ANEXO TÉCNICO

Provisión de servicios de desarrollo de software y pruebas para la ejecución de iniciativas de transformación digital en la entidad determinada por la Corporación.

2025

1. ANTECEDENTES

La entidad designada por la corporación, a través de su Dirección de Tecnología e Información, continúa avanzando en la implementación de la política de Gobierno Digital, en cumplimiento del Decreto 1008 de 2018 y del Modelo Integrado de Planeación y Gestión (MIPG) definido en la Ley 1753 de 2015. En este marco, la entidad designada por la corporación ha desarrollado y actualizado su Arquitectura Empresarial, alineada con el Marco de Referencia de Arquitectura Empresarial del Estado Colombiano, con el fin de garantizar que la adopción y el uso de las Tecnologías de la Información y la Comunicación (TIC) respondan a las necesidades estratégicas de la entidad y de sus grupos de interés.

Como parte de esta evolución, La entidad designada por la corporación ha definido su Plan Estratégico de Tecnología de la Información (PETI), el cual establece una hoja de ruta clara para la transformación digital de la entidad, alineando los proyectos tecnológicos con los objetivos estratégicos y misionales de la entidad. Entre estos objetivos se destacan:

1. **Fortalecer el análisis y divulgación de información relevante para los grupos de interés**, garantizando la accesibilidad y disponibilidad de datos confiables sobre los procesos de evaluación educativa en Colombia.
2. **Incursionar en nuevos mercados y ofrecer servicios de mayor valor agregado al ciudadano**, a través de plataformas digitales innovadoras que faciliten el acceso a trámites y servicios del La entidad designada por la corporación.
3. **Optimizar los procesos misionales**, mejorando la eficiencia y la calidad en la planeación, diseño, aplicación y análisis de pruebas estandarizadas a nivel nacional.
4. **Fortalecer el uso de tecnología en los procesos internos y externos**, asegurando la modernización y evolución de las plataformas digitales que soportan la gestión de la entidad.

En línea con estos propósitos, La entidad designada por la corporación ha adoptado el ciclo de desarrollo DevSecOps para sus proyectos tecnológicos, integrando prácticas de desarrollo, seguridad y operaciones que permiten una entrega continua y segura de soluciones digitales. Este enfoque garantiza que las aplicaciones desarrolladas cumplan con los más altos estándares de calidad, seguridad y eficiencia, respondiendo de manera ágil a las necesidades de los usuarios y asegurando la protección de la información.

DevSecOps (Desarrollo, Seguridad y Operaciones) es una evolución del modelo

tradicional de DevOps, donde la seguridad se integra de manera continua en todas las fases del ciclo de vida del desarrollo de software. Su objetivo principal es asegurar que las aplicaciones sean seguras desde su concepción, sin comprometer la velocidad de desarrollo y despliegue.

A diferencia de los enfoques tradicionales donde la seguridad se introduce en las últimas fases del desarrollo, en DevSecOps la seguridad es un componente clave desde el diseño del software, incorporando controles automatizados que permiten detectar y corregir vulnerabilidades de manera temprana.

PRINCIPIOS DE DEVSECOPS APLICADOS EN LA ENTIDAD

Para la implementación de DevSecOps en los proyectos de la entidad designada por la corporación en 2025, se adoptarán los siguientes principios:

1. Automatización de Seguridad en el CI/CD
    - Se integrarán herramientas de análisis estático y dinámico de código (SAST y DAST) en las fases de construcción y despliegue continuo.
    - Se implementarán escáneres de seguridad en los repositorios de código para detectar vulnerabilidades en dependencias de terceros y configuraciones de infraestructura.
2. Infraestructura como Código (IaC) Segura
    - Se definirán políticas de configuración segura desde el inicio, asegurando que la infraestructura en la nube cumpla con estándares de seguridad.
    - Se usarán herramientas para verificar la integridad y conformidad de los despliegues automatizados.
3. Monitoreo Continuo y Respuesta a Incidentes
    - Se adoptarán prácticas de observabilidad con monitoreo en tiempo real de las aplicaciones y la infraestructura.
    - Se establecerán mecanismos de alerta temprana y respuestas automatizadas ante eventos sospechosos o ataques cibernéticos.
4. Pruebas de Seguridad Tempranas y Frecuentes
    - Se integrarán pruebas de penetración automatizadas en los procesos de desarrollo para identificar vulnerabilidades antes del despliegue.
    - Se implementarán controles de seguridad en cada commit de código, asegurando que solo las versiones seguras sean liberadas.
5. Cultura de Seguridad y Capacitación Continua
    - Se promoverá una cultura de seguridad dentro de los equipos de desarrollo, operaciones y pruebas mediante entrenamientos en ciberseguridad, hacking ético y manejo de vulnerabilidades.
    - Se establecerán revisiones periódicas de código y auditorías de

seguridad con herramientas automatizadas y evaluaciones manuales.

Entre las iniciativas principales para el año 2025, se destacan:

Aplicación móvil: Tras el lanzamiento de su primera versión en 2024, esta aplicación está próxima a ser presentada al público. La app busca ofrecer a los usuarios una plataforma intuitiva y accesible para acceder a información relevante, servicios y trámites relacionados con las evaluaciones de la entidad. La aplicación permitirá a los estudiantes familiarizarse con los diferentes exámenes que aplica la entidad designada por la corporación, ofreciendo preguntas diseñadas bajo los marcos de evaluación de la entidad.

Sede Electrónica: Se continuará con el desarrollo y mejora de la Sede Electrónica de La entidad designada por la corporación, optimizando la disposición de trámites, servicios e información. Esta plataforma facilitará el registro, consulta de información y realización de trámites en línea, notificando oportunamente a los usuarios sobre las acciones necesarias en cada proceso. El objetivo es ofrecer una experiencia de usuario mejorada, centrada en las necesidades de los ciudadanos y alineada con la estrategia gov.co.

Desarrollo de Simulacros Avanzados a través de "PLEXI": Se fortalecerán las funcionalidades de "PLEXI", el software que permite la aplicación de pruebas electrónicas, incorporando nuevos tipos de ítems y funcionalidades que soporten tanto las pruebas institucionales como nuevos servicios. Además, se integrará un sistema de supervisión, monitoreo y vigilancia remota de exámenes, mejorando la capacidad de la entidad para aplicar pruebas en diferentes modalidades y garantizar su integridad.

Adicionalmente se considera la intervención de cualquier otro software propiedad de La entidad designada por la corporación del cual se tenga control del código fuente y los derechos de autor, que requieran ser modificadas o soportadas durante el tiempo de vigencia del contrato.

ENFOQUE EN CALIDAD Y ASEGURAMIENTO

Para garantizar la calidad de los desarrollos tecnológicos, La entidad designada por la corporación continuará con la aplicación de **pruebas funcionales y no funcionales**, asegurando que los productos cumplen con los estándares definidos y con las necesidades de los grupos de interés. El aseguramiento de calidad será una actividad formal en cada fase del desarrollo, aplicando **metodologías de pruebas de software y certificaciones internacionales como ISTQB®**.

Adicionalmente, la entidad reafirma la necesidad de mantener la independencia de

los equipos de desarrollo y pruebas, asegurando que cada rol dentro del ciclo de vida del software opere de manera separada, garantizando objetividad y cumplimiento de los criterios de aceptación previamente establecidos.

2. ALCANCE GENERAL DEL CONTRATO

El presente contrato consta de dos partes, que se describen a continuación:

1. Fábrica de Desarrollo: Prestación de Servicios de construcción de Softwares para los proyectos estratégicos y misionales de La entidad designada por la corporación
2. Fábrica de Pruebas: Prestación de Servicios para la elaboración y producción de las pruebas para los proyectos estratégicos y misionales de La entidad designada por la corporación.

2.1. ALCANCE 1. FABRICA DESARROLLO

Fábrica de Desarrollo: prestará un servicio especializado para la implementación de soluciones tecnológicas en los sistemas de información de la entidad, el cual se ejecutara mediante una bolsa de 9.000 horas de servicios especializados en desarrollo de software bajo la modalidad de fábrica de software, para la implementación, mantenimiento, optimización y modernización de los sistemas de La entidad designada por la corporación, aplicando el enfoque DevSecOps.

El servicio incluirá el desarrollo de nuevos requerimientos, optimización, mantenimiento y modernización de las plataformas actuales, asegurando que los sistemas misionales de la entidad cuenten con funcionalidades que fortalezcan sus capacidades, mejoren la operación y garanticen la seguridad e integridad de la información.

Bajo el enfoque DevSecOps, la Fábrica de Desarrollo integrará seguridad desde el diseño, prácticas de automatización de pruebas y despliegues, así como mecanismos de monitoreo y respuesta temprana a vulnerabilidades.

De manera general, el objeto a contratar incluirá los siguientes servicios:

1. Análisis y diseño seguro

- Levantamiento de requerimientos con criterios de seguridad desde el inicio.
- Diseño de arquitecturas escalables y seguras alineadas con la Arquitectura Empresarial de La entidad designada por la corporación.

2. Desarrollo e integración continua (CI/CD)

- Programación segura con validaciones automatizadas de código.
- Uso de análisis estático y dinámico (SAST/DAST) para detectar vulnerabilidades antes del despliegue.

3. Automatización de pruebas
- Pruebas funcionales y de seguridad automatizadas en cada iteración.
- Simulación de ataques y pruebas de rendimiento para garantizar estabilidad y protección.

4. Despliegue continuo y monitoreo
- Implementación de pipelines CI/CD con entregas frecuentes y controladas.
- Monitoreo en tiempo real para detectar fallos y responder a incidentes de seguridad.

5. Infraestructura como Código (IaC) y gestión segura de entornos
- Automatización de infraestructura para garantizar configuraciones seguras y escalables.
- Aplicación de políticas de seguridad en la nube y entornos híbridos

2.1.1. SERVICIOS A CONTRATAR

Con el fin de fortalecer la seguridad, eficiencia y confiabilidad en los desarrollos de La entidad designada por la corporación, la fábrica operará bajo la metodología DevSecOps, la cual integra desarrollo, seguridad y operaciones en todas las etapas del ciclo de vida del software.

La adopción de DevSecOps en la Fábrica de Desarrollo permitirá:

✓ Desarrollos seguros desde el inicio, evitando vulnerabilidades en fases tardías.
✓ Automatización de pruebas y despliegues, reduciendo tiempos y errores en las entregas.
✓ Monitoreo continuo y respuesta rápida a incidentes, garantizando estabilidad y rendimiento.
✓ Cumplimiento de estándares de calidad y seguridad, alineados con OWASP, NIST y normativas del Gobierno Digital Colombiano.

Este modelo asegurará que el software desarrollado cumpla con las expectativas de La entidad designada por la corporación y sus grupos de interés, optimizando los servicios digitales y fortaleciendo la transformación digital de la entidad.

La Fábrica de Desarrollo de La entidad designada por la corporación operará bajo un enfoque estructurado en fases iterativas e integradas dentro del ciclo de vida de

desarrollo de software, aplicando la metodología DevSecOps. Este modelo garantiza que cada entrega sea segura, confiable y alineada con los estándares tecnológicos y estratégicos de la entidad.

A diferencia del desarrollo tradicional, en DevSecOps cada fase del proceso incorpora seguridad, automatización y monitoreo continuo, asegurando que las soluciones sean robustas y escalables desde el inicio.

FASES DE EJECUCIÓN DE LA FÁBRICA DE DESARROLLO

FASE 1: Descubrimiento y Diseño de Soluciones

Objetivo: Comprender los requerimientos del negocio y definir la arquitectura y diseño de la solución.

Actividades:

1.1 Levantamiento de Requerimientos Funcionales y Técnicos

- Reuniones con áreas funcionales y técnicas para identificar necesidades del negocio.
- Definición de criterios de aceptación con el usuario final.
- Identificación de riesgos y dependencias con otros sistemas de la entidad.

1.2 Análisis de Impacto y Diseño de Arquitectura

- Evaluación de la arquitectura actual para determinar si se debe adaptar o construir una nueva.
- Definición de arquitectura alineada con la Arquitectura Empresarial de la entidad.
- Establecimiento de políticas de seguridad desde el diseño (Security by Design).
- Identificación de mecanismos de integración con otros sistemas internos y externos.

FASE 2: Desarrollo Seguro e Integración Continua (CI/CD)

Objetivo: Construir software aplicando estándares de calidad y seguridad, asegurando integraciones eficientes.

Actividades:

2.1 Programación Segura y Desarrollo de Software

- Implementación de código seguro siguiendo estándares OWASP y Secure Coding.
- Aplicación de principios de desarrollo ágil y modular.
- Construcción de API's y microservicios cuando sea requerido.

2.2 Integración con Otros Sistemas y Bases de Datos

- Validación de compatibilidad con el modelo de datos de la entidad.
- Aplicación de buenas prácticas de seguridad en accesos y manipulación de datos.

2.3 Control de Versiones y Auditoría de Código
- Uso de repositorios de código con trazabilidad de cambios.
- Auditoría de seguridad con herramientas SAST/DAST.
- Implementación de revisiones de código automatizadas (Code Review).

FASE 3: Pruebas Unitarias y Validación Técnica
Objetivo: Garantizar la calidad del software antes de su entrega a la Fábrica de Pruebas.

Actividades:
3.1 Ejecución de Pruebas Unitarias
- Desarrollo de pruebas unitarias para validar cada componente de software.
- Análisis de cobertura de código para asegurar calidad en la implementación.

3.2 Corrección de Defectos y Optimización de Código
- Identificación y corrección de errores detectados en pruebas unitarias.
- Refactorización de código para mejorar rendimiento y mantenimiento.

3.3 Entrega a la Fábrica de Pruebas
- Validación de cumplimiento de requisitos funcionales y técnicos.
- Documentación de código y pasos de prueba.

FASE 4: Soporte y Mantenimiento Evolutivo
Objetivo: Garantizar la estabilidad de los sistemas y su evolución tecnológica.

Actividades:
4.1 Corrección de Incidentes y Optimización
- Resolución de errores detectados en los sistemas en producción.
- Optimización de desempeño y mejoras en tiempos de respuesta.

4.2 Aplicación de Mejoras Tecnológicas
- Implementación de nuevas funcionalidades según las necesidades de la entidad.
- Actualización de frameworks y tecnologías en sistemas existentes.

ENTREGABLES POR FASE
FASE 1: Descubrimiento y Diseño

📌 Documento de análisis y diseño (Arquitectura y requerimientos).

📌 Propuesta de integración con sistemas existentes.

FASE 2: Desarrollo Seguro e Integración
📌 Código fuente documentado y almacenado en repositorio.
📌 Reporte de auditoría de seguridad y análisis de código (SAST/DAST).
📌 Reporte de pruebas unitarias y cobertura de código.

FASE 3: Validación y Entrega a la Fábrica de Pruebas
📌 Resultados de pruebas unitarias y reporte de correcciones.
📌 Documentación técnica del desarrollo.

FASE 4: Soporte y Mantenimiento
📌 Reporte de incidencias y ajustes aplicados.
📌 Registro de mejoras tecnológicas implementadas.

2.2. ALCANCE 2: FABRICA DE PRUEBAS

Fábrica de Pruebas: prestará servicios especializados en aseguramiento de calidad de software, garantizando que los desarrollos cumplan con los estándares de seguridad, funcionalidad, rendimiento y usabilidad antes de ser liberados a producción, aplicando DevSecOps integrando pruebas automatizadas, detección de vulnerabilidades y certificación de software. Además, se deberá gestionar y desplegar los ambientes de desarrollo, pruebas y producción el cual se ejecutara mediante una bolsa de 3.000 horas de servicios.

De manera general, el alcance deberá contratar incluirá los siguientes servicios:

1. Pruebas Funcionales
- Validación del cumplimiento de los requerimientos del negocio.
- Ejecución de pruebas de regresión para asegurar la estabilidad de los sistemas.
- Pruebas de integración para verificar la interoperabilidad con otros sistemas de La entidad designada por la corporación.

2. Pruebas de Seguridad
- Aplicación de pruebas de penetración (Pentesting) para detectar vulnerabilidades.
- Análisis estático y dinámico del código fuente (SAST/DAST).
- Validación de autenticación, cifrado y control de accesos.

3. Pruebas de Rendimiento y Carga
- Evaluación del comportamiento de las aplicaciones bajo condiciones de alta demanda.

- Simulación de tráfico concurrente para identificar cuellos de botella.
- Pruebas de estabilidad y escalabilidad del software.

4. Pruebas de Usabilidad y Experiencia de Usuario
- Evaluación de accesibilidad, alineación con estándares UX/UI y facilidad de uso.
- Validación de compatibilidad en distintos dispositivos y navegadores.

5. Automatización de Pruebas
- Implementación de pruebas automatizadas en los procesos de validación continua.
- Integración de pruebas con pipelines CI/CD para detección temprana de fallos.

6. Gestión y Despliegue de Ambientes
- Administración de entornos de desarrollo, pruebas y producción.
- Configuración y mantenimiento de infraestructura para la ejecución de pruebas.
- Automatización de despliegues con herramientas de infraestructura como código (IaC).

7. Monitoreo y Validación Post-Despliegue

- Evaluación del software en producción para detectar errores o vulnerabilidades emergentes.
- Implementación de herramientas de monitoreo para análisis de comportamiento en tiempo real.

2.2.1. ALCANCE SERVICIO PARA LAS PRUEBAS DE SOFTWARE

La entidad designada por la corporación, requiere los servicios profesionales especializados, para realizar las pruebas funcionales y no funcionales bajo demanda sobre todas las soluciones tecnológicas definidas por la Dirección de Tecnología e Información.

Para lo cual, el proceso de fábrica de pruebas funcionales y no funcionales estará encaminado a los mantenimientos y nuevos desarrollos que se realicen a través de las diferentes líneas de desarrollo con las que actualmente la entidad se encuentra operando.

A través de este modelo de servicios, se deberán realizar las pruebas funcionales y no funcionales a los nuevos componentes y módulos de las aplicaciones que actualmente se están optimizando y ajustando a través del grupo de desarrollo inhouse

que tiene la entidad. De igual manera, se le deberán realizar la pruebas funcionales y no funcionales a las nuevas herramientas que se desarrollarán a través de la fábrica de software.

En cuanto al aseguramiento de la calidad, este servicio debe estar incorporado en cada una de las etapas que conforma el flujo de pruebas funcionales y no funcionales, para lo cual se debe documentar y generar los instrumentos que permitan evaluar el cumplimiento de la calidad en cada una de las etapas, con el objetivo de cumplir con las finalidades de cada una de las pruebas planeadas.
Por último, el servicio de pruebas funcionales y no funcionales estará dado por horas integrales; es decir, una hora integral de pruebas debe contemplar las etapas de planeación, diseño, ejecución, incidencias, certificación de pruebas y documentación, las cuales se describen a continuación:

2.2.2. CICLO DE PRUEBAS PARA LA CALIDAD DEL SOFTWARE

- Estimación (planeación)
- Estrategia y plan (planeación)
- Elaboración de componentes (diseño)
- Ejecución
- Reporte de Avance de incidencias (calidad, documentación)
- Registro de procesos e informe final (calidad, certificación de pruebas y documentación)

2.2.2.1. Estrategia y Plan

Para la ejecución del servicio contratado en la modalidad bajo demanda, se desarrollarán las actividades de pruebas bajo el marco de trabajo DevSecOps y se realizarán de acuerdo con lo programado en cada sprint. Se pagará conforme los costos unitarios definidos descritos con la categorización especificada para pruebas funcionales y no funcionales.

2.2.2.2. Elaboración de componentes

De acuerdo con la estructura de componentes establecida para el software desarrollado, se definen pruebas de calidad de software alineadas con cada uno de los productos a las cuales se le van a hacer pruebas.

Todos los entregables del ciclo de desarrollo deben ser sometidos a revisiones de calidad, no sólo del código, sino también de las especificaciones funcionales, diseños técnicos, manuales y demás documentación.

2.2.2.3 Ejecución

Se deben diseñar los casos de pruebas para cada uno de los componentes desarrollados y entregados. Los casos de prueba deben corresponder a las historias de usuario que serán probadas.

Se deben ejecutar las pruebas de calidad de software, para lo cual el equipo de pruebas debe organizarse y dividirse por historias de usuario. Debe existir visibilidad de los casos e incidencias que impidan la ejecución de otros casos de prueba para tomar acciones.
Adicionalmente, cualquier situación con el entorno (no disponibilidad o errores no asociados al desarrollo), debe ser reportado al equipo técnico de la entidad designada por la corporación.

2.2.2.4. Reporte de Avance de incidencias

Se debe llevar un reporte periódico del avance de las pruebas, que puede ser diario o varias veces al día para historias de usuario complejas o críticos, en el cual se debe informar los casos de prueba totales, casos de prueba ejecutados, casos exitosos, casos fallidos, casos pendientes, número de incidencias, entre otros aspectos.

Cada error reportado al ejecutar los casos de prueba debe registrar un reporte de incidencia, el cual debe incluir como mínimo la Fecha y Hora, Título descriptivo (Historia de usuario), descripción detallada que permita a otros reconocerlo, localización y entorno en el que se encontró (incluyendo el usuario y roles con los que se estaba probando), resaltar cual es el error si tiene una ubicación especifica en la pantalla y los pasos para reproducirlo, el reporte se deberá realizar en la herramienta que La entidad designada por la corporación indique.

2.2.2.5. Certificación de la prueba

Las pruebas funcionales y no funcionales una vez superadas las incidencias y los diferentes errores que se presenten en cada una de las historias de usuario probadas, la fábrica de pruebas deberá generar un documento donde certifique el buen funcionamiento y cumplimiento funcional y técnico de las pruebas ejecutadas.

2.2.2.6. Registro de procesos e informe final

Se debe finalizar el registro y organización de las evidencias de prueba de cada historia de usuario y otra documentación de los casos de prueba ejecutados.

Una vez finalizadas las pruebas de cada historia de usuario, se debe elaborar un informe final que reporte las pruebas ejecutadas, incluyendo los casos, los resultados,

los problemas que se presentaron, lecciones aprendidas y otros aspectos, esta información deberá ser actualizada en la herramienta que La entidad designada por la corporación indique.

3. FASES DE EJECUCIÓN DE LA FÁBRICA DE PRUEBAS

Fase 1: Planificación y Diseño de Pruebas
Objetivo: Definir estrategias y casos de prueba basados en los requerimientos del software.

Actividades:

Análisis de requerimientos funcionales y técnicos.
Identificación de criterios de aceptación del software.
Diseño de casos de prueba alineados con los objetivos del sistema.
Definición del plan de pruebas y estrategia de automatización.

Entregables:

📌 Plan de pruebas detallado.
📌 Matriz de trazabilidad de requerimientos vs. casos de prueba.
📌 Escenarios de prueba funcionales y no funcionales.

Fase 2: Preparación y Configuración de Ambientes de Prueba
Objetivo: Asegurar que los entornos de prueba estén listos para la ejecución de validaciones.

Actividades:

Despliegue y configuración de entornos (desarrollo, pruebas y preproducción).
Creación de datos de prueba.
Validación de conectividad e integraciones.

Entregables:

📌 Reporte de configuración de entornos.
📌 Datos de prueba generados y validados.

Fase 3: Ejecución de Pruebas y Registro de Defectos
Objetivo: Verificar el correcto funcionamiento del software mediante pruebas funcionales y no funcionales.

Actividades:

Ejecución de pruebas funcionales (unitarias, regresión e integración).
Ejecución de pruebas de seguridad (SAST/DAST).
Ejecución de pruebas de rendimiento y carga.
Identificación, registro y seguimiento de defectos.

Entregables:

📌 Reportes de ejecución de pruebas con evidencias.
📌 Registro de defectos documentados en herramientas de gestión.

Fase 4: Validación Final y Aceptación del Software
Objetivo: Asegurar que el software cumple con los criterios de calidad antes de ser liberado.

Actividades:

Revisión de defectos corregidos.
Re-ejecución de pruebas de regresión.
Validación final con los usuarios y áreas técnicas.

Entregables:

📌 Informe de certificación de calidad del software.
📌 Reporte de defectos resueltos y pendientes (si aplica).

PROCEDIMIENTO DE ESTIMACIÓN DE REQUERIMIENTOS

Matriz de Estimaciones y Planificación

Al inicio del contrato, La entidad designada por la corporación y el CONTRATISTA deberán acordar una matriz de estimaciones, en la cual se definan los niveles de complejidad y esfuerzo para los diferentes tipos de requerimientos. Esta matriz servirá como herramienta fundamental para la planificación, gestión y control de los proyectos a desarrollar durante la ejecución del contrato.

Especificación de Requerimientos

Después de realizar la reunión de levantamiento de la necesidad con los usuarios de La entidad designada por la corporación, el CONTRATISTA deberá documentar y detallar el requerimiento en un máximo de tres (3) días hábiles. La metodología para

la estimación del esfuerzo se establecerá en el acta de inicio del contrato, acordada entre ambas partes.

Entendimiento y Caracterización de Requerimientos
Para garantizar un levantamiento preciso de los requerimientos, el CONTRATISTA deberá llevar a cabo entrevistas, mesas de trabajo y presentaciones grupales con los equipos de la entidad. Estas actividades permitirán una mejor comprensión de las necesidades y una caracterización adecuada del alcance del requerimiento.

📌 **Registro obligatorio: Se deberá documentar la fecha de las reuniones, asistentes, temas tratados y conclusiones.**

Estimación y Cronograma

Una vez el usuario solicitante haya dado visto bueno a la definición del requerimiento, la estimación de esfuerzo deberá completarse en un máximo de dos (2) días hábiles. Posteriormente, el CONTRATISTA presentará un cronograma de entrega que incluya todas las fases del ciclo de vida del desarrollo.

Modelado y Desarrollo de Artefactos de Software

El CONTRATISTA deberá modelar y documentar los requerimientos y desarrollar los artefactos correspondientes en las áreas de software y/O soporte técnico. Antes de su implementación, los entregables deberán ser revisados y aprobados por La entidad designada por la corporación, garantizando el cumplimiento de los lineamientos de arquitectura empresarial establecidos.

Aprobación de Requerimientos

Todos los requerimientos deberán ser aprobados y firmados por el supervisor del contrato, en coordinación con el área solicitante.

Autorización y Priorización de Desarrollo

Solo los requerimientos debidamente aprobados y priorizados por el(los) supervisor(es) del contrato podrán ser desarrollados.

Cumplimiento de Cronogramas y Niveles de Servicio

El incumplimiento de los cronogramas establecidos para cada requerimiento dará lugar a la aplicación de los Acuerdos de Niveles de Servicio (ANS) definidos en el contrato. Este incumplimiento podría derivar en sanciones contractuales según lo estipulado.

📌 Nota:

- La entidad designada por la corporación y la Corporación Colombia Digital NO reconocerá mayores costos derivados de errores en la estimación del esfuerzo realizada por el CONTRATISTA, siempre que estas hayan sido aceptadas por las partes.
- El CONTRATISTA no podrá iniciar el desarrollo de un requerimiento si este no ha sido previamente aprobado por La entidad designada por la corporación.
- Si se requiere modificar el alcance del requerimiento y esto afecta la estimación de horas de desarrollo, la Corporación Colombia digital y La entidad designada por la corporación reconocerán el ajuste correspondiente.
- En caso de que La entidad designada por la corporación decida detener o cancelar un requerimiento ya aprobado y en ejecución, se facturará de manera proporcional según el volumen de horas autorizadas y trabajadas hasta el momento de la cancelación.

4. PERFILES MÍNIMOS PARA LA EJECUCIÓN DEL CONTRATO

GERENTE DE PROYECTOS
Experiencia:

- Gestión y dirección de proyectos de desarrollo de software y aseguramiento de calidad.
- Implementación de metodologías ágiles y marcos de trabajo como **Scrum, Kanban, SAFe** y enfoques tradicionales **PMI o PRINCE2**.
- Coordinación de equipos multidisciplinarios en entornos **DevSecOps**.
- Administración de contratos y control de ejecución de servicios tercerizados por horas.
- Seguimiento de indicadores de calidad, costos y tiempos en proyectos tecnológicos.

Responsabilidades:

✓ **Planificación y Seguimiento del Proyecto**

- Definir el **plan de trabajo, hitos y cronograma** de las fábricas de desarrollo y pruebas.
- Coordinar la asignación de recursos y el cumplimiento de entregables.
- Supervisar la ejecución del contrato asegurando alineación con los objetivos de La entidad designada por la corporación y La Corporación Colombia Digital.

✓ **Gestión de Equipos y Coordinación General**

- Asegurar la comunicación efectiva entre la **Fábrica de Desarrollo, la Fábrica**

de Pruebas y la La entidad designada por la corporación y la Corporación.
- Liderar reuniones de seguimiento con las partes interesadas.
- Resolver conflictos o bloqueos en el desarrollo y validación de software.

✓ **Control de Calidad y Cumplimiento de Estándares**
- Garantizar que los desarrollos cumplen con las especificaciones funcionales y técnicas.
- Asegurar que las pruebas validen completamente los criterios de aceptación.
- Velar por el uso adecuado de herramientas de integración, pruebas y seguridad en **DevSecOps**.

✓ **Monitoreo de KPIs y Reporte de Avances**
- Supervisar indicadores clave del proyecto (cumplimiento de entregables, defectos, tiempos de respuesta, etc.).
- Presentar informes de avances a La entidad designada por la corporación y a La Corporación y gestionar ajustes en el plan del proyecto.
- Proponer mejoras en procesos para optimizar la ejecución del contrato.

✓ **Gestión de Riesgos y Cumplimiento Contractual**
- Identificar riesgos en el desarrollo y validación del software.
- Implementar estrategias de mitigación y planes de contingencia.
- Asegurar el cumplimiento de términos contractuales y normativas del **Gobierno Digital Colombiano**.

Perfiles de la Fábrica de Desarrollo

🔹 **Arquitecto de Software**
Experiencia:
Diseño e implementación de arquitecturas de software escalables y seguras.
Integración de soluciones con arquitecturas de microservicios, APIs REST y bases de datos distribuidas.
Definición de patrones de desarrollo y buenas prácticas en DevSecOps.
Responsabilidades:
✓ Definir y validar la arquitectura de las soluciones desarrolladas.
✓ Asegurar la interoperabilidad entre sistemas y cumplimiento de estándares de la entidad designada por la corporación.
✓ Implementar estrategias de seguridad en el diseño del software.
✓ Apoyar la toma de decisiones tecnológicas.

🔹 **Desarrollador Full Stack**
Experiencia:
Desarrollo de aplicaciones frontend y backend con frameworks modernos.
Implementación de buenas prácticas de programación segura (OWASP, Secure

Coding).
Manejo de herramientas de integración continua (CI/CD).
Responsabilidades:
✓ Implementar los requerimientos funcionales y técnicos de cada desarrollo.
✓ Aplicar controles de seguridad en el código.
✓ Integrar APIs y servicios en la arquitectura definida.
✓ Asegurar la calidad del software mediante pruebas unitarias y revisiones de código.

🔹 **Ingeniero de Integración y DevSecOps**
Experiencia:
Configuración y administración de pipelines de integración y entrega continua (CI/CD).
Implementación de análisis estático y dinámico de código (SAST/DAST).
Automatización de procesos de despliegue y control de infraestructura.
Responsabilidades:
✓ Gestionar la integración continua de los desarrollos en entornos de prueba y producción.
✓ Aplicar mecanismos de control de calidad y seguridad en cada iteración del software.
✓ Optimizar los tiempos de despliegue mediante automatización.
✓ Asegurar el cumplimiento de estándares de seguridad en la infraestructura del software.

🔹 **Soporte Técnico y Mantenimiento**
Experiencia:
Diagnóstico y solución de incidencias en entornos de producción.
Optimización de aplicaciones para mejorar rendimiento y estabilidad.
Aplicación de parches y actualizaciones en sistemas en operación.
Responsabilidades:
✓ Atender y resolver incidentes de software reportados en producción.
✓ Aplicar mejoras y optimización de código cuando sea necesario.
✓ Documentar los ajustes y correcciones realizadas.

Perfiles de la Fábrica de Pruebas
🔹 **Líder de Pruebas**
Experiencia:
Coordinación de equipos de aseguramiento de calidad de software.
Definición de estrategias de pruebas funcionales, de seguridad y de rendimiento.
Uso de herramientas de gestión de pruebas y defectos.
Responsabilidades:
✓ Supervisar y gestionar el proceso de pruebas dentro del ciclo de desarrollo.

✓ Definir y actualizar estrategias de pruebas.
✓ Coordinar la ejecución de validaciones con el equipo de pruebas.
✓ Asegurar el cumplimiento de criterios de aceptación del software.

🔹 **Analista de Pruebas Funcionales**
Experiencia:
Diseño y ejecución de casos de prueba manuales y automatizados.
Validación de cumplimiento de requerimientos funcionales.
Identificación y documentación de defectos en herramientas de gestión.
Responsabilidades:
✓ Diseñar y ejecutar pruebas funcionales y de regresión.
✓ Identificar y reportar defectos en el software.
✓ Garantizar que el software cumpla con las especificaciones funcionales.
✓ Documentar evidencias de pruebas realizadas.

🔹 **Ingeniero de Pruebas de Seguridad**
Experiencia:
Aplicación de pruebas de análisis estático y dinámico del código (SAST/DAST).
Validación de controles de autenticación, cifrado y gestión de accesos.
Identificación de vulnerabilidades en aplicaciones y servicios.
Responsabilidades:
✓ Ejecutar análisis de seguridad en el software antes de su liberación.
✓ Identificar y reportar vulnerabilidades en las aplicaciones.
✓ Coordinar con el equipo de desarrollo la corrección de problemas de seguridad.
✓ Validar que las soluciones cumplan con estándares de seguridad de La entidad designada por la corporación.

🔹 **Ingeniero de Pruebas de Rendimiento**
Experiencia:
Diseño y ejecución de pruebas de carga y estrés.
Uso de herramientas para la simulación de tráfico concurrente.
Análisis de métricas de desempeño de software.
Responsabilidades:
✓ Evaluar el comportamiento del software bajo diferentes cargas de trabajo.
✓ Identificar y reportar problemas de rendimiento y estabilidad.
✓ Validar la capacidad de respuesta de los sistemas en condiciones de alta demanda.

🔹 **Especialista en Gestión y Despliegue de Ambientes**
Experiencia:
Administración y configuración de entornos de desarrollo, prueba y producción.

Automatización de despliegues con herramientas IaC (Terraform, Ansible, etc.).
Gestión de recursos en la nube o servidores on-premise.
Responsabilidades:
✓ Configurar y mantener los entornos de pruebas y preproducción.
✓ Asegurar la disponibilidad de los entornos para la ejecución de pruebas.
✓ Coordinar con la Fábrica de Desarrollo el despliegue de nuevas versiones.

Resumen de Roles y Responsabilidades

FÁBRICA	PERFIL	RESPONSABILIDAD PRINCIPAL
GENERAL	Gerente de Proyectos	Coordinación y seguimiento de ejecución contractual
DESARROLLO	Arquitecto de Software	Definir la arquitectura y estándares técnicos
DESARROLLO	Desarrollador Full Stack	Construcción segura de software
DESARROLLO	Ingeniero de Integración y DevSecOps	Automatización y gestión de CI/CD
DESARROLLO	Soporte Técnico y Mantenimiento	Resolución de incidentes y optimización
PRUEBAS	Líder de Pruebas	Supervisión y estrategia de pruebas
PRUEBAS	Analista de Pruebas Funcionales	Validación de requerimientos
PRUEBAS	Ingeniero de Pruebas de Seguridad	Identificación de vulnerabilidades
PRUEBAS	Ingeniero de Pruebas de Rendimiento	Evaluación de carga y desempeño
PRUEBAS	Especialista en Gestión de Ambientes	Configuración y despliegue de entornos

La documentación que acredita la condición del Equipo Humano deberá presentarse por el Contratista al momento de iniciar la ejecución del contrato, el cual deberá ser aprobado por el Supervisor responsable.

5. DERECHOS DE PROPIEDAD INTELECTUAL Y DERECHOS DE AUTOR

Atendiendo los lineamientos dados ha conocer por la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente a través de la Guía denominada: *"GUÍA DE PROPIEDAD INTELECTUAL EN LA CONTRATACIÓN PÚBLCA"*, serán adoptados en su integridad en el marco del presente contrato, lo cual forma parte integral en el cumplimiento de las obligaciones ha cargo del Contratista; lo anterior, en concordancia con las disposiciones previstas en el artículo 669 del Código Civil Colombiano, de lo cual se permite concluir que la Propiedad Intelectual de los productos obtenidos del correspondiente contrato radican en cabeza de La entidad designada por la corporación su titularidad.

En lo referente a los Derechos de Autor de los productos obtenidos en el presente contrato tendrán el tratamiento descrito en la referida Guía emitida por Colombia Compra Eficiente.

ANEXO COMPLEMENTARIO.
CONSIDERACIONES DEL PROCESO.

I. CONSIDERACIONES DE SEGURIDAD

- **CONFIDENCIALIDAD DE LA INFORMACIÓN**

Se considera información confidencial:

A. Toda la información relacionada con la prestación de los servicios contratados en el desarrollo del objeto de este contrato.
B. Las características y especificaciones de los productos, servicios y programas de La entidad designada por la corporación y la Corporación Colombia Digital, que no sean de público conocimiento.
C. Cualquier información técnica, financiera, estratégica y de políticas, escrita, oral o visual, que tenga el carácter de reservado o haya sido marcada o anunciada como confidencial por el La entidad designada por la corporación y la Corporación Colombia Digital.
D. Toda la información de datos personales que conozca en virtud de la presente invitación y el contrato eventual.
E. Toda la documentación y demás información sobre el hardware y el software que utiliza La entidad designada por la corporación y La Corporación Colombia Digital, en el desarrollo de sus actividades.
F. Toda la información que haya sido catalogada como pública reservada o pública clasificada por la entidad.

El prestador del servicio deberá cumplir con la cláusula de confidencialidad de la información, donde acepta y reconoce de manera expresa que la información que reciba elabore, cree, conozca, formule, deduzca o concluya en virtud o con ocasión del desarrollo y ejecución de los servicios contratados, es información confidencial, de exclusiva titularidad de La entidad designada por la corporación y la Corporación Colombia Digital, por lo cual no podrá revelar, durante la vigencia de este contrato ni en los años siguientes a su expiración.
El incumplimiento de dicho acuerdo dará lugar al inicio de las acciones legales que correspondan para el cobro de los perjuicios que pudieran producirse a la Corporación Colombia Digital y La entidad designada por la corporación, por la divulgación de información considerada confidencial o por el incumplimiento de dicho acuerdo, según lo establecido en el mismo.

- **SEGURIDAD DE LA INFORMACIÓN**

Es una obligación para el prestador del servicio, cumplir con las políticas y normas de seguridad de la información La entidad designada por la corporación y la

Corporación Colombia Digital, por lo cual el personal involucrado debe conocer la siguiente cláusula:
"Durante la ejecución del presente contrato, las partes se comprometen a conocer y cumplir con los lineamientos del Sistema de Gestión de Seguridad de la Información (SGSI), el manual de Seguridad y Privacidad de la Información y los procedimientos que lo componen y al Manual de Políticas y procedimientos de protección de datos personales. En caso de que exista información sujeta a alguna reserva legal, las partes deben mantener la confidencialidad de esta información, la cual deberá estar previamente marcada como tal, para ello, debe comunicar a la otra parte que la información suministrada tiene el carácter de confidencial. Cada una de las partes acuerdan mantener la confidencialidad de la información confidencial de la otra parte durante un periodo de tres años contados a partir de la fecha de revelación".

- **DERECHO A AUDITAR**

El prestador del servicio accede a ser auditado sobre todas las actividades relacionadas con la prestación de los servicios contratados en el desarrollo del objeto de este contrato. Además, se compromete a aportar toda la información y apoyo que La entidad designada por la corporación y la Corporación Colombia Digital soliciten en el marco de las auditorías bajo las cuales sea auditado de acuerdo con los criterios que se considere pertinentes auditar.

- **OBLIGACIONES ESPECIFICAS DEL CONTRATISTA:**

Para el cumplimiento del objeto del contrato, el proveedor deberá cumplir con las siguientes obligaciones específicas:

1. Desarrollar el objeto del Contrato, en las condiciones de calidad, oportunidad, y obligaciones definidas en el estudio previo, incluyendo lo establecido en el documento Anexo Técnico y ejecutando el servicio objeto del contrato como un proyecto, basado en los estándares del PMI y cumpliendo los lineamientos que La entidad designada por la corporación indique al contratista con respecto a la gestión, reporte y control del proyecto.
2. Cumplir con los diferentes requerimientos objeto de pruebas desde sus fases iniciales hasta las puestas en producción, en los tiempos establecidos.
3. Garantizar que durante la prestación del servicio se disponga del equipo de trabajo capacitado técnicamente de acuerdo con lo definido en el Anexo Técnico. El contratista deberá realizar el reemplazo de integrantes del equipo de trabajo, de acuerdo con los requerimientos que realice el supervisor y según las necesidades de los proyectos.
4. Garantizar que el aseguramiento de calidad cubra tanto los desarrollos de los grupos internos de La entidad designada por la corporación. Como el software desarrollado en un modelo tercerizado.
5. Informar al Supervisor del contrato, previo al inicio de la ejecución, las herramientas a utilizar para llevar a cabo todas las actividades que hagan parte

del proceso, tanto para la planeación, gestión y seguimiento del proyecto.

6. Presentar los entregables de la ejecución del servicio de pruebas de software y aseguramiento de calidad, de acuerdo con lo definido en el Anexo Técnico.
7. Participar activamente de las reuniones y/o actividades de planeación, seguimiento y desarrollo de los proyectos que involucran actividades de pruebas y aseguramiento de calidad.
8. Cumplir con los ANS establecidos en el Anexo Técnico, y realizar los descuentos incurridos en los periodos de facturación en caso de incumplimiento, previa validación entre EL CONTRATISTA y el supervisor.
9. Atender los requerimientos que realice La entidad designada por la corporación a través del supervisor del Contrato.
10. Mantener durante la ejecución del contrato, la organización técnica y administrativa presentada en su propuesta, en forma permanente y con altos niveles de eficiencia técnica y profesional, para atender todas las obligaciones.
11. Contar con las herramientas incluido el licenciamiento y recursos necesarios para ejecutar su labor, dentro de los que se incluyen elementos informáticos y de ofimática. Para tal efecto, el contratista y su personal se obligan cumplir las políticas y lineamientos de seguridad establecidos en la entidad designada por la corporación y de sus sistemas de gestión.
12. Reemplazar a algún miembro del grupo de trabajo si La entidad designada por la corporación y La Corporación Colombia Digital así lo determina.
13. Cumplir con los lineamientos establecidos por La entidad designada por la corporación para la Seguridad de la Información. El contratista debe difundir a todo el personal que participe en la ejecución del contrato las políticas de seguridad que les permitan entender y aplicar las políticas definidas. La no observación o no aplicación de las políticas de seguridad de La entidad designada por la corporación por parte del contratista, dará lugar al incumplimiento del contrato.
14. Permitir a La entidad designada por la corporación instalar en los equipos de cómputo de propiedad del contratista herramientas de protección y prevención tales como: agentes de monitoreo de software y agentes de prevención de fuga de información.
15. Notificar, por escrito y en forma inmediata a La entidad designada por la corporación y a la Corporación Colombia Digital cualquier retraso en la ejecución y desarrollo del contrato, manifestando la causa y tiempo estimado de cumplimento.

- **GARANTÍAS:**

EL CONTRATISTA deberá constituir la Garantía Única a favor de La Corporación Colombia Digital identificado con el N.I.T. 830.101.214-4, a favor de 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:

1. **CUMPLIMIENTO:** En equivalente al diez por ciento (10%) del valor total del contrato, con vigencia igual al termino de ejecución del contrato y seis (06) meses más.
2. **CALIDAD DE SERVICIO: :** En equivalente al diez por ciento (10%) del valor total del contrato, con una vigencia desde la finalización del plazo de ejecución del contrato y hasta un (1) año más.
3. **SALARIOS, PRESTACIONES SOCIALES LEGALES E INDEMNIZACIONES LABORALES**: Cuantía equivalente al cinco por ciento (5%) del valor total del contrato, con una vigencia igual al término del contrato y tres (3) años más.

II. CONSIDERACIONES GENERALES

El proponente deberá tener en cuenta las siguientes consideraciones:

- La Corporación Colombia Digital se reserva el derecho de solicitar cualquier aclaración que considere necesario con el fin de verificar el cumplimiento de los requisitos de formación y experiencia solicitada.

- El proponente deberá garantizar que el personal asignado no registre antecedentes penales ni disciplinarios y en el caso de personal masculino deberán contar con la libreta militar. En caso de inhabilidades el contratista asume la responsabilidad en cada caso y deberá postular a otra persona con iguales o mejores condiciones al personal postulado inicialmente.

- El servicio será prestado por proponente adjudicatario utilizando el equipo de trabajo necesario para la ejecución de las actividades de pruebas funcionales, no funcionales y aseguramiento de calidad y será únicamente de su responsabilidad el tipo de vinculación de estos con aquel, entendiéndose que no existe ningún tipo de relación laboral entre el equipo de trabajo y/o el contratista y la entidad designada por la corporación o la Coporación.

- En cualquier momento de la ejecución del contrato, el supervisor podrá solicitar cambio del personal del proyecto, si considera que no satisface los requerimientos necesarios para desarrollar adecuadamente el objeto contratado.

- Como requisito en la ejecución del contrato, el supervisor del contrato podrá en determinado momento, solicitar las hojas de vida de los profesionales que se encuentren realizando las actividades asociadas al desarrollo del objeto contratado.

- El proponente deberá garantizar la continuidad de la realización de las actividades del desarrollo del proyecto, independientemente de las vacaciones, incapacidades y/o novedades que se llegarán a presentar con los recursos asignados.

- La entidad adelantara un acuerdo de confidencialidad entre las partes para la protección de información.

- Toda propiedad intelectual que desarrolle el contratista en coherencia con la ejecución del contrato será propiedad de la Corporación Colombia Digital.