No.183-2021

CONTRATO DE SERVICIO DE CONSULTORÍA PARA LA GESTIÓN DE CIBERSEGURIDAD, ANÁLISIS DE VULNERABILIDADES Y HACKING ÉTICO DEL BANCO CENTRAL DE HONDURAS

Nosotros, **ARACELY O'HARA GUILLÉN**, mayor de edad, casada, licenciada en Economía, hondureña y de este domicilio, con Documento Nacional de Identificación (DNI) No.0601-1965-00042, actuando en mi condición de **GERENTE Y REPRESENTANTE LEGAL DEL BANCO CENTRAL DE HONDURAS**, nombrada en dicho cargo mediante la Resolución No.412-10/2018, emitida por el Directorio de dicha Institución el 18 de octubre de 2018, debidamente facultada para la suscripción de este documento según consta en la Resolución No.580-11/2021, emitida por el mismo Órgano Colegiado el 25 de noviembre de 2021; Institución que posee el Registro Tributario Nacional No.08019995284049 y que en lo sucesivo se denominará **"EL BANCO"**, por una parte y por la otra, la señora **OLGA MARINA VALLADARES MONCADA**, mayor de edad, casada, ingeniera en Sistemas, hondureña y de este domicilio, con Documento Nacional de Identificación (DNI) No.0801-1982-18212, actuando en mi condición de Representante Legal de la sociedad **SISTEMAS APLICATIVOS SISAP S.A.**, con Registro Tributario Nacional No.08019009251597, constituida mediante Instrumento Público No.67, otorgado en la ciudad de Tegucigalpa, MDC, el 3 de agosto de 2009, ante los oficios del Notario Luis Alfredo Galeano Ordóñez, inscrita bajo la Matrícula No.2510842 del No.3617 del Registro Mercantil, Centro Asociado del Instituto de la Propiedad de la ciudad de Tegucigalpa, Departamento de Francisco Morazán; debidamente facultada para firmar este tipo de contratos según consta en Poder General de Administración otorgado mediante Instrumento Público No.62, en la ciudad de Tegucigalpa, MDC, el 7 de abril de 2016, ante los oficios del Notario Carlos Humberto Medrano Irías, debidamente inscrito bajo el No.33682, Matrícula No.2510842 del Registro Mercantil Centro Asociado del Instituto de la Propiedad de la ciudad de Tegucigalpa, Departamento de Francisco Morazán y quien en lo sucesivo se denominará **"EL CONSULTOR"**; hemos convenido en celebrar, como en efecto lo hacemos, el presente "CONTRATO DE SERVICIO DE CONSULTORÍA PARA LA GESTIÓN DE CIBERSEGURIDAD, ANÁLISIS DE VULNERABILIDADES Y HACKING ÉTICO DEL BANCO CENTRAL DE HONDURAS", el cual se regirá por los términos y condiciones que ambas partes estipulamos en las siguientes cláusulas:

CLÁUSULA PRIMERA
CLÁUSULA DE INTEGRIDAD

Las partes, en cumplimiento a lo establecido en el Artículo 7 de la Ley de Transparencia y Acceso a la Información Pública (LTAIP), de conformidad con el Acuerdo Institucional No.SE-037-2013, emitido por el Instituto de Acceso a la Información Pública el veinticinco (25) de junio de dos mil trece (2013) y publicado en el Diario Oficial "La Gaceta" el veintitrés (23) de agosto de dos mil trece (2013), y con la convicción de que evitando las prácticas de corrupción podremos apoyar la consolidación de una cultura de transparencia, equidad y rendición de cuentas en los procesos de contratación y adquisiciones del Estado, para así fortalecer las bases del Estado de Derecho, nos comprometemos libre y voluntariamente a:

1. Mantener el más alto nivel de conducta ética, moral y de respeto a las leyes de la República, así como los valores de: integridad, lealtad contractual, equidad, tolerancia, imparcialidad y discreción con la información confidencial que manejamos, absteniéndonos de dar declaraciones públicas sobre la misma.

2. Asumir una estricta observancia y aplicación de los principios fundamentales bajos los cuales se rigen los procesos de contratación y adquisiciones públicas establecidos en la Ley de Contratación del Estado, tales como: transparencia, igualdad y libre competencia.

3. Que durante la ejecución del Contrato ninguna persona que actúe debidamente autorizada en nuestro nombre y representación y que ningún empleado o trabajador, socio o asociado, autorizado o no, realizará:

   a) Prácticas Corruptivas: entendiéndose éstas como, aquellas en la que se ofrece dar, recibir, o solicitar directa o indirectamente, cualquier cosa de valor para influenciar las acciones de la otra parte.

   b) Prácticas Colusorias: entendiéndose éstas como aquellas en las que denoten, sugieran o demuestren que existe un acuerdo malicioso entre dos o más partes o entre una de las partes y uno o varios terceros, realizado con la intención de alcanzar un propósito inadecuado, incluyendo influenciar en forma inapropiada las acciones de la otra parte.

4. Revisar y verificar toda la información que deba ser presentada a través de terceros a la otra parte para efectos del Contrato y dejamos manifestado que, durante el proceso de contratación o adquisición a causa de este Contrato, la información intercambiada fue debidamente revisada y verificada, por lo que ambas partes asumen y asumirán la responsabilidad por el suministro de información inconsistente, imprecisa o que no corresponda a la realidad, para efectos de este Contrato.

5. Mantener la debida confidencialidad sobre toda la información a que se tenga acceso por razón del Contrato y no proporcionarla ni divulgarla a terceros y a su vez, abstenernos de utilizarla para fines distintos.

6. Aceptar las consecuencias a que hubiere lugar, en caso de declararse el incumplimiento de alguno de los compromisos de esta Cláusula por Tribunal competente y sin perjuicio de la responsabilidad civil o penal en la que se incurra.

7. Denunciar en forma oportuna ante las autoridades correspondientes cualquier hecho o acto irregular cometido por nuestros empleados o trabajadores, socios o asociados, del cual se tenga un indicio razonable y que pudiese ser constitutivo de responsabilidad civil y/o penal.

Lo anterior se extiende a los subcontratistas con los cuales el **"EL CONSULTOR"** contrate, así como a los socios, asociados, ejecutivos y trabajadores de aquellos.

El incumplimiento de cualquiera de los enunciados de esta cláusula dará lugar:

a) De parte de **"EL CONSULTOR"**:

   I. A la inhabilitación para contratar con el Estado, sin perjuicio de las responsabilidades que pudieren deducírsele.

   II. A la aplicación al trabajador, ejecutivo, representante, socio, asociado o apoderado que haya incumplido esta Cláusula, de las sanciones o medidas disciplinarias derivadas del régimen laboral y, en su caso entablar las acciones legales que correspondan.

b) De parte de **"EL BANCO"**:

   I. A la eliminación definitiva de su Registro de Proveedores y Contratistas que al efecto llevare para no ser sujeto de elegibilidad futura en procesos de contratación.

II. A la aplicación al empleado o funcionario infractor, de las sanciones que correspondan según el Código de Conducta Ética del Servidor Público, sin perjuicio de exigir la responsabilidad administrativa, civil y/o penal a las que hubiere lugar. En fe de lo anterior, las partes manifiestan la aceptación de los compromisos adoptados en el presente documento, bajo el entendido que esta Declaración forma parte integral del Contrato, firmando voluntariamente para constancia.

CLÁUSULA SEGUNDA
ANTECEDENTES DEL CONTRATO

"EL BANCO" manifiesta que mediante la Resolución No.580-11/2021 emitida el 25 de noviembre de 2021 por su Directorio, resolvió adjudicar a **"EL CONSULTOR"** el Concurso Privado No.02/2021 para la contratación de los servicios de consultoría para la gestión de ciberseguridad, análisis de vulnerabilidades y hacking ético del BCH.

CLÁUSULA TERCERA
MONTO DEL CONTRATO Y FORMA DE PAGO

1. Por la prestación del servicio objeto del presente Contrato, **"EL BANCO"** pagará a **"EL CONSULTOR"** la cantidad de **CUATRO MILLONES TRESCIENTOS SETENTA MIL LEMPIRAS (L4,370,000.00)**, que incluye **TRES MILLONES CIENTO VEINTIOCHO MIL LEMPIRAS (L3,128,000.00)** por honorarios profesionales, **SEISCIENTOS SETENTA Y DOS MIL LEMPIRAS (L672,000.00)** por gastos administrativos y **QUINIENTOS SETENTA MIL LEMPIRAS (L570,000.00)** por concepto de impuestos sobre ventas, debiendo efectuarse la retención del doce punto cinco por ciento (12.5%) de impuesto sobre la renta sobre los honorarios profesionales, salvo que la empresa acredite mediante constancia del Servicio de Administración de Rentas (SAR) que está sujeta al Régimen de Pagos a Cuenta.

2. El costo del servicio será cancelado en moneda nacional mediante pagos parciales por fase, contra la presentación de los entregables correspondientes a cada fase de la consultoría, dentro de los cuarenta y cinco (45) días calendario siguientes a la recepción de la factura acompañada de la solvencia fiscal vigente y demás documentación necesaria para efectuar el pago, con las correspondiente actas de aceptación emitidas por **"EL BANCO"** según la fase que corresponda, siempre y cuando la recepción de los servicios sea a entera satisfactoria para **"EL BANCO"**, sustentado en dichas actas suscritas por el Coordinador General del Proyecto adscrito al Departamento de Gestión de Riesgos, observando lo dispuesto en el numeral 3 de esta Cláusula y con el visto bueno del Jefe de Departamento de Gestión de Riesgos.

3. Condiciones para los pagos:

   3.1 Para el pago de cada porcentaje (%) programado a cancelar por los entregables de todas las fases de esta consultoría, **"EL CONSULTOR"** una vez que cuente con el Acta de Aceptación correspondiente, suscrita por el Gerente de Proyecto y Coordinador General del Proyecto, ambos de **"EL BANCO"**; conforme al numeral 7, Cláusula Quinta de este Contrato, podrá presentar la factura correspondiente ante el Departamento de Adquisiciones y Bienes Nacionales; presentando la documentación siguiente:

   3.1.1 Factura.
   3.1.2 Acta de Aceptación suscrita por el Gerente de Proyecto y Coordinador General del Proyecto, ambos de **"EL BANCO"**.
   3.1.3 Acta de Cierre de Proyecto (solo aplica para el último pago).

3.2 Para atender las gestiones de los pagos de **"EL CONSULTOR"**, **"EL BANCO"** realizará el procedimiento siguiente:

3.2.1 En el término de cuarenta y cinco (45) días calendario posteriores a la presentación de la factura por fase por parte de **"EL CONSULTOR"**, el Departamento de Adquisiciones y Bienes Nacionales debe gestionar la validación de la misma ante el Jefe del Departamento de Gestión de Riesgos para que conforme a normativa y procedimiento vigente se proceda con el pago correspondiente.

3.2.2 Todas las facturas previo a su cancelación deben contar con la validación del Jefe de Departamento de Gestión de Riesgos.

4. Los pagos se realizarán de acuerdo al grado de avance de la manera siguiente:

Fase	Descripción	% de pago	Entregables
0	Kickoff del proyecto y Plan de trabajo	10	Documentos: • Plan de trabajo. • Plan de pruebas.
I	SWIFT (Programa de Seguridad al Cliente)	15	• Informe técnico y un informe ejecutivo que contengan los resultados obtenidos de la revisión de vulnerabilidades conocidas en los componentes que conforman el entorno de mensajería SWIFT y plan de acción de remediación para las potenciales vulnerabilidades en la implementación del Programa de Seguridad al Cliente de SWIFT por **"EL BANCO"**, utilizando la estructura indicada en el **numeral 2.18 de la Cláusula Sexta.** • Informe técnico y un informe ejecutivo según lo definido en el marco de evaluación independiente (Independent Assessment Framework - IAF) en lo que respecta a la **evaluación externa independiente,** previo al cumplimiento de los controles SWIFT 2021 o 2022, utilizando la estructura indicada en el **numeral 2.18 de la Cláusula Sexta.**
II	Servicios en DMZ (internet y extranet) Remediación y seguimiento fase anterior.	25	• Informe técnico y un informe ejecutivo de análisis de vulnerabilidades y hacking ético y plan de acción de remediación para las potenciales vulnerabilidades en los Servicios en DMZ (internet y extranet), utilizando la estructura indicada en el **numeral 2.18 de la Cláusula Sexta.** • Informe con un análisis de los riesgos principales, recomendaciones agrupadas por tipo de dispositivo, sistema operativo, bases de datos o servidores de dominio, acciones de mitigación priorizadas y clasificadas por esfuerzo, enfatizando detalles técnicos y recomendaciones; así como evidencia de las principales vulnerabilidades encontradas, utilizando la

Fase	Descripción	% de pago	Entregables
			estructura indicada en el **numeral 2.18 de la Cláusula Sexta.**
III	Sistemas que soportan procesos críticos	25	• Informe técnico y un informe ejecutivo de análisis de vulnerabilidades y hacking ético y plan de acción de remediación para las potenciales vulnerabilidades en los sistemas que soportan procesos críticos, utilizando la estructura indicada en el **numeral 2.18 de la Cláusula Sexta.** • Informe con un análisis de los riesgos principales, recomendaciones agrupadas por tipo de dispositivo, sistema operativo, bases de datos o servidores de dominio, acciones de mitigación priorizadas y clasificadas por esfuerzo, enfatizando detalles técnicos y recomendaciones; así como evidencia de las principales vulnerabilidades encontradas, utilizando la estructura indicada en el **numeral 2.18 de la Cláusula Sexta.**
IV	Red interna, concientización en ciberseguridad, SWIFT y cierre del proyecto	25	**Respecto a la red interna:** 1. Informe técnico y un informe ejecutivo de análisis de vulnerabilidades y hacking ético y plan de acción de remediación para las potenciales vulnerabilidades de la red interna, utilizando la estructura indicada en el **numeral 2.18 de la Cláusula Sexta.** **Respecto a la concientización en ciberseguridad:** 2. Certificados de participación en charlas de sensibilización en ciberseguridad. 3. Material de presentaciones en formato PDF. 4. Informe que contengan los resultados obtenidos de la evaluación de la conciencia en ciberseguridad y un detalle de las actividades de charlas, capacitación y demás, utilizando la estructura indicada en el **numeral 2.18 de la Cláusula Sexta.** **Respecto a SWIFT:** 5. Informe técnico y un informe ejecutivo según lo definido en el marco de evaluación independiente (Independent Assessment Framework - IAF) en lo que respecta a la **evaluación externa independiente,** previo al cumplimiento de los controles SWIFT 2022 o 2023 (siguiente año al evaluado en la fase 1), utilizando la estructura indicada en el **numeral 2.18 de la Cláusula Sexta.**

Fase	Descripción	% de pago	Entregables
			Respecto al cierre del proyecto: 6. Catálogo de amenazas de ciberseguridad a las que está expuesto **"EL BANCO"**. 7. Informe ejecutivo final dirigido a la Gerencia de **"EL BANCO"**, que contenga descripción del trabajo realizado, las principales actividades realizadas, los resultados y productos finales obtenidos, lecciones aprendidas, las desviaciones con relación a los objetivos de la consultoría, conclusiones y recomendaciones. 8. Presentación ejecutiva editable que se realizará al Comité de Riesgos o al Directorio de **"EL BANCO"** sobre el resultado de la consultoría y un documento resumen de dicha presentación para entregar a la audiencia. 9. Informe técnico final que contenga la descripción de todas las pruebas realizadas, metodologías utilizadas, vulnerabilidades encontradas, descripción de las vulnerabilidades encontradas, nivel de criticidad y las acciones para su remediación.

Las facturas que presente **"EL CONSULTOR"** para su cancelación, conforme a la tabla precedente, contendrán como mínimo la descripción del producto del servicio (entregable) facturado, el valor total y los impuestos que correspondan de acuerdo a Ley.

5. Para efectos tributarios y cuando proceda, **"EL BANCO"** aplicará los impuestos que conforme a Ley correspondan; asimismo, en el caso del impuesto sobre la renta **"EL BANCO"** efectuará dicha retención sobre los honorarios profesionales, salvo que **"EL CONSULTOR"** acredite mediante constancia emitida por el Servicio de Administración de Rentas (SAR), debidamente autenticada, que se encuentra sujeto al Régimen de Pagos a Cuenta del Impuesto Sobre la Renta.

6. **"EL BANCO"** no efectuará ningún pago mientras no se suscriba el contrato correspondiente y no esté aprobado por el Directorio

CLÁUSULA CUARTA
OBJETIVOS Y ALCANCE DE LA CONSULTORÍA

1. Objetivos

1.1 Objetivo General

Contratar una empresa consultora especializada en ciberseguridad, análisis de vulnerabilidades y hacking ético con el fin de obtener un diagnóstico de vulnerabilidades en redes internas y externas, sistemas que soportan procesos críticos de **"EL BANCO"**.

1.2 Objetivos Específicos

1.2.1. Evaluar la gobernanza en ciberseguridad de **"EL BANCO"** con base en estándares internacionales y la normativa emitida por la Comisión Nacional de Bancos y Seguros (CNBS) vigente.

1.2.2. Analizar los riesgos asociados a los activos de información para proteger los sistemas informáticos utilizados para el procesamiento de datos, frente a amenazas internas o externas, deliberadas o accidentales.

1.2.3. Evaluar la efectividad de los controles existentes en los Servicios en DMZ (internet y extranet), Implementación del Programa de Seguridad del Cliente de SWIFT, Red interna y Sistemas que soportan procesos críticos de **"EL BANCO"**.

1.2.4. Definir planes de acción para mitigar la materialización de amenazas contra interrupción de los servicios y sistemas informáticos.

1.2.5. Evaluar el grado actual de conciencia en materia de ciberseguridad en los empleados de la institución.

2. Alcance de la consultoría

Considerando que la ciberseguridad se encarga del tratamiento de amenazas internas y externas a los activos de información digital, centrándose en los sistemas que soportan los procesos críticos del negocio, procesamiento de señales, análisis de riesgo y la ingeniería de seguridad de los sistemas de información, la consultoría debe ejecutarse de forma trimestral, de conformidad a las fases siguientes:

Fases	Ámbito de revisión y remediación de vulnerabilidades	Trimestres
0	Kickoff del proyecto y plan de trabajo	1
I	SWIFT (Programa de Seguridad al Cliente)	
II	Servicios en DMZ (internet y extranet)	2
III	Sistemas que soportan procesos críticos	3
IV	Red interna, concientización en ciberseguridad, SWIFT y cierre del proyecto	4

Cumpliendo con los requerimientos y condiciones especificados en la Cláusula Sexta de este Contrato, así como la inclusión de buenas prácticas sobre gobernanza de la ciberseguridad y su gestión con base en los estándares internacionales, utilizando como referencia mínima según corresponda por fase lo desarrollado por el NIST respecto al marco de ciberseguridad (CSF) y sus cinco funciones: identificar, proteger, detectar, responder y recuperar, pudiendo ser el Manual metodológico abierto de pruebas de seguridad (OSSTMM), Marco de evaluación de seguridad de sistemas de información (ISSAF) y la Guía de Pruebas OWASP u otras que **"EL CONSULTOR"** considere apropiadas y que incluya el uso de metodologías para realizar hacking ético; siempre apegado a mejores prácticas internacionales, el marco de evaluación externa independiente de SWIFT, según corresponda para cada una de las fases.

Además, para el desarrollo de la consultoría debe considerarse -en lo aplicable- las normas ISO/IEC 27001, 27002, ISO 27005, ISO 27032, ISO 27035-n, Magerit, Common Attack Pattern Enumeration and Classification (CAPEC™) en sus versiones vigentes.

CLÁUSULA QUINTA
VIGENCIA DEL SERVICIO

1. El plazo para la ejecución y terminación de los servicios de la consultoría para la gestión de ciberseguridad, análisis de vulnerabilidades y hacking ético de **"EL BANCO"**, es de **un (1) año** contado a partir del siguiente día hábil de la fecha de orden de inicio emitida por el Coordinador General del Proyecto de **"EL BANCO"** y notificada a **"EL CONSULTOR"** por el Departamento de Adquisiciones y Bienes Nacionales.

   Todo lo anterior sin perjuicio del derecho que se le confiere a **"EL BANCO"** a poner término a los servicios profesionales de consultoría según lo dispuesto en la Cláusula Décima Tercera de este Contrato.

2. En caso de necesitar prórroga para el desarrollo de la consultoría, **"EL CONSULTOR"**, debe presentar solicitud por escrito debidamente justificada ante **"EL BANCO"** antes del vencimiento del plazo contractual, para lo cual **"EL BANCO"** verificará la razonabilidad de lo solicitado, notificando por escrito a **"EL CONSULTOR"** la aprobación o no de la prórroga conforme a normativa y procedimiento vigente. En caso que la prórroga fuere autorizada, **"EL CONSULTOR"** elaborará un nuevo cronograma de actividades para aprobación de **"EL BANCO"**, el cual sustituirá al original o precedente y tendrá el mismo valor contractual del sustituido. En caso de denegarse la solicitud de prórroga, se aplicarán las sanciones indicadas en este Contrato.

3. Todos los entregables y demás documentos derivados o solicitados a esta consultoría deben ser presentados por **"EL CONSULTOR"** a **"EL BANCO"**, mediante el Departamento de Adquisiciones y Bienes Nacionales, quien la remitirá al Gerente de Proyecto de **"EL BANCO"**, que al efecto designe **"EL BANCO"**, para su revisión, emisión y suscripción conjunta con el Coordinador General del Proyecto del Acta de Aceptación correspondiente conforme lo descrito en el numeral 8 de esta Cláusula.

4. **"EL CONSULTOR"** presentará los entregables de cada fase concluida a más tardar cinco (5) días hábiles después de finalizada la misma con el fin de obtener el Acta de Aceptación correspondiente; dicha entrega será en el edificio de **"EL BANCO"**, ubicado en el Bulevar Fuerzas Armadas en la capital de la República.

5. **"EL CONSULTOR"** debe suministrar los entregables en medio físico y óptico a **"EL BANCO"**, de la forma siguiente: un original y una (1) copia en formato duro (impreso y encuadernado) y óptico (1 copia en formato PDF y 1 copia en formato editable de la Suite Microsoft Office).

6. El Gerente de Proyecto de **"EL BANCO"**, en un plazo máximo de cinco (5) días hábiles a partir del siguiente día de haber recibido cada entregable por fase de parte de **"EL CONSULTOR"**, debe aceptarlo o rechazarlo presentando las observaciones pertinentes y notificándolo por escrito al Departamento de Adquisiciones y Bienes Nacionales; si el entregable es rechazado, **"EL CONSULTOR"** podrá realizar los ajustes y enmiendas correspondientes para su presentación nuevamente ante el Gerente de Proyecto de **"EL BANCO"** cinco (5) días hábiles posterior a la fecha de la notificación del rechazo, observando lo indicado en los dos numerales anteriores.

7. La cantidad máxima de rechazos del informe que presente **"EL CONSULTOR"** será de dos (2) veces; agotada esta condición, **"EL BANCO"** se reserva el derecho de aplicar la sanción pecuniaria conforme a normativa vigente que rige este Contrato; sin perjuicio que **"EL CONSULTOR"** presente nuevamente el entregable correspondiente.

8. Por cada entregable por fase que presente **"EL CONSULTOR"** y que haya sido aceptado por el Gerente de Proyecto de **"EL BANCO"**, éste último emitirá la correspondiente Acta de Aceptación de dicho entregable, misma que suscribirá en conjunto con el Coordinador General del Proyecto de **"EL BANCO"** en un término máximo de tres (3) días hábiles posterior de la fecha de notificación de la aceptación.

9. Si por error u omisión imputables a **"EL CONSULTOR"** deben realizarse trabajos adicionales o rectificaciones, estos serán a su cargo y sin costo adicional para **"EL BANCO"**. Es responsabilidad de **"EL CONSULTOR"** cumplir con el trabajo de acuerdo con los Términos de Referencia que rigieron el Concurso Privado No.02/2021 y con las condiciones de este Contrato.

10. El plazo para la presentación de los entregables detallados en la Cláusula Sexta de este Contrato, se definirán en el cronograma de actividades del plan de trabajo que apruebe **"EL BANCO"**.

11. **"EL CONSULTOR"** se compromete durante la ejecución de la consultoría, a facilitar al Gerente de Proyecto de **"EL BANCO"** toda la información y documentación adicional que se le solicite para disponer de un pleno conocimiento técnico relacionado con la ejecución del Contrato.

CLÁUSULA SEXTA
REQUERIMIENTOS TÉCNICOS, ENTREGABLES Y CONDICIONES QUE DEBE CUMPLIR EL CONSULTOR

1. REQUERIMIENTOS TÉCNICOS

Fase	Requerimiento	Descripción del requerimiento
SECCIÓN I: DESCRIPCIÓN DETALLADA DE LOS SERVICIOS REQUERIDOS		
0	Kickoff del proyecto y Plan de trabajo.	**0.1 Plan de trabajo:** Desarrollar el documento correspondiente al plan de trabajo que incluya todas las actividades que deben ejecutarse en las cuatro fases del proyecto, estableciéndose como mínimo lo siguiente: a. Objetivos. b. Alcance. c. Estructura de desglose de trabajo (EDT). d. Tiempos de vigencia y cronograma de ejecución de cada fase. e. Calendario de entrega de cada uno de los entregables definidos en la "SECCIÓN II: ENTREGABLES", así como los documentos adicionales presentados en la oferta técnica. f. Calendario de las reuniones de seguimiento presenciales o remotas. g. Calendario de las charlas de concientización de ciberseguridad. h. Roles y responsables. i. Plan de comunicaciones. j. Actividades para evaluación de la gobernanza en ciberseguridad. k. Control de cambios del proyecto. l. Hitos importantes de la consultoría y una guía gráfica (Gantt) que ayude a visualizar el avance como parte del seguimiento de este para el cumplimiento de las condiciones y requerimientos técnicos. m. Plan de pruebas para análisis de vulnerabilidades y hacking ético con el cronograma de actividades de ejecución, debiendo ser homologado con **"EL BANCO"** (Gerente de Proyecto y Coordinador General del Proyecto) previo a su aceptación.

Fase	Requerimiento	Descripción del requerimiento
		La metodología utilizada debe ser acorde a estándares internacionales, utilizando como referencia mínima según corresponda por fase lo desarrollado por el NIST respecto al marco de ciberseguridad (CSF) y sus cinco funciones: identificar, proteger, detectar, responder y recuperar, pudiendo ser el Manual metodológico abierto de pruebas de seguridad (OSSTMM), Marco de evaluación de seguridad de sistemas de información (ISSAF) y la Guía de Pruebas OWASP u otras que **"EL CONSULTOR"** considere apropiadas y que incluya el uso de metodologías para realizar hacking ético; siempre apegado a mejores prácticas internacionales, el marco de evaluación externa independiente (Independent Assessment Framework - IAF) de SWIFT, según corresponda para cada una de las fases. Dentro del contenido del Plan de Trabajo, debe definirse el plan de pruebas siguiente: **0.1.1 Plan de pruebas para detección, análisis de vulnerabilidades y hacking ético**: Condiciones y requerimientos técnicos. Para la ejecución de las pruebas para el análisis de vulnerabilidades y hacking ético de las cuatro fases I, II, III y IV de la consultoría, debe estar aprobado el plan de trabajo y el plan de pruebas para dicho análisis; el cual debe incluir lo siguiente: a. Objetivo, alcance, supuestos, riesgos y estrategias de mitigación de las pruebas en cada fase (debe existir una validación previa en conjunto con personal técnico del Departamento de Gestión de Riesgos y con el apoyo del Departamento de Tecnología y Comunicaciones, para determinar por criticidad operativa si las pruebas pueden realizarse en horarios de oficina). b. Fecha de realización. c. Hora de inicio de las pruebas. d. Hora de finalización de las pruebas. e. Identificar los posibles riesgos a los que se exponen las redes, servicios y sistemas críticos de **"EL BANCO"**, proponiendo los controles de mitigación correspondientes. f. Describir las técnicas de detección y análisis de vulnerabilidades que utilizará. g. Describir en qué consistirán las pruebas de hacking ético internas y externas según corresponda por fase. h. Describir en qué consistirán las pruebas de ingeniería social (ataques controlados, infección de malware personalizado por medio de usuarios de **"EL BANCO"**, etc.) según corresponda por fase.

Fase	Requerimiento	Descripción del requerimiento
		i. **"EL BANCO"** podrá solicitar evidencia de la potencial materialización de vulnerabilidades identificadas, para descartar posibles falsos positivos. j. Según la fase que corresponda, **"EL CONSULTOR"** debe proporcionar la base de firmas de ataques actualizada durante el tiempo que dure la presente consultoría, de forma de poder detectar las nuevas vulnerabilidades que van surgiendo e informar sobre las mismas a **"EL BANCO"**. k. Si se detectan vulnerabilidades estas deben ser clasificadas altas, medias o bajas y de identificarse categorías altas o críticas y si fuese necesario apoyo técnico, se solicitará al equipo de **"EL CONSULTOR"** una reunión extraordinaria presencial o remota en la que se explique con mayor detalle sobre el hallazgo. l. Requerimientos técnicos específicos que debe proporcionar el Departamento de Tecnología y Comunicaciones de **"EL BANCO"**.
I	SWIFT (Programa de Seguridad al Cliente)	**"EL CONSULTOR"** conforme al **"0.1.1 Plan de pruebas para detección y análisis de vulnerabilidades y hacking ético"** correspondiente a esta fase, debe realizar las pruebas para evaluar la efectividad de los controles implementados sobre los activos de la información de los servicios en análisis, considerando lo siguiente: a. Las pruebas deben utilizar técnicas de hacking ético. b. Identificar vulnerabilidades conocidas en los componentes que conforman el entorno de mensajería SWIFT incluidos los sistemas que lo utilizan, según los requerimientos solicitados en el Programa de Seguridad al Cliente (CSP) vigente de SWIFT, debe incluir los controles mandatorios y los sugeridos; bajo una estrategia de "*Defense in Depth o* defensa en profundidad". c. Evaluar las vulnerabilidades identificadas cumplimiento de los controles obligatorios de SWIFT 2021 o 2022 según lo definido en el marco de evaluación independiente (Independent Assessment Framework - IAF) en lo que respecta a la **evaluación externa independiente,** que evidencien una posible materialización de amenazas, debiendo realizar un análisis con el propósito de proponer mejoras en la implementación de los controles actuales en función del Programa de Seguridad al Cliente (CSP) vigente de SWIFT y de las necesidades de **"EL BANCO"**. d. Presentar un informe técnico y ejecutivo que contengan los resultados obtenidos de la revisión de vulnerabilidades conocidas en los componentes que conforman el entorno de mensajería SWIFT y plan de acción de remediación para las potenciales vulnerabilidades en la implementación del Programa de Seguridad al Cliente de SWIFT por **"EL BANCO"**, utilizando la estructura indicada en el **numeral 2.18 de esta Cláusula.**

Fase	Requerimiento	Descripción del requerimiento
		e. Presentar un informe técnico y ejecutivo según lo definido en el marco de evaluación independiente (Independent Assessment Framework - IAF) en lo que respecta a la **evaluación externa independiente,** previo al cumplimiento de los controles SWIFT 2021 o 2022, utilizando la estructura indicada en el **numeral 2.18 de esta Cláusula**.
II	Servicios en DMZ (internet y extranet) Remediación y seguimiento fase anterior.	**"EL CONSULTOR"** conforme **"0.1.1 Plan de pruebas para detección y análisis de vulnerabilidades y hacking ético"** correspondiente a esta fase, debe realizar las pruebas para evaluar la efectividad de los controles implementados sobre los activos de la información de los servicios en análisis, considerando lo siguiente: a. Dar seguimiento a la fase anterior, revisando el avance del plan de remediación propuesto referente a la mitigación de potenciales vulnerabilidades encontradas de la fase I. b. Las pruebas deben programarse fuera de horario hábil u operativo sin afectar la integridad ni la disponibilidad de los servicios tecnológicos. c. Las pruebas deben utilizar técnicas de pentesting y hacking ético. d. Para las pruebas en internet, **"EL CONSULTOR"** debe realizar el análisis de vulnerabilidades bajo la modalidad "Black Box o caja negra". e. Las pruebas deben realizarse mediante exploración de direcciones IP públicas asignadas a **"EL BANCO"** por los ISP's contratados. f. Deben realizarse pruebas mediante exploración de puertos abiertos, cerrados y filtrados (TCP y UDP). g. En los puertos que se encuentren abiertos, deben realizar análisis del servicio habilitado, indicando el tipo de servicio, vulnerabilidades encontradas, valoración del riesgo, probabilidad de materialización de una amenaza según hallazgo en cada segmento. h. Para los servicios habilitados (HTTPS, HTTP, NTP, DNS, VPN (acceso remoto), SMTP (correo), Proxy, red inalámbrica para invitados e interna vía Wi-fi, entre otros) que evidencien la posible materialización de amenazas, deben realizar en análisis con el propósito de sugerir mejoras en los controles para fortalecer la seguridad y así la reducción del impacto, en función de las necesidades de **"EL BANCO"**. i. Trazabilidad de rutas desde internet -el equipo de **"EL CONSULTOR"**- hacia los servicios y sistemas identificados. j. El alcance de la evaluación de los servicios en DMZ respecto a la extranet serán desde la perspectiva de **"EL BANCO"**. k. Presentar un informe técnico y ejecutivo de análisis de vulnerabilidades y hacking ético y plan de acción de remediación para las potenciales vulnerabilidades en la Servicios en DMZ

Fase	Requerimiento	Descripción del requerimiento
		(internet y extranet), utilizando la estructura indicada en el **numeral 2.18 de esta Cláusula**. l. Presentar un informe con un análisis de los riesgos principales, recomendaciones agrupadas por tipo de dispositivo, sistema operativo, servidores de dominio, acciones de mitigación priorizadas y clasificadas por esfuerzo, enfatizando detalles técnicos y recomendaciones; así como evidencia de las principales vulnerabilidades encontradas, utilizando la estructura indicada en el **numeral 2.18 de esta Cláusula**.
III	Sistemas que soportan procesos críticos Remediación y seguimiento a fases anteriores.	**"EL CONSULTOR"** conforme al **"0.1.1 Plan de pruebas para detección y análisis de vulnerabilidades y hacking ético"** correspondiente a esta fase, debe realizar las pruebas para evaluar la efectividad de los controles implementados sobre los activos de la información de los servicios en análisis, considerando lo siguiente: a. Dar seguimiento a las fases anteriores, revisando el avance del plan de remediación propuesto referente a la mitigación de potenciales vulnerabilidades encontradas de la fase I y II. b. Las pruebas deben utilizar técnicas de pentesting y hacking ético. c. Realizar en coordinación con el Gerente de Proyecto de **"EL BANCO"**, adscrito al Departamento de Gestión de Riesgos, el análisis de los activos de información de al menos tres (3) sistemas que soportan procesos críticos de **"EL BANCO"** para determinar lo siguiente: 1. Valoración de los activos de información. 2. Identificación de vulnerabilidades. 3. Identificación de amenazas. 4. Análisis de vulnerabilidades. 5. Probabilidad de ocurrencia. 6. Potencial impacto cualitativo. 7. Análisis de Riesgos. 8. Controles aplicables. d. La evaluación sobre los activos de información de los sistemas que soportan los procesos críticos que se definan deben incluir como mínimo lo siguiente: 1. Accesos lógicos a los servicios que soportan los procesos críticos de **"EL BANCO"**. 2. Sistemas operativos de los equipos que soportan los procesos críticos de **"EL BANCO"**. 3. Sistemas de Gestión de Bases de datos de los sistemas que soportan los procesos críticos seleccionados para análisis. 4. Componente de software cliente que conecta con el servidor que prestan servicios a los procesos críticos de **"EL BANCO"**.

Fase	Requerimiento	Descripción del requerimiento
		5. Aplicaciones web en producción y su correspondiente análisis utilizando la metodología Guía de Pruebas OWASP. 6. Trazabilidad de rutas desde los equipos de usuarios o redes internas o externas hacia los sistemas que soportan procesos críticos de **"EL BANCO"**. e. Presentar un informe técnico y ejecutivo de análisis de vulnerabilidades y hacking ético y plan de acción de remediación para las potenciales vulnerabilidades en los sistemas que soportan procesos críticos, utilizando la estructura indicada en el **numeral 2.18 de esta Cláusula**. f. Presentar un informe con un análisis de los riesgos principales, recomendaciones agrupadas por tipo de dispositivo, sistema operativo, bases de datos o servidores de dominio, acciones de mitigación priorizadas y clasificadas por esfuerzo, enfatizando detalles técnicos y recomendaciones; así como evidencia de las principales vulnerabilidades encontradas, utilizando la estructura indicada en el **numeral 2.18 de esta Cláusula**.
IV	Red interna, concientización en ciberseguridad, SWIFT y cierre del proyecto Remediación, seguimiento a fases anteriores y cierre de proyecto.	**"EL CONSULTOR"** conforme al **"0.1.1 Plan de pruebas para detección y análisis de vulnerabilidades y hacking ético"** correspondiente a esta fase, debe realizar las pruebas para evaluar la efectividad de los controles implementados sobre los activos de la información de los servicios en análisis, considerando lo siguiente: 1. Dar seguimiento a las fases anteriores, revisando el avance del plan de remediación propuesto referente a la mitigación de potenciales vulnerabilidades encontradas de la fase I, II y III. **Respecto a la red interna:** 1. Las pruebas deben utilizar técnicas de pentesting y hacking ético. 1. Para las pruebas de análisis de vulnerabilidades en la red interna, **"EL CONSULTOR"** debe realizar el análisis bajo la modalidad "Grey Box o caja gris". 1. La evaluación sobre la red interna de **"EL BANCO"**, debe incluir como mínimo lo siguiente: **1.** Controles de acceso a los servicios y sistemas en la red LAN de **"EL BANCO"** por parte de los usuarios finales. **2.** Enumeración de los equipos de usuarios finales en la red LAN con prioridad los que utilizan sistemas que soportan los procesos críticos de **"EL BANCO"**, identificando dirección ip, dirección mac, sistema operativo, usuarios, puertos y servicios con su versión correspondiente. **3.** Trazabilidad de rutas desde los equipos de usuarios o redes internas a los servicios y sistemas identificados en la red LAN. **4.** Protección contra malware: antivirus, anti spam, antispyware, entre otros.

Fase	Requerimiento	Descripción del requerimiento
		5. Estrategia para protección de acceso a las redes (ejemplo: segmentación, ACL´s, Firewall, entre otros). **6.** Controles sobre navegación en internet. **7.** Controles sobre el uso de software. **8.** Control de inventarios del hardware que se conecta a la red. **9.** Controles de uso de servicios por dispositivos móviles. **10.** Capacidad de recuperación de datos. **11.** Control en el uso de correo electrónico corporativo. 1. Presentar un Informe técnico y ejecutivo de análisis de vulnerabilidades y hacking ético y plan de acción de remediación para las potenciales vulnerabilidades de la red interna, utilizando la estructura indicada en el **numeral 2.18 de esta Cláusula**. **Respecto a la concientización en ciberseguridad:** 1. Debe evaluar el grado actual de conciencia de ciberseguridad de los empleados de **"EL BANCO"**, a través de aplicación de pruebas de conocimiento e ingeniería social disponibles, con el objeto de determinar áreas de oportunidad que permitan reforzar la conciencia sobre esta temática, para enfrentar diferentes escenarios de riesgos que podrían presentarse y afectar a la disponibilidad, integridad y confidencialidad de los activos de **"EL BANCO"**. 1. Considerando el resultado obtenido en el numeral anterior debe proporcionar charlas de sensibilización y capacitación por personal certificado en seguridad de la información y ciberseguridad, según el esquema siguiente: **1.** Una (1) charla de sensibilización sobre seguridad de la información y ciberseguridad dirigida al nivel directivo de **"EL BANCO"** misma que debe tener una duración de una (1) hora aproximadamente (mostrando ejemplos reales y actuales en la banca). **2.** Una (1) charla de sensibilización sobre seguridad de la información y ciberseguridad dirigida a personal del nivel operativo (administradores y operadores de los sistemas que soportan procesos críticos de **"EL BANCO"**) misma que debe tener una duración de dos (2) horas aproximadamente (mostrando ejemplos reales y actuales en la banca). **3.** Un (1) taller de capacitación para ocho (8) personas sobre seguridad de la información y ciberseguridad, cantidad distribuida así: seis (6) para el Departamento de Gestión de Riesgos y dos (2) para el Departamento de Tecnología y Comunicaciones. **4.** Todas las charlas y talleres se impartirán por un profesional especializado en capacitación y certificado en ciberseguridad en las instalaciones de **"EL BANCO"** (presencial o remoto).

Fase	Requerimiento	Descripción del requerimiento
		5. Las fechas en que serán impartidas las charlas, deben definirse en el plan de trabajo indicado en la **fase 0,** mismas que pueden distribuirse a lo largo de la vigencia de este contrato y pueden ser definidas en base a necesidad por **"EL BANCO"**. 1. Presentar un informe que contenga los resultados obtenidos de la evaluación de la conciencia en ciberseguridad y un detalle de las actividades de charlas, capacitación y demás, utilizando la estructura indicada en el **numeral 2.18 de esta Cláusula.** **Respecto a SWIFT:** 1. Evaluar las vulnerabilidades identificadas cumplimiento de los controles obligatorios de SWIFT 2022 o 2023 (siguiente año al evaluado en la fase 1) según lo definido en el marco de evaluación independiente (Independent Assessment Framework - IAF) en lo que respecta a la **evaluación externa independiente**, que evidencien una posible materialización de amenazas, debiendo realizar un análisis con el propósito de proponer mejoras en la implementación de los controles actuales en función del Programa de Seguridad al Cliente (CSP) vigente de SWIFT y de las necesidades de **"EL BANCO"**. 1. Presentar un informe técnico y ejecutivo según lo definido en el marco de evaluación independiente (Independent Assessment Framework - IAF) en lo que respecta a la **evaluación externa independiente,** previo al cumplimiento de los controles SWIFT 2022 o 2023 (siguiente año al evaluado en la fase 1), utilizando la estructura indicada en el **numeral 2.18 de esta Cláusula.** **Respecto al cierre del proyecto:** 1. Debe entregar un informe ejecutivo dirigido a la Gerencia de **"EL BANCO"**, que contenga descripción del trabajo realizado, las principales actividades realizadas, los resultados y productos finales obtenidos, lecciones aprendidas, las desviaciones con relación a los objetivos de la consultoría, el análisis de los riesgos principales con una valoración del impacto al negocio de forma cualitativa, recomendaciones agrupadas por tipo de redes, servicios y sistemas que soportan los procesos críticos de **"EL BANCO"**, resumen del plan de remediación para potenciales vulnerabilidades detectadas y pendientes de atender, que incluya las acciones de mitigación priorizadas y clasificadas por esfuerzo, tipo de riesgo, conclusiones y recomendaciones. 1. Debe realizar una presentación ejecutiva al Comité de Riesgos o al Directorio de **"EL BANCO"** sobre el resultado de la Consultoría, tomando de base el informe ejecutivo descrito en el numeral anterior; misma que debe ser programada en el plan de trabajo aprobado por **"EL BANCO"**.

Fase	Requerimiento	Descripción del requerimiento
		1. Debe presentar un informe técnico final que contenga la descripción de todas las pruebas realizadas, metodologías utilizadas, vulnerabilidades encontradas, descripción de las vulnerabilidades encontradas, nivel de criticidad y las acciones para su remediación.
SECCIÓN II: ENTREGABLES		
Fase	**Requerimiento**	**Descripción del entregable**
0	Kickoff del proyecto y Plan de trabajo.	• Plan de trabajo que incluya: o Plan de pruebas.
I	SWIFT (Programa de Seguridad al Cliente).	• Informe técnico y un informe ejecutivo que contengan los resultados obtenidos de la revisión de vulnerabilidades conocidas en los componentes que conforman el entorno de mensajería SWIFT y plan de acción de remediación para las potenciales vulnerabilidades en la implementación del Programa de Seguridad al Cliente de SWIFT por **"EL BANCO"**, utilizando la estructura indicada en el **numeral 2.18 de esta Cláusula.** • Informe técnico y un informe ejecutivo según lo definido en el marco de evaluación independiente (Independent Assessment Framework - IAF) en lo que respecta a la **evaluación externa independiente,** previo al cumplimiento de los controles SWIFT 2021 o 2022, utilizando la estructura indicada en el **numeral 2.18 de esta Cláusula.**
II	Servicios en DMZ (internet y extranet)	• Informe técnico y un informe ejecutivo de análisis de vulnerabilidades y hacking ético y plan de acción de remediación para las potenciales vulnerabilidades en los Servicios en DMZ (internet y extranet), utilizando la estructura indicada en el **numeral 2.18 de esta Cláusula.** • Informe con un análisis de los riesgos principales, recomendaciones agrupadas por tipo de dispositivo, sistema operativo, bases de datos o servidores de dominio, acciones de mitigación priorizadas y clasificadas por esfuerzo, enfatizando detalles técnicos y recomendaciones; así como evidencia de las principales vulnerabilidades encontradas, utilizando la estructura indicada en el **numeral 2.18 de esta Cláusula.**
III	Sistemas que soportan procesos críticos.	• Informe técnico y un informe ejecutivo de análisis de vulnerabilidades y hacking ético y plan de acción de remediación para las potenciales vulnerabilidades en los sistemas que soportan procesos críticos, utilizando la estructura indicada en el **numeral 2.18 de esta Cláusula.** • Informe con un análisis de los riesgos principales, recomendaciones agrupadas por tipo de dispositivo, sistema operativo, bases de datos o servidores de dominio, acciones de mitigación priorizadas y clasificadas por esfuerzo, enfatizando detalles técnicos y recomendaciones; así como evidencia de las principales vulnerabilidades encontradas, utilizando la estructura indicada en el **numeral 2.18 de esta Cláusula.**

Fase	Requerimiento	Descripción del requerimiento
IV	Red interna, concientización en ciberseguridad, SWIFT y cierre del proyecto	**Respecto a la red interna:** 1. Informe técnico y un informe ejecutivo de análisis de vulnerabilidades y hacking ético y plan de acción de remediación para las potenciales vulnerabilidades de la red interna, utilizando la estructura indicada en el **numeral 2.18 de esta Cláusula.** **Respecto a la concientización en ciberseguridad:** 2. Certificados de participación en charlas de sensibilización en ciberseguridad. 3. Material de presentaciones en formato PDF. 4. Informe que contenga los resultados obtenidos de la evaluación de la conciencia en ciberseguridad y un detalle de las actividades de charlas, capacitación y demás, utilizando la estructura indicada en el **numeral 2.18 de esta Cláusula.** **Respecto a SWIFT:** 5. Informe técnico y un informe ejecutivo según lo definido en el marco de evaluación externa independiente de SWIFT previo al cumplimiento de los controles SWIFT 2022 o 2023 (siguiente año al evaluado en la fase 1), utilizando la estructura indicada en el **numeral 2.18 de esta Cláusula.** **Respecto al cierre del proyecto:** 6. Catálogo de amenazas de ciberseguridad a las que está expuesto **"EL BANCO"**. 7. Informe ejecutivo final dirigido a la Gerencia de **"EL BANCO"**, que contenga descripción del trabajo realizado, las principales actividades realizadas, los resultados y productos finales obtenidos, lecciones aprendidas, las desviaciones con relación a los objetivos de la consultoría, conclusiones y recomendaciones. 8. Presentación ejecutiva editable que se realizará al Comité de Riesgos o al Directorio de **"EL BANCO"** sobre el resultado de la Consultoría, y un documento resumen de dicha presentación para entregar a la audiencia. 9. Informe técnico final que contenga la descripción de todas las pruebas realizadas, metodologías utilizadas, vulnerabilidades encontradas, descripción de las vulnerabilidades encontradas, nivel de criticidad y las acciones para su remediación.

2. CONDICIONES QUE DEBE CUMPLIR "EL CONSULTOR":

2.1 Comunicada la orden de inicio por **"EL BANCO"** a través del Departamento de Adquisiciones y Bienes Nacionales posterior a la suscripción y aprobación del Contrato, **"EL CONSULTOR"** debe presentar al

Gerente de Proyecto de "**EL BANCO**", como máximo diez (10) días hábiles; la propuesta del Plan de Trabajo, dando inicio así a la fase 0.

2.2 En el plan de trabajo (presentado en la fase 0) deben quedar definidas las fechas de vigencia de cada fase y de cada uno de los entregables, respetando el tiempo máximo establecido para el desarrollo de la consultoría; el cual es de un (1) año a partir del siguiente día hábil de la fecha de orden de inicio notificada por "**EL BANCO**" a través del Departamento de Adquisiciones y Bienes Nacionales, misma que se realizará posterior a la suscripción y aprobación de este Contrato.

2.3 **"EL CONSULTOR"** en el inicio de la fase 0 debe definir en común acuerdo con el Coordinador General del Proyecto de "**EL BANCO**" y quedar plasmado en el plan de trabajo, los canales y protocolos de comunicación, control de documentos, comunicaciones oficiales y no oficiales, plan de entrega de los entregables, proceso para solicitar requerimientos para el desarrollo de las fases, entre otros; definiendo además los formatos a utilizar para la recepción y acuses de recibos.

2.4 **"EL CONSULTOR"** debe ejecutar las actividades a su cargo en coordinación con el equipo de trabajo designado por "**EL BANCO**".

2.5 Comunicada la orden de inicio del proyecto por parte de **"EL BANCO"** posterior a la suscripción y aprobación de este Contrato, **"EL CONSULTOR"** debe presentar ante el Coordinador General del Proyecto de "**EL BANCO**" la estructura funcional de su equipo de trabajo, consignando los nombres de los profesionales que cumplirán con los roles y responsabilidades requeridos según lo establecido en el numeral 3, Cláusula Sexta dentro de las **"Experiencia y Condiciones"**.

2.6 El Gerente de Proyecto de **"EL BANCO"**, gestionará la participación a demanda del personal técnico requerido al Departamento de Tecnología y Comunicaciones, según lo definido en el plan de trabajo.

2.7 **"EL CONSULTOR"** debe proporcionar a **"EL BANCO"** el nombre y cargo de los consultores responsables de ejecutar las fases de la consultoría, incluyendo el consultor especialista que proporcionará los talleres, capacitaciones y charlas solicitadas en la fase IV "**Respecto a la concientización en ciberseguridad**", designando a un Gerente de Proyecto, así como el nombre y cargo de la persona que se encargará de las comunicaciones con **"EL BANCO"** para la ejecución de este Contrato, a su vez será responsable de atender oportunamente todos los requerimientos que formule **"EL BANCO"** sobre la ejecución y cumplimiento del mismo.

2.8 Para el desarrollo de la consultoría, el equipo de especialistas de **"EL CONSULTOR"** debe realizar al menos cuatro (4) visitas en sitio en el edificio de **"EL BANCO"** ubicado en el Bulevar Fuerzas Armadas en la capital de la República para ejecutar los trabajos que le permitan desarrollar actividades propias de las fases conforme distribución indicada en el alcance de la consultoría en el numeral 2 de la Cláusula Sexta, con el fin de ejecutar pruebas, validar, homologar datos obtenidos durante dichas pruebas para el análisis de vulnerabilidades y hacking ético y remediaciones en dichas instalaciones; a continuación, el detalle:

Visita	Actividad	Días hábiles	Personal mínimo del consultor	Ámbito de revisión y remediación
1	Kickoff del proyecto, plan de trabajo (fase 0) y ejecución de fase I y remediación.	Veinticinco (25)	• Gerente de Proyecto. • Al menos (2) profesionales certificados responsables de ejecutar las fases de la consultoría.	SWIFT (Programa de Seguridad al Cliente)
2	Ejecución de fase II, remediación y seguimiento fase anterior.	Veinte (20)		Servicios en DMZ (internet y extranet)
3	Ejecución de fase III, remediación y seguimiento a fases anteriores.	Veinte (20)		Sistemas que soportan procesos críticos
4	Ejecución de fase IV, remediación, seguimiento a fases anteriores y cierre de proyecto.	Veinte (20)	• Gerente de Proyecto. • Al menos (2) profesionales certificados responsables de ejecutar las fases de la consultoría. • Profesional experto en capacitación en Ciberseguridad.	SWIFT, Red interna, concientización en ciberseguridad y cierre del proyecto.

Cuando el caso lo amerite, se podrán realizar reuniones extraordinarias, con el Gerente de Proyecto o Coordinador General del Proyecto de **"EL BANCO"** pudiendo estos, solicitar la participación de cualquiera de los miembros de los equipos de proyecto de **"EL CONSULTOR"** o de **"EL BANCO"**.

2.9 **"EL CONSULTOR"** podrá ejecutar parte de los trabajos de cada fase desde las instalaciones de su empresa, pudiendo intercambiar los archivos electrónicos de los avances de cada fase con el Coordinador General del Proyecto de **"EL BANCO"** a través de medios electrónicos observando controles de seguridad informática para garantizar la confidencialidad de dicha información; las entregas finales de cada fase deben realizarse conforme lo indicado en la Cláusula Quinta.

2.10 Mensualmente conforme al calendario de reuniones establecido en el plan de trabajo, durante la vigencia del proyecto que será de un (1) año, se realizarán ocho (8) reuniones de seguimiento en la que participarán de forma obligatoria el Gerente de Proyecto de **"EL BANCO"** y el Gerente de Proyecto de **"EL CONSULTOR"** respectivamente; estas reuniones son adicionales a las que se realicen en sitio durante la visita de **"EL CONSULTOR"** conforme lo planificado; las mismas serán presididas por el Coordinador General del Proyecto de **"EL BANCO"**, en la que se tratarán como mínimo los siguientes puntos de agenda:

2.10.1 Revisión de pendientes de las minutas de acuerdos anteriores.

2.10.2 Avance de los entregables de la fase.

2.10.3 Seguimiento a gestiones de pagos.

2.10.4 Homologación de minuta de acuerdos de la reunión e intercambio de la misma.

2.11 Durante la vigencia de la consultoría, **"EL CONSULTOR"** debe brindar asesoría técnica para que los responsables de acciones correctivas puedan implementar los controles que se consideren necesarios para remediar las potenciales vulnerabilidades encontradas; esta asesoría podrá consistir en consultas y respuestas vía correo electrónico, reuniones basadas en video conferencias o plataformas web, guías, material técnico, y en general cualquier otra forma que **"EL CONSULTOR"** estime conveniente y no afecte los intereses ni la seguridad de la información de **"EL BANCO"**.

2.12 Si durante el análisis de vulnerabilidades en cada fase se concluye que se requieren controles adicionales o cambios en configuraciones en redes, equipos, servicios y sistemas que administra **"EL BANCO"**, estas recomendaciones deben ser comunicadas en forma inmediata al Gerente de Proyecto de **"EL BANCO"**, para su evaluación, y además ser incorporadas en forma detallada en el informe que forma parte del entregable de cada fase.

2.13 **"EL CONSULTOR"** debe brindar la asesoría y acompañamiento técnico para ejecutar las pruebas para el análisis de vulnerabilidades y hacking ético.

2.14 **"EL CONSULTOR"** debe presentar las propuestas de mejoras para el tratamiento de las potenciales debilidades de seguridad informáticas identificadas en cada fase, que permitan a **"EL BANCO"**, con el acompañamiento de **"EL CONSULTOR"** definir un plan de acción para mitigar o corregir las mismas, además deben ser incorporadas en los informes respectivos por cada fase.

Para tal efecto, **"EL CONSULTOR"** debe indicar con claridad a qué área o dependencia de **"EL BANCO"** corresponde la evaluación, prueba e implementación de los controles para lograr la solución.

2.15 El equipamiento para realizar las pruebas especializadas, el análisis de vulnerabilidades y hacking ético por fase a las redes, servicios, equipos y sistemas de **"EL BANCO"**, debe ser provisto por **"EL CONSULTOR"**; sin perjuicio que se puedan utilizar herramientas complementarias de análisis provistas por **"EL BANCO"**.

2.16 **"EL CONSULTOR"** debe indicar en el plan de pruebas el tipo de herramientas a utilizar para el análisis de vulnerabilidades y hacking ético en cada fase y a su vez el nivel de intrusión que estas poseen.

2.17 **"EL CONSULTOR"** debe destruir todas las evidencias recolectadas y cualquier información o datos obtenidos durante las pruebas de análisis de vulnerabilidades de cada fase, y preparar un informe con las acciones realizadas junto con la descripción del software utilizado que demuestren al personal del Departamento de Gestión de Riesgos la destrucción de dicha información. En caso de que determinada evidencia requiera almacenamiento y custodia, **"EL CONSULTOR"** debe seguir los procedimientos y mejores prácticas de seguridad de la información, debiendo quedar documentado en la bitácora de la consultoría.

2.18 Los informes técnicos y ejecutivos de cada fase deben contener como mínimo los siguientes elementos que apliquen:

2.18.1 Resumen de las actividades realizadas.

2.18.2 Descripción del alcance y período de realización de las pruebas.

2.18.3 Gráficos de tendencias de vulnerabilidades detectadas según sistema.

2.18.4 Gráficos de tendencias de vulnerabilidades detectadas según criticidad.

2.18.5 Detalle de vulnerabilidades detectadas, incluido el análisis de las que más se repiten.

2.18.6 Propuesta de plan de remediación por fase de la consultoría que incluya actividades recomendadas para minimizar la explotación de vulnerabilidades en las redes, servicios o sistemas que soportan los procesos críticos de **"EL BANCO"** conforme sus capacidades.

2.18.7 Conclusiones y recomendaciones generales de ciberseguridad.

2.18.8 Anexos detallados correspondientes a:

2.18.8.1 Matriz sobre el análisis de riesgos, impacto y vulnerabilidades por cada una las solicitudes definidas en la evaluación de vulnerabilidades y la efectividad de los controles implementados a los activos de las redes, servicios o sistemas evaluados, la cual debe reflejar la valorización de los activos de información, el número de hallazgo, la amenaza de la que deriva el riesgo, vulnerabilidad, posibilidad de ocurrencia de la falla, potencial impacto cualitativo, control de mitigación sugerido adaptado a las características propias de **"EL BANCO"**, nivel de exposición al riesgo desde un enfoque cualitativo.

2.18.8.2 La matriz debe proporcionarse en formato técnico original generado por la herramienta de trabajo utilizada por **"EL CONSULTOR"** y además una matriz resumida en formato no técnico en Excel, para una fácil interpretación a nivel ejecutivo; con el fin de facilitar el seguimiento; su estructura debe ser conforme lo descrito en el numeral anterior.

2.18.8.3 Catálogo de amenazas de ciberseguridad a las que está expuesto **"EL BANCO"**.

2.19 Cualquier otra evaluación o servicio que **"EL CONSULTOR"** estime conveniente y que agregue valor y no represente costo adicional a **"EL BANCO"**, debe quedar descrito en el plan de trabajo señalado en la fase 0 de esta Cláusula.

3. EXPERIENCIA Y CONDICIONES

3.1 **"EL CONSULTOR"** debe contar con las capacidades técnicas y categorización similar a las empresas incluidas en el directorio de proveedores de servicios de seguridad cibernética (directory of cyber security service providers) de SWIFT, publicado en el sitio https://www.swift.com/myswift/customer-security-programme-csp_/community-engagement/cyber-firms-directory .

3.2 **"EL CONSULTOR"** debe presentar un equipo de especialistas para realizar los trabajos en sitio (ver detalle en el numeral 2, Cláusula Sexta dentro de las "Condiciones que debe cumplir **"EL CONSULTOR"**) que esté conformado por un (1) Gerente de Proyecto y al menos dos (2) especialistas.

3.3 El equipo de especialistas presentado por **"EL CONSULTOR"**, conforme lo descrito en el numeral 3.2 de esta Cláusula, deben contar con al menos dos (2) certificaciones en seguridad de la información o seguridad informática reconocidas internacionalmente, quienes se encargarán de ejecutar el plan de trabajo derivado de esta contratación, debiendo acreditar, adicionalmente, que cuenta con al menos un (1) profesional del equipo de especialistas con al menos una (1) certificación en Ethical Hacking reconocida internacionalmente; para tal efecto debe presentar, hojas de vida, y que además acrediten la experiencia en los últimos cinco (5) años realizando consultorías similares al objeto de este Contrato dentro o fuera del país, formación académica y nivel profesional del personal que asignará para el desarrollo de la consultoría.

El Gerente de Proyecto además debe contar con título universitario (pregrado o posgrado) en: Gestión de Proyectos, o carreras afines o contar con certificación en gestión de proyectos PMP emitida por el Project Management Institute (PMI) o certificación similar.

Las hojas de vida de cada uno los profesionales que conformarán el equipo de especialistas deben incluir al menos lo siguiente:

3.1.1 Nombres completos.
3.1.2 Profesión universitaria y certificaciones vigentes que ostenta.
3.1.3 Años de experiencia realizando consultorías similares al objeto de este Contrato.
3.1.4 Proyectos o consultorías en las que ha trabajado en los últimos cinco (5) años.
3.1.5 Al menos uno (1) de los consultores debe ostentar certificaciones en Ethical Hacking.
3.1.6 Documentación como ser: copia de títulos profesionales, diplomas y certificaciones que avalen sus competencias.

4. Plan de Trabajo

El plan de trabajo debe tener un detalle pormenorizado de las actividades y entregables de cada una de las siguientes fases (según como se establece en el numeral 1. de esta Cláusula):

0	Kickoff del proyecto y plan de trabajo
I	SWIFT (Programa de Seguridad al Cliente)
II	Servicios en DMZ (internet y extranet)
III	Sistemas que soportan procesos críticos
IV	Red interna, concientización en ciberseguridad, SWIFT y cierre del proyecto

Una vez aprobado el plan de trabajo, el Departamento de Gestión de Riesgos, realizará la gestión correspondiente ante el Departamento de Tecnología y Comunicaciones requiriendo la participación a demanda de especialistas técnicos, para apoyar conforme su competencia durante el desarrollo de la consultoría. La metodología utilizada para la actividad debe ser acorde a estándares internacionales, utilizando como referencia mínima según corresponda por fase lo desarrollado por el NIST respecto al marco de ciberseguridad (CSF) y sus cinco funciones: identificar, proteger, detectar, responder y recuperar, pudiendo ser el manual metodológico abierto de pruebas de seguridad (OSSTMM), Marco de evaluación de seguridad de sistemas de información (ISSAF) y la Guía de Pruebas OWASP u otras que **"EL CONSULTOR"** considere apropiadas y que incluya el uso de metodologías para realizar hacking ético; siempre apegado a mejores prácticas internacionales, el marco de evaluación externa independiente (Independent Assessment Framework - IAF) de SWIFT, según corresponda para cada una de las fases.

CLÁUSULA SÉPTIMA
OBLIGACIONES GENERALES Y ESPECIALES DEL CONTRATO

1. Lugar y Documentos de Trabajo:

1.1 Para el desarrollo de la consultoría, **"EL CONSULTOR"** debe realizar al menos cuatro (4) visitas en sitio en la ciudad de Tegucigalpa, Honduras para ejecutar los trabajos que le permitan desarrollar las actividades propias de cada fase o trimestre, con el fin de desarrollar el análisis de vulnerabilidades y hacking ético a redes internas y externas y sistemas de procesos críticos, plan de acción para remediación basado en los riesgos identificados y seguimiento a las remediaciones de cada fase; el tiempo de la estadía por cada visita en sitio será al menos de veinte (20) días hábiles programados según el plan de trabajo homologado y aprobado por **"EL BANCO"**, a excepción de la primera visita que será al menos de veinticinco (25) días hábiles siendo que incluye lo relativo a la planificación del proyecto.

A continuación, el detalle:

Visita	Actividad	Días hábiles
1	Kickoff del proyecto, plan de trabajo (fase 0) y ejecución de fase I y remediación.	Veinticinco (25)
2	Ejecución de fase II, remediación y seguimiento fase anterior.	Veinte (20)
3	Ejecución de fase III, remediación y seguimiento a fases anteriores.	Veinte (20)
4	Ejecución de fase IV, remediación, seguimiento a fases anteriores y cierre de proyecto.	Veinte (20)

Cuando **"EL CONSULTOR"** no se encuentre en las instalaciones de **"EL BANCO"**, este podrá brindar respuesta a consultas realizadas por **"EL BANCO"**, seguimiento de las actividades, entre otras, a través de correo electrónico, reuniones basadas en video conferencias o plataformas web.

1.2 **"EL CONSULTOR"** durante su estadía en las oficinas de **"EL BANCO"** debe sujetarse a las disposiciones administrativas de **"EL BANCO"** relativas a la seguridad física, seguridad de la información y de movilización dentro de la Institución.

1.3 **"EL BANCO"** suministrará a **"EL CONSULTOR"** toda la documentación física o en formato digital que requiere de acuerdo al alcance de esta consultoría; **"EL CONSULTOR"** debe designar una (1) persona responsable para recibir dicha documentación.

1.4 **"EL CONSULTOR"** se comprometerá a utilizar la documentación que le proporcione **"EL BANCO"** con absoluta confidencialidad; para lo cual, se obligará a que su revisión se efectúe dentro de las instalaciones de **"EL BANCO"**, en el local que para tal fin le será asignado o por la naturaleza del servicio podrá ser revisada fuera de las instalaciones de **"EL BANCO"** aplicando controles de seguridad para mantener la confidencialidad requerida, para lo cual, deberá suscribir un Acuerdo de Confidencialidad.

1.5 Dicho acuerdo debe ser firmado por el Representante Legal de la empresa de **"EL CONSULTOR"**, a favor de la misma y de manera individual, lo firmará cada uno de los especialistas asignados; dicho documento debe ser autenticado por Notario; por lo anterior **"EL CONSULTOR"** es responsable por daños y perjuicios que ocasione a **"EL BANCO"** cualquier revelación no autorizada.

2. **Obligaciones Laborables:**

2.1. **"EL CONSULTOR"** deberá asumir en forma directa y exclusiva, en su condición de patrono, todas las obligaciones laborales y de seguridad social con las personas que designe y cualquier otro personal relacionado para desarrollar y cumplir las labores objeto de este Contrato, eximiendo completamente y en forma incondicional a **"EL BANCO"** de toda responsabilidad laboral derivada de la relación contractual, incluso en caso de accidentes de trabajo o enfermedad profesional y además a responder por cualquier daño o deterioro que en ocasión de la ejecución de los trabajos se cause a los bienes, valores e imagen de la Institución.

2.2. En caso de ausencia temporal o definitiva de alguna de las personas asignadas por **"EL CONSULTOR"**, ésta debe ser sustituida de inmediato a fin de mantener el mismo número y calidad de consultores propuestos; en estos casos, **"EL CONSULTOR"** debe cumplir durante la vigencia de contrato, lo siguiente:

2.2.1. De presentarse la necesidad de hacer algún cambio en el personal designado o agregar nuevos consultores, durante la vigencia de presente contrato, **"EL CONSULTOR"** debe notificarlo con anticipación con al menos diez (10) días calendario, salvo excepciones de fuerza mayor y debidamente justificadas al Departamento de Adquisiciones y Bienes Nacionales de **"EL BANCO"**; quien lo turnará para la validación del perfil y competencias requeridas al Coordinador General de este Proyecto de **"EL BANCO"**, adscrito al Departamento de Gestión de Riesgos.

2.2.2. **"EL CONSULTOR"** se obliga en casos de ausencia temporal o definitiva de sus labores de una o más personas asignadas, a sustituirlos conforme lo indicado en el numeral que precede con el perfil requerido por **"EL BANCO"** a fin de que se mantenga el mismo número y calidad de consultores propuestos.

2.2.3. Todo cambio en el personal asignado al servicio debe ser previamente aprobado por **"EL BANCO"**.

2.2.4. **"EL BANCO"** se reserva el derecho de objetar al personal designado por **"EL CONSULTOR"**, si éstos no cumplen con las capacidades técnicas, disposiciones administrativas internas relativas a la seguridad, movilización y comportamiento adecuado, pudiendo exigir su reemplazo.

CLÁUSULA OCTAVA
COORDINACIÓN Y SUPERVISIÓN

1. **"EL BANCO"** designará un equipo de trabajo conformado por un Coordinador General del Proyecto y Gerente de Proyecto adscritos al Departamento de Gestión de Riesgos; también lo integrarán especialistas técnicos adscritos a los departamentos de Gestión de Riesgos y Tecnología y Comunicaciones, el Coordinador General del Proyecto de **"EL BANCO"** será el responsable de la supervisión y seguimiento de la consultoría y en conjunto con el Gerente de Proyecto brindar la aceptación y aprobación por parte de **"EL BANCO"** de los entregables por cada fase emitiendo y suscribiendo las correspondientes actas de aceptación, mismas que servirán de soporte para ejecutar los pagos respectivos.

2. La notificación a **"EL CONSULTOR"** de los nombres de los empleados de **"EL BANCO"** que conformarán el equipo de trabajo estará a cargo de la Jefatura del Departamento de Gestión de Riesgos, quien la realizará máximo un (1) día hábil posterior a la notificación de la orden de inicio para la consultoría por parte de **"EL BANCO"** posterior a la suscripción y aprobación del presente contrato.

3. El Gerente de Proyecto será el responsable de la gestión de aspectos técnicos para el desarrollo del trabajo objeto de este Contrato; asimismo, proporcionará a **"EL CONSULTOR"** la información física o en medio electrónico necesaria para el desarrollo de la consultoría. En caso de ausencia del Gerente de Proyecto o Coordinador General del Proyecto de **"EL BANCO"**, serán sustituidos por el representante en funciones que el Departamento de Gestión de Riesgos de **"El BANCO"** designe en cada rol, realizando las funciones que a éstos le competen durante el tiempo de la ausencia.

4. En el caso de determinarse incumplimiento en las obligaciones indicadas en las cláusulas contractuales, el Coordinador General del Proyecto de **"EL BANCO"** notificará a **"EL CONSULTOR"**, a través del Departamento de Adquisiciones y Bienes Nacionales, las observaciones o reclamos a que hubiere lugar; si estos no fueren atendidos dentro del plazo que se le señale para tal efecto **"EL BANCO"**, además de aplicar la multa estipulada en este Contrato, pudiendo considerarse la resolución total del mismo.

CLÁUSULA NOVENA
OBLIGACIONES LABORALES DE "EL CONSULTOR"

"EL CONSULTOR" asume en forma directa y exclusiva en su condición de patrono, todas las obligaciones laborales y de seguridad social con las personas que designe y cualquier otro personal relacionado para desarrollar y cumplir las labores objeto de este Contrato, eximiendo completamente y en forma incondicional a **"EL BANCO"** de toda responsabilidad laboral derivada de la relación contractual, incluso en caso de accidentes de trabajo o enfermedad profesional y además a responder por cualquier daño o deterioro que en ocasión de la ejecución de los trabajos se cause a los bienes, valores e imagen de **"EL BANCO"**, durante la vigencia del presente Contrato.

CLÁUSULA DÉCIMA
GARANTÍA DE CUMPLIMIENTO

Para garantizar la buena ejecución y fiel cumplimento de todas y cada una de las cláusulas del presente Contrato, **"EL BANCO"** retendrá a **"EL CONSULTOR"** en calidad de Garantía de Cumplimiento de Contrato el diez por ciento (10%) de cada pago parcial en concepto de honorarios, que se efectué a **"EL CONSULTOR"**.

Dicho valor será devuelto a **"EL CONSULTOR"** conforme lo dispone el Artículo 106 de la Ley de Contratación del Estado, después de recibido a satisfacción el Informe final y demás documentos detallados en la Cláusula Sexta de este Contrato.

CLÁUSULA DÉCIMA PRIMERA
PENAL

Sin perjuicio del cumplimiento del presente Contrato por parte de **"EL CONSULTOR"**, por las demoras no justificadas en la prestación del servicio objeto del presente Contrato o el incumplimiento de cualquier otra cláusula que **"EL BANCO"** estime de suma trascendencia, éste aplicará una multa por cada día calendario de retraso, conforme lo establecido en las Disposiciones Generales del Presupuesto de Ingresos y Egresos de la República vigentes al momento del incumplimiento, sin perjuicio del cumplimiento de las demás obligaciones a cargo de **"EL CONSULTOR"** u otra disposición legalmente aplicable.

Si la demora no justificada diese lugar a que el pago acumulado por la multa aquí establecida excediera del diez por ciento (10%) del valor de este Contrato, **"EL BANCO"** podrá considerar la resolución total del mismo y sin más trámite hacer efectiva la Garantía de Cumplimiento, excepto en los casos en que el área técnica de **"EL BANCO"** recomiende la continuidad de la ejecución del Contrato.

CLÁUSULA DÉCIMA SEGUNDA
CESIÓN DEL CONTRATO O SUBCONTRATACIÓN

No se permitirá la cesión ni la subcontratación, por consiguiente, es entendido por las partes que **"EL CONSULTOR"** no podrá transferir, asignar, cambiar, modificar, traspasar su derecho de recibir pagos o tomar cualquier disposición que se refiera al Contrato, sin previo consentimiento por escrito de **"EL BANCO"**. Si así sucediese, la cesión o subcontratación, será considerada como incumplimiento del mismo.

CLÁUSULA DÉCIMA TERCERA
RESOLUCIÓN DEL CONTRATO

"EL BANCO" ejercerá su derecho para resolver o dar por terminado el presente Contrato en los siguientes casos:

a) El grave o reiterado incumplimiento de las cláusulas convenidas por parte de **"EL CONSULTOR"**.

b) La sentencia firme emitida por tribunal competente en la cual se declare que la empresa, su representante o socios están comprendidos en alguna de las inhabilidades, prohibiciones, ni situaciones irregulares a que se refiere la Ley Especial Contra el Lavado de Activos y la demás legislación que rige la materia.

c) La disolución de la sociedad mercantil.

d) La declaración de quiebra o de suspensión de pagos de **"EL CONSULTOR"** o su comprobada incapacidad financiera.

e) Los motivos de interés público o las circunstancias imprevistas calificadas como caso fortuito o fuerza mayor, sobrevivientes a la celebración de Contrato, que imposibiliten o agraven desproporcionalmente su ejecución.

f) El mutuo acuerdo de las partes.

g) En caso de recorte presupuestario de fondos nacionales, que se efectúe por razón de la situación económica y financiera del país, la estimación de la percepción de ingresos menor a los gastos proyectados y en caso de necesidades imprevistas o de emergencia, de conformidad con las Disposiciones Generales del Presupuesto vigentes.

h) Las demás que establezca expresamente este Contrato y la Ley de Contratación del Estado y su Reglamento.

"EL BANCO" podrá en cualquier momento resolver el Contrato, sin que mediare fuerza mayor, si **"EL CONSULTOR"** incumpliera de manera relevante alguna de las obligaciones que asume y que sean significativas para la adecuada prestación de los servicios derivados del presente Contrato.

En especial, sin que esta enumeración sea taxativa, constituyen causales de incumplimiento del Contrato por **"EL CONSULTOR"** las siguientes:

a) La transferencia, aunque fuese parcial, de las obligaciones que asume sin previa autorización de **"EL BANCO"**.

b) La inobservancia de las condiciones generales y especiales del Contrato.

c) Las demás que establezca expresamente este Contrato, la Ley de Contratación del Estado y su Reglamento.

La notificación de la resolución del Contrato se hará por escrito, a partir de la cual se considerará efectiva la misma, explicando en la nota los motivos en que tal acción se fundamenta.

CLÁUSULA DÉCIMA CUARTA
DOCUMENTOS INTEGRANTES DEL CONTRATO

Forman parte de este Contrato y forman un sólo cuerpo con idéntica fuerza de ley entre las partes, los documentos siguientes:

a) Los Términos de Referencia que rigen el Concurso Privado No.02/2021, sus anexos y enmiendas.

b) La Oferta Técnica y Económica presentada por **"EL CONSULTOR"**;

c) Resolución No.580-11/2021 del 25 de noviembre de 2021 emitida por el Directorio de esta Institución.

d) Los demás documentos complementarios que se hayan originado de esta transacción y en general toda la correspondencia que se gire entre las partes contratantes.

CLÁUSULA DÉCIMA QUINTA
MEDIDAS DE SEGURIDAD, CONFIDENCIALIDAD Y AUDITORÍA

Considerando la naturaleza de la información por suministrarse, así como a la que tendrá acceso como resultado del Contrato, **"EL CONSULTOR"** y en general el personal que designe para la ejecución del contrato, se comprometen a mantener en absoluta confidencialidad y a abstenerse de divulgar, publicar o comunicar la información, configuraciones técnicas, manuales y procedimientos propiedad de **"EL BANCO"** a las cuales eventualmente tenga acceso durante la ejecución de su trabajo, siendo responsables por los daños y perjuicios que por la divulgación de la misma pueda acarrear **"EL BANCO"**.

"EL BANCO" se reserva el derecho de realizar auditorías por parte de terceros o personal interno, sobre los servicios suministrados por **"EL CONSULTOR"**.

"EL CONSULTOR" se obliga a cumplir con todas las medidas de seguridad que **"EL BANCO"** tiene establecidas, para cuyo propósito acatará lo indicado por el Departamento de Seguridad de **"EL BANCO"**, a efecto de instruir a su personal sobre el cumplimiento de tales medidas.

CLÁUSULA DÉCIMA SEXTA
CASO FORTUITO O FUERZA MAYOR

El incumplimiento parcial o total sobre las obligaciones que le corresponden a **"EL CONSULTOR"**, de acuerdo con el presente Contrato, no será considerado como tal, si a juicio de **"EL BANCO"** es atribuible a caso fortuito o fuerza mayor, debidamente justificado.Se entenderá por fuerza mayor o caso fortuito, todo acontecimiento que no ha podido preverse o que, previsto, no ha podido resistirse y que impide el exacto incumplimiento de las obligaciones contractuales, tales como: catástrofes provocadas por fenómenos naturales, accidentes, huelgas, guerras, revoluciones o sediciones, naufragio e incendios.

CLÁUSULA DÉCIMA SÉPTIMA
VALIDEZ Y APROBACIÓN DEL CONTRATO

El presente Contrato requerirá la aprobación del Directorio de **"EL BANCO"** para su validez; asimismo, requerirá la aprobación del Congreso Nacional en caso de producir o prolongar sus efectos al siguiente período de Gobierno.

CLÁUSULA DÉCIMA OCTAVA
JURISDICCION Y COMPETENCIA

Para definir cualquier situación controvertida que no pudiere solucionarse conciliatoriamente, ambas partes expresamente se someten a la jurisdicción y competencia del juzgado correspondiente del Departamento de Francisco Morazán.

CLÁUSULA DÉCIMA NOVENA
NORMAS APLICABLES

Lo no previsto en el presente Contrato, se regulará por las normas contenidas en la Constitución de la República, la Ley de Contratación del Estado y su Reglamento, las Normas que Rigen la Contratación y Adquisición de Bienes y Servicios del Banco Central de Honduras, lo previsto en las resoluciones números 406-8/2021 y 580-11/2021 del 12 de agosto y 25 de noviembre de 2021, respectivamente, los Términos de Referencia del Concurso Privado No.02/2021, y la demás legislación que rige la materia.

Para constancia y ante testigos, suscribimos el presente Contrato en tres (3) ejemplares de un mismo contenido, en la ciudad de Tegucigalpa, Municipio del Distrito Central, a los veintidós (22) días del mes de diciembre del año dos mil veintiuno (2021).

ARACELY O'HARA GUILLÉN
"EL BANCO"
BANCO CENTRAL DE HONDURAS

OLGA MARINA VALLADARES MONCADA
"EL CONSULTOR"
SISTEMAS APLICATIVOS SISAP, S.A.

CARLOS ALBERTO VIJIL VERDE
TESTIGO

NICOLLE BARAHONA ZAVALA
TESTIGO