ANEXO_1-ANEXO TÉCNICO

Adquirir créditos y soporte enterprise en la infraestructura de nube pública AWS.

Tabla de Contenido

Antecedentes 3
1. Aplicaciones en operación en AWS 3
2. Servicios en operación y arquitectura técnica desplegada en AWS 3
2.1. Configuración técnica por aplicación – Cómputo y almacenamiento 9
2.2. Arquitectura Multinube 9
2.3. Métricas de consumo (último mes) 10
3. Definición del alcance y características técnicas de la necesidad. 11
3.1. Requisitos de negocio (Entidad). 11
3.2. Capacidades requeridas desde el punto de vista funcional. 15
3.2.1. Servicios de cómputo 15
3.2.2. Servicios de almacenamiento: 15
3.2.3. Servicios de soporte: AWS Enterprise Support 16
3.2.4. AWS Marketplace 17
4. Capacidades requeridas 24
5. Condiciones transversales 24
6. Acuerdos de Nivel de Servicio 24

Antecedentes

En 2023, se suscribió el **contrato 170 de 2023**, mediante la **Orden de Compra 122576**, con la empresa Hightech Software S.A.S., por un valor de $10.029.643.658,07, cuyo objeto fue la adquisición de créditos y soporte Enterprise para la infraestructura de nube pública AWS. Esta contratación fue realizada a través del Acuerdo Marco CCE-241-AMP-2021, de acuerdo con los lineamientos de Colombia Compra Eficiente.

1. Aplicaciones en operación en AWS

Actualmente, la entidad cuenta con infraestructura desplegada en AWS que soporta aplicaciones críticas de la Rama Judicial, tales como el Sistema de Gestión Procesal Laboral del Sistema Integrado de Gestión Judicial, la plataforma de gestión de servicio de la mesa de ayuda y de las seccionales - Ivanti, Soluciones de apoyo al análisis de sentencias y la plataforma de interoperabilidad; por esta razón se hace indispensable contar con los recursos necesarios para garantizar la continuidad de estos servicios que son de impacto crítico para la prestación de servicios de la Rama Judicial.

Objetivos principales (Entidad).

- Recargar Créditos en la nube AWS para mantener la continuidad de la infraestructura de nube aprovisionada, y soportar nuevas cargas de trabajo bajo una arquitectura de multinube.
- Habilitar los crecimientos necesarios para la implementación efectiva de la estrategia de transformación digital.
- Adquirir las capacidades de nube pública para los servicios actualmente desplegados en la nube AWS (SIUGJ, Plataforma de interoperabilidad, Seguridad y Monitoreo de la Plataforma, Pruebas de Carga, Análisis de Sentencias, Ivanti, IA, etc.) y capacidades por aprovisionar; los cuales se han beneficiado de las ventajas de la nube pública como alta disponibilidad, escalabilidad, eficiencia operativa, reducción de tiempos de provisión y fortalecimiento de la seguridad.

2. Servicios en operación y arquitectura técnica desplegada en AWS

A continuación, se describen los servicios y aplicaciones que actualmente operan en la nube pública AWS, destacando su funcionalidad y rol estratégico para la Rama Judicial.

Aplicación asociada	Descripción de la aplicación	Nivel de uso
SIUGJ- Sistema de gestión de procesos laboral	Sistema Integrado de Gestión Judicial de la Rama Judicial – SIUGJ, es conjunto de soluciones tecnológicas que integra servicios digitales de acceso, registro y tramitación electrónica de los procedimientos judiciales, la gestión documental electrónica del expediente judicial y los servicios transversales de apoyo a la gestión judicial, bajo parámetros de accesibilidad, seguridad de la información, basado en un marco de interoperabilidad que facilite la	Hoy el SIUGJ ambiente de Preproducción y Producción opera en infraestructura propia en AWS desde el 2024. En octubre de 2024 se tenían vinculados 210 despachos judiciales a SIUGJ. 621 despachos 4.167 usuarios 140.526 procesos en operación

Aplicación asociada	Descripción de la aplicación	Nivel de uso
	integración e intercambio de información y el aprovechamiento de los datos de la gestión judicial.	
Ivanti	Ivanti es una solución diseñada para optimizar y automatizar la gestión de la mesa de ayuda (Service Desk) de la Rama Judicial, brindando una plataforma centralizada para el soporte técnico y la gestión de servicios de TI. Su enfoque principal es mejorar la eficiencia operativa, reducir tiempos de respuesta y elevar la satisfacción del usuario.	Se utiliza para la mesa de servicio- JUDIT por parte de toda la Rama Judicial Se utiliza por la Seccional de Medellín, Bogotá, Manizales y Quibdó con un portafolio de 5 servicios con 79 categorías.
Matriz RBAC-Identidad Digital	Aplicación para la captura de información de los roles y permisos de cada usuario a los diferentes recursos tecnológicos de la entidad, esta información hace parte del proyecto de mejora de la gestión de identidad	Actualmente se encuentra en operación puesto que se adelanta la consultoría para Implementar controles y mecanismos de gestión de identidad prioritarios, para mejorar las condiciones de ciberseguridad de la Rama Judicial mediante el contrato 153 de 2024.
Plataforma de Interoperabilidad	Plataforma que facilita el intercambio de información tanto a nivel interno como externo.	Actualmente la plataforma actualizada está operativa con el 100% de los servicios migrados de IFX en producción. Actualmente, se encuentran desplegados 10 servicios en producción: 1. Consulta Nacional de abogados (Permite consultar información de SIRNA) 2. InformaciónArbolTutela (Permite consultar información de las tutelas interpuestas en un rango de fechas) 3. CPNU (Permite consultar información de los procesos registrados en CPNU, se planea para consultas masivas por parte de entidades del Estado con las que el CSJ tenga convenios interadministrativos suscritos para tal fin) 4. RUES (permite consultar información de personas

Aplicación asociada	Descripción de la aplicación	Nivel de uso
		jurídicas, empresas o entidades) 5. Consultar Cédulas (Permite verificar los datos de identidad de un ciudadano) 6. SIGEP (permite consultar la hoja de vida de los funcionarios públicos) 7. Autenticación mediante Cédula Digital (permite verificar los datos de identidad de un ciudadano a través de la aplicación de cédula digital de la Registraduría) 8. UARIV (Permite consultar la información de víctimas) 9. Superintendencia de Notariado y Registro (permite consultar la información de predios para la restitución de tierras) 10. Traslado a segunda instancia (permitirá a la Superintendencia de Salud, a través de JustiFácil de Minjusticia, hacer el traslado para segunda instancia de procesos judiciales).
Análisis de sentencias	Solución basada en inteligencia artificial para analizar y extraer información clave de sentencias judiciales en PDF (planos y enriquecidos) y documentos asociados. Esto permite automatizar procesos hasta la fase de liquidación mediante un motor de reglas y análisis avanzado.	Esta solución hace parte de los ejercicios de IA que se adelantan en el marco del Acuerdo 12243 de 2024. Se encuentra en pruebas para entrar en producción.
Inteligencia Artificial	Implementación progresiva de iniciativas piloto basadas en Inteligencia Artificial para apoyar la transformación digital de la justicia y dar cumplimiento a lo señalado en el ACUERDO PCSJA24-12243 del 16 de diciembre de 2024 “Por el cual se adoptan lineamientos para el uso y aprovechamiento respetuoso, responsable, seguro y ético de la inteligencia artificial en la Rama Judicial” “Artículo 12. Análisis para soluciones o proyectos institucionales. La Unidad de Transformación Digital e Informática,	Durante el periodo 2025-2026 se proyecta ejecutar entre 3 y 5 pilotos en distintos frentes estratégicos (relatoría, gestión administrativa y documental, apoyo a la gestión judicial). Cada piloto se implementará de forma modular, sobre cargas de trabajo específicas, evaluando progresivamente su desempeño y valor agregado. Esta fase experimental permitirá sentar las bases para la adopción institucional de soluciones basadas en IA en el mediano plazo.

Aplicación asociada	Descripción de la aplicación	Nivel de uso
	en coordinación con las unidades competentes, deberá priorizar las siguientes acciones tendientes a la implementación de proyectos, la habilitación y disposición de soluciones institucionales con IA: 1. Adelantar pruebas y estudios de viabilidad para implementar proyectos, disponer y habilitar soluciones o herramientas institucionales de IA, enfocados inicialmente en los siguientes tipos de uso, sin perjuicio de otros que sean identificados o solicitados: a. Gestión administrativa y documental: reparto, agenda para la programación de diligencias, digitalización y clasificación de expedientes, revisión de completitud de documentos, textualización de las grabaciones de las audiencias, sistemas de relatoría y motores de búsqueda de jurisprudencia y anonimización de datos. b. Apoyo a la función judicial: referenciación de jurisprudencia, seguimiento de líneas jurisprudenciales, análisis de datos estadísticos, identificación de temas repetitivos, asistencia en procesos de notificaciones, orientar el acceso a servicios y trámites e interacción con usuarios, sin que estos usos supongan una labor de creación de contenido, interpretación de hechos o textos, ni solución de casos. c. Corrección y síntesis de textos, con supervisión humana posterior para su aplicación. 2. Avanzar, en el análisis de idoneidad y pertinencia del desarrollo, habilitación o el uso de sistemas, servicios o herramientas de IA generativa	Asimismo, estos pilotos nos permitirán avanzar en la valoración de herramientas de IA sobre las cuales la Rama Judicial podría hacer uso verificando condiciones de seguridad, demanda de recursos, capacidades de infraestructura requeridas, entre otros, de forma que dependiendo de los resultados se puedan adoptar e incluir dentro de la operación de la entidad de manera segura y progresiva.

Aplicación asociada	Descripción de la aplicación	Nivel de uso
	especializados en jurisprudencia y normativa, para el apoyo en el ejercicio de la función pública de administración de justicia.	
Backups IFX	Backups histórico, son contractuales según lo definido en las condiciones definidas por Colombia Compra Eficiente y corresponden a la OC 124016 (contrato 004/2024) aplica para las aplicaciones alojadas durante la ejecución del citado contrato y que generaron backups según las políticas definidas por la entidad y acordadas con el operador IFX.	Desde la incidencia de seguridad de IFX se adelantó un proceso de migración de aplicaciones y servicios de IFX a las nubes públicas seleccionadas. Se mantuvo esta copia de seguridad con el fin de poder restaurarlo para propósitos de auditoria o consulta histórica. Los backups son de alrededor de 48 máquinas virtuales -MV- en las cuales se alberga principalmente la información de aplicaciones que en este momento ya no están en nube privada, tales como el portal de Restitución de Tierras, portal histórico, Portal Consejo de Estado entre otras, así misma copia de la MV únicamente de las aplicaciones y base de datos del Ecosistema de Grabaciones (no incluye la data de las grabaciones). Estos backups son de tipo full sintético de las MV (mensuales, con 6 puntos de retención) es decir que dentro de ellos esta las configuraciones y su data, en las MV que contenía BD que para estos casos todas eran SQL, se contenía en dicho archivo de respaldo, todas las copias de seguridad se realizaron usando la herramienta del operador Veeam Backup. La retención de estos backups contractuales definidos en el contrato 004/2024 suscrito con IFX solo es por seis meses. Cumplido este periodo daremos de baja esta información de la infraestructura de IFX que corresponde a 43.7 Tb.

Aplicación asociada	Descripción de la aplicación	Nivel de uso
Seguridad y monitoreo de la plataforma	Incorporación de soluciones de seguridad de AWS con el fin de asegurar la infraestructura tecnológica de seguridad de las soluciones allí alojadas: - Web Application Firewall (WAF) - Automated Security Response on AWS. - AWS Security Hub - AWS Inspector - AWS Macie - AWS GuardDuty - AWS Shield Advanced	Hacen parte de la infraestructura de seguridad implementada para toda la infraestructura.
Pruebas de concepto de Inteligencia artificial	Realización de pruebas de concepto de servicios y herramientas de inteligencia artificial que permitan aumentar la productividad de los despachos judiciales	Por demanda
Pruebas de carga	Apoyo en la realización de pruebas de carga sobre las aplicaciones previo a su salida a producción con el fin de minimizar los riesgos inherentes en el proceso. Soluciones: CarJUD, Portal Rama Judicial, Ventanilla Reparto, App Credencial Digital Abogados, Portal Publicaciones Procesales y Firma Electrónica.	Por demanda, con cargo a las horas de especialistas.
Pruebas de concepto de inteligencia artificial	Realización de pruebas de concepto: - Utilización de herramientas suplemento de herramientas de otros fabricantes como ReCaptcha de Google. - Cargue y descargue de grandes volúmenes de información de centro de datos On Premise desde y hacia la nube pública	Realización de pruebas para determinar desempeño, tiempos de carga y descarga, tamaños, herramientas y capacidades requeridas con el fin de apoyar la toma de decisiones.
Arquitecto Senior en Nube Hibrida	Disponibilidad de personal especializado para apoyar al equipo de administración de la plataforma para atender situaciones imprevistas que puedan darse durante la operación que requieran de acompañamiento especializado. El número de horas solicitado es mucho menor al utilizado en el contrato anterior debido a que la demanda de las mismas bajo dos razones fundamentalmente: Por otra parte, la administración de la plataforma fue asumida por el equipo	Horas experto

Aplicación asociada	Descripción de la aplicación	Nivel de uso
	de la Unidad de Transformación Digital – División de Servicios Tecnológicos.	

2.1. Configuración técnica por aplicación – Cómputo y almacenamiento

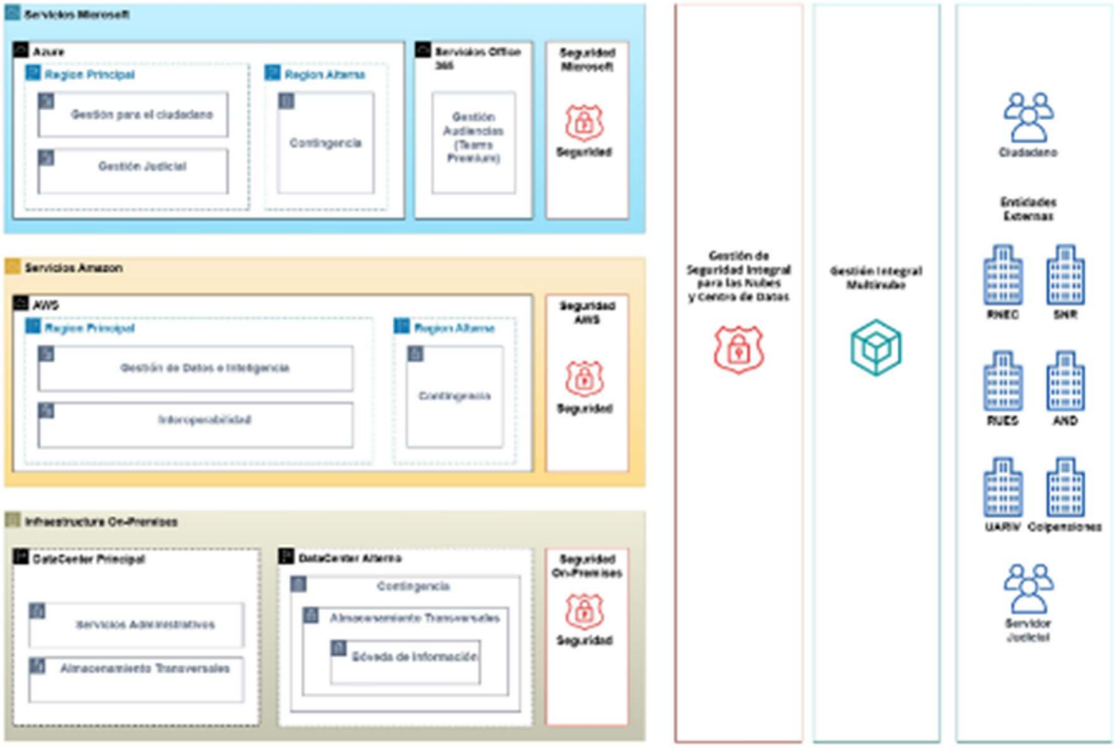
Resumen técnico de los recursos consumidos por aplicación crítica en términos de instancias, almacenamiento y servicios asociados:

Aplicación asociada	Servicios de cómputo	Servicios de almacenamiento	Servicios de Aplicaciones
SIUGJ- Laboral	AWS Fargate, Amazon ECS 37 vCPUS-125GiB	EBS: 633741,2 GiB S3: 564.019,2 GiB	Amazon RDS, Amazon EFS Amazon EFS Application Load Balancer
Ivanti	EC2 64 vCPUS, 360 GiB	S3 6900 GiB	EC2 S3 Application Load Balancer
Análisis de sentencias	EC2 4 vCPUS – 16 GiB	S3 1.154 GiB	EC2 S3 Application Load Balancer
Matriz RBAC-Identidad Digital	EC2 8 vCPUS -16 GiB	S3 500 GiB	EC2 S3
Plataforma de Interoperabilidad	EC2 106 vCPUS -344 GiB	S3 2.986 GiB	EC2 S3 Application Load Balancer AWS Database Migration Service
Seguridad y monitoreo de la plataforma	Habilitación de servicios y componentes de seguridad		EC2 S3 Application Load Balancer AWS Elastic Disaster Recovery
Pruebas de carga	EC2 8 vCPUS -16 GiB	S3 500 GiB	EC2 S3 Application Load Balancer
Pruebas de concepto	EC2 8 vCPUS -16 GiB	S3 500 GiB	EC2 S3 Application Load Balancer

2.2. Arquitectura Multinube

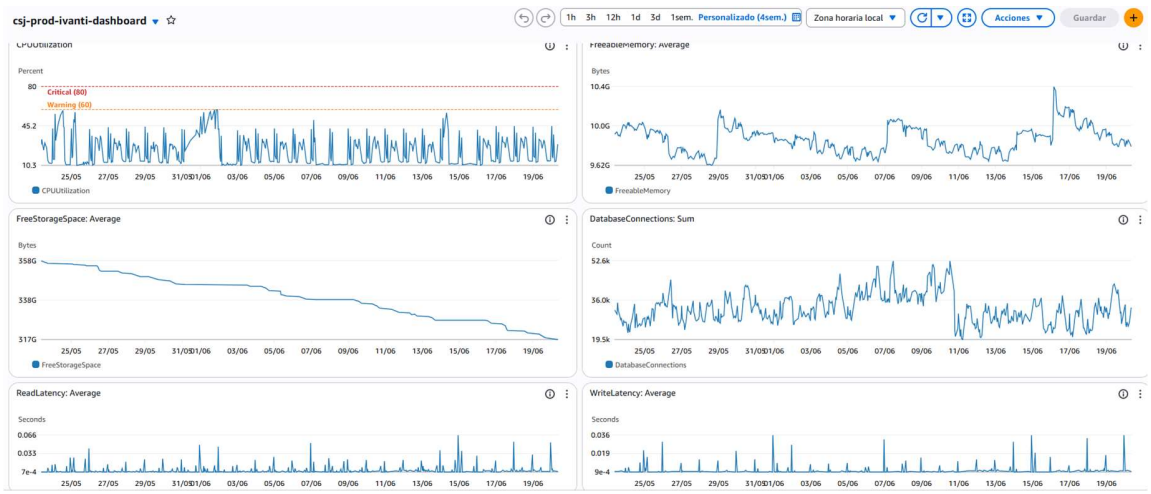
El proyecto multinube tiene en principio dos nubes públicas definidas en donde se podrán alojar servicios de la Rama Judicial (Azure y AWS).

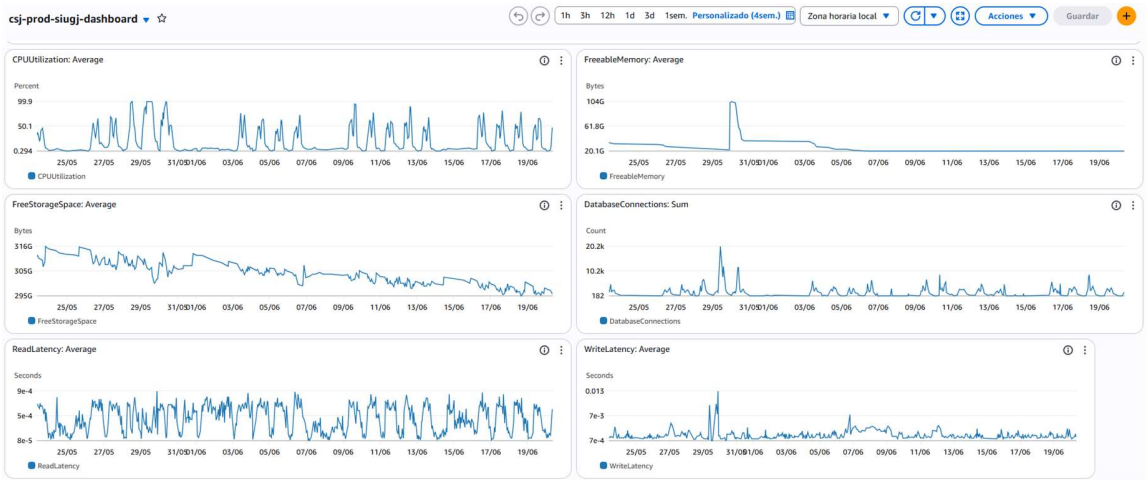
Se plantean las premisas de la estrategia de multinube híbrida para la Rama Judicial confirmando el modelo de multinube híbrida, compuesto por dos nubes públicas, y el fortalecimiento de la infraestructura on premise para contar con un data center principal y uno alterno, con la correspondiente seguridad perimetral. Adicionalmente, se presenta la evaluación realizada para establecer las dos nubes públicas recomendadas.



2.3. Métricas de consumo (último mes)

El proyecto





3. Definición del alcance y características técnicas de la necesidad.

3.1. Requisitos de negocio (Entidad).

i. Alineación estratégica y descripción de la necesidad.

AWS es un conjunto de servicios en la nube que opera bajo un modelo de consumo por demanda y suscripción, ofreciendo capacidades en cómputo, almacenamiento, inteligencia artificial, bases de datos, monitoreo, ciberseguridad, entre otros. Esta infraestructura ha sido adoptada progresivamente para soportar sistemas críticos de la Rama Judicial en el marco de su estrategia de transformación digital.

Actualmente se alojan en la nube AWS los siguientes servicios:

Proyecto o Aplicativo	Descripción del proyecto	Servicio en AWS	Perspectiva de crecimiento
SIUGJ	Sistema Integrado de Gestión Judicial de la Rama Judicial – SIUGJ, es conjunto de soluciones tecnológicas que integra servicios digitales de acceso, registro y tramitación electrónica de los procedimientos judiciales, la gestión documental electrónica del expediente judicial y los servicios transversales de apoyo a la gestión judicial, bajo parámetros de accesibilidad, seguridad de la información, basado en un marco de interoperabilidad que facilite la integración e intercambio de información y el aprovechamiento de los datos de la gestión judicial.	Amazon RDS, AWS Fargate, Amazon EFS, Application Load Balancer, Amazon ECR	Hoy el SIUGJ ambiente de Preproducción y Producción opera en infraestructura propia en AWS desde el 2024. En octubre de 2024 se tenían vinculados 210 despachos judiciales a SIUGJ.

Proyecto o Aplicativo	Descripción del proyecto	Servicio en AWS	Perspectiva de crecimiento
Plataforma de interoperabilidad	Disponer de una plataforma que permita la construcción de los servicios, orquestación y despliegue de los mismos, siempre dando cumplimiento a los estándares del Min TIC y la Rama Judicial, de forma tal que se facilite la entrega de los servicios digitales a los ciudadanos y otras entidades. La actual plataforma de interoperabilidad se encuentra en funcionamiento en el datacenter del CAN, con deficiencias de capacidad y seguridad	Open Shift Container Platform with Application Foundations Premium	Actualmente Migrado y en producción en AWS.
Seguridad y Monitoreo de la Plataforma	Es preciso anotar que esta infraestructura tecnológica requiere la protección de sistemas de seguridad, por ello se debe contar con la habilitación de la infraestructura de seguridad necesaria de modo que permita además el monitoreo constante de todos los recursos desplegados en la nube (AWS Web Application Firewall), la toma de decisiones basadas en inteligencia artificial y la implementación de políticas de seguridad que resguarden la información frente a cualquier tipo de ataque cibernético y una capa adicional (Amazon CloudFront) de seguridad que es un punto de entrada global y escalable que usa la red perimetral global de Amazon y estará protegiendo ataques que puedan ingresar por HTTP y HTTPS.	WAF, Elastic Load Balancing, AWS Config, AWS Security Hub, Amazon GuardDuty, AWS Cloud trail, amazon Athena, CloudWatch, AWS Backup, Virtual Private Cloud AWS GuardDuty, AWS Macie, AWS Inspector, AWS Shield	Estos servicios ya se encuentran implementados para cada una de las cargas de trabajo que ya se encuentran en la nube de AWS. AWS Shield es una protección contra ataques DDoS.
Pruebas de Carga	Servicio que se solicita por demanda al contratista quien nos apoya con especialistas en pruebas de carga.	AWS EC2, Jmeter	Servicio prestado por el contratista Nuvu para pruebas de carga para aplicativos antes de su migración y/o salida en vivo a producción como Portal Publicaciones Procesales, Portal Rama Judicial, Carrera Judicial, Alfresco, Tarjeta Digital, entre otros.
Análisis de Sentencias	Solución de Inteligencia Artificial para el procesamiento automatizado de sentencias en Asistencia Legal. Analiza expedientes con PLN e IA Generativa, extrayendo y estructurando información clave, que luego se transfiere a EFINOMINA	Desarrollada con el framework HOUNDOC, la solución orquesta servicios de AWS para procesar expedientes y extraer entidades clave, utilizando: Amazon S3,	En 2025, el Grupo de Sentencias de la Unidad de Asistencia Legal planea procesar aproximadamente 14.000 expedientes represados desde 2019. Asimismo, se está evaluando

Proyecto o Aplicativo	Descripción del proyecto	Servicio en AWS	Perspectiva de crecimiento
	para la generación del acto administrativo.	AWS Lambda, AWS Glue, AWS Opensearch, AWS Step Functions, Amazon Simple Email Service, Amazon Elastic Container Service, Amazon Elastic Load Balancing, Amazon Relational Database Service, Amazon Textract, Amazon Bedrock, Amazon Cloudwatch, AWS Identity and Access Management, AWS Secrets Manager	la viabilidad de la fase 2 del proyecto, que permitiría a los usuarios radicar expedientes a través de un portal web. Este portal validaría los documentos antes de enviarlos a la solución para la extracción automatizada de entidades.
Inteligencia Artificial	Implementación progresiva de iniciativas piloto basadas en Inteligencia Artificial para apoyar la transformación digital de la justicia y dar cumplimiento a lo señalado en el **ACUERDO PCSJA24-12243** del 16 de diciembre de 2024 "Por el cual se adoptan lineamientos para el uso y aprovechamiento respetuoso, responsable, seguro y ético de la inteligencia artificial en la Rama Judicial" "**Artículo 12. Análisis para soluciones o proyectos institucionales.** La Unidad de Transformación Digital e Informática, en coordinación con las unidades competentes, deberá priorizar las siguientes acciones tendientes a la implementación de proyectos, la habilitación y disposición de soluciones institucionales con IA: 1. Adelantar pruebas y estudios de viabilidad para implementar proyectos, disponer y habilitar soluciones o herramientas institucionales de IA, enfocados inicialmente en los siguientes tipos de uso, sin perjuicio de otros que sean identificados o solicitados: a. Gestión administrativa y documental: reparto, agenda	Amazon Bedrock, Amazon Textract, Amazon Comprehend, AWS Lambda, Amazon S3, Amazon CloudWatch, AWS IAM	Durante el periodo 2025-2026 se proyecta ejecutar entre 3 y 5 pilotos en distintos frentes estratégicos (relatoría, gestión administrativa y documental, apoyo a la gestión judicial). Cada piloto se implementará de forma modular, sobre cargas de trabajo específicas, evaluando progresivamente su desempeño y valor agregado. Esta fase experimental permitirá sentar las bases para la adopción institucional de soluciones basadas en IA en el mediano plazo. Asimismo, estos pilotos nos permitirán avanzar en la valoración de herramientas de IA sobre las cuales la Rama Judicial podría hacer uso verificando condiciones de seguridad, demanda de recursos, capacidades de infraestructura requeridas, entre otros, de forma que dependiendo de los resultados se puedan adoptar e incluir dentro de la operación de la entidad de manera segura y progresiva.

Proyecto o Aplicativo	Descripción del proyecto	Servicio en AWS	Perspectiva de crecimiento
	para la programación de diligencias, digitalización y clasificación de expedientes, revisión de completitud de documentos, textualización de las grabaciones de las audiencias, sistemas de relatoría y motores de búsqueda de jurisprudencia y anonimización de datos. b. Apoyo a la función judicial: referenciación de jurisprudencia, seguimiento de líneas jurisprudenciales, análisis de datos estadísticos, identificación de temas repetitivos, asistencia en procesos de notificaciones, orientar el acceso a servicios y trámites e interacción con usuarios, sin que estos usos supongan una labor de creación de contenido, interpretación de hechos o textos, ni solución de casos. c. Corrección y síntesis de textos, con supervisión humana posterior para su aplicación. 2. Avanzar, en el análisis de idoneidad y pertinencia del desarrollo, habilitación o el uso de sistemas, servicios o herramientas de IA generativa especializados en jurisprudencia y normativa, para el apoyo en el ejercicio de la función pública de administración de justicia.		
Arquitecto Senior en Nube Hibrida	Se requieren 580 horas para apoyar al equipo de administración de la plataforma para atender situaciones imprevistas que puedan darse durante la operación que requieran de acompañamiento especializado. El número de horas solicitado es mucho menor al utilizado en el contrato anterior debido a que la demanda de las mismas bajo dos razones fundamentalmente: Por otra parte, la administración de la plataforma fue asumida por el equipo de la Unidad de Transformación	Horas experto	Estas horas serán consumidas por demanda dependiendo de las necesidades de la operación.

Proyecto o Aplicativo	Descripción del proyecto	Servicio en AWS	Perspectiva de crecimiento
	Digital – División de Servicios Tecnológicos.		
Ivanti	Ivanti es una solución diseñada para optimizar y automatizar la gestión de la mesa de ayuda (Service Desk) de la Rama Judicial, brindando una plataforma centralizada para el soporte técnico y la gestión de servicios de TI. Su enfoque principal es mejorar la eficiencia operativa, reducir tiempos de respuesta y elevar la satisfacción del usuario.	EC2, RDS	Actualmente alojada en la nube de AWS. Se tiene previsto el incremento de su infraestructura para atender la entrada en operación de las ventanillas administrativas de seccionales y la unidad administrativa.

Fuente: Elaboración propia. UTDI.

3.2. Capacidades requeridas desde el punto de vista funcional.

Actualmente, los créditos de nube y el soporte son administrados a través de cuentas institucionales, con acompañamiento de un Cloud Service Provider (CSP) autorizado por Amazon y un account manager especializado en sector público. Esto permite a la Rama Judicial gestionar el consumo, permisos, pagos y aprovisionamiento de servicios de manera centralizada y eficiente.

3.2.1. Servicios de cómputo

Entre los servicios en operación actualmente se encuentran:

- SIUGJ: Plataforma de gestión procesal laboral en producción, que atiende más de 600 despachos y 87.000 procesos.
- Ivanti (JUDIT): Sistema de gestión de servicios TI, con implementación nacional y portafolio ampliado en la Seccional Medellín.
- Matriz RBAC: Herramienta de identidad digital integrada con mecanismos de control de acceso (Contrato 153 de 2024).
- Plataforma de interoperabilidad: En operación tras migración desde IFX.
- Análisis de sentencias con IA: En fase de pruebas para producción.
- Servicios de ciberseguridad y monitoreo: Implementación de WAF, GuardDuty, Inspector, Security Hub, entre otros.
- Pruebas de carga y concepto: Validaciones previas al paso a producción.

3.2.2. Servicios de almacenamiento:

La gestión de almacenamiento se realiza principalmente con:

- **Amazon S3:** Repositorio de objetos con políticas de acceso, cifrado y gestión de versiones.
- **Amazon EBS/EFS:** Almacenamiento en bloque y de archivos, respectivamente.

Durante la ejecución de la Orden de Compra 122576, el promedio mensual de consumo ha sido de 1235 terabytes, cifra que evidencia el crecimiento en digitalización y necesidades

operativas. *(Ver Anexo 2 - Configuración técnica por aplicación – Cómputo y almacenamiento)*

3.2.3. Servicios de soporte: AWS Enterprise Support

AWS Enterprise Support es el servicio de soporte técnico más completo ofrecido por Amazon Web Services, disponible 24/7, que brinda atención especializada por parte de ingenieros expertos, herramientas avanzadas y tecnologías de monitoreo que permiten gestionar proactivamente el estado de los entornos en la nube. Adicionalmente, incorpora un Administrador Técnico de Cuentas (TAM), quien acompaña estratégicamente en temas de arquitectura, operación y optimización, ajustándose a las particularidades de las aplicaciones implementadas.

Si bien AWS dispone de esquemas de soporte básico y avanzado, la complejidad y criticidad de los sistemas de información de la Rama Judicial hace necesario contar con el nivel de soporte empresarial. Este es el único que garantiza atención prioritaria, gestión especializada de incidentes y un acompañamiento técnico permanente, alineado con las exigencias de disponibilidad y continuidad del servicio.

El servicio se encuentra incluido en el costo mensual de la infraestructura contratada y comprende los siguientes beneficios:

- Atención prioritaria por parte de ingenieros especializados, con tiempos de respuesta reducidos.
- Soporte multicanal (teléfono, chat y correo electrónico) para la gestión de incidentes.
- Acompañamiento en casos complejos, que requieren análisis o resolución técnica detallada.
- Acceso a herramientas avanzadas, como la API de soporte, la aplicación móvil de AWS y flujos de trabajo de automatización.

El consumo de estos servicios se resume a continuación:

Tema de soporte	Casos	Servicio utilizado
VPC	15	Conectividad y seguridad de redes.
DataSync	14	Problemas en las tareas de sincronización de datos.
RDS	13	Problemas de rendimiento y replicación en bases de datos.
S3	11	Replicación y configuración de sitios web estáticos.
Otros servicios		Se registraron incidencias en servicios como Systems Manager, EC2, Service Quotas y otros, cada uno con entre 1 y 9 casos, abarcando temas desde ajustes de límites y configuraciones hasta problemas específicos de seguridad y administración.

3.2.4. AWS Marketplace

A través de la AWS Marketplace, la Rama Judicial ha integrado soluciones complementarias de terceros con rápida implementación, centralización de pagos y control del consumo mediante créditos contratados.

ii. Infraestructura y tipo de infraestructura (virtualizada o dedicada), plataformas y software requeridos para la necesidad.

Los créditos adquiridos deberán permitir el consumo flexible, seguro y escalable de los siguientes servicios AWS, conforme a las necesidades operativas de la Rama Judicial:

a) Procesamiento

- Instancias virtuales (EC2, Lambda u otras) de cómputo de alto desempeño, para ejecutar sistemas judiciales, motores de inteligencia artificial y aplicaciones de análisis de datos jurisprudenciales.
- Autoescalamiento de recursos según demanda transaccional.
- Contenedores y microservicios para soluciones modulares.

b) Almacenamiento

- Servicios de almacenamiento persistente y replicado (S3, EFS, Glacier, etc.) para sistemas judiciales, respaldos institucionales y conservación digital de documentos.
- Encriptación en reposo y en tránsito.
- Políticas de retención y gestión del ciclo de vida.

c) Seguridad de la información

- Gestión de accesos e identidades (IAM, RBAC), con autenticación multifactor y políticas de acceso mínimo.
- Servicios de detección de amenazas (GuardDuty), protección de aplicaciones (WAF), gestión de llaves (KMS) y registros de auditoría (CloudTrail).
- Cumplimiento de normativas como ISO 27001, NIST y estándares nacionales de protección de datos.

d) Red y conectividad

- Redes virtuales privadas (VPC), subredes segmentadas, VPN site-to-site, gateways y balanceadores de carga (ELB).
- Alta disponibilidad en múltiples zonas de disponibilidad (AZ).
- Servicios de resolución DNS, firewall de red, detección de anomalías de tráfico.

e) Servicios administrados y analíticos

- Bases de datos relacionales y no relacionales (RDS, DynamoDB).
- Servicios de analítica, búsqueda y visualización de datos (Athena, QuickSight, OpenSearch).
- Integración con herramientas para automatización, analítica y flujos de trabajo (Step Functions, EventBridge).

f) Interoperabilidad y APIs

- Infraestructura para la exposición y consumo de APIs (API Gateway).
- Gestión de eventos judiciales en tiempo real y sincronización con otras entidades públicas.
- Soporte para arquitecturas orientadas a eventos (Event-driven).

g) Soporte técnico especializado

- Acceso a soporte técnico de AWS en español con disponibilidad 24/7.
- Capacidad de atención de incidentes críticos de infraestructura.
- Acompañamiento técnico para configuración, optimización, seguridad y respuesta ante fallas.

iii. Requisitos de gobierno y gestión de datos para la necesidad.

Los requisitos de gobierno y gestión de datos son esenciales para garantizar una administración eficaz, segura y conforme a normativas en entornos AWS. A continuación, se presentan los principales requisitos que una organización debe tener en cuenta al implementar estrategias de gobierno y gestión de datos en AWS:

- Políticas de Gobernanza de Datos: Establecer políticas claras de gobernanza que definan roles, responsabilidades y procesos relacionados con la gestión de datos en AWS. Estas políticas deben incluir la clasificación de datos críticos, niveles de sensibilidad y políticas de retención, alineadas con servicios como AWS Organizations y AWS Control Tower.

- Control de Acceso y Seguridad: Aplicar controles estrictos mediante AWS Identity and Access Management (IAM) para la autenticación y autorización, junto con cifrado de datos en reposo y en tránsito utilizando AWS Key Management Service (KMS) y AWS Certificate Manager (ACM).

- Auditoría y Seguimiento: Habilitar AWS CloudTrail para registrar todas las actividades relacionadas con los datos y recursos, y usar Amazon CloudWatch para el monitoreo en tiempo real. Esto permite cumplir requisitos regulatorios y detectar actividades anómalas.

- Gestión de Identidad y Acceso (IAM): Utilizar políticas de IAM para otorgar acceso basado en el principio de menor privilegio, y complementar con AWS SSO o federación con directorios corporativos para un control centralizado y seguro de identidades.

- Catalogación y Metadatos: Implementar AWS Glue Data Catalog para crear un repositorio centralizado de metadatos, lo cual facilita la exploración, clasificación y descubrimiento de datos dentro del ecosistema de AWS.

- Calidad de Datos: Utilizar herramientas como AWS Glue, Amazon Deequ o soluciones integradas de terceros para validar, limpiar y estandarizar datos antes de su análisis o almacenamiento definitivo.

- Cumplimiento Normativo: Asegurar el cumplimiento con normativas como GDPR, HIPAA, PCI DSS u otras, apoyándose en servicios como AWS Artifact, AWS Config y los estándares predefinidos de AWS Security Hub para evaluar el estado de cumplimiento.

- Respaldo y Recuperación: Establecer estrategias de respaldo y recuperación con AWS Backup, Amazon S3 Versioning, Amazon RDS snapshots o AWS Elastic Disaster Recovery, asegurando así la continuidad del negocio frente a posibles fallos o pérdida de datos.

- Gestión del Ciclo de Vida de Datos: Definir políticas de ciclo de vida de almacenamiento utilizando características como S3 Lifecycle Policies, Intelligent-Tiering o automatización con AWS Data Lifecycle Manager para eliminar, archivar o mover datos según su antigüedad y uso.

- Evaluación de Riesgos: Realizar evaluaciones periódicas de riesgos de seguridad y privacidad mediante AWS Security Hub, Amazon Inspector y AWS Trusted Advisor, identificando vulnerabilidades, malas prácticas o configuraciones incorrectas que puedan poner en riesgo los datos.

iv. Requisitos de seguridad para la necesidad.

La seguridad es un componente esencial al utilizar servicios en la nube como AWS. A continuación, se detallan los principales requisitos de seguridad que deben considerarse para proteger la infraestructura, los datos y los usuarios en AWS:

- Políticas de Seguridad: Definir políticas de seguridad claras que aborden la gestión de contraseñas, rotación de claves, acceso a recursos, auditoría y mejores prácticas alineadas con el AWS Well-Architected Framework – Pilar de Seguridad.

- Control de Acceso: Gestionar el acceso a los recursos a través de AWS Identity and Access Management (IAM) usando políticas basadas en roles (RBAC), políticas de acceso condicional y principios de privilegio mínimo.

- Autenticación Multifactor (MFA): Habilitar MFA para usuarios con privilegios elevados y cuentas críticas a través de AWS IAM o AWS IAM Identity Center (anteriormente AWS SSO), fortaleciendo la autenticación.

- Gestión de Identidad: Integrar soluciones de identidad corporativas mediante federación SAML o sincronización con directorios mediante AWS Directory Service, y gestionar el acceso de forma centralizada con IAM Identity Center.

- Seguridad de Red: Utilizar Amazon VPC con Security Groups y Network ACLs, implementar AWS WAF (Web Application Firewall) y AWS Network Firewall para proteger redes, aplicaciones y controlar el tráfico entrante/saliente.

- Seguridad de Datos: Aplicar cifrado en reposo con AWS KMS o claves administradas por el cliente (CMK), y cifrado en tránsito usando TLS. Además, utilizar Amazon Macie para identificar y clasificar datos sensibles.

- Auditoría y Monitorización: Implementar monitoreo y auditoría con AWS CloudTrail, Amazon CloudWatch, AWS Config y AWS Security Hub para registrar, visualizar y correlacionar eventos de seguridad en tiempo real.

- Respuesta a Incidentes: Definir un plan de respuesta a incidentes que incluya la integración con herramientas como AWS Systems Manager, automatización con AWS Lambda, y uso de AWS GuardDuty para la detección de amenazas.

- Actualizaciones y Parches: Usar AWS Systems Manager Patch Manager para automatizar la aplicación de parches y actualizaciones de seguridad en sistemas operativos y software administrado.

- Cumplimiento Normativo: Validar el cumplimiento de normas y estándares como ISO 27001, GDPR, HIPAA, PCI DSS, usando AWS Artifact, AWS Config y AWS Audit Manager para generar evidencias y reportes.

- Educación y Entrenamiento: Capacitar al personal en seguridad en la nube mediante cursos oficiales de AWS Training and Certification y prácticas recomendadas en AWS Well-Architected Labs.

- Evaluación de Riesgos: Realizar evaluaciones periódicas con herramientas como Amazon Inspector para análisis de vulnerabilidades, AWS Trusted Advisor para identificar configuraciones inseguras y Security Hub para centralizar hallazgos.

- Respaldo y Recuperación: Establecer mecanismos de respaldo automatizado con AWS Backup, S3 Versioning o Snapshots de EBS/RDS, y definir estrategias de recuperación ante desastres con AWS Elastic Disaster Recovery.

v. Requisitos de privacidad para la necesidad.

La privacidad de los datos es un aspecto crítico al operar en la nube, especialmente cuando se gestionan datos personales, confidenciales o sensibles. A continuación, se presentan los principales requisitos de privacidad que deben considerarse en entornos AWS para garantizar la protección de la información y el cumplimiento normativo:

- Evaluación de Datos Sensibles: Identificar, clasificar y etiquetar los datos que se almacenarán o procesarán en AWS, especialmente aquellos que contienen información personal, financiera o de salud. Herramientas como Amazon Macie ayudan a detectar automáticamente datos sensibles, como PII (Personally Identifiable Information).

- Cumplimiento Normativo: Verificar el cumplimiento de marcos regulatorios como GDPR, HIPAA, CCPA, PCI DSS, entre otros. AWS proporciona recursos como AWS Artifact para acceder a reportes de cumplimiento y auditorías de terceros que certifican los controles implementados.

- Políticas de Privacidad Claras: Establecer y comunicar políticas de privacidad que definan cómo se recopilan, almacenan, procesan y comparten los datos en AWS. Estas políticas deben ser comprensibles y disponibles para los usuarios finales y las partes interesadas.

- Consentimiento Transparente: Diseñar procesos claros para la obtención del consentimiento de los usuarios, cumpliendo con regulaciones aplicables y asegurando el registro verificable del mismo. Esto se puede apoyar en flujos de aplicación y almacenamiento cifrado de consentimientos.

- Cifrado de Datos: Aplicar cifrado de datos en reposo utilizando AWS KMS o claves gestionadas por el cliente (CMK), y cifrado en tránsito mediante TLS/SSL en servicios como Amazon S3, RDS, EBS, Redshift, entre otros.

- Control de Acceso: Utilizar AWS IAM e IAM Identity Center para aplicar control de acceso basado en roles (RBAC), asegurando que solo usuarios autorizados accedan a los datos según el principio de mínimo privilegio.

- Auditoría y Seguimiento: Habilitar AWS CloudTrail y AWS Config para registrar toda actividad relacionada con recursos y datos. También se recomienda usar AWS CloudWatch para generar alertas y análisis en tiempo real.

- Notificación de Brechas: Establecer procedimientos claros para la notificación de incidentes de seguridad o violaciones de datos, cumpliendo con los tiempos establecidos por las normativas. Se recomienda integrar AWS SNS, AWS Lambda y AWS Security Hub para automatizar alertas y respuestas.

- Eliminación Segura de Datos: Configurar políticas de ciclo de vida en Amazon S3, o usar mecanismos como Delete Markers, versión de objetos, AWS Data Lifecycle Manager o herramientas de destrucción segura de datos para asegurar la eliminación definitiva cuando los datos ya no sean necesarios.

- Gobernanza de Datos: Aplicar principios de gobernanza utilizando AWS Lake Formation, AWS Glue Data Catalog y etiquetas (tags) para asegurar la trazabilidad, integridad y correcta gestión de los datos a lo largo de su ciclo de vida.

- Evaluación de Proveedores: Verificar que los servicios de terceros que se integran en el entorno AWS cumplan con los mismos estándares de privacidad. Esto puede incluir la revisión de certificaciones SOC 2, ISO 27018 y otros reportes disponibles en AWS Marketplace o AWS Artifact.

- Educación y Entrenamiento: Proporcionar formación en privacidad y protección de datos a los empleados que interactúan con datos en AWS. AWS ofrece recursos y capacitaciones específicas mediante AWS Training and Certification y el AWS Compliance Learning Path.

vi. Requisitos de cumplimiento de regulaciones para la necesidad.

Cumplir con las regulaciones aplicables es fundamental al utilizar AWS para alojar datos, sistemas y aplicaciones. Las regulaciones varían según el sector y la jurisdicción, por lo que es clave implementar prácticas de cumplimiento adaptadas a cada contexto. A continuación, se presentan los requisitos generales a tener en cuenta:

- Identificación de Regulaciones Aplicables: La organización debe identificar las regulaciones que rigen su operación, como GDPR, HIPAA, PCI DSS, SOC 2, ISO

27001, FedRAMP, entre otras. AWS proporciona recursos en el portal de cumplimiento (AWS Compliance Center) y reportes oficiales en AWS Artifact.

- Auditoría y Seguimiento: Implementar soluciones de auditoría con AWS CloudTrail, AWS Config, Amazon CloudWatch Logs, y AWS Security Hub para registrar y supervisar actividades clave, generar evidencia de cumplimiento y detectar anomalías de seguridad.

- Seguridad de Datos: Aplicar cifrado de datos en tránsito (TLS) y en reposo (AES-256) usando AWS KMS, además de establecer controles de acceso y políticas de protección de datos con IAM, S3 Bucket Policies y Resource Access Manager (RAM).

- Control de Acceso: Usar AWS Identity and Access Management (IAM) e IAM Identity Center (SSO) para definir controles granulares basados en roles (RBAC), y políticas de acceso condicional (como uso de MFA, ubicaciones confiables, etc.).

- Gestión de Identidad y Acceso (IAM): Implementar modelos de privilegio mínimo con IAM y gestionar identidades desde directorios corporativos integrados (usando AWS Directory Service o federación SAML) para asegurar el acceso adecuado a recursos regulados.

- Notificación de Brechas: Establecer mecanismos de detección y notificación de incidentes que cumplan con regulaciones como GDPR o HIPAA, utilizando herramientas como AWS GuardDuty, Amazon Macie, AWS Config y flujos automatizados con AWS Lambda y SNS para notificaciones inmediatas.

- Cumplimiento de Privacidad: Adoptar controles que aseguren la protección de datos personales y los derechos de los usuarios, incluyendo monitoreo con Macie, herramientas para auditoría de accesos, y retención/anonimización de datos personales.

- Cumplimiento Normativo: Usar AWS Audit Manager para mapear automáticamente controles técnicos a marcos regulatorios (PCI DSS, GDPR, NIST, etc.) y generar reportes de cumplimiento. Las certificaciones de AWS (ISO, SOC, FedRAMP) están disponibles para clientes a través de AWS Artifact.

- Gestión de Ciclo de Vida de Datos: Establecer políticas de retención y eliminación con herramientas como Amazon S3 Lifecycle Policies, AWS Backup, y AWS Data Lifecycle Manager para garantizar cumplimiento con normativas de conservación de registros y borrado seguro.

- Capacitación y Concienciación: Brindar formación continua a los empleados sobre prácticas de cumplimiento, seguridad y privacidad en la nube. AWS ofrece capacitaciones como AWS Security Essentials, Compliance Fundamentals y AWS Well-Architected Framework.

- Evaluación de Riesgos y Pruebas de Vulnerabilidad: Realizar evaluaciones periódicas mediante herramientas como Amazon Inspector para escaneos automáticos, además de AWS Security Hub y Trusted Advisor para identificar vulnerabilidades y recomendaciones de seguridad.

vii. Requisitos de interoperabilidad e integración para la necesidad incluyendo, sin limitarse a, la siguiente información para cada uno de los sistemas a integrarse:

Actualmente la plataforma de interoperabilidad migrada y modernizada en la nube de AWS permite el intercambio de información con entidades como Registraduría Nacional del Estado Colombiano (RNEC), Confecámaras, el Departamento de Función pública, la Superintendencia de Notariado y Registro y la Defensoría. Se están llevando a cabo actividades para que: i) la Rama Judicial pueda consumir el Servicio web de la RNEC que permite consumir la información del Sistema de Información de Registro Civil, ii) la Agencia Nacional de Defensa Jurídica del Estado, Colpensiones y la Contraloría General de la República (CGR) consuma los servicios web de la Consulta de Procesos Nacional Unificada (CPNU), iii) la Superintendencia de Industria y Comercio consuma los servicios web para consultar el Sistema de Registro Nacional de Abogados, iv) el Sistema de Información de Planeación de la Rama Judicial (proyecto en ejecución) consuma los servicios web que provee SIIF para la consulta de información presupuestal, v) la Superintendencia de Salud con intermediación del Ministerio de Justicia y del Derecho trasladen los procesos y expedientes judiciales para segunda instancia, vi) el liquidador judicial de lo contencioso administrativo consuma servicios web del Banco de la República, el DANE, la Superintendencia Financiera y Función Pública.

Por otro lado, se están adelantando acciones dentro de proyectos que están en etapa de ejecución para que el bus de servicios de interoperabilidad sea el integrador entre sistemas de la Rama Judicial así: SIERJU - Efinómina, SIERJU - SAMAI, SIERJU - SIUGJ

viii. Ambientes requeridos (desarrollo, pruebas y producción) para la necesidad.
Desarrollo, Test y Producción.

ix. Servicios complementarios requeridos para la necesidad.

Se prevé que todas las soluciones deben contar con ambientes de desarrollo, pruebas, pre-producción y producción, sin embargo, el aprovisionamiento en AWS se está realizando sobre la cuenta Productiva (ambientes de producción) y sobre una nueva cuenta de Desarrollo Test y Preproducción (ambientes de Dev-Test).

x. Requisitos de administración de múltiples sistemas, ambientes o nubes (públicas o privadas).

Nube pública AWS soportada por Amazon y Administrada por personal de la CSJ.

xi. Estimación de cantidad de usuarios finales del sistema para el periodo contratado o, si es un sistema que presta servicios a otro(s) sistema(s), cantidad de llamados estimados para el periodo contratado; puede ser medido en días y/o meses y/o años (puede presentar el caso en que el sistema preste servicio a usuarios finales y a otros sistemas).

Volumen Estimado de Demanda del Sistema	Tiempo
SIUGJ: 635 despachos judiciales 62.500 expedientes abiertos en 2024	1 año
IVANTI: 63.652 usuarios	1 año

Volumen Estimado de Demanda del Sistema	Tiempo
ANALISIS DE SENTENCIAS: 14.000 expedientes	1 año
Identidad Digital: Monitoreo de 40.000 activos incluyendo equipos de cómputo y servidores, 189 fuentes de información correlacionada	1 año
Interoperabilidad: Intercambio de información con más de 10 entidades públicas, 20.993 consultas diarias	1 año

4. Capacidades requeridas

En el Anexo_2_Ficha Técnica AWS se detallan para cada aplicación las cantidades de cada uno de los servicios.

Asimismo, se relaciona la proyección de capacidades que determinan el total de créditos a ser adquiridos, es preciso aclarar **que la entidad tiene la posibilidad de asignar y/o quitar capacidades a las soluciones existentes o nuevas soluciones y servicios**, siempre y cuando tenga disponibilidad de créditos al momento de realizar el aprovisionamiento requerido.

La url de la calculadora de AWS utilizada para realizar la proyección de créditos fue:

https://calculator.aws/#/estimate?id=36f0a02699bce5f2daf5405bbe57203cb8465648

En términos generales el alcance de la presente contratación incluye capacidades previstas en el catalogo de servicios de AWS, Soporte Premium de AWS y horas Experto.

5. Condiciones transversales

Las condiciones transversales aplicables al servicio a contratar están descritas en el *Anexo_3_Condiciones_Transversales*

6. Acuerdos de Nivel de Servicio

Los Acuerdos de Nivel de Servicio (ANS) definidos para el presente proceso se pueden consultar en el *Anexo_4_ANS Servicio*