSTO					
Etapa	**Participantes**	**Orientador**	**Duración (Horas)**	**Costo unitario**	**Costo total**
Conocimiento interno Dispositivos móviles	26	Interno	12,0	$ -	$ -
Conocimiento interno DVR y bases de datos	26	Interno	12,0	$ -	$ -
Conocimiento especializado sistemas de información	27	Externo	16,0	$ 1.128.000	$ 30.456.000
Conocimiento especializado cloud computing	27	Externo	20,0	$ 2.300.000	$ 62.100.000
			Valor Total		**$ 92.556.000**

Figura 72. Estimación proyecto nivelación de capacidades técnicas. Fuente: elaboración propia.

5.7 Plan de migración

Los proyectos planteados se someten a un proceso de priorización con el fin de establecer la estrategia de implementación y migración del ejercicio de arquitectura; para tal efecto se utilizan como base algunos de los conceptos definidos en el método de priorización multicriterio AHP (Analitic Hierarchy Process), formulado por Thomas L. Saaty; este método simplifica la priorización de alternativas permitiendo llevar un problema multidimensional a un problema en escala unidimensional (Moreno Jiménez, 2002).

En primer lugar, se plantean las alternativas (proyectos) a priorizar y los criterios de priorización.

Iniciativas	
Código	**Descripción**
A1	Orden digital
A2	EMP virtual
A3	Asistente virtual AVIF
A4	Orquestador
A5	Nivelación de capacidades técnicas

criterios de priorización	
Código	**Descripción**
C1	Tiempo de ejecución
C2	Costo de ejecución
C3	Impacto sobre los objetivos planteados

Figura 73. Proyectos y criterios de priorización. Fuente: elaboración propia

En segundo lugar, se realiza una confrontación entre los criterios definidos aplicando juicio de expertos; el resultado es la ponderación de los criterios.

En los procesos de confrontación se utiliza la escala de ponderación de Saaty:

	C1	C2	C3
C1	1	1/5	1/7
C2	5	1	1/3
C3	7	3	1
∑	13	4,2	1,476

Porcentajes por columna			Promedio Fila	Valor ponderado	
0,0769	0,0476	0,0968	0,073776269	**7,4%**	C1
0,3846	0,2381	0,2258	0,282848738	**28,3%**	C2
0,5385	0,7143	0,6775	0,643418009	**64,3%**	C3

Figura 74. Ponderación de criterios. Fuente: elaboración propia

El siguiente paso es ponderar las alternativas planteadas con base en cada criterio definido.

C1	A1	A2	A3	A4	A5
A1	1	1/3	5	1/5	1/7
A2	3	1	5	1/5	1/7
A3	1/5	1/5	1	1/7	1/9
A4	5	5	7	1	1/5
A5	7	7	9	5	1
∑	16,2	13,53	27	6,54	1,597

Porcentajes por columna					Promedio Fila	Valor ponderado
0,0617	0,0246	0,18519	0,03057	0,08946	0,078315006	**7,8%**
0,1852	0,0739	0,18519	0,03057	0,08946	0,11285858	**11,3%**
0,0123	0,0148	0,03704	0,02183	0,06958	0,031115521	**3,1%**
0,3086	0,3695	0,25926	0,15284	0,12525	0,24308926	**24,3%**
0,4321	0,5172	0,33333	0,76419	0,62624	0,534621633	**53,5%**

C2	A1	A2	A3	A4	A5
A1	1	1/5	5	1/5	1/5
A2	5	1	7	3	1/3
A3	1/5	1/7	1	1/7	1/7
A4	5	1/3	7	1	1/3
A5	5	3	7	3	1
∑	16,2	4,676	27	7,34	2,01

Porcentajes por columna					Promedio Fila	Valor ponderado
0,0617	0,0428	0,18519	0,02724	0,09953	0,083289372	**8,3%**
0,3086	0,2138	0,25926	0,40856	0,16588	0,271237522	**27,1%**
0,0123	0,0305	0,03704	0,01946	0,07109	0,034095583	**3,4%**
0,3086	0,0713	0,25926	0,13619	0,16588	0,188249576	**18,8%**
0,3086	0,6415	0,25926	0,40856	0,49763	0,423127948	**42,3%**

C3	A1	A2	A3	A4	A5
A1	1	1	1/3	1/5	1
A2	1	1	1/3	1/5	1
A3	3	3	1	1/3	3
A4	5	5	3	1	5
A5	1	1	1/3	1/5	1
∑	11	11	5	1,93	11

Porcentajes por columna					Promedio Fila	Valor ponderado
0,0909	0,0909	0,06667	0,10345	0,09091	0,088568443	**8,9%**
0,0909	0,0909	0,06667	0,10345	0,09091	0,088568443	**8,9%**
0,2727	0,2727	0,2	0,17241	0,27273	0,238119122	**23,8%**
0,4545	0,4545	0,6	0,51724	0,45455	0,496175549	**49,6%**
0,0909	0,0909	0,06667	0,10345	0,09091	0,088568443	**8,9%**

Figura 75. Ponderación de alternativas. Fuente: elaboración propia

Por último, se obtiene la prioridad general como resultado de multiplicar la matriz conformada por los vectores de prioridad de alternativas, con el vector de prioridad de criterios (Vidal et al., 2012).

	C1	C2	C3
A1	0	0	0
A2	1/9	1/4	0
A3	0	0	1/4
A4	1/4	1/5	1/2
A5	1/2	3/7	0

C1	0,07
C2	0,28
C3	0,64

A1	9%
A2	14%
A3	17%
A4	39%
A5	22%

Figura 76. Cálculo de las prioridades generales. Fuente: elaboración propia

De acuerdo con el resultado obtenido, los proyectos se deben ejecutar en el siguiente orden:

1. Proyecto Orquestador
2. Nivelación de capacidades
3. Asistente virtual AVIF
4. Proyecto EMP Virtual
5. Proyecto Orden digital

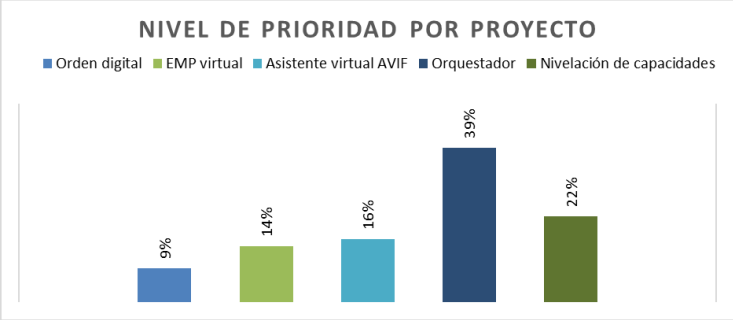


Figura 77. Orden ejecución de proyectos. Fuente: elaboración propia

Considerando que existen dependencias tecnológicas entre las iniciativas, algunos de los proyectos deben ser divididos en fases; el nuevo plan de ejecución se presenta a continuación. Se asume que el incremento en los costos de ejecución, producto de la fragmentación de los proyectos, puede ser cubierto con el porcentaje de holgura estimado para cada iniciativa.

Tabla 14

Orden de ejecución de proyectos por fases

Orden de ejecución	Nombre del proyecto	Descripción del alcance
1	Orquestador Fase I	Creación del módulo de analítica experta con las reglas de estimación y priorización. Ingreso de las solicitudes y las características técnicas de los elementos materiales probatorios a través de una interfaz de usuario provisional.
2	Nivelación de capacidades	Ejecución total
3	EMP Virtual	Ejecución total
4	Orquestador Fase II	Integración con la aplicación EMP virtual para la consulta de las características técnicas de los elementos materiales probatorios
5	Asistente virtual Fase I	Creación de la aplicación web con los formularios electrónicos para el cargue de información

Orden de ejecución	Nombre del proyecto	Descripción del alcance
6	Orden Digital	Ejecución total
7	Orquestador Fase III	Integración con la aplicación orden digital para la asignación automática de la orden de trabajo
8	Asistente virtual Fase II	Integración con la aplicación orden digital para permitir la consulta del informe y la evidencia forense asociados a una orden a policía judicial

Fuente: elaboración propia.

Los proyectos detallados se agrupan en cinco paquetes de trabajo usando como criterio de agrupación el grado de relación y dependencia que existe entre ellos.

Paquete de trabajo 1:

- Proyecto Orquestador fase I

Paquete de trabajo 2:

- Nivelación de capacidades de informática forense

Paquete de trabajo 3:

- Proyecto EMP Virtual
- Proyecto Orquestador fase II

Paquete de trabajo 4:

- Proyecto Asistente virtual Fase I

Paquete de trabajo 5:

- Proyecto Orden digital
- Proyecto Asistente virtual fase II
- Proyecto Orquestador fase III

El plan de implementación de estos paquetes de trabajo tiene como prerrequisito la existencia de los componentes que serán impactados, los cuales están incluidos en el proceso de renovación tecnológica propuesto en el plan estratégico de tecnologías de información 2017 – 2020 de la Fiscalía General de la Nación.

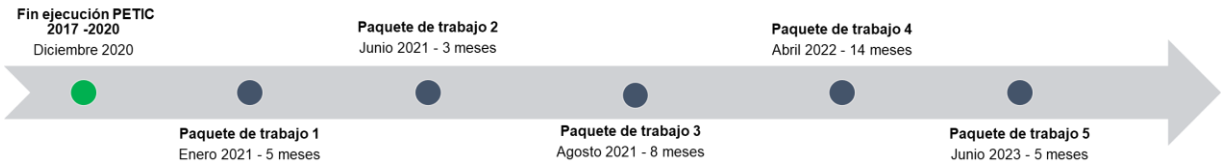


Figura 78. Plan de implementación. Fuente: elaboración propia.

5.8 Próximos pasos

La arquitectura empresarial es un proceso iterativo de mejora continua que, basado en una visión integral, "permite mantener actualizada la estructura de información organizacional alineando procesos, datos, aplicaciones e infraestructura tecnológica en cuatro dimensiones: negocios, datos/información, aplicaciones y tecnología" (Amazing, 2014) citado por (Guerrero Silva, Rojas Contreras, Sánchez Delgado, & Villamizar Estrada, 2017, p.89).

El presente trabajo se ocupa de las oportunidades de mejora que tienen una mayor relevancia para el logro de los objetivos planteados por los autores, sin embargo, durante el proceso investigativo se han identificado otros aspectos del proceso que deben ser considerados para futuras iteraciones del ciclo de arquitectura:

- A partir de la información recopilada en los sistemas de información propuestos en este trabajo de investigación; establecer indicadores claves de rendimiento, en adelante KPIs, que permitan valorar el desempeño del Grupo de Informática Forense, en las diferentes las etapas del proceso.
- Establecer una estrategia de difusión para informar a investigadores y autoridades solicitantes sobre los tipos de actividades que son competencia del grupo de informática forense. El objetivo es socializar las capacidades técnicas que la Fiscalía General de la Nación tiene a su disposición, además de reducir el número de solicitudes relacionadas con actividades que no requieren el conocimiento técnico especializado que tienen los peritos del Grupo.
- Evaluar el rendimiento de las herramientas de hardware y software que se emplean en el grupo actualmente y con base en indicadores de medición y lecciones aprendidas determinar cuáles son las ventajas de cada una y especificar de forma jerárquica con qué herramientas se obtienen resultados más rápidos o mejores.
- Reforzar el equipo de peritos forenses con personas jóvenes que estén familiarizadas con el uso de redes sociales y dispositivos electrónicos de última tecnología.
- Evaluar el uso de herramientas cloud (Infraestructura como servicio IAAS), para ejecutar programas de software especializado que demandan altos recursos de

procesamiento; dichos programas son utilizados en actividades de extracción y recuperación de información, obtención de imágenes forenses, entre otras.

- Llevar a cabo un análisis de herramientas de hardware y software forense disponibles en el mercado, establecer cuales representan un mejor desempeño costo/beneficio y con base en la demanda de solicitudes, actualizar el stock de herramientas especializadas disponibles en el Grupo de Informática Forense.
- Implementar una solución de inteligencia artificial que identifique las relaciones existentes entre solicitudes independientes de informática forense. El objetivo es incrementar la relevancia de la evidencia digital obtenida, aprovechando el conocimiento adquirido al atender otras solicitudes relacionadas con el mismo caso o con casos similares.

6 Conclusiones

La ausencia de un único procedimiento oficial para la emisión de solicitudes de informática forense, en el nivel central de la Fiscalía General de la Nación, dificulta la generación de estadísticas y la creación de KPIs que ayuden a visibilizar el desempeño del Grupo de Informática Forense y su contribución al logro de los objetivos estratégicos de la Entidad.

Establecer un mecanismo de comunicación entre las autoridades judiciales que emiten las solicitudes de informática forense y los técnicos que ejecutan las actividades periciales, permite focalizar el esfuerzo del personal especializado. Este entendimiento previo, propicia la realización de búsquedas dirigidas que requieran menos tiempo de atención y potencien la entrega de valor con la evidencia digital obtenida.

La asignación del trabajo de forma manual es un proceso que no aporta la eficiencia requerida por el grupo, automatizar este proceso permite una mejor distribución del trabajo, considerando todas las variables posibles respecto a la disponibilidad del recurso humano y las capacidades técnicas con las que cuenta el grupo.

El desarrollo de un ejercicio de arquitectura empresarial como práctica estratégica resulta ser muy valioso porque más allá de dar solución inmediata a una necesidad o problema específico, conlleva a la identificación de todos los aspectos de la organización que intervienen en la problemática, lo cual conduce a que el planteamiento de la solución considere todos los ámbitos relacionados con la necesidad.

Diseñar un portafolio de servicios que defina de forma específica cuales son las solicitudes que atiende el grupo y bajo qué condiciones se presta el servicio, se requiere de forma prioritaria para dar inicio a un proceso que estandarice la forma en que se reciben las solicitudes, defina los tiempos promedio para la atención de cada requerimiento y determine cuáles son los resultados que pueden ser obtenidos al finalizar los estudios forenses. Tan importante como el diseño del portafolio es su socialización con todos los usuarios.

Los sistemas de información que en la actualidad intervienen en el proceso para la atención de solicitudes, no proveen los recursos necesarios para el seguimiento, distribución y reporte del trabajo que se desarrolla en el Grupo, por tanto resulta importante trabajar en las mejoras propuestas con el presente ejercicio de arquitectura empresarial, las cuales buscan optimizar la atención de las solicitudes, eliminar reprocesos y lograr que las inversiones en sistemas de información se vean reflejadas en el apoyo real a las necesidades del grupo y se alineen con el PETIC 2017-2020 de la FGN.

La falta de un proceso de gestión de conocimiento y lecciones aprendidas, está generando pérdida de oportunidad en la resolución de problemas de forma rápida y efectiva.

Toda la información digital que llega a conocimiento de la Fiscalía a través de los procesos técnicos que adelanta el grupo de Informática Forense, tiene un valor estratégico que no ha sido completamente explotado, por tanto, resulta conveniente proponer la implementación de tecnologías de última generación que permitan a la Entidad generar conocimiento a través del análisis y correlación de casos sobre grandes volúmenes de información digital.

La entrega de resultados de los exámenes técnicos que adelanta el Grupo de Informática Forense, en la actualidad demanda gran cantidad de recursos representados en papel y medios de almacenamiento digital, dicha situación va en contravía de la política cero papel dispuesta por la administración pública. Una implementación eficiente de sistemas de información como los propuestos en el presente ejercicio de arquitectura empresarial lleva a la sustitución de dichos recursos, disminuyendo la afectación al medio ambiente.

Considerando que, el avance de la tecnología está generando que cada vez sea mayor el volumen de información digital de interés para las investigaciones y que las herramientas empleadas para los estudios forenses demanden cada vez mayores niveles de procesamiento y almacenamiento, la Entidad debe trabajar en la evaluación de tecnologías en la nube que provean el rendimiento de máquina requerido por las herramientas forenses y el almacenamiento digital que requiere la información obtenida, garantizando la confidencialidad que exige el manejo de este tipo de información en la Entidad.

Con el fin de promover el aprovechamiento y uso efectivo los sistemas de información, se debe trabajar en la usabilidad y la generación de confianza que garanticen una mejor adopción de las herramientas tecnológicas.

Los sistemas de información propuestos con el presente ejercicio de arquitectura empresarial deben ser considerados como críticos, teniendo en cuenta la información que estos gestionarán, por tanto, deben resguardarse bajo mecanismos de seguridad robustos que garanticen la integridad, confidencialidad y disponibilidad de la información.

Se debe trabajar en una estrategia de uso y apropiación que muestre los beneficios esperados con las nuevas implementaciones y se trabaje en la generación de una cultura en la que se adopten y aprovechen los nuevos recursos y la nueva estructura del proceso.

Referencias

Arango Serna, M. D., Branch Bedoya, J. W., & Londoño Salazar, J. E. (2014). Arquitectura empresarial como instrumento para gestionar la complejidad operativa en las organizaciones. *Revista DYNA, 81* doi:10.15446/dyna.v81n185.41928

Arango Serna, M. D., Londoño Salazar, J. E., & Zapata Cortes, J. A. (2010). Arquitectura empresarial – una visión general. *Revista Ingenierías Universidad De Medellín, 9*(16), 101-111. Recuperado de http://www.scielo.org.co/pdf/rium/v9n16/v9n16a09.pdf

Arias Valencia, M. M. (1999). La triangulación metodológica: Sus principios, alcances y limitaciones, 13. https://doi.org/10.1001/archneurpsyc.1953.02320250135014

Avella Franco, P. O. (2007). Estructura del proceso penal acusatorio. Recuperado de https://www.fiscalia.gov.co/colombia/wp-content/uploads/2012/01/EstructuradelProcesoPenalAcusatorio.pdf

Bondel, G. (2016). Zachman framework. Recuperado de https://eam-initiative.org/pages/kmjcfa5nejo4/Zachman-Framework

Buckl, S., Schweda, C. M., & Matthes, F. (2010). *A design theory nexus for situational enterprise architecture management – approach and application example.* Recuperado de https://wwwmatthes.in.tum.de/pages/15w49evisyoy6/sebis%20Public%20Website/_/Bu10o%20-%20A%20Design%20Theory%20Nexus%20for%20Situational%20Enterprise%20Architecture...

Bustamante, J. C. (s.f.a). *Curso: Arquitectura Empresarial basado en TOGAF Fase B*. Recuperado de http://www.ucipfg.com/Repositorio/MATI/MATI-04/BLOQUE-ACADEMICO/Unidad-2/lecturas/Resumen-2-Fase-B.pdf

Bustamante, J. C. (s.f.b). *Curso: Arquitectura Empresarial basado en TOGAF Fase C*. Recuperado de http://www.ucipfg.com/Repositorio/MATI/MATI-04/BLOQUE-ACADEMICO/Unidad-2/lecturas/Resumen-3-Fase-C.pdf

Canabal, R., Cabarcas, A., & Martelo, R. J. (2017). Aplicación de un esquema de arquitectura empresarial (TOGAF) para una pequeña empresa (PYME) utilizando aplicaciones

colaborativas de google. *Revista Información Tecnológica, 28*doi:10.4067/S0718-07642017000400011

Carrión Ortega, M. A., & Gómez Crandall, P. del C. (2003). *Propuesta de programa de inducción para los nuevos empleados del área de operación en la empresa Tecnollantas SA de CV*. Universidad de las Américas Puebla. Recuperado de http://catarina.udlap.mx/u_dl_a/tales/documentos/lad/carrion_o_am/capitulo4.pdf

Constitución política de colombia; (1991). Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991_pr008.html#250

Código de procedimiento penal; (2004). Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/ley_0906_2004.html

Decreto ley 898; (2017). Recuperado de http://es.presidencia.gov.co/normativa/normativa/DECRETO%20898%20DEL%2029%20DE%20MAYO%20DE%202017.pdf

Departamento Nacional de Planeación. (2019). *Bases del plan nacional de desarrollo 2018-2022, pacto por colombia pacto por la equidad.* (). Recuperado de https://colaboracion.dnp.gov.co/CDT/Prensa/PND-2018-2022.pdf

Desfray, P, & Raymond, G. (2014). *Togaf®. Modeling Enterprise Architecture with TOGAF*. https://doi.org/10.1016/B978-0-12-419984-2.00001-X

Fernandez Suarez, P., Jimenez Rubio, L., Villar Ledo, L., & Infante Abreu, M. B. (2017). Comparación de marcos de trabajo de arquitectura empresarial.*Revista Técnica Administrativa, 16*(4) Recuperado de http://www.cyta.com.ar/ta/article.php?id=160402

Fiscalía General de la Nación. (2017a). *Plan estratégico de tecnologías de la información y las comunicaciones [PETIC] 2017-2020.* Manuscrito no publicado.

Fiscalía General de la Nación. (2017b). *Direccionamiento estratégico FGN 2016-2020*. Recuperado de https://www.fiscalia.gov.co/colombia/wp-content/uploads/Direccionamiento-Estrat%C3%A9gico-2016-2020Vd.pdf

Fiscalía General de la Nación. Resolución 0032 de 2017, Pub. L. No. 0032, 181 (2017c). Recuperado de https://www.fiscalia.gov.co/colombia/wp-content/uploads/Manual-Específico-de-Funciones-y-Requisitos-de-la-FGN-Versión-3.pdf

Fiscalía General de la Nación. (2017d). Mapa de procesos fiscalía general de la nación. Recuperado de http://web_app/Documentacion/Procesos/Mapa%20de%20procesos%202017.jpg

Fiscalía General de la Nación. (2018a). *Manual para la identificación, formulación e inscripción de proyectos en el banco de proyectos.* Manuscrito no publicado.

Función Pública. (2018b). *Guía para la administración del riesgo y el diseño de controles en entidades pública* Recuperado de http://www.funcionpublica.gov.co/documents/418548/34150781/Gu%C3%ADa+para+la+administraci%C3%B3n+del+riesgo+y+el+dise%C3%B1o+de+controles+en+entidades+p%C3%BAblicas+-+Riesgos+de+gesti%C3%B3n%2C+corrupci%C3%B3n+y+seguridad+digital+-+Versi%C3%B3n+4+-+Octubre+de+2018.pdf/68d324dd-55c5-11e0-9f37-2e5516b48a87?t=1542226781163&download=true

Fiscalia General de la Nación. (2018c). Programa de gestión documental – PGD 2018-2020. Recuperado de https://www.fiscalia.gov.co/colombia/wp-content/uploads/PGD-ACTUALIZADO-2018-2020-Versi%C3%B3n-Final-8-VI-2018.pdf

Fiscalía General de la Nación. (2019a). *Manual único de policía judicial versión 2* Recuperado de https://www.fiscalia.gov.co/colombia/wp-content/uploads/Manual-de-Policia-Judicial-Actualizado.pdf

Fiscalía General de la Nación. (2019b). Estructura orgánica de la fiscalía general de la nación. Recuperado de https://www.fiscalia.gov.co/colombia/la-entidad/organigrama/

Fiscalía General de la Nación. (2019c). *Mapa de riesgos.* Manuscrito no publicado

Guerrero Silva, W. G., Rojas Contreras, W. M., Sánchez Delgado, M. del P., & Villamizar Estrada, A. (2017). Arquitectura Empresarial – Dominios Y Beneficios. *FACE: Revista de La Facultad de Ciencias Económicas y Empresariales*, *16*(1), 87. https://doi.org/10.24054/01204211.v1.n1.2016.2082

Hurtado, T., & Bruno, G. (2005). *El Proceso de análisis jerárquico (AHP) como herramienta para la toma de decisiones en la selección de proveedores : aplicación en la selección del proveedor para la Empresa Gráfica Comercial MyE S.R.L.* Recuperado de http://sisbib.unmsm.edu.pe/bibvirtualdata/Tesis/Basic/toskano_hg/cap3.PDF

Informática Forense Colombia. (2017). La Evidencia Digital. Recuperado de https://www.informaticaforense.com.co/la-evidencia-digital/

Kommadi, B. (2015). Federal enterprise architecture framework. Retrieved from https://iasaglobal.org/itabok3_0/engagement-model-overview-3-0/federal-enterprise-architecture-framework/

Lillis, D., Becker, B. A., Osullivan, T., & Scanlon, M. (2016). Current challenges and future research areas for digital forensic investigation. Paper presented at the *Annual ADFSL Conference on Digital Forensics, Security and Law,* Recuperado de https://commons.erau.edu/cgi/viewcontent.cgi?article=1346&context=adfsl

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). *Guía general de un proceso de arquitectura empresarial.* (). Recuperado de https://www.mintic.gov.co/arquitecturati/630/articles-9435_Guia_Proceso.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2018). *Manual de gobierno digital* Recuperado de http://estrategia.gobiernoenlinea.gov.co/623/articles-81473_recurso_1.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones, [MINTIC]. (2013). Arquitectura empresarial el camino hacia un gobierno integrado.*Revista CIO GOV,* Recuperado de https://www.mintic.gov.co/gestionti/615/articles-5322_Revista_pdf.pdf

Ministerio de Tecnologías de Información y las Comunicaciones. (2018b). *Boletín Trimestral de las TIC Cifras Primer Trimestre de 2018*. Recuperado de https://colombiatic.mintic.gov.co/679/articles-75854_archivo_pdf.pdf

Moreno Jiménez, J. M. (2002). el proceso analítico jerárquico (AHP). fundamentos , metodología y aplicaciones, 33. Recuperado de users.dcc.uchile.cl/~nbaloian/DSS-DCC/ExplicacionMetodoAHP(verpaginas11-16).pdf

National Institute of Standards and Technology, [NIST]. (2006). *Guide to integrating forensic techniques into incident response.* Recuperado de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

Pérez Vélez, J. D. (2012). *Método para la Selección y Priorización de Portafolios de I+D+i en el Contexto Institucional de un Centro de Desarrollo Tecnológico en Colombia*. Medellín Colombia. Recuperado de http://bdigital.unal.edu.co/9157/1/71229656.2012.pdf

Raynham, M. (2009). MEGA introduces DoDAF architecture suite. Recuperado de https://www.businesswire.com/news/home/20090223005705/en/MEGA-Introduces-DoDAF-Architecture-Suite

Reguant Alvarez, M., & Martínez Olmo, F. (2014). *operacionalización de conceptos/ variables*. Barcelona España. Recuperado de http://diposit.ub.edu/dspace/bitstream/2445/57883/1/Indicadores-Repositorio.pdf

Salas Villegas, V. S. (2011). *Modelo de priorización de proyectos de inversión pública con enfoque multicriterio: caso seMapa*. Cochabamba, Bolivia. Recuperado de http://www.redalyc.org/pdf/4259/425941257004.pdf

Scientific Working Group on Digital Evidence, [SWGDE]. (2016). Digital and multimedia evidence glossary. Recuperado de https://www.swgde.org/documents/Current%20Documents/SWGDE%20Digital%20and%20Multimedia%20Evidence%20Glossary

Scholarium SAS. (2017). ORFEO - Sistema de Gestión Documental | SCHOLARIUM SAS - Servicios Integrales de optimización, gestión y sistematización de procesos de negocio. Recuperado de http://scholarium.info/orfeo-sistema-de-gestion-documental/

Session Roger. (2008). *Simple architectures for complex enterprises* (1st ed.). Estados Unidos: Microsoft Press.

Suárez Fernández, P., Jiménez Rubido, Lisbeth de las Mercedes, Villar Ledo, L., & Infante Abreu, M. B. (2017). Comparación de marcos de trabajo de arquitectura empresarial.*16*(4) Recuperado de http://www.cyta.com.ar/ta/article.php?id=160402

Tamm, T., Seddon, P. B., Shanks, G., & Reynolds, P. (2011). How does enterprise architecture add value to organisations. *Communications of the Association for Information System, 28*(10) Recuperado de https://aisel.aisnet.org/cgi/viewcontent.cgi?article=3581&context=cais

Taoufikallah, A. (1990). El método AHP, 46–49. Recuperado de http://bibing.us.es/proyectos/abreproy/70496/fichero/Capitulo+4+El+método+AHP.pdf

The Open Group. (2013). *TOGAF version 9.1 guía de bolsillo* Recuperado de https://www.vanharen.net/Samplefiles/9789087537104SMPL.pdf

The Open Group. (2016). The open group service integration maturity model (OSIMM) version 2 Recuperado de http://www.opengroup.org/soa/source-book/osimmv2/p2.htm

The Open Group. (2018). TOGAF® standard, version 9.2. Recuperado de http://pubs.opengroup.org/architecture/togaf92-doc/arch/

The Open Group. (2017). ArchiMate® 3.0.1 Specification. Recuperado de http://pubs.opengroup.org/architecture/archimate3-doc/chap01.html#_Toc489945947

United Nations Office on Drugs and Crime, [UNODC]. (2019). Informe de la reunión del grupo de expertos encargado de realizar un estudio exhaustivo sobre el delito cibernético celebrada en viena del 27 al 29 de marzo de 2019. Paper presented at the Recuperado de https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Report/UNODC_CCPCJ_EG.4_2019_2_S.pdf

Uribe Ramirez, N., González Rengifo, A. R., Osorio Gómez, J. C., & Manotas Duque, D. F. (2010). *diseño de una metodología multicriterio para la priorización de proyectos de inversión del banco de proyectos de la universidad del valle*. Sao Carlos. Recuperado de http://www.abepro.org.br/biblioteca/enegep2010_TI_ST_115_756_16846.pdf

Vidal H, C. J., Bravo B, J. J., Cajiao G, E., Meza H, P. P., Arango S, S., Franco L, D., & Calserón S, J. H. (2012). *Guía metodológica para la priorización de proyectos: Un enfoque aplicado a la infraestructura, logística y la conectividad*. Cali, Colombia. Recuperado por vitela.javerianacali.edu.co/bitstream/handle/11522/3451/Guia Metodologica_Infraestructura.pdf?sequence=1&isAllowed=y

Watts, S. (2018, Feb 20,). Enterprise architecture frameworks (EAF): The complete beginner’s guide. Recuperado de https://www.bmc.com/blogs/enterprise-architecture-frameworks/

Anexos

Anexo 1 Formularios Entrevistas

Formulario guía de entrevista Coordinador

¿Cuál es su rol dentro del proceso, qué actividades realiza?

¿Qué tipo de solicitudes atiende el grupo de informática forense?

¿Cuáles son las solicitudes más comunes?

Desde su punto de vista, ¿Cuál es el ciclo de vida de un requerimiento de informática forense?

¿Qué otros roles identifican dentro del proceso investigativo?

¿Qué parámetros debe cumplir un requerimiento para ser atendido?
Ayuda: (¿escrito, verbal, otro?)

Quien origina las solicitudes que atiende el grupo (¿qué personas o autoridades puede hacer requerimientos?)

¿Cómo se hace la asignación de los requerimientos?
Ayuda: (quien asigna y de qué forma)

Que parámetros se tienen en cuenta para la asignación del requerimiento a alguno de los funcionarios del grupo de informática forense.

¿Hay un tiempo específico para la atención de requerimiento?, ¿cómo se establece?

¿Considera que la forma en que se asigna el tiempo para la atención del requerimiento es la adecuada? En caso negativo: ¿Cómo lo mejoraría?

¿Qué tipo de requerimientos generan dificultad para elegir quien debe atenderlo?

¿Cuáles son las dificultades más comunes al realizar su trabajo?

¿Existe un procedimiento estándar para la atención de cada tipo de requerimiento?
En caso afirmativo: ¿Qué tan estricto es el cumplimiento de ese procedimiento'?

¿Cuáles son las solicitudes que representan mayor desgaste o que generan complicaciones?

¿Qué tipo de seguimiento o control realiza a los requerimientos una vez han sido asignados?

¿Cómo se mide el aporte de cada requerimiento atendido al objetivo misional?

¿Para el desarrollo de su labor debe hacer uso de algún S.I.?
¿Cuál es?
Describa de forma resumida las actividades que ejecuta sobre el S.I

¿Considera que el SI cubre completamente las necesidades del rol que usted ejecuta?

¿Qué mejoraría del SI para que apoye de forma más eficiente su labor?

¿Qué aspectos del proceso cree usted que se pueden mejorar?

Si pudiese cambiar algo del proceso actual. ¿Qué cambiaría? Y ¿Por qué?

¿Qué temas considera usted, hacen falta conocer para que en el grupo se realice una mejor labor?

¿Qué tan frecuentemente excede el horario laboral?

Formulario guía de entrevista Asistente

¿Cuál es su rol dentro del proceso, qué actividades realiza?

¿Qué conocimiento debe tener para ejercer el rol? – Listado de temas.

¿Qué tipo de solicitudes atiende el grupo de informática forense?

¿Qué parámetros debe cumplir un requerimiento para ser atendido?
Ayuda: (¿escrito, verbal, otro?)

Quien origina las solicitudes que atiende el grupo (¿qué personas o autoridades puede hacer requerimientos?)

¿Cuáles son las solicitudes más comunes que se reciben en el grupo?

Desde su punto de vista, ¿Cuál es el ciclo de vida de un requerimiento de informática forense?

¿Qué roles identifica en el proceso?

¿Cómo se hace la asignación de los requerimientos?
Ayuda: (quien asigna y de qué forma)

¿Hay un tiempo específico para la atención de requerimiento?, ¿cómo se establece?

¿Para el desarrollo de su labor debe hacer uso de algún S.I.?
¿Cuál es?
Describa de forma resumida las actividades que ejecuta sobre el S.I

¿Considera que el SI cubre completamente las necesidades del rol que usted ejecuta?

¿Qué mejoraría del SI para que apoye de forma más eficiente su labor?

¿Qué aspectos del proceso cree usted que se pueden mejorar?

Si pudiese cambiar algo del proceso actual. ¿Qué cambiaría? Y ¿Por qué?

De las capacitaciones que usted tiene ¿Cuáles han sido útiles para ejecutar su labor?

¿Alguna vez ha tenido que auto - capacitarse para atender algún requerimiento?
En caso Afirmativo: ¿Recuerda el o los temas?

Que temas considera usted, hacen falta conocer para ejecutar su labor.

¿Cuáles son las dificultades más comunes al realizar su trabajo?

¿Qué tan frecuentemente excede el horario laboral?

Formulario guía de entrevista Investigador Informática Forense

¿Qué tipo de solicitudes atiende el grupo de informática forense?

Quien origina las solicitudes que atiende el grupo (¿qué personas o autoridades puede hacer requerimientos?)

¿Qué parámetros debe cumplir un requerimiento para ser atendido?
Ayuda: (¿escrito, verbal, otro?)

Desde su punto de vista, ¿Cuál es el ciclo de vida de un requerimiento de informática forense?

¿Cuál es su rol dentro del proceso, qué actividades realiza?

¿Qué otros roles identifican dentro del proceso?

¿Cuáles son las solicitudes más comunes que usted recibe?

¿Existe un procedimiento estándar para la atención de cada tipo de requerimiento?
En caso afirmativo: ¿Qué tan estricto es el cumplimiento de ese procedimiento'?

¿Hay un tiempo específico para la atención de requerimiento?, ¿cómo se establece?

¿Considera que la forma en que se asigna el tiempo para la atención del requerimiento es la adecuada? En caso negativo: ¿Cómo lo mejoraría?

¿Cómo se prioriza la atención de los requerimientos?

¿Para atender los requerimientos cuenta con diferentes herramientas con las que puede obtener resultados iguales o similares? En caso afirmativo ¿Cómo se define que herramienta debe utilizar?

¿Cuáles son las dificultades más comunes al realizar su trabajo?

¿Para el desarrollo de su labor debe hacer uso de algún S.I.?
¿Cuál es?
Describa de forma resumida las actividades que ejecuta sobre el S.I

¿Alguna vez ha tenido que auto - capacitarse para atender algún requerimiento?
En caso Afirmativo: ¿Recuerda el o los temas?

¿Qué tan frecuentemente excede el horario laboral?

Si pudiese cambiar algo del proceso actual. ¿Qué cambiaría? Y ¿Por qué?

Formulario guía de entrevista Fiscal

¿Qué tipo de solicitudes realiza al grupo de informática forense?

¿Cuál es su rol dentro del proceso investigativo, qué actividades realiza?

¿En qué etapa de la investigación es necesario un estudio de informática forense?

¿Cuáles son los parámetros que debe cumplir un requerimiento para que sea atendido por el Grupo de Informática Forense?

Ayuda: (¿escrito, verbal, otro?)

¿Debe hacer uso de algún S.I. para interactuar con los servicios que presta el grupo de Informática Forense? ¿Cuál es?
Describa de forma resumida las actividades que ejecuta sobre el S.I

¿Hay un tiempo específico para que el requerimiento sea atendido?, ¿cómo se establece ese tiempo?

¿Considera que la forma en que se asigna el tiempo para la atención del requerimiento es la adecuada? En caso negativo: ¿Cómo lo mejoraría?

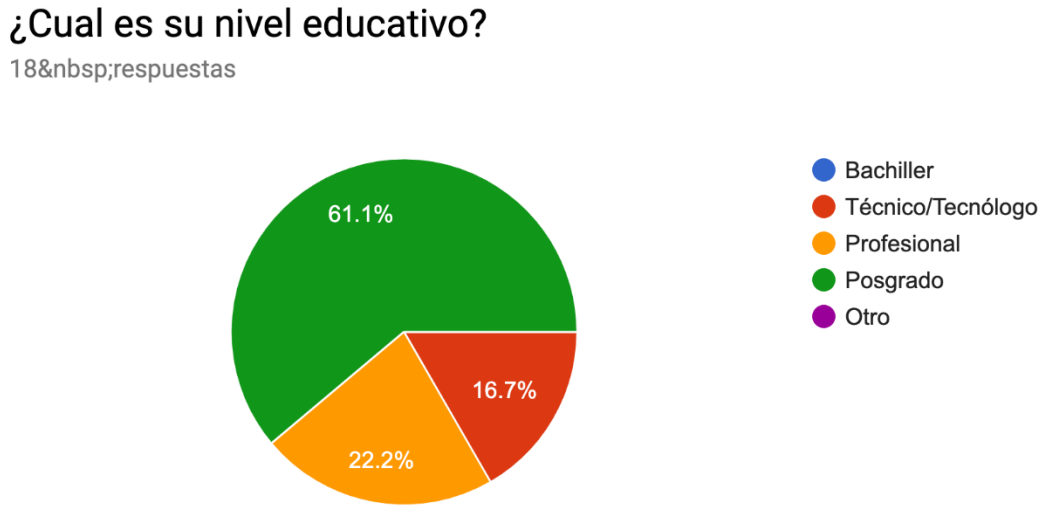
¿Qué aspectos del proceso de informática forense cree usted que se pueden mejorar?

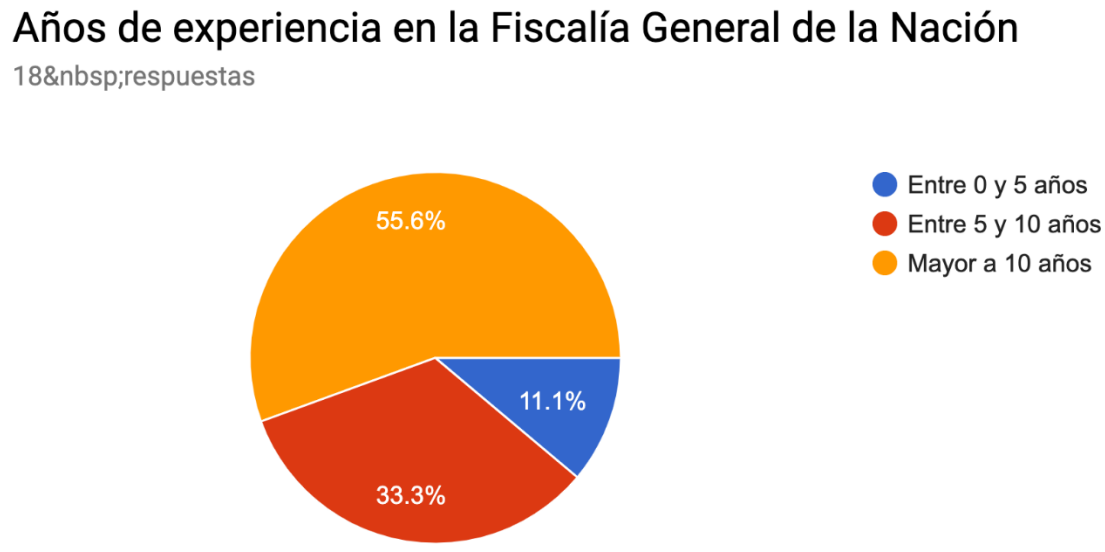
Considera útiles los productos generados por el Grupo de Informática Forense para las investigaciones? En caso afirmativo, Cuáles? ¿Por qué?

Si pudiese cambiar algo del proceso de informática forense. ¿Qué cambiaría? Y ¿Por qué?

Anexo 2 Tabulación datos encuestas

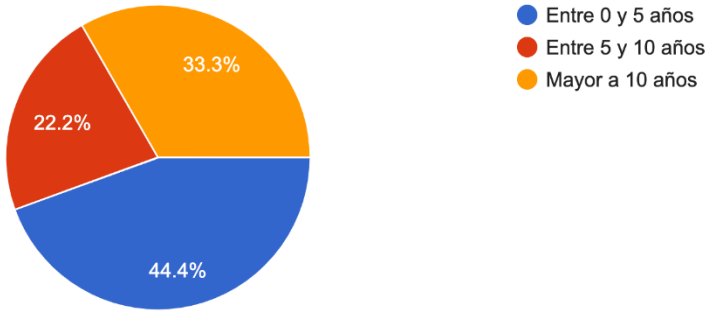
Encuesta Capacidades Grupo Informática Forense





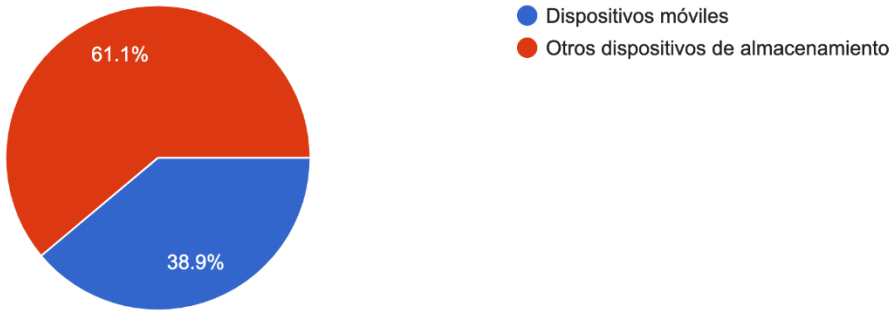
Años de experiencia en la labor de informática forense

18 respuestas

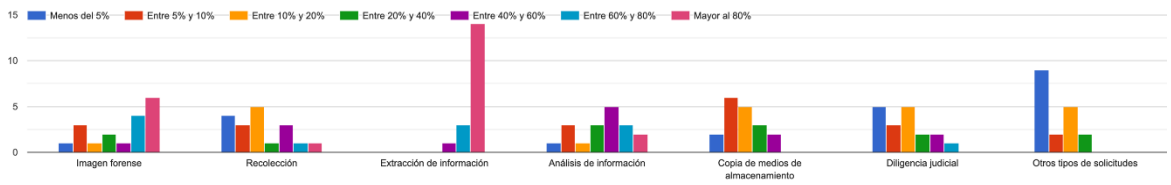


¿A qué área de trabajo pertenece dentro del grupo de Informática Forense?

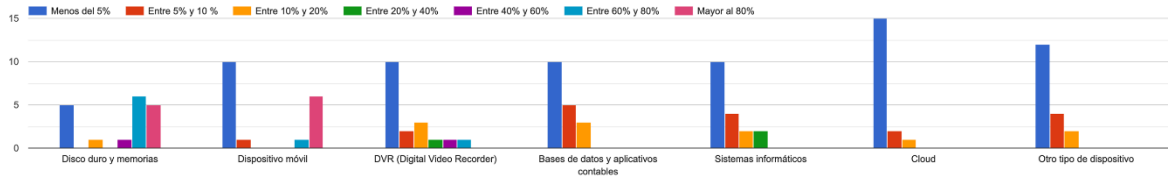
18 respuestas



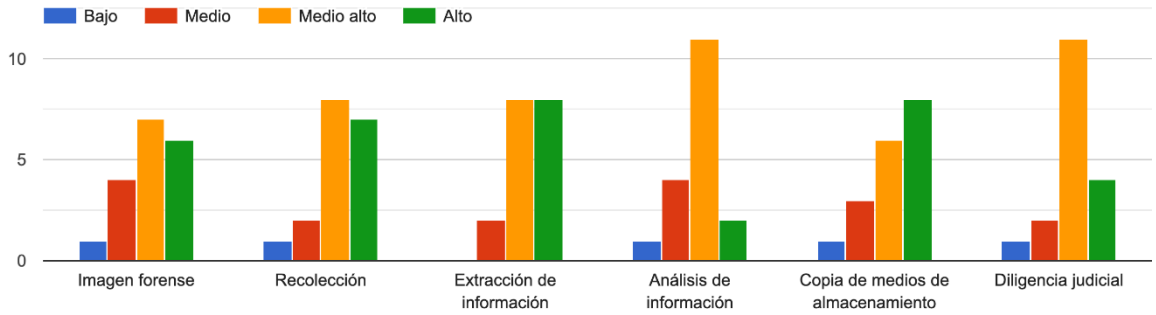
En promedio, del total de órdenes de trabajo que le han asignado, que porcentaje corresponde a las siguientes actividades



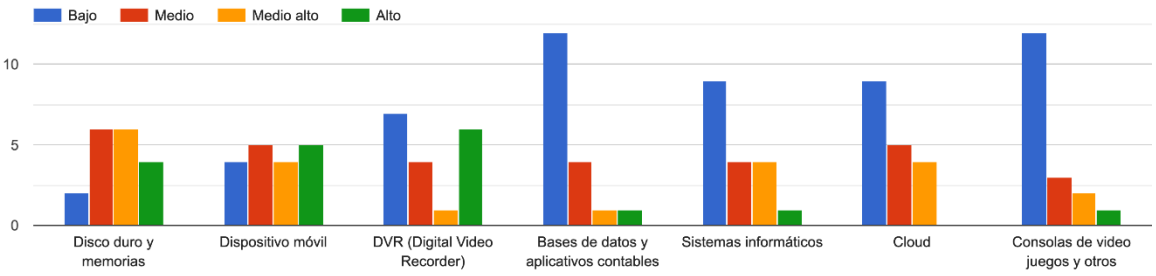
En promedio, del total de elementos que le han asignado para examen forense, que porcentaje corresponde a:



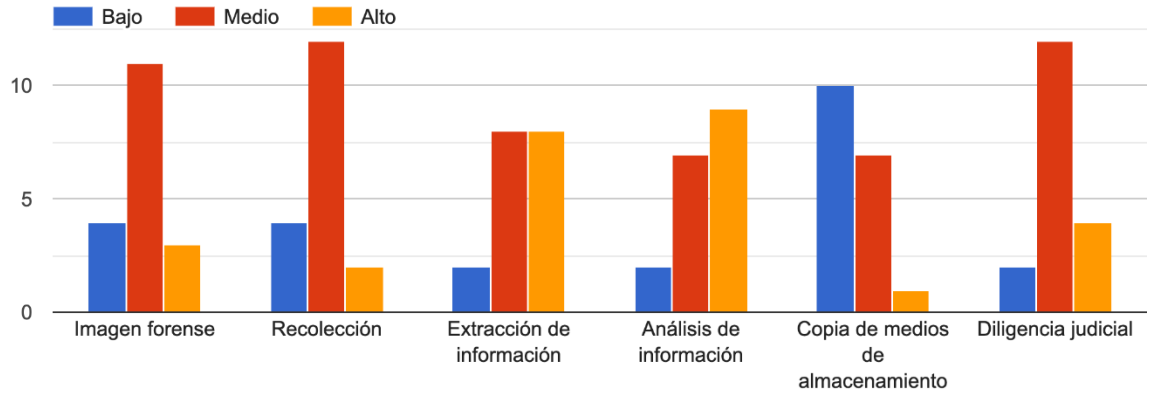
Seleccione su nivel de conocimiento para realizar cada actividad



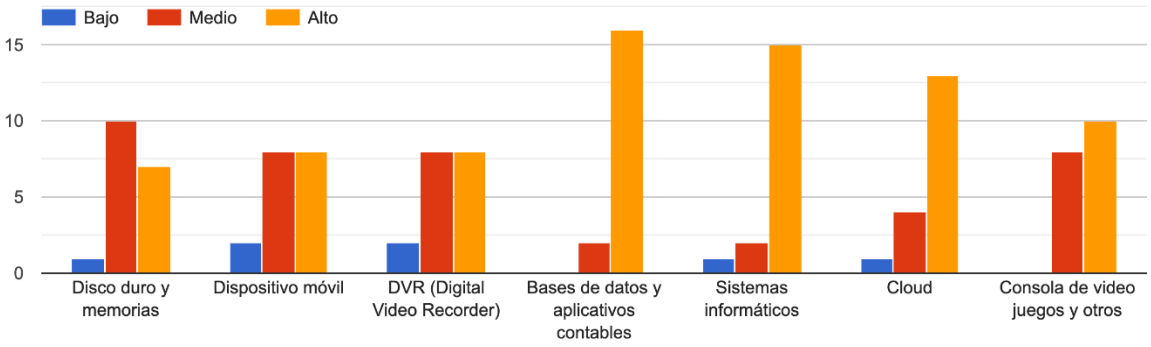
Seleccione su nivel de conocimiento para realizar examen forense de:



Para usted, que nivel de complejidad se puede presentar en el desarrollo de las siguientes actividades

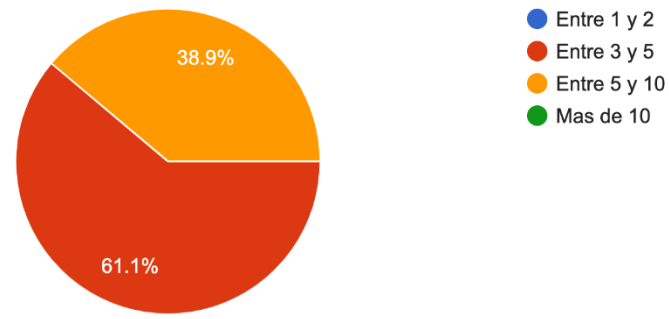


Para usted, que nivel de complejidad se puede presentar en el examen forense de

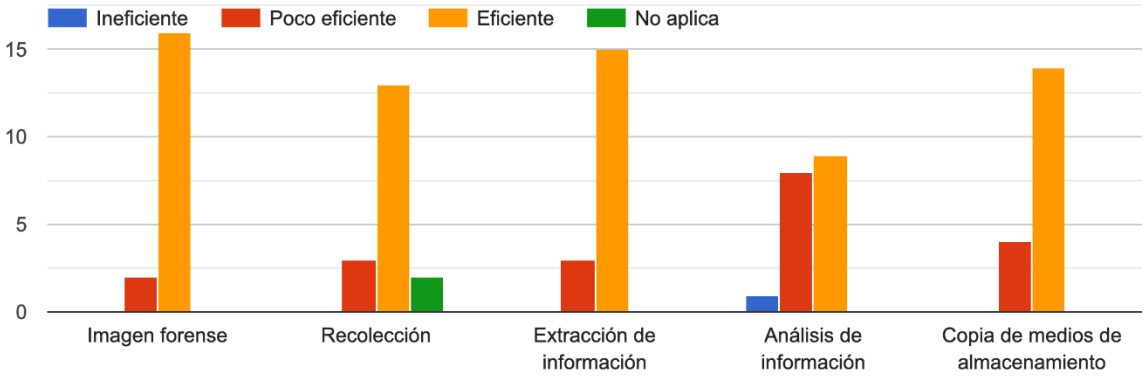


En promedio, cuantas ordenes de trabajo le son asignadas al mes

18 respuestas



Evalúe la forma en que las herramientas tecnológicas disponibles en el grupo, apoyan la atención de los siguientes requerimientos



Evalúe la forma en que las herramientas tecnológicas disponibles en el grupo apoyan los procesos técnicos para el examen forense de: