

Destinatario: DAVID FERNANDO DIAZ PALACIO

Fecha: 30/10/2025 17:42:13.951 Anexos: 0

Asunto: Consecutivo de Comunicaciones Oficiales Internas

Remitente: DIEGO MAURICIO SALAS RAMIREZ

Radicador: Miguel Angel Parra Hernandez

COMUNICACIÓN INTERNA

Para: DAVID FERNANDO DIAZ PALACIO
Subdirector de abastecimiento y servicios generales

De: DIEGO MAURICIO SALAS RAMIREZ
Subdirector de Área de Subdirección Información

ASUNTO: Solicitud de Contratación Línea PAA-593

Cordial saludo,

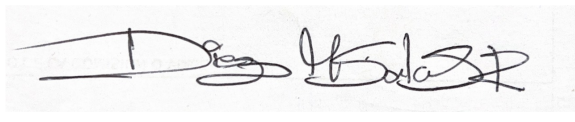
Se requiere la contratación de la línea 593, cuyo objeto es **"Contratar una solución SaaS para el Icfes enfoca en la habilitación de entornos de trabajo virtuales seguros para el Banco de Items, utilizando Houndoc como plataforma SaaS."** Perteneciente a la Subdirección de Información. Para este propósito, se adjuntan los siguientes documentos:

- Estudios previos
- Solicitud de CDP
- CDP
- Matriz de Riesgos
- Anexo técnico
- Estudio de Mercado

Enlace:https://icfesgovco.sharepoint.com/:f:/s/RepositorioDTI/EigMkG_8N_9PppmPB_m93d0B6dNe1RE9JgtsmzguHgsImA?e=tbvscF

Cordialmente,


Aprobado por:

A handwritten signature in black ink, appearing to read 'Diego Salas Ramirez', is written over a horizontal line.

Nombre: Diego Mauricio Salas Ramirez

Identificación: 11226503

Fecha: 2025-10-30 17:50:59

	ESTUDIO PREVIO – TIENDA VIRTUAL DEL ESTADO COLOMBIANO		Código: GAB -FT055
	GESTIÓN DE ABASTECIMIENTO		Versión: 003
Clasificación de la información	<input type="checkbox"/> PÚBLICA	<input type="checkbox"/> CLASIFICADA	<input type="checkbox"/> RESERVADA

Fecha de elaboración: 28/10/2025

1. COMPRA QUE REALIZARÁ A TRAVÉS DE LA TIENDA VIRTUAL DEL ESTADO COLOMBIANO: Marque con una (X) según corresponda


Acuerdo Marco de Precios	
Bienes de grandes superficies	
Otros instrumentos de agregación de demanda	X

2. ANÁLISIS Y JUSTIFICACIÓN DE LA NECESIDAD QUE EL ICFES PRETENDE SATISFACER CON LA CONTRATACIÓN

a. Competencia

El Instituto Colombiano para la Evaluación de la Educación – Icfes, con el liderazgo de la Dirección de Tecnología e Información en conjunto con sus Subdirecciones y con el propósito de avanzar en la transformación digital para impactar positivamente la prestación de los servicios hacia los usuarios, generando valor público en cada una de sus interacciones y mejorando la provisión de servicios digitales de calidad y confianza; ha venido incorporando las acciones y los lineamientos que señala el Gobierno nacional a través del Ministerio de Tecnologías de la Información y las Comunicaciones para la implementación de la política de Gobierno Digital, Decreto 1078 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”, modificado por en el Decreto 1008 de 2018 “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones”.

En atención a lo anterior, la Dirección de Tecnología e Información, ha elaborado su Plan Estratégico de TI (Tecnología e Información) el cual se encuentra alineado con los objetivos estratégicos del Instituto y define las iniciativas, programas y proyectos que se deben implementar para “promover e identificar oportunidades de transformación digital que permitan agilizar y simplificar los procesos del Instituto, administrar de manera eficiente los recursos, fortalecer las capacidades institucionales requeridas para ofrecer servicios de información que apoyen el proceso de toma de decisiones basados en datos, generar confianza en los servicios de T.I (Tecnología e Información), facilitando su uso y apropiación de forma continua y oportuna, fortalecer la capacidad de Innovación Tecnológica para ofrecer trámites y servicios de calidad y confianza y; consolidar relaciones de cooperación con entidades públicas y privadas, a través de la implementación de servicios de Interoperabilidad”.

 Icfes	ESTUDIO PREVIO – TIENDA VIRTUAL DEL ESTADO COLOMBIANO		Código: GAB -FT055
	GESTIÓN DE ABASTECIMIENTO		Versión: 003
Clasificación de la información	<input type="checkbox"/> PÚBLICA	<input type="checkbox"/> CLASIFICADA	<input type="checkbox"/> RESERVADA

A su vez y de conformidad con el artículo 21 del Decreto 5014 de 2009, son funciones de la Subdirección de Información las siguientes:

1. Administrar, construir y consolidar las bases de datos que apoyen el proceso de análisis y desarrollo de nuevos productos.
2. Diseñar, implementar, administrar y mantener actualizado un Sistema Nacional de Información de la Calidad de la Educación, con base en los resultados alcanzados en los exámenes de Estado, así como en los factores asociados a dichos resultados.
3. Dar soporte para automatizar las consultas sistemáticas de información del Sistema Nacional de Información de la Calidad de la Educación.
4. Las demás asignadas, según la naturaleza de la dependencia.

Que, conforme a lo expuesto, le corresponde a la Subdirección de Información gestionar la contratación de una solución de analítica e inteligencia artificial que fortalezcan la capacidad de análisis y optimización de datos del Instituto.


b. Necesidad específica por satisfacer, conveniencia y oportunidad.

El Instituto Colombiano para la Evaluación de la Educación (Icfes) requiere modernizar la operación del Banco de Items, actualmente limitada por restricciones operativas en su sistema de almacenamiento. El Banco de Items es un área crítica de alta seguridad donde se realizan procesos fundamentales como la diagramación, revisión y armado de las pruebas que el Icfes aplica a nivel nacional.

La infraestructura actual presenta limitaciones significativas de capacidad de almacenamiento y procesamiento, no cuenta con sistemas de respaldo adecuados y existe un riesgo considerable de pérdida de información sensible acumulada a lo largo de los años. Estos factores comprometen la eficiencia operativa y la seguridad de los datos críticos que maneja el Icfes en sus procesos de evaluación.

Así las cosas, evidenciada la anterior necesidad, con la contratación que se justifica con el presente documento de estudios previos, se pretende la búsqueda de una solución para implementar entornos de trabajo virtuales seguros para el Banco de Items utilizando Houndoc como plataforma SaaS. Esta implementación permitirá establecer un entorno escalable, con sistemas de respaldo automáticos y mecanismos robustos de seguridad. La solución mantendrá los estrictos protocolos de seguridad necesarios para proteger la confidencialidad de la información del Banco de Items.

La solución propuesta está diseñada para atender las necesidades de los usuarios permanentes del área de diagramación y los usuarios ocasionales como gestores de pruebas y correctores de estilo, mejorando su eficiencia operativa mientras se permite el

 Icfes	ESTUDIO PREVIO – TIENDA VIRTUAL DEL ESTADO COLOMBIANO		Código: GAB -FT055
	GESTIÓN DE ABASTECIMIENTO		Versión: 003
Clasificación de la información	<input type="checkbox"/> PÚBLICA	<input type="checkbox"/> CLASIFICADA	<input type="checkbox"/> RESERVADA

cumplimiento de los requisitos de seguridad y confidencialidad propios de este proceso crítico para el Icfes. Adicionalmente, se contempla la capacitación del personal de tecnología del Icfes para permitir la adecuada administración y aprovechamiento de los nuevos entornos virtuales de trabajo.

c. Definición técnica de la forma en que el Icfes puede satisfacer su necesidad

1. El alcance de este proyecto comprende la implementación de una solución integral para la habilitación de entornos de trabajo virtuales seguros para el Banco de Items del Icfes mediante la plataforma SaaS Houndoc, abarcando los siguientes componentes:

1.1 Áreas de intervención


La solución propuesta contempla tres áreas principales de intervención:

- Entornos de trabajo virtuales seguros:** Implementación de una plataforma escalable basada en Houndoc que permita la creación y gestión de hasta 30 espacios de trabajo virtuales para los usuarios del Banco de Items, con acceso a todas las herramientas necesarias para la diagramación y gestión de pruebas.
- Sistema de seguridad y control de acceso:** Establecimiento de mecanismos robustos para permitir la confidencialidad e integridad de la información, incluyendo VPN dedicada, control de acceso granular basado en roles y auditoría completa de actividades.
- Integración con sistemas existentes:** Configuración de conectores e interfaces que permitan la integración fluida entre los entornos virtuales de Houndoc , la plataforma Prisma y el directorio activo de la institución.

1.2 Objetivos principales

Los objetivos fundamentales que persigue este proyecto son:

- Implementar entornos de trabajo virtuales seguros para los usuarios del Banco de Items utilizando la plataforma Houndoc.
- Establecer una solución escalable que elimine las limitaciones actuales de capacidad y permita el crecimiento según las necesidades del Icfes.
- Configurar sistemas robustos de respaldo automático que eliminen el riesgo de pérdida de información.

 Icfes	ESTUDIO PREVIO – TIENDA VIRTUAL DEL ESTADO COLOMBIANO		Código: GAB -FT055
	GESTIÓN DE ABASTECIMIENTO		Versión: 003
Clasificación de la información	<input type="checkbox"/> PÚBLICA	<input type="checkbox"/> CLASIFICADA	<input type="checkbox"/> RESERVADA


4. Habilitar entornos de trabajo virtuales que mantengan o mejoren los controles de seguridad existentes.
5. Facilitar la integración con sistemas actuales como la plataforma Prisma, el directorio activo y las herramientas de la suite de Adobe utilizadas para la diagramación.
6. Capacitar al personal de tecnología del Icfes para la utilización efectiva y administración de los nuevos entornos virtuales, permitiendo la transferencia de conocimiento necesaria para su gestión autónoma.

1.3 Actividades principales

Para lograr los objetivos planteados, se desarrollarán las siguientes actividades clave:

1. **Análisis y diseño:** Levantamiento detallado de requisitos técnicos y de seguridad, análisis de los flujos de trabajo actuales, diseño de la arquitectura de entornos virtuales y definición de políticas de seguridad.
2. **Implementación de entornos virtuales y seguridad:** Configuración de la plataforma Houndoc, aprovisionamiento de espacios de trabajo virtuales, implementación de sistemas de respaldo automático, configuración de mecanismos de autenticación y permisos de acceso.
3. **Configuración de entornos de trabajo virtuales:** Personalización de los espacios virtuales para los usuarios del Banco de Items, instalación de aplicaciones necesarias (suite de Adobe), configuración de acceso a la plataforma Prisma y mantenimiento del sistema actual de carpetas y permisos.
4. **Configuración de almacenamiento seguro:** Establecimiento de repositorios seguros para la información del Banco de Items dentro de la plataforma Houndoc, con políticas de respaldo y recuperación automáticas.
5. **Capacitación y transición:** Formación al personal de tecnología del Icfes, elaboración de documentación técnica y acompañamiento en la transición hacia los nuevos entornos virtuales.
6. **Monitoreo y ajustes:** Seguimiento del rendimiento del sistema y verificación continua de la seguridad tras la implementación.

Esta solución permitirá modernizar la operación del Banco de Items mediante entornos de trabajo virtuales seguros basados en Houndoc, permitiendo la seguridad de la información

 Icfes	ESTUDIO PREVIO – TIENDA VIRTUAL DEL ESTADO COLOMBIANO		Código: GAB -FT055
	GESTIÓN DE ABASTECIMIENTO		Versión: 003
Clasificación de la información	<input type="checkbox"/> PÚBLICA	<input type="checkbox"/> CLASIFICADA	<input type="checkbox"/> RESERVADA

y mejorando significativamente la eficiencia operativa, sin comprometer los estrictos protocolos de confidencialidad requeridos para este proceso crítico del Icfes.

2. Detalle de alcance

El detalle del alcance para el proyecto de habilitación de entornos de trabajo virtuales seguros para el Banco de Items se estructura en fases claramente definidas, cada una con actividades específicas y resultados concretos:

2.1 Fase de análisis y diseño

Esta fase inicial establece las bases técnicas y operativas para la implementación exitosa de la solución:

1. Levantamiento detallado de requisitos técnicos y de seguridad

- **Resultado:** Documento de especificación de requisitos técnicos y de seguridad
- **Actividades:** Entrevistas con usuarios clave, análisis de infraestructura actual, identificación de necesidades específicas de seguridad y acceso

2. Análisis de flujos de trabajo actuales

- **Resultado:** Informe de procesos actuales y sistema de archivos
- **Actividades:** Documentación de los flujos de trabajo existentes, identificación de oportunidades de mejora, análisis del sistema de permisos actual

3. Diseño de la arquitectura de entornos virtuales con Houndoc


- **Resultado:** Documento de arquitectura con diagramas técnicos
- **Actividades:** Diseño de la configuración de Houndoc, especificación de entornos virtuales, definición de componentes de seguridad

4. Definición de políticas de seguridad y acceso

- **Resultado:** Documento de políticas de seguridad para los entornos virtuales
- **Actividades:** Establecimiento de controles de acceso y definición de políticas de auditoría

2.2 Fase de implementación de entornos virtuales y seguridad

En esta fase se implementan los componentes fundamentales de la plataforma:

 Icfes	ESTUDIO PREVIO – TIENDA VIRTUAL DEL ESTADO COLOMBIANO		Código: GAB -FT055
	GESTIÓN DE ABASTECIMIENTO		Versión: 003
Clasificación de la información	<input type="checkbox"/> PÚBLICA	<input type="checkbox"/> CLASIFICADA	<input type="checkbox"/> RESERVADA

1. Configuración de la plataforma Houndoc

- **Resultado:** Plataforma base configurada y lista para personalización
- **Actividades:** Aprovisionamiento de recursos, configuración de capacidad, implementación de escalabilidad automática

2. Implementación de sistemas de respaldo automático

- **Resultado:** Sistema de respaldo configurado y validado
- **Actividades:** Configuración de políticas de respaldo, programación de copias de seguridad, validación del proceso de recuperación

3. Implementación de sistemas de seguridad

- **Resultado:** Sistemas de seguridad configurados y validados
- **Actividades:** Configuración de VPN dedicada, implementación de cifrado de datos y configuración de permisos de acceso granulares

2.3 Fase de configuración de entornos de trabajo virtuales

Esta fase se enfoca en establecer los espacios de trabajo para los usuarios:

1. Creación y configuración de entornos virtuales

- **Resultado:** Entornos virtuales operativos con sistema operativo instalado
- **Actividades:** Creación de 30 espacios virtuales, configuración de recursos (CPU, memoria, almacenamiento), establecimiento de políticas de acceso

2. Instalación y configuración de aplicaciones


- **Resultado:** Entornos de trabajo con aplicaciones instaladas y configuradas
- **Actividades:** Instalación de suite de Adobe, configuración de aplicaciones específicas, validación de funcionamiento

2.4 Fase de configuración de integraciones

Esta fase crítica permite la interoperabilidad con los sistemas existentes del Icfes:

1. Integración con sistemas existentes

- **Resultado:** Conectores e interfaces configurados para sistemas del Icfes

 Icfes	ESTUDIO PREVIO – TIENDA VIRTUAL DEL ESTADO COLOMBIANO		Código: GAB -FT055
	GESTIÓN DE ABASTECIMIENTO		Versión: 003
Clasificación de la información	<input type="checkbox"/> PÚBLICA	<input type="checkbox"/> CLASIFICADA	<input type="checkbox"/> RESERVADA

- **Actividades:** Desarrollo de conectores para Prisma, conexión con directorio LDAP, configuración de interfaces de comunicación, pruebas de integración

2. Verificación de integridad de la información

- **Resultado:** Informe de verificación de integridad de datos
- **Actividades:** Comprobaciones automatizadas de integridad, verificaciones manuales selectivas, validación de estructura de datos

3. Pruebas de funcionamiento con datos reales

- **Resultado:** Informe de pruebas funcionales
- **Actividades:** Pruebas de acceso a datos, validación de funcionamiento del sistema de archivos actual en el nuevo entorno, verificación de rendimiento con carga real

4. Configuración de accesos a sistemas existentes

- **Resultado:** Integración con plataforma Prisma y directorio activo LDAP
- **Actividades:** Configuración de conectividad, validación de accesos, pruebas de integración

2.5 Fase de capacitación y transición

Esta fase permite la adopción efectiva de los nuevos entornos virtuales:

1. Capacitación al personal de tecnología del Icfes


- **Resultado:** Sesiones de capacitación y material de referencia técnica
- **Actividades:** Formación en administración de la plataforma Houndoc, gestión de seguridad, monitoreo y resolución de incidencias

2. Elaboración de documentación técnica

- **Resultado:** Manuales técnicos de administración y operación
- **Actividades:** Desarrollo de guías de administración, procedimientos operativos, documentación de arquitectura

3. Capacitación a usuarios finales

- **Resultado:** Usuarios capacitados en el uso de los entornos virtuales
- **Actividades:** Sesiones de formación, elaboración de guías de usuario, resolución de dudas específicas

 Icfes	ESTUDIO PREVIO – TIENDA VIRTUAL DEL ESTADO COLOMBIANO		Código: GAB -FT055
	GESTIÓN DE ABASTECIMIENTO		Versión: 003
Clasificación de la información	<input type="checkbox"/> PÚBLICA	<input type="checkbox"/> CLASIFICADA	<input type="checkbox"/> RESERVADA

2.6 Fase de monitoreo

Esta fase final permite la estabilización de la solución:

1. Monitoreo del rendimiento del sistema

- **Resultado:** Informes periódicos de rendimiento
- **Actividades:** Configuración de herramientas de monitoreo, análisis de métricas, identificación de oportunidades de mejora

2. Verificación continua de la seguridad

- **Resultado:** Informes de seguridad y recomendaciones
- **Actividades:** Análisis de logs de seguridad, verificación de controles, recomendaciones de mejora

La ejecución metódica de estas fases y actividades permitirá una implementación exitosa de entornos de trabajo virtuales seguros para el Banco de Items utilizando Houndoc como plataforma SaaS, cumpliendo con todos los objetivos establecidos y permitiendo la continuidad operativa de este componente crítico para el Icfes. El enfoque propuesto mantiene el sistema actual de manejo de carpetas y permisos con el que los usuarios están familiarizados, mientras mejora significativamente la seguridad, disponibilidad y eficiencia operativa.


3. Características de la solución

La solución propuesta para la habilitación de entornos de trabajo virtuales seguros para el Banco de Items se caracteriza por los siguientes componentes y funcionalidades, diseñados específicamente para atender las necesidades del Icfes:

3.1 Plataforma Houndoc como servicio (SaaS)

La base de la solución es la plataforma Houndoc, que ofrece:

- **Entornos virtuales seguros:** Espacios de trabajo aislados y protegidos que permiten la ejecución de aplicaciones y el acceso a datos de manera segura y controlada.
- **Alta disponibilidad:** Arquitectura redundante que permite el acceso continuo a los entornos de trabajo, minimizando los tiempos de inactividad.

 Icfes	ESTUDIO PREVIO – TIENDA VIRTUAL DEL ESTADO COLOMBIANO		Código: GAB -FT055
	GESTIÓN DE ABASTECIMIENTO		Versión: 003
Clasificación de la información	<input type="checkbox"/> PÚBLICA	<input type="checkbox"/> CLASIFICADA	<input type="checkbox"/> RESERVADA

- **Respaldo automático:** Sistema de copias de seguridad programadas con políticas de retención configurables, permitiendo la recuperación ante cualquier incidente.
- **Monitoreo continuo:** Supervisión permanente del estado de los servicios, rendimiento y capacidad, con alertas automáticas ante cualquier anomalía.
- **Escalabilidad:** Capacidad para aumentar o reducir recursos (procesamiento, memoria, almacenamiento) según las necesidades operativas sin interrumpir el servicio.

3.2 Sistema de seguridad y control de acceso

La a protección de la información sensible del Banco de Items se habilita mediante:


- **Control de acceso basado en roles:** Asignación granular de permisos según el rol y responsabilidades de cada usuario dentro del proceso del Banco de Items.
- **VPN dedicada:** Conexión privada y cifrada que permite que solo los usuarios autorizados desde ubicaciones aprobadas puedan acceder al entorno.
- **Cifrado de datos:** Protección de la información tanto en tránsito como en reposo, permitiendo la confidencialidad en todo momento.
- **Aislamiento de sesiones:** Separación lógica entre sesiones de usuarios para evitar interferencias o accesos no autorizados entre entornos de trabajo.
- **Registro detallado de actividades:** Logs completos de todas las acciones realizadas en el sistema, facilitando auditorías y análisis de seguridad.

3.3 Entornos de trabajo virtuales personalizados

Los usuarios del Banco de Items contarán con espacios de trabajo que incluyen:

- **Entornos personalizados según rol:** Configuración específica según el tipo de usuario (diagramadores, gestores, correctores), con las herramientas y permisos adecuados para cada función.
- **Suite completa de Adobe:** Integración de las herramientas necesarias para la diagramación en los entornos virtuales.
- **Acceso a Prisma:** Conexión segura a la plataforma Prisma para la gestión de ítems, manteniendo los flujos de trabajo actuales.
- **Rendimiento optimizado:** Recursos de procesamiento adecuados para permitir una experiencia fluida incluso en tareas exigentes de diseño gráfico.
- **Persistencia de datos:** Almacenamiento persistente de archivos y configuraciones de usuario, permitiendo continuidad en el trabajo entre sesiones.

3.4 Sistemas de almacenamiento seguro

 Icfes	ESTUDIO PREVIO – TIENDA VIRTUAL DEL ESTADO COLOMBIANO		Código: GAB -FT055
	GESTIÓN DE ABASTECIMIENTO		Versión: 003
Clasificación de la información	<input type="checkbox"/> PÚBLICA	<input type="checkbox"/> CLASIFICADA	<input type="checkbox"/> RESERVADA

La gestión de la información del Banco de Items se realiza mediante:

- **Repositorio centralizado:** Almacenamiento estructurado y organizado de todos los archivos relacionados con el Banco de Items.
- **Gestión de permisos granular:** Control detallado sobre quién puede ver, editar o eliminar cada tipo de documento.

3.5 Integración con sistemas existentes


La solución permite la continuidad operativa mediante:

- **Conectores con Prisma:** Integración transparente con la plataforma actual de gestión de ítems, permitiendo el flujo bidireccional de información.
- **Integración con directorio LDAP:** Conexión con el directorio LDAP existente del ICFES a través de AWS SSO.
- **Mantenimiento del sistema de archivos:** Preservación de la estructura de carpetas y permisos con la que los usuarios están familiarizados.
- **Flujos de trabajo inalterados:** Conservación de los procesos actuales de diagramación, revisión y armado de pruebas.
- **Interfaces consistentes:** Experiencia de usuario similar a la actual, minimizando la curva de aprendizaje.

La combinación de estas características proporciona una solución integral que no solo resuelve las limitaciones actuales de infraestructura, sino que también mejora significativamente la seguridad, disponibilidad y eficiencia operativa del Banco de Items, permitiendo la continuidad de este proceso crítico para el Icfes a través de entornos virtuales seguros basados en la plataforma Houndoc.

4. Arquitectura de referencia

La arquitectura propuesta para la habilitación de entornos de trabajo virtuales seguros para el Banco de Items se ha diseñado utilizando la plataforma Houndoc como base, integrada con servicios específicos de AWS para habilitar los requisitos de seguridad, disponibilidad y rendimiento necesarios para este componente crítico del Icfes.

 Icfes	ESTUDIO PREVIO – TIENDA VIRTUAL DEL ESTADO COLOMBIANO		Código: GAB -FT055
	GESTIÓN DE ABASTECIMIENTO		Versión: 003
Clasificación de la información	<input type="checkbox"/> PÚBLICA	<input type="checkbox"/> CLASIFICADA	<input type="checkbox"/> RESERVADA

A continuación, se presenta la estructura de capas y componentes que conforman la solución:

4.1 Capa de acceso y conectividad

Esta capa establece los mecanismos de conexión segura a los entornos virtuales:

- **AWS VPN:** Servicio que establece túneles cifrados entre la red del Icfes y la infraestructura de Houndoc en AWS, permitiendo que las comunicaciones permanezcan privadas y protegidas.
- **AWS IAM (Identity and Access Management):** Sistema centralizado para la gestión de identidades y permisos de los usuarios, aplicando políticas de seguridad consistentes en toda la infraestructura.
- **AWS SSO (Single Sign-On):** Servicio que proporciona autenticación centralizada para el acceso a los recursos de AWS y Houndoc, con integración al directorio LDAP existente del Icfes.

4.2 Capa de ingestión y preparación de datos

Esta capa facilita la integración de datos y sistemas necesarios para el funcionamiento de los entornos virtuales:

- **AWS DataSync:** Servicio para la transferencia segura y eficiente de datos desde los sistemas actuales del Icfes hacia el almacenamiento en Houndoc, optimizando la disponibilidad de información en los entornos virtuales.


4.3 Capa de almacenamiento y procesamiento

Esta capa gestiona el almacenamiento de datos y la capacidad de procesamiento:

- **Amazon EC2:** Instancias que proporcionan capacidad de cómputo para los servicios de backend de Houndoc, permitiendo el rendimiento y la disponibilidad del sistema.
- **Amazon S3:** Servicio escalable para el almacenamiento de los datos del Banco de Items, con capacidad inicial de 5TB y posibilidad de crecimiento automático.
- **AWS Backup:** Servicio dedicado a la creación, gestión y almacenamiento de copias de seguridad, con políticas de retención configurables según los requisitos del Icfes.

4.4 Capa de entornos de trabajo virtuales

Esta capa proporciona los espacios de trabajo para los usuarios:

 Icfes	ESTUDIO PREVIO – TIENDA VIRTUAL DEL ESTADO COLOMBIANO		Código: GAB -FT055
	GESTIÓN DE ABASTECIMIENTO		Versión: 003
Clasificación de la información	<input type="checkbox"/> PÚBLICA	<input type="checkbox"/> CLASIFICADA	<input type="checkbox"/> RESERVADA

- **AWS WorkSpaces:** Servicio de escritorios virtuales en la nube que proporciona entornos de trabajo personalizados para los diferentes tipos de usuarios (diagramadores, gestores, correctores), con acceso a las aplicaciones necesarias como la suite de Adobe.

4.5 Capa de seguridad transversal

Los componentes de seguridad se implementan de manera transversal en toda la arquitectura:

- **AWS GuardDuty:** Servicio de detección de amenazas que monitorea continuamente la actividad maliciosa y el comportamiento anómalo en la infraestructura.
- **AWS Secrets Manager:** Servicio para el almacenamiento seguro y la gestión de credenciales, certificados y otros secretos necesarios para la operación.
- **AWS Security Hub:** Servicio centralizado para la gestión de la seguridad y el cumplimiento, proporcionando una visión integral del estado de seguridad de la infraestructura.
- **AWS KMS (Key Management Service):** Servicio para la gestión de claves de cifrado, protegiendo la información tanto en tránsito como en reposo.

4.6 Capa de monitoreo


Esta capa proporciona visibilidad sobre el estado y rendimiento de la infraestructura:

- **AWS CloudWatch:** Servicio de monitoreo que supervisa el rendimiento, disponibilidad y estado de salud de todos los componentes, generando alertas ante anomalías.
- **AWS CloudTrail:** Servicio que registra y almacena todas las actividades realizadas en la cuenta de AWS, facilitando la auditoría y el análisis forense.
- **AWS Config:** Servicio para evaluar, auditar y verificar las configuraciones de los recursos de AWS, permitiendo el cumplimiento de políticas y mejores prácticas.

4.7 Integraciones con sistemas existentes

La arquitectura incluye integraciones clave con sistemas existentes del Icfes:

- **Integración con Prisma:** Conexión directa desde la plataforma Houndoc a la plataforma Prisma, permitiendo el flujo de trabajo continuo para la gestión de ítems, construcción y revisión de preguntas.

 Icfes	ESTUDIO PREVIO – TIENDA VIRTUAL DEL ESTADO COLOMBIANO		Código: GAB -FT055
	GESTIÓN DE ABASTECIMIENTO		Versión: 003
Clasificación de la información	<input type="checkbox"/> PÚBLICA	<input type="checkbox"/> CLASIFICADA	<input type="checkbox"/> RESERVADA

- **Integración con LDAP:** Conexión con el directorio LDAP existente del Icfes para autenticación centralizada mediante AWS SSO, permitiendo mantener las políticas de gestión de identidades actuales.

4.8 Flujos de trabajo principales


1. **Flujo de autenticación:**
 - a. Los usuarios se autentican a través de AWS SSO, que valida sus credenciales contra el directorio LDAP existente
 - b. AWS IAM aplica los permisos correspondientes según el rol del usuario
 - c. Se establece una conexión segura mediante AWS VPN
2. **Flujo de acceso a entornos virtuales:**
 - a. Los usuarios acceden a sus escritorios virtuales (AWS WorkSpaces) a través de conexiones VPN seguras
 - b. Los escritorios virtuales tienen acceso a las aplicaciones necesarias (suite de Adobe) y a los datos almacenados en S3
 - c. Las integraciones con Prisma permiten el flujo de trabajo continuo para la gestión de ítems
3. **Flujo de trabajo colaborativo:**
 - a. Los usuarios trabajan en sus entornos virtuales con acceso a todas las herramientas necesarias
 - b. Los datos se almacenan de forma segura en S3 con respaldos automáticos mediante AWS Backup
 - c. AWS CloudTrail registra todas las actividades para auditoría y seguimiento
 - d. AWS GuardDuty monitorea continuamente la seguridad del entorno

Esta arquitectura proporciona una base sólida para la implementación de entornos de trabajo virtuales seguros basados en Houndoc e integrados con servicios AWS, permitiendo que todos los requisitos técnicos y de seguridad sean adecuadamente atendidos, mientras se mantiene la integración con los sistemas existentes del Icfes y se permite la flexibilidad necesaria para adaptarse a necesidades futuras.

Adicionalmente, esta contratación se encuentra prevista en el Plan Anual de Adquisiciones para la vigencia 2025, así:

No. Línea	Área	Rubro	Producto	Valor
593	Subdirección de Información	825320202008003011	211110013	\$ 632.068.660

3. OBJETO A CONTRATAR

 Icfes	ESTUDIO PREVIO – TIENDA VIRTUAL DEL ESTADO COLOMBIANO		Código: GAB -FT055
	GESTIÓN DE ABASTECIMIENTO		Versión: 003
Clasificación de la información	<input type="checkbox"/> PÚBLICA	<input type="checkbox"/> CLASIFICADA	<input type="checkbox"/> RESERVADA

Contratar una solución SaaS para el Icfes enfoca en la habilitación de entornos de trabajo virtuales seguros para el Banco de Items, utilizando Houndoc como plataforma SaaS.

4. ALCANCE

Lo descrito en el anexo técnico, el cual hace parte integral del presente proceso.

5. ESPECIFICACIONES DE ORDEN TÉCNICO

Las descritas en el anexo técnico el cual hace parte integral del proceso.


6. MODALIDAD DE SELECCIÓN DEL CONTRATISTA Y FUNDAMENTOS JURÍDICOS

La modalidad de selección por medio de la cual se elegirá al contratista se regula en lo dispuesto en el artículo 18 del Acuerdo N° 000003 de 2023, Manual de Contratación del Instituto, el cual señala: *“El Ices deberá hacer uso de los Acuerdos Marco de Precios suscritos por Colombia Compra Eficiente o la entidad que haga sus veces, como instrumento de agregación de demanda y de coordinación de decisiones en la adquisición de bienes y/o servicios de características técnicas uniformes, con el fin de producir economías de escala e incrementar el poder de negociación de la entidad. Para tal fin, la entidad se vinculará a la Tienda Virtual del Estado Colombiano, identificará la necesidad que pretende satisfacer y aplicará a sus procesos de contratación los Catálogos de los Acuerdos Marco de Precios diseñados por Colombia Compra Eficiente o la entidad que haga sus veces.”*

En consecuencia, el Icfes realizará la adquisición de una solución de software como servicio (SaaS) para el Instituto Colombiano para la Evaluación de la Educación (ICFES) que garantice la habilitación de entornos de trabajo virtuales seguros para el Banco de Items, a través del Instrumento de Agregación De Demanda CCE-SNG-IAD-002-2024, Sistema Dinámico De Adquisición (Iad/Sda) De Software por Catálogo II, suscrito por la Agencia Nacional de Contratación - Colombia Compra Eficiente, el cual se encuentra vigente hasta el 21 de noviembre del año 2027, para lo cual se constato la disponibilidad de las especificaciones técnicas requeridas por la entidad dentro del respectivo catalogo

Este mecanismo de adquisición permite a las entidades estatales contratar soluciones tecnológicas que garantizan idoneidad técnica, jurídica y financiera de los proveedores, simplificando los procesos de contratación y asegurando la eficiencia en la gestión de recursos públicos.

El fundamento jurídico que soporta la adopción de esta modalidad se encuentra en las siguientes disposiciones:

 Icfes	ESTUDIO PREVIO – TIENDA VIRTUAL DEL ESTADO COLOMBIANO		Código: GAB -FT055
	GESTIÓN DE ABASTECIMIENTO		Versión: 003
Clasificación de la información	<input type="checkbox"/> PÚBLICA	<input type="checkbox"/> CLASIFICADA	<input type="checkbox"/> RESERVADA

- Artículo 18 del Manual de Contratación de Colombia Compra Eficiente, el cual define los criterios bajo los cuales se pueden utilizar los instrumentos de agregación de demanda.

El uso del IAD/SDA para la adquisición de la solución tecnológica responde a los principios de economía, transparencia y eficiencia en la contratación pública, asegurando que el proceso de selección del contratista se realice bajo condiciones competitivas, objetivas y alineadas con las necesidades del ICFES. Además, este mecanismo permite la contratación de soluciones ya probadas en el mercado, optimizando tiempos de implementación y garantizando la compatibilidad con la infraestructura tecnológica de la entidad.

7. PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será hasta el treinta y uno (31) de diciembre de 2025, plazo que se empezará a contar a partir de la suscripción del acta de inicio, previo cumplimiento de los requisitos de ejecución, a saber: Expedición del Registro Presupuestal y Aprobación de la Garantía.

8. DEFINICIÓN DE LAS GARANTÍAS


De conformidad con el numeral 15.2 de la minuta del Instrumento de Agregación De Demanda, Sistema Dinámico De Adquisición (Iad/Sda) De Software Por Catálogo II, Los Proveedores deben constituir una garantía de cumplimiento dentro de los tres (3) días hábiles siguientes a la colocación de la Orden de Compra a favor de la Entidad Compradora, por el valor, amparos y vigencia establecidos en la siguiente tabla:

El proveedor adjudicatario deberá constituir la Garantía que exija el acuerdo marco de precios, con formato para entidades públicas con régimen privado de contratación, expedida por una compañía de seguros autorizada para funcionar en Colombia o una garantía bancaria que ampare los riesgos y vigencias en los siguientes términos:

AMPARO	SUFICIENCIA	VIGENCIA
Cumplimiento del contrato	10 % de la Orden de Compra	Duración de la Orden de Compra y seis (6) meses más.
Calidad y correcto funcionamiento de los bienes	10 % de la Orden de Compra	Duración de la Orden de Compra y seis (6) meses más.
Calidad del servicio	10 % de la Orden de Compra	Duración de la Orden de Compra y seis (6) meses más.
Pago de salarios, prestaciones sociales legales e indemnizaciones laborales	5% del Valor de la Orden de Compra	Duración de la Orden de Compra y (3) tres años más

9. EL ANÁLISIS DEL RIESGO Y LA FORMA DE MITIGARLO

Se anexa Matriz de Riesgo de Agregación de Demanda, Sistema Dinámico de Adquisición (IAD/SDA) de Software por Catálogo II, dispuesto por la Agencia Nacional para la Contratación Pública Colombia Compra Eficiente.

 Icfes	ESTUDIO PREVIO – TIENDA VIRTUAL DEL ESTADO COLOMBIANO		Código: GAB -FT055
	GESTIÓN DE ABASTECIMIENTO		Versión: 003
Clasificación de la información	<input type="checkbox"/> PÚBLICA	<input type="checkbox"/> CLASIFICADA	<input type="checkbox"/> RESERVADA

10. ESTUDIO DE MERCADO Y ANÁLISIS DEL SECTOR


Dentro del proceso de estudio de mercado, el ICFES ha considerado los análisis realizados por la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente, en el marco del Instrumento de Agregación de Demanda, Sistema Dinámico de Adquisición (IAD/SDA) de Software por Catálogo II.

En este sentido, se realizó el evento RFI No. 200815, el cual nos arroja que los proveedores INDRA COLOMBIA S.A.S, INDRA COLOMBIA S.A.S, SERVIFORMACION, NUEVA ERA SOLUCIONES S.A.S, REDNEET y XERTICA COLOMBIA SAS no cuenta con el software requerido, los proveedores UNION TEMPORAL BGH y CONVIEST SAS no allegaron respuesta y el proveedor HIGH TECH SOFTWARE S.A.S, allegó propuesta indicando que son los propietarios del servicio, empero no fue allegado certificado que acredite lo anterior, es por ello, que, mediante correo electrónico se le solicito al proveedor allegar certificado de propiedad intelectual, con ello se identificó que el software Houndoc, propiedad de la Empresa HIGH TECH SOFTWARE S.A.S tal y como se evidencia en el certificado N° 13-89-396 expedido por la Dirección Nacional de Derechos de Autor cumple a cabalidad con la necesidad técnica de la entidad, cumpliendo con las características técnicas exigidas para la solución integral de habilitación de entornos de trabajo virtuales seguros para el Banco de ITEMS, garantizando la eficiencia en el análisis de datos y la toma de decisiones estratégicas. Por lo anterior, se recomienda proceder con la contratación de HIGH TECH SOFTWARE S.A.S. mediante el mecanismo establecido en el IAD/SDA.

Finalmente, se encuentra necesario señalar que lo antes señalado se encuentra en concordancia con lo dispuesto en el catalogo del IAD, el que señala que los servicios a contratar cuentan con proveeduría exclusiva.

11. PRESUPUESTO

El presupuesto oficial de la entidad será de SEISCIENTOS TREINTA Y DOS MILLONES SESENTA Y OCHO MIL SEISCIENTOS SESENTA PESOS (\$632.068.660), empero de acuerdo con el simulador del IAD disponible en la tienda virtual del Estado Colombiano de la Agencia Nacional de Contratación – Colombia Compra Eficiente o lo estipulado en el acuerdo marco de precios, el presupuesto estimado es la suma de SEISCIENTOS TREINTA Y SEIS MILLONES CIENTO CUARENTA Y DOS MIL CUATROCIENTOS TRES PESOS (\$636.142.403) Incluido IVA, y todos los costos directos e indirectos a que haya lugar conforme a la naturaleza del contrato, lo anterior, debido a que al momento de

 Icfes	ESTUDIO PREVIO – TIENDA VIRTUAL DEL ESTADO COLOMBIANO		Código: GAB -FT055
	GESTIÓN DE ABASTECIMIENTO		Versión: 003
Clasificación de la información	<input type="checkbox"/> PÚBLICA	<input type="checkbox"/> CLASIFICADA	<input type="checkbox"/> RESERVADA

generar el resumen de cotización el servicio lo genera con IVA, es pertinente aclarar, que, durante este trámite, se evidenció que al generar el resumen de cotización, el sistema aplica automáticamente el Impuesto sobre las Ventas (IVA) a la totalidad de los productos y servicios cotizados. No obstante, esta aplicación resulta jurídicamente improcedente respecto de los bienes y servicios cuya naturaleza está exenta del impuesto, conforme a lo establecido en el artículo 476 del Estatuto Tributario Colombiano, el cual exceptúa del IVA a los servicios de licenciamiento de software prestados bajo la modalidad de Software as a Service (SaaS).

En efecto, tratándose de soluciones tecnológicas ofrecidas bajo licenciamiento en la modalidad SaaS, donde no se transfiere la propiedad del software ni se entrega un bien físico, y que son adquiridas a través de un instrumento contractual centralizado (como lo es el IAD/SDA administrado por Colombia Compra Eficiente), es jurídicamente procedente que dichos productos estén incluidos de la aplicación del IVA.

12. FORMA DE PAGO

El valor de la presente orden se pagará, según lo establecido en la cláusula 11 de la minuta del Instrumento de Agregación De Demanda, Sistema Dinámico de Adquisición (Iad/Sda) De Software Por Catálogo II CCE-SNG-IAD-002-2024.

13. CRITERIOS DE DESEMPATE

Los criterios de desempate serán los establecidos en el Decreto 1860 de 2021 o las normas que lo modifiquen, adicionen y complementen.


14. SITIO DE EJECUCIÓN Y/O SITIO DE ENTREGA

El contrato a celebrar se ejecutará en la ciudad de Bogotá D.C.

15. SUPERVISOR

La supervisión de la ejecución y cumplimiento de las obligaciones contraídas por el contratista a favor de la Entidad estará a cargo del **Subdirector de Información**, o quien designe el ordenador del gasto, el cual deberá cumplir las obligaciones y actividades establecidas en el Manual de Contratación del ICFES.



 Icfes	ESTUDIO PREVIO – TIENDA VIRTUAL DEL ESTADO COLOMBIANO		Código: GAB -FT055
	GESTIÓN DE ABASTECIMIENTO		Versión: 003
Clasificación de la información	<input type="checkbox"/> PÚBLICA	<input type="checkbox"/> CLASIFICADA	<input type="checkbox"/> RESERVADA

DIEGO MAURICIO SALAS
Subdirector de Información

Proyectó: Henedy Johana Taborda – Abogada TI





ANEXO TÉCNICO

Objeto: Contratar una solución SaaS para el Icfes enfoca en la habilitación de entornos de trabajo virtuales seguros para el Banco de Items, utilizando Houndoc como plataforma SaaS

Octubre 2025



1. Requerimiento General

El Instituto Colombiano para la Evaluación de la Educación (ICFES), en su compromiso con la transformación digital y la mejora continua de la calidad educativa, busca optimizar y gestionar de manera eficiente su infraestructura tecnológica mediante la contratación de una solución de virtualización avanzada. Esta solución tiene como objetivo consolidar las capacidades actuales de la infraestructura en la nube, mejorar la eficiencia operativa y garantizar la seguridad de los datos, complementando y potenciando el uso de su Data Lake mediante una adecuada virtualización de la información.

La solución de virtualización propuesta permitirá la implementación de un entorno unificado que cubra las siguientes necesidades:

- **Orquestación de Cargas de Trabajo Críticas y Servicios de Atención Ciudadana:** Implementar una infraestructura virtual segura, escalable y resiliente para garantizar la disponibilidad y continuidad de los servicios esenciales del ICFES; esta solución permitirá la ejecución de servicios de atención al ciudadano, pruebas educativas y la gestión de grandes volúmenes de información. Alineado con la estrategia de Ecosistema Seguro del PETIC, esta solución proporcionará un entorno digital confiable y seguro tanto para los usuarios como para las instituciones.
- **Automatización de Procesos y Gestión de Datos:** Habilitar mecanismos automatizados para la clasificación, curaduría y análisis de grandes volúmenes de información estructurada y no estructurada. La virtualización de estos datos garantizará que la información esté actualizada, organizada y fácilmente accesible, lo que potenciará el Data Lake existente, asegurando que los datos estén correctos y virtualizados, facilitando su posterior análisis y uso para la toma de decisiones. Este enfoque está alineado con la estrategia de Gobierno y Datos del PETIC, que promueve la eficiencia en el uso y gestión de la información.
- **Integración de Flujos de Trabajo Asincrónicos:** Desarrollar flujos de trabajo que permitan automatizar tareas y gestionar procesos de manera eficiente. Este enfoque responde a la estrategia de Prevención del PETIC, implementando medidas proactivas para evitar riesgos y amenazas en los flujos de trabajo críticos. Los flujos de trabajo automatizados aumentarán la productividad, reduciendo el error humano y asegurando el cumplimiento de las normativas de la entidad.



- **Seguridad y Cumplimiento Normativo:** La solución de virtualización implementará controles adecuados de acceso y seguridad para asegurar que la infraestructura cumpla con los estándares de seguridad y normativas vigentes. A través de las mejores prácticas en seguridad, se garantizará la protección de datos sensibles, permitiendo un monitoreo constante de la infraestructura para prevenir riesgos y amenazas, alineándose con la estrategia del Ecosistema Seguro del PETIC.

Esta solución tiene como objetivo mejorar la disponibilidad, la seguridad y la eficiencia de las aplicaciones críticas del ICFES, al tiempo que potencia el Data Lake al proporcionar datos correctamente gestionados y virtualizados, que faciliten su posterior procesamiento y análisis. Con ello, se asegura que el ICFES pueda aprovechar al máximo sus capacidades de almacenamiento, análisis y toma de decisiones basadas en información precisa y accesible, además, contribuirá a mejorar la disponibilidad, la seguridad y la eficiencia de las aplicaciones críticas, en línea con los objetivos estratégicos del PETIC 2024–2027.

A continuación, se describen los servicios necesarios para garantizar una gestión integral, optimización continua y protección de los datos, en un entorno que permita la escalabilidad y adaptabilidad según las necesidades del ICFES.

1.1 Funcionalidades de la solución

La solución de virtualización propuesta deberá integrar y consolidar los entornos tecnológicos del ICFES, proporcionando una infraestructura escalable, de alta disponibilidad y diseñada para soportar de manera continua los sistemas críticos de la entidad. Esta solución se centrará en mejorar la eficiencia operativa, optimizar la administración de los recursos y garantizar la continuidad del servicio institucional, mediante la automatización, el monitoreo y la seguridad avanzada.

- **Plataforma de Infraestructura Tecnológica Eficiente**

La solución deberá integrar una plataforma tecnológica robusta, capaz de gestionar de manera eficiente los sistemas de información críticos del ICFES. La plataforma deberá consolidar la infraestructura existente y permitir la expansión futura según las necesidades operativas, garantizando una alta disponibilidad y redundancia para asegurar la continuidad de los servicios.



- **Optimización Dinámica de Recursos**

La solución deberá integrar mecanismos para el ajuste dinámico de recursos de cómputo y almacenamiento, adaptándose de manera automática a los patrones de uso y garantizando la eficiencia operativa. De esta forma, la solución optimizará el uso de los recursos sin comprometer el rendimiento, mejorando la capacidad de respuesta de la infraestructura ante diferentes demandas operativas.

- **Clasificación y Balanceo Automático de Cargas de Trabajo**

La solución deberá incorporar la funcionalidad de clasificación automatizada de cargas de trabajo según su criticidad, facilitando la distribución y el balanceo dentro del entorno virtualizado. Esto permitirá que los recursos más críticos reciban la prioridad necesaria, mientras que las cargas menos exigentes se gestionen de manera eficiente, optimizando el rendimiento general de la infraestructura.

- **Monitoreo de Comportamientos Anómalos**

La solución deberá contar con capacidades avanzadas de monitoreo, que permitirán la detección temprana de comportamientos anómalos o fallos potenciales en la infraestructura. Mediante algoritmos de inteligencia artificial, la solución será capaz de identificar patrones inusuales y anticipar posibles problemas, lo que permitirá tomar decisiones informadas para prevenir incidencias antes de que afecten la operatividad.

- **Recomendaciones Automáticas para Optimización de Recursos**

La solución deberá integrar algoritmos de inteligencia artificial aplicada, proporcionando recomendaciones automáticas para la configuración de los recursos virtuales, políticas de respaldo y asignación de servicios. Estas recomendaciones estarán basadas en el análisis continuo de los datos operacionales, asegurando que la infraestructura se mantenga optimizada frente a los cambios en las demandas de la entidad.

- **Recuperación Automática ante Incidentes**

La solución deberá incorporar capacidades para la ejecución autónoma de rutinas de recuperación ante fallos, garantizando la continuidad de los servicios incluso en escenarios de incidentes críticos. Esta funcionalidad permitirá que la infraestructura recupere su operatividad en el menor tiempo posible, minimizando las interrupciones y protegiendo la integridad de los servicios esenciales.

- **Monitoreo Integral de Recursos y Rendimiento**



La solución deberá integrar un sistema de monitoreo integral que permita supervisar de manera continua y eficiente las métricas críticas de los servicios virtualizados. Esto incluirá el monitoreo del uso de recursos de procesamiento, la transferencia de datos, el rendimiento de la memoria, los discos de almacenamiento y las métricas generales del sistema. Los resultados deberán estar disponibles y podrán ser consultados en cualquier momento para asegurar el rendimiento óptimo de la infraestructura.

- **Seguridad Avanzada y Protección de Datos**

La solución deberá integrar mecanismos avanzados de seguridad para proteger los datos y aplicaciones virtualizados; esto incluirá el cifrado de datos, la gestión de accesos mediante controles basados en roles, y la implementación de políticas adaptativas para la defensa ante amenazas cibernéticas. Además, se deberán establecer políticas de respaldo automáticas para asegurar la integridad y disponibilidad de los datos.

- **Escalabilidad y Preparación para Integraciones futuras**

La arquitectura de la solución deberá ser escalable, permitiendo el crecimiento de la infraestructura conforme aumenten las necesidades operativas del ICFES. Además, deberá ser capaz de integrarse fácilmente con futuros servicios de analítica avanzada o automatización de procesos, garantizando que la infraestructura continúe siendo eficiente y capaz de adaptarse a nuevas demandas tecnológicas.

- **Alta Disponibilidad y Redundancia**

La solución deberá garantizar alta disponibilidad en todos los componentes clave de la infraestructura, mediante la implementación de mecanismos de redundancia que aseguren la continuidad operativa incluso en caso de fallos en la infraestructura. Esto permitirá que los servicios críticos del ICFES continúen operando sin interrupciones, brindando un nivel de servicio constante.

- **Capacidad para Soportar Crecimiento en la Demanda Transaccional**

La solución deberá ser capaz de soportar el crecimiento en la demanda transaccional de la entidad, adaptándose a un mayor volumen de usuarios y transacciones sin comprometer la calidad del servicio ni el rendimiento de la infraestructura. Esto garantizará que la infraestructura esté preparada para el futuro.

- **Herramientas de Monitoreo y Administración en Tiempo Real**



La solución deberá integrar herramientas de monitoreo y administración en tiempo casi real, permitiendo a los administradores optimizar el rendimiento de la infraestructura y detectar posibles incidencias de manera proactiva. Estas herramientas ayudarán a realizar ajustes inmediatos para maximizar la eficiencia operativa y garantizar la estabilidad del sistema.

2. Gestión de Infraestructura en la Nube

El servicio de gestión de infraestructura en la nube deberá asegurar una operación eficiente de las aplicaciones misionales del ICFES. Este servicio deberá garantizar que los recursos en la nube estén alineados con los objetivos operativos del ICFES, asegurando la disponibilidad de las aplicaciones críticas y la capacidad para manejar el creciente volumen de trabajo.

2.1 Evaluación y Validación de la Infraestructura

El servicio de evaluación de infraestructura deberá incluir una validación completa de la infraestructura existente en la nube, revisando la arquitectura y la alineación con los estándares de seguridad y conformidad. Esto deberá incluir una evaluación del nivel de madurez de la seguridad mediante el modelo de madurez en seguridad, así como una revisión arquitectónica utilizando el Well-Architected Review Process para asegurar la adecuación de los recursos a las necesidades del ICFES.

2.2 Optimización de la Infraestructura

El servicio de optimización de la infraestructura deberá ajustar los recursos de la nube para maximizar la eficiencia operativa. Este servicio deberá estar enfocado en la optimización de costos, asegurando que la infraestructura sea capaz de manejar tanto los picos de demanda como los períodos de baja actividad, ajustando los recursos de manera adecuada a las necesidades del ICFES.

2.3 Gestión Continua de la Infraestructura

El servicio de gestión continua de infraestructura deberá proporcionar monitoreo y control regular de los recursos, implementando medidas de seguridad para proteger los datos y asegurar la disponibilidad de los servicios. Este servicio también deberá incluir la entrega de informes mensuales sobre el consumo de recursos, costos, recomendaciones de optimización y el estado general de la infraestructura.



3. Alcance

El alcance de este proyecto se enfoca en dos frentes principales: la implementación de una solución de virtualización eficiente para la infraestructura tecnológica del ICFES y la optimización de las cargas de trabajo dentro de este entorno virtual. El objetivo es asegurar que la infraestructura del ICFES sea escalable, eficiente, segura y capaz de manejar las demandas operativas de manera rentable. Para lograr estos objetivos, se deberán implementar los siguientes procesos de servicios gestionados dentro de la solución de virtualización, alineados con las necesidades operativas del ICFES.

3.1 Gestión Eficiente de la Infraestructura Virtualizada

El objetivo principal de este componente es la gestión integral de la infraestructura virtualizada, garantizando una operación continua, eficiente y segura de los recursos tecnológicos del ICFES.

3.1.1 Validación de la Infraestructura Existente

Antes de comenzar con la gestión activa de la infraestructura virtualizada, se realizará una validación de la infraestructura actual para asegurarse de que los recursos sean adecuados para las necesidades del ICFES y estén alineados con los objetivos operativos. Este proceso incluirá:

- **Revisión de la Arquitectura Actual:** Evaluación de la infraestructura actual para garantizar que sea compatible con las mejores prácticas de virtualización y que pueda satisfacer las demandas operativas de manera eficiente.
- **Modelo de Madurez en Seguridad:** Aplicación de un modelo de madurez en seguridad para evaluar los niveles de protección de la infraestructura virtualizada y garantizar que los datos estén debidamente protegidos, con controles adecuados para el acceso autorizado.

3.1.2 Gestión Activa de la Infraestructura Virtualizada

Una vez validada la infraestructura, se procederá con la gestión activa de la infraestructura virtualizada. Esto incluye la optimización de los recursos, la mejora continua de la disponibilidad, la seguridad de los servicios y la gestión proactiva de los incidentes y cambios. Las actividades principales incluyen:

- **Evaluación y Control de Costos:** Gestión de los costos asociados con la infraestructura virtualizada, garantizando el uso eficiente de los recursos y la optimización del gasto operativo.
- **Gestión de la Calidad del Servicio:** Asegurar que los servicios virtualizados cumplan con los Acuerdos de Nivel de Servicio (ANS)



establecidos, manteniendo la disponibilidad, el rendimiento y la seguridad adecuados.

- **Optimización de Disponibilidad y Seguridad:** Asegurar que los servicios virtualizados sean robustos, confiables y seguros mediante la implementación de mecanismos avanzados de protección y monitoreo continuo.
- **Planificación y Control de Cambios:** Implementación de un proceso estructurado de gestión de cambios para mantener la estabilidad de la infraestructura mientras se realizan ajustes y mejoras necesarias.
- **Gestión de Incidentes y Accesos:** Control de incidentes y gestión de accesos, asegurando que las políticas de seguridad se mantengan de forma continua y se resuelvan rápidamente cualquier anomalía que pueda surgir.

3.2. Optimización de Cargas de Trabajo en el Entorno Virtualizado

Este componente se enfoca en la optimización de las cargas de trabajo dentro del entorno virtualizado, asegurando que la infraestructura se ajuste a las necesidades operativas del ICFES de manera eficiente y rentable. La optimización de cargas de trabajo se realizará inicialmente, con la posibilidad de ajustes periódicos según las necesidades cambiantes.

3.2.1 Análisis de Cargas y Ajuste de Recursos Virtuales

Se realizará un análisis detallado de las cargas de trabajo actuales del ICFES, con el objetivo de ajustar los recursos de virtualización (procesamiento, almacenamiento y redes) para garantizar una operación eficiente y rentable. Este análisis permitirá definir la capacidad adecuada para cada tipo de carga, asegurando que la infraestructura sea capaz de soportar tanto los picos de demanda como los períodos de baja actividad.

3.2.2 Escalabilidad Automática

La solución de virtualización permitirá la configuración de escalabilidad automática, ajustando dinámicamente los recursos virtuales según las fluctuaciones de la demanda. Esto garantizará que los recursos sean utilizados de manera eficiente, reduciendo los costos operativos durante los períodos de baja demanda y escalando automáticamente durante los picos de actividad.

4. Detalle del alcance

Este proyecto deberá llevarse a cabo mediante una serie de actividades clave que se realizarán de acuerdo con los procesos establecidos. Cada actividad generará información relevante que deberá ser consolidada en un único



entregable mensual denominado Informe de Gestión de Servicios. Este informe incluirá secciones detalladas que cubrirán cada una de las actividades y los reportes obtenidos durante el mes.

4.1. Validación de la Infraestructura Existente

Antes de proceder con la gestión continua de la infraestructura y la optimización de cargas, se deberá llevar a cabo una validación de la infraestructura existente para verificar que los recursos en la nube estén alineados con los objetivos operativos del ICFES. Este proceso deberá incluir:

- **Revisión de la Arquitectura Actual:** Evaluar la alineación de la infraestructura con las mejores prácticas de diseño y la capacidad de la infraestructura para satisfacer las demandas del ICFES.
- **Modelo de Madurez en Seguridad:** Evaluar el nivel de madurez en términos de seguridad y conformidad, revisando que la infraestructura proteja adecuadamente los datos y permita el acceso autorizado. Este modelo ayudará a identificar áreas de mejora en la seguridad.

Para cada una de estas partes del proceso se deberá generar un entregable respectivamente, donde se analizarán la arquitectura actual, se darán recomendaciones de mejora y se indicarán las áreas que requieren optimización.

4.2. Gestión y Optimización de Costos

Se deberá evaluar y controlar los costos de los servicios administrados en la infraestructura, verificando que los recursos sean utilizados de manera eficiente y se identifiquen oportunidades de ahorro.

En el Informe de Gestión de Servicios, deberá incluir un desglose detallado de los consumos mensuales, el análisis de los costos operativos y las recomendaciones para optimizar el gasto.

4.3. Gestión de Niveles de Servicio

Se deberá monitorear la calidad del servicio prestado y revisar que se cumplan los Acuerdos de Nivel de Servicio (ANS).

El Informe de Gestión de Servicios, deberá incluir un reporte detallado sobre el cumplimiento de los ANS y las acciones correctivas tomadas para revisar que los servicios cumplan con los objetivos establecidos.

4.4. Gestión de la Disponibilidad

Se deberá verificar que los servicios estén siempre disponibles y operativos, minimizando cualquier tiempo de inactividad y revisando la confiabilidad de la infraestructura.



El Informe de Gestión de Servicios, deberá proporcionar un reporte detallado sobre la disponibilidad de los servicios, el tiempo de inactividad y las medidas correctivas implementadas.

4.5. Gestión de la Seguridad de la Información

Se deberá implementar y monitorear medidas de seguridad para proteger los datos y los recursos en la nube, verificando su confidencialidad, integridad y disponibilidad.

El Informe de Gestión de Servicios, deberá incluir un informe detallado sobre las medidas de seguridad implementadas, los incidentes gestionados y las soluciones aplicadas.

4.6. Gestión de Cambios

Se deberá planificar, evaluar y ejecutar los cambios necesarios en la infraestructura, verificando que estos cambios se implementen de manera controlada y sin interrumpir los servicios.

El Informe de Gestión de Servicios, deberá incluir los cambios realizados, su impacto en los servicios y las pruebas realizadas para verificar que la calidad del servicio no se vea afectada.

4.7. Validación y Pruebas del Servicio

Se deberá revisar que las nuevas versiones de los servicios e infraestructura cumplan con los requisitos de calidad previamente acordados y que no afecten la operatividad de la infraestructura.

El Informe de Gestión de Servicios, deberá incluir los resultados de las pruebas realizadas para verificar que las nuevas versiones de los servicios cumplen con los estándares de calidad establecidos.

4.8. Gestión de la Configuración y Activos del Servicio

Se deberá controlar los activos de la infraestructura y su configuración, verificando que todos los componentes estén actualizados y correctamente documentados.

El Informe de Gestión de Servicios, deberá incluir un reporte sobre el estado de la infraestructura, los activos gestionados y las actualizaciones realizadas.

4.9. Gestión de Eventos

Se deberá monitorear los eventos en la infraestructura que puedan indicar errores o problemas, gestionándolos de manera proactiva para evitar que afecten el rendimiento de los servicios.



El Informe de Gestión de Servicios, deberá incluir un reporte sobre los eventos gestionados, su clasificación, impacto y las acciones correctivas tomadas.

4.10. Gestión de Incidentes

Se deberá resolver de manera eficiente cualquier interrupción en el servicio, restaurando la operatividad lo antes posible y permitiendo el cumplimiento de los ANS.

El Informe de Gestión de Servicios, deberá incluir un resumen de los incidentes gestionados, el tiempo de resolución y las acciones correctivas tomadas.

4.11. Gestión de Requerimientos

Se deberá atender las solicitudes de los usuarios, verificando que se les proporcione acceso eficiente a los servicios conforme a las políticas establecidas.

El Informe de Gestión de Servicios, deberá incluir un informe sobre las solicitudes gestionadas, su tipo, tiempo de respuesta y cualquier requerimiento especial atendido.

4.12. Gestión de Accesos

Se deberá controlar el acceso a los recursos en la nube, verificando que solo los usuarios autorizados tengan acceso a los servicios y recursos según las políticas de seguridad.

El Informe de Gestión de Servicios, deberá incluir un reporte detallado sobre la gestión de accesos, el control de permisos y las incidencias relacionadas con accesos no autorizados.

4.13. Gestión de Problemas

Se deberá identificar las causas subyacentes de problemas recurrentes en la infraestructura, aplicando soluciones a largo plazo para evitar su repetición.

El Informe de Gestión de Servicios, deberá incluir un análisis de los problemas recurrentes, las soluciones implementadas y las medidas preventivas tomadas.

4.14. Optimización de Cargas

Se deberá llevar a cabo una optimización de cargas al inicio del proyecto una única vez para revisar que las cargas de trabajo estén distribuidas de manera eficiente en la infraestructura. Esto incluirá la identificación de cargas infrautilizadas o desbalanceadas y la optimización para mejorar el rendimiento y reducir los costos operativos.



Se entregará un único informe de Optimización de Cargas, que incluirá el análisis de las cargas optimizadas, el impacto de la optimización en el rendimiento y las recomendaciones para mantener la eficiencia.

5. Características de la solución

La solución de virtualización propuesta se centrará en la gestión integral de la infraestructura virtualizada del ICFES. Este servicio de gestión abarcará todos los aspectos clave de la administración de los recursos virtuales, asegurando que se logre una operación eficiente, segura, disponible y optimizada en términos de costos. A continuación, se describen las principales características de la solución:

5.1. Escalabilidad y Flexibilidad de la Solución

La solución de virtualización deberá adaptarse a las necesidades operativas del ICFES. Gracias a su capacidad de escalabilidad automática, los recursos virtualizados deberán ajustarse dinámicamente según la demanda. Esto garantizará que los servicios puedan manejar picos de tráfico sin comprometer el rendimiento, mientras se optimizan los costos asociados. Además, la optimización de cargas se llevará a cabo al inicio del proyecto para ajustar la infraestructura a las necesidades específicas del ICFES, asegurando el uso eficiente de los recursos desde el comienzo.

5.2. Seguridad Robusta en la Infraestructura Virtual

La solución de virtualización deberá incluir un conjunto robusto de medidas de seguridad para proteger los recursos virtualizados. Estas incluirán cifrado de datos, protección contra ataques de denegación de servicio (DDoS) y control de acceso mediante políticas estrictas de autenticación y autorización. La seguridad será un aspecto primordial de la solución, asegurando la confidencialidad, integridad y disponibilidad de los datos en todo momento. Asimismo, se llevará a cabo una evaluación inicial de la madurez en seguridad para ajustar las configuraciones de seguridad de la solución según las mejores prácticas.

5.3. Alta Disponibilidad y Resiliencia de la Solución Virtualizada

La solución de virtualización garantizará que los servicios estén siempre disponibles, incluso en situaciones imprevistas. Esto se logrará mediante el aprovechamiento de la alta disponibilidad y resiliencia de la infraestructura virtualizada, utilizando mecanismos de redundancia para asegurar la continuidad del servicio en caso de fallos en componentes clave. La solución se diseñará para garantizar que los servicios continúen operativos sin interrupciones, incluso durante incidentes imprevistos.

5.4. Optimización de Costos mediante Virtualización



La solución de virtualización pondrá un énfasis particular en la optimización de costos. Esto incluirá la asignación adecuada de instancias virtuales, almacenamiento virtual y redes virtualizadas, con el objetivo de garantizar el uso eficiente de los recursos y evitar el sobreaprovisionamiento. Se implementarán políticas de escalado automático, que permitirán ajustar los recursos según la demanda, reduciendo los costos operativos sin sacrificar el rendimiento. Además, se utilizarán herramientas de monitoreo de costos para gestionar los recursos de manera eficiente y asegurarse de que se mantengan alineados con las necesidades operativas del ICFES.

5.5. Monitoreo y Gestión Proactiva de la Solución

La solución de virtualización deberá ser monitoreada de manera continua, con alertas configuradas para detectar problemas potenciales antes de que afecten el rendimiento. Se implementarán prácticas de monitoreo proactivo, que permitirán identificar y resolver incidentes antes de que se conviertan en problemas significativos, asegurando una operación fluida y sin interrupciones. Las métricas clave serán monitoreadas en tiempo real para garantizar el rendimiento óptimo de los recursos virtuales.

5.6. Automatización y Gestión de Cambios en la Solución

La solución de virtualización incluirá la automatización de tareas repetitivas, reduciendo el riesgo de error humano y mejorando la eficiencia operativa. Además, los cambios en la infraestructura virtualizada se gestionarán de manera controlada y documentada, permitiendo actualizaciones y ajustes sin interrumpir la continuidad del servicio. Se utilizarán herramientas de automatización para gestionar los cambios en los recursos virtualizados, mejorando así la infraestructura de manera ágil y continua.

5.7. Gestión Integral de la Infraestructura Virtualizada

La solución de virtualización proporcionará una administración integral de todos los componentes virtualizados, incluyendo la provisión, configuración, monitoreo y mantenimiento de los recursos virtuales. Este enfoque garantizará que todos los componentes estén alineados y funcionando de manera óptima en todo momento. Se llevará a cabo una validación inicial para verificar que la infraestructura virtualizada cumpla con las mejores prácticas de arquitectura.

5.8. Conformidad y Cumplimiento de Normativas

La solución de virtualización deberá alinearse con las normativas y estándares de seguridad aplicables, asegurando que los requisitos regulatorios del ICFES sean cumplidos en todo momento. La infraestructura virtualizada deberá ser diseñada e implementada siguiendo las mejores prácticas para la protección



de datos y la privacidad. Se realizará una revisión de conformidad al inicio del proyecto para asegurar que la solución cumpla con las normativas pertinentes y las políticas internas de seguridad.

5.9. Soporte y Mantenimiento Continuo de la Solución

Un equipo especializado ofrecerá soporte continuo para la solución de virtualización, gestionando y resolviendo cualquier incidencia de manera rápida y eficiente. Se brindará mantenimiento preventivo para revisar el buen funcionamiento de los recursos virtualizados, con revisiones periódicas para garantizar que la infraestructura continúe cumpliendo con los requisitos operativos y de seguridad del ICFES.

Esta solución de virtualización proporcionará al ICFES una infraestructura escalable, segura, eficiente y rentable, adaptada a sus necesidades operativas actuales y futuras. Al integrar capacidades avanzadas de automatización, monitoreo proactivo y optimización de costos, el ICFES podrá maximizar el uso de sus recursos virtualizados, mejorar la continuidad del servicio y garantizar una administración eficiente de la infraestructura.

6. Arquitectura de la infraestructura actual de la entidad

La infraestructura en la nube del ICFES se compone de una red privada virtual (VPC), que está organizada en varias subredes públicas y privadas. Las subredes públicas albergan los componentes que interactúan con el tráfico externo, mientras que las subredes privadas gestionan los recursos internos, como servicios de procesamiento de datos y almacenamiento.

La conectividad entre la infraestructura en la nube y los sistemas locales del ICFES se realiza mediante una red privada virtual (VPN), que facilita el acceso tanto a usuarios internos como externos. Los usuarios internos se conectan a través de la red privada de la nube, y los usuarios externos acceden mediante servicios de distribución de contenido.

En cuanto a la seguridad, la infraestructura está protegida mediante controles de acceso, cifrado de datos y medidas contra amenazas externas. Además, se lleva a cabo un monitoreo continuo de la infraestructura para verificar que los recursos y servicios estén funcionando adecuadamente.

La infraestructura incluye una estrategia de respaldo y recuperación de datos, y se gestionan las actualizaciones y el mantenimiento de los recursos para asegurar la disponibilidad y el buen funcionamiento de los servicios.



7. Requerimiento de línea de tiempo por parte del Icfes

La gestión de la infraestructura en la nube deberá llevarse a cabo desde noviembre de 2025 hasta julio de 2026, siguiendo una metodología estructurada que incluirá distintas fases y actividades clave para garantizar la eficiencia operativa, la seguridad y la optimización de la infraestructura del ICFES. Durante este periodo, se entregarán informes mensuales de gestión de servicios y se realizarán revisiones específicas que incluirán la evaluación de la infraestructura y la seguridad.

7.1 Fases de la Gestión de la Infraestructura

7.1.1 Fase 1: Validación Inicial y Revisión de la Infraestructura

Esta fase se centrará en la validación de la infraestructura existente durante dos meses, con las siguientes actividades clave que incluirán:

Mes 1 2025: Se llevará a cabo una revisión de la arquitectura en la nube para evaluar la alineación de la infraestructura con las mejores prácticas establecidas.

Mes 2 2025: Se realizará una evaluación de la seguridad utilizando un modelo de madurez para identificar el nivel de madurez y proponer mejoras en la protección de los datos y la infraestructura.

Entregables:

- Informe de Revisión de Arquitectura en la Nube
- Informe de Evaluación de Seguridad

7.1.2 Fase 2: Optimización Única de Cargas

Durante esta fase, se deberá realizar una optimización única de cargas, con el objetivo de ajustar la infraestructura a las necesidades específicas del ICFES. Este proceso incluirá el análisis de las cargas de trabajo y el ajuste de la infraestructura para mejorar el rendimiento y la eficiencia operativa.

Entregables:

Informe único de Optimización de Cargas, e incluirá el análisis de las cargas optimizadas, las recomendaciones para el mantenimiento y la eficiencia de las cargas de trabajo.

7.1.3 Fase 3: Gestión Continua y Optimización Proactiva

En esta fase, se dará continuidad a la gestión activa de la infraestructura, con la implementación de los procesos de servicios gestionados, optimización



continua de recursos y seguridad, y monitoreo proactivo. Las actividades de esta fase incluirán la revisión constante del uso de los recursos, optimización de costos y escalabilidad automática. Además, se gestionarán los aspectos operativos críticos de la infraestructura, como disponibilidad, incidentes y cambios.

Entregables:

Informe de Gestión de Servicios (mensual), que deberá entregarse de forma continua.

7.2 Resumen de Entregables Clave

- Informe de Revisión de Arquitectura en la Nube
- Informe de Evaluación de Seguridad
- Informe único de Optimización de Cargas
- Informe de Gestión de Servicios, que deberá entregarse mensualmente.

Codigos SKU

Codigo SKU	Descripción	Moneda	Valor	Unidad	Mes
NUV-HOU-03-01	Houndoc 1 US Dolar Procesamiento Nube	Dólares (USD)	\$	1 Dolar	5.456
Configuracion, Parametrización y Capacitación					
Codigo SKU	Descripción	Moneda	Valor	Unidad	Mes
IT-SW-09-02	Configuración y parametrización de los Productos	Colombian Pesos (COP)	\$ 385.000	Hora	1.268
IT-SW-09-02	Configuración y parametrización de los Productos	Colombian Pesos (COP)	\$ 385.000	Hora	1
Soporte Premium					
Codigo SKU	Descripción	Moneda	Valor	Unidad	Mes
IT-SW-02-02	Soporte técnico en sitio	Colombian Pesos (COP)	\$ 32.250.000	Mes	1

Diego Mauricio Salas
Subdirección de Información



SOLICITUD DE CERTIFICADO DE DISPONIBILIDAD PRESUPUESTAL
SECRETARÍA GENERAL
SUBDIRECCIÓN FINANCIERA Y CONTABLE

Página 1 de 1
Programa EBS
Usuario DMSALASR
Fecha 09-OCT-25
Hora 09:41:47

INFORMACIÓN BÁSICA

Fecha: 09/10/2025 No. Solicitud 22803
Concepto ITEM_1025

AFECTACIÓN PRESUPUESTAL 2025

RUBRO	DESCRIPCIÓN	ÁREA	PROYECTO	VALOR
825320202008003011	SERVICIOS DE CONSULTORÍA EN ADMINISTRACIÓN Y SERVICIOS DE GESTIÓN	SDINFOR	10000081	632068660
TOTAL:				632,068,660.00

Elaborado Por:

SALAS RAMIREZ, DIEGO MAURICIO

Revisado Por:

Aprobado por:

SALAS RAMIREZ, DIEGO MAURICIO

VoBo: _____

INFORMACIÓN BÁSICA				
Fecha	10-OCT-25	Estado:	APROBADO	No. CDP 15579
Concepto	ITEM_1025			

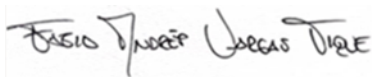
Valor del Presente Certificado : 632,068,660.00

EL SUSCRITO RESPONSABLE DE PRESUPUESTO, CERTIFICA QUE PARA ATENDER EL GASTO, OBJETO DEL COMPROMISO, HAY DISPONIBILIDAD PRESUPUESTAL HASTA POR LA SUMA QUE SE INDICA CON CARGO AL PRESUPUESTO 2025 Y SU REGISTRO SE HA EFECTUADO CONTRA LA SIGUIENTE APROPIACIÓN.

INFORMACIÓN EN VIGENCIA FUTURA		
Vigencias Futuras	Año	Valor

AFECTACIÓN PRESUPUESTAL 2025				
RUBRO	NOMBRE DEL RUBRO	ÁREA	PROYECTO	VALOR
825320202008003011	SERVICIOS DE CONSULTORÍA EN ADMINISTRACIÓN Y SERVICIOS DE GESTIÓN	SDINFOR	211110013	632,068,660.00

TOTAL PRESUPUESTADO: 632,068,660.00
TOTAL DISPONIBILIDAD: 632,068,660.00



Elaboró:



Subdirector Financiero y Contable:

Recibido Por:

nuvu

Datalake

Icfes

Acuerdos de Niveles de Servicio

Para la solución

Feb/2025

1. Metodología de soporte

1.1. Registro de Solicitudes de Servicio

Toda solicitud que se genere en el marco del servicio que se ofrece deberá ser reportada para su atención por parte de NUVU en horario de acuerdo a la contratación del servicio, a través de la herramienta Service Center de la empresa, la cual se accede a través de Internet en la siguiente dirección soporte.nuvu.cc

Las solicitudes deben ser registradas por los usuarios encargados de canalizar los requerimientos a NUVU a través de la herramienta antes mencionada, se sugiere un líder de cada área. El reporte debe incluir la información requerida para poder diagnosticar el problema: número interno, categoría, urgencia, impacto, hora y fecha de registro, cliente, usuario que reporta, usuario que origina, método de notificación, descripción de los síntomas, estado del incidente, incidentes relacionados, persona asignada, problema relacionado, error conocido, instrucciones para replicar el error, datos de ejemplo en ambiente de pruebas (opcional), pantallas o reporte con el error, se deben documentar los incidentes en el formato estándar de reporte de incidentes definido.

Cualquier requerimiento que no sea reportado en los medios antes indicados no será atendido por NUVU y se exonera de cualquier responsabilidad sobre el mismo.

1.2. Admisión y Clasificación

Las solicitudes serán evaluadas para determinar si hace parte del alcance de los servicios contratados y se clasificará la misma, cambiando su estado de abierta a aceptada o rechazada (en cuyo caso se indicará y registrará en el SERVICE CENTER la razón por la cual se rechaza).

Una vez aceptada la solicitud, se procederá a clasificarla acorde al módulo y tipo de solicitud reportada y se analizarán el impacto y prioridad del mismo para determinar el tiempo máximo de que se dispone para su solución acorde a los ANS.

1.3. Diagnóstico

El diagnóstico puede efectuarse por cualquiera de los siguientes mecanismos, en este orden:

1. Análisis de la documentación enviada con la solicitud (pantallas, datos de réplica etc.) para buscar identificar el incidente y documentar su solución a través de la herramienta.
2. Búsqueda en la base de conocimiento acerca de coincidencias con incidencias previamente reportadas por otros clientes o problemas conocidos.
3. Verificación mediante diagnóstico presencial entre el consultor In situ y los líderes de área definidos por el cliente, de acuerdo con la prioridad y planeación de los casos y/o verificación directa con el usuario final.

2. Acuerdos de niveles de servicio (ANS)

A continuación, se presentan los compromisos de respuesta (Acuerdos de Niveles de Servicio) a los requerimientos recibidos en el marco del proyecto Datalake:

Prioridad	Descripción	Tiempo de Atención	Tiempo de Solución provisional	Tiempo de Solución Definitivo
1	Crítico	1 hora	10 horas	28 horas
2	Alto	2 horas	20 horas	44 horas
3	Medio	4 horas	NA	56 horas
4	Bajo	8 horas	NA	80 horas
5	Planeado	8 horas	NA	176 horas

Tabla. Acuerdos de Niveles de Servicio (ANS)

Para determinar la prioridad se utilizarán las siguientes definiciones:

Prioridad	Definición	Ejemplo
Crítico	La solución no opera en producción de una manera razonable.	Incidentes que impiden el cumplimiento de las normas o de operación
Alto	Algunas funciones importantes de la solución no están disponibles en producción. Hay impacto en el nivel de servicios de la Entidad.	Incidentes que impiden la ejecución de tareas transaccionales diarias que no sean de carácter obligatorio o de cumplimiento de norma.

Medio	Errores en la solución que permiten a la Entidad operar en producción sin deterioro de su nivel de servicio.	Incidentes que impiden la ejecución de tareas transaccionales diarias requeridas al interior de la Entidad para operar
Bajo	Errores de apariencia o menores que igualmente permiten operar las funcionalidades de la solución relacionadas con el error.	Incidentes que afectan la apariencia de la solución o la experiencia del usuario o consultas de información sin impedir la operación. Todas las demás operaciones, procesos y generación de información no contemplada en las prioridades anteriores.
Planeado	Se trata de un incidente previsto, cuya solución es compleja y requiere largo tiempo.	Incidentes que se pueden prever y requieren autorización del cliente para ejecutar la solución, dado que es compleja y toma tiempo hacerla.



2025-110-0000852-3

Destinatario: DIEGO MAURICIO SALAS RAMIREZ
Fecha: 07/11/2025 17:45:25.226 Anexos: 0
Asunto: ICFES
Remitente: LUIS GONZAGA MARTINEZ SIERRA
Radicador: Luis Gonzaga Martinez
Destinatario: dmsalsr@icfes.gov.co

COMUNICACIÓN INTERNA

PARA: **DIEGO MAURICIO SALAS**
Subdirector de información

HENEDY JOHANA TABORDA
Contratista Subdirección de Información

DE: **SECRETARIA GENERAL**

ASUNTO: **Designación Comité Evaluador RFQ N° 201526**

Cordial saludo,

De manera respetuosa y actuando de conformidad con lo dispuesto por el artículo 27 del Acuerdo N° 000003 de 2023 por el cual se adopta el Manual de Contratación del Instituto, se tiene que *“El ordenador del gasto o quien éste delegue designará al Comité Evaluador plural e impar para cada proceso de selección contractual, el cual será conformado por los servidores y/o colaboradores de la entidad (...) Los miembros del Comité de Evaluación actuarán dentro del ámbito de sus competencias y responderán por el acápite de la evaluación que les haya sido asignado: jurídico, financiero, técnico y económico. En todo caso, el Comité suscribirá en pleno, el consolidado de la evaluación y la recomendación para el ordenador del gasto. (...) Deberá realizarse la evaluación dentro del término establecido en el pliego de condiciones y de conformidad con los factores y/o criterios de evaluación señalados en el respectivo documento, su ponderación y el procedimiento que para el efecto corresponda.”*

En consideración a lo anterior, se hace necesario la conformación de un Comité Evaluador con el fin de que asesore al Ordenador del Gasto durante el evento de solicitud de cotizaciones RFQ N° 201526, mediante el cual se pretende la celebración de orden de compra para la satisfacción del siguiente objeto contractual: *“Contratar una solución SaaS para el Icfes enfoca en la habilitación de entornos de trabajo virtuales seguros para el Banco de Items, utilizando Houndoc como plataforma SaaS.”*, por tanto, se designan a los siguientes colaboradores del Instituto Colombiano para la Evaluación de la Educación–Icfes, como miembros del Comité Evaluador como se indica a continuación:

AREA A EVALUAR EN LA OFERTA	FUNCIONARIO / CONTRATISTA DESIGNADO	ROL
Verificación de los aspectos técnicos y económicos de las cotizaciones presentadas	DIEGO MAURICIO SALAS	Subdirector de información
	HENEDY JOHANA TABORDA	Contratista Subdirección de Información

Las funciones del Comité Evaluador serán las siguientes:

1. Verificar y revisar el cumplimiento de las condiciones habilitantes que confieren a los proponentes el derecho a la evaluación de sus ofertas.
2. Cotejar los ofrecimientos de quienes resulten habilitados con los resultados que, en materia de precio y condiciones de mercado, hayan sido establecidos en el estudio elaborado por la entidad.

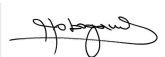
3. Asesorar al Icfes durante el proceso de selección y validar el contenido de los requerimientos técnicos.
4. Evaluar, calificar las propuestas presentadas dentro del proceso de selección, de manera objetiva, ciñéndose exclusivamente a las reglas contenidas en el documento de condiciones y suscribir los respectivos informes de evaluación de acuerdo con su competencia.
5. Presentar los respectivos informes de evaluación y calificación.
6. Recomendar al Ordenador del Gasto, el sentido de la decisión a adoptar de conformidad con la evaluación efectuada y dar la recomendación de Adjudicación o Declaratoria Fallido del proceso al ordenador del Gasto, según sea el caso.
7. Resolver las observaciones que se susciten con ocasión y durante todo el proceso de selección.
8. Actuar con diligencia, buena fe y transparencia durante el desarrollo de su labor. Por lo anterior, ante el conocimiento de alguna irregularidad que afecte la transparencia del proceso, deberá informar inmediatamente de este hecho al Ordenador del Gasto.

Es importante tener en cuenta que será responsabilidad de los miembros del Comité Evaluador, informar con la debida antelación al Ordenador del Gasto, cualquier ausencia o impedimento que no le permita cumplir cabalmente con las funciones aquí asignadas, en especial el cumplimiento de las actividades establecidas en el cronograma. Igualmente, en el momento de la designación, los miembros deberán informar si tienen alguna observación sobre la misma.


De otra parte, en virtud de lo previsto en los artículos 4º y 5º del Acuerdo N° 000003 de 2023 – Manual de Contratación, los miembros del Comité Evaluador están sujetos a las disposiciones allí contenidas sobre inhabilidades, incompatibilidades y conflicto de intereses y el carácter de asesor no los exime de la responsabilidad del ejercicio de la labor encomendada.


Por último, la labor asignada debe ser adelantada dentro de los parámetros establecidos en el Manual de Contratación y en lo establecido en el Instrumento de Agregación De Demanda, Sistema Dinámico De Adquisición (Iad/Sda) De Software Por Catálogo II suscrito por la Agencia Nacional de Contratación - Colombia Compra Eficiente, sin perjuicio de lo que aplique, según lo dispuesto en el artículo 13 de la Ley 1150 de 2007, que ordena a las entidades públicas sometidas a régimen especial de contratación, aplicar en el desarrollo de su actividad contractual los principios de la función administrativa y de la gestión fiscal de que tratan los artículos 209 y 267 de la Constitución Política.


Cordialmente,




LUIS GONZAGA MARTÍNEZ SIERRA
SECRETARIO GENERAL

Revisó: Mónica Marcela Mora Moreno - Contratista Secretaría General 

Revisó: David Fernando Díaz Palacio -Subdirector de Abastecimiento y Servicios Generales. 

Revisó: Víctor Raúl Tovar Méndez - Coordinador Contractual Subdirección Abastecimiento y Servicios Generales 

Proyectó: Julián Torres Valenzuela - Contratista- Subdirección de Abastecimiento y Servicios Generales 





EVALUACIÓN EVENTO DE SIMULACIÓN WEB NO. 201526

OBJETO: “Contratar una solución SaaS para el Icfes enfoca en la habilitación de entornos de trabajo virtuales seguros para el Banco de Items, utilizando Houndoc como plataforma SaaS”

En atención a la designación efectuada de conformidad con el radicado N° 2025-110-0000852-3-del 07de noviembre de 2025 y obrando de conformidad con los artículos 4º y 5º del Acuerdo No. 000003 de 2023 – Manual de Contratación, se procede a verificar la cotizaciones allegadas dentro del evento de cotización N° 201526 tramitado a través del Instrumento de Agregación De Demanda, Sistema Dinámico De Adquisición (Iad/Sda) De Software Por Catálogo II, para lo cual inicialmente se encuentra imperativo manifestar que en atención En atención al segmento y categoría de la adquisición, según la GUÍA PARA COMPRAR EN LA TIENDA VIRTUAL DEL ESTADO COLOMBIANO)A TRAVÉS DEL ACUERDO MARCO DE PRECIOS, el criterio de seleccón del proveedor corresponde al siguiente: “la entidad debera elegir la cotizacion que cumpla con las características solicitadas, y que haya cotizado el menor precio relacionado”.

Así las cosas, en atención al trámite realizado, se evidencia la presentación de las siguientes cotizaciones:

Respuestas

Exportar							Vista	Todo
Proveedor	Nombre de la respuesta	Enviado	Precio base	Capacidad	Precio ofertado	Ahorros		
Información Localizada S.A.S.	Información Localizada S.A.S. - #1251976	31/10/25 10:52 -0500	636.142.403,00 COP	100%	0,00 COP	636.142.403,00 COP		
Hightech Software S.A.S.	Hightech Software S.A.S. - #1252051	31/10/25 12:11 -0500	636.142.403,00 COP	100%	632.065.298,00 COP	4.077.105,00 COP		
UNION TEMPORAL BGH 2024	UNION TEMPORAL BGH 2024 - #1252506	03/11/25 19:57 -0500	636.142.403,00 COP	100%	0,00 COP	636.142.403,00 COP		
NUEVA ERA SOLUCIONES SAS	NUEVA ERA SOLUCIONES SAS - #1252677	04/11/25 09:05 -0500	636.142.403,00 COP	100%	0,00 COP	636.142.403,00 COP		
Comware S.A.	Comware S.A. - #1252734	04/11/25 09:42 -0500	636.142.403,00 COP	100%	0,00 COP	636.142.403,00 COP		
Convist SAS	Convist SAS - #1252803	04/11/25 10:12 -0500	636.142.403,00 COP	100%	0,00 COP	636.142.403,00 COP		
INDRA COLOMBIA S.A.S.	INDRA COLOMBIA S.A.S. - #1253252	06/11/25 16:18 -0500	636.142.403,00 COP	100%	0,00 COP	636.142.403,00 COP		
REDNEET SAS	REDNEET SAS - #1253361	06/11/25 08:57 -0500	636.142.403,00 COP	100%	0,00 COP	636.142.403,00 COP		
Xertica Colombia SAS	Xertica Colombia SAS - #1253690	05/11/25 09:13 -0500	636.142.403,00 COP	100%	6.707.000.000.000,00 COP	-6.706.363.857.597,00 COP		

Ahora bien, el proveedor Xertica Colombia SAS, presentó oferta económica por valor de \$6.707.000.000.000, empero simultáneamente allego certificado indicando que “no cuenta con el software específico que cumple con todas las especificaciones detalladas en la convocatoria”.


Adicional, se deja constancia que en el desarrollo del procedimiento de consolidación del Evento 201526, el proveedor Hightech Software S.A.S, allego certificado de la DIRECCION NACIONAL DE DERECHO DE AUTOR UNIDAD ADMINISTRATIVA ESPECIAL N° 13-89-396 el cual evidencia que Hightech Software S.A.S. tiene la titularidad de los derechos patrimoniales derivados de la solución tecnológica requerida por el instituto, por lo que se determina que la cotización presentada por valor de \$632.065.298, cumple a cabalidad con la necesidad técnica de la entidad, cumpliendo con las características técnicas exigidas para la consolidación, integración, procesamiento y visualización de información en el Data Lake del ICFES, garantizando la eficiencia en el análisis de datos y la toma de decisiones estratégicas. Por lo anterior, se recomienda proceder con la contratación de HIGH TECH SOFTWARE S.A.S. mediante el mecanismo establecido en el IAD/SDA, lo anterior conforme con los parámetros de escogencia establecidos en la GUÍA PARA COMPRAR EN LA TIENDA VIRTUAL DEL ESTADO COLOMBIANO.

En coherencia con lo anterior el proveedor Hightech Software S.A.S cumple con los requisitos tecnicos, juridicos y economicos, por lo que se recomienda la celebración de la orden de compra respectiva con dicho proveedor.

En constancia se suscribe por el comité evaluador el 06 de noviembre de 2025.

Diego Mauricio Salas
Subdirector de Información

Henedy Johana Taborda
Contratista Subdireccion Información.

	<div>MINISTERIO DEL INTERIOR</div> <div>DIRECCION NACIONAL DE DERECHO DE AUTOR</div> <div>UNIDAD ADMINISTRATIVA ESPECIAL</div> <div>OFICINA DE REGISTRO</div> <div>CERTIFICADO DE HOUNDOC</div>	<div>Libro - Tomo - Partida</div> <div>13-89-396</div> <div>Fecha Registro</div> <div>02-may.-2022</div>
Page 1 of 2		
<div>1. DATOS DE LAS PERSONAS</div> <div><div><div>AUTOR</div><div><div>Nombres y Apellidos</div><div>LUIS FERNANDO ORTEGA MELO</div></div><div><div>No de identificación</div><div>80833377</div></div><div><div>CC</div><div></div></div></div><div><div>Nacional de</div><div>COLOMBIA</div></div><div><div>Dirección</div><div>CARRERA 21 # 37 85 OF 202</div></div><div><div>Ciudad:</div><div>BOGOTA D.C.</div></div></div> <div><div>AUTOR</div><div><div>Nombres y Apellidos</div><div>EDWIN FABIAN PEREZ POVEDA</div></div><div><div>No de identificación</div><div>80187008</div></div><div><div>CC</div><div></div></div></div> <div><div>Nacional de</div><div>COLOMBIA</div></div> <div><div>Dirección</div><div>CL 40 24 - 76 AP 202</div></div> <div><div>Ciudad:</div><div>BOGOTA D.C.</div></div>		

AUTOR

Nombres y Apellidos

YIDAIDO ROJAS ROJAS BARRANTE

No de identificación

1016011156

CC

Nacional de

COLOMBIA

Dirección

TRANSVERSAL 51 # 1-51

Ciudad:

BOGOTA D.C.

TITULAR DERECHO PATRIMONIAL

Razón Social

HIGH TECH SOFTWARE S.A.S.

Nit

9007183367

Dirección

KR 5 69 - 14 OF 302

Ciudad:

BOGOTA D.C.

PRODUCTOR

Razón Social

HIGH TECH SOFTWARE S.A.S.

Nit

9007183367

Dirección

KR 5 69 - 14 OF 302

Ciudad:

BOGOTA D.C.

	<p>MINISTERIO DEL INTERIOR DIRECCION NACIONAL DE DERECHO DE AUTOR UNIDAD ADMINISTRATIVA ESPECIAL OFICINA DE REGISTRO <u>CERTIFICADO DE HOUNDOC</u></p>	<p>Libro - Tomo - Partida 13-89-396 Fecha Registro 02-may.-2022</p>
<p>Page 2 of 2</p>		
<div></div> <hr/> <p>JULIAN DAVID RIATIGA IBÁÑEZ JEFE OFICINA DE REGISTRO (E)</p>		
<p>MZP</p>		

Nota: El derecho de autor protege exclusivamente la forma mediante la cual las ideas del autor son descritas, explicadas, ilustradas o incorporadas a las obras . No son objeto de protección las ideas contenidas en las obras literarias y artísticas, o el contenido ideológico o técnico de las obras científicas, ni su aprovechamiento industrial o comercial (artículo 7o. de la Decisión 351 de 1993).

Rta RFI - Banco de Items

Migración a la nube

10/2025

Contenido

1. Introducción	4
2. Alcance	4
2.1 Áreas de intervención	4
2.2 Objetivos principales	5
2.3 Actividades principales	5
3. Detalle de alcance	6
3.1 Fase de análisis y diseño	6
3.2 Fase de implementación de entornos virtuales y seguridad	7
3.3 Fase de configuración de entornos de trabajo virtuales	8
3.4 Fase de configuración de integraciones	8
3.5 Fase de capacitación y transición	9
3.6 Fase de monitoreo	9
4. Características de la solución	10
4.1 Plataforma Houndoc como servicio (SaaS)	10
4.2 Sistema de seguridad y control de acceso	11
4.3 Entornos de trabajo virtuales personalizados	11
4.4 Sistemas de almacenamiento seguro	12
4.5 Integración con sistemas existentes	12
5. Arquitectura de referencia	13
5.1 Capa de acceso y conectividad	13
5.2 Capa de ingestión y preparación de datos	14
5.3 Capa de almacenamiento y procesamiento	14
5.4 Capa de entornos de trabajo virtuales	14
5.5 Capa de seguridad transversal	14
5.6 Capa de monitoreo	15
5.7 Integraciones con sistemas existentes	15
5.8 Flujos de trabajo principales	15
6. Metodología	16
6.1 Enfoque metodológico	16
6.1.1 Fase de Iniciación	17
6.2 Gestión del proyecto	18

6.3 Control de calidad	19
7. Cronograma	19
7.1 Distribución de actividades por mes	20
7.2 Actividades principales y su distribución temporal	20
7.3 Consideraciones sobre el cronograma	21
8. Metodología de soporte y mantenimiento	22
8.1 Soporte y mantenimiento correctivo	22
8.2 Soporte y mantenimiento preventivo	23
8.3 Soporte y mantenimiento evolutivo	24
8.4 Canales de atención y escalamiento	24
8.5 Informes y documentación	24
9. Propuesta económica	¡Error! Marcador no definido.
10. Condiciones comerciales	¡Error! Marcador no definido.
10.1 Forma de Pago	¡Error! Marcador no definido.
10.2 Plazo de Implementación	¡Error! Marcador no definido.
10.3 Vigencia de la Oferta	¡Error! Marcador no definido.
10.4 Duración del Servicio	¡Error! Marcador no definido.
10.5 Ajustes de Alcance	¡Error! Marcador no definido.
10.6 Confidencialidad	¡Error! Marcador no definido.
10.7 Propiedad Intelectual	¡Error! Marcador no definido.
10.8 Terminación Anticipada	¡Error! Marcador no definido.
11. Garantía	25
11.1 Cobertura de la garantía	25
11.2 Período de garantía	26
11.3 Servicios incluidos en la garantía	26
11.4 Tiempos de respuesta durante la garantía	26
11.5 Proceso para reportar incidentes bajo garantía	27
11.6 Limitaciones de la garantía	27
11.7 Condiciones para mantener la validez de la garantía	27
12. Supuestos	28

1. Introducción

El Instituto Colombiano para la Evaluación de la Educación (Icfes) requiere modernizar la operación del Banco de Items, actualmente limitada por restricciones operativas en su sistema de almacenamiento. El Banco de Items es un área crítica de alta seguridad donde se realizan procesos fundamentales como la diagramación, revisión y armado de las pruebas que el Icfes aplica a nivel nacional.

La infraestructura actual presenta limitaciones significativas de capacidad de almacenamiento y procesamiento, no cuenta con sistemas de respaldo adecuados y existe un riesgo considerable de pérdida de información sensible acumulada a lo largo de los años. Estos factores comprometen la eficiencia operativa y la seguridad de los datos críticos que maneja el Icfes en sus procesos de evaluación.

La presente propuesta técnica detalla la solución para implementar entornos de trabajo virtuales seguros para el Banco de Items utilizando Houndoc como plataforma SaaS. Esta implementación permitirá establecer un entorno escalable, con sistemas de respaldo automáticos y mecanismos robustos de seguridad. La solución mantendrá los estrictos protocolos de seguridad necesarios para proteger la confidencialidad de la información del Banco de Items.

La solución propuesta está diseñada para atender las necesidades de los usuarios permanentes del área de diagramación y los usuarios ocasionales como gestores de pruebas y correctores de estilo, mejorando su eficiencia operativa mientras se permite el cumplimiento de los requisitos de seguridad y confidencialidad propios de este proceso crítico para el Icfes. Adicionalmente, se contempla la capacitación del personal de tecnología del Icfes para permitir la adecuada administración y aprovechamiento de los nuevos entornos virtuales de trabajo.

2. Alcance

El alcance de este proyecto comprende la implementación de una solución integral para la habilitación de entornos de trabajo virtuales seguros para el Banco de Items del Icfes mediante la plataforma SaaS Houndoc, abarcando los siguientes componentes:

2.1 Áreas de intervención

La solución propuesta contempla tres áreas principales de intervención:

1. **Entornos de trabajo virtuales seguros:** Implementación de una plataforma escalable basada en Houndoc que permita la creación y gestión de hasta 30 espacios de trabajo virtuales para los usuarios del Banco de Items, con

acceso a todas las herramientas necesarias para la diagramación y gestión de pruebas.

2. **Sistema de seguridad y control de acceso:** Establecimiento de mecanismos robustos para permitir la confidencialidad e integridad de la información, incluyendo VPN dedicada, control de acceso granular basado en roles y auditoría completa de actividades.
3. **Integración con sistemas existentes:** Configuración de conectores e interfaces que permitan la integración fluida entre los entornos virtuales de Houndoc, la plataforma Prisma y el directorio activo de la institución.

2.2 Objetivos principales

Los objetivos fundamentales que persigue este proyecto son:

1. Implementar entornos de trabajo virtuales seguros para los usuarios del Banco de Items utilizando la plataforma Houndoc.
2. Establecer una solución escalable que elimine las limitaciones actuales de capacidad y permita el crecimiento según las necesidades del Icfes.
3. Configurar sistemas robustos de respaldo automático que eliminen el riesgo de pérdida de información.
4. Habilitar entornos de trabajo virtuales que mantengan o mejoren los controles de seguridad existentes.
5. Facilitar la integración con sistemas actuales como la plataforma Prisma, el directorio activo y las herramientas de la suite de Adobe utilizadas para la diagramación.
6. Capacitar al personal de tecnología del Icfes para la utilización efectiva y administración de los nuevos entornos virtuales, permitiendo la transferencia de conocimiento necesaria para su gestión autónoma.

2.3 Actividades principales

Para lograr los objetivos planteados, se desarrollarán las siguientes actividades clave:

1. **Análisis y diseño:** Levantamiento detallado de requisitos técnicos y de seguridad, análisis de los flujos de trabajo actuales, diseño de la arquitectura de entornos virtuales y definición de políticas de seguridad.

2. **Implementación de entornos virtuales y seguridad:** Configuración de la plataforma Houndoc, aprovisionamiento de espacios de trabajo virtuales, implementación de sistemas de respaldo automático, configuración de mecanismos de autenticación y permisos de acceso.
3. **Configuración de entornos de trabajo virtuales:** Personalización de los espacios virtuales para los usuarios del Banco de Items, instalación de aplicaciones necesarias (suite de Adobe), configuración de acceso a la plataforma Prisma y mantenimiento del sistema actual de carpetas y permisos.
4. **Configuración de almacenamiento seguro:** Establecimiento de repositorios seguros para la información del Banco de Items dentro de la plataforma Houndoc, con políticas de respaldo y recuperación automáticas.
5. **Capacitación y transición:** Formación al personal de tecnología del Icfes, elaboración de documentación técnica y acompañamiento en la transición hacia los nuevos entornos virtuales.
6. **Monitoreo y ajustes:** Seguimiento del rendimiento del sistema y verificación continua de la seguridad tras la implementación.

Esta solución permitirá modernizar la operación del Banco de Items mediante entornos de trabajo virtuales seguros basados en Houndoc, permitiendo la seguridad de la información y mejorando significativamente la eficiencia operativa, sin comprometer los estrictos protocolos de confidencialidad requeridos para este proceso crítico del Icfes.

3. Detalle de alcance

El detalle del alcance para el proyecto de habilitación de entornos de trabajo virtuales seguros para el Banco de Items se estructura en fases claramente definidas, cada una con actividades específicas y resultados concretos:

3.1 Fase de análisis y diseño

Esta fase inicial establece las bases técnicas y operativas para la implementación exitosa de la solución:

1. Levantamiento detallado de requisitos técnicos y de seguridad

- **Resultado:** Documento de especificación de requisitos técnicos y de seguridad

- **Actividades:** Entrevistas con usuarios clave, análisis de infraestructura actual, identificación de necesidades específicas de seguridad y acceso

2. Análisis de flujos de trabajo actuales

- **Resultado:** Informe de procesos actuales y sistema de archivos
- **Actividades:** Documentación de los flujos de trabajo existentes, identificación de oportunidades de mejora, análisis del sistema de permisos actual

3. Diseño de la arquitectura de entornos virtuales con Houndoc

- **Resultado:** Documento de arquitectura con diagramas técnicos
- **Actividades:** Diseño de la configuración de Houndoc, especificación de entornos virtuales, definición de componentes de seguridad

4. Definición de políticas de seguridad y acceso

- **Resultado:** Documento de políticas de seguridad para los entornos virtuales
- **Actividades:** Establecimiento de controles de acceso y definición de políticas de auditoría

3.2 Fase de implementación de entornos virtuales y seguridad

En esta fase se implementan los componentes fundamentales de la plataforma:

1. Configuración de la plataforma Houndoc

- **Resultado:** Plataforma base configurada y lista para personalización
- **Actividades:** Aprovisionamiento de recursos, configuración de capacidad, implementación de escalabilidad automática

2. Implementación de sistemas de respaldo automático

- **Resultado:** Sistema de respaldo configurado y validado
- **Actividades:** Configuración de políticas de respaldo, programación de copias de seguridad, validación del proceso de recuperación

3. Implementación de sistemas de seguridad

- **Resultado:** Sistemas de seguridad configurados y validados
- **Actividades:** Configuración de VPN dedicada, implementación de cifrado de datos y configuración de permisos de acceso granulares

3.3 Fase de configuración de entornos de trabajo virtuales

Esta fase se enfoca en establecer los espacios de trabajo para los usuarios:

1. Creación y configuración de entornos virtuales

- **Resultado:** Entornos virtuales operativos con sistema operativo instalado
- **Actividades:** Creación de 30 espacios virtuales, configuración de recursos (CPU, memoria, almacenamiento), establecimiento de políticas de acceso

2. Instalación y configuración de aplicaciones

- **Resultado:** Entornos de trabajo con aplicaciones instaladas y configuradas
- **Actividades:** Instalación de suite de Adobe, configuración de aplicaciones específicas, validación de funcionamiento

3.4 Fase de configuración de integraciones

Esta fase crítica permite la interoperabilidad con los sistemas existentes del Icfes:

1. Integración con sistemas existentes

- **Resultado:** Conectores e interfaces configurados para sistemas del Icfes
- **Actividades:** Desarrollo de conectores para Prisma, conexión con directorio LDAP, configuración de interfaces de comunicación, pruebas de integración

2. Verificación de integridad de la información

- **Resultado:** Informe de verificación de integridad de datos
- **Actividades:** Comprobaciones automatizadas de integridad, verificaciones manuales selectivas, validación de estructura de datos

3. Pruebas de funcionamiento con datos reales

- **Resultado:** Informe de pruebas funcionales
- **Actividades:** Pruebas de acceso a datos, validación de funcionamiento del sistema de archivos actual en el nuevo entorno, verificación de rendimiento con carga real

4. Configuración de accesos a sistemas existentes

- **Resultado:** Integración con plataforma Prisma y directorio activo LDAP
- **Actividades:** Configuración de conectividad, validación de accesos, pruebas de integración

3.5 Fase de capacitación y transición

Esta fase permite la adopción efectiva de los nuevos entornos virtuales:

1. Capacitación al personal de tecnología del Icfes

- **Resultado:** Sesiones de capacitación y material de referencia técnica
- **Actividades:** Formación en administración de la plataforma Houndoc, gestión de seguridad, monitoreo y resolución de incidencias

2. Elaboración de documentación técnica

- **Resultado:** Manuales técnicos de administración y operación
- **Actividades:** Desarrollo de guías de administración, procedimientos operativos, documentación de arquitectura

3. Capacitación a usuarios finales

- **Resultado:** Usuarios capacitados en el uso de los entornos virtuales
- **Actividades:** Sesiones de formación, elaboración de guías de usuario, resolución de dudas específicas

3.6 Fase de monitoreo

Esta fase final permite la estabilización de la solución:

1. Monitoreo del rendimiento del sistema

- **Resultado:** Informes periódicos de rendimiento
- **Actividades:** Configuración de herramientas de monitoreo, análisis de métricas, identificación de oportunidades de mejora

2. Verificación continua de la seguridad

- **Resultado:** Informes de seguridad y recomendaciones
- **Actividades:** Análisis de logs de seguridad, verificación de controles, recomendaciones de mejora

La ejecución metódica de estas fases y actividades permitirá una implementación exitosa de entornos de trabajo virtuales seguros para el Banco de Items utilizando Houndoc como plataforma SaaS, cumpliendo con todos los objetivos establecidos y permitiendo la continuidad operativa de este componente crítico para el Icfes. El enfoque propuesto mantiene el sistema actual de manejo de carpetas y permisos con el que los usuarios están familiarizados, mientras mejora significativamente la seguridad, disponibilidad y eficiencia operativa.

4. Características de la solución

La solución propuesta para la habilitación de entornos de trabajo virtuales seguros para el Banco de Items se caracteriza por los siguientes componentes y funcionalidades, diseñados específicamente para atender las necesidades del Icfes:

4.1 Plataforma Houndoc como servicio (SaaS)

La base de la solución es la plataforma Houndoc, que ofrece:

- **Entornos virtuales seguros:** Espacios de trabajo aislados y protegidos que permiten la ejecución de aplicaciones y el acceso a datos de manera segura y controlada.
- **Alta disponibilidad:** Arquitectura redundante que permite el acceso continuo a los entornos de trabajo, minimizando los tiempos de inactividad.
- **Respaldo automático:** Sistema de copias de seguridad programadas con políticas de retención configurables, permitiendo la recuperación ante cualquier incidente.

- **Monitoreo continuo:** Supervisión permanente del estado de los servicios, rendimiento y capacidad, con alertas automáticas ante cualquier anomalía.
- **Escalabilidad:** Capacidad para aumentar o reducir recursos (procesamiento, memoria, almacenamiento) según las necesidades operativas sin interrumpir el servicio.

4.2 Sistema de seguridad y control de acceso

La protección de la información sensible del Banco de Items se habilita mediante:

- **Control de acceso basado en roles:** Asignación granular de permisos según el rol y responsabilidades de cada usuario dentro del proceso del Banco de Items.
- **VPN dedicada:** Conexión privada y cifrada que permite que solo los usuarios autorizados desde ubicaciones aprobadas puedan acceder al entorno.
- **Cifrado de datos:** Protección de la información tanto en tránsito como en reposo, permitiendo la confidencialidad en todo momento.
- **Aislamiento de sesiones:** Separación lógica entre sesiones de usuarios para evitar interferencias o accesos no autorizados entre entornos de trabajo.
- **Registro detallado de actividades:** Logs completos de todas las acciones realizadas en el sistema, facilitando auditorías y análisis de seguridad.

4.3 Entornos de trabajo virtuales personalizados

Los usuarios del Banco de Items contarán con espacios de trabajo que incluyen:

- **Entornos personalizados según rol:** Configuración específica según el tipo de usuario (diagramadores, gestores, correctores), con las herramientas y permisos adecuados para cada función.
- **Suite completa de Adobe:** Integración de las herramientas necesarias para la diagramación en los entornos virtuales.
- **Acceso a Prisma:** Conexión segura a la plataforma Prisma para la gestión de ítems, manteniendo los flujos de trabajo actuales.
- **Rendimiento optimizado:** Recursos de procesamiento adecuados para permitir una experiencia fluida incluso en tareas exigentes de diseño gráfico.

- **Persistencia de datos:** Almacenamiento persistente de archivos y configuraciones de usuario, permitiendo continuidad en el trabajo entre sesiones.

4.4 Sistemas de almacenamiento seguro

La gestión de la información del Banco de Items se realiza mediante:

- **Repositorio centralizado:** Almacenamiento estructurado y organizado de todos los archivos relacionados con el Banco de Items.
- **Gestión de permisos granular:** Control detallado sobre quién puede ver, editar o eliminar cada tipo de documento.

4.5 Integración con sistemas existentes

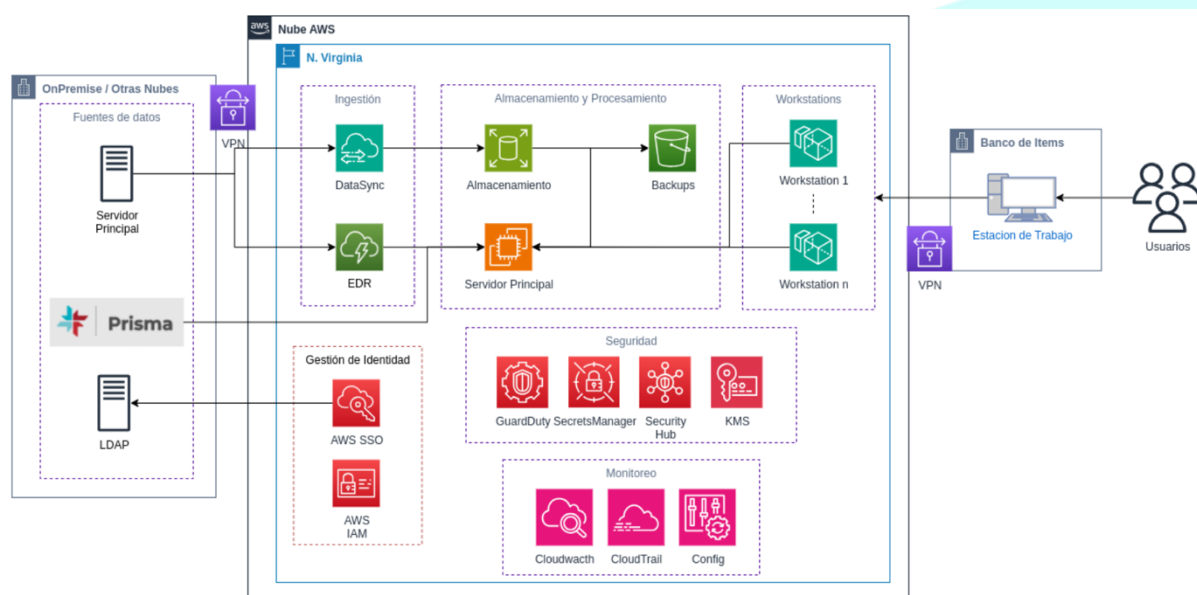
La solución permite la continuidad operativa mediante:

- **Conectores con Prisma:** Integración transparente con la plataforma actual de gestión de ítems, permitiendo el flujo bidireccional de información.
- **Integración con directorio LDAP:** Conexión con el directorio LDAP existente del ICFES a través de AWS SSO.
- **Mantenimiento del sistema de archivos:** Preservación de la estructura de carpetas y permisos con la que los usuarios están familiarizados.
- **Flujos de trabajo inalterados:** Conservación de los procesos actuales de diagramación, revisión y armado de pruebas.
- **Interfaces consistentes:** Experiencia de usuario similar a la actual, minimizando la curva de aprendizaje.

La combinación de estas características proporciona una solución integral que no solo resuelve las limitaciones actuales de infraestructura, sino que también mejora significativamente la seguridad, disponibilidad y eficiencia operativa del Banco de Items, permitiendo la continuidad de este proceso crítico para el Icfes a través de entornos virtuales seguros basados en la plataforma Houndoc.

5. Arquitectura de referencia

La arquitectura propuesta para la habilitación de entornos de trabajo virtuales seguros para el Banco de Items se ha diseñado utilizando la plataforma Houndoc como base, integrada con servicios específicos de AWS para habilitar los requisitos de seguridad, disponibilidad y rendimiento necesarios para este componente crítico del Icfes.



A continuación, se presenta la estructura de capas y componentes que conforman la solución:

5.1 Capa de acceso y conectividad

Esta capa establece los mecanismos de conexión segura a los entornos virtuales:

- **AWS VPN:** Servicio que establece túneles cifrados entre la red del Icfes y la infraestructura de Houndoc en AWS, permitiendo que las comunicaciones permanezcan privadas y protegidas.
- **AWS IAM (Identity and Access Management):** Sistema centralizado para la gestión de identidades y permisos de los usuarios, aplicando políticas de seguridad consistentes en toda la infraestructura.
- **AWS SSO (Single Sign-On):** Servicio que proporciona autenticación centralizada para el acceso a los recursos de AWS y Houndoc, con integración al directorio LDAP existente del Icfes.

5.2 Capa de ingestión y preparación de datos

Esta capa facilita la integración de datos y sistemas necesarios para el funcionamiento de los entornos virtuales:

- **AWS DataSync:** Servicio para la transferencia segura y eficiente de datos desde los sistemas actuales del Icfes hacia el almacenamiento en Houndoc, optimizando la disponibilidad de información en los entornos virtuales.

5.3 Capa de almacenamiento y procesamiento

Esta capa gestiona el almacenamiento de datos y la capacidad de procesamiento:

- **Amazon EC2:** Instancias que proporcionan capacidad de cómputo para los servicios de backend de Houndoc, permitiendo el rendimiento y la disponibilidad del sistema.
- **Amazon S3:** Servicio escalable para el almacenamiento de los datos del Banco de Items, con capacidad inicial de 5TB y posibilidad de crecimiento automático.
- **AWS Backup:** Servicio dedicado a la creación, gestión y almacenamiento de copias de seguridad, con políticas de retención configurables según los requisitos del Icfes.

5.4 Capa de entornos de trabajo virtuales

Esta capa proporciona los espacios de trabajo para los usuarios:

- **AWS WorkSpaces:** Servicio de escritorios virtuales en la nube que proporciona entornos de trabajo personalizados para los diferentes tipos de usuarios (diagramadores, gestores, correctores), con acceso a las aplicaciones necesarias como la suite de Adobe.

5.5 Capa de seguridad transversal

Los componentes de seguridad se implementan de manera transversal en toda la arquitectura:

- **AWS GuardDuty:** Servicio de detección de amenazas que monitorea continuamente la actividad maliciosa y el comportamiento anómalo en la infraestructura.
- **AWS Secrets Manager:** Servicio para el almacenamiento seguro y la gestión de credenciales, certificados y otros secretos necesarios para la operación.

- **AWS Security Hub:** Servicio centralizado para la gestión de la seguridad y el cumplimiento, proporcionando una visión integral del estado de seguridad de la infraestructura.
- **AWS KMS (Key Management Service):** Servicio para la gestión de claves de cifrado, protegiendo la información tanto en tránsito como en reposo.

5.6 Capa de monitoreo

Esta capa proporciona visibilidad sobre el estado y rendimiento de la infraestructura:

- **AWS CloudWatch:** Servicio de monitoreo que supervisa el rendimiento, disponibilidad y estado de salud de todos los componentes, generando alertas ante anomalías.
- **AWS CloudTrail:** Servicio que registra y almacena todas las actividades realizadas en la cuenta de AWS, facilitando la auditoría y el análisis forense.
- **AWS Config:** Servicio para evaluar, auditar y verificar las configuraciones de los recursos de AWS, permitiendo el cumplimiento de políticas y mejores prácticas.

5.7 Integraciones con sistemas existentes

La arquitectura incluye integraciones clave con sistemas existentes del Icfes:

- **Integración con Prisma:** Conexión directa desde la plataforma Houndoc a la plataforma Prisma, permitiendo el flujo de trabajo continuo para la gestión de ítems, construcción y revisión de preguntas.
- **Integración con LDAP:** Conexión con el directorio LDAP existente del Icfes para autenticación centralizada mediante AWS SSO, permitiendo mantener las políticas de gestión de identidades actuales.

5.8 Flujos de trabajo principales

1. **Flujo de autenticación:**
 - a. Los usuarios se autentican a través de AWS SSO, que valida sus credenciales contra el directorio LDAP existente
 - b. AWS IAM aplica los permisos correspondientes según el rol del usuario
 - c. Se establece una conexión segura mediante AWS VPN

2. Flujo de acceso a entornos virtuales:

- a. Los usuarios acceden a sus escritorios virtuales (AWS WorkSpaces) a través de conexiones VPN seguras
- b. Los escritorios virtuales tienen acceso a las aplicaciones necesarias (suite de Adobe) y a los datos almacenados en S3
- c. Las integraciones con Prisma permiten el flujo de trabajo continuo para la gestión de ítems

3. Flujo de trabajo colaborativo:

- a. Los usuarios trabajan en sus entornos virtuales con acceso a todas las herramientas necesarias
- b. Los datos se almacenan de forma segura en S3 con respaldos automáticos mediante AWS Backup
- c. AWS CloudTrail registra todas las actividades para auditoría y seguimiento
- d. AWS GuardDuty monitorea continuamente la seguridad del entorno

Esta arquitectura proporciona una base sólida para la implementación de entornos de trabajo virtuales seguros basados en Houndoc e integrados con servicios AWS, permitiendo que todos los requisitos técnicos y de seguridad sean adecuadamente atendidos, mientras se mantiene la integración con los sistemas existentes del Icfes y se permite la flexibilidad necesaria para adaptarse a necesidades futuras.

6. Metodología

Para la implementación exitosa del proyecto de habilitación de entornos de trabajo virtuales seguros para el Banco de Items utilizando Houndoc, se propone una metodología estructurada y adaptativa que combina las mejores prácticas de gestión de proyectos con un enfoque ágil para implementación de plataformas SaaS. Esta metodología permitirá una ejecución controlada, minimizando riesgos y habilitando resultados de alta calidad.

6.1 Enfoque metodológico

La metodología propuesta se estructura en seis fases claramente definidas, cada una con objetivos específicos y resultados tangibles:

6.1.1 Fase de Iniciación

Esta fase establece las bases para el éxito del proyecto:

- **Definición del alcance detallado:** Refinamiento de los requerimientos y límites del proyecto, permitiendo un entendimiento común entre todas las partes interesadas.
- **Establecimiento de la gobernanza del proyecto:** Definición de roles y responsabilidades, canales de comunicación, procedimientos de toma de decisiones y mecanismos de escalamiento.
- **Planificación inicial:** Desarrollo del cronograma preliminar, identificación de hitos clave y establecimiento de métricas de éxito.
- **Análisis de riesgos preliminar:** Identificación de posibles obstáculos y desarrollo de estrategias de mitigación.

6.1.2 Fase de Diseño

Durante esta fase se definen todos los aspectos técnicos de la solución:

- **Diseño de arquitectura detallada:** Especificación técnica completa de todos los componentes de la solución Houndoc, incluyendo configuraciones específicas y dimensionamiento.
- **Diseño de seguridad:** Definición de políticas de seguridad, controles de acceso, estrategias de cifrado y mecanismos de protección.
- **Planificación de integraciones:** Desarrollo de la estrategia detallada para la integración con sistemas existentes como Prisma y el directorio activo LDAP.
- **Diseño de pruebas:** Elaboración de planes de prueba para cada componente y para la solución integrada.

6.1.3 Fase de Implementación

Esta fase se ejecuta de manera iterativa, dividiendo el trabajo en sprints de dos semanas:

- **Sprint 1-2: Configuración base de Houndoc:** Implementación de la plataforma base, configuración de componentes de red y seguridad básica.
- **Sprint 3-4: Entornos de trabajo virtuales:** Configuración de espacios de trabajo virtuales en Houndoc y personalización según roles de usuario.
- **Sprint 5-6: Almacenamiento y respaldo:** Implementación de repositorios seguros, estrategias de respaldo y políticas de retención.
- **Sprint 7-8: Integración:** Conexión con sistemas existentes como Prisma, manteniendo los flujos de trabajo.

6.1.4 Fase de Integración y Pruebas

Esta fase crítica se ejecuta siguiendo un enfoque metodológico específico para permitir la calidad:

- **Pruebas de integración:** Validación de la correcta interoperabilidad entre Houndoc y los sistemas a integrar.
- **Pruebas de seguridad:** Verificación de todos los controles de seguridad implementados.
- **Pruebas de rendimiento:** Evaluación del comportamiento del sistema bajo diferentes cargas de trabajo.
- **Pruebas de aceptación:** Validación con usuarios finales para confirmar que la solución cumple con los requisitos establecidos.

6.1.5 Fase de Estabilización

Esta fase permite que la solución funcione de manera óptima antes de su entrega final:

- **Pruebas de carga:** Validación del rendimiento del sistema bajo condiciones de uso intensivo, simulando acceso simultáneo de múltiples usuarios.
- **Resolución de incidencias:** Identificación y corrección de cualquier problema detectado durante las pruebas.
- **Documentación técnica:** Finalización de toda la documentación necesaria para la operación y mantenimiento del sistema.

6.1.6 Fase de Cierre

Esta fase final formaliza la entrega de la solución:

- **Capacitación completa:** Formación al personal técnico del Icfes en todos los aspectos de la administración y operación de los entornos virtuales en Houndoc.
- **Transferencia de conocimiento:** Sesiones específicas para permitir que el equipo del Icfes comprenda todos los aspectos de la solución implementada.
- **Entrega de documentación:** Provisión de manuales técnicos, guías de usuario, procedimientos operativos y documentación de arquitectura.
- **Cierre formal:** Aceptación final del proyecto por parte del Icfes y establecimiento de los mecanismos de soporte post-implementación.

6.2 Gestión del proyecto

Para permitir una ejecución efectiva, se implementarán los siguientes mecanismos de gestión:

- **Reuniones semanales de seguimiento:** Sesiones estructuradas con el equipo del Icfes para revisar avances, discutir problemas y planificar las siguientes actividades.
- **Informes de estado periódicos:** Documentos formales que detallan el progreso, riesgos, problemas y próximos pasos, distribuidos cada mes.
- **Gestión de cambios:** Proceso formal para evaluar, aprobar e implementar cualquier modificación al alcance original, permitiendo la trazabilidad y control de impactos.
- **Gestión de riesgos activa:** Identificación continua de posibles riesgos, evaluación de su impacto y probabilidad, y desarrollo de estrategias de mitigación.

6.3 Control de calidad

La calidad se habilitará mediante:

- **Revisiones técnicas periódicas:** Evaluaciones formales de los componentes implementados para verificar el cumplimiento de estándares y requisitos.
- **Pruebas continuas:** Validación de cada componente a medida que se implementa, sin esperar a la integración completa.
- **Validaciones de seguridad:** Verificaciones específicas para permitir que todos los controles de seguridad funcionen según lo esperado.
- **Auditorías internas:** Revisiones independientes para verificar el cumplimiento de los procesos y estándares establecidos.
- **Gestión de la configuración:** Control estricto de versiones y cambios en todos los componentes de la solución.

Esta metodología estructurada pero flexible permitirá una implementación exitosa de los entornos de trabajo virtuales seguros basados en Houndoc para el Banco de Items, habilitando que se cumplan todos los objetivos técnicos y de negocio mientras se minimiza el impacto en las operaciones diarias del Icfes.

7. Cronograma

El proyecto de habilitación de entornos de trabajo virtuales seguros para el Banco de Items utilizando Houndoc como plataforma SaaS se desarrollará siguiendo un cronograma estructurado en 14 meses, con actividades específicas distribuidas estratégicamente para permitir una implementación ordenada y exitosa. A continuación, se presenta el cronograma detallado según la planificación definida:

Actividad	M1	M2	M3	M4	M5	M6
Planeación						
Plataforma Base						
Entornos Virtuales						
Configuración de Aplicaciones						
Seguridad y monitoreo						
Transferencia de Conocimiento						
Soporte						
Cloud						

7.1 Distribución de actividades por mes

Mes 1:

- Planeación detallada del proyecto
- Implementación de la plataforma base Houndoc
- Configuración inicial de la seguridad
- Configuración inicial de entornos virtuales de trabajo

Mes 2:

- Configuración de seguridad y monitoreo
- Personalización de entornos virtuales según roles
- Integración con sistemas existentes
- Transferencia de conocimiento inicial al equipo técnico del Icfes

Meses 3-6:

- Soporte continuo post-implementación
- Monitoreo del rendimiento de la solución
- Resolución de incidencias
- Capacitación continua a usuarios

7.2 Actividades principales y su distribución temporal

1. Planeación (Mes 1)

- Definición detallada del alcance
- Establecimiento de la gobernanza del proyecto
- Análisis detallado de requisitos técnicos
- Diseño de la arquitectura de entornos virtuales con Houndoc

2. Plataforma Base (Mes 1)

- Configuración del entorno base de Houndoc
- Implementación de servicios de red (VPN)

- Configuración inicial de seguridad (IAM, SSO)
- Implementación de servicios de almacenamiento
- Configuración de sistemas de respaldo

3. Entornos Virtuales (Mes 1)

- Configuración de espacios de trabajo virtuales en Houndoc
- Definición de perfiles según roles de usuario
- Asignación de recursos según necesidades de cada perfil
- Pruebas iniciales de rendimiento

4. Configuración de Aplicaciones (Mes 2)

- Instalación de aplicaciones necesarias (Suite de Adobe)
- Configuración de acceso a Prisma
- Implementación de herramientas de colaboración
- Pruebas de rendimiento y funcionalidad

5. Seguridad y Monitoreo (Mes 2)

- Implementación de controles de seguridad
- Configuración de sistemas de monitoreo
- Implementación de auditoría y registro
- Configuración de alertas y notificaciones
- Pruebas de seguridad

6. Transferencia de Conocimiento (Mes 2)

- Capacitación al personal de tecnología del Icfes
- Entrega de documentación técnica
- Sesiones prácticas de administración y operación
- Documentación de procedimientos operativos

7. Soporte (Meses 3-6)

- Soporte técnico continuo
- Resolución de incidencias
- Acompañamiento en la operación
- Capacitación continua a nuevos usuarios
- Implementación de mejoras identificadas

7.3 Consideraciones sobre el cronograma

- **Implementación concentrada:** Las actividades principales de implementación técnica se concentran en los dos primeros meses, permitiendo una puesta en marcha rápida de la solución y minimizando el impacto en las operaciones del Banco de Items.

- **Soporte extendido:** Se contempla un período de soporte de un (1) mes posterior a la implementación para permitir la estabilidad de la solución, así como la adopción efectiva por parte de los usuarios.
- **Paralelización de actividades:** Durante el primer mes se desarrollarán varias actividades en paralelo para optimizar tiempos de implementación, aprovechando las capacidades de la plataforma Houndoc para configurar simultáneamente diferentes componentes.
- **Transferencia de conocimiento temprana:** La capacitación al equipo del Icfes se realizará tan pronto como la implementación técnica esté completada, permitiendo una transición fluida hacia la gestión autónoma de la plataforma.
- **Mejora continua:** El cronograma incluye períodos de revisión a lo largo la vigencia del soporte, permitiendo ajustar la solución según los comentarios de los usuarios y las necesidades emergentes.

Este cronograma está diseñado para proporcionar una implementación eficiente y un soporte continuo, permitiendo que el Banco de Items pueda operar de manera óptima en los nuevos entornos virtuales seguros basados en Houndoc desde etapas tempranas del proyecto.

8. Metodología de soporte y mantenimiento

Tras la implementación exitosa de los entornos de trabajo virtuales seguros para el Banco de Items utilizando la plataforma Houndoc, se establece un modelo integral de soporte y mantenimiento diseñado para permitir la continuidad operativa y responder eficazmente ante cualquier incidencia. Esta metodología se estructura en tres componentes principales:

8.1 Soporte y mantenimiento correctivo

El equipo de soporte se encargará de atender y corregir los incidentes que se presenten en el uso de los entornos virtuales implementados:

- **Registro de solicitudes:** Toda solicitud deberá ser reportada a través de la herramienta de gestión de incidentes en horario 5x8, incluyendo la información necesaria para diagnosticar el problema.
- **Admisión y clasificación:** Las solicitudes serán evaluadas y clasificadas según su tipo, impacto y prioridad para determinar los tiempos de solución acorde a los ANS definidos:
 - **Prioridad Alta:** Incidentes que impiden completamente el acceso o uso de los entornos virtuales
 - **Prioridad Media:** Problemas que afectan parcialmente la funcionalidad pero permiten seguir trabajando

- **Prioridad Baja:** Consultas, mejoras o problemas menores que no afectan la operación
- **Diagnóstico y solución:** El diagnóstico se efectuará mediante análisis de logs, búsqueda en base de conocimiento, conexión remota o desplazamiento a instalaciones según sea necesario.
- **Acuerdos de nivel de servicio (ANS):**
 - **Tiempo de atención:** Máximo cuatro (4) horas para todos los incidentes
 - **Tiempo de solución:**
 - Prioridad Alta: Máximo seis (6) horas
 - Prioridad Media: Máximo doce (12) horas
 - Prioridad Baja: Máximo veinticuatro (24) horas
 - En casos de mayor complejidad, se coordinará el tiempo de solución con la entidad
- **Verificación y cierre:** Toda solución será verificada internamente antes de su envío y el cliente dispondrá de cinco (5) días hábiles para validar la solución, tras lo cual se procederá al cierre del incidente.

8.2 Soporte y mantenimiento preventivo

Para habilitar el óptimo funcionamiento de los entornos virtuales implementados:

- **Actividades programadas:**
 - Evaluación del rendimiento de los entornos virtuales
 - Verificación de uso de recursos (CPU, memoria, almacenamiento)
 - Actualizaciones de la plataforma Houndoc
 - Actualizaciones de seguridad
 - Pruebas de funcionalidad de integraciones
- **Periodicidad:** Los mantenimientos preventivos se realizarán bimestralmente, con posibilidad de mantenimientos extraordinarios cuando exista necesidad técnica.
- **Ventanas de mantenimiento:** Se programarán en coordinación con el Icfes para minimizar el impacto en la operación, preferentemente en horarios no laborales o de baja actividad.
- **Documentación:** Se mantendrá un registro detallado de todas las actividades realizadas y se generarán informes que documenten los cambios, pruebas y resultados obtenidos.

8.3 Soporte y mantenimiento evolutivo

Para atender las necesidades de mejora y adaptación de la solución:

- **Identificación de necesidades:** Recopilación y análisis de solicitudes de cambios o mejoras, evaluando su impacto y viabilidad técnica.
- **Priorización y planificación:** Clasificación de solicitudes según criticidad y valor, definiendo alcance, recursos y plazos estimados.
- **Implementación:** Diseño, desarrollo, pruebas y despliegue de nuevas funcionalidades o ajustes siguiendo las mejores prácticas.
- **Documentación y capacitación:** Actualización de la documentación técnica y material de capacitación para los usuarios.
- **Tipos de evoluciones:**
 - **Mejoras funcionales:** Nuevas características o capacidades para los entornos virtuales
 - **Adaptaciones tecnológicas:** Actualizaciones para mantener compatibilidad con nuevas versiones de software
 - **Escalamiento:** Ampliación de recursos o capacidades según el crecimiento de las necesidades

8.4 Canales de atención y escalamiento

Para facilitar la comunicación y gestión de incidentes, se establecen múltiples canales:

- **Sistema de tickets:** Plataforma centralizada para el registro y seguimiento de incidentes, accesible 24/7.
- **Correo electrónico dedicado:** Canal directo para reportar incidentes o consultas, monitoreado durante el horario de soporte.
- **Línea telefónica de soporte:** Para situaciones que requieran atención inmediata, disponible en horario laboral.

Se establecerá una matriz de escalamiento con niveles claramente definidos para permitir la resolución oportuna de incidencias según su criticidad:

- **Nivel 1:** Soporte inicial, resolución de problemas básicos
- **Nivel 2:** Especialistas en la plataforma Houndoc
- **Nivel 3:** Expertos técnicos y desarrolladores
- **Nivel 4:** Gerencia de proyecto y dirección técnica

8.5 Informes y documentación

Para mantener la transparencia y seguimiento del servicio:

- **Informes de incidentes:** Dentro de las 72 horas siguientes al cierre de cada incidencia, detallando el problema, diagnóstico, solución implementada y recomendaciones.
- **Informes mensuales:** Detallando las actividades de soporte y mantenimiento realizadas, incluyendo:
 - Estadísticas de incidentes (cantidad, tipo, tiempo de resolución)
 - Resultados de actividades preventivas
 - Uso de recursos y rendimiento
 - Recomendaciones de mejora
- **Informe de cierre:** Al finalizar el período de soporte contratado, con un análisis completo del servicio prestado y recomendaciones para el futuro.
- **Base de conocimiento:** Documentación actualizada de problemas comunes y sus soluciones, accesible para el equipo técnico del Icfes.

Esta metodología de soporte y mantenimiento está diseñada para permitir que los entornos de trabajo virtuales seguros basados en Houndoc para el Banco de Items operen de manera óptima, segura y confiable, minimizando el impacto de posibles incidencias y permitiendo la evolución continua de la plataforma para adaptarse a las necesidades futuras del Icfes.

10. Garantía

La garantía para el proyecto de habilitación de entornos de trabajo virtuales seguros para el Banco de Items utilizando Houndoc como plataforma SaaS se ha diseñado para proporcionar al Icfes la tranquilidad y respaldo necesarios respecto al funcionamiento adecuado de la solución implementada. A continuación, se detallan los términos y condiciones de la garantía:

10.1 Cobertura de la garantía

La garantía cubre los siguientes aspectos de la solución implementada:

1. **Funcionamiento de la plataforma Houndoc:** La garantía abarca el correcto funcionamiento de todos los componentes de la plataforma Houndoc configurados para el proyecto, incluyendo los entornos virtuales, sistemas de almacenamiento, mecanismos de seguridad y herramientas de colaboración.
2. **Integridad de datos:** La garantía incluye la verificación de que la información almacenada en los entornos virtuales mantiene su integridad y consistencia durante su uso normal.
3. **Configuración de seguridad:** La garantía contempla que los mecanismos de seguridad implementados operen correctamente según las

especificaciones acordadas, incluyendo controles de acceso, cifrado y auditoría.

4. **Entornos virtuales de trabajo:** Se incluye el correcto funcionamiento de los entornos virtuales configurados para los usuarios del Banco de Items, incluyendo el acceso a las aplicaciones instaladas.
5. **Integración con sistemas existentes:** Se incluye la correcta integración con la plataforma Prisma y el directorio institucional, permitiendo la interoperabilidad entre los diferentes componentes.

10.2 Período de garantía

- La garantía tendrá una vigencia de seis (6) meses contados a partir de la fecha de entrega final y aceptación formal del proyecto por parte del Icfes.
- Durante este período, cualquier defecto o mal funcionamiento atribuible a la implementación será corregido sin costo adicional para el Icfes.

10.3 Servicios incluidos en la garantía

Durante el período de garantía, se proporcionarán los siguientes servicios sin costo adicional:

1. **Corrección de errores:** Resolución de cualquier defecto o mal funcionamiento atribuible a la implementación realizada.
2. **Ajustes de configuración:** Modificaciones necesarias en la configuración de Houndoc o los entornos virtuales para corregir problemas detectados.
3. **Soporte técnico:** Atención a consultas y resolución de dudas relacionadas con la solución implementada.
4. **Documentación actualizada:** Actualización de la documentación técnica cuando sea necesario como resultado de correcciones realizadas.

10.4 Tiempos de respuesta durante la garantía

Los tiempos de respuesta y resolución durante el período de garantía serán los mismos establecidos en los Acuerdos de Nivel de Servicio (ANS) definidos en la sección de Metodología de Soporte y Mantenimiento:

- **Tiempo de atención:** Máximo cuatro (4) horas.
- **Tiempo de solución:**
 - Prioridad Alta: Máximo seis (6) horas
 - Prioridad Media: Máximo doce (12) horas
 - Prioridad Baja: Máximo veinticuatro (24) horas

Para casos de mayor complejidad, se coordinará el tiempo de solución específico con el Icfes.

10.5 Proceso para reportar incidentes bajo garantía

1. Los incidentes deberán ser reportados a través de la herramienta de gestión de incidentes proporcionada.
2. Cada reporte debe incluir la descripción detallada del problema, evidencias (capturas de pantalla, logs) y pasos para reproducirlo.
3. Se asignará un número de caso para seguimiento.
4. Se notificará al Icfes una vez resuelto el incidente para su verificación y aprobación.

10.6 Limitaciones de la garantía

La garantía no cubre los siguientes aspectos:

1. **Problemas causados por uso indebido:** Daños o mal funcionamiento resultantes del uso inadecuado de la plataforma por parte de los usuarios.
2. **Modificaciones no autorizadas:** Problemas derivados de cambios realizados en la configuración sin previa coordinación con el equipo de soporte.
3. **Fallas en infraestructura no gestionada:** Problemas originados en componentes o sistemas que no forman parte del alcance del proyecto.
4. **Causas de fuerza mayor:** Interrupciones o fallos causados por eventos fuera del control razonable, como desastres naturales o interrupciones masivas del servicio de AWS.
5. **Defectos en software de terceros:** Problemas inherentes a productos de software de terceros que no fueron desarrollados o modificados como parte del proyecto, como la suite de Adobe u otras aplicaciones instaladas en los entornos virtuales.

10.7 Condiciones para mantener la validez de la garantía

Para mantener la validez de la garantía, el Icfes deberá:

1. Utilizar la plataforma Houndoc y los entornos virtuales de acuerdo con las instrucciones y recomendaciones proporcionadas.
2. No realizar modificaciones en la configuración sin previa coordinación con el equipo de soporte.
3. Permitir la implementación de actualizaciones de seguridad críticas cuando sean recomendadas.
4. Reportar oportunamente cualquier anomalía detectada en el funcionamiento de la plataforma.
5. Mantener activos los servicios de soporte y mantenimiento contratados.

Esta garantía representa nuestro compromiso con la calidad y confiabilidad de la solución implementada, apoyando al Icfes en la operación de sus entornos de trabajo virtuales seguros para el Banco de Items durante el período establecido.

11. Supuestos

Para la exitosa ejecución del proyecto de habilitación de entornos de trabajo virtuales seguros para el Banco de Items utilizando Houndoc como plataforma SaaS, se han identificado los siguientes supuestos fundamentales que constituyen la base para el desarrollo de la propuesta técnica y económica presentada. Estos supuestos definen el marco operativo y las condiciones necesarias para alcanzar los objetivos establecidos:

11.1 Acceso a Fuentes de Datos

- El Icfes proporcionará acceso oportuno a la información necesaria sobre los procesos actuales del Banco de Items para permitir la correcta configuración de los entornos virtuales.
- Se dispondrá de la documentación existente sobre la estructura de datos, carpetas y permisos actuales para facilitar la replicación de estos en los entornos virtuales.
- El Icfes facilitará los detalles de integración necesarios para la conexión con la plataforma Prisma y el directorio institucional.

11.2 Infraestructura y Conectividad

- El Icfes cuenta con la conectividad de red adecuada para soportar el acceso de los usuarios a los entornos virtuales en Houndoc, con un ancho de banda mínimo de 10 Mbps por usuario concurrente.
- Se dispone de los mecanismos necesarios para establecer conexiones seguras entre las instalaciones del Icfes y la plataforma Houndoc.
- Los equipos de los usuarios finales cumplen con los requisitos mínimos para acceder a los entornos virtuales (navegador actualizado, capacidad de ejecutar el cliente de Houndoc).
- El Icfes proporcionará acceso a su infraestructura de red actual para configurar las integraciones necesarias.

11.3 Sistemas Existentes e Integraciones

- La plataforma Prisma cuenta con interfaces o mecanismos documentados que permiten su integración con Houndoc para mantener los flujos de trabajo actuales.
- El directorio institucional existente puede integrarse con los mecanismos de autenticación de Houndoc para la gestión centralizada de identidades.
- Las aplicaciones utilizadas actualmente en el Banco de Items son compatibles con entornos virtuales en Houndoc o existen alternativas viables.

11.4 Licenciamiento y Software

- El Icfes cuenta con las licencias necesarias para la suite de Adobe que debe ser instalada en los entornos virtuales, o está dispuesto a adquirirlas como parte del proyecto.
- El Icfes autoriza la instalación y configuración del software requerido en los entornos virtuales de Houndoc.
- Las licencias de software existentes permiten su uso en entornos virtuales o pueden ser transferidas a estos sin costo adicional.

11.5 Recursos Humanos y Participación

- El Icfes designará un líder de proyecto con capacidad de toma de decisiones y disponibilidad para coordinar actividades durante toda la duración del proyecto.
- El personal técnico del Icfes estará disponible para participar en sesiones de levantamiento de información, validación de diseños y pruebas de aceptación.
- Los usuarios clave del Banco de Items participarán en las pruebas de funcionalidad para validar que los entornos virtuales cumplen con sus necesidades operativas.
- El Icfes proporcionará acceso a los usuarios finales para las sesiones de capacitación y adopción de la solución.

11.6 Procesos Operativos

- Los procesos actuales de trabajo del Banco de Items están documentados o pueden ser explicados detalladamente por el personal responsable.
- El Icfes proporcionará información sobre las políticas de seguridad específicas que deben aplicarse en los entornos virtuales.
- Se cuenta con procedimientos establecidos para la gestión de cambios y actualizaciones en el entorno productivo.

11.7 Ventanas de Tiempo

- El Icfes facilitará ventanas de tiempo adecuadas para realizar actividades que puedan impactar la operación, como pruebas con usuarios y capacitaciones.
- Se dispondrá de acceso a los sistemas durante horarios no laborales cuando sea necesario para actividades críticas que no puedan realizarse durante la jornada normal.
- Los usuarios finales tendrán disponibilidad para participar en las sesiones de capacitación programadas.

11.8 Cambios en el Alcance

- Cualquier modificación significativa en los requisitos o el alcance después de la aprobación de la propuesta será gestionada mediante un proceso formal de control de cambios y podría implicar ajustes en tiempos y costos.
- La adición de usuarios o entornos virtuales más allá de los 30 inicialmente contemplados se considerará un cambio de alcance.

11.9 Limitaciones Conocidas

- Se reconoce que pueden existir aplicaciones específicas que requieran adaptaciones para funcionar correctamente en los entornos virtuales de Houndoc.
- La experiencia de usuario en los entornos virtuales puede variar ligeramente respecto al uso directo de aplicaciones instaladas localmente, especialmente en operaciones que requieren alto rendimiento gráfico.
- El rendimiento de los entornos virtuales dependerá en parte de la calidad de la conexión a internet disponible en las instalaciones del Icfes y en las ubicaciones remotas de los usuarios.

Es importante destacar que estos supuestos han sido establecidos con base en la información disponible al momento de elaborar esta propuesta. Si durante la ejecución del proyecto se identificara que alguno de estos supuestos no se cumple, se evaluará el impacto correspondiente y se propondrán las medidas de mitigación necesarias, lo cual podría implicar ajustes en el alcance, cronograma o costos del proyecto.

COMWARE NO HACE PARTE DE ESE SEGMENTO

Bogotá D.C., 6 de noviembre de 2025.

Señores

Instituto Colombiano para la Evaluación de la Educación - ICFES

REF: RFQ - SG - OTRO - BANCO DE ITEMS - Evento 201526

Respetados Señores,

Por medio de la presente, le agradecemos su interés en los servicios que nuestra compañía ofrece. Sin embargo, en atención a su solicitud, **"RFQ - SG - OTRO - BANCO DE ITEMS - Evento 201526"** le informamos que el servicio solicitado, "Houndoc 1 US Dolar Procesamiento Nube." y los demás servicios mencionados en el RFQ, no forman parte del catálogo de productos y servicios actualmente disponibles en nuestra empresa.

Lamentablemente, no podemos dar curso a su solicitud en los términos planteados. No obstante, estamos a su disposición para ofrecerle alternativas que se ajusten a sus necesidades y a los servicios que sí ofrecemos. Si lo desea, podemos proporcionarle información adicional sobre otras opciones que podrían ser de su interés.

Le agradecemos su comprensión y quedamos atentos a cualquier consulta adicional que pueda surgir.

Cordialmente,

INDRA COLOMBIA S.A.S
NIT 830.013.774-1

**REDNEET NO HACE PARTE DEL TIPO DE SOLUCIONES, NUESTRO
PORTAFOLIO EN CCE ES TDWIIT Y MANAGE ENGINE**



Bogotá, 5 de noviembre 2025

Señores

ICFES

Dirección

Ref: Respuesta a la Solicitud del evento **RFQ 201526 - Instrumento de Agregación de Demanda de Software por Catálogo II.**

Asunto:

Estimados señores:

En respuesta a la solicitud de respuesta al evento **RFQ 201526** para el instrumento de agregación de demanda de software por catálogo, con número de referencia **RFQ 201526** queremos agradecerles por considerarnos como posibles proveedores.

Después de una cuidadosa evaluación de los requisitos técnicos y funcionales solicitados, lamentamos informarles que, en este momento, **Xertica Colombia SAS** no cuenta con el software específico que cumple con todas las especificaciones detalladas en la convocatoria.

Actualmente no contamos con los desarrollos tecnológicos necesarios para satisfacer las necesidades particulares de este proyecto.

Agradecemos nuevamente la oportunidad de participar en este proceso y les deseamos éxito en la búsqueda de un proveedor que se ajuste a sus requerimientos.

Quedamos a su disposición para cualquier consulta adicional.

Atentamente,

Xertica Colombia SAS



REGISTRO PRESUPUESTAL
SECRETARÍA GENERAL
SUBDIRECCIÓN FINANCIERA Y CONTABLE


Programa EBS
Usuario MVESCOBARC
Fecha 11-NOV-25
Hora 17:34:51

Página 1 de 1

INFORMACIÓN BASICA						
Fecha	11-NOV-25	Estado:	ASIGNADO	No. RP	16021	
Beneficiario	900718336 - HIGH TECH SOFTWARE S. A. S			Valor. RP	\$632,065,298.00	
Descripción	Cto 654-2025- OC 155127- Contratar una solución SaaS para el Icfes enfoca en la habilitación de entornos de trabajo virtuales seguros para el (...) Plazo 31 diciembre 2025					
Supervisor	Subdirector de información					
Certificado	Disponibilidad No.	15579	Fecha	10-OCT-25	Valor. CDP	\$ 632,068,660.00
INFORMACIÓN DE VIGENCIAS FUTURAS						
Vigencias Futuras		Año		Valor		

INFORMACIÓN DE AFECTACIÓN PRESUPUESTAL						
RUBRO	DESCRIPCION RUBRO	RECURSO	ÁREA	PROYECTO	PRODUCTO	VALOR
2025825320202008003011	SERVICIOS DE CONSULTORÍA EN ADMINISTRACIÓN Y SERVICIOS DE GESTIÓN		SDINFOR	10000081	211110013	632,065,298.00

Total Compromiso :	\$632,065,298.00
--------------------	------------------


Elaboró:


Subdirector Financiero y Contable:

Recibido Por:

No. PÓLIZA	NB-100416570	No. ANEXO	0	No. CERTIFICADO	72663812	No. RIESGO	
TIPO DE DOCUMENTO		FECHA DE EXPEDICIÓN	13/11/2025	SUC. EXPEDIDORA	BOGOTA		
VIGENCIA DESDE	VIGENCIA HASTA	DÍAS	VIGENCIA DEL CERTIFICADO DESDE	VIGENCIA DEL CERTIFICADO HASTA			
00:00 Horas Del	11/11/2025	24:00 Horas Del	31/12/2028	N/A	N/A	N/A	N/A

CONDICIONES PARTICULARES

solicitar la exclusión de alguno estos canales por medio de:
Página web: www.segurosmundial.com.co
Correo electrónico: mundial@segurosmundial.com.co
Líneas de atención: Bogotá (+601) 3274712 - (+601) 3274713 Nacional 018000111935"



**Condiciones generales de la
póliza de seguro de cumplimiento ante
entidades públicas con régimen
privado de contratación**



Condiciones generales de la
póliza de seguro de cumplimiento ante
**entidades públicas con régimen
privado de contratación**



C O N T E N I D O

	Pág.
1. AMPAROS	4
1.1. Seriedad de los ofrecimientos	4
1.2. Amparo de buen manejo y correcta inversión del anticipo	5
1.3. Amparo de devolución de pagos anticipados	5
1.4. Amparo de cumplimiento del contrato	5
1.5. Amparo de pago de salarios, prestaciones sociales legales e indemnizaciones laborales	5
1.6. Amparo de estabilidad y calidad de obra	6
1.7. Amparo de calidad de elementos, bienes y equipos que entregue el contratista	6
1.8. Amparo de calidad del servicio	6
1.9. Amparo de provisión de repuestos	6
1.10. Otros amparos	6
2. EXCLUSIONES	7
3. TÉRMINO DEL AMPARO	8
4. VALOR ASEGURADO	8
5. SINIESTROS	8
5.1. Aviso	8
5.2. Cuantía y ocurrencia	8
5.3. Oportunidad para el pago de la prestación asegurada	11
5.4. Compensaciones	11
5.5. No proporcionalidad	11
5.6. Proporcionalidad de la cláusula penal	11
6. INOPONIBILIDAD	11



Condiciones generales de la
póliza de seguro de cumplimiento ante
**entidades públicas con régimen
privado de contratación**



C O N T E N I D O

	Pág.
7. CESIÓN	12
8. PROCESOS CONCURSALES Y PRECONCURSALES	12
9. ARBITRAMENTO	12
10. PRESCRIPCIÓN EXTINTIVA DE LOS DERECHOS DERIVADOS DEL CONTRATO DE SEGURO	12
11. SUBROGACIÓN	12
12. RENOVACIÓN UNILATERAL	13
13. DOMICILIO DEL CONTRATO	13



CONDICIONES GENERALES DE LA PÓLIZA DE SEGURO DE CUMPLIMIENTO ANTE ENTIDADES PÚBLICAS CON RÉGIMEN PRIVADO DE CONTRATACIÓN

Compañía Mundial de Seguros S.A., en adelante denominada la aseguradora, expide el presente contrato de seguro, sujeto a estas condiciones generales, las cuales están debidamente depositadas en la superintendencia financiera de Colombia y a las condiciones particulares que se delimitan en su alcance y vigencia según los amparos otorgados en forma expresa en la caratula del seguro, conforme a lo normado en el artículo 1047 del código de comercio.



1. AMPAROS

1.1. SERIEDAD DE LOS OFRECIMIENTOS

La aseguradora cubre a la entidad por las sanciones impuestas al proponente como consecuencia del incumplimiento de las obligaciones establecidas en el pliego de condiciones, los términos de la referencia, el estudio previo y/o las reglas de participación, que sean imputables a su responsabilidad, en los siguientes eventos:

- 1.1.1. La no suscripción del contrato sin justa causa por parte del proponente seleccionado.
- 1.1.2. La no ampliación de la vigencia de la garantía de seriedad de la oferta cuando el termino previsto en el pliego de condiciones, los términos de referencia, el estudio previo y/o las reglas de participación, se prorrogue o cuando el termino previsto para la suscripción del contrato se prorrogue, siempre y cuando esas prorrogas no excedan un término de tres (3) meses.
- 1.1.3. El retiro de la oferta después de vencido el termino fijado para la presentación de las propuestas.
- 1.1.4. La falta de otorgamiento por parte del proponente seleccionado de la garantía de cumplimiento exigida por la entidad para amparar el incumplimiento de las obligaciones del contrato.



1.2. AMPARO DE BUEN MANEJO Y CORRECTA INVERSIÓN DEL ANTICIPO

Se cubre a la entidad asegurada contra los perjuicios imputables al contratista derivados de la no inversión, uso indebido, apropiación indebida de las sumas en dinero o especie que sean entregadas en calidad de anticipo. Se entiende que ello ha ocurrido cuando los bienes o dinero no se han aplicado o utilizado en el desarrollo del contrato o en las obligaciones a cargo del contratista.

Cuando se trate de bienes entregados en calidad de anticipo, estos deberán tasarse en dinero previamente en el contrato.

1.3. AMPARO DE DEVOLUCIÓN DE PAGOS ANTICIPADOS

Se cubre a la entidad asegurada contra los perjuicios imputables al contratista derivados del no reintegro de las sumas de dinero o especie que sean entregadas en calidad de pago anticipado y que el contratista no devuelva a la entidad.

En caso de cumplimiento parcial de las obligaciones, se estimará la proporción de la parte cumplida del contrato, para descontarla de la indemnización.

1.4. AMPARO DE CUMPLIMIENTO DEL CONTRATO

El amparo de cumplimiento del contrato cubre los perjuicios directos imputables al contratista, derivados del incumplimiento de las obligaciones adquiridas por el contratista con la suscripción del contrato, y contempla también el cumplimiento tardío, defectuoso o imperfecto de las mismas, así como multas y clausula penal, según se pacten en el contrato.

1.5. AMPARO DE PAGO DE SALARIOS, PRESTACIONES SOCIALES LEGALES E INDEMNIZACIONES LABORALES

El amparo de pago de salarios, prestaciones sociales de origen legal e indemnizaciones laborales, cubre a la entidad en su calidad de contratante, contra los perjuicios imputables al contratista derivados del incumplimiento de las obligaciones a su cargo, derivadas de contratos laborales a que está obligado en su calidad de empleador, incluidas las de pagos de salarios y prestaciones sociales legales, liquidación de contratos de acuerdo a las obligaciones de ley asumidas por el empleador y que guardan relación directa con el personal utilizado en la ejecución del contrato amparado en el territorio nacional y sobre las que el asegurado pudiese resultar solidariamente responsable.



Condiciones generales de la
póliza de seguro de cumplimiento ante
**entidades públicas con régimen
privado de contratación**

1.6 AMPARO DE ESTABILIDAD Y CALIDAD DE OBRA

El amparo de estabilidad y calidad de obra, cubrirá a la entidad contratante, con motivo de los perjuicios que se le ocasionen como consecuencia de cualquier daño o deterioro, generado en condiciones normales de uso y mantenimiento, sufridos por la obra entregada a satisfacción, que resulten imputables al contratista garantizado.

1.7 AMPARO DE CALIDAD DE ELEMENTOS, BIENES Y EQUIPOS QUE ENTREGUE EL CONTRATISTA

El amparo de calidad y correcto funcionamiento de los bienes y equipos suministrados cubrirá al asegurado por los perjuicios imputables al contratista, causados como consecuencia de la mala calidad, la calidad deficiente o desempeño defectuoso de los elementos, bienes y equipos suministrados por el contratista, frente a las especificaciones contenidas en la ley 1480 de 2011 y las normas que la modifiquen, y aquellas adicionales propias del bien, equipo y elemento, así como aquellas que se pacten en el contrato.

1.8 AMPARO DE CALIDAD DEL SERVICIO

El amparo de calidad del servicio cubre los perjuicios imputables al contratista causados por la mala calidad, la calidad deficiente o desempeño defectuoso, frente a las especificaciones que se pacten en el contrato, todos ellos siempre que sean exigibles en la etapa post-contractual, una vez finalice el plazo de ejecución.

1.9. AMPARO DE PROVISIÓN DE REPUESTOS

El amparo de provisión de repuestos cubre los perjuicios imputables al contratista causados por el incumplimiento por no suministrar los repuestos, partes, materiales e insumos necesarios para la reparación y mantenimiento de bienes suministrados por el contratista, frente a las especificaciones que se pacten en el contrato o previstas en la ley en la etapa post-contractual.

1.10 OTROS AMPAROS

Adicionalmente, en la medida en que fueren exigidos por la entidad contratante, la aseguradora podrá otorgar los amparos requeridos para cubrir los demás incumplimientos de obligaciones que la entidad contratante considera deben ser amparados de manera proporcional y acorde a la naturaleza del contrato y que se definan en la carátula o en los anexos que se expidan a la presente póliza



Condiciones generales de la
póliza de seguro de cumplimiento ante
**entidades públicas con régimen
privado de contratación**



2. EXCLUSIONES

Los amparos previstos en la presente póliza no operarán en los siguientes casos:

- 2.1. Causa extraña, esto es la fuerza mayor o caso fortuito, el hecho de un tercero o la culpa exclusiva de la víctima (el asegurado).
- 2.2. En caso de pactarse o imponerse condiciones, cambiar los términos del contrato y no reportarlo debidamente al asegurador y que no sean aceptadas expresamente por él, este quedara relevado del pago de la prestación asegurada, derivada de tales cambios, pactos o modificaciones.
- 2.3. Este seguro no cubre los perjuicios derivados de los reclamos de terceros ajenos al contrato, con ocasión de eventuales responsabilidades de carácter civil extracontractual. Tampoco se cubre la responsabilidad civil de carácter patronal, derivada de accidente de trabajo.
- 2.4. Vicios por transcurso del tiempo. Los perjuicios derivados del simple transcurso del tiempo sobre bienes y objetos.
- 2.5. El uso indebido o inadecuado o la falta de mantenimiento preventivo a que este obligada la entidad contratante.
- 2.6. Terrorismo nuclear, biológico, químico y radioactivo
- 2.7. Riesgos/ataques cibernéticos
- 2.8. Pandemias / epidemias / enfermedades por coronavirus no cubre las pérdidas (múltiples o individuales), reclamaciones, daños a personas o bienes, responsabilidad, la interrupción de las actividades comerciales, la pérdida de beneficios o cualquier gasto consecuente o coste de cualquier naturaleza directa o indirectamente causado por, que surja de, que resulte de o en conexión con, o miedo a una epidemia o pandemia (declarada o no como tal por las autoridades competentes) o enfermedad infecciosa real o percibida incluido pero no limitado a: a) enfermedades por coronavirus (covid-19); b) síndrome respiratorio agudo severo coronavirus 2 (sars-cov-2); c) cualquier variación o mutación. También excluye cualquier pérdida, reclamación, daño a personas o bienes, responsabilidad, la interrupción de las actividades comerciales, la pérdida de beneficios o cualquier gasto consecuente o coste de cualquier naturaleza directa o indirectamente causado por, que surja de, resultante de o en conexión con cualquier acción llevada a cabo o fracaso a la hora de tomar medidas para controlar, prevenir, suprimir dicha epidemia, pandemia o enfermedad infecciosa o cualquier variación o mutación de la misma.



3. TÉRMINO DEL AMPARO

La vigencia de los amparos se registra en la caratula de la póliza. Cuando el contratista o la entidad requieran al asegurador para ampliar la vigencia de la garantía, el asegurador podrá hacerlo, mediante anexo a la póliza, las vigencias podrán ser modificadas de común acuerdo con el asegurador.



4. VALOR ASEGURADO

El valor asegurado para cada uno de los amparos otorgados se registra en la caratula de la póliza. Cuando el contratista o la entidad requieran al asegurador para ampliar el valor asegurado de la garantía, el asegurador podrá hacerlo, mediante anexo a la póliza, las sumas aseguradas podrán ser modificadas de común acuerdo con el asegurador.

En todo caso, las sumas aseguradas para cada amparo constituyen el límite máximo y no se acumulan entre sí, para aumentar el valor asegurado total de la garantía. Lo anterior sin perjuicio de lo dispuesto en el inciso segundo del artículo 1074 del código de comercio.



5. SINIESTROS

5.1. AVISO

La entidad estará obligada a dar noticia al asegurador de la ocurrencia del siniestro, dentro de los diez (10) días hábiles siguientes a la fecha en que lo hayan conocido o debido conocer. Este término podrá ampliarse, más no reducirse por las partes

El asegurador no podrá alegar el retardo o la omisión si, dentro del mismo plazo, interviene en las operaciones de salvamento o de comprobación del siniestro.

5.2. CUANTÍA Y OCURRENCIA

En concordancia con lo normado en el artículo 1077 del código de comercio, la entidad deberá acreditar la ocurrencia del siniestro y la cuantía de la reclamación.

Sin perjuicio de la libertad que tiene la entidad para demostrar la ocurrencia y la cuantía del siniestro, esta se acreditará con la comunicación en la que consta el incumplimiento que resulte del procedimiento establecido para tal fin en el contrato y que se describe a continuación:



Condiciones generales de la
póliza de seguro de cumplimiento ante
**entidades públicas con régimen
privado de contratación**

Procedimiento para declarar el incumplimiento contractual y para exigir el pago de la cláusula penal de apremio y/o clausula penal pecuniaria.

Cuando se presente un posible incumplimiento parcial o total del contrato atribuible al CONTRATISTA respecto de cualquiera de las obligaciones del mismo, LA ENTIDAD, deberá evacuar el siguiente procedimiento para declarar dicho incumplimiento: A) Evidenciado un posible incumplimiento de las obligaciones a cargo de EL CONTRATISTA, según conste en informes elaborados por la Supervisión o la Interventoría, LA ENTIDAD lo citara a él y al GARANTE, mediante comunicación que por escrito se remitirá al domicilio del CONTRATISTA y del GARANTE, a una audiencia para debatir lo ocurrido. LA ENTIDAD, fijara la fecha para realizar la audiencia, como mínimo al quinto día hábil siguiente a la fecha de recepción de la comunicación de citación a audiencia al CONTRATISTA y al GARANTE. En la citación, se hará mención expresa y detallada de los hechos que la soportan y por ello deberá indicar los presuntos incumplimientos contractuales atribuibles al CONTRATISTA, acompañado el informe de la supervisión o interventoría en el que se sustente la actuación y las demás pruebas que soporten la citación y enunciara las normas o clausulas posiblemente violadas y las consecuencias que podrían derivarse para EL CONTRATISTA, de acuerdo con las estipulaciones contractuales. En la misma se establecerá el lugar, fecha y hora para la realización de la audiencia la que deberá tener lugar a la mayor brevedad posible, atendida la naturaleza del contrato y la periodicidad establecida para el cumplimiento de las obligaciones contractuales. B) En desarrollo de la audiencia, el Subgerente de Contratación, presentará las circunstancias de hecho que motivan la actuación contractual, indicará los presuntos incumplimientos contractuales atribuidos al CONTRATISTA, enunciará las posibles normas o clausulas posiblemente violadas y las consecuencias que podrían derivarse para EL CONTRATISTA, según las estipulaciones contractuales. Acto seguido se concederá el uso de la palabra al representante legal del CONTRATISTA o a quien lo represente y al GARANTE, para que ejerzan su derecho de defensa y se pronuncien sobre las imputaciones de incumplimiento, en desarrollo de lo cual podrán rendir las explicaciones del caso, solicitar y aportar pruebas y controvertir las presentadas por la entidad. C) Una vez evacuada la práctica de las pruebas o recibidos los medios probatorios aportados por los interesados, se cerrará la audiencia para que la ENTIDAD mediante decisión contractual motivada que constara por escrito, proceda a resolver sobre la exigibilidad o no de la sanción o declaratoria o no del incumplimiento. Si se resuelve que no hubo incumplimiento, se archivará la actuación contractual. Por el contrario, si se decide que hubo incumplimiento contractual, en el mismo documento, se hará la tasación de la suma a favor de LA ENTIDAD y a cargo del CONTRATISTA y/o EL GARANTE, como consecuencia del incumplimiento de acuerdo con las estipulaciones contractuales. La respectiva decisión, se informará mediante comunicación escrita que se remitirá al domicilio del CONTRATISTA y del GARANTE. EL CONTRATISTA y el GARANTE, podrán presentar por escrito de reconsideración ante LA ENTIDAD, dentro de los cinco (5) días hábiles siguientes a la fecha de adopción de la decisión que declara el incumplimiento contractual. Si declarado este ni EL CONTRATISTA, ni EL GARANTE, presentan el



Condiciones generales de la
póliza de seguro de cumplimiento ante
**entidades públicas con régimen
privado de contratación**

escrito de reconsideración o lo hacen en forma extemporánea, se entenderá que esa decisión se ratifica y se procede para su posterior cobro. La decisión sobre el escrito de reconsideración, si se presenta, será resuelta por LA ENTIDAD por escrito, dentro de los 15(quince) días hábiles siguientes a su recepción y remitida al CONTRATISTA y del GARANTE. El plazo anteriormente descrito podrá ser prorrogado por un término igual al inicialmente pactado. Por el contrato, si se resuelve que no hubo incumplimiento, se comunicara por escrito a los interesados y se archivara la actuación contractual. D) En todo caso, en cualquier momento del desarrollo de la audiencia contractual, el Subgerente de Contratación, podrá suspender la audiencia cuando el oficio o petición de parte, ello resulte en su criterio necesario para allegar o practicar pruebas que estime conducentes y pertinentes, o cuando por cualquier otra razón debidamente sustentada, ello resulte necesario para el correcto desarrollo de la actuación contractual. En todo caso, al adoptar la decisión, se señalará fecha y hora para reanudar la audiencia. LA ENTIDAD podrá ordenar el archivo de la actuación contractual en cualquier momento, si se prueba la cesación de situación de incumplimiento que dio lugar a este procedimiento.

PARÁGRAFO PRIMERO. Plazos para el pago de la obligación económica a cargo del CONTRATISTA y/o garante como consecuencia de la declaratoria de incumplimiento parcial o total. El CONTRATISTA deberá pagar la totalidad de la obligación a su cargo y a favor de LA ENTIDAD, conforme a lo indicado en la decisión de declaratoria de incumplimiento, dentro de los ocho (8) días hábiles siguientes a la fecha de confirmación de la declaratoria de incumplimiento. Cuando el GARANTE, sea una entidad bancaria, deberá pagar la totalidad de la obligación a su cargo y a favor de LA ENTIDAD, conforme a lo indicado en la decisión de declaratoria de incumplimiento, dentro de los ocho (8) días hábiles siguientes a la fecha de confirmación de declaratoria de incumplimiento. Cuando EL GARANTE, sea una compañía de seguros, deberá pagar la totalidad de la obligación a su cargo y a favor de LA ENTIDAD, conforme a lo indicado en la decisión de declaratoria de incumplimiento, dentro del término establecido en el artículo 1080 del Código de Comercio. El plazo para el pago de la obligación económica señalada en la decisión de declaratoria de incumplimiento, se contará a partir de la fecha del recibo de la comunicación escrita respectiva en la que conste la confirmación de la declaratoria de incumplimiento o desde el vencimiento del término para presentar el escrito de reconsideración.

PARÁGRAFO SEGUNDO. Para los efectos del presente contrato, el documento donde conste la declaratoria de incumplimiento contractual parcial o total atribuible al CONTRATISTA, se constituye en la prueba de la ocurrencia y la cuantía del siniestro.

PARÁGRAFO TERCERO. Para efectos de valores a favor de LA ENTIDAD, referentes a cláusula penal de apremio, cláusula penal pecuniaria, cantidades de obra contractuales que no requieran adición de mayores valores contractuales, ajustes posteriores a las actas de obra parciales y/o definitiva, procederá la compensación de los saldos a favor del contratista.



Condiciones generales de la
póliza de seguro de cumplimiento ante
**entidades públicas con régimen
privado de contratación**

5.3. OPORTUNIDAD PARA EL PAGO DE LA PRESTACIÓN ASEGURADA

El asegurador estará obligado a efectuar el pago del siniestro dentro del mes siguiente a la fecha en que la entidad acredite su derecho en la forma prevista en el numeral 5.2 anterior. Vencido este plazo, el asegurador reconocerá y pagará a la entidad, además de la obligación a su cargo y sobre el importe de ella, un interés moratorio igual al certificado como bancario corriente por la superintendencia financiera, aumentado en la mitad.

5.4. COMPENSACIONES

Si la entidad al momento de tener conocimiento del incumplimiento, o en cualquier momento posterior a este y anterior al pago de la indemnización, fuere deudor del contratista garantizado por cualquier concepto, la indemnización se disminuirá en el monto de las acreencias siempre y cuando estas sean objeto de compensación de acuerdo con la ley, de conformidad con lo reglado en los artículos 1714 y siguiente del código civil. Los montos compensados se disminuirán del valor de la indemnización. En aquellos casos en que la aseguradora haya pagado indemnizaciones en virtud de declaratorias de incumplimiento, una vez se inicie la etapa de liquidación del respectivo contrato la entidad deberá comunicar al asegurador si hay saldos a favor del contratista, para los fines que el asegurador estime pertinentes.

5.5. NO PROPORCIONALIDAD

De presentarse incumplimiento parcial de las obligaciones, la indemnización de perjuicios a cargo del asegurador no se tasarán en proporción del valor asegurado equivalente al porcentaje incumplido de la obligación.

5.6. PROPORCIONALIDAD DE LA CLAUSULA PENAL

En virtud de lo previsto en el artículo 1596 del código civil si el contratista cumple solamente una parte de la obligación principal y la entidad acepta esta parte, el primero tendrá derecho a que se rebaje proporcionalmente la pena estipulada en la cláusula penal.



6. INOPONIBILIDAD

A la entidad no le serán oponibles por parte del asegurador las excepciones o defensas provenientes de la conducta del tomador del seguro, en especial las derivadas de las inexactitudes o reticencias en que este hubiere incurrido con ocasión de la contratación del seguro ni en general, cualesquiera otras excepciones que posea el asegurador en contra de la persona garantizada.



7. CESIÓN

Si por incumplimiento del contratista, la aseguradora resolviera continuar con la ejecución del contrato y así lo convenga con la entidad, el contratista acepta desde ahora la cesión del contrato a favor de la aseguradora o de quien ella designe, según el objeto contractual.



8. PROCESOS CONCURSALES Y PRECONCURSALES

La entidad está obligada a hacer valer los derechos que le correspondan en cualquier proceso concursal o preconcursal previsto en la ley, en el que llegare a ser admitido el contratista, en la forma en que debiese hacerlo, aun si no contase con la garantía otorgada por este seguro, y deberá dar el aviso respectivo a la aseguradora. De no cumplir con esta obligación la aseguradora podrá deducir de la indemnización el monto del valor de los perjuicios que le cause dicho incumplimiento tal como lo regula el artículo 1078 del código de comercio.



9. ARBITRAMENTO

En caso de que la aseguradora sea llamada en garantía dentro de un proceso arbitral, con ocasión de una controversia entre el contratista y la entidad, la aseguradora quedará vinculada a los efectos del pacto arbitral suscrito por ellos en los términos del parágrafo primero del artículo 37 de la ley 1563 de 2012 y las normas que la modifiquen reemplacen o adicionen.



10. PRESCRIPCIÓN EXTINTIVA DE LOS DERECHOS DERIVADOS DEL CONTRATO DE SEGURO

LA PRESCRIPCIÓN DE LAS ACCIONES DERIVADAS DE ESTE SEGURO SIGUE LO NORMADO POR EL ARTICULO 1081 DEL CÓDIGO DE COMERCIO Y LAS LEYES QUE LO ADICIONEN, COMPLEMENTEN O MODIFIQUEN ASÍ COMO NORMAS, DISPOSICIONES O LEY ESPECIALES QUE SEAN APLICABLES.



11. SUBROGACIÓN

En virtud del pago de la indemnización, de acuerdo con el artículo 1096 del código de comercio, en concordancia con el artículo 203 del decreto 663 de 1993 – estatuto orgánico del sistema financiero,



Condiciones generales de la
póliza de seguro de cumplimiento ante
**entidades públicas con régimen
privado de contratación**

una vez que la aseguradora pague la indemnización se subrogara por ministerio de la ley y hasta concurrencia de su importe, en los derechos de la entidad contra el contratista o las personas responsables del siniestro.

La entidad no puede renunciar en ningún momento a sus derechos en contra del contratista garantizado y si lo hiciere, perderá el derecho a la indemnización.



12. RENOVACIÓN UNILATERAL

El asegurador renuncia a aplicar la cláusula de revocación unilateral del contrato de seguro.



13. DOMICILIO DEL CONTRATO

Se fija como domicilio del contrato de las partes en este contrato de seguros, la ciudad de Bogotá distrito capital. Lo anterior sin perjuicio de lo que dispongan las normas procesales.

En fe de lo anterior, se firma a los ____ días del mes de _____ de 20 ____.

Firma Autorizada
Compañía Mundial de Seguros S.A.
Angela Munar



COMPAÑÍA MUNDIAL DE SEGUROS S.A.

EL TOMADOR/ASEGURADO



Condiciones generales de la
póliza de seguro de cumplimiento ante

**entidades públicas con régimen
privado de contratación**



LA COMPAÑÍA MUNDIAL DE SEGUROS S.A

CERTIFICA:

Que la garantía de Cumplimiento contenida en la póliza **NB-100416570** y endoso, **0** cuyo afianzado es: **HIGH TECH SOFTWARE SAS** Asegurado o Beneficiario: **INSTITUTO COLOMBIANO PARA LA EVALUACION DE LA EDUCACION-ICFE / INSTITUTO COLOMBIANO PARA LA EVALUACION DE LA EDUCACION-ICFE** , expedida por la Compañía en **13/11/2025**, no expirará por falta de pago de la prima de la póliza o de los certificados o anexos que se expidan con fundamento en ella o por revocación unilateral por parte del Tomador o de la Compañía.

BOGOTÁ a los **14** días del mes **NOVIEMBRE** del año **2025**.



Firma Autorizada
Compañía mundial de Seguros S.A.

LÍNEAS DE ATENCIÓN AL CLIENTE

Bogotá: (+601) 327 47 12/13 | Nacional: 01 8000 111 935 | Sitio Web: www.segurosmondial.com.co



Cumplimos con los sueños de nuestro planeta
reciclando responsablemente. Protege el Medio
Ambiente evitando la impresión de este documento.

@SegurosMundial



- CLIENTE -

Referencia de Pago No.

72663812

Fecha de Facturación

13/11/2025

POLIZA DE SEGURO DE CUMPLIMIENTO
ENTIDADES PUBLICAS REGIMEN PRIVADO DE CONTRATACION

Póliza No.

NB-100416570

Periodo Facturado

11/11/2025

31/12/2028

Fecha Límite de Pago

13/12/2025

Prima (incluye gastos de expedición)

443.463,00

IVA

84.258,00

VALOR TOTAL A PAGAR \$

527.721,00

EFECTIVO

\$

Datos del Cliente

Nombre / Razón Social

HIGH TECH SOFTWARE SAS

CARRERA 7 NO 71-21 PISO 12

900718336

Intermediario

CARRASCO RODRIGUEZ CR CIA

Cheque

Banco

No Cuenta

No Cheque

Valor Cheque

TOTAL

Apreciado Cliente:

1. No se aceptan pagos parciales.
2. Al realizar su pago de forma presencial (ante el cajero del banco) **UNICAMENTE** presente esta boleta de recaudo para garantizar la correcta referenciación del pago.
3. Si esta boleta no ha sido recaudada efectivamente el se aplicará la cláusula de terminación automática especificada en el condicionado de la póliza y en la carátula de esta (artículo 1068 código de comercio)
4. Si realiza su pago en cheque o de forma mixta (efectivo y cheque), solamente gire cheque local a nombre de **PATRIMONIOS AUTÓNOMOS CREDICORP CAPITAL FIDUCIARIA Nit 900531292-7**, al respaldo endóselo correctame y diligencie los datos del girador (nombre, NIT, teléfono) y el número de referencia de esta boleta. En caso de devolución del cheque se cobrará sanción del 20% de acuerdo con lo establecido en el artículo 731 del código de comercio. **NO SE ACEPTAN CHEQUES DE OTRAS PLAZAS.**
5. Para realizar el pago a través del botón PSE, ingrese a nuestra página web www.segurosmundial.com.co en la imagen de PSE haga clic y continúe el proceso de pago.

ESPACIO PARA EL TIMBRE

VÁLIDO COMO RECIBO DE PAGO

- BANCO -

Referencia de Pago No.

72663812

Fecha de Facturación

13/11/2025

POLIZA DE SEGURO DE CUMPLIMIENTO
ENTIDADES PUBLICAS REGIMEN PRIVADO DE CONTRATACION

Póliza No.

NB-100416570

Periodo Facturado

11/11/2025

31/12/2028

Fecha Límite de Pago

13/12/2025

Prima (incluye gastos de expedición)

443.463,00

IVA

84.258,00

VALOR TOTAL A PAGAR \$

527.721,00

EFECTIVO

\$

Datos del Cliente

Nombre / Razón Social

HIGH TECH SOFTWARE SAS

CARRERA 7 NO 71-21 PISO 12

900718336

Intermediario

CARRASCO RODRIGUEZ CR CIA

Cheque

Banco

No Cuenta

No Cheque

Valor Cheque

TOTAL

Corresponsales
OPCIÓN 1

(415)7709998434219(8020)00000072663812(3900)52772100(96)20251213

Bancos
Corresponsales
OPCIÓN 2

(415)7709998039933(8020)031594(8020)229900000072663812(3900)52772100(96)20251213

INFORMACIÓN DE PAGO

A continuación te brindamos información de los distintos medios de pago que tendrás a disposición:


OPCIÓN 1




CORRESPONSALES



OPCIÓN 2



BANCOS





CORRESPONSALES





DATOS DE LA POLIZA

Código de Seguridad	qBt1gLezLhsYLqfNuaLRQ==	Número de póliza	100416570
Número de anexo	0	Ramo	CUMPLIMIENTO - ENTIDADES PUBLICAS REGIMEN PRIVADO DE CONTRATACION
Fecha de expedición	13/11/2025	Inicio de vigencia Global	11/11/2025
Fin de vigencia Global	31/12/2028	Tomador	HIGH TECH SOFTWARE SAS
		Asegurado	INSTITUTO COLOMBIANO PARA LA EVALUACION DE LA EDUCACION-ICFE
Valor asegurado	221.222.854,30		
Movimiento	EXPEDICION		
Objeto de póliza	GARANTIZAR EL PAGO DE LOS PERJUICIOS DERIVADOS DEL INCUMPLIMIENTO DE LAS OBLIGACIONES CONTENIDAS EN EL CONTRATO No.155127 , CUYO OBJETO ES ICFES-654-2025 - CONTRATAR UNA SOLUCIÓN SAAS PARA EL ICFES ENFOCA EN LA HABILITACIÓN DE ENTORNOS DE TRABAJO VIRTUALES SEGUROSPARA EL BANCO DE ITEMS, UTILIZANDO HOUNDOC COMO PLATAFORMA SAAS.		

Amparos

Nombre del Amparo	Vigencia Desde	Vigencia Hasta	Suma Asegurada	Valor Prima
CUMPLIMIENTO	00:00 Horas del 11/11/2025	24:00 Horas del 30/06/2026	\$ 63.206.529,80	\$ 80.004,00
PRESTACIONES SOCIALES	00:00 Horas del 11/11/2025	24:00 Horas del 31/12/2028	\$ 31.603.264,90	\$ 198.451,00
CALIDAD DEL SERVICIO	00:00 Horas del 11/11/2025	24:00 Horas del 30/06/2026	\$ 63.206.529,80	\$ 80.004,00
CALIDAD Y CORRECTO FUNCIONAMIENTO	00:00 Horas del 11/11/2025	24:00 Horas del 30/06/2026	\$ 63.206.529,80	\$ 80.004,00

Esta información debe coincidir con la póliza impresa.
Si es diferente te invitamos a notificarlo al correo mundial@segurosmondial.com.co o también puedes llamar a la línea nacional 01 8000 111 935 - 3274712/13

ACTA DE APROBACIÓN DE GARANTÍAS CONTRACTUALES

En virtud de las facultades conferidas en la Resolución No. 154 del 9 de abril de 2024, el Subdirector de Abastecimiento y Servicios Generales del ICFES

APRUEBA

La garantía contractual contenida en la PÓLIZA DE SEGURO DE CUMPLIMIENTO No. NB-100416570, expedida el 13 de noviembre de 2025 por la COMPAÑÍA MUNDIAL DE SEGUROS S.A., identificada con NIT 860.037.013-6, aportada por el tomador HIGH TECH SOFTWARE S.A.S., identificado con NIT 900.718.336-0, para garantizar el cumplimiento de las obligaciones emanadas de la Orden de Compra No. 155127 del ICFES. (**Contrato ICFES-654-2025**).

Los amparos constituidos son los siguientes:

Amparos	Vigencia desde	Vigencia hasta	Valor asegurado
CUMPLIMIENTO DEL CONTRATO	11/11/2025	30/06/2026	\$63.206.529,80
CALIDAD Y CORRECTO FUNCIONAMIENTO DE LOS BIENES	11/11/2025	30/06/2026	\$63.206.529,80
CALIDAD DEL SERVICIO	11/11/2025	30/06/2026	\$63.206.529,80
PAGO DE SALARIOS, PRESTACIONES SOCIALES LEGALES E INDEMNIZACIONES LABORALES	11/11/2025	31/12/2028	\$31.603.264,90

Los amparos constituidos, sus vigencias y cuantías, se ajustan a lo exigido en el numeral 15.2. “*Garantía a favor de la entidad compradora*” de la minuta del del IAD Software por Catalogo II - CCE-SNG-IAD-002-2024.

Teniendo en cuenta lo anterior, se imparte aprobación a la Garantía antes enunciada el día 13 denoviembre de 2025.



DAVID FERNANDO DÍAZ PALACIO
Subdirector de Abastecimiento y Servicios Generales

Revisó: Víctor Raúl Tovar Méndez – Coordinadora Contractual Subdirección Abastecimiento y Servicios Generales


Proyectó: José Julián Torres Valenzuela - Contratista- Subdirección de Abastecimiento y Servicios Generales

Instituto Colombiano para la Evaluación de la Educación

Edificio Elemento, Ac. 26 #69-76

601 5144370

www.icfes.gov.co

 Icfes	INFORMACIÓN GENERAL DEL CONTRATO AL SUPERVISOR		Código: GAB-FT023
	GESTIÓN DE ABASTECIMIENTO		Versión: 004
Clasificación de la información	<input checked="checked" type="checkbox"/> PÚBLICA	<input type="checkbox"/> CLASIFICADA	<input type="checkbox"/> RESERVADA

De conformidad con la designación de supervisión efectuada en la **orden de compra 155127 – Contrato ICFES-654-2025**, que se suscribió a través de la tienda virtual del Estado Colombiano el día **11 de noviembre de 2025**, le informo que a través del siguiente link <https://operaciones.colombiacompra.gov.co/tienda-virtual-del-estado-colombiano/ordenes-compra/155127> encontrará la información necesaria para el cumplimiento de sus funciones como supervisor.

De igual forma, se recomienda al **Subdirector de Información** tener en cuenta la siguiente información:

No. Contrato	Nombre Contratista	Fecha RP	Fecha Aprobación de Póliza	Fecha afiliación ARL
Orden de compra 155127 ICFES-654-2025	Hightech Software S.A.S.	16021 11/11/2025	13/11/25	N/A

Corresponde a las entidades públicas a través de los supervisores de los contratos que suscribe, vigilar permanentemente la correcta ejecución del objeto contratado.


Los supervisores están facultados para llevar a cabo la vigilancia de la ejecución del contrato, en los términos previstos en el mismo, solicitar a los contratistas informes, aclaraciones y explicaciones sobre el desarrollo de la ejecución contractual, y serán responsables por mantener informado al Icfes de los hechos o circunstancias que puedan afectar la ejecución del contrato.

Por tanto, corresponde al supervisor que en caso de existir riesgo en el cumplimiento del objeto o las obligaciones contractuales, o cuando tal incumplimiento se presente o en caso de mora en su ejecución, informar oportunamente a la Subdirección de Abastecimiento y Servicios Generales y a la Oficina Asesora Jurídica, con el propósito de obtener la asesoría legal necesaria y tomar de manera conjunta las acciones que correspondan, de acuerdo con lo establecido en el contrato.

Por otra parte, en ejercicio de la actividad de supervisión, deberán autorizarse los pagos respectivos previa verificación de los informes de ejecución y los soportes debidos en los cuales se describa detalladamente cada una de las actividades realizadas durante el período, en el formato diseñado para el efecto por parte del Icfes, teniendo en cuenta las particularidades de cada contrato.

El supervisor deberá revisar y analizar los informes antes de certificar el cumplimiento y avalar el pago, los cuales deben reflejar la certeza de las condiciones de ejecución del contrato, anexando los productos o documentos que soporten las actividades del periodo correspondiente, que además sean pertinentes para el efecto.

El supervisor deberá hacer seguimiento en la información que debe ser publicada en la plataforma transaccional de contratos de acuerdo con lo descrito en el Manual de contratación.

 Icfes	INFORMACIÓN GENERAL DEL CONTRATO AL SUPERVISOR		Código: GAB-FT023
	GESTIÓN DE ABASTECIMIENTO		Versión: 004
Clasificación de la información	<input checked="checked" type="checkbox"/> PÚBLICA	<input type="checkbox"/> CLASIFICADA	<input type="checkbox"/> RESERVADA

Modificaciones, prórrogas, cesiones, suspensiones y adiciones contractuales.

Toda modificación planteada por el contratista deberá solicitarse a través del supervisor del contrato, antes de la fecha de vencimiento del plazo del contrato.


Para adelantar las modificaciones contractuales, deben tenerse en cuenta las siguientes recomendaciones:

- Las adiciones deberán contar con disponibilidad presupuestal previa.
- Las modificaciones en tiempo o en valor, implicará ajuste a la garantía única del contrato, respecto de las nuevas condiciones contractuales.
- En caso de cesión, el contratista no podrá ceder total o parcialmente su posición contractual ni los derechos u obligaciones contractuales sin la autorización previa, expresa y escrita del Icfes.
- Para efectos de terminación anticipada, deberá observarse las causales que se encuentran enunciadas en la respectiva cláusula del contrato electrónico.
- Para solicitar la suspensión de los contratos deberá señalarse de forma clara la fecha a partir de la cual se suspende el contrato y la fecha de reanudación del mismo.

Cordialmente,



DAVID FERNANDO DIAZ PALACIO
Subdirector Abastecimiento y Servicios Generales

 Icfes	ACTA DE INICIO PARA CONTRATOS		Código: GAB-FT024
	GESTIÓN DE ABASTECIMIENTO		Versión: 002
Clasificación de la información	<input type="checkbox"/> PÚBLICA	<input type="checkbox"/> CLASIFICADA	<input type="checkbox"/> RESERVADA

CONTRATO:	654-2025
CONTRATANTE:	Instituto Colombiano para la Evaluación de la Educación - ICFES
CONTRATISTA:	Hightech Software S.A.S.
OBJETO:	Contratar una solución SaaS para el Icfes enfoca en la habilitación de entornos de trabajo virtuales seguros para el Banco de Items, utilizando Houndoc como plataforma SaaS
SUPERVISOR:	Subdirector de Información
AREA:	Subdirección de Información
VALOR:	\$632.065.298,00
FECHA DE INICIO:	13/11/2025
FECHA DE TERMINACIÓN:	31/12/2025

El 13 de noviembre de 2025, en la ciudad de Bogotá D.C., se reunieron **Diana Carolina Villamizar Bohorquez**, identificada con cédula de ciudadanía N° Diana Carolina C.C. No. 1090394391 de Cúcuta, en su calidad de Representante Legal de la Empresa, **HIGH TECH SOFTWARE SAS** identificada con NIT 900.718.336-7, y, **DIEGO MAURICIO SALAS**, en calidad de Supervisor del citado contrato por parte del **INSTITUTO COLOMBIANO PARA LA EVALUACIÓN DE LA EDUCACIÓN - ICFES**, con el fin de suscribir la presente Acta de Inicio, a partir de la fecha.

Las partes expresan conocer a cabalidad las respectivas obligaciones contractuales.

Para constancia se firma la presente por quienes en ella intervinieron, a los trece (13) días del mes de noviembre del año dos mil veinticinco 2025.



Supervisor



Contratista