1. OBJETO

Prestar los servicios para el diseño, planeación y ejecución de una simulación de respuesta ante incidentes de ciberseguridad, una simulación de cibercrisis y jornadas de capacitación.

2. LOCALIZACION

La localización de la ejecución del servicio o el lugar de entrega del servicio para todos los efectos legales es la ciudad de Bogotá D.C.

3. PLAZO

El plazo de ejecución del CONTRATO es de SEIS (6) meses, contados a partir de la suscripción del Acta de Inicio del CONTRATO.

Dicho plazo contempla la ejecución de las actividades. El plazo establecido para cada actividad puede concurrir con la ejecución de otras. En todo caso, las actividades requieren autorización del supervisor para su inicio.

4. FORMULA DE REAJUSTE

En el Apéndice Datos Esenciales del Contrato se indica que no aplican reajustes al contrato.

5. GASTOS REMBOLSABLES

No se reconocerán gastos reembolsables para el presente contrato.

6. ALCANCE

El presente documento describe el **alcance técnico particular** del objeto a contratar. Para la ejecución del contrato, el **CONTRATISTA** deberá cumplir igualmente con los lineamientos, condiciones y obligaciones establecidas en los demás documentos, apéndices y anexos que hacen parte integral del contrato.

El alcance de los servicios a contratar comprende, como mínimo, el desarrollo de las siguientes actividades y componentes:

I. Simulación de Respuesta ante incidentes de ciberseguridad

Diseñar, planear y ejecutar una (1) **Simulación de Respuesta ante incidentes de ciberseguridad**, orientada a ejercitar y evaluar las capacidades del Equipo de Respuesta ante Incidentes de Ciberseguridad de la Transportadora de Gas Internacional S.A. E.S.P., considerando su estructura organizacional, procesos y activos críticos.

Esta simulación deberá contemplar, como mínimo:

- Diseño de un **escenario realista de incidente de ciberseguridad**, alineado con el perfil de amenazas, riesgos y operación de la organización.

- Ejecución de un **ejercicio de simulación tipo escritorio (tabletop exercise)**, incorporando **estímulos tácticos y operativos** que permitan evaluar la toma de decisiones, la coordinación entre equipos y la aplicación de procedimientos vigentes.
- De ser técnicamente viable y previamente autorizado por TGI, la **ejecución controlada de ataques simulados y/o ejercicios de defensa en vivo**, asegurando en todo momento la no afectación de los ambientes productivos.
- Evaluación de las capacidades de **detección, análisis, contención, erradicación, recuperación, escalamiento y comunicación** durante la atención del incidente de ciberseguridad.
- Identificación de brechas, oportunidades de mejora y recomendaciones prácticas para el fortalecimiento del proceso de respuesta a incidentes de ciberseguridad.

II. Simulación de Cibercrisis

Diseñar, planear y ejecutar un (1) ejercicio de simulación de cibercrisis orientado a evaluar la capacidad del Comité Directivo y del Comité de Crisis para gestionar impactos estratégicos, reputacionales, regulatorios y operacionales derivados de un incidente de ciberseguridad.

Esta simulación deberá como mínimo:

- Plantear un **escenario de cibercrisis** con potencial impacto **estratégico, operativo, regulatorio, financiero y reputacional**.
- Evaluar los mecanismos de **gobernanza, toma de decisiones estratégicas, liderazgo, comunicación interna y externa, escalamiento y coordinación interáreas**.
- Poner a prueba los **roles y responsabilidades establecidos** en los planes de gestión de crisis, continuidad del negocio y respuesta a incidentes de ciberseguridad.
- Analizar la articulación entre las decisiones ejecutivas y los equipos técnicos durante la evolución de la crisis.
- Generar conclusiones y recomendaciones orientadas al fortalecimiento del modelo de **Gestión de Crisis y Ciber resiliencia organizacional**.

III. Capacitaciones para personal de TGI en Continuidad de Negocio / Gestión de Crisis

Desarrollar y ejecutar 6 **jornadas de capacitación y transferencia de conocimiento virtuales** dirigidas al personal de la Transportadora de Gas Internacional S.A. E.S.P., con el objetivo de fortalecer las competencias técnicas, operativas y estratégicas en **Continuidad del Negocio y Gestión de Crisis.** Además entre otras tipologías que pueden generar estos eventos, tener en cuenta el componente de Respuesta a Incidentes de Ciberseguridad.

Las capacitaciones deberán:

- Estar alineadas con los **manuales, planes y documentos institucionales vigentes** de TGI.
- Facilitar la **comprensión y apropiación de roles, responsabilidades, procesos y flujos de comunicación**.
- Incorporar aprendizajes derivados de las simulaciones ejecutadas.
- Asegurar la transferencia efectiva de conocimiento, contribuyendo al fortalecimiento de las capacidades organizacionales de preparación, respuesta y recuperación ante escenarios de Continuidad de negocio y/o Crisis. Además entre otras tipologías que pueden generar estos eventos, tener en cuenta el componente de Respuesta a Incidentes de Ciberseguridad y Cibercrisis.

7. OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA

El CONTRATISTA deberá ejecutar las actividades descritas a continuación, **sin perjuicio de aquellas adicionales** que se deriven del objeto contractual, del alcance técnico, de los anexos, apéndices, lineamientos y demás documentos que hacen parte integral del proceso de contratación.

7.1 Obligaciones Transversales (aplican para todo el contrato)

El **CONTRATISTA** deberá:

a) **Presentar un Plan de Trabajo** que incluya cronograma, metodología, roles, responsables, requerimientos logísticos/técnicos, matriz de participantes, y plan de comunicaciones con el Supervisor del contrato.
b) **Alinear** el diseño y ejecución de los ejercicios y capacitaciones con los **manuales, planes y documentos vigentes** de TGI (Respuesta a Incidentes, Gestión de Crisis, Continuidad, Comunicaciones, etc.). En el caso que se requieran ajustar documentos existentes el proveedor deberá sugerir las actualizaciones a los documentos.
c) **Definir reglas del ejercicio** (rules of engagement) y controles para garantizar que cualquier actividad tipo "en vivo" sea **controlada, autorizada previamente** y no afecte la operación ni ambientes productivos.
d) Garantizar el **manejo seguro y confidencial** de la información de TGI (incluida data cruda/técnica), evitando la exposición de datos sensibles y aplicando medidas de custodia y acceso.
e) Asegurar la **trazabilidad**: toda recomendación o plan de mejora deberá estar vinculada a una evidencia/observación del ejercicio (bitácoras, actas, artefactos, decisiones).
f) Ejecutar **reuniones de coordinación y validación** con el Supervisor para aprobar escenarios, participantes, agenda y logística antes de las sesiones presenciales.
g) Entregar todos los productos en los **formatos acordados** (editable y PDF si aplica), con **control de versión**, fecha, responsables y consistencia documental.

7.2. Simulación de Respuesta ante incidentes de ciberseguridad:

Ejecutar y describir las actividades: definición, desarrollo, validación, simulación y reporte, desglosadas en actividades tangibles con sus entregables.

- Ejecutar mínimo un (1) taller presencial (in situ) de 3 horas.
- Desarrollar y estructurar actividades remotas con los siguientes componentes: definición, diseño, validación y reporte.
- Desarrollar el ejercicio incluyendo los siguientes componentes:
  - Definición de objetivo y alcance.
  - Reglas del ejercicio.
  - Ejecución con estímulos técnicos progresivos.
  - Autoevaluación estructurada.
  - Cierre formal con conclusiones.

7.3. Simulación de Cibercrisis

Ejecutar y describir: la definición, desarrollo, validación, simulación y reporte, con actividades tangibles y sus entregables.

- Un (1) taller presencial (in situ) de 3 horas.
- Actividad previa de capacitación breve.

- Simulación de entrevista con vocero (sin medios reales).
- Evaluación estructurada de gobernanza y toma de decisiones.
- Reporte ejecutivo con plan de mejora.

7.4. Capacitaciones para personal de TGI en Continuidad de Negocio / Gestión de Crisis

Las capacitaciones deben estar alineadas con los siguientes parámetros:

- Especificar la metodología bajo la cual se desarrollarán los entregables y/o actividades.
- Deben integrar la documentación existente en cuanto a Planes y Manuales aplicables a la Continuidad de Negocio y Gestión de Crisis vigentes en TGI.
- Las sesiones deben estar orientadas a garantizar la transferencia de conocimiento para fortalecer competencias y habilidades en Continuidad de Negocio y Gestión de Crisis del personal de TGI.
- Las sesiones deben estar orientadas a garantizar la comprensión de roles y responsabilidades en Continuidad de Negocio y Gestión de Crisis del personal de TGI.
- Las sesiones deben ser personalizadas y con contenidos diferenciales dirigidos según la audiencia (equipos Estratégico, Táctico y Operativo de TGI)
- Las sesiones de capacitación deben ofrecer diversas opciones de agenda para garantizar la asistencia del personal de TGI. Para el equipo Estratégico (1 sesión), equipo Táctico (2 sesiones) y Operativo (3 sesiones).
- Sesiones interactivas que permitan espacios de preguntas en doble vía, retroalimentación y discusión.
- Evaluación de la comprensión y transferencia de conocimiento en cada sesión.

8. ENTREGABLES

I. Simulación de Respuesta ante incidentes de ciberseguridad:

- Resumen ejecutivo.
- Escenario planteado y estímulos.
- Línea de tiempo de decisiones.
- Evaluación de desempeño.
- Fortalezas.
- Oportunidades de mejora priorizadas.
- Recomendaciones técnicas y organizacionales.
- Plan de mejora sugerido.
- Data cruda y técnica de lo identificado sobre la simulación

II. Simulación de Cibercrisis

- Resumen ejecutivo estratégico.
- Evaluación del comité de crisis.
- Análisis de gobernanza.
- Evaluación de tiempos de reacción.
- Fortalezas.
- Oportunidades de mejora priorizadas.
- Plan de fortalecimiento.
- Recomendaciones de comunicación estratégica.
- Data cruda y técnica de lo identificado sobre la simulación

III. Capacitaciones para personal de TGI en Continuidad de Negocio / Gestión de Crisis

- Plan de capacitaciones (cronograma y metodología).
- Contenido o material de las sesiones de capacitación (Presentaciones y/o material tipo memorias de la sesión)
- Resultado de las evaluaciones ejecutadas en las sesiones de capacitación.

9. PERSONAL DEL CONTRATISTA

EL CONTRATISTA debe contar con el personal entrenado, calificado, necesario y suficiente para la apropiada ejecución del objeto requerido, incluyendo el personal necesario para la Gerencia, Administración, Supervisión y Operación en el caso que se requiera. Además, podrá proveer el personal adicional al mínimo requerido, que considere necesario sin que esto represente un mayor costo para LA EMPRESA.

EL CONTRATISTA debe como mínimo garantizar y proponer en su organigrama los recursos descritos a continuación.

I. Simulación de Respuesta ante incidentes de ciberseguridad:

- Director del Ejercicio / Líder Técnico Principal
- Especialista en Respuesta Técnica / Threat Simulation Lead
- Facilitador Metodológico / Observador de Madurez
- Gerente de Proyecto (Rol obligatorio)

II. Simulación de Cibercrisis

- Director Estratégico de Crisis
- Especialista en Gestión de Crisis y Comunicación
- Analista de Gobernanza y Cumplimiento
- Gerente de Proyecto (Rol obligatorio)

III. Capacitaciones para personal de TGI en Continuidad de Negocio / Gestión de Crisis

- Líder o Gerente de Proyecto
- Consultor Senior Gestión de Crisis
- Consultor Senior Continuidad de Negocio
- Consultor con experiencia relacionada en proyectos similares

9.1. PERFILES

A continuación, se presentan los perfiles mínimos exigibles para los profesionales que ocuparán los cargos indicados anteriormente, quienes serán los encargados de asegurar el cumplimiento del alcance contractual:

Simulación de Respuesta ante incidentes de ciberseguridad			
Rol	**Responsabilidades**	**Experiencia Mínima**	**Certificaciones obligatorias**
Director del Ejercicio / Líder Técnico Principal	Diseño estratégico del escenario y de los estímulos tácticos/operativos. Supervisión metodológica. Dirección del taller (Dirigir la ejecución del ejercicio y la toma de decisiones técnicas) Validación técnica de hallazgos. Presentación del informe ejecutivo. Conducir el cierre técnico y consolidar lecciones aprendidas y mejoras.	8 años en ciberseguridad. 5 años liderando equipos SOC o respuesta a incidentes. Experiencia comprobable en mínimo 3 simulaciones similares.	Certificaciones obligatorias (al menos dos): CISSP CISM GIAC (GCIA, GCIH o equivalente) ISO 27001 Lead Auditor o Lead Implementer
Especialista en Respuesta Técnica / Threat Simulation Lead	Diseño de estímulos tácticos. Simulación de vectores de ataque realistas. Enriquecimiento técnico basado en MITRE ATT&CK. Evaluación técnica del desempeño del equipo.	5 años en operaciones SOC o CSIRT. Experiencia en análisis forense o respuesta a incidentes reales. Experiencia en simulación o ejercicios Red Team / Purple Team.	Certificaciones obligatorias (al menos una): GCIH GCFA CEH (no junior) OSCP CRTO o equivalente
Facilitador Metodológico / Observador de Madurez	Control de tiempos. Registro estructurado de decisiones. Evaluación de madurez. Consolidación de oportunidades de mejora.	5 años en gestión de riesgos o continuidad. Experiencia en ISO 27035 o NIST IR.	Certificaciones obligatorias (al menos una): ISO 27035 ISO 22301 CISA CISM
Gerente de Proyecto (Rol obligatorio) El proveedor deberá designar formalmente un Gerente de Proyecto responsable del control integral del servicio. Este rol podrá ser asumido por el Director del Ejercicio siempre que cumpla los requisitos indicados.	Planeación y control del cronograma. Gestión de alcance. Coordinación con el equipo designado por la organización. Gestión de riesgos del proyecto. Control de calidad de entregables. Seguimiento hasta entrega final del informe.	5 años gestionando proyectos de ciberseguridad o continuidad. Participación en mínimo 2 ejercicios similares.	Certificaciones obligatorias (al menos una): PMP (certificación vigente) PRINCE2 Certificación en gestión de proyectos (Agile o equivalente)

Simulación de Cibercrisis			
Rol	**Responsabilidades**	**Experiencia Mínima**	**Certificaciones obligatorias**
Director Estratégico de Crisis	Diseño del escenario estratégico. Dirección del ejercicio. Evaluación del comité de crisis. Presentación de conclusiones a alta dirección.	10 años en gestión de riesgos o continuidad. Experiencia en mínimo 3 simulaciones de crisis con alta dirección.	Certificaciones obligatorias (al menos dos): CISSP CISM ISO 22301 Lead Implementer CBCP ISO 27001 Lead Auditor
Especialista en Gestión de Crisis y Comunicación	Diseño de estímulos reputacionales y regulatorios. Simulación de entrevista con vocero. Evaluación de comunicación estratégica.	5 años en gestión de crisis corporativa. Experiencia en escenarios reputacionales.	Certificaciones deseables (al menos una): ISO 22301 Certificación en Gestión de Crisis Certificación en Comunicación de Crisis
Analista de Gobernanza y Cumplimiento	Evaluación del impacto legal y regulatorio. Análisis de brechas en procedimientos. Revisión de gobernanza.	5 años en cumplimiento o gobierno de seguridad.	Certificaciones obligatorias (al menos una): CISA CRISC ISO 27001 LA Certificación en gestión de riesgos (ISO 31000 o equivalente)
Gerente de Proyecto (Rol obligatorio) Este rol podrá ser asumido por el Director Estratégico si cumple los requisitos establecidos.	Gestión integral del servicio. Coordinación logística con alta dirección. Gestión de riesgos del ejercicio. Control de calidad del informe. Seguimiento hasta cierre formal.	5 años en gestión de proyectos estratégicos. Experiencia en mínimo 2 ejercicios de crisis.	Certificaciones obligatorias (al menos una): PMP (certificación vigente) PRINCE2 Certificación equivalente en gestión de proyectos

Capacitaciones Continuidad de Negocio y Gestión de Crisis		
ROL	**Formación Específica Mínima**	**Experiencia especifica**
Líder o Gerente de Proyecto	Administrador, Ingeniero, o afines con posgrado en las temáticas de Continuidad de Negocio, Crisis, Riesgos y/o relacionados.	Mínimo 10 años de experiencia en la ejecución de proyectos relacionados con gestión de Continuidad de Negocio, Gestión de Crisis, documentación y construcción de planes y manuales de Continuidad y Crisis, capacitaciones / formaciones en Continuidad y Crisis, todo lo anterior con enfoque en sectores de Oil & Gas.

Capacitaciones Continuidad de Negocio y Gestión de Crisis		
ROL	**Formación Específica Mínima**	**Experiencia especifica**
Consultor Senior Gestión de Crisis	Administrador, Ingeniero, o afines con posgrado en las temáticas de Continuidad de Negocio, Crisis, Riesgos y/o relacionados.	Mínimo 10 años de experiencia en la ejecución de proyectos relacionados con gestión de Crisis, documentación y construcción de planes y manuales de Crisis, capacitaciones / formaciones en gestión de Crisis. Todo lo anterior con enfoque en sectores de Oil & Gas.
Consultor Senior Continuidad de Negocio	Administrador, Ingeniero, o afines con posgrado en las temáticas de Continuidad de Negocio, Crisis, Riesgos y/o relacionados.	Mínimo 10 años de experiencia en la ejecución de proyectos relacionados con gestión de Continuidad de Negocio, documentación y construcción de planes y manuales de Continuidad, capacitaciones / formaciones en Continuidad. Todo lo anterior con enfoque en sectores de Oil & Gas.
Consultor con experiencia relacionada en proyectos similares	Administrador, Ingeniero, o afines con posgrado en las temáticas de Continuidad de Negocio, Crisis, Riesgos y/o relacionados.	5 años de experiencia en la Gestión de Continuidad de negocio, Gestión de Crisis y capacitaciones / formaciones relacionadas con la temática en sectores de Oil & Gas.

El CONTRATISTA debe asegurar que los horarios y turnos de trabajo del personal designado para la ejecución del Contrato, se encuentren en cumplimiento de la legislación laboral colombiana vigente, así como de los estándares de LA EMPRESA, de manera que se controlen factores de seguridad y salud en el trabajo como fatiga y cansancio. Igualmente, el CONTRATISTA debe asegurar que ninguno de sus trabajadores ingiera o se encuentre bajo los efectos de bebidas alcohólicas o drogas alucinógenas durante los días de trabajo.

10. DOCUMENTOS PREVIOS AL ACTA DE INICIO DEL CONTRATO

Los siguientes documentos serán entregados dentro de los 15 días hábiles siguientes a la suscripción del contrato.

- **POLIZAS DEL CONTRATO Aplica SI (X) NO ( )**
- **PLAN DE SEGURIDAD, SALUD EN EL TRABAJO Aplica SI ( ) NO (X)**

11. DOCUMENTOS EN LA ETAPA DE ACTOS PREPARATORIOS

Los siguientes documentos serán entregados por el contratista dentro de los 5 días hábiles siguientes a la firma del acta de inicio.

La interventoría y/o supervisión aprobará los documentos, una vez se atiendan las subsanaciones solicitadas, si estas aplican, dentro de los 5 días hábiles siguientes a la entrega de estos por parte del contratista, aprobación que será requisito para el inicio de la ejecución física del contrato.

Se entiende que estos plazos hacen parte del plazo total del contrato.

- **PLAN DE TRABAJO Aplica SI (X) NO ( )**

El Plan de Trabajo debe estar ajustado al cronograma oficial de **LA EMPRESA**, debe incluir un diagrama de barras (Diagrama de Gantt) y uno de ruta crítica (CPM), en el que se indique el orden, dependencia y secuencia de las actividades. El diagrama debe comprender todas las actividades relacionadas con el objeto del contrato.

- **PLAN DE CALIDAD Aplica SI ( ) NO (X)**

- **HOJAS DE VIDA Y SOPORTES DEL PERSONAL MÍNIMO Aplica SI (X) NO ( )**

EI CONTRATISTA deberá presentar las hojas de vida del personal mínimo establecido en el numeral **PERSONAL DEL CONTRATISTA** del presente documento, con los respectivos soportes, que cumplan con la experiencia, formación y perfiles, allí solicitados. Los títulos académicos provenientes del exterior deberán encontrarse debidamente homologados por la autoridad competente. Para acreditar la experiencia se deberán presentar las respectivas certificaciones expedidas por el contratante.

LA EMPRESA no tendrá vínculo laboral con el equipo de trabajo mínimo aprobado, puesto que éste depende totalmente del **CONTRATISTA.**

En caso de que alguno de los cargos requeridos no cumpla los requisitos indicados o que no se cumpla con el número mínimo de profesionales solicitado, **EL CONTRATISTA** seleccionado deberá presentar las hojas de vida faltantes para aprobación de **LA EMPRESA**.

Solamente se aceptarán sustituciones del personal aceptado en caso de fuerza mayor, enfermedad comprobable que le impida ejercer sus responsabilidades o por causas que a juicio de **LA EMPRESA** lo justifiquen; en este caso las sustituciones se harán con personal que también a juicio de **LA EMPRESA** tenga una experiencia igual o superior a la del personal originalmente aceptado. El no cumplimiento de este requerimiento se considerará incumplimiento del contrato que se llegue a celebrar. Cuando **EL CONTRATISTA** deba cambiar alguno de los profesionales propuestos, deberá avisar a **LA EMPRESA** con al menos ocho (8) días hábiles de anticipación y presentar la nueva hoja de vida y los soportes de la misma para su aprobación.

LA EMPRESA podrá solicitar al **CONTRATISTA** el cambio del personal del equipo de trabajo que a juicio de ésta requiera ser reemplazado para la ejecución de los trabajos, obligándose **EL CONTRATISTA** a realizar los cambios solicitados, en un tiempo no mayor a quince (15) días, en todo caso, este personal deberá contar con las mismas o superiores calidades del personal que está reemplazando

- **DOCUMENTOS DE SUBCONTRATISTAS Aplica SI ( ) NO (X)**

- **NIT DE ESTRUCTURAS PLURALES Aplica SI (X) NO ( )**