--APROBACIÓN--
Luz Adriana Loaiza Moreno
CC53081198
2026-09-21 10:53:58 -05:00

FONDO NACIONAL DE GARANTÍAS S.A. – FNG

DOCUMENTO DE JUSTIFICACIÓN DE LA CONTRATACIÓN

PRESTAR LOS SERVICIOS ESPECIALIZADOS PARA REALIZAR PRUEBAS DE VULNERABILIDADES, ETHICAL HACKING E INGENIERÍA SOCIAL SOBRE LA INFRAESTRUCTURA TECNOLÓGICA Y LOS FUNCIONARIOS DEL FNG

BOGOTÁ D.C., SEPTIEMBRE DE 2026

I. DEFINICIÓN DE LA NECESIDAD

1. Naturaleza del FNG y Objeto Social.

El Fondo Nacional de Garantías – FNG S. A., es una sociedad anónima de carácter mercantil y de economía mixta del Orden Nacional cuya creación fue autorizada mediante el Decreto 3788 del 29 de diciembre de 1981, vinculada al Ministerio de Hacienda y Crédito Público y sometida a la supervisión de la Superintendencia Financiera.

Que de conformidad con lo dispuesto en el artículo 241 del Decreto Ley 663 de 1993, modificado por el artículo 38 de la Ley 2069 de 2020 el objeto social del Fondo Nacional de Garantías S.A., consiste en obrar de manera principal pero no exclusiva como fiador o bajo cualquier otra forma de garante de toda clase de operaciones activas de las instituciones financieras, valores representativos de deuda, valores representativos de capital social y fondos de inversión colectiva conforme la regulación vigente, con los usuarios de sus servicios, sean personas naturales o jurídicas, así como actuar en tales calidades respecto de dicha clase de operaciones frente a otra especie de establecimientos de crédito legalmente autorizados para desarrollar actividades, sean nacionales o extranjeros, patrimonios autónomos constituidos ante entidades que legalmente contemplen dentro de sus actividades el desarrollo de estos negocios, las entidades cooperativas y demás formas asociativas del sector solidario, las fundaciones, las corporaciones, las cajas de compensación familiar y otros tipos asociativos privados o públicos que promuevan programas de desarrollo social.

Adicionalmente, el Fondo Nacional de Garantías S.A., podrá otorgar avales o garantías a valores de naturaleza negociable que hagan parte de una emisión, así como a favor de vehículos de inversión como fondos de inversión colectiva que tengan como propósito impulsar y/o apalancar proyectos productivos generadores de crecimiento económico y empleo.

El Fondo Nacional de Garantías S.A., dentro del giro ordinario de sus negocios, está facultado para otorgar garantías sobre créditos y otras operaciones activas de esta naturaleza que se contraigan a favor de entidades que no posean la calidad de intermediarios financieros, por parte de personas naturales o jurídicas que obran como comercializadores o distribuidores de sus productos y bienes en el mercado.

Se entenderán comprendidos dentro de las actividades propias de su objeto social, todas las enajenaciones a cualquier título que el FNG S.A., realice de bienes muebles o inmuebles cuyas propiedades se le hayan transferido o que figuren a su nombre como consecuencia de negociaciones o producto del ejercicio de las acciones judiciales o extrajudiciales que ejercite tendientes a obtener la recuperación de las sumas que hubiere satisfecho a los beneficiarios de las garantías.

2. De las funciones del Director de Seguridad de la Información

De acuerdo con la normativa interna vigente y el marco de funciones establecido para la gestión de riesgos y seguridad de la información, la Dirección de Seguridad de la Información tiene a su cargo, entre otras, las siguientes responsabilidades:

(...)24. Definir, liderar y orientar las estrategias y políticas del FNG en materia de seguridad de la información garantizando su administración para el cumplimiento de las metas y objetivos de la entidad.

Así mismo, conforme a las responsabilidades y funciones asignadas al cargo de Director de Seguridad de la Información dentro de la estructura organizacional de la entidad, se contemplan, entre otras, las siguientes funciones:

1. Apoyar la identificación de riesgos de seguridad de la información, análisis de amenazas y vulnerabilidades de los activos de la información.
2. Realizar pruebas de vulnerabilidades, Ingeniería Social y Hacking Ético, coordinando con la Vicepresidencia de TI su remediación y aseguramiento, para minimizar el riesgo de ataque cibernético.
3. Definir y promover la implementación de lineamientos, estrategias y controles en materia de seguridad de la información.
4. Liderar la gestión de riesgos de seguridad de la información y ciberseguridad, incluyendo su identificación, evaluación, priorización y tratamiento.
5. Mantener informada a la alta dirección sobre los riesgos, amenazas y tendencias relevantes que puedan impactar la seguridad de la información de la entidad.
6. Coordinar las acciones necesarias para la protección de los activos de información y el cumplimiento de los objetivos estratégicos de seguridad.

Por lo anterior, el FNG, está en la constante búsqueda de fortalecer la seguridad de la información que es gestionada por diferentes procesos institucionales, con el fin de contribuir a que la entidad cuente con adecuadas estrategias y mecanismos que garanticen la confidencialidad de los datos y el cumplimiento de las disposiciones reglamentarias definidas dentro del marco de la ley de protección de datos personales.

3. Antecedentes:

Una vez verificado en el registro histórico de la Entidad, se evidenció que en los últimos años se han suscrito contratos con características técnicas iguales o similares a las del presente proceso. Resulta importante precisar que los últimos procesos llevados por la entidad se detallan con un alcance similar corresponden al detallado a continuación:

Contrato	Contratista	Objeto	Valor	Plazo de ejecución
2024400076	2SECURE S.A.S.	Prestar el servicio de pruebas de vulnerabilidades, Ethical Hacking e Ingeniería Social a la Infraestructura Tecnológica y funcionarios del FNG	41.037.864	El plazo de ejecución del contrato fue hasta el 31 de

				diciembre de 2024, término contado a partir de la suscripción del contrato.
2025400075	Softweb asesores SAS	Prestar servicios de pruebas de ingeniería social, análisis de vulnerabilidades y ethical hacking sobre la infraestructura tecnológica del FNG.	45.190.250	El plazo del presente contrato fue hasta el 31 de diciembre de 2025 término contado a partir de la suscripción del contrato.

Los resultados obtenidos como parte del desarrollo de los contratos permitieron identificar oportunidades de mejora y definir planes de remediación encaminados a fortalecer la postura de seguridad y ciberseguridad del FNG. No obstante, considerando la naturaleza dinámica de las amenazas cibernéticas, la incorporación permanente de nuevas tecnologías, cambios en la infraestructura tecnológica y la necesidad de verificar la efectividad de las acciones implementadas, se requiere mantener un proceso continuo de evaluación y validación de controles de seguridad.

En este contexto, surge la necesidad de adelantar una nueva contratación durante la vigencia 2026 que permita realizar pruebas especializadas de análisis de vulnerabilidades, Ethical Hacking, revalidación de remediaciones (re-test) e ingeniería social y/o pruebas de intrusión, con el fin de identificar nuevas vulnerabilidades, validar la efectividad de los controles implementados y dar cumplimiento a los lineamientos de la Política de Gobierno Digital, particularmente aquellos orientados a la ejecución de monitoreos de seguridad sobre los activos digitales institucionales, incluyendo actividades de escaneo de vulnerabilidades para la detección oportuna de debilidades de seguridad, así como a las prácticas de hardening o endurecimiento de sistemas, encaminadas a reducir la superficie de exposición, eliminar configuraciones por defecto y fortalecer la protección de la infraestructura tecnológica frente a amenazas y ataques cibernéticos. al numeral 2.3.7 de la Circular Externa 007 de 2018 de la Superintendencia Financiera de Colombia y a las mejores prácticas aplicables en materia de seguridad de la información y ciberseguridad.

4. Descripción de la necesidad

Marco jurídico.

La adecuada gestión de vulnerabilidades constituye un elemento esencial para la protección de los activos de información y la mitigación de riesgos de ciberseguridad. En este contexto, una vulnerabilidad corresponde a una debilidad presente en un activo o control que puede ser explotada por una amenaza, incluyendo aquellas derivadas de la interacción de los sistemas en el ciberespacio, conforme a lo señalado en la Circular Básica Jurídica (C.E. 006 de 2025, que reexpidió y actualizó la C.E. 029 de 2014), Parte I, Título II, Capítulo I de cumplimiento.

2.3.7 Análisis de vulnerabilidades

Las entidades deben implementar un sistema de análisis de vulnerabilidades informáticas que cumpla al menos con los siguientes requisitos:

2.3.7.1. Estar basado en un hardware de propósito específico (appliance) totalmente separado e independiente de cualquier dispositivo de procesamiento de información, de comunicaciones y/o de seguridad informática.

2.3.7.2. Generar de manera automática por lo menos 2 veces al año un informe consolidado de las vulnerabilidades encontradas. Los informes de los últimos 2 años deben estar a disposición de la SFC.

2.3.7.3. Las entidades deben tomar las medidas necesarias para remediar las vulnerabilidades detectadas en sus análisis.

2.3.7.4. Realizar un análisis diferencial de vulnerabilidades, comparando el informe actual con respecto al inmediatamente anterior.

2.3.7.5. Las herramientas usadas en el análisis de vulnerabilidades deben estar homologadas por el CVE (Common Vulnerabilities and Exposures) y actualizadas a la fecha de su utilización.

2.3.7.6. Para la generación de los informes solicitados se debe tomar como referencia la lista de nombres de vulnerabilidades CVE publicada por la corporación Mitre.

En consecuencia, se deja constancia previa y expresa de la necesidad de adelantar el presente proceso contractual, cuyo objeto radica en garantizar la ejecución de las pruebas y el análisis periódico de vulnerabilidades sobre la infraestructura tecnológica y canales digitales de la entidad. La actuación encuentra su fundamento jurídico en lo dispuesto por la Circular Básica Jurídica de la Superintendencia Financiera de Colombia (Parte I, Título II, Capítulo I, numeral 2.3.7 y Parte I, Título IV, Capítulo V, numerales 4.1.11 y 4.2.2), marco normativo que le impone de manera vinculante el deber de autoevaluar periódicamente el riesgo de ciberseguridad y de seguridad de la información dentro de su Sistema de Administración de Riesgo Operativo (SARO), manteniendo dicha evaluación y su plan de acción a disposición de la SFC, para preservar la ciberseguridad y la continuidad operativa.

Impacto presupuestal.

La contratación genera un impacto presupuestal debidamente previsto y respaldado mediante el Certificado de Disponibilidad Presupuestal 200252752 asignado al rubro de **Análisis de vulnerabilidades para fortalecer la seguridad de la infraestructura tecnológica del FNG**.

Consecuencia de no realizar la contratación.

De no llevarse a cabo dicho proceso, se podrían materializar riesgos que generan afectación sobre los activos de información del FNG, asociados a incidentes de seguridad de la información, ciberataques, indisponibilidad de servicios y la consecuente afectación patrimonial y reputacional.

Necesidad de la actuación.

Con el fin de identificar oportunamente debilidades y validar la efectividad de los controles implementados, es necesario realizar actividades especializadas de evaluación de seguridad que permitan fortalecer la gestión de riesgos y la protección de los activos de información de la entidad.

1. **Análisis de vulnerabilidades**: Permite identificar debilidades en los activos de información y establecer acciones de remediación para reducir la exposición a riesgos de seguridad.

2. **Hacking Ético:** Permite evaluar la efectividad de los controles de seguridad mediante pruebas controladas, identificando oportunidades de mejora en la protección de la infraestructura tecnológica y la información.

3. **Pruebas de Ingeniería Social:** Permiten evaluar el nivel de concienciación de los colaboradores frente a amenazas asociadas al factor humano y fortalecer la cultura de seguridad de la información.

Justificación de la necesidad.

En atención a lo expuesto, se requiere la contratación de un servicio especializado e independiente que permita evaluar el nivel de seguridad de la información y ciberseguridad de la infraestructura tecnológica del Fondo Nacional de Garantías S.A. mediante la ejecución de pruebas de análisis de vulnerabilidades, Hacking Ético e ingeniería social. Estos ejercicios permitirán identificar oportunamente debilidades, validar la efectividad de los controles implementados, establecer acciones de mitigación frente a los riesgos identificados y fortalecer la protección de los activos de información, contribuyendo a la continuidad de la operación y a la reducción de impactos operativos, el cumplimiento normativo vigente por parte de la Entidad.

Descripción del servicio.

Se requiere contratar un servicio servicio especializado e independiente que evalué el nivel de madurez de la Seguridad de la Información y ciberseguridad de la Infraestructura Tecnológica del FNG mediante pruebas llamadas **"Pruebas de Vulnerabilidades y Ethical Hacking"** en modalidad de caja negra, caja gris y pruebas de Ingeniería Social para ser ejecutadas sobre los activos del FNG.

Los objetivos del documento de anexo técnico de Seguridad de la Información para la prestación de servicios para la ejecución de pruebas de vulnerabilidad, Ethical hacking e ingeniería social para el FNG se detallan a continuación:

1. Efectuar una (1) prueba de análisis de vulnerabilidades en modalidad de caja negra, la cual debe ser desarrollada en el segundo semestre de 2026.
2. Efectuar una (1) prueba de análisis de vulnerabilidades sobre la red de datos interna en modalidad de caja gris para 200 activos definidos por el FNG, en el segundo semestre de 2026.
3. Efectuar una (1) prueba de re-test a los objetivos externos e internos con los que cuenta el FNG.
4. Efectuar una (1) prueba de ingeniería social dirigida a 100 colaboradores.

5. Análisis acerca de Acuerdo Marco de Precios.

Finalmente, se realizó la revisión de los Acuerdos Marco de Precios vigentes en la página de Colombia Compra Eficiente (https://www.colombiacompra.gov.co) sin encontrar ninguno que se ajuste a las características del bien y/o servicio que el **FNG** requiere contratar.

6. Supervisión.

En virtud de lo establecido en el Manual de Supervisión del **FNG**, en el numeral 6.1.1.1.1. el cual indica que las funciones del cargo que desempeña la persona que sea designada como supervisor(a), deben guardar relación con el contrato a vigilar de manera le permitan hacer un seguimiento adecuado acerca del cumplimiento del objeto del contrato a supervisar, la Vicepresidencia de Riesgos, determina que el profesional más idóneo para ejercer la supervisión del contrato es Director de Seguridad de la Información.

II. INSTANCIA APROBATORIA DE LA CONTRATACIÓN

INSTANCIA APROBATORIA:	No. del Acta:	Fecha del Acta:
De acuerdo con el literal a) numeral 3.5. del Manual de Contratación del **FNG,** los procesos cuyo valor supere el valor de la mínima cuantía deben ser aprobados en el Comité de Adquisición de Bienes y Servicios.	No Aplica	No Aplica

III. MODALIDAD DE SELECCIÓN

En virtud de lo establecido en el numeral 3.4.1.1 del Manual de Contratación de la Entidad, el FNG determina la escogencia del contratista a través de la modalidad de Contratación de Mínima cuantía, al tratarse de adquisiciones con presupuesto estimado superior a los gastos de caja menor, y hasta sesenta y cinco (65) salarios mínimos legales mensuales vigentes (SMMLV).

IV. OBJETO A CONTRATAR

Prestar los servicios especializados para realizar pruebas de vulnerabilidades, Ethical hacking e ingeniería social sobre la infraestructura tecnológica y los funcionarios del FNG.

V. CERTIFICACIONES O DOCUMENTOS DE CONTENIDO TÉCNICO

El proponente deberá relacionar el equipo de trabajo que se requerirá para el desarrollo de las pruebas considerando para cada una de las personas involucradas:

1. Rol/función de la persona.
2. Profesión.
3. Experiencia en años en proyectos similares.
4. Certificaciones relacionadas con el objeto contractual.

Previo al inicio de ejecución del contrato el Supervisor verificará que el personal que realizará las actividades contratadas deberá contar con al menos una (1) de las siguientes certificaciones:

1. Ethical Hacking Certified C-EH.
2. Certificado en ejecución de pruebas de penetración LPT.

3. Certificado como especialista en Seguridad E.C.S.S. / (CISM).

En caso de contar con otra certificación relacionada, la misma puede ser mencionada y justificada.

El proponente deberá especificar el tipo de perfil que se requiere por parte del FNG para el desarrollo de cada una de las fases o hitos establecidos como parte del proceso de implementación de la iniciativa.

VI. CARACTERÍSTICAS TÉCNICAS Y OBLIGACIONES ESPECÍFICAS (Aplica para el contratista y/o el FNG)

a. **Características técnicas:** En desarrollo del objeto contractual el contratista deberá prestar sus servicios especializados teniendo en cuenta las siguientes características técnicas:

Características Técnicas:

A continuación, se describe los aspectos a tener en cuenta para el diseño e implementación de las pruebas:

1. **Tecnología de la Información - TI:** La arquitectura empresarial abarca la tecnología utilizada. Esto implica la definición de estándares tecnológicos, la evaluación de la infraestructura actual y futura, y la identificación de soluciones tecnológicas que respalden los procesos y objetivos empresariales.
2. **Datos y Gestión de la Información:** La gestión de datos es un componente fundamental de la arquitectura empresarial. Se debe definir cómo se capturan, almacenan, procesan y utilizan los datos en el FNG. Esto incluye la definición de modelos de datos, sistemas de gestión de datos y estrategias de análisis.
3. **Seguridad y Cumplimiento Normativo:** Se deben definir y aplicar políticas y prácticas de seguridad de la información en toda la Entidad. Además, la arquitectura empresarial debe asegurarse de que la organización cumpla con todas las regulaciones y estándares relevantes.
4. **Gestión de Cambios:** La implementación de la arquitectura empresarial a menudo implica cambios significativos. Se deben establecer planes de gestión de cambios que aborden la transición hacia la nueva arquitectura, incluyendo la comunicación, la formación y la gestión de resistencias.
5. **Medición y Monitoreo:** La arquitectura empresarial debe definir indicadores clave de rendimiento (KPI) para evaluar el éxito de la implementación y el rendimiento continuo. También se deben establecer mecanismos de monitoreo para asegurarse de que la arquitectura empresarial siga siendo efectiva a lo largo del tiempo.
6. **Comunicación y Colaboración:** Fomentar la comunicación y la colaboración entre los diferentes departamentos y equipos dentro del FNG y es esencial para una implementación exitosa de la arquitectura empresarial.
7. **Plan Estratégico de Tecnologías de la Información y las Comunicaciones y Transformación Digital (PETI):** En este componente se abarcan aspectos relacionados con la tecnología y su integración en la entidad; a continuación, los aspectos para tener en cuenta en el fortalecimiento de este.
8. **Estrategia Tecnológica:** La Vicepresidencia de TIC y TD en sus funciones tiene la función de definir la visión y dirección tecnológica a corto, mediano y largo plazo de la entidad, incluyendo la adopción de nuevas tecnologías y la actualización de las existentes.
9. **Gobierno y Gestión Tecnológica:** El Fondo Nacional de Garantías – FNG, establece las estructuras y procesos para la toma de decisiones, la asignación de recursos y la supervisión de las iniciativas tecnológicas.

10. **Infraestructura Tecnológica:** La Dirección de Infraestructura realizará la planificación y el mantenimiento de la infraestructura de hardware, redes y sistemas necesarios para soportar las operaciones del FNG.
11. **Ciberseguridad:** Siendo hoy en día un tema sensible para todas las entidades, el FNG definirá las políticas, prácticas y tecnologías para proteger los activos digitales y los datos confidenciales contra amenazas cibernéticas.
12. **Desarrollo y Mantenimiento de Sistemas:** La Dirección de Desarrollo y Aplicaciones establece las prácticas para el desarrollo, implementación y mantenimiento de aplicaciones y sistemas informáticos al servicio del FNG.
13. **Transformación Digital:** Una de las principales funciones de la Vicepresidencia de Transformación Digital e Innovación es identificar oportunidades que tiene el FNG para mejorar y optimizar los procesos a través de soluciones digitales, como automatización y digitalización.
14. **Continuidad del Negocio:** Este aspecto para el FNG es fundamental, con el fin de definir planes y estrategias para garantizar la disponibilidad de sistemas y servicios en situaciones de emergencia o interrupciones.
15. **Capacitación y Desarrollo del Personal:** EL FNG prepara el talento humano con habilidades desarrolladas al tenerlos en un plan que incluye la formación en habilidades tecnológicas y el fomento de una cultura de Seguridad de la información.
16. **Gestión de Ciberseguridad:** Dentro del ecosistema del FNG se encuentran herramientas que permiten realizar pruebas internas de análisis de vulnerabilidades y ethical hacking, lo que contribuye a efectuar remediaciones de manera oportuna.

Entregables

FASE 1

Pruebas de análisis de vulnerabilidades Modalidad caja negra.

DESCRIPCIÓN	ACTIVIDADES	ENTREGABLES
Planeación y organización	Definir el plan de trabajo de las pruebas a ejecutar. Realizar el análisis de interesados claves. Definir necesidades por parte del FNG y del proveedor. Definir y realizar la presentación de la metodología a seguir en la ejecución de las pruebas.	Plan de trabajo (cronograma) de ejecución de las pruebas de análisis de vulnerabilidades. Recursos institucionales (competencias del personal, conocimiento de la institución, procesos documentados, entre otros) y accesos requeridos para el desarrollo de las pruebas.
Ejecución	1. Efectuar una (1) prueba de análisis de vulnerabilidades en modalidad de caja negra. En caso de que dicho análisis identifique vulnerabilidades que puedan comprometer la seguridad de la información o de los servicios	Documento con el plan de ejecución de cada una de las pruebas a realizar, en sus distintas modalidades.

	evaluados, deberá realizarse una prueba de penetración en modalidad de caja negra, con el fin de evaluar el alcance real de riesgo identificado y validar la efectividad de los controles existentes. 2. Las pruebas deberán realizarse sin conocimiento previo de credenciales, configuraciones o arquitectura interna.	
Resultados	Emitir los informes resultantes del desarrollo de cada una de las pruebas a ser ejecutadas.	Informes detallados de las posibles brechas de seguridad identificadas sobre los objetivos declarados al final de las pruebas (caja negra). Dichos informes deben contener los hallazgos y recomendaciones para cada escenario de prueba realizada. Los resultados como mínimo deberán incluir la lista de vulnerabilidades identificadas con detalles como: • Nombre de la vulnerabilidad • Descripción del problema • Servicio o sistema afectado • Gravedad (criticidad) • Impacto potencial • Recomendación para corregir la vulnerabilidad identificada. Estas vulnerabilidades deberán clasificarse usando estándares reconocidos, como: • CVSS (Common Vulnerability Scoring System)

FASE II

Pruebas de análisis de vulnerabilidades Modalidad Caja Gris

DESCRIPCIÓN	ACTIVIDADES	ENTREGABLES

Planeación y organización	Definir el plan de trabajo de las pruebas a ejecutar. Realizar el análisis de interesados claves. Definir necesidades por parte del FNG y del proveedor. Definir y realizar la presentación de la metodología a seguir en la ejecución de las pruebas.	Plan de trabajo (cronograma) de ejecución de las pruebas de análisis de vulnerabilidades. Recursos institucionales (competencias del personal, conocimiento de la institución, procesos documentados, entre otros) y accesos requeridos para el desarrollo de las pruebas.
Ejecución	Efectuar una (1) prueba de análisis de vulnerabilidades sobre la red de datos interna en modalidad de caja gris para 200 activos definidos por el FNG, en el segundo semestre de 2026.	Documento con el plan de ejecución de cada una de las pruebas a realizar, en sus distintas modalidades.
Resultados	Emitir los informes resultantes del desarrollo de cada una de las pruebas a ser ejecutadas.	Informes detallados de las posibles brechas de seguridad identificadas sobre los objetivos declarados al final de las pruebas (caja gris). Dichos informes deben contener los hallazgos y recomendaciones para cada escenario de prueba realizada. Los resultados como mínimo deberán incluir la lista de vulnerabilidades identificadas con detalles como: • Nombre de la vulnerabilidad • Descripción del problema • Servicio o sistema afectado • Gravedad (criticidad) • Impacto potencial • Recomendación para corregir la vulnerabilidad identificada. Estas vulnerabilidades deberán clasificarse usando estándares reconocidos, como: • CVSS (Common Vulnerability Scoring System)

FASE III

Prueba de re-test a los objetivos externos e internos del FNG.

DESCRIPCIÓN	ACTIVIDADES	ENTREGABLES
Alcance y preparación	Confirmar el listado exacto de hallazgos a retestear (IDs del informe, CVE, Activo afectado). Confirmar ventana de tiempo y accesos necesarios	Lista de Hallazgos a verificar con sus IDs y activos asociados.
Ejecución	Verificación del estado actual de cada vulnerabilidad previamente reportada	Tabla de resultados por hallazgo verificado
Resultados	Emitir el informe resultado de las pruebas de validación adelantadas	Informe final de re-test con el estado anterior y actual de cada una de las vulnerabilidades analizadas. El informe deberá incluir el porcentaje de hallazgos corregidos, hallazgos pendientes y hallazgos reincidentes.

FASE IV

Pruebas de Ingeniería Social

DESCRIPCIÓN	ACTIVIDADES	ENTREGABLES
Planeación y organización (Fase preliminar y visión)	Plan de trabajo de las pruebas a ser ejecutadas. Definición del tipo de pruebas a ser desarrolladas de acuerdo con los lineamientos establecidos de común acuerdo con el FNG.	Cronograma de las actividades a ser ejecutadas como parte del desarrollo de la prueba de ingeniería social.
Ejecución	Efectuar una (1) prueba completa de Ingeniería Social para 100 usuarios.	Documento con el plan de implementación y desarrollo de la prueba a ejecutar.
Resultados	Emitir el informe resultante del desarrollo de la prueba a ser ejecutada.	Informe que contenga, entre otras, la siguiente información:

	La identificación individual únicamente será entregada al supervisor del contrato para fines de sensibilización y mejora.	• Porcentaje de personas que cayeron en el engaño. • Listado de objetivos que fueron engañados y cómo. Bajo acceso restringido del FNG y conforme al protocolo de tratamiento de datos personales. • Impacto potencial ante un ataque real. • Documentación de cómo se realizó la prueba. • Detalle y soporte de las evidencias y resultados de las pruebas de ingeniería social ejecutadas.

Obligaciones especificas:

1. Efectuar una (1) prueba de análisis de vulnerabilidades en modalidad de caja negra. En caso de que dicho análisis identifique vulnerabilidades cuya explotación pueda comprometer la seguridad de la información o de los servicios evaluados, deberá realizarse una prueba de penetración controlada en modalidad de caja negra, con el fin de evaluar el alcance real del riesgo identificado y validar la efectividad de los controles existentes.
2. Efectuar una (1) prueba de análisis de vulnerabilidades sobre la red de datos interna en modalidad de caja gris para 200 activos definidos por el FNG.
3. Efectuar una (1) prueba de intrusión (una ejecución) para 5 activos de la red interna del fondo.
4. Efectuar una (1) prueba de re-test a los objetivos externos e internos con los que cuenta el FNG.
5. Efectuar una (1) prueba de ingeniería social dirigida a 100 colaboradores de FNG.
6. Realizar acompañamiento al personal del FNG durante la ejecución del contrato en la identificación y análisis de vulnerabilidades, así como en las recomendaciones para la remediación.
7. Entregar al Supervisor del Contrato los informes detallados de las brechas de seguridad informática realizadas a los objetivos declarados en las pruebas de vulnerabilidad, Ethical Hacking e Ingeniería Social. Dicho informe debe contener los hallazgos y recomendaciones para cada escenario de prueba realizada.
8. El contratista se compromete a tomar todas las medidas necesarias para que la información no llegue a manos de terceros en ninguna circunstancia y se obliga a no utilizarla para ningún objeto diferente al de adelantar las tareas que se deriven directamente del cumplimiento de las actividades que se desprenden del contenido del contrato.
9. Cumplir con las características técnicas del presente contrato.
10. Cumplir con la oferta presentada y con todas sus características técnicas definidas, la cual hace parte integral del presente contrato.

VII. FACTORES DE SELECCIÓN

Con el fin de garantizar la selección objetiva y para los fines que se pretenden satisfacer con esta contratación; se tendrán en cuenta los siguientes aspectos con su respectiva ponderación, así:

Factores de Evaluación			Puntaje Total
Criterio Calidad: (Según lo establezca el área)	**Ofrecimiento**	**Puntaje**	N/A
	N/A	N/A	
	N/A	N/A	
	N/A	N/A	
	N/A	N/A	
Criterio Económico (Según lo establezca el área)			N/A
Apoyo a la Industria Nacional			N/A
Apoyo al Emprendimiento a Mujeres			N/A
Vinculación de Trabajadores en condición de Discapacidad (Aplica cuando se establezcan criterios de calidad)			N/A
Total			N/A

VIII. PRESUPUESTO ESTIMADO PARA LA CONTRATACIÓN

1. Presupuesto Estimado

Para determinar el valor del contrato de conformidad con el numeral 3.8.4.1.5 literal e) del Manual de Contratación del FNG y 2.1.1.7 ibidem, el área de la Dirección de Seguridad de la Información empleó el mecanismo de solicitud de cotizaciones mediante correo electrónico institucional a los siguientes ocho (8) proveedores: **INVOTECSA SAS**, **CEO INVESTIGACIONES DIGITALES Y SEGURIDAD S.A.S**, **SISA**, **SOFTSECURITY S.A.S.**, **CINTEL**, **QC INGENIERIA LTDA**, **FORENSICT/KURUVA**, **CCD COMPAÑIA DE CIBERSEGURIDAD Y DEFENSA S.A.S.,** el pasado 14, Julio, del 2026, de las cuales se obtuvo respuesta por parte de los siguientes cuatro (4) proveedores **(INVOTECSA SAS, CEO INVESTIGACIONES DIGITALES Y SEGURIDAD S.A.S, FORENSICT/KURUVA, CCD COMPAÑIA DE CIBERSEGURIDAD Y DEFENSA S.A.S.)**.

De acuerdo con lo anterior, la Dirección de Seguridad de la Información procedió a consolidar el comparativo de las cotizaciones allegadas con el fin de analizar y evaluar las propuestas bajo los mismos criterios técnicos, jurídicos y económicos establecidos por la entidad como se relaciona a continuación:

			CCD		CEOIDS		KURUVA/FORENSICT		INVOTECSA	
ITEM	DESCRIPCION DEL BIEN Y/O SERVICIO	CANTIDAD	Valor Unitario Antes de IVA	Valor Total	Valor Unitario Antes de IVA	Valor Total	Valor Unitario Antes de IVA	Valor Total	Valor Unitario Antes de IVA	Valor Total
1	Efectuar una (1) prueba de penetración y una (1) prueba de análisis de vulnerabilidades en modalidad de caja negra, la cual debe ser desarrollada en el segundo semestre de 2026.	1	$ 11.931.818,00	$ 11.931.818,00	$ 13.000.000,00	$ 13.000.000,00	$ 28.800.000,00	$ 28.800.000,00	$ 13.859.389,00	$ 13.859.389,00
2	Efectuar una (1) prueba de análisis de vulnerabilidades sobre la red de datos interna en modalidad de caja gris para mínimo 200 activos definidos por el FNG, en el segundo semestre de 2026.	1	$ 11.931.818,00	$ 11.931.818,00	$ 20.000.000,00	$ 20.000.000,00	$ 24.000.000,00	$ 24.000.000,00	$ 14.683.689,00	$ 14.683.689,00
3	Efectuar una (1) prueba de re-test a los objetivos externos e internos con los que cuenta el FNG, esta prueba deberá implementarse en el segundo semestre de 2026.	1	$ 11.931.818,00	$ 11.931.818,00	$ 8.000.000,00	$ 8.000.000,00	$ -	$ -	$ 22.040.689,00	$ 22.040.689,00
4	Efectuar una (1) prueba de ingeniería social de acuerdo con los lineamientos establecidos de común acuerdo con el FNG y a los funcionarios respectivos, en el segundo semestre de 2026.	1	$ 11.931.818,00	$ 11.931.818,00	$ 6.000.000,00	$ 6.000.000,00	$ 12.000.000,00	$ 12.000.000,00	$ 15.289.789,00	$ 15.290.789,00
			Subtotal	$ 47.727.272,00	Subtotal	$ 47.000.000,00	Subtotal	$ 64.800.000,00	Subtotal	$ 65.874.556,00
		19%	IVA(Si aplica)	$ 9.068.181,68	IVA(Si aplica)	$ 8.930.000,00	IVA(Si aplica)	$ 12.312.000,00	IVA(Si aplica)	$ 12.516.165,64
			Valor Total	$ 56.795.453,68	Valor Total	$ 55.930.000,00	Valor Total	$ 77.112.000,00	Valor Total	$ 78.390.721,64

Una vez analizado el cuadro comparativo de las cotizaciones, y teniendo en cuenta que los valores cotizados por las sociedades **INVOTECSA SAS, CEO INVESTIGACIONES DIGITALES Y SEGURIDAD S.A.S, FORENSICT/KURUVA, CCD COMPAÑIA DE CIBERSEGURIDAD Y DEFENSA S.A.S.,** presentan diferencias porcentuales significativas, y de conformidad con lo establecido en el numeral 3.8.4.1.5, literal e), subnumeral ii) del Manual de Contratación del Fondo Nacional de Garantías S.A. – FNG, se realizó el análisis de precios históricos tomando como referencia el último contrato celebrado para la prestación de servicios con características técnicas y alcance similares a los requeridos para la presente contratación.

Para tal efecto, se tomó como antecedente del Contrato No. **2025400075** celebrado con la empresa **SOFTWEB ASESORES S.A.S**., cuyo objeto consistió en "Prestar servicios de pruebas de ingeniería social, análisis de vulnerabilidades y Ethical Hacking sobre la infraestructura tecnológica del FNG", por valor de **$45.190.250.**

Análisis de precios históricos.

Se verificó que las actividades desarrolladas en el marco de dicho contrato corresponden al mismo servicio que se pretende contratar para la vigencia 2026, relacionado con la realización de pruebas de vulnerabilidades, Ethical Hacking e Ingeniería Social sobre la infraestructura tecnológica y los funcionarios del FNG, manteniéndose las características y el alcance técnico del servicio requerido.

En cumplimiento de la metodología prevista en el Manual de Contratación, se tomó como base el valor del último contrato y se efectuó su actualización con el Índice de Precios al Consumidor (IPC) correspondiente a la vigencia 2025, certificado por el Departamento Administrativo Nacional de Estadística – DANE, cuya variación anual fue del **5,10 %**.

La actualización del valor histórico se realizó mediante la siguiente fórmula:

Valor histórico actualizado = Valor contrato 2025 × (1 + IPC 2025)

Valor histórico actualizado = $45.190.250 × (1 + 5,10 %)

Valor histórico actualizado = $47.494.953

En consecuencia, el valor actualizado del contrato correspondiente a la vigencia 2025 asciende a la suma de **$47.494.953**, constituyéndose este valor en el referente histórico actualizado para efectos de analizar la razonabilidad del presupuesto estimado para la contratación de la vigencia 2026.

Vigencia	Contrato / Contratista	Valor histórico (IVA incluido)	IPC aplicado	Valor histórico actualizado
2025	Contrato No. 2025400075 – Softweb Asesores S.A.S.	$45.190.250	5,10%	**$47.494.953**

De acuerdo con lo anterior, y con el objetivo de garantizar que la propuesta económica de menor valor presentada por el proponente **CEO INVESTIGACIONES DIGITALES Y SEGURIDAD S.A.S** se encuentre a precios de mercado, se procedió a aplicar algunas métricas estadísticas como el promedio, la desviación estándar, el límite inferior y superior de las cotizaciones como se muestra a continuación.

No.	EMPRESA	VALOR TOTAL OFERTADO INCLUIDO IVA
1	CCD	$ 56.795.454
2	CEOIDS	$ 55.930.000
3	KURUBA	$ 77.112.000
4	INVOTECA	$ 78.390.722
5	CTO 2025400075	$ 45.190.250
	Promedio	$ 62.683.685
	Desv Estándar	$ 12.970.668
	Límite Inferior	$ 49.713.018
	Límite Superior	$ 75.654.353

De acuerdo con lo anterior se evidencia que la propuesta económica de menor valor se encuentra a precios de mercado, por lo cual la Dirección de Seguridad de la Información procedió a elegir la propuesta económica del proponente **CEO INVESTIGACIONES DIGITALES Y SEGURIDAD S.A.S,**

teniendo en cuenta la modalidad de contratación de mínima cuantía, cuyo único criterio de selección es el menor valor ofertado que cumpla las características técnicas exigidas.

En consecuencia, se establece que el presupuesto estimado para la presente contratación es por la suma de **($55.930.000) CINCUENTA Y CINCO MILLONES NOVECIENTOS TREINTA MIL PESOS IVA INCLUIDO.**

Considerando la cuantía de la presente contratación, en virtud de lo establecido en el numeral 3.4.1.1 del Manual de Contratación de la Entidad, el **FNG** determina la escogencia del contratista a través de la modalidad de selección de mínima cuantía tomando como único criterio de selección del contratista el ofrecimiento económico más bajo. Conforme el procedimiento contemplado en el numeral 3.8.4.3.5.4. se establece como proveedor seleccionado a la firma **CEO INVESTIGACIONES DIGITALES Y SEGURIDAD S.A.S**

Tamaño Empresarial

La Entidad procedió a verificar el tamaño empresarial de las empresas cotizantes como se relaciona continuación:

TAMAÑO EMPRESARIAL	INVOTECSA	CCD	CEOIDS	KURUVA
Microempresa			**X**	
Pequeña				
Mediana	**X**	**X**		**X**
Grande				

Constancia: De acuerdo con la manifestado en la fase de sondeo de mercado, se deja constancia que, ni los representantes legales, ni las empresas que representan y que conforman el sondeo de marcado, ni sus socios tienen ninguna inhabilidad, incompatibilidad o conflicto de interés que les impida contratar con el FNG, de acuerdo con lo establecido en la Constitución Política, los artículos 8° y 9° de la Ley 80 de 1993, la Ley 1474 de 2011 y demás normas concordantes, así como el Código de Ética y Buen Gobierno Corporativo publicado en la página Web de la Entidad.

1. Presupuesto Estimado

PRESUPUESTO ESTIMADO	
VALOR SIN IVA	$47.000.000
IVA	$8.930.000

VALOR TOTAL	$55.930.000

2. CDP y/o Vigencia Futura.

Nro.	Fecha	Valor
200252752	03 septiembre 2026	55.930.000

IX. FORMA DE PAGO

El valor de este Contrato es hasta por la suma de **CINCUENTA Y CINCO MILLONES NOVECIENTOS TREINTA MIL PESOS ($55.930.000) IVA INCLUIDO,** y todo gasto directo e indirecto en que deba incurrir el contratista, discriminado por vigencia, así:

Vigencia	Valor
2026	**$55.930.000**
Total	**$55.930.000**

Los pagos se realizarán teniendo en cuenta los valores unitarios ofertados por el contratista seleccionado:

ITEM	DESCRIPCIÓN DEL BIEN Y/O SERVICIO	Cantidad	Valor Unitario	IVA	Valor Total
1	Efectuar una (1) prueba de penetración y una (1) prueba de análisis de vulnerabilidades en modalidad de caja negra, la cual debe ser desarrollada en el segundo semestre de 2026.	1	$13.000.000	$2.470.000	$15.470.000
2	Efectuar una (1) prueba de análisis de vulnerabilidades sobre la red de datos interna en modalidad de caja gris para mínimo 200 activos definidos por el FNG, en el segundo semestre de 2026.	1	$20.000.000	$3.800.000	$23.800.000
3	Efectuar una (1) prueba de re-test a los objetivos externos e internos con los que cuenta el FNG, esta prueba deberá implementarse en el segundo semestre de 2026.	1	$8.000.000	$1.520.000	$9.520.000
4	Efectuar una (1) prueba de ingeniería social de acuerdo con los lineamientos establecidos de común acuerdo con el FNG y a los funcionarios respectivos, en el segundo semestre de 2026.	1	$6.000.000	$1.140.000	$7.140.000
				TOTAL	$55.930.000

Estructura de Pagos

1. El FNG realizará un primer pago por valor de **VEINTISIETE MILLONES NOVECIENTOS SESENTA Y CINCO MIL PESOS M/CTE ($27.965.000), INCLUIDO IVA,** equivalente al 50% del valor del contrato, previa aprobación y recibo a satisfacción por parte del Supervisor del Contrato de los documentos e informe de ejecución con sus soportes de las pruebas de penetración y prueba de análisis de vulnerabilidades en modalidad de caja negra y las pruebas de análisis de vulnerabilidades en modalidad de caja gris para mínimo 200 activos definidos por el FNG, correspondientes a las fases I y II de la ejecución del contrato, previa presentación de la factura y previa aprobación del reporte de actividades realizadas.

2. El FNG realizará un segundo pago por valor de **VEINTISIETE MILLONES NOVECIENTOS SESENTA Y CINCO MIL PESOS M/CTE ($27.965.000), INCLUIDO IVA,** equivalente al 50% del valor del contrato, previa aprobación y recibo a satisfacción por parte del Supervisor del Contrato de los documentos e informe de ejecución de la prueba de re- test a los objetivos externos e internos con los que cuenta el FNG y de la prueba de ingeniería social, correspondientes a las fases III y IV de la ejecución del contrato, previa presentación de la factura y previa aprobación del reporte de actividades realizadas.

Requisitos de pago: El pago se realizará dentro de los 30 días calendario posteriores al cumplimiento de los siguientes requisitos:

- **Documento de Ejecución:** El contratista deberá entregar un documento en donde conste la ejecución del objeto contractual, el cual deberá contener la evidencia de los servicios prestados, así como los entregables pactados.
- **Certificación de Cumplimiento Laboral:** Debe entregar un certificado firmado por el Representante Legal o Revisor Fiscal que confirme el cumplimiento de las obligaciones laborales y de Seguridad Social, conforme al Artículo 50 de la Ley 789 de 2002.
- **Factura:** La factura debe estar completa y cumplir con los requisitos del Estatuto Tributario.
- **Informe de Supervisión:** Un informe parcial del supervisor que confirme la recepción satisfactoria del trabajo realizado.

X. PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será hasta el 31 de diciembre de 2026, término contado a partir de la aprobación de las garantías exigidas en el presente contrato.

XI. AMPAROS

Aplica X

No aplica	☐
Justificación No aplica	N/A

AMPARO	%	VIGENCIA
Cumplimiento de las obligaciones	20	Con una vigencia igual al plazo de ejecución del contrato y cuatro (4) meses más.
Calidad del servicio	10	Con una vigencia igual al plazo de ejecución del contrato y cuatro (4) meses más.
Otros	N/A	N/A

XII. ACUERDO MARCO DE PRECIOS

¿Existe Acuerdo Marco de Precios vigente para esta contratación?	**SI** ☐	**NO** ☒	N/A
¿El Comité llevó a cabo el estudio de la viabilidad de adherirnos a este Acuerdo Marco de Precios?	**SI** ☐	**NO** ☒	N/A

--APROBACIÓN--
Karen Yiset Gutiérrez Rojas
CC1030555911
2026-09-21 12:48:37 -05:00

Karen Yiset Guitierrez Rojas
VoBo. Director de Contratación

--APROBACIÓN--
Juan David Parada Tovar
CC79956044
2026-09-21 10:53:48 -05:00

Juan David Parada Tovar
VoBo. Profesional que revisa el trámite

XIII. PLAN ANUAL DE ADQUISICIONES

¿Esta Contratación está relacionada en el Plan Anual de Adquisiciones de la Entidad?	**SI** ☒	**NO** ☐

NÚMERO DE CONSECUTIVO PLAN ANUAL DE ADQUISICIONES 106

NOTA: Por favor registrar el consecutivo bajo el cual ésta relacionada la contratación en el Plan Anual de Adquisiciones que se encuentra publicado en la página web de la Entidad.

Si no está relacionado en el Plan Anual de Adquisiciones, describa en el siguiente cuadro la razón por la que no se publicó.	N/A

XIV. VALIDACIONES COMPLEMENTARIAS

COMPONENTE TECNOLÓGICO: Toda contratación que involucre software, plataformas digitales, servicios tecnológicos o infraestructura informática deberá contar con la revisión y aprobación previa de la Vicepresidencia de Transformación Digital e innovación.

Es fundamental garantizar que cada solución tecnológica agregue valor, sea segura y esté alineada con la visión de largo plazo del FNG. Con esta validación el área de TI podrá asegurar:

- Estándares técnicos y de seguridad centralizados
- Gestión eficiente de integraciones y datos
- Control de accesos e identidades
- Evaluación de proveedores y contratos desde el punto de vista tecnológico
- Visión estratégica de Arquitectura Empresarial

SEGURIDAD DE LA INFORMACIÓN: Cuando el objeto contractual implique el acceso o uso de los activos de información del FNG por parte del contratista, o cuando los entregables incluyan componentes relacionados con la seguridad de la información (como control de accesos, registros de auditoría, privacidad de datos, entre otros), el contrato deberá ser revisado previamente por la Subdirección de Seguridad de la Información. Esta revisión tiene como finalidad garantizar que se contemplen adecuadamente las medidas de protección, confidencialidad, integridad y disponibilidad de la información, en cumplimiento de los lineamientos institucionales y normativos vigentes.

SISTEMA INTEGRAL DE ADMINISTRACIÓN DE RIESGOS (CONTINUIDAD DE NEGOCIO)

¿Los servicios contratados se encuentran asociados a un proceso Critico para el FNG? (en caso de requerir orientación, por favor contactar a la subdirección de Riesgos No Financieros)

a. Si su respuesta es positiva, ¿Se pactarán Acuerdos de Niveles de Servicio? (Ver Manual de Contratación del FNG)

b. Si su respuesta al literal “a” es positiva, por favor describir los Acuerdos de Niveles de Servicio a continuación: (Incluir los ANS)

Es preciso mencionar que, los Acuerdos de Nivel de Servicio anteriormente enunciados serán incorporados en el futuro contrato o anexo.

De conformidad con lo anterior, ¿La contratación a realizar contiene componentes que deban ser validados por las siguientes áreas del FNG? (Marque con una X según sea el caso)

Componente Tecnológico		**Seguridad de la información**		**Sistema Integral de Administración de Riesgos (Continuidad de Negocio)**	
SÍ	NO	SÍ	NO	SÍ	NO
X		**X**		**X**	
Vo.Bo. --APROBACIÓN-- Daniel Betancur Salazar CC1128407632 2026-09-21 10:54:37 -05:00 (Área Responsable de la validación)		Vo.Bo. Área Solicitante		Vo.Bo. --APROBACIÓN-- Nelson Jiménez Torres CC79815174 2026-09-21 10:54:35 -05:00 (Área Responsable de la validación)	

XV. DECLARACIÓN HABILITANTE PARA PROCESOS CONTRACTUALES – Conflicto de Interés

En cumplimiento de lo establecido en el Código de Ética y Buen Gobierno Corporativo de la Entidad, los suscriptores del presente documento manifiestan que NO existe ningún tipo de impedimento o conflicto de interés que afecte la verificación técnica y jurídica del proveedor (es) evaluado en los acápites anteriores.

Para tal efecto, se deja constancia de que no concurre ninguna situación que represente un interés particular o directo frente al proceso, ni relación personal, sentimental o legal con alguno de los proponentes o sus socios, incluyendo los grados de parentesco previstos en la normatividad (hasta el cuarto grado de consanguinidad, segundo de afinidad o primero civil).

En caso de que, durante el desarrollo del proceso, se identifique alguna situación que configure un impedimento, esta será reportada de manera inmediata a la Dirección de Cumplimiento, de acuerdo con los procedimientos internos vigentes.

XVI. FIRMAS (Área solicitante)

Adrián Gómez Vargas
CC. 80088226
Firma Electrónica
2026-09-21 14:08:25 -05:00

ADRIÁN GÓMEZ VARGAS
Director de Seguridad de la Información

ANEXO Nro. 1 - MATRIZ DE RIESGOS DE LA CONTRATACIÓN

EVENTO	ETAPA	CONSECUENCIA DE LA OCURRENCIA DEL EVENTO	PROBABILIDAD INHERENTE	IMPACTO INHERENTE	MAYOR IMPACTO INHERENTE	NIVEL DE RIESGO - INHERENTE	ASIGNADO A	PORCENTAJE DE RESPONSABILIDAD	CONTROLES A APLICAR	DETALLE CONTROL	PROPÓSITO DEL CONTROL	CLASIFICACIÓN CONTROL	DISMINUCIÓN PROBABILIDAD	DISMINUCIÓN IMPACTO	PROBABILIDAD RESIDUAL	IMPACTO RESIDUAL	NIVEL DE RIESGO - RESIDUAL
Modificaciones en el plan de trabajo y/o cronograma del contrato.	Contractual	Incumplimiento de los tiempos definidos dentro de la planeación establecida	Probable	Moderado	Tiempo	Alto	Contratista y Contratante	Contratista: 50% Contratante: 50%	Monitoreos periódicos de la ejecución contractual	Responsable: Contratista y contratante Periodicidad: Quincenal Explicación: Reuniones de seguimiento para validar el cumplimiento de los tiempos y condiciones establecidos.	Preventivo	Fuerte	2	0	Raro	Moderado	Bajo
Complejidad en la recolección, tratamiento o emisión de la información, necesaria para la ejecución del contrato.	Contractual	Falta de oportunidad en la ejecución de las pruebas y entregables definidos contractualmente	Probable	Mayor	Tiempo	Alto	Contratista y Contratante	Contratista: 20% Contratante: 80%	Monitoreos periódicos de la ejecución contractual	Responsable: Contratista y contratante Periodicidad: Quincenal Explicación: Reuniones de seguimiento para validar el cumplimiento de los tiempos y condiciones establecidos.	Preventivo	Fuerte	2	0	Raro	Mayor	Medio
Imposibilidad de realizar reuniones, capacitaciones y/o presentaciones dentro del plazo de ejecución.	Contractual	Falta de oportunidad en la ejecución de las pruebas y entregables definidos contractualmente	Raro	Menor	Tiempo	Bajo	Contratista y Contratante	Contratista: 50% Contratante: 50%	Socialización o sensibilización	Responsable: Contratista y contratante Periodicidad: Por demanda Explicación: Definición de plan de comunicaciones y gobierno.	Preventivo	Fuerte	2	0	Raro	Menor	Bajo
Demora en la constitución de las respectivas pólizas del contrato. Se presentan cuando una vez solicitadas las pólizas con el fin de amparar el cumplimiento contractual, el contratista seleccionado no allega las mismas en el termino pactado en el contrato con prontitud.	Precontractual	Imposibilidad de perfeccionamiento del contrato y por tanto, no puede ejecutarse legalmente.	Raro	Menor	Tiempo	Bajo	Contratista	Contratista: 100% Contratante: 0	Socialización o sensibilización	Responsable: Contratante Periodicidad: Antes de firmar el contrato Explicación: Entregar al supervisor del contrato las pólizas exigidas antes de las formalización del contrato	Preventivo	Fuerte	2	0	Raro	Menor	Bajo
Pérdida de capacidad jurídica del CONTRATISTA para ejecutar el contrato por hechos sobrevinientes.	Contractual	El contrato puede ser terminado unilateralmente por la entidad contratante, al evidenciarse la imposibilidad jurídica del contratista para continuar con su ejecución.	Raro	Severo	Alcance	Alto	Contratista	Contratista: 90% Contratante: 10%	Cláusula Contractual	Responsable: Contratante Periodicidad: Al inicio del contrato Explicación: Definición de una clausula relacionando el evento como una causal de terminación del contrato	Correctivo	Fuerte	0	2	Raro	Moderado	Bajo
Efectos desfavorables por alteración, modificación y/o divulgación indebida de la información, violación de seguridad de datos personales o confidenciales a los que se tenga acceso en virtud de la ejecución del contrato.	Contractual	consecuencias legales, contractuales, administrativas y, en algunos casos, penales, dependiendo de la gravedad y la normativa aplicable (como la protección de datos personales o el régimen de contratación pública).	Improbable	Mayor	Alcance	Alto	Contratista	Contratista: 90% Contratante: 10%	Cláusula Contractual	Responsable: Contratante Periodicidad: Al inicio del contrato Explicación: Definición de una clausula relacionando el evento como una causal de terminación del contrato y/o del inicio de acciones legales correspondientes	Correctivo	Fuerte	0	2	Improbable	Menor	Bajo

No entrega al supervisor de los formularios definidos por la Entidad para la actualización de consulta en listas restrictivas realizadas por la Oficina de Cumplimiento del FNG durante la ejecución del contrato. (Actualización Anual o cada novedad respecto del RL o socios del proveedor)	**Contractual**	**Incumplimiento contractual por omisión en una obligación formal requerida para mantener actualizado el proceso de debida diligencia del contratista.**	Raro	Mayor	Alcance	Medio	Contratista	Contratista: 100% Contratante: 0%	Socialización o sensibilización	Responsable: Contratante Periodicidad: Al inicio del contrato Explicación: Socialización de la relevancia de entrega de los documentos solicitados por el FNG	Preventivo	Fuerte	2	0	Raro	Mayor	Medio
No facturación de los servicio prestados por el proveedor que generan saldos en el contrato una vez finalizado el plazo de ejecución	**Poscontractual**	**reconocimiento y pago de las obligaciones contractuales a favor del proveedor.**	Raro	Menor	Costo	Bajo	Contratista y Contratante	Contratista: 50% Contratante: 50%	Cláusula Contractual	Responsable: Contratante Periodicidad: Al inicio del contrato Explicación: Definición de clausula contrata cual relacionada con el pago de las obligaciones contractuales previa presentación de la factura y recibo a satisfacción por parte del supervisor del contrato	Preventivo	Moderado	1	0	Raro	Menor	Bajo
No acreditación del pago de aportes al SGSS y/o parafiscales	**Contractual**	**Imposibilidad de pago por parte de la entidad contratante**	Probable	Menor	Costo	Medio	Contratista y Contratante	Contratista: 50% Contratante: 50%	Cláusula Contractual	Responsable: Contratante Periodicidad: Al inicio del contrato Explicación: Definición de clausula contrata cual relacionada con la obligación de contratista del pago oportuno de los parafiscales	Preventivo	Fuerte	2	0	Raro	Menor	Bajo

Elaboró	Luz Adriana Loaiza Moreno	Profesional de Seguridad de la Información
Revisó	Adrián Gómez Vargas	Director de Seguridad de la Información
Revisó	Juan David Parada Tovar	Profesional de Gestión Contractual